W tej części przyjrzymy się różnym aspektom hakowania systemu. Jak pamiętasz z Części III, cykl hakowania systemu składa się z sześciu kroków. Pierwszy etap - wyliczenie - omówiono w poprzedniej części. Ta część obejmuje pięć pozostałych kroków:

* Łamanie haseł

* Eskalacja uprawnień

* Wykonywanie aplikacji

* Ukrywanie plików

* Zakrywanie śladów

Najprostszy sposób na zdobycie hasła

Wiele prób hakerskich rozpoczyna się od uzyskania hasła do systemu docelowego. Hasła to kluczowa informacja potrzebna do uzyskania dostępu do systemu, a użytkownicy często wybierają hasła łatwe do odgadnięcia. Wiele haseł do ponownego wykorzystania lub wybiera takie, które są proste - takie jak imiona zwierząt domowych - aby pomóc im je zapamiętać. Z powodu tego czynnika ludzkiego większość zgadywania haseł jest skuteczna, jeśli znane są pewne informacje o celu. Gromadzenie i rozpoznawanie informacji może pomóc w uzyskaniu informacji, które pomogą hakerowi odgadnąć hasło użytkownika. Odgadnięcie lub złamanie hasła może być punktem uruchamiania eskalacji uprawnień, uruchamiania aplikacji, ukrywania plików i zakrywania śladów. Jeśli zgadywanie hasła nie powiedzie się, hasła mogą zostać złamane ręcznie lub za pomocą automatycznych narzędzi, takich jak słownik lub metoda brute-force, z których każda jest omówiona później.

Rodzaje haseł

Kilka rodzajów haseł służy do zapewnienia dostępu do systemów. Znaki tworzące hasło mogą należeć do dowolnej z tych kategorii:

* Tylko litery

* Tylko cyfry

*N Tylko znaki specjalne

* Litery i cyfry

* Tylko litery i znaki specjalne

* Tylko cyfry i znaki specjalne

* Litery, cyfry i znaki specjalne

Silne hasło jest mniej podatne na atak hakera. Podczas tworzenia hasła należy stosować następujące zasady, aby chronić je przed atakami:

* Nie może zawierać żadnej części nazwy konta użytkownika

* Musi mieć co najmniej osiem znaków

* Musi zawierać znaki z co najmniej trzech z następujących kategorii:

* symbole niealfanumeryczne ($,: "% @! #)

*Numery

* Duże litery

* Małe litery

Haker może używać różnych rodzajów ataków, aby zidentyfikować hasło i uzyskać większy dostęp do systemu. Rodzaje ataków haseł są następujące:

Pasywny Tryb Online : Podsłuch w sieciowej wymianie haseł. Pasywne ataki online obejmują ataki sniffing, man-in-the-middle i ataki powtórzeniowe.

Aktywny tryb online : Odgadywanie hasła administratora. Aktywne ataki online obejmują zautomatyzowane zgadywanie haseł.

Ataki w trybie offline : ataki słownikowe, hybrydowe i brut-force.

Nieelektroniczne surfowanie przez ramię, sniffing klawiatury i inżynieria społeczna.

Przyjrzymy się każdemu z tych ataków bardziej szczegółowo w poniższych sekcjach.

Pasywne ataki online

Pasywny atak online jest również znany jako sniffowanie hasła w sieci przewodowej lub bezprzewodowej. Pasywny atak nie jest wykrywalny dla użytkownika końcowego. Hasło jest przechwytywane podczas procesu uwierzytelniania i może zostać porównane z plikiem słownika lub listy słów. Hasła do kont użytkowników są zwykle mieszane lub szyfrowane, gdy są wysyłane w sieci, aby zapobiec nieautoryzowanemu dostępowi i użyciu. Jeśli hasło jest chronione za pomocą szyfrowania lub mieszania, do przełamania algorytmu można użyć specjalnych narzędzi w pakiecie narzędzi hakera. Kolejny pasywny atak online znany jest jako man-in-the-middle (MITM). W ataku MITM haker przechwytuje żądanie uwierzytelnienia i przekazuje je na serwer. Wstawiając sniffer pomiędzy klientem a serwerem, haker jest w stanie wykryć oba połączenia i przechwycić hasła w procesie. Atak powtórzeń jest również pasywnym atakiem online; Występuje, gdy haker przechwytuje hasło w drodze do serwera uwierzytelniania, a następnie przechwytuje i ponownie wysyła pakiety uwierzytelniające w celu późniejszego uwierzytelnienia. W ten sposób haker nie musi łamać hasła ani uczyć się hasła poprzez MITM, ale przechwytuje hasło i ponownie wykorzystuje pakiety uwierzytelniające hasła w celu uwierzytelnienia się jako klient.

Aktywne ataki online

Najłatwiejszym sposobem uzyskania dostępu do systemu na poziomie administratora jest odgadnięcie prostego hasła przy założeniu, że administrator użył prostego hasła. Zgadywanie hasła to aktywny atak online. Opiera się na czynniku ludzkim związanym z tworzeniem haseł i działa tylko przy słabych hasłach. W części 3, kiedy omawialiśmy fazę enumeracji hakowania w systemie, nauczyłeś się o lukach w enumeracji NetBIOS i sesjach zerowych. Zakładając, że port NetBIOS TCP 139 jest otwarty, najskuteczniejszą metodą włamania się do systemu Windows NT lub Windows 2000 jest zgadywanie hasła. Odbywa się to poprzez próbę połączenia z wyliczonym udziałem (IPC $ lub C $) i próbą połączenia nazwy użytkownika i hasła. Najczęściej używanymi kombinacjami konta i hasła administratora są słowa takie jak Admin, Administrator, Sysadmin lub Password lub hasło puste. Haker może najpierw spróbować połączyć się z domyślnym udziałem Admin $, C $ lub C: \ Windows. Aby połączyć się z ukrytym udziałem dysku C: na przykład, wpisz następujące polecenie w polu Uruchom (Start ➪ Uruchom): \\ adres_IP \ c $

Zautomatyzowane programy mogą szybko generować pliki słowników, listy słów lub każdą możliwą kombinację liter, cyfr i znaków specjalnych, a następnie próbować zalogować się przy użyciu tych

poświadczeń. Większość systemów zapobiega tego typu atakom, ustawiając maksymalną liczbę prób logowania w systemie, zanim konto zostanie zablokowane. W następnych sekcjach omówimy, w jaki sposób hakerzy mogą ściślej odgadywać hasła, a także sposoby przeciwdziałania takim atakom.

Wykonywanie automatycznego odgadywania hasła

Aby przyspieszyć zgadywanie hasła, hakerzy korzystają z automatycznych narzędzi. Łatwym procesem automatyzacji zgadywania hasła jest użycie poleceń powłoki systemu Windows opartych na standardowej składni NET USE. Aby utworzyć prosty, zautomatyzowany skrypt zgadywania haseł, wykonaj następujące czynności:

1. Utwórz prosty plik nazwy użytkownika i hasła za pomocą Notatnika Windows. Zautomatyzowane narzędzia, takie jak Generator Słowników, są dostępne do utworzenia tej listy słów. Zapisz plik na dysku C: jako credentials.txt.

