Skanowanie sieci

Cele kształcenia

Po zidentyfikowaniu celu i przeprowadzeniu wstępnego rekonesansu, omówionego w module Footprinting i Rozpoznanie, atakujący rozpoczynają poszukiwania punktu wejścia do docelowego systemu. Atakujący powinni określić, czy systemy docelowe są aktywne, czy nieaktywne, aby skrócić czas skanowania. Warto zauważyć, że samo skanowanie nie jest faktycznym włamaniem, ale rozszerzoną formą rekonesansu, w ramach której atakujący dowiaduje się więcej o swoim celu, w tym o systemach operacyjnych, usługach i wszelkich błędach w konfiguracji. Informacje zebrane podczas takiego rekonesansu pomagają atakującemu wybrać strategie ataku na docelowy system lub sieć. Ten moduł rozpoczyna się od omówienia skanowania sieci i zapewnia wgląd w różne techniki wykrywania hostów, których można użyć do sprawdzenia aktywnych i aktywnych systemów. Ponadto omawia różne techniki wykrywania portów i usług, techniki wykrywania systemów operacyjnych oraz techniki skanowania poza systemami IDS i zaporami ogniowymi. Na końcu kończy się przeglądem rysowania diagramów sieciowych. Pod koniec tego modułu będziesz w stanie:

* Opisać koncepcje skanowania sieciowego

* Używać różnych narzędzi do skanowania

* Wykonać wykrywanie hosta, aby sprawdzić działające systemy

* Wykonywać wykrywania portów i usług przy użyciu różnych technik skanowania

* Wykonać wykrywanie systemu operacyjnego (OS).

* Skanować poza systemami wykrywania włamań (IDS) i zaporami sieciowymi

* Wyjaśnić różne środki zaradcze związane ze skanowaniem sieci

Pojęcia dotyczące skanowania sieciowego

Jak już wspomniano, footprinting to pierwsza faza hakowania, w której atakujący uzyskuje podstawowe informacje o potencjalnym celu. Następnie wykorzystuje te informacje w fazie skanowania, aby zebrać więcej szczegółów na temat celu.

Omówienie skanowania sieciowego

* Skanowanie sieci odnosi się do zestawu procedur służących do identyfikowania hostów, portów i usług w sieci Wysyła sondy TCP/IP

* Skanowanie sieci jest jednym z elementów gromadzenia danych wywiadowczych, które atakujący może wykorzystać do stworzenia profilu docelowej organizacji

Cele skanowania sieciowego

* Aby odkryć systemy operacyjne i architekturę systemu

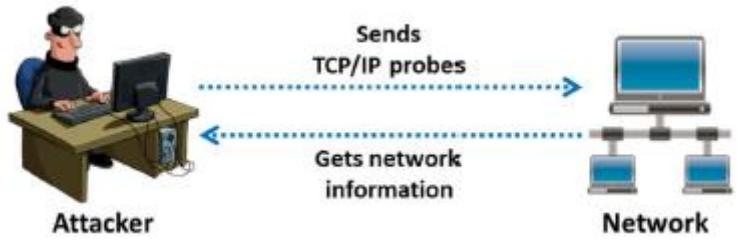
* Aby odkryć usługi działające na hostach

* Aby wykryć luki w hostach na żywo

Omówienie skanowania sieciowego

Skanowanie to proces zbierania dodatkowych szczegółowych informacji o celu przy użyciu bardzo złożonych i agresywnych technik rozpoznawczych. Skanowanie sieci odnosi się do zestawu procedur

używanych do identyfikowania hostów, portów i usług w sieci. Skanowanie sieci jest również wykorzystywane do wykrywania aktywnych komputerów w sieci i identyfikowania systemu operacyjnego działającego na komputerze docelowym. Jest to jeden z najważniejszych etapów zbierania danych wywiadowczych przez atakującego, który umożliwia mu stworzenie profilu atakowanej organizacji. W trakcie skanowania osoba atakująca próbuje zebrać informacje, w tym konkretne adresy IP, do których można uzyskać dostęp przez sieć, system operacyjny i architekturę systemu docelowego oraz porty wraz z odpowiednimi usługami uruchomionymi na każdym komputerze.



Celem skanowania jest odkrycie możliwych do wykorzystania kanałów komunikacyjnych, sondowanie jak największej liczby słuchaczy i śledzenie tych, które odpowiadają lub są przydatne dla określonych potrzeb atakującego. W fazie skanowania atakujący próbuje znaleźć różne sposoby wtargnięcia do systemu docelowego. Atakujący próbuje również uzyskać więcej informacji o systemie docelowym, aby określić obecność jakichkolwiek uchybień w konfiguracji. Następnie atakujący wykorzystuje uzyskane informacje do opracowania strategii ataku.

Rodzaje skanowania

* Skanowanie portów - wyświetla listę otwartych portów i usług. Skanowanie portów to proces sprawdzania usług uruchomionych na komputerze docelowym poprzez wysłanie sekwencji komunikatów w celu próby włamania. Skanowanie portów obejmuje łączenie się lub sprawdzanie portów TCP i UDP systemu docelowego w celu określenia, czy usługi są w stanie słuchania. Stan nasłuchiwania dostarcza informacji o systemie operacyjnym i aktualnie używanej aplikacji. Czasami aktywne usługi, które nasłuchują, mogą umożliwiać nieautoryzowanym użytkownikom błędną konfigurację systemów lub uruchamianie oprogramowania z lukami w zabezpieczeniach.

* Skanowanie sieci — wyświetla listę aktywnych hostów i adresów IP. Skanowanie sieci to procedura identyfikowania aktywnych hostów w sieci w celu ich zaatakowania lub oceny bezpieczeństwa sieci.

