Podczas ataku DoS (Denial-of-Service) haker czyni system bezużytecznym lub znacznie spowalnia system przez przeciążenie zasobów lub uniemożliwienie uprawnionym użytkownikom dostępu do systemu. Ataki te mogą być popełniane przeciwko indywidualnemu systemowi lub całej sieci i zwykle są skuteczne w swoich próbach. Atak hakerski jest jednym z dostępnych, co oznacza, że uprawnieni użytkownicy nie mają już dostępu do sieci. Przejęcie sesji to metoda hakerska, która tworzy tymczasowy DoS dla użytkownika końcowego, gdy atakujący przejmie sesję. Przejęcie sesji jest wykorzystywane przez hakerów do przejęcia bieżącej sesji po ustanowieniu uwierzytelnionej sesji. Przejęcie sesji może być również użyte do wykonania ataku man-in-the-middle, gdy haker wchodzi pomiędzy serwer i legalnego klient oraz przechwytuje cały ruch. W tej części wyjaśniono ataki DoS, rozproszone ataki typu DoS (Denial of Service) oraz elementy przechwytywania sesji, takie jak metody podszywania się, potrójne uzgadnianie TCP, przewidywanie numerów sekwencyjnych oraz sposób, w jaki hakerzy używają narzędzi do przechwytywania sesji. Ponadto środki zaradcze dotyczące DoS i porwań sesji omówiono na końcu tego rozdziału.

Odmowa usługi

Atak typu DoS jest próbą włamania hakera do systemu użytkownika lub organizacji. Jako etyczny hacker musisz znać typy ataków DoS i rozumieć, jak działają ataki DoS i DDoS. Powinieneś także zapoznać się z robotami (BOT) i sieciami robotów (BOTNET), a także z atakami smurf i flooding SYN. Wreszcie, jako etyczny hacker, musisz znać różne środki zaradcze przeciw DoS i DDoS. Istnieją dwie główne kategorie ataków DoS:

* Ataki wysyłane przez pojedynczy system do jednego celu (proste DoS)

* Ataki wysyłane przez wiele systemów do jednego celu (rozproszona odmowa usługi lub DDoS).

Celem DoS nie jest uzyskanie nieautoryzowanego dostępu do maszyn lub danych, ale uniemożliwienie korzystania z niego uprawnionym użytkownikom usługi. Atak DoS może wykonywać następujące czynności:

* Zalanie sieci ruchem, zapobiegając w ten sposób prawidłowemu ruchowi sieciowemu.

* Przerywanie połączenia między dwoma komputerami, uniemożliwiając dostęp do usługi.

* Uniemożliwienie danej osobie dostępu do usługi.

* Przerwij usługę do określonego systemu lub osoby.

Różne narzędzia wykorzystują różne rodzaje ruchu, aby zalać ofiarę, ale wynik jest taki sam: usługa w systemie lub cały system jest niedostępna dla użytkownika, ponieważ jest zajęty próbą odpowiedzi na wygórowaną liczbę żądań.

Atak Denial of Service

Wieczorem, 28 maja 2008 r. Firma, alfasystems.com nagle porzuciła Internet. Ich serwery internetowe nie były już dostępne z Internetu. W ciągu minuty od rozpoczęcia ataku inżynierowie Alpha Systems przekonali się, że mieli do czynienia z jakimś atakiem typu "zalewanie pakietami". Po przejrzeniu plików dziennika routera Cisco pokazało, że oba ich interfejsy T1 do Internetu otrzymywały ruch o maksymalnej wartości 1,54 megabita, podczas gdy ruch wychodzący spadł prawie do zera. Utonęli w potopie złośliwego ruchu, a ważny ruch nie mógł się wydostać. Alpha Systems padł ofiarą ataku typu "odmowa usługi", częściej określanego jako DoS. Inżynierowie wiedzieli, że muszą zrobić coś szybko, aby powstrzymać atak i odzyskać serwery internetowe dostępne dla swoich klientów. Ale nikt tak naprawdę nie wiedział, co robić, ponieważ nigdy wcześniej tak się nie działo. Wtedy ktoś pomyślał o

możliwościach filtrowania pakietów routera. Na szczęście, ponieważ ten atak DoS był podatny na filtrowanie, Alpha Systems była w stanie wyeliminować złe pakiety i przywrócić ich normalną pracę. W ciągu dwóch minut inżynierowie Alpha Systems zastosowali filtry "brute force" do swoich routerów, wyłączając cały ruch UDP i ICMP, a alfaystems.com natychmiast powrócił do Internetu. Ostatecznie ustalono, że ich serwer został zaatakowany przez 474 pozbawione zabezpieczeń komputery z systemem Windows, tzw. "zombie" atakujące zdalnie, w klasycznym ataku DoS generowanym przez skoordynowane wysiłki setek pojedynczych komputerów.

Atak DoS to zwykle atak ostatniej instancji. Jest uważany za niewyszukany atak, ponieważ nie zapewnia hakerom dostępu do jakichkolwiek informacji, ale denerwuje cel i przerywa jego usługi. Ataki DoS mogą być destrukcyjne i mieć znaczny wpływ, gdy są wysyłane z wielu systemów jednocześnie (ataki DDoS).

Narzędzia hakerskie

Ping of Death to atak, który może spowodować blokadę systemu poprzez wysłanie wielu pakietów IP, które po ponownym złożeniu będą zbyt duże dla systemu odbierającego. Ping of Death może spowodować DoS dla klientów próbujących uzyskać dostęp do serwera, który padł ofiarą ataku.