2. Wywołaj ten plik za pomocą polecenia FOR:

C: \> FOR / F "token = 1, 2 *"% i in (credentials.txt)

3. Wpisz net use \\ targetIP \ IPC $% i / u:% j, aby użyć pliku credentials.txt, aby zalogować się do ukrytego zasobu w systemie docelowym

Innym przykładem użycia przez atakującego polecenia FOR jest wyczyszczenie zawartości dysku twardego za pomocą zer przy użyciu składni komend ((i = 0; i <11; i ++)); wykonaj dd jeśli = / dev / random z = / dev / hda && dd if = / dev / zero of = dev / hda done. Polecenie czyszczenia może być również użyte do wyczyszczenia danych z twardego dysku za pomocą polecenia $ wipe -fik / dev / hda1.

Obrona przed odgadnięciem hasła

Istnieją dwie opcje obrony przed zgadywaniem haseł i atakami hasłami. Zarówno karty inteligentne, jak i dane biometryczne dodają warstwę bezpieczeństwa do niepewności związanej z tworzeniem przez użytkowników własnych haseł. Użytkownik może również zostać uwierzytelniony i zweryfikowany za pomocą danych biometrycznych. Dane biometryczne wykorzystują cechy fizyczne, takie jak odciski palców, skanowanie geometrii dłoni i skanowanie siatkówki jako dane uwierzytelniające użytkowników. Zarówno karty inteligentne, jak i biometryczne wykorzystują uwierzytelnianie dwuskładnikowe, które wymaga dwóch form identyfikacji (takich jak rzeczywista karta inteligentna i hasło) podczas sprawdzania użytkownika. Wymagając czegoś, co fizycznie posiada użytkownik (w tym przypadku karta inteligentna) i coś, co użytkownik zna (hasło), zwiększa się bezpieczeństwo, a proces uwierzytelniania nie jest podatny na ataki haseł. RSA Secure ID to dwuskładnikowy system uwierzytelniania, który wykorzystuje token i hasło.

Ataki offline

Ataki w trybie offline są wykonywane z lokalizacji innej niż rzeczywisty komputer, na którym znajdują się lub były używane hasła. Ataki offline zazwyczaj wymagają fizycznego dostępu do komputera i kopiowania pliku haseł z systemu na nośniki wymienne. Hacker przenosi wtedy plik do innego komputera, aby wykonać łamanie. Istnieje kilka rodzajów ataków haseł offline, jak widać w Tabeli 4.1.

Rodzaj ataku	Cechy	Przykładowe hasło
Atak słownikowy	Próby użycia haseł z listy słowa słownika	Administrator
Atak hybrydowy	Zastępuje liczbę symboli dla znaków hasła	Administrator

Atak Brute-Force Rozwiązuje wszystkie możliwe kombinacje

liter, liczby i znaki specjalne Ms! Tr245 @ F5a

Atak słownikowy to najprostszy i najszybszy rodzaj ataku. Służy do identyfikacji a hasło, które jest rzeczywistym słowem, które można znaleźć w słowniku. Najczęściej atak wykorzystuje plik słownika możliwych słów, który jest mieszany przy użyciu tego samego algorytmu, co w procesie uwierzytelniania. Następnie zaszyfrowane słowa są porównywane z hasłami podczas logowania użytkownika lub z hasłami przechowywanymi w pliku na serwerze. Atak słownikowy działa tylko wtedy, gdy hasło jest rzeczywistym słowem słownikowym; dlatego ten rodzaj ataku ma pewne ograniczenia. Nie można jej używać przeciwko silnym hasłom zawierającym liczby lub inne symbole. Atak hybrydowy to kolejny poziom ataku hakera, jeśli nie można znaleźć hasła przy użyciu ataku słownikowego. Atak hybrydowy rozpoczyna się od pliku słownika i zastępuje liczby i symbole znaków w haśle. Na przykład wielu użytkowników dodaje numer 1 na końcu hasła, aby spełnić wysokie wymagania dotyczące hasła. Hybrydowy atak ma na celu znalezienie tych typów anomalii w hasłach. Najbardziej czasochłonnym typem ataku jest brute-force, który próbuje wszystkich możliwych kombinacja wielkich i małych liter, cyfr i symboli. Atak brute-force jest najwolniejszym z trzech rodzajów ataków z powodu wielu możliwych kombinacji znaków w haśle. Jednak brute-force jest skuteczna; mając wystarczająco dużo czasu i mocy obliczeniowej, można ostatecznie zidentyfikować wszystkie hasła.

Tęczowa tabela to lista słów słownikowych, które zostały już zhashowane. Tęczowe tabele mogą przyspieszyć wykrywanie i łamanie haseł poprzez wstępne obliczanie skrótów dla wspólnych ciągów znaków. Na przykład tablica tęczowa może zawierać znaki od a do z lub od A do Z. Zasadniczo narzędzia tęczowe są hashami. Tradycyjny cracker brute-force wypróbuje kolejno wszystkie możliwe hasła w postaci zwykłego tekstu. W ten sposób łamanie skomplikowanych haseł jest czasochłonne. Ideą tabel tęczowych jest wcześniejsze wykonanie obliczeń czasu łamania.

Ataki nieelektroniczne

Ataki nieelektroniczne - lub nietechniczne - to ataki, które nie wykorzystują żadnej technicznej wiedzy ani umiejętności. Ten rodzaj ataku może obejmować socjotechnikę, surfowanie prze ramię, sniffowanie klawiatury i nurkowanie w śmietniku. Inżynieria społeczna to sztuka interakcji z ludźmi twarzą w twarz lub przez telefon i dostarczania im wartościowych informacji, takich jak hasła. Inżynieria społeczna opiera się na dobrej naturze ludzi i chęci pomagania innym. Wiele razy helpdesk jest celem ataku socjotechnicznego, ponieważ jego zadaniem jest pomaganie ludziom - a odzyskiwanie lub resetowanie haseł jest wspólną funkcją działu pomocy technicznej. Najlepszą obroną przed atakami socjotechnicznymi jest szkolenie w zakresie świadomości bezpieczeństwa dla wszystkich pracowników oraz procedury bezpieczeństwa dotyczące resetowania haseł. Surfing przez ramię polega na przeglądaniu przez czyjeś ramię podczas wpisywania hasła. Może to być skuteczne, gdy haker znajduje się w pobliżu użytkownika i systemu. Specjalne ekrany, które utrudniają oglądanie ekranu komputera pod kątem, mogą zmniejszyć obciążenie podczas surfowania przez ramię. Ponadto świadomość i szkolenie pracowników może praktycznie wyeliminować ten rodzaj ataku.