* Skanowanie luk w zabezpieczeniach — pokazuje obecność znanych słabych punktów. Skanowanie pod kątem luk w zabezpieczeniach to metoda sprawdzania, czy system można wykorzystać, poprzez identyfikację jego luk w zabezpieczeniach. Skaner podatności składa się z silnika skanującego i katalogu. Katalog zawiera listę typowych plików ze znanymi lukami i typowymi exploitami dla szeregu serwerów. Skaner luk w zabezpieczeniach może na przykład szukać plików kopii zapasowych lub exploitów związanych z przeglądaniem katalogów. Silnik skanujący utrzymuje logikę odczytu listy exploitów, przesyłania żądania do serwera WWW i analizowania żądań w celu zapewnienia bezpieczeństwa serwera. Narzędzia te generalnie atakują luki w zabezpieczeniach, które konfiguracje bezpiecznych hostów mogą łatwo naprawić za pomocą zaktualizowanych poprawek zabezpieczeń i przejrzystego dokumentu internetowego. Złodziej, który chce włamać się do domu, szuka punktów dostępu, takich jak drzwi i okna. Są to zwykle słabe punkty domu, ponieważ są łatwo dostępne. Jeśli chodzi o systemy i sieci komputerowe, porty są drzwiami i oknami systemu, przez które intruz uzyskuje dostęp. Ogólna zasada dotycząca systemów komputerowych jest taka, że im większa liczba otwartych portów w

systemie, tym bardziej system jest podatny na ataki. Istnieją jednak przypadki, w których system z mniejszą liczbą otwartych portów niż inna maszyna przedstawia znacznie wyższy poziom podatności.

Cele skanowania sieciowego

Im więcej informacji na temat docelowej organizacji, tym większe są szanse na poznanie luk w zabezpieczeniach sieci, a w konsekwencji na uzyskanie do niej nieautoryzowanego dostępu. Oto niektóre cele skanowania sieci:

• Odkryj hosty na żywo w sieci, adresy IP i otwarte porty hostów na żywo. Korzystając z otwartych portów, atakujący określi najlepszy sposób wejścia do systemu.

• Odkryj system operacyjny i architekturę systemu docelowego. Jest to również znane jako pobieranie odcisków palców. Atakujący może sformułować strategię ataku w oparciu o luki w systemie operacyjnym.

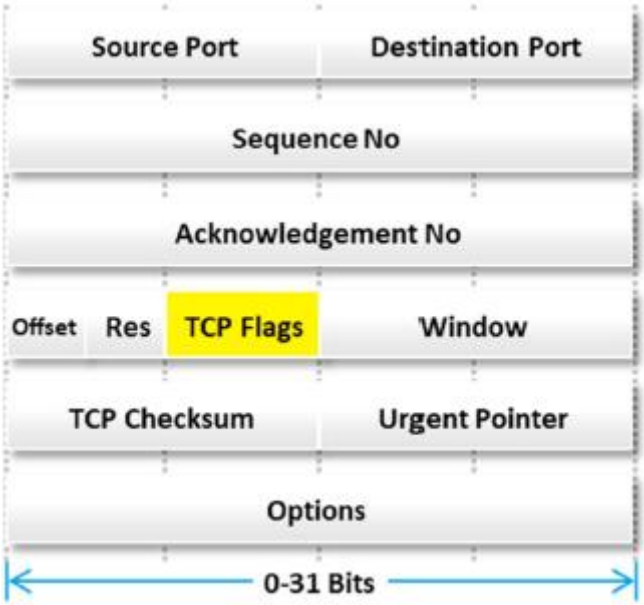
• Odkryj usługi uruchomione/nasłuchujące w systemie docelowym. W ten sposób osoba atakująca może wskazać luki w zabezpieczeniach (w zależności od usługi), które można wykorzystać w celu uzyskania dostępu do systemu arget.

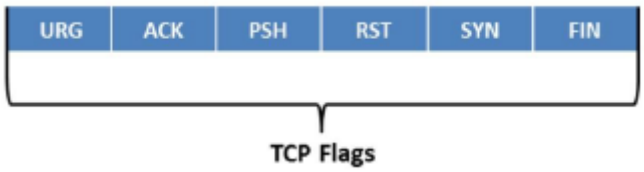
• Zidentyfikuj konkretne aplikacje lub wersje określonej usługi.

• Zidentyfikuj luki w dowolnym systemie sieciowym. Pomaga to atakującemu w naruszeniu docelowego systemu lub sieci za pomocą różnych exploitów.

Flagi komunikacji TCP

Nagłówek TCP zawiera różne flagi sterujące transmisją danych przez połączenie TCP. Sześć flag kontrolnych TCP zarządza połączeniem między hostami i przekazuje instrukcje systemowi. Cztery z tych flag (SYN, ACK, FIN i RST) regulują nawiązywanie, utrzymywanie i przerywanie połączenia. Pozostałe dwie flagi (PSH i URG) przekazują instrukcje systemowi. Rozmiar każdej flagi to 1 bit. Ponieważ w sekcji Flagi TCP znajduje się sześć flag, rozmiar tej sekcji wynosi 6 bitów. Gdy wartość flagi jest ustawiona na „1”, ta flaga jest automatycznie włączana.





Poniżej przedstawiono flagi komunikacji TCP:

* Synchronizuj lub „SYN”: Powiadamia o transmisji nowego numeru sekwencyjnego. Ta flaga ogólnie reprezentuje ustanowienie połączenia (trójstronne uzgadnianie) między dwoma gospodarzami.

* Potwierdzenie lub „ACK”: Potwierdza odbiór transmisji i identyfikuje następny oczekiwany numer sekwencyjny. Kiedy system pomyślnie odbiera pakiet, ustawia wartość swojej flagi na „1”, co oznacza, że odbiorca powinien zwrócić na niego uwagę.

* Push lub „PSH”: Gdy jest ustawiony na „1”, oznacza to, że nadawca podniósł operację push do odbiorcy; oznacza to, że zdalny system powinien informować aplikację odbierającą o zbuforowanych danych pochodzących od nadawcy. System podnosi flagę PSH na początku i na końcu przesyłania danych i ustawia ją na ostatnim segmencie pliku, aby zapobiec zakleszczeniu bufora.