SSPing to program, który wysyła kilka dużych, podzielonych, pakietów danych ICMP (Internet Control Message Protocol) do systemu docelowego. Spowoduje to zawieszenie komputera, gdy pakiety danych zostaną zamrożone podczas próby ponownego złożenia fragmentów.

Atak LAND wysyła pakiet do systemu, w którym źródłowy adres IP jest ustawiony tak, aby pasował do adresu IP systemu docelowego. W rezultacie system próbuje odpowiedzieć samemu sobie, powodując, że system tworzy pętlę - która wiąże zasoby systemowe i może ostatecznie doprowadzić do awarii systemu operacyjnego.

CPUHog to narzędzie do ataku DoS, które wykorzystuje zasoby procesora w systemie docelowym, czyniąc go niedostępnym dla użytkownika.

WinNuke to program, który szuka docelowego systemu z portem 139 i wysyła niepożądany ruch IP do systemu na tym porcie. Atak ten jest również znany jako atak poza granice (OOB) i powoduje przeciążenie stosu IP - w końcu system ulega awarii.

Jolt2 to narzędzie DoS, które wysyła dużą liczbę pofragmentowanych pakietów IP do systemu Windows. To wiąże zasoby systemowe i ostatecznie blokuje system. Jolt2 nie jest specyficzne dla Windows; wiele routerów Cisco i innych bram może być podatnych na atak Jolt2.

Bubonic to narzędzie DoS, które działa poprzez wysyłanie pakietów TCP z losowymi ustawieniami, w celu zwiększenia obciążenia komputera docelowego, aby ostatecznie się zawiesił.

Targa to program, który może być używany do uruchamiania ośmiu różnych ataków DoS. Osoba atakująca ma możliwość uruchomienia pojedynczych ataków lub wypróbowania wszystkich ataków, dopóki nie zakończy się pomyślnie.

RPC Locator to usługa, która, jeśli nie została skasowana, ma podatność na przepełnienie. Szczegóły dotyczące łatania systemu, aby zapobiec podatności na RPC zostaną omówione w dalszej części . Usługa lokalizatora RPC w systemie Windows umożliwia uruchamianie aplikacji rozproszonych w sieci. Jest podatny na ataki DoS, a wiele narzędzi do przeprowadzania ataków DoS wykorzystuje tę lukę.

Ponieważ ataki DoS są tak potężne i mogą okaleczyć system produkcyjny lub sieć, nie udostępnimy żadnych ćwiczeń narzędzi DoS. Jeśli chcesz przetestować wymienione tutaj narzędzia, upewnij się, że nie używasz ich w sieci produkcyjnej lub systemie. Narzędzia DoS mogą sprawić, że systemy docelowe staną się bezużyteczne.

Ataki DDoS mogą być wykonywane przez BOT i BOTNETy, które są zagrożonymi systemami, które atakujący używa do przeprowadzenia ataku na ofiarę. System lub sieć, która została naruszona, jest wtórną ofiarą, podczas gdy ataki DoS i DDoS zalewają główną ofiarę lub cel.

Jak działają ataki DDoS

DDoS to zaawansowana wersja ataku DoS. Podobnie jak DoS, DDoS próbuje odmówić dostępu do usług działających w systemie, wysyłając pakiety do systemu docelowego w sposób, który nie może obsłużyć systemu docelowego. Klucz ataku DDoS polega na tym, że przekazuje on ataki z wielu różnych hostów (które muszą najpierw zostać zaatakowane), a nie z pojedynczego hosta, takiego jak DoS. DDoS to skoordynowany atak na dużą skalę na system ofiary.

Narzędzia hakerskie

Trinoo to narzędzie, które wysyła ruch User Datagram Protocol (UDP) w celu utworzenia ataku DDoS. Master Trinoo to system używany do uruchamiania ataku DoS przeciwko jednemu lub kilku systemom docelowym. Mistrz poleca procesy agentowe (zwane demonami) na wcześniej zainfekowanych systemach (ofiary wtórne), aby zaatakować jeden lub więcej adresów IP. Ten atak występuje przez określony czas. Agent lub demon Trinoo jest zainstalowany w systemie, w którym występuje usterka przepełnienia bufora. WinTrinoo jest wersją Trinoo dla Windows i ma taką samą funkcjonalność jak Trinoo.

Shaft jest pochodną narzędzia Trinoo, które wykorzystuje komunikację UDP między wzorcami i agentami. Shaft dostarcza statystyki ataków flood, których atakujący mogą użyć, aby dowiedzieć się, kiedy system ofiary jest zamknięty; Shaft zapewnia opcje ataków typu zalania UDP, ICMP i TCP.

Tribal Flood Network (TFN) umożliwia atakującemu korzystanie z obu pasm i ataki polegające na wyczerpywaniu zasobów. TFN powoduje zalewanie UDP i ICMP, a także ataki TCP SYN i smurf. TFN2K jest oparty na TFN, z funkcjami zaprojektowanymi specjalnie w celu utrudnienia rozpoznawania i filtrowania ruchu TFN2K. Zdalnie wykonuje polecenia, ukrywa źródło ataku wykorzystując podszywanie się pod adres IP i wykorzystuje wiele protokołów transportowych (w tym UDP, TCP i ICMP).

Stacheldraht jest podobny do TFN i obejmuje opcje ICMP flood, UDP flood i TCP SYN. Zapewnia również bezpieczne połączenie telnet (za pomocą symetrycznego szyfrowania klucza) między atakującym a systemami agentów (ofiary wtórne). Zapobiega to przechwytywaniu i identyfikowaniu tego ruchu przez administratorów systemu.

Mstream używa sfałszowanych pakietów TCP z ustawioną flagą ACK do ataku na cel. Składa się z modułu obsługi i agenta, ale dostęp do programu obsługi jest chroniony hasłem.