Surfowanie przez ramię

Sue jest recepcjonistką w gabinecie zajętego lekarza. Pracowała przy swoim komputerze, kiedy do biura wszedł pracownik dostarczający kwiaty. Powiedział Sue, że ma dostawę kwiatów dla doktora Smitha. To było nazwisko doktora, które zobaczył na drzwiach biura, gdy wszedł do poczekalni. Sue była zajęta tego dnia, a doktor Smith był z pacjentem, więc powiedziała czlowiekowi że może zostawić

kwiaty na biurku, a ona upewni się, że lekarz je otrzymał. Powiedział, że musi poczekać i przekazać je bezpośrednio osobie wymienionej na liście przewozowym. Tak więc, Sue poprosiła go, aby został w poczekalni, dopóki Dr. Smith nie będzie mógł odebrać kwiatów. Kiedy Sue wróciła do swojego komputera, aby zakończyć pisanie e-maila, który zaczęła, była rozproszona myślą o pracy, którą miała przed sobą. Szybko wpisała hasło, aby odblokować stację roboczą Windows. Człowiek dostarczający kwiaty zatrzymał się na chwilę, po czym odwrócił się i usiadł w poczekalni. Kiedy zatrzymał się, był w stanie zobaczyć pięcioznakowe hasło Sue wpisane, aby odblokować ekran. W ten sposób był w stanie rozpoznać jej hasło i kontynuować proces hakerski. Hasło zostało zebrane za pomocą surfingu przez ramię, formy inżynierii ispołecznej. Hakerzy nurkujący na śmietniku przeglądają kosz w poszukiwaniu informacji, takich jak hasła, które można zapisać na kartce papieru. Ponownie, szkolenie w zakresie świadomości bezpieczeństwa dotyczące niszczenia ważnych dokumentów może uniemożliwić hakerowi zbieranie haseł przez nurkowanie na śmietniku.

Łamanie hasła

Ręczne łamanie haseł polega na próbie zalogowania się przy użyciu różnych haseł. Haker wykonuje następujące czynności:

1. Znajdź prawidłowe konto użytkownika (takie jak Administrator lub Gość).

2. Utwórz listę możliwych haseł.

3. Ranga haseł od wysokiego do niskiego prawdopodobieństwa.

4. Wprowadź każde hasło.

5. Spróbuj ponownie, dopóki nie zostanie znalezione pomyślne hasło.

Haker może również utworzyć plik skryptu, który próbuje każdego hasła na liście. Jest to nadal uważane za łamanie ręczne, ale jest czasochłonne i zazwyczaj nieskuteczne. Bardziej skutecznym sposobem złamania hasła jest uzyskanie dostępu do pliku haseł w systemie. Większość systemów hashuje (szyfruje jednokierunkowo) hasło do przechowywania w systemie. Podczas logowania hasło wprowadzane przez użytkownika jest mieszane za pomocą tego samego algorytmu, a następnie porównywane z hashami przechowywanymi w pliku. Haker może próbować uzyskać dostęp do algorytmu mieszania przechowywanego na serwerze, zamiast próbować odgadnąć lub w inny sposób zidentyfikować hasło. Jeśli zakończy się powodzeniem, może odszyfrować hasła przechowywane na serwerze. Hasła są przechowywane w pliku Security Accounts Manager (SAM) w systemie Windows oraz w pliku shadow password w systemie Linux.

Narzędzia hakerskie

Legion automatyzuje zgadywanie haseł w sesjach NetBIOS. Legion skanuje wiele zakresów adresów IP dla Windows, a także oferuje ręczne narzędzie do ataku słownikowego. NTInfoScan to skaner bezpieczeństwa dla NT 4.0. Ten skaner luk w zabezpieczeniach generuje raport oparty na języku HTML na temat problemów bezpieczeństwa znalezionych w systemie docelowym i innych informacji. L0phtCrack to pakiet do kontroli i odzyskiwania haseł dystrybuowany przez oprogramowanie @stake, które jest obecnie własnością firmy Symantec. Wykonuje przechwytywania pakietów Server Message Block (SMB) w lokalnym segmencie sieci i przechwytuje indywidualne sesje logowania. L0phtCrack zawiera funkcje słownika, brutalnej siły i hybrydowego ataku. Firma Symantec niedawno zaprzestała opracowywania narzędzia L0phtCrack, ale nadal można je znaleźć w Internecie. LC5 to kolejne dobre narzędzie do łamania haseł. LC5 jest odpowiednim zamiennikiem L0phtCrack. John the Ripper to narzędzie wiersza poleceń zaprojektowane do łamania haseł Unix i NT. Łamane hasła nie uwzględniają

wielkości liter i mogą nie odzwierciedlać rzeczywistego hasła o mieszanym zakresie. KerbCrack składa się z dwóch programów: kerbsniff i kerbcrack. Sniffer nasłuchuje w sieci i rejestruje loginy Kerberos Windows 2000 / XP. Kraker możne użyć go do znalezienia haseł z pliku przechwytywania za pomocą ataku brute-force lub ataku słownikowego.

Zrozumienie skrótu LAN Managera

System Windows 2000 wykorzystuje hashowanie NT LAN Manager (NTLM) do zabezpieczania haseł podczas przesyłania w sieci. W zależności od hasła, mieszanie NTLM może być słabe i łatwe do złamania. Na przykład załóżmy, że hasło to 123456abcdef. Gdy to hasło jest szyfrowane przy użyciu algorytmu NTLM, jest ono najpierw konwertowane na wielkie litery: 123456ABCDEF. Hasło jest wypełnione znakami pustymi (puste), aby mieć 14 znaków: 123456ABCDEF__. Przed zaszyfrowaniem hasła 14-znakowy łańcuch dzieli się na pół: 123456A i BCDEF__. Każdy ciąg jest szyfrowany indywidualnie, a wyniki są łączone:

123456A = 6BF11E04AFAB197F

BCDEF__ = F1E9FFDCC75575B15

Hash to 6BF11E04AFAB197FF1E9FFDCC75575B15.

Pierwsza połowa hasła zawiera znaki alfanumeryczne; L0pht- Crack zajmie 24 godziny, aby złamać tę część. Druga połowa zawiera tylko litery i symbole, a złamanie zajmie 60 sekund. Wynika to z faktu, że w drugiej połowie hashowanego hasła istnieje o wiele mniej kombinacji. Jeśli hasło ma siedem znaków lub mniej, drugą połowa hasha będzie zawsze AAD3B435B51404EE.

Łamanie haseł Windows 2000

Plik SAM w systemie Windows zawiera nazwy użytkowników i hashowane hasła. Znajduje się w katalogu Windows \ system32 \ config. Plik jest zablokowany, gdy system operacyjny jest uruchomiony, aby haker nie mógł próbować skopiować pliku, gdy komputer jest uruchamiany z systemem Windows. Jedną z opcji kopiowania pliku SAM jest uruchomienie alternatywnego systemu operacyjnego, takiego jak DOS lub Linux z boot CD. Alternatywnie plik można skopiować z katalogu napraw. Jeśli administrator systemu używa funkcji RDISK systemu Windows do tworzenia kopii zapasowej systemu, wówczas skompresowana kopia pliku SAM o nazwie SAM._ jest tworzona w C: \ windows \ repair. Aby rozwinąć ten plik, użyj następującego polecenia w wierszu polecenia:

C: \> expand sam._ sam

Po nieskompresowaniu pliku można uruchomić atak słownikowy, hybrydowy lub brute-force w stosunku do pliku SAM za pomocą narzędzia takiego jak L0phtCrack. Podobnym narzędziem do L0phtcrack jest Ophcrack. W ćwiczeniu 4.1 pokazano, jak używać Ophcrack do łamania haseł.

Narzędzia hakerskie

Win32CreateLocalAdminUser to program, który tworzy nowego użytkownika z nazwą użytkownika i hasłem X i dodaje użytkownika do grupy lokalnego administratora. Ta akcja jest częścią projektu Metasploit i może zostać uruchomiona w środowisku Metasploit w systemie Windows. Resetowanie hasła offline NT to metoda resetowania hasła do konta administratora, gdy system nie jest uruchamiany z systemem Windows. Najpopularniejszą metodą jest uruchomienie boot CD systemu Linux, a następnie dostęp do partycji NTFS, która nie jest już chroniona, i zmiana hasła.