* Pilne lub „URG”: nakazuje systemowi jak najszybsze przetworzenie danych zawartych w pakietach. Gdy system ustawia flagę na „1”, pierwszeństwo ma przetwarzanie pilnych danych, a wszystkie inne przetwarzanie danych jest zatrzymywane.

* Zakończ lub „FIN”: Ustawia się na „1”, aby ogłosić, że żadne dalsze transmisje nie będą wysyłane do systemu zdalnego, a połączenie ustanowione przez flagę SYN zostanie zakończone.

* Reset lub „RST”: Gdy w bieżącym połączeniu wystąpi błąd, ta flaga jest ustawiana na „1”, a połączenie jest przerywane w odpowiedzi na błąd. Atakujący używają tej flagi do skanowania hostów i identyfikowania otwartych portów.

Skanowanie SYN dotyczy głównie trzech flag: SYN, ACK i RST. Możesz użyć tych trzech flag do zbierania nielegalnych informacji z serwerów podczas wyliczania.

Komunikacja TCP/IP

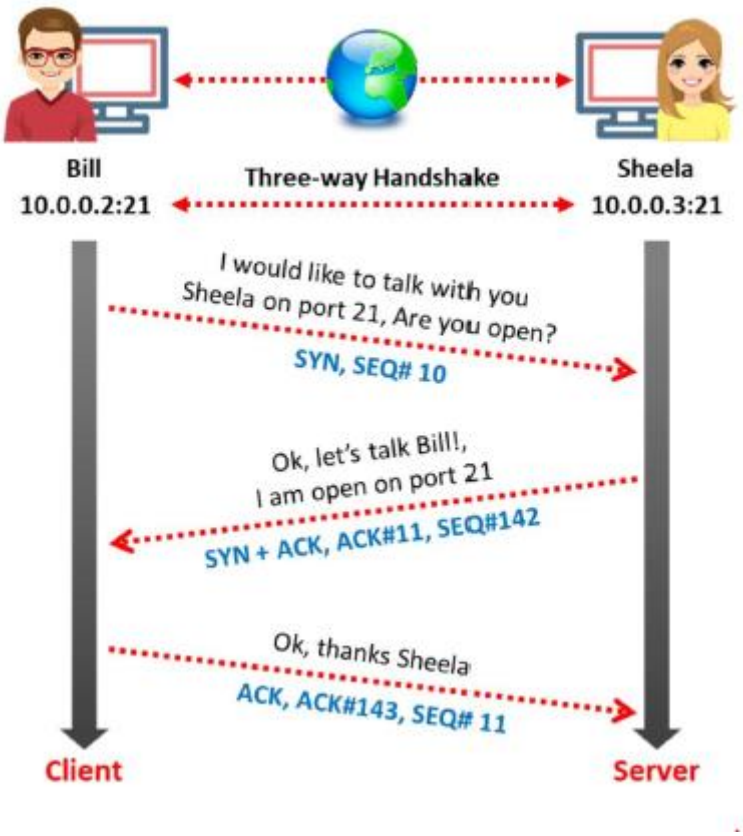
Protokół TCP jest zorientowany na połączenie, tj. nadaje priorytet ustanawianiu połączenia przed przesyłaniem danych między aplikacjami. To połączenie między protokołami jest możliwe dzięki trójstronnemu uzgadnianiu. Sesja TCP jest inicjowana przy użyciu mechanizmu trójstronnego uzgadniania:* Aby uruchomić połączenie TCP, źródło (10.0.0.2:21) wysyła pakiet SYN do miejsca docelowego (10.0.0.3:21).

* Po otrzymaniu pakietu SYN miejsce docelowe odpowiada, wysyłając pakiet SYN/ACK z powrotem do źródła.

* Pakiet ACK potwierdza nadejście pierwszego pakietu SYN do źródła.

* Na koniec źródło wysyła pakiet ACK dla pakietu ACK/SYN przesłanego przez miejsce docelowe.

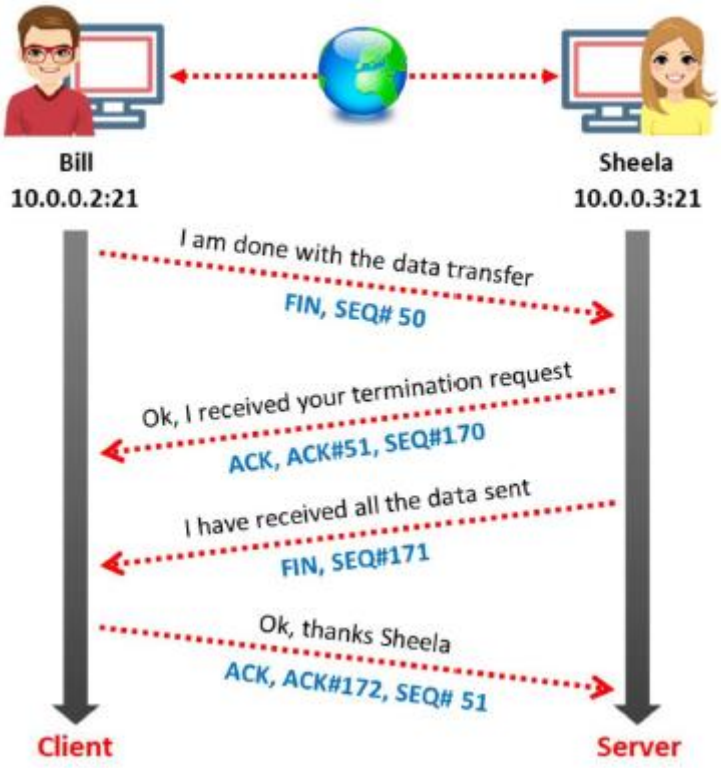
* Uruchamia to połączenie „OPEN”, umożliwiając w ten sposób komunikację między źródłem a miejscem docelowym, która trwa, dopóki jedno z nich nie wyśle pakietu „FIN” lub „RST” w celu zamknięcia połączenia.