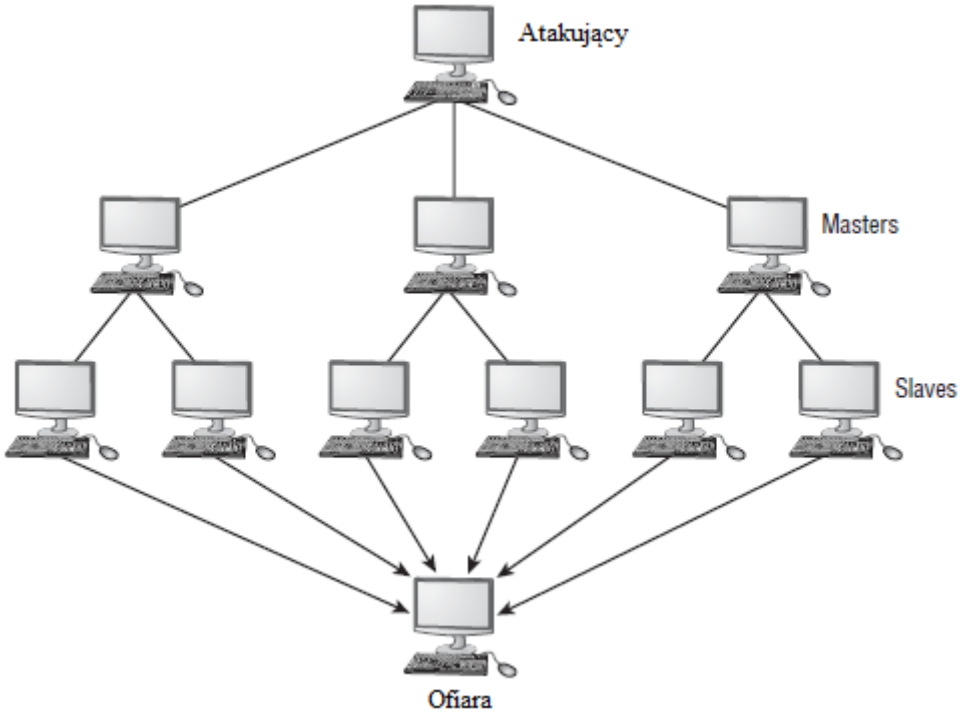
Zaatakowane usługi to te, które padły ofiarą; złamane systemy wykorzystywane do przeprowadzenia ataku są ofiarami wtórnymi. Te złamane systemy, które wysyłają DDoS do głównej ofiary, są czasami nazywane zombie lub BOTami. Zazwyczaj są atakowane przez inny atak, a następnie wykorzystywane do rozpoczęcia ataku na ofiarę pierwotną w określonym czasie lub pod pewnymi warunkami. Śledzenie źródła ataków może być trudne, ponieważ pochodzą one z kilku adresów IP. Zwykle DDoS składa się z trzech części:

* Master / handler

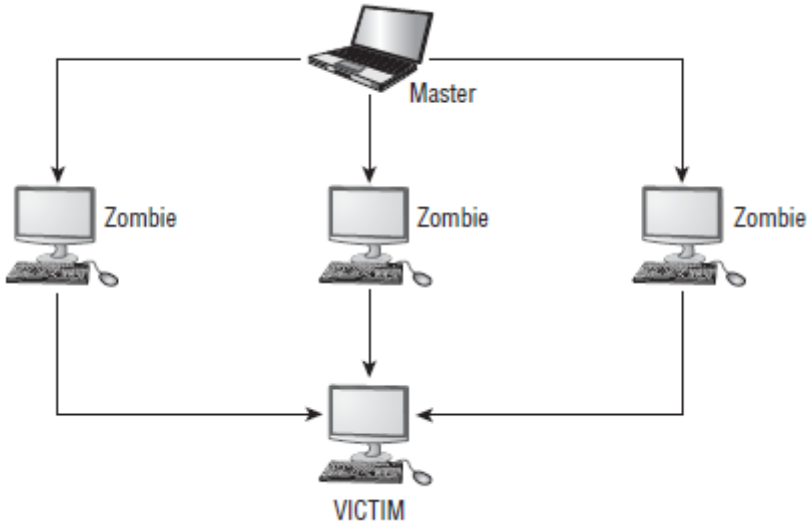
* Slave / ofiara wtórna / zombie / agent / BOT / BOTNET

* Ofiara / główna ofiara

Master to narzędzie uruchamiające atak.Slave to host, który jest zagrożony i kontrolowany przez administratora. Ofiara jest systemem docelowym. Master kieruje slave'y, aby rozpocząć atak na system ofiary