<u>Ćwiczenie 4 .1</u>

Użycie Ophcrack do łamania haseł

1. Pobierz i zainstaluj ophcrack ze strony http://ophcrack.sourceforge.net/.

2. Uruchom program ophcrack i ustaw liczbę wątków w zakładce Preferencje na liczbę rdzeni komputera z ophcrack plus jeden. Jeśli zmienisz tę wartość, musisz wyjść z ophcrack i zrestartować ją, aby zapisać zmianę.

Uwaga: ten krok jest opcjonalny, ale przyspieszy proces łamania

3. Kliknij przycisk Załaduj, aby dodać hash'e. Istnieje wiele sposobów dodawania skrótów:

* Wprowadź ręcznie hash (opcja Single Hash)

* Zaimportuj plik tekstowy zawierający skróty utworzone przez pwdump, fgdump lub podobne narzędzia innych firm (opcja Plik PWDUMP)

* Wyodrębnij skróty z plików SYSTEM i SAM (opcja szyfrowanego SAM)

* Zrzuć SAM z komoutera z działającym ophcrack (opcja Local SAM)

* Zrzuć SAM ze zdalnego komputera (opcja zdalnego SAM)

Uwaga: W przypadku opcji Zaszyfrowane SAM, SAM znajduje się w katalogu system32 / config systemu Windows i można uzyskać do niego dostęp tylko w przypadku nieaktywnej partycji Windows. W przypadku opcji Local SAM i Remote SAM użytkownik musi być zalogowany z uprawnieniami administratora na komputerze, na którym ma zostać zrzucone narzędzie SAM.

4. Kliknij przycisk Tabele.

5. Kliknij przycisk włączania (zielony i żółty).

6. Posługując się strzałkami w górę iw dół, posortuj tabele tęczowe, których chcesz użyć. Pamiętając, że przechowywanie tablic tęczowych na szybkim nośniku, takim jak dysk twardy, znacznie przyspieszy proces łamania.

7. Kliknij przycisk Crack, aby rozpocząć proces łamania. Zobaczysz postęp programu , proces łamania w dolnych polach okna ophcrack. Gdy hasło zostaje znalezione, będzie wyświetlane w polu NT Pwd. Możesz zapisać wyniki sesji łamania sesji w dowolnym momencie, klikając przycisk Zapisz.

Przekierowanie logowania SMB do atakującego

Innym sposobem na wykrycie haseł w sieci jest przekierowanie loginu Server Message Block (SMB) do komputera atakującego, aby hasła zostały wysłane do hakera. Aby to zrobić, haker musi sniffować odpowiedzi NTLM z serwera uwierzytelniającego i skłonić ofiarę do próby uwierzytelnienia systemu Windows na komputerze atakującego. Powszechną techniką jest wysyłanie ofierze wiadomości e-mail z osadzonym linkiem do fałszywego serwera SMB. Po kliknięciu łącza użytkownik nieświadomie wysyła swoje poświadczenia przez sieć.

SMBRelay : Serwer SMB przechwytujący nazwy użytkowników i skróty hasłowe od przychodzącego ruchu SMB. SMBRelay może również wykonywać ataki typu "man-in-the-middle" (MITM).

SMBRelay2 Podobne do SMBRelay, ale używa nazw NetBIOS zamiast adresów IP do przechwytywania nazw użytkowników i haseł.

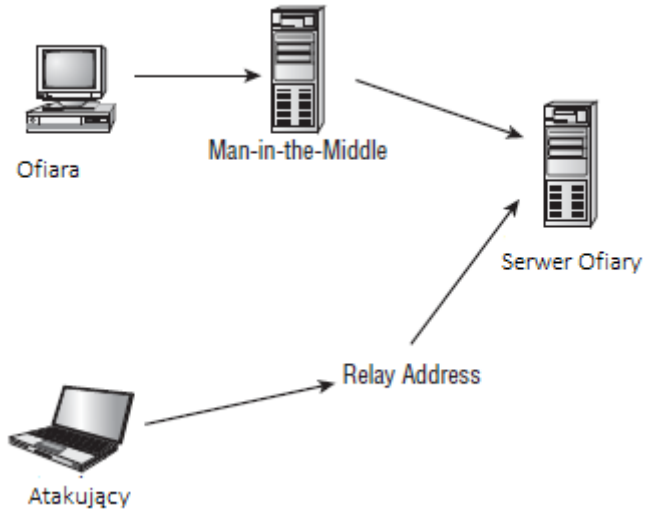
pwdump2 Program wyodrębniający skróty hasła z pliku SAM w systemie Windows. Wyodrębnione skróty hasła można następnie uruchomić za pomocą L0phtCrack, aby złamać hasła.

Samdump Inny program wyodrębniający NTLM zakodował hasła z pliku SAM.

C2MYAZZ Program szpiegujący, który sprawia, że klienci systemu Windows wysyłają swoje hasła jako czysty tekst. Wyświetla nazwy użytkowników i ich hasła, gdy użytkownicy dołączają do zasobów serwera.

Ataki SMB Relay MITM i środki zaradcze

Atak SMB Relay MITM ma miejsce, gdy atakujący tworzy fałszywy serwer z adresem przekazującym. Gdy klient ofiary łączy się z nieuczciwym serwerem, serwer MITM przechwytuje połączenie, przesyła hasło i przekazuje połączenie do serwera ofiary. Rysunek ilustruje taki atak.



Środki zaradcze SMB obejmują konfigurację systemu Windows 2000 do korzystania z podpisywania SMB, co powoduje, że szyfruje on każdy blok komunikacji SMB.

Narzędzia hakerskie

Funkcja SMBGrind zwiększa szybkość sesji L0phtCrack na zrzutach snifferów, usuwając duplikaty i umożliwiając kierowanie na określonych użytkowników bez konieczności ręcznego edytowania plików zrzutu. Narzędzie SMBDie powoduje awarię komputerów z systemem Windows 2000, XP lub NT, wysyłając specjalnie spreparowane żądania SMB. NBTdeputy może rejestrować nazwę komputera NetBIOS w sieci i odpowiadać na żądania zapytań nazw NetBIOS przez TCP / IP (NetBT). Upraszcza korzystanie z SMBRelay. Przekaźnik może być nazywany przez nazwę komputera zamiast adresu IP.

Ataki NetBIOS DoS

Atak typu DoS (Denial of Service) systemu NetBIOS przesyła komunikat o nazwie NetBIOS Name Release do usługi NetBIOS Name Service na docelowym systemie Windows i zmusza system do umieszczenia nazwy w konflikcie, aby nazwa nie mogła być już używana. Zasadniczo blokuje to klientowi udział w sieci NetBIOS i tworzy DoS sieci dla tego systemu.

Narzędzie hakerskie

Nazwa NBName może wyłączyć całe sieci LAN i uniemożliwić ponowne podłączenie komputerów. Węzły w sieci NetBIOS zainfekowane przez narzędzie uważają, że ich nazwy są już używane przez inne

komputery. Innym sposobem na stworzenie bezpieczniejszego i zapadającego w pamięć hasła jest stosowanie powtarzalnego wzorca, który umożliwi ponowne utworzenie hasła w razie potrzeby.