Protokół TCP utrzymuje stanowe połączenia dla wszystkich protokołów zorientowanych na połączenie w Internecie i działa podobnie do zwykłej komunikacji telefonicznej, w której podnosi się słuchawkę telefonu, słyszy sygnał wybierania i wybiera numer, który wyzwala dzwonienie na drugim końcu, dopóki ktoś podnosi słuchawkę i mówi: „Cześć".

System kończy nawiązaną sesję TCP w następujący sposób:

Po zakończeniu wszystkich transferów danych przez ustanowione połączenie TCP, nadawca wysyła żądanie zakończenia połączenia do odbiorcy za pośrednictwem pakietu FIN lub RST. Po otrzymaniu żądania zakończenia połączenia, odbiorca potwierdza żądanie zakończenia, wysyłając pakiet ACK do nadawcy i ostatecznie wysyła własny pakiet FIN. Następnie system przerywa nawiązane połączenie.



Narzędzia do skanowania

Narzędzia skanujące służą do skanowania i identyfikowania aktywnych hostów, otwartych portów, uruchomionych usług w sieci docelowej, informacji o lokalizacji, informacji NetBIOS oraz informacji o wszystkich otwartych portach TCP/IP i UDP. Informacje uzyskane z tych narzędzi pomogą etycznemu hakerowi w stworzeniu profilu docelowej organizacji i przeskanowaniu sieci w poszukiwaniu otwartych portów podłączonych urządzeń.

Nmap

Nmap („Network Mapper") to skaner bezpieczeństwa do eksploracji sieci i hakowania. Pozwala wykryć hosty, porty i usługi w sieci komputerowej, tworząc w ten sposób „mapę" sieci. Wysyła specjalnie spreparowane pakiety do hosta docelowego, a następnie analizuje odpowiedzi, aby osiągnąć swój cel. Skanuje rozległe sieci dosłownie setek tysięcy maszyn. Nmap zawiera wiele mechanizmów skanowania portów (TCP i UDP), wykrywania systemu operacyjnego, wykrywania wersji, sprawdzania pingów i tak dalej. Zarówno administrator sieci, jak i osoba atakująca mogą użyć tego narzędzia do swoich konkretnych potrzeb. Administratorzy sieci mogą używać Nmap do inwentaryzacji sieci, zarządzania harmonogramami aktualizacji usług oraz monitorowania czasu pracy hosta lub usługi. Atakujący używają Nmap do wydobywania informacji, takich jak aktywne hosty w sieci, otwarte porty, usługi (nazwa i wersja aplikacji), typ filtrów pakietów/zapór ogniowych, szczegóły MAC i systemy operacyjne wraz z ich wersjami.

Składnia: # nmap <opcje> <Docelowy adres IP>

Hping3

Hping3 to zorientowane na wiersz poleceń narzędzie do skanowania sieci i tworzenia pakietów dla protokołu TCP/IP, które wysyła żądania echa ICMP i obsługuje protokoły TCP, UDP, ICMP i raw-IP. Wykonuje audyty bezpieczeństwa sieci, testowanie zapory, ręczne wykrywanie MTU ścieżki,

zaawansowane traceroute, zdalny odcisk palca systemu operacyjnego, zdalne zgadywanie czasu pracy, audyt stosów TCP/IP i inne funkcje. Może wysyłać niestandardowe pakiety TCP/IP i wyświetlać odpowiedzi docelowe w sposób podobny do program ping z odpowiedziami ICMP. Obsługuje fragmentację, a także dowolną treść i rozmiar pakietu i może być używany do przesyłania zahermetyzowanych plików w obsługiwanych protokołach. Obsługuje również skanowanie bezczynnego hosta. Podszywanie się pod adresy IP i skanowanie sieci/hostów może służyć do anonimowego sondowania usług. Hping3 posiada również tryb Traceroute, który umożliwia atakującym przesyłanie plików między ukrytymi kanałami. Określa również, czy host działa, nawet jeśli host blokuje pakiety ICMP. Jego użycie przypominające Firewalk umożliwia wykrywanie otwartych portów za zaporami ogniowymi. Wykonuje ręczne wykrywanie MTU ścieżki i umożliwia atakującym wykonanie zdalnego odcisku palca systemu operacyjnego. Korzystając z Hping, osoba atakująca może zbadać zachowanie bezczynnego hosta i uzyskać informacje o celu, takie jak usługi oferowane przez hosta, porty obsługujące usługi oraz system operacyjny celu. Ten rodzaj skanowania jest poprzednikiem cięższych ataków sondujących lub bezpośrednich ataków.

Składnia: # hping3 <opcje> <Docelowy adres IP>

Komendy Hping

Różne polecenia Hping są następujące:

ping ICMP

Ex. hping3 -1 10.0.0.25

Skanowanie ping lub Internet Control Message Protocol (ICMP) to proces wysyłania żądania ICMP ping do wszystkich hostów w sieci w celu ustalenia, które z nich działają. System operacyjny, router, przełącznik i urządzenia oparte na protokole IP używają tego protokołu za pośrednictwem polecenia ping do żądania echa i odpowiedzi echa jako testera łączności między różnymi hostami. Hping wykonuje skanowanie ping ICMP, podając argument -1 w wierszu poleceń. Możesz użyć -ICMP lub -1 jako argumentu w wierszu poleceń. Wydając powyższe polecenie, hping wysyła żądanie echa ICMP do 10.0.0.25 i odbiera odpowiedź ICMP podobnie jak narzędzie ping.

o Skanowanie ACK na porcie 80

Ex. hping3 -A 10.0.0.25 -p 80

Ta technika skanowania może być wykorzystana do zbadania istnienia zapory i jej zestawów reguł. Proste filtrowanie pakietów umożliwia nawiązanie połączenia (pakiety z ustawionym bitem ACK), podczas gdy wyrafinowany firewall stanowy nie pozwala na nawiązanie połączenia. Hping można skonfigurować do wykonywania skanowania ACK, podając argument -A w wierszu poleceń. Tutaj ustawiasz flagę ACK w pakietach sondujących i przeprowadzasz skanowanie. Wykonujesz to skanowanie, gdy host nie odpowiada na żądanie ping. Wydając to polecenie, Hping sprawdza, czy host działa w sieci. Jeśli znajdzie działającego hosta i otwarty port, zwraca odpowiedź RST.