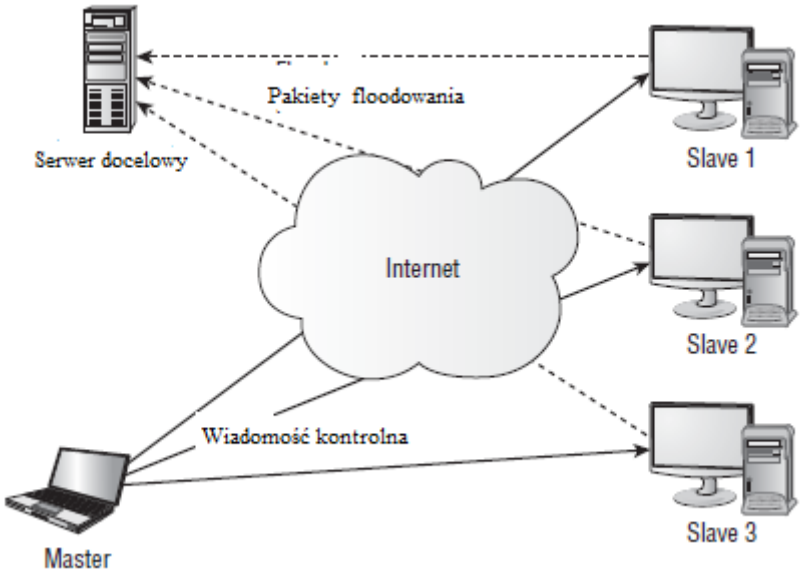


DDoS odbywa się w dwóch fazach. W fazie ataku haker łamie słabe systemy w różnych sieciach na całym świecie i instaluje narzędzia DDoS w tych złamanych systemach slave. W fazie ataku DDoS uruchamiane są systemy slave, które powodują atakowanie głównej ofiary.



Jak działają BOT / BOTNETY

BOT jest skrótem od robota internetowego i jest zautomatyzowanym programem, który zachowuje się inteligentnie. Spamerzy często używają BOTów do automatyzowania wysyłania wiadomości spamowych w grupach dyskusyjnych lub wysyłania e-maili. BOT mogą być również używane jako narzędzia do zdalnego ataku. Najczęściej BOT to agenty oprogramowania sieciowego, które łączą się ze stronami internetowymi. Na przykład roboty sieciowe (pająki) są robotami sieciowymi zbierającymi informacje o stronach internetowych. Najbardziej niebezpieczne BOT to te, które ukrywają się na komputerach użytkowników w złych zamiarach. Niektóre BOTy komunikują się z innymi użytkownikami usług internetowych za pośrednictwem komunikatorów, Internet Relay Chat (IRC) lub innego interfejsu internetowego. Te BOT pozwalają użytkownikom IRQ zadawać pytania w prostym języku angielskim, a następnie formułować właściwą odpowiedź. Takie BOT mogą często obsługiwać wiele zadań, w tym raportowanie pogody; udostępnianie informacji o kodach pocztowych; notowanie wyników sportowych; przeliczanie jednostek miar, takich jak waluta; i tak dalej. BOTNET to grupa systemów BOT. BOTNETy służą różnym celom, w tym atakom DDoS; tworzenie lub niewłaściwe użycie przekaźników poczty Simple Mail Transfer Protocol (SMTP) dla spamu; Oszustwa marketingu internetowego; oraz kradzieży numerów seryjnych aplikacji, identyfikatorów logowania i informacji finansowych, takich jak numery kart kredytowych. Ogólnie BOTNET odnosi się do grupy skompromitowanych systemów z uruchomionym BOTem w celu uruchomienia skoordynowanego ataku DDoS.



Ataki Smurf i SYN Flood

Atak typu smurf wysyła dużą ilość ruchu ICMP Echo (ping) do rozgłaszanego adresu IP ze sfałszowanym adresem źródłowym ofiary. Host każdej wtórnej ofiary w tej sieci IP odpowiada na żądanie echa ICMP z odpowiedzią Echo, mnożąc ruch przez liczbę hostów odpowiadających. W sieci z wieloma dostępami setki komputerów mogą odpowiadać na każdy pakiet. Tworzy to powiększony atak DoS odpowiedzi ping, zalewając główną ofiarę. Serwery IRC są główną ofiarą ataków typu smurf w Internecie. Atak typu SYN flood powoduje, że żądania połączenia TCP są szybsze niż komputer może je przetworzyć. Atakujący tworzy losowy adres źródłowy dla każdego pakietu i ustawia flagę SYN, aby zażądać nowego połączenia z serwerem ze sfałszowanego adresu IP. Ofiara reaguje na sfałszowany adres IP, a następnie czeka na potwierdzenie TCP, które nigdy nie dotarło. W konsekwencji ofiara połączenia wypełnia tabelę czekając na odpowiedzi; po zapełnieniu tabeli wszystkie nowe połączenia są ignorowane.

Uprawnieni użytkownicy są również ignorowani i nie mogą uzyskać dostępu do serwera. Atak typu SYN flood można wykryć za pomocą komendy netstat. Oto niektóre metody zapobiegania atakom typu SYN flood:

SYN Cookies : Pliki cookie SYN zapewniają, że serwer nie przydziela zasobów systemowych do momentu zakończenia udanego potrójnego uzgadniania.

RST Cookies: Zasadniczo serwer odpowiada na ramkę SYN klienta za pomocą nieprawidłowej

SYN ACK : Klient powinien następnie wygenerować pakiet RST informujący serwer, że coś jest nie tak. W tym momencie serwer wie, że klient jest ważny i będzie normalnie akceptował połączenia przychodzące od tego klienta.

Mikro-bloki Mikro-bloki zapobiegają powodziom SYN poprzez przydzielanie tylko niewielkiej ilości miejsca w pamięci na zapis połączenia. W niektórych przypadkach ten przydział pamięci jest tak mały, jak 16 bajtów.

Ulepszanie stosu : Ta metoda polega na zmianie stosu TCP / IP, aby zapobiec powodziom SYN. Techniki dostosowywania stosu obejmują selektywne upuszczanie przychodzących połączeń lub zmniejszanie limitu czasu, gdy stos zwolni pamięć przydzieloną dla połączenia.

W ćwiczeniu 7.1 dowiesz się, jak zapobiegać atakom typu SYN flood w systemie serwera Windows.