1. Zacznij od niezapomnianej frazy, takiej jak Maryhadalittlelamb

2. Zmieniaj każdy co drugi znak na wielkie, powodując MaRyHaDaLiTtLeLaMb

3. Zmień a na @ i i na 1, aby uzyskać M @ RyH @ D @ L1TtLeL @ Mb

4. Upuść co drugą parę, aby uzyskać bezpieczne powtarzalne hasło lub M @ H @ L1LeMb

Teraz masz hasło, które spełnia wszystkie wymagania, ale w razie potrzeby można je "przerobić".

Przeciwdziałanie łamaniu haseł

W celu ochrony przed łamaniem haseł należy zastosować najsilniejsze hasła. Systemy powinny wymuszać 8-12-znakowe hasła alfanumeryczne. Aby uchronić się przed złamaniem algorytmu haszowania dla haseł przechowywanych na serwerze, należy zadbać o fizyczną izolację i ochronę serwera. Administrator systemu może użyć narzędzia SYSKEY w systemie Windows, aby dodatkowo zabezpieczyć hashe przechowywane na dysku twardym serwera. Dzienniki serwera powinny być również monitorowane pod kątem brute-force na konta użytkowników. Administrator systemu może wdrożyć następujące środki bezpieczeństwa, aby zmniejszyć skuteczność próby złamania hasła typu brute force:

* Nigdy nie zostawiaj domyślnego hasła.

* Nigdy nie używaj hasła, które można znaleźć w słowniku.

* Nigdy nie używaj hasła związanego z nazwą hosta, nazwą domeny ani żadnymi innymi informacjami, które można znaleźć w Whois.

* Nigdy nie używaj hasła związanego z hobby, zwierzętami domowymi, rodziną lub datą urodzenia.

* W ostateczności użyj słowa, które ma więcej niż 21 znaków ze słownika jako hasło.

Interwał zmiany hasła

Hasła powinny wygasać po pewnym czasie, aby użytkownicy byli zmuszeni je zmienić. Jeśli interwał hasła jest ustawiony zbyt nisko, użytkownicy zapomną swoich aktualnych haseł; w rezultacie administrator systemu będzie musiał często resetować hasła użytkowników. Z drugiej strony, jeśli hasła będą mogły być używane zbyt długo, bezpieczeństwo może zostać naruszone. Zalecany interwał zmiany hasła wynosi co 30 dni. Ponadto większość specjalistów ds. bezpieczeństwa zalecała, aby użytkownicy nie mogli ponownie wykorzystywać trzech ostatnich haseł. Nie można całkowicie zablokować ataków haseł typu "brute force", jeśli haker przełącza serwer proxy, w którym generowany jest pakiet źródłowy. Administrator systemu może dodawać tylko funkcje bezpieczeństwa, aby zmniejszyć prawdopodobieństwo, że ataki haseł o charakterze brutalnej siły będą przydatne.

Monitorowanie dzienników Podglądu zdarzeń

Administratorzy powinni monitorować dzienniki Podglądu zdarzeń, aby wykryć wszelkie próby włamań, zanim się pojawią lub podczas ich wystąpienia. Zwykle kilka nieudanych prób jest rejestrowanych w dziennikach systemowych przed pomyślnym włamaniem lub atakiem haseł. Dzienniki bezpieczeństwa są tak dobre, jak administratorzy systemu, którzy je monitorują. Narzędzia takie jak VisualLast pomagają administratorowi sieci w rozszyfrowywaniu i analizowaniu plików dziennika bezpieczeństwa. VisualLast zapewnia lepszy wgląd w dzienniki zdarzeń NT, dzięki czemu

administrator może dokładniej i wydajniej ocenić aktywność sieci. Program ma umożliwić administratorom sieci przeglądanie i raportowanie czasu logowania i wylogowania poszczególnych użytkowników; zdarzenia te mogą być wyszukiwane zgodnie z ramami czasowymi, co jest bezcenne dla analityków bezpieczeństwa, którzy szukają szczegółów dotyczących włamań. Dziennik zdarzeń znajdujący się pod adresem c: \\ windows \ system32 \ config \ Sec.Event.Evt zawiera ślad prób brute-force atakującego

Zrozumienie keyloggerów i innych technologii spyware

Jeśli wszystkie inne próby zebrania haseł się nie powiodą, to wtedy keystroke logger jest narzędziem wybieranym przez hakerów. Rejestratory klawiszy (keyloggery) można zaimplementować za pomocą sprzętu lub oprogramowania. Sprzętowe keyloggery to małe urządzenia, które łączą klawiaturę z komputerem i zapisują każde naciśnięcie klawisza w pliku lub w pamięci urządzenia sprzętowego. Aby zainstalować keylogger sprzętowy, haker musi mieć fizyczny dostęp do systemu. Keyloggery programowe to fragmenty ukrytego oprogramowania, które znajdują się pomiędzy sprzętem klawiatury i systemem operacyjnym, dzięki czemu mogą rejestrować każde naciśnięcie klawisza. Keyloggery programowe mogą być wdrażane w systemie przez trojany lub wirusy.

Narzędzia hakerskie

Spector to oprogramowanie szpiegujące, które rejestruje wszystko, co system robi w Internecie, podobnie jak kamera nadzorująca. Spector automatycznie wykonuje setki migawek każdej godziny, co jest na ekranie komputera i zapisuje te migawki w ukrytym miejscu na dysku twardym systemu. Spector może zostać wykryty i usunięty za pomocą Anti-Spector. eBlaster to internetowe oprogramowanie szpiegowskie, które rejestruje przychodzące i wychodzące wiadomości e-mail i natychmiast przekazuje je na inny adres e-mail. eBlaster może również przechwytywać obie strony rozmowy Instant Messengera, rejestrować naciśnięcia klawiszy i rejestrować odwiedzane strony internetowe. SpyAnywhere to narzędzie, które pozwala na przeglądanie aktywności systemu i działań użytkownika, zamykanie / ponowne uruchamianie, blokowanie / zatrzymywanie, a nawet przeglądanie systemu plików w systemie zdalnym. SpyAnywhere pozwala kontrolować otwarte programy i okna w systemie zdalnym oraz przeglądać historie internetowe i powiązane informacje. Invisible KeyLogger Stealth (IKS) Software Logger to wysokowydajny sterownik urządzeń wirtualnych (VxD), który działa dyskretnie na najniższym poziomie systemu operacyjnego Windows 95, 98 lub ME. Wszystkie naciśnięcia klawiszy są zapisywane w pliku binarnego naciśnięcia klawisza. Fearless Key Logger to trojan, który pozostaje w pamięci i przechwytuje wszystkie naciśnięcia klawiszy użytkownika. Przechwycone naciśnięcia klawiszy są przechowywane w pliku dziennika i mogą być odzyskiwane przez hakera. Keylogger poczty e-mail rejestruje wszystkie wiadomości e-mail wysłane i odebrane w systemie docelowym. E-maile mogą być przeglądane przez nadawcę, odbiorcę, temat i godzinę / datę. Zawartość wiadomości e-mail i wszelkie załączniki są również rejestrowane.