o Skanowanie UDP na porcie 80

Ex. hping3 -2 10.0.0.25 -p 80

Hping używa protokołu TCP jako domyślnego protokołu. Użycie argumentu -2 w wierszu poleceń określa, że Hping działa w trybie UDP. Możesz użyć -udp lub -2 jako argumentu w wierszu poleceń. Wydając powyższe polecenie, Hping wysyła pakiety UDP na port 80 na hoście (10.0.0.25). Zwraca

komunikat o nieosiągalności portu ICMP, jeśli znajdzie port zamknięty i nie zwraca komunikatu, jeśli port jest otwarty.

o Zbieranie początkowego numeru sekwencyjnego

Ex. hping3 192.168.1.103 -Q -p 139

Używając argumentu -Q w wierszu poleceń, Hping zbiera wszystkie numery sekwencyjne TCP wygenerowane przez hosta docelowego (192.168.1.103).

o Zapory sieciowe i znaczniki czasu

Ex. hping3 -S 72.14.207.99 -p 80 --tcp-timestamp

Wiele zapór odrzuca te pakiety TCP, które nie mają ustawionej opcji TCP Timestamp. Dodając argument --tcp-timestamp w wierszu poleceń, możesz włączyć opcję znacznika czasu TCP w Hping i spróbować odgadnąć częstotliwość aktualizacji znacznika czasu i czas pracy hosta docelowego (72.14.207.99).

o Skanowanie SYN na porcie 50-60

Ex. hping3 -8 50-60 -S 10.0.0.25 -V

Używając argumentu -8 lub -scan w wierszu poleceń, uruchamiasz Hping w trybie skanowania, aby przeskanować zakres portów na hoście docelowym. Dodanie argumentu -S umożliwia wykonanie skanowania SYN. Dlatego powyższe polecenie wykonuje skanowanie SYN na portach 50-60 na hoście docelowym.

o Skanowanie FIN, PUSH i URG na porcie 80

Ex. hping3 -F -P -U 10.0.0.25 -p 80

Dodając argumenty -F, -P i -U w wierszu poleceń, ustawiasz pakiety FIN, PUSH i URG w pakietach sondujących. Wydając to polecenie, wykonujesz skanowanie FIN, PUSH i URG na porcie 80 hosta docelowego (10.0.0.25). Jeśli port 80 jest otwarty, nie otrzymasz odpowiedzi. Jeśli port jest zamknięty, Hping zwróci odpowiedź RST.

o Przeskanuj całą podsieć w poszukiwaniu żywego hosta

Ex. hping3 -1 10.0.1.x --rand-dest -I ethO

Wydając to polecenie, Hping wykonuje skanowanie ICMP ping w całej podsieci 10.0.1.x; innymi słowy, losowo wysyła żądanie echa ICMP (-rand-dest) do wszystkich hostów od 10.0.1.0 do 10.0.1.255, które są podłączone do interfejsu ethO. Hosty, których porty są otwarte, odpowiedzą odpowiedzią ICMP. W tym przypadku nie ustawiłeś portu; stąd Hping domyślnie wysyła pakiety do portu 0 na wszystkich adresach IP.

o Przechwytuj cały ruch zawierający sygnaturę HTTP

Ex. hping3 -9 HTTP -I etO

Argument -9 ustawi Hping w trybie nasłuchiwania. Stąd, wydając polecenie -9 HTTP, Hping zaczyna nasłuchiwać na porcie 0 (ze wszystkich urządzeń podłączonych w sieci do interfejsu ethO), przechwytuje wszystkie pakiety zawierające sygnaturę HTTP i zrzuca dane od końca sygnatury do końca pakietu.

o SYN zalewa ofiarę

Ex. hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood

Atakujący wykorzystuje techniki zalewania TCP SYN przy użyciu sfałszowanych adresów IP w celu przeprowadzenia ataku DoS.

Metasploit

Metasploit to projekt typu open source, który zapewnia infrastrukturę, zawartość i narzędzia do przeprowadzania testów penetracyjnych i szeroko zakrojonych audytów bezpieczeństwa. Dostarcza informacji o lukach w zabezpieczeniach i pomaga w testach penetracyjnych i opracowywaniu sygnatur IDS. Ułatwia zadania atakującym, autorom exploitów i autorom ładunków. Główną zaletą frameworka jest podejście modułowe, tj. umożliwiające połączenie dowolnego exploita z dowolnym ładunkiem. Umożliwia zautomatyzowanie procesu wykrywania i wykorzystywania oraz zapewnia narzędzia niezbędne do przeprowadzenia ręcznej fazy testowania testu penetracyjnego. Możesz używać Metasploit Pro do skanowania w poszukiwaniu otwartych portów i usług, wykorzystywania luk w zabezpieczeniach, dalszego wchodzenia w sieć, zbierania dowodów i tworzenia raportów z wyników testów.

NetScanTools Pro

NetScanTools Pro to narzędzie badawcze, które umożliwia rozwiązywanie problemów, monitorowanie, wykrywanie i wykrywanie urządzeń w sieci. Korzystając z tego narzędzia, możesz łatwo zebrać informacje o lokalnej sieci LAN, a także o użytkownikach Internetu, adresach IP, portach i tak dalej. Atakujący mogą znaleźć luki w zabezpieczeniach i odsłonięte porty w systemie docelowym. Pomaga atakującym automatycznie lub ręcznie (przy użyciu narzędzi ręcznych) wyświetlać adresy IPv4/IPv6, nazwy hostów, nazwy domen, adresy e-mail i adresy URL. NetScanTools Pro łączy w sobie wiele narzędzi sieciowych i narzędzi skategoryzowanych według ich funkcji, takich jak aktywny, pasywny, DNS i komputer lokalny.