Ćwiczenie 7.1

Zapobieganie atakom SYN Flood na serwerach Windows

1. Uruchom edytor rejestru systemu Windows, klikając kolejno Start ✎ Uruchom i wpisując Regedit.

2. Przejdź do HKLM \ SYSTEM \ CurrentControlSet \ Services \ Tcpip \ Parameters Registry key

3. Dodaj wartość DWORD SynAttackProtect = 2 do klucza rejestru.

4. Zamknij program regedit.

Ta zmiana pozwoli systemowi operacyjnemu obsłużyć więcej żądań SYN. Kiedy wartość SynAttackProtect wynosi 2, system Windows opóźnia utworzenie gniazda do czasu zakończenia uzgadniania potrójnego. Ta zmiana skutecznie uniemożliwi atakom SYN flood wiązanie zasobów na serwerze Windows.

Przeciwdziałanie DoS / DDoS

Istnieje kilka sposobów wykrywania, zatrzymywania lub zapobiegania atakom DoS. Poniżej przedstawiono typowe funkcje zabezpieczeń:

Filtrowanie z wejściami sieciowymi : Wszyscy dostawcy dostępu do sieci powinni implementować filtrowanie z sieci, aby zatrzymać wstrzykiwanie pakietów fałszywych adresy w Internecie. Chociaż nie powstrzymuje to ataku, znacznie ułatwia znalezienie źródła ataku i szybkie zakończenie ataku. Większość IDS, firewall i routery zapewniają funkcje filtrowania adresów sieciowych.

Ograniczający ruch sieciowy : liczba routerów dostępnych obecnie na rynku ma funkcje które pozwalają ograniczyć ilość pasma, które mogą pobierać niektóre typy ruchu. To jest czasami określane jako kształtowanie ruchu.

Systemy wykrywania włamań : System wykrywania włamań (IDS) służy do wykrywania napastników komunikujących się z maszynami typu slave, master lub agent. Dzięki temu dowiesz się, czy komputer

w twojej sieci jest używany do przeprowadzenia znanego ataku, ale prawdopodobnie nie wykryje nowych odmian tych ataków ani narzędzi, które je zaimplementują. Większość dostawców IDS ma sygnatury do wykrywania ruchu sieciowego Trinoo, TFN lub Stacheldraht.

Zautomatyzowane narzędzia do śledzenia sieci : Śledzenie strumieni pakietów z fałszywymi adresami za pośrednictwem sieci jest czasochłonnym zadaniem, które wymaga współpracy wszystkich sieci obsługujących ruch i które należy wykonać w trakcie ataku.

Narzędzia do audytu serwera i narzędzia do audytu sieciowego : Dostępne są narzędzia do skanowania plików, które próbują wykryć obecność znanych plików binarnych klienta i serwera narzędzia DDoS w systemie. Narzędzia do skanowania sieciowego próbują wykryć obecność agentów DDoS działających na hostach w sieci.

Narzędzia do skanowania DoS

Find_ddos to narzędzie, które skanuje lokalny system, który prawdopodobnie zawiera program DDoS. Może wykryć kilka znanych narzędzi ataków DoS.

SARA zbiera informacje o zdalnych hostach i sieciach, sprawdzając usługi sieciowe. Obejmuje to informacje o usługach sieciowych, a także potencjalne luki w zabezpieczeniach, takie jak nieprawidłowo skonfigurowane lub skonfigurowane usługi sieciowe, dobrze znane błędy w systemie lub luki w oprogramowaniu systemu sieciowego wymienione w bazie danych Common Vulnerabilities and Exposures (CVE), i słabe decyzje zasad.

RID to darmowe narzędzie do skanowania, które wykrywa obecność klientów Trinoo, TFN lub Stacheldraht.

Zombie Zapper nakazuje rutynowym operacjom zombie spać, zatrzymując ich atak. Możesz użyć tych samych poleceń, których atakujący użyłby do zatrzymania ataku.

Przejęcie sesji

Przejęcie sesji to sytuacja, w której haker przejmuje kontrolę nad sesją użytkownika po pomyślnym uwierzytelnieniu użytkownika na serwerze. Przejęcie sesji obejmuje atak identyfikujący bieżące identyfikatory sesji komunikacji klient / serwer i przejmowanie sesji klienta. Przejęcie sesji jest możliwe dzięki narzędziom, które wykonują przewidywanie numerów sekwencyjnych. Szczegóły przewidywania liczby sekwencji zostaną omówione w dalszej części w sekcji przewidywania sekwencji. Ataki fałszowania różnią się od ataków typu "hijacking". Podczas ataku podszywania się, haker wykonuje sniffowanie i nasłuchuje ruchu, gdy jest przekazywany w sieci od nadawcy do odbiorcy. Następnie haker wykorzystuje zebrane informacje do podszywania się pod fałszywy adres lub używa legalnego systemu. Przejęcie oznacza aktywne zabranie innego użytkownika do trybu offline w celu przeprowadzenia ataku. Atakujący polega na uwierzytelnionym użytkowniku, który nawiązuje połączenie i uwierzytelnia. Następnie atakujący przejmuje sesję, a ważna sesja użytkownika zostaje przerwana. Przejęcie sesji obejmuje następujące trzy kroki w celu podtrzymania ataku:

Śledzenie sesji Haker identyfikuje otwartą sesję i przewiduje numer sekwencji następnego pakietu.

Desynchronizowanie połączenia Haker wysyła do systemu poprawnego użytkownika pakiet resetowania TCP (RST) lub zakończenia (FIN), aby spowodować zamknięcie sesji.

Wstrzykiwanie pakietu atakującego Haker wysyła serwerowi pakiet TCP z przewidywanym numerem kolejnym, a serwer akceptuje go jako następny pakiet prawidłowego użytkownika.