Eskalacja przywilejów

Eskalacja przywilejów to trzeci etap cyklu hakerskiego. Eskalacja uprawnień oznacza w zasadzie dodanie większej liczby uprawnień lub uprawnień do konta użytkownika. Mówiąc prosto, eskalacja uprawnień powoduje, że zwykłe konto użytkownika staje się kontem administratora. Zasadniczo konta administratora mają bardziej rygorystyczne wymagania dotyczące haseł, a ich hasła są ściślej strzeżone. Jeśli nie można znaleźć nazwy użytkownika i hasła konta z uprawnieniami administratora, haker może wybrać konto z mniejszymi uprawnieniami. W takim przypadku haker musi eskalować przywileje tego konta. Osiąga się to przez uzyskanie pierwszego dostępu za pomocą konta użytkownika innego niż administrator, zazwyczaj przez zebranie nazwy użytkownika i hasła za pośrednictwem jednej z wcześniej omówionych metod, a następnie zwiększenie uprawnień konta do poziomu administratora.

Narzędzia hakerskie

GetAdmin.exe to mały program dodający użytkownika do lokalnej grupy administratorów. Wykorzystuje niskopoziomową procedurę jądra NT, aby umożliwić dostęp do dowolnego działającego procesu. Do uruchomienia programu wymagane jest zalogowanie do konsoli serwera. Program GetAdmin.exe uruchamiany jest z wiersza poleceń lub przeglądarki. Działa tylko z dodatkiem Service Pack 3 dla systemu Windows NT 4.0. Narzędzie Hk.exe udostępnia lukę lokalnego wywołania procedury (LPC) w systemie Windows NT. Użytkownik niebędący administratorem może być eskalowany do grupy administratorów za pomocą tego narzędzia. Gdy haker ma prawidłowe konto użytkownika i hasło, następnym krokiem jest wykonanie aplikacji. Ogólnie rzecz biorąc, haker musi mieć konto z dostępem na poziomie administratora, aby instalować programy, dlatego tak ważne jest eskalowanie uprawnień. W następnych sekcjach zobaczymy, co hakerzy mogą zrobić ze swoim systemem, gdy mają uprawnienia administratora.

Wykonywanie aplikacji

Gdy haker uzyskał dostęp do konta z uprawnieniami administratora, kolejną rzeczą, którą robi, jest uruchamianie aplikacji w systemie docelowym. Celem wykonywania aplikacji może być zainstalowanie backdoora w systemie, instalacja rejestratora klawiszy w celu zbierania poufnych informacji, kopiowania plików lub po prostu powodowania uszkodzeń systemu - zasadniczo wszystkiego, co haker chce zrobić w systemie. Gdy haker będzie w stanie wykonywać aplikacje, system jest uważany za własność i pod kontrolą hakera.

Narzędzia hakerskie

PsExec to program, który łączy się i wykonuje pliki w systemach zdalnych. W systemie zdalnym nie trzeba instalować żadnego oprogramowania. Remoxec wykonuje program za pomocą usług RPC (Task Scheduler) lub DCOM (Windows Management Instrumentation). Administratorzy o zerowym lub słabym haseł mogą być wykorzystywani przez Harmonogram zadań (1025 / tcp lub wyższy) lub Tryb obiektów składowych rozproszonych (DCOM; domyślnie 135 / tcp).

Przepełnienie bufora

Przepełnienie bufora to próby włamania, które wykorzystują lukę w kodzie aplikacji. Zasadniczo atak przepełnienia bufora wysyła zbyt wiele informacji do zmiennej pola w aplikacji, co może spowodować błąd aplikacji. W większości przypadków aplikacja nie wie, co należy dalej wykonać, ponieważ została nadpisana danymi dotyczącymi przepełnienia. Dlatego też wykonuje polecenie w danych przepełnienia lub wyświetla wiersz polecenia, aby umożliwić użytkownikowi wprowadzenie następnego polecenia. Wiersz polecenia lub powłoka jest kluczem dla hakera i może być używany do uruchamiania innych aplikacji.

Zrozumienie rootkitów

Rootkit to rodzaj programu często wykorzystywanego do ukrywania narzędzi w zagrożonym systemie. Rootkity to tak zwane backdoory, które pomagają intruzom w łatwiejszym dostępie do systemu. Na przykład rootkit może ukryć aplikację, która uruchamia powłokę, gdy atakujący połączy się z określonym portem sieciowym w systemie. Backdoor może także zezwalać na procesy uruchamiane przez nieuprzywilejowanego użytkownika do wykonywania funkcji zwykle zarezerwowanych dla administratora. Rootkit jest często wykorzystywany, aby programista rootkita mógł zobaczyć i uzyskać dostęp do nazw użytkowników i informacji logowania do witryn, które ich potrzebują. Istnieje kilka rodzajów rootkitów, w tym :

Rootkity na poziomie jądra rootkity na poziomie jądra dodają kod i / lub zastępują część kodu jądra zmodyfikowanym kodem, aby pomóc ukryć backdoor w systemie komputerowym. Często odbywa się to poprzez dodanie nowego kodu do jądra za pośrednictwem sterownika urządzenia lub ładowalnego modułu, takiego jak ładowalne moduły jądra w systemie Linux lub sterowniki urządzeń w systemie Windows. Rootkity na poziomie jądra są szczególnie niebezpieczne, ponieważ mogą być trudne do wykrycia bez odpowiedniego oprogramowania.

Rootkity na poziomie biblioteki Rootkity na poziomie biblioteki często łatają, zawieszają lub zamieniają wywołania systemowe na wersje, które ukrywają informacje, które mogą pozwolić na identyfikację hakerów.

Rootkity na poziomie aplikacji rootkity na poziomie aplikacji mogą zastąpić zwykłe pliki binarne aplikacji trojanizowanymi podróbkami lub mogą modyfikować zachowanie istniejących aplikacji przy użyciu haków, poprawek, wstrzykniętego kodu lub innych środków.

Sadzenie rootkitów na maszynach Windows 2000 i XP

Rootkit systemu Windows NT / 2000 jest zbudowany jako sterownik trybu jądra, który można dynamicznie ładować w środowisku wykonawczym. Rootkit działa z uprawnieniami systemowymi w rdzeniu jądra NT, dzięki czemu ma dostęp do wszystkich zasobów systemu operacyjnego. Rootkit może również ukrywać procesy, ukrywać pliki, ukrywać wpisy rejestru, przechwytywać naciśnięcia klawiszy wpisane na konsoli systemowej, wywoływać przerwanie debugowania, aby spowodować niebieski ekran śmierci i przekierować pliki EXE. Rootkit zawiera sterownik urządzenia trybu jądra o nazwie _root_.sys i program uruchamiający o nazwie DEPLOY.EXE. Po uzyskaniu dostępu do systemu docelowego, atakujący kopiuje pliki _root_.sys i DEPLOY.EXE do systemu docelowego i wykonuje DEPLOY.EXE. Spowoduje to zainstalowanie sterownika urządzenia rootkit i uruchomienie go. Atakujący później usuwa DEPLOY.EXE z komputera docelowego. Atakujący może następnie zatrzymać i zrestartować rootkita zgodnie z poleceniem net stop _root_ i net start _root_. Po uruchomieniu rootkita plik _root_.sys nie pojawia się już na listach katalogów; rootkit przechwytuje wywołania systemowe dla list plików i ukrywa wszystkie pliki zaczynające się _root_ od wyświetlenia.