Poniżej wymieniono niektóre dodatkowe narzędzia do skanowania:

- sx (https://github.com)

- Unicornscan (https://sourceforge.net)

- Skaner portów SolarWinds (https://www.solorwinds.com)

- Monitor sieci PRTG (https://www.poessler.com)

- Analizator protokołów sieciowych OmniPeek (https://www.savvius.com)

Narzędzia do skanowania dla urządzeń mobilnych

IP Scanner

IP Scanner dla iOS skanuje Twoją sieć lokalną, aby określić tożsamość wszystkich jej aktywnych komputerów i urządzeń internetowych. Umożliwia atakującym wykonywanie czynności skanowania sieci wraz ze skanowaniem ping i portów.

Fing

Fing to aplikacja mobilna na Androida i iOS, która skanuje i dostarcza pełne informacje o sieci, takie jak adres IP, adres MAC, dostawca urządzenia i lokalizacja dostawcy usług internetowych. Pozwala atakującym wykryć wszystkie urządzenia podłączone do sieci Wi-Fi wraz z ich adresami IP i MAC, a

także nazwą dostawcy/producenta urządzenia. Pozwala również atakującym na wykonywanie czynności pingowania i śledzenia sieci przez określone porty, takie jak SSH, FTP, NetBIOS itp.

Network Scanner

Network Scanner to aplikacja mobilna na Androida, która umożliwia atakującym identyfikację aktywnych hostów w zakresie możliwych adresów w sieci. Wyświetla również adresy IP, adresy MAC, nazwy hostów i dane dostawców wszystkich dostępnych urządzeń w sieci. To narzędzie umożliwia również atakującym skanowanie portów docelowych za pomocą określonych numerów portów.

Wykrywanie hosta

Skanowanie to proces zbierania informacji o systemach, które „żyją" i reagują w sieci. Wykrywanie hosta jest uważane za podstawowe zadanie w procesie skanowania sieci. Aby wykonać pełne skanowanie i zidentyfikować otwarte porty i usługi, konieczne jest sprawdzenie aktywnych systemów. Wykrywanie hostów zapewnia dokładny stan systemów w sieci, co pozwala atakującemu uniknąć skanowania każdego portu w każdym systemie na liście adresów IP w celu ustalenia, czy docelowy host działa. Wykrywanie hosta to pierwszy krok w skanowaniu sieci. W tej sekcji omówiono sposób sprawdzania aktywnych systemów w sieci za pomocą różnych technik skanowania ping. Omówiono również, jak przeszukiwać sieć w celu wykrycia hostów/systemów na żywo, a także różne narzędzia do przeszukiwania pingów.

Techniki wykrywania hostów

Można zastosować techniki wykrywania hostów w celu wykrycia aktywnych/żywych hostów w sieci. Jako etyczny haker musisz znać różne rodzaje technik wykrywania hostów. Poniżej wymieniono niektóre techniki wykrywania hostów:

* Skanowanie pingów ARP

* Skanowanie pingów UDP

* Skanowanie ICMP ping

* ICMP ECHO Ping

* ICMP ECHO Ping Sweep

* Ping sygnatury czasowej ICMP

* Ping maski adresu ICMP

* Skanowanie pingiem TCP

* TCP SYN Ping

* TCP ACK Ping

* Skanowanie protokołu IP

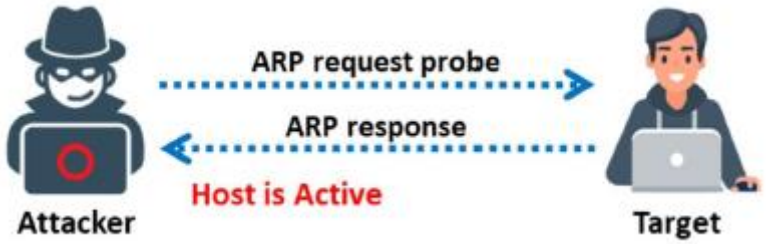
Skanowanie pingów ARP

Podczas skanowania ARP ping pakiety ARP są wysyłane w celu wykrycia wszystkich aktywnych urządzeń w zakresie IPv4, mimo że obecność takich urządzeń jest ukrywana przez restrykcyjne zapory sieciowe. W większości sieci wiele adresów IP jest w danej chwili nieużywanych, szczególnie w prywatnych zakresach adresów sieci LAN. Dlatego, gdy atakujący próbują wysłać pakiety IP, takie jak żądanie echa

ICMP, do hosta docelowego, system operacyjny musi określić sprzętowy adres docelowy (ARP) odpowiadający docelowemu adresowi IP, aby poprawnie zaadresować ramkę ethernetową. W tym celu wysyłana jest seria żądań ARP. Skanowanie ARP służy do wyświetlania adresu MAC interfejsu sieciowego urządzenia, a także może wyświetlać adresy MAC wszystkich urządzeń współużytkujących ten sam adres IPv4 w sieci LAN. Jeśli adres IP hosta z odpowiednim sprzętowym adresem docelowym jest aktywny, odpowiedź ARP zostanie wygenerowana przez hosta; w przeciwnym razie, po określonej liczbie prób ping, oryginalny system operacyjny rezygnuje z hosta. Innymi słowy, gdy atakujący wysyłają sondy żądań ARP do hosta docelowego, jeśli otrzymają jakąkolwiek odpowiedź ARP, oznacza to, że host jest aktywny. Jeśli okaże się, że host docelowy nie odpowiada, host źródłowy dodaje niekompletny wpis do docelowego adresu IP w swojej tablicy ARP jądra. Atakujący używają narzędzia Nmap do wykonywania skanowania ping ARP w celu wykrycia aktywnych hostów w sieci. W Zenmap opcja -PR służy do wykonywania skanowania ping ARP.

Uwaga: -sn to polecenie Nmap do wyłączania skanowania portów. Ponieważ Nmap używa skanowania ping ARP jako domyślnego skanowania ping, aby go wyłączyć i wykonać inne pożądane skanowanie ping, możesz użyć --

disable arp-ping.