Hakerzy mogą wykorzystywać dwa typy przechwytywania sesji: aktywne i pasywne. Podstawową różnicą między hijackowaniem aktywnym i pasywnym jest poziom zaangażowania hakera w sesję. W aktywnym ataku atakujący znajduje aktywną sesję i przejmuje sesję za pomocą narzędzi, które przewidują następny numer sekwencji używany w sesji TCP. W ataku pasywnym atakujący przechwytuje sesję, a następnie obserwuje i rejestruje cały ruch, który jest wysyłany przez prawowitego użytkownika. Bierne przechwytywanie sesji to tak naprawdę nie tylko sniffowanie. Gromadzi informacje, takie jak hasła, a następnie wykorzystuje te informacje do uwierzytelniania jako osobna sesja.

Pojęcia TCP: trójdrożny uzgadnianie

Dwie kluczowe cechy TCP to niezawodność i uporządkowane dostarczanie pakietów. Aby osiągnąć te cele, TCP wykorzystuje pakiety potwierdzenia (ACK) i numery porządkowe. Manipulowanie tymi liczbami jest podstawą do przechwytywania sesji TCP. Aby zrozumieć przejmowanie sesji, przyjrzyjmy się potrójnemu uzgodnieniu TCP :

1. Właściwy użytkownik inicjuje połączenie z serwerem. Jest to realizowane przez wysyłanie pakietu na serwer z ustawionym bitem SYN i początkowym numer porządkowy (ISN) użytkownika.

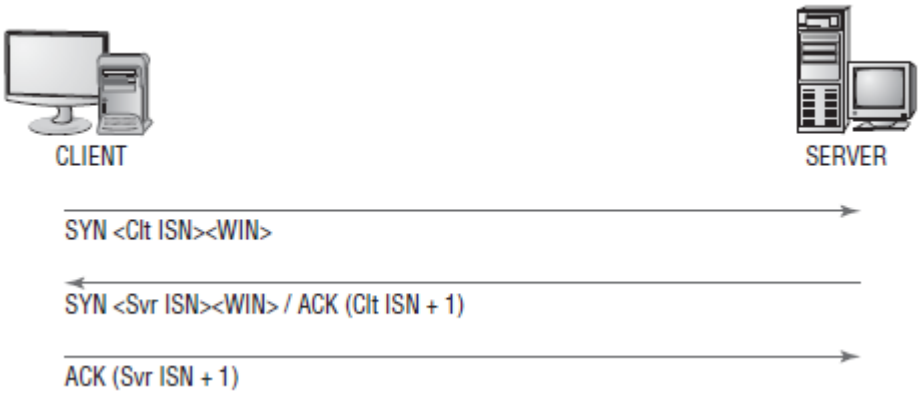
2. Serwer odbiera ten pakiet i odsyła pakiet z zestawem bitów SYN i numerem ISN serwera oraz zestawem bitów ACK identyfikującym numer ISN użytkownika zwiększony o wartość 1.

3. Prawidłowy użytkownik potwierdza serwer, zwracając pakiet z ustawionym bitem ACK i zwiększenie numeru ISN serwera o 1.

To połączenie może zostać zamknięte z dowolnej strony z powodu przekroczenia limitu czasu lub po otrzymaniu pakietu z zestawem flag FIN lub RST. Po wyodebraniu pakietu z zestawem flag RST, system odbierający zamyka połączenie, a wszelkie przychodzące pakiety dla sesji są odrzucane. Jeśli flaga FIN jest ustawiona w pakiecie, system odbierający przechodzi przez proces zamykania połączenia, a wszystkie pakiety odebrane podczas zamykania połączenia są nadal przetwarzane. Wysyłanie pakietu z zestawem flag FIN lub RST jest najczęstszym sposobem, który porywacze używają do zamknięcia sesji klienta z serwerem i przejęcia sesji, działając jako klient.

Przewidywanie sekwencji

TCP jest protokołem zorientowanym na połączenie, odpowiedzialnym za ponowne zestawianie strumieni pakietów w ich pierwotnej zamierzonej kolejności. Każdemu pakietowi należy przypisać unikalny numer sesji, który umożliwia urządzeniu odbierającemu ponowne złożenie strumienia pakietów w ich pierwotnej i zamierzonej kolejności; ten unikalny numer jest znany jako numer kolejny. Jeśli pakiety przychodzą nieregularnie, tak jak dzieje się to regularnie przez Internet, to SN jest używany do prawidłowego przesyłania pakietów. Jak pokazano, system inicjujący sesję TCP przesyła pakiet z ustawionym bitem SYN. Nazywa się to pakietem synchronizacji i zawiera numer ISN klienta. ISN jest pseudolosowo generowaną liczbą z ponad 4 miliardami możliwych kombinacji, ale jest to statystycznie możliwe do powtórzenia. Gdy pakiet ACK jest wysyłany, każde urządzenie używa SN z potwierdzanego pakietu plus przyrost. To nie tylko poprawnie potwierdza odbiór określonego pakietu, ale także informuje nadawcę o następnym oczekiwanym SN pakietu TCP. W ramach potrójnego uzgadniania wartość przyrostu wynosi 1. W normalnej komunikacji danych wartość przyrostu jest równa wielkości danych w bajtach (na przykład, jeśli transmitowane jest 45 bajtów danych, ACK odpowiada za pomocą SN pakietu przychodzącego plus 45).