Rootkit Embedded TCP / IP Stack

Nowa funkcja rootkita systemu Windows NT / 2000 to bezstanowy stos TCP / IP. Działa poprzez ustalenie stanu połączenia na podstawie danych w pakiecie przychodzącym. Rootkit ma zakodowany adres IP (10.0.0.166), na który zareaguje. Rootkit wykorzystuje surowe połączenia Ethernet do karty sieciowej systemu, więc jest bardzo wydajny. Port docelowy nie ma znaczenia; haker może telnetować do dowolnego portu w systemie. Ponadto wiele osób może zalogować się do rootkita na raz.

Rootkit Środki zaradcze

Wszystkie rootkity wymagają dostępu administratora do systemu docelowego, więc bezpieczeństwo haseł jest krytyczne. W przypadku wykrycia rootkita należy wykonać kopię zapasową ważnych danych i ponownie zainstalować system operacyjny i aplikacje z zaufanego źródła. Administrator powinien również udostępniać dobrze udokumentowaną zautomatyzowaną procedurę instalacji i zaufany nośnik przywracania. Innym środkiem zaradczym jest użycie narzędzia sum kontrolnych MD5. Suma kontrolna MD5 dla pliku jest wartością 128-bitową, podobnie jak odcisk palca pliku. (Istnieje niewielka możliwość uzyskania dwóch identycznych sum kontrolnych dla dwóch różnych plików.) Algorytm ten został zaprojektowany tak, aby zmiana nawet jednego bitu w danych pliku powodowała inną wartość sumy kontrolnej. Ta funkcja może być przydatna przy porównywaniu plików i zapewnieniu ich integralności. Inną dobrą funkcją jest stała długość sumy kontrolnej, niezależnie od wielkości pliku

źródłowego. Suma kontrolna MD5 zapewnia, że plik się nie zmienił. Może to być przydatne w sprawdzaniu integralności pliku, jeśli rootkit został znaleziony w systemie. Narzędzia takie jak Tripwire implementują sumy kontrolne MD5 w celu identyfikacji plików, na które ma wpływ rootkit.

Narzędzia przeciwdziałania

Tripwire to program do sprawdzania integralności systemu plików dla systemów operacyjnych Unix i Linux. Oprócz jednej lub więcej kryptograficznych sum kontrolnych reprezentujących zawartość każdego katalogu i pliku, baza danych Tripwire zawiera również informacje, które umożliwiają weryfikację uprawnień dostępu i ustawień trybu plików, nazwę użytkownika właściciela pliku, datę i godzinę ostatniego dostępu do pliku i ostatnia modyfikacja dokonana w elemencie.

Ukrywanie plików

Haker może chcieć ukryć pliki w systemie, aby zapobiec ich wykryciu. Pliki te można następnie wykorzystać do przeprowadzenia ataku na system. Istnieją dwa sposoby ukrywania plików w systemie Windows. Pierwszym z nich jest użycie polecenia attrib. Aby ukryć plik za pomocą polecenia attrib, wpisz następujące polecenie w wierszu polecenia:

attrib + h [plik / katalog]

Drugim sposobem na ukrycie pliku w systemie Windows jest przesyłanie strumieniowe danych alternatywnych NTFS. Systemy plików NTFS używane w systemach Windows NT, 2000 i XP mają funkcję o nazwie alternatywne strumienie danych które umożliwiają przechowywanie danych w ukrytych plikach połączonych z normalnym, widocznym plikiem. Strumienie nie są ograniczone wielkością; więcej niż jeden strumień można połączyć z normalnym plikiem.

Strumieniowanie plików NTFS

Strumieniowe przesyłanie plików NTFS umożliwia utworzenie ukrytego pliku w legalnym pliku. Ukryty plik nie pojawia się w spisie katalogów, ale prawowity plik robi. Użytkownik zwykle nie podejrzewa, że plik jest zgodny z prawem, ale ukryty plik może być używany do przechowywania lub przesyłania informacji. W ćwiczeniu 4.2 dowiesz się, jak ukrywać pliki za pomocą strumieniowania plików NTFS.

Ćwiczenie 4. 2

Ukrywanie plików przy użyciu strumieniowania plików NT FS

Uwaga: to ćwiczenie będzie działać tylko w systemach korzystających z systemu plików NTFS. Aby utworzyć i przetestować strumień plików NTFS:

1. W wierszu poleceń wprowadź polecenie notepad test.txt.

2. Umieść dane w pliku, zapisz plik i zamknij Notatnik. Krok 1 otworzy Notatnik.

3. W wierszu poleceń wpisz dir test.txt i zanotuj rozmiar pliku.

4. W wierszu poleceń wprowadź polecenie notepad test.txt: hidden.txt. Wpisz trochę tekstu do Notatnika, zapisz plik i zamknij go.

5. Sprawdź ponownie rozmiar pliku (powinien być taki sam jak w kroku 3).

6. Otwórz test.txt. Widzisz tylko oryginalne dane.

7. Wpisz typ test.txt: hidden.txt w wierszu poleceń. Komunikat o błędzie składni jest wyświetlany

Narzędzie hakerskie

makestrm.exe to narzędzie, które przenosi dane z pliku do alternatywnego strumienia danych połączonego z oryginalnym plikiem.

NTFS Stream Przeciwdziałanie

Aby usunąć plik strumieniowy, skopiuj pierwszy plik na partycję FAT, a następnie skopiuj go z powrotem do partycji NTFS. Strumienie są tracone po przeniesieniu pliku na partycję FAT, ponieważ są one funkcją systemu NTFS i dlatego istnieją tylko na partycji NTFS.

Narzędzie przeciwdziałania

Możesz użyć lns.exe do wykrywania strumieni NTFS. LNS zgłasza istnienie i lokalizację plików zawierających alternatywne strumienie danych.

Zrozumienie technologii steganograficznych

Steganografia to proces ukrywania danych w innych typach danych, takich jak obrazy lub pliki tekstowe. Najpopularniejszą metodą ukrywania danych w plikach jest wykorzystywanie obrazów graficznych jako kryjówek. Atakujący mogą osadzić dowolne informacje w pliku graficznym za pomocą steganografii. Haker może ukryć wskazówki dotyczące wykonania bomby, tajnego numeru konta bankowego lub odpowiedzi na test. Każdy tekst, jaki można sobie wyobrazić, może być ukryty na obrazie. W ćwiczeniu 4.3 użyjesz funkcji Ukryj obraz, aby ukryć tekst w obrazie.

Narzędzia hakerskie

ImageHide to program steganograficzny, który ukrywa duże ilości tekstu w obrazach. Nawet po dodaniu bajtów danych nie ma zwiększenia rozmiaru obrazu. Obraz wygląda tak samo w normalnym programie graficznym. Ładuje i zapisuje pliki, dzięki czemu jest w stanie ominąć większość snifferów pocztowych. Blindside to aplikacja steganograficzna, która ukrywa informacje w obrazach BMP (bitmapowych). To narzędzie wiersza polecenia. MP3Stego ukrywa informacje w plikach MP3 podczas procesu kompresji. Dane są kompresowane, szyfrowane, a następnie ukrywane w strumieniu danych MP3. Snow to program do steganografii białych znaków, który ukrywa wiadomości w tekście ASCII, dołączając białe znaki do końca linii. Ponieważ spacje i tabulatory na ogół nie są widoczne w przeglądarkach tekstowych, wiadomość jest skutecznie ukrywana przed przypadkowymi obserwatorami. Jeśli używane jest wbudowane szyfrowanie, wiadomości nie można odczytać, nawet jeśli zostanie wykryta. CameraShy współpracuje z Windows i Internet Explorer i pozwala użytkownikom udostępniać ocenzurowane lub wrażliwe informacje przechowywane w zwykłym obrazie GIF. Stealth to narzędzie filtrujące pliki PGP. Usuwa informacje identyfikujące z nagłówka, po czym plik może być używany do steganografii.