Zalety:

* Skanowanie ARP ping jest uważane za bardziej wydajne i dokładne niż inne techniki wykrywania hostów

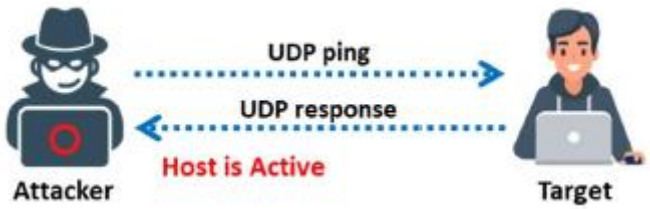
* Skanowanie ARP ping automatycznie obsługuje żądania ARP, retransmisje i limity czasu według własnego uznania

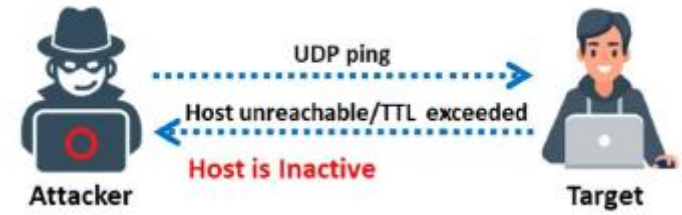
* Skanowanie ARP ping jest przydatne do wykrywania systemu, gdzie może być konieczne przeskanowanie dużych przestrzeni adresowych

* Skanowanie ARP ping może wyświetlać czas odpowiedzi lub opóźnienie urządzenia na pakiet ARP

Skanowanie pingów UDP

Skanowanie ping UDP jest podobne do skanowania ping TCP; jednak podczas skanowania ping UDP Nmap wysyła pakiety UDP do hosta docelowego. Domyślny numer portu używany przez Nmap do skanowania ping UDP to 40 125. Ten bardzo rzadki port jest używany jako domyślny do wysyłania pakietów UDP do celu. Ten domyślny numer portu można skonfigurować za pomocą DEFAULT_UDP_PROBE_PORT_SPEC podczas kompilacji w Nmap. Atakujący wysyłają pakiety UDP do hosta docelowego, a odpowiedź UDP oznacza, że host docelowy jest aktywny. Jeśli host docelowy jest w trybie offline lub jest nieosiągalny, mogą zostać zwrócone różne komunikaty o błędach, takie jak nieosiągalność hosta/sieci lub przekroczenie czasu TTL. W Zenmap opcja -PU służy do wykonywania skanowania ping UDP.





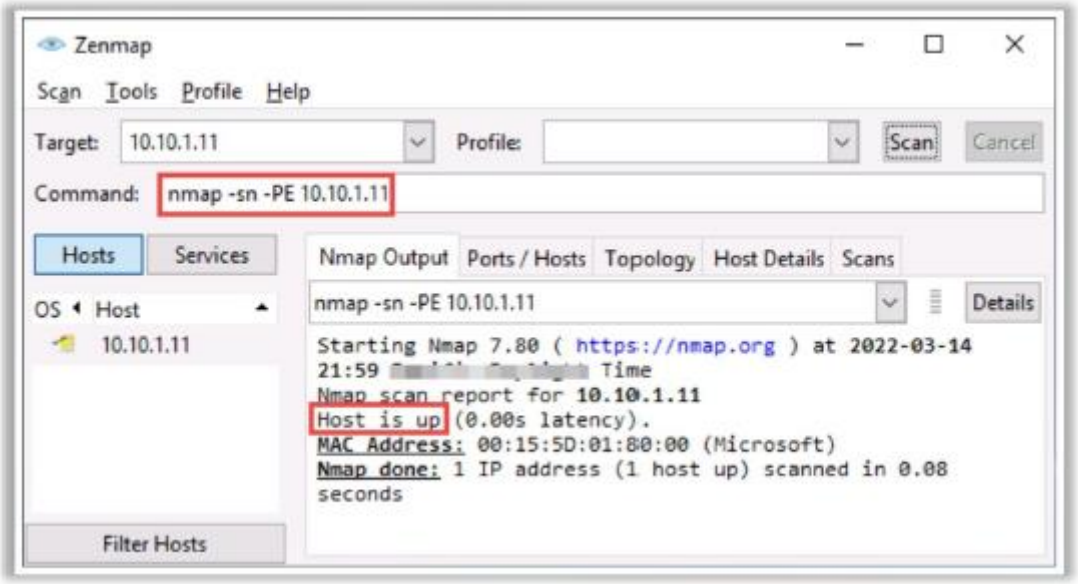
Zalety:

Skanowania ping UDP mają tę zaletę, że wykrywają systemy za zaporami sieciowymi ze ścisłym filtrowaniem TCP, zapominając o ruchu UDP.

Skanowanie ICMP ECHO Ping

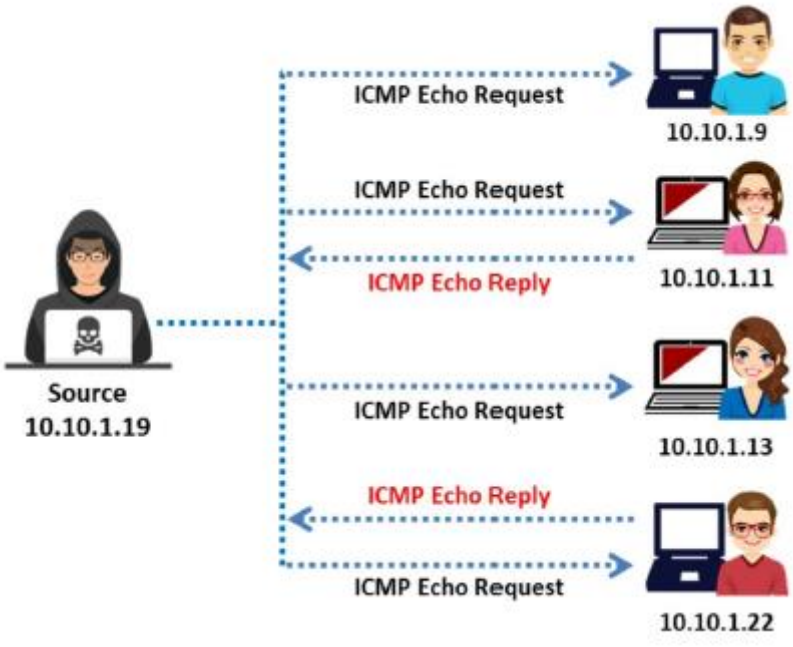
Atakujący używają skanowania ICMP ping do wysyłania pakietów ICMP do systemu docelowego w celu zebrania wszystkich niezbędnych informacji na jego temat. Dzieje się tak, ponieważ protokół ICMP nie obejmuje abstrakcji portów i różni się od skanowania portów. Jednak przydatne jest określenie, które hosty w sieci są uruchomione, wysyłając pakiety ping do wszystkich. Skanowanie ping ICMP ECHO obejmuje wysyłanie żądań ICMP ECHO do hosta. Jeśli host żyje, zwróci odpowiedź ICMP ECHO. To skanowanie jest przydatne do lokalizowania aktywnych urządzeń lub określania, czy protokół ICMP przechodzi przez zaporę.