Narzędzia hakerskie służące do przechwytywania sesji przewidują numer sekwencji. Aby pomyślnie wykonać atak przewidywania sekwencji TCP, haker musi wykryć ruch między dwoma systemami. Następnie haker lub narzędzie hakerskie musi z powodzeniem odgadnąć SN lub zlokalizować ISN, aby obliczyć następny numer sekwencji. Proces ten może być trudniejszy, niż się wydaje, ponieważ pakiety podróżują bardzo szybko. Gdy haker nie jest w stanie powąchać połączenia, znacznie trudniej jest odgadnąć następny SN. Z tego powodu większość narzędzi służących do przechwytywania sesji zawiera funkcje do zezwolenia na sniffowanie pakietów w celu określenia SN. Hakerzy generują pakiety przy użyciu fałszywego adresu IP systemu, który miał sesję z systemem docelowym. Narzędzia hakerskie wysyłają pakiety z SN, których oczekuje system docelowy. Ale pakiety hakerów muszą dotrzeć przed pakietami z zaufanego systemu, którego połączenie zostało przejęte. Osiąga się to poprzez zalanie zaufanego systemu pakietami lub wysłanie pakietu RST do zaufanego systemu tak, że nie jest możliwe wysyłanie pakietów do systemu docelowego.

Narzędzia hakerskie

Juggernaut to sniffer sieciowy, za pomocą którego można przechwytywać sesje TCP. Działa na systemach operacyjnych Linux i może być używany do oglądania całego ruchu sieciowego lub może otrzymać słowo kluczowe, takie jak hasło do wyszukiwania. Program pokazuje wszystkie aktywne połączenia sieciowe, a atakujący może następnie wybrać sesję do przejęcia.

Hunt to program, który może być używany do wykrywania i przejęcia aktywnych sesji w sieci. Hunt wykonuje zarządzanie połączeniami, spoofing ARP (Address Resolution Protocol), resetowanie połączeń, monitorowanie połączeń, wykrywanie adresów Media Access Control (MAC) i sniffowanie ruchu TCP.

TTYWatcher to narzędzie do przechwytywania sesji, które pozwala porywaczowi zwrócić skradzioną sesję do prawidłowego użytkownika, tak jakby nigdy nie została przejęta. TTYWatcher jest przeznaczony tylko dla systemów Sun Solaris.

IP Watcher to narzędzie do przechwytywania sesji, które umożliwia atakującemu monitorowanie połączeń i przejęcie sesji. Ten program może monitorować wszystkie połączenia w sieci, umożliwiając intruzowi oglądanie dokładnej kopii sesji w czasie rzeczywistym.

T-Sight to narzędzie do monitorowania i przechwytywania sesji dla systemu Windows, które może pomóc w przypadku próby włamania do sieci lub wystąpienia kompromisu. Dzięki T-Sight administrator systemu może monitorować wszystkie połączenia sieciowe w czasie rzeczywistym i obserwować wszelkie podejrzane działania, które mają miejsce. T-Sight może również przejąć kontrolę nad sesją TCP w sieci. Ze względów bezpieczeństwa, En Garde Systems udziela licencji na to oprogramowanie tylko z góry ustalonymi adresami IP.

Narzędzie zdalnego resetowania sesji TCP wyświetla bieżącą sesję TCP i informacje o połączeniu, takie jak adresy IP i numery portów. Narzędzie służy przede wszystkim do resetowania sesji TCP.

Niebezpieczeństwa stwarzane przez porwanie sesji

Przejęcie sesji TCP jest niebezpiecznym atakiem: większość systemów jest na nie podatna, ponieważ używają protokołu TCP / IP jako głównego protokołu komunikacyjnego. Nowsze systemy operacyjne próbowały zabezpieczyć się przed przechwyceniem sesji, wykorzystując generatory liczb pseudolosowych do obliczenia numeru ISN, przez co numer sekwencji trudniej zgadnąć. Jednak ten środek bezpieczeństwa jest nieskuteczny, jeśli atakujący jest w stanie sniffować pakiety, co daje wszystkie informacje wymagane do przeprowadzenia tego ataku. Oto powody, dla których ważne jest, aby etyczny hacke wiedział o przechwytywaniu sesji:

* Większość komputerów, jest narażonych.

* Dostępnych jest kilka środków zaradczych w celu odpowiedniej ochrony przed nim.

* Ataki polegające na przejmowaniu sesji są łatwe do uruchomienia.

* Przejęcie jest niebezpieczne ze względu na informacje, które można zebrać podczas ataku.

Zapobieganie przechwyceniu sesji

Aby bronić się przed atakami typu "hijack", sieć powinna wykorzystywać kilka mechanizmów obronnych. Najbardziej skuteczną ochroną jest szyfrowanie, takie jak Internet Protocol Security (IPSec). To także chroni przed wszelkimi innymi wektorami ataku, które zależą od sniffingu. Atakujący mogą być w stanie pasywnie monitorować twoje połączenie, ale nie będą w stanie interpretować zaszyfrowanych danych. Inne środki zaradcze obejmują używanie zaszyfrowanych aplikacji, takich jak Secure Shell (SSH, szyfrowany telnet) i Secure Sockets Layer (SSL, dla ruchu HTTPS). Możesz zapobiec przechwytywaniu sesji, zmniejszając potencjalne metody uzyskiwania dostępu do sieci - na przykład eliminując zdalny dostęp do systemów wewnętrznych. Jeśli w sieci znajdują się zdalni użytkownicy, którzy muszą się połączyć, aby wykonywać swoje obowiązki, użyj wirtualnych sieci prywatnych (VPN) zabezpieczonych protokołami tunelowania i szyfrowaniem (protokół tunelowania warstwy 3 [L3TP] / protokół tunelowania punkt-punkt [PPTP] i IPSec). Korzystanie z wielu siatek bezpieczeństwa jest zawsze najlepszym środkiem zaradczym dla każdego potencjalnego zagrożenia. Wykorzystanie jednego środka zaradczego może nie być wystarczające, ale użycie ich razem w celu zabezpieczenia przedsiębiorstwa sprawi, że wskaźnik sukcesu ataku będzie minimalny dla każdego, ale najbardziej profesjonalnego i oddanego atakującemu.