Ćwiczenie 4 .3

Ukrywanie danych w obrazie przy użyciu funkcji ImageHide

Aby ukryć dane w obrazie za pomocą ImageHide:

1. Pobierz i zainstaluj program ImageHide.

2. Dodaj obraz do programu Image Hide.

3. Dodaj tekst w polu u dołu ekranu ImageHide.

4. Ukryj tekst w obrazie za pomocą ImageHide.

Steganografia może być wykryta przez niektóre programy, chociaż jest to trudne. Pierwszym krokiem w wykryciu jest zlokalizowanie plików z ukrytym tekstem, co można zrobić, analizując wzorce w obrazach i zmiany w palecie kolorów.

Narzędzia przeciwdziałania

Stegdetect to automatyczne narzędzie do wykrywania treści steganograficznych w obrazach. Jest zdolny do wykrywania różnych metod steganograficznych do osadzania ukrytych informacji w obrazach JPEG. Dskprobe to narzędzie na instalacyjnym dysku CD systemu Windows 2000. Jest to niskopoziomowy skaner dysku twardego, który wykrywa steganografię.

Maskowanie swoich tras i usuwanie dowodów

Gdy intruzi uzyskają dostęp administratora w systemie, próbują ukryć swoje ślady, aby uniemożliwić wykrycie ich obecności (obecnej lub przeszłej) w systemie. Haker może również próbować usunąć dowody tożsamości lub działania w systemie, aby zapobiec śledzeniu ich tożsamości lub lokalizacji przez władze. Aby zapobiec wykryciu, haker zazwyczaj usuwa wszystkie komunikaty o błędach lub zdarzenia bezpieczeństwa, które zostały zarejestrowane. Wyłączenie audytu i wyczyszczenie dziennika zdarzeń to dwie metody używane przez hakera do ukrywania swoich tras i unikania wykrycia. Pierwszą rzeczą, którą intruzi robią po uzyskaniu uprawnień administratora, jest wyłączenie audytu. Audyt systemu Windows rejestruje określone zdarzenia w pliku dziennika przechowywanym w Przeglądarce zdarzeń systemu Windows. Zdarzenia mogą obejmować logowanie do systemu, aplikacji lub dziennika zdarzeń. Administrator może wybrać poziom rejestrowania zaimplementowany w systemie. Hakerzy chcą określić poziom rejestrowania zaimplementowany, aby sprawdzić, czy muszą wyczyścić zdarzenia wskazujące na ich obecność w systemie.

Narzędzie hakerskie

Auditpol to narzędzie zawarte w zestawie Windows NT Resource Kit dla administratorów systemu. To narzędzie może wyłączyć lub włączyć inspekcję z wiersza poleceń systemu Windows. Można go również wykorzystać do określenia poziomu logowania zaimplementowanego przez administratora systemu.

Intruzi mogą z łatwością usunąć dzienniki zabezpieczeń w Przeglądarce zdarzeń systemu Windows. Wydarzenie log zawierający jedno lub kilka zdarzeń jest podejrzany, ponieważ zwykle oznacza, że inne zdarzenia zostały usunięte. Wciąż trzeba wyczyścić dziennik zdarzeń po wyłączeniu kontroli, ponieważ za pomocą narzędzia Auditpol umieszcza się wpis w dzienniku zdarzeń wskazujący, że inspekcja została wyłączona. Istnieje kilka narzędzi do wyczyszczenia dziennika zdarzeń lub haker może to zrobić ręcznie w Przeglądarce zdarzeń systemu Windows.

Narzędzia hakerskie

Narzędzie elsave.exe to proste narzędzie do czyszczenia rejestru zdarzeń. Jest oparty na linii poleceń. WinZapper to narzędzie, którego atakujący może użyć do selektywnego usuwania rekordów zdarzeń z dziennika zabezpieczeń w systemie Windows 2000. Program WinZapper zapewnia również, że żadne zdarzenia bezpieczeństwa nie są rejestrowane podczas działania programu. Evidence Eliminator to system do czyszczenia danych dla komputerów z systemem Windows. Zapobiega trwałemu ukryciu niepożądanych danych w systemie. Czyści Kosz, pamięć podręczną Internetu, pliki systemowe, foldery tymczasowe itd. Evidence Eliminator może być również użyty przez hakera do usuwania dowodów z systemu po ataku.

Podsumowanie

Rzeczywiste włamanie systemu docelowego można podzielić na proste kroki. Zgadywanie lub łamanie haseł, eskalacja przywilejów, ukrywanie plików i zakrywanie ścieżek są częścią procesu hakerskiego. To właśnie te kroki zwykle zawierają najcenniejsze informacje dla hakerów. Jednak nie należy zapominać o etapach zbierania informacji i skanowania, ponieważ mają one kluczowe znaczenie w uzyskaniu jak największej ilości informacji na temat celu i jego słabości. Dobre gromadzenie informacji może znacznie poprawić skuteczność i szybkość kroków hakerskich.

Do Zapamiętania!

* Zrozumiałeś znaczenie zabezpieczenia hasłem. Wdrożenie interwałów wymiany hasła, silnych haseł alfanumerycznych i innych zabezpieczeń hasłem ma kluczowe znaczenie dla bezpieczeństwa sieci.

* Poznałeś różne rodzaje ataków haseł. Pasywne ataki online obejmują sniffowanie , man-in-the-middle i powtórz. Aktywne ataki online obejmują pasywne i automatyczne odgadywanie haseł. Ataki offline obejmują słownik, hybrydę i brute-force. Ataki nieelektroniczne obejmują surfowanie na ramieniu, wąchanie klawiatury i inżynierię społeczną.

* Zapoznałeś się z różnymi rodzajami ataków haseł offline. Ataki słownikowe, hybrydowe i brute-force są atakami haseł w trybie offline.

* Poznałeś sposoby obrony przed zgadywaniem haseł. Karty inteligentne i biometria to dwa sposoby na zwiększenie bezpieczeństwa i obronę przed zgadywaniem haseł.

* Zrozumiałeś różnice między typami ataków nieelektronicznych. Inżynieria społeczna, surfowanie przez ramę i nurkowanie w śmietnikach to wszelkiego rodzaju ataki nieelektroniczne.

* Dowiedziałeś się, w jaki sposób ataki hakerów eliminują aktywność hakerską. Czyszczenie dzienników zdarzeń i wyłączanie inspekcji to metody wykorzystywane przez intruzów do ukrywania swoich ścieżek.

* Uświadom sobie, że ukrywanie plików to środki wykorzystywane do wymykania się poufnymi informacjami. Steganografia, strumieniowanie NTFS i polecenie attrib to wszystko, w jaki sposób hakerzy mogą ukrywać i kradnąć pliki.