Poniżej znajduje się lista kontrolna środków zaradczych, które należy zastosować, aby zapobiec przechwyceniu sesji:

* Użyj szyfrowania.

* Użyj bezpiecznego protokołu.

* Ogranicz przychodzące połączenia.

* Minimalizuj zdalny dostęp.

* Masz silne uwierzytelnienie.

* Edukuj swoich pracowników.

* Zachowaj inną nazwę użytkownika i hasła dla różnych kont.

* Należy używać przełączników Ethernet zamiast koncentratorów, aby zapobiec atakom polegającym na przechwytywaniu sesji.

Podsumowanie

Ataki typu "odmowa usługi" są używane do renderowania systemu lub sieci i są uznawane za ataki na dostępność danych użytkownika. Kiedy inne próby włamania się nie powiodą, haker może użyć ataków DoS jako sposobu na atakowanie systemu. Mimo że dane nie mogą zostać pozyskane przez hakera używającego DoS, haker może uniemożliwić uprawnionym użytkownikom dostęp do danych. Ataki DoS, a zwłaszcza ataki DDoS, są trudne do przeciwdziałania. Najlepszą opcją jest próba zapobieżenia atakom przy użyciu filtrowania ruchu na zaporze lub IDS. Przejęcie sesji jest wykorzystywane przez hakera do przechwytywania połączenia użytkownika i umieszczania się pomiędzy uprawnionym użytkownikiem a serwerem. Przejęcie sesji polega na przewidywaniu numerów sekwencyjnych i przechwytywaniu legalnych danych TCP / IP i zastępowaniu ich atakiem hakerskim. Przejęcie sesji jest niebezpiecznym atakiem służącym do zbierania wartościowych danych użytkownika, a większość systemów, które uruchamiają stos TCP / IP, jest podatnych na przechwytywanie sesji.

Do Zapamiętania!

* Poznałeś cel ataków typu DoS i DDoS. Celem ataku DoS jest wysłanie tak dużego ruchu do systemu docelowego, że użytkownicy nie mogą uzyskać dostępu do systemu. Rozproszony atak typu "odmowa usługi" (DDoS) jest skoordynowanym atakiem wielu systemów wysłanych do jednego celu, podczas gdy DoS obejmuje pojedynczy system atakujący cel.

* Dowiedziałeś się, jak zapobiegać atakom DoS. Filtrowanie ruchu sieciowego, IDS i narzędzia audytu są wszystkimi sposobami wykrywania i zapobiegania atakom DoS.

* Poznałeś dwie fazy DDoS. Podczas pierwszej fazy systemy są zagrożone i jakie narzędzia DDoS są zainstalowane, dzięki czemu systemy zombie lub slave'ów; nazywa się to fazą intruzji. Druga faza polega na rozpoczęciu ataku na system ofiary.

* Dowiedziałeś się, kim zombie, slave i master są w ataku DDoS. Zombie lub slave to system, który został złamany przez hakera i może zostać poproszony o udział w wysyłaniu ataku DDoS do systemu docelowego. Master jest systemem kontrolującym w scenariuszu ataku DDoS. Informuje zombie, kiedy rozpocząć atak.

* Zrozumiałeś przechwytywania sesji i podszywania się. Przejęcie sesji polega na przejęciu sesji innego użytkownika po uwierzytelnieniu w celu uzyskania dostępu do systemu. Fałszowanie polega na sztucznej identyfikacji adresu źródłowego pakietu, w którym adres ten jest często wyprowadzany ze śledzonego ruchu sieciowego, podczas gdy przejęcie odnosi się do skompromitowanej sesji - zwykle takiej, w której osoba atakująca przenosi użytkownika w tryb offline i korzysta z jego sesji.

* Zapoznałeś się z różnicą między przechwytywaniem sesji aktywnej i pasywnej a niektórymi używanymi narzędziami. Aktywne przejmowanie sesji jest częstsze z dwóch typów i polega na przejmowaniu sesji innego użytkownika i desynchronizacji połączenia użytkownika. Pasywne przechwytywanie monitoruje sesję i umożliwia hakerom zbieranie poufnych informacji przez wąchanie pakietów. Juggernaut, Hunt, TTYWatcher, IP Watcher, T-Sight i narzędzie TCP Reset to narzędzia do przechwytywania sesji.

* Zrozumiałeś znaczenie numerów sekwencji podczas ataku polegającego na przejmowaniu sesji. Konieczne jest odgadnięcie lub zlokalizowanie numerów sekwencji w celu zainicjowania ataku

polegającego na przejmowaniu sesji. Numery sekwencji są używane do zamawiania pakietów i zezwalania stacji odbiorczej na prawidłowe składanie danych.

* Zapoznałeś się z niebezpieczeństwami i przeciwdziałaniem porwania sesji. Większość komputerów jest podatna na ataki polegające na przejmowaniu sesji, a dostępne środki zaradcze nie zawsze są skuteczne. Poufne i ważne informacje, takie jak hasła, informacje o koncie i numery kart kredytowych, można uzyskać poprzez ataki polegające na przejmowaniu sesji. Użyj szyfrowania, silnego uwierzytelniania i bezpiecznych protokołów; ograniczać połączenia przychodzące; zminimalizować połączenia zdalnego dostępu; kształcić pracowników; i utrzymywać unikalne nazwy użytkownika i hasła dla różnych kont.