Maszyny oparte na systemach UNIX/Linux i BSD używają skanowania echa ICMP; implementacje stosu TCP/IP w tych systemach operacyjnych odpowiadają na żądania echa ICMP kierowane do adresów rozgłoszeniowych. Ta technika nie działa w sieciach opartych na systemie Windows, ponieważ ich implementacja stosu TCP/IP nie odpowiada na sondy ICMP skierowane na adres rozgłoszeniowy. Nmap używa opcji -p do skanowania celu przez ICMP. Użytkownik może również zwiększyć liczbę równoległych pingów za pomocą opcji -L. Przydatne może być również dostosowanie wartości limitu czasu ping za pomocą opcji -T. W Zenmap opcja -PE jest używana do wykonywania skanowania ping ICMP ECHO. Aktywne hosty są wyświetlane jako „Host jest aktywny”, jak pokazano na zrzucie ekranu.



ICMP ECHO Ping Sweep

Przeszukiwanie ping (znane również jako przeszukiwanie ICMP) to podstawowa technika skanowania sieci stosowana w celu określenia zakresu adresów IP mapowanych na aktywne hosty (komputery). Chociaż pojedynczy pakiet ping poinformuje użytkownika, czy w sieci istnieje określony komputer hosta, test ping składa się z żądań ICMP ECHO wysyłanych do wielu hostów. Jeśli określony host jest aktywny, zwróci odpowiedź ICMP ECHO. Przeszukiwanie pingów to jedna z najstarszych i najwolniejszych metod używanych do skanowania sieci. To narzędzie jest dystrybuowane na prawie wszystkie platformy i działa jak apel dla systemów; system aktywny w sieci odpowiada na zapytanie ping wysyłane przez inny system. Skanowanie echa ICMP wysyła pakiety ping do wszystkich komputerów w sieci docelowej w celu wykrycia aktywnych komputerów. Atakujący wysyłają sondy ICMP na adres rozgłoszeniowy lub sieciowy, który przekazuje je do wszystkich adresów hostów w podsieci. Aktywne systemy wyślą komunikat odpowiedzi ICMP echo do źródła sondy echa ICMP.



Aby lepiej zrozumieć pingi, należy być w stanie zrozumieć pakiet TCP/IP. Gdy system wysyła polecenie ping, wysyła pojedynczy pakiet przez sieć na określony adres IP. Ten pakiet zawiera 64 bajty (56 bajtów danych i 8 bajtów informacji nagłówka protokołu). Następnie nadawca czeka lub nasłuchuje na pakiet zwrotny z systemu docelowego. Jeśli połączenia są dobre, a komputer docelowy „żyje", oczekiwany jest dobry pakiet zwrotny. Nie będzie to jednak miało miejsca w przypadku zakłóceń w komunikacji. Pingi określają również czas potrzebny pakietowi na wykonanie całej podróży, zwany „czasem podróży w obie strony". Pomagają również w rozwiązywaniu nazw hostów. W takim przypadku, jeśli pakiet odbija się po wysłaniu na adres IP, ale nie po wysłaniu na nazwę, oznacza to, że system nie jest w stanie uzgodnić nazwy z określonym adresem IP. Osoby atakujące obliczają maski podsieci za pomocą kalkulatorów masek podsieci w celu określenia liczby hostów obecnych w podsieci. Następnie używają funkcji ping sweep do utworzenia wykazu aktywnych systemów w podsieci.

ICMP ECHO Ping Sweep przy użyciu Nmap

Nmap pomaga atakującemu przeprowadzić analizę ping, która określa hosty na żywo z zakresu adresów IP. W Zenmap, opcja -PE z listą adresów IP jest używana do wykonania ICMP ECHO ping sweep.

ICMP Timestamp Ping Scan

Oprócz tradycyjnego ICMP ECHO ping istnieją inne rodzaje technik ping ICMP, takie jak ICMP timestamp ping scan i ICMP address mask ping scan, które atakujący może zastosować w określonych warunkach. ICMP ping znacznika czasu to opcjonalny i dodatkowy rodzaj pingu ICMP, w którym osoby atakujące wysyłają zapytanie do wiadomości sygnatury czasowej w celu uzyskania informacji związanych z bieżącym czasem z docelowego komputera hosta. Maszyna docelowa odpowiada odpowiedzią z sygnaturą czasową na każde otrzymane zapytanie o sygnaturę czasową. Jednak odpowiedź hosta docelowego jest warunkowa i może, ale nie musi, odpowiedzieć z wartością czasu, w zależności od konfiguracji dokonanej przez administratora na końcu celu. To pingowanie znacznika czasu ICMP jest zwykle używane do synchronizacji czasu. Taka metoda ping jest skuteczna w identyfikowaniu, czy docelowy komputer hosta jest aktywny, szczególnie w sytuacji, gdy administrator blokuje tradycyjne żądania ping ICMP ECHO. W Zenmap opcja -PP jest używana do wykonywania skanowania ping ICMP znacznika czasu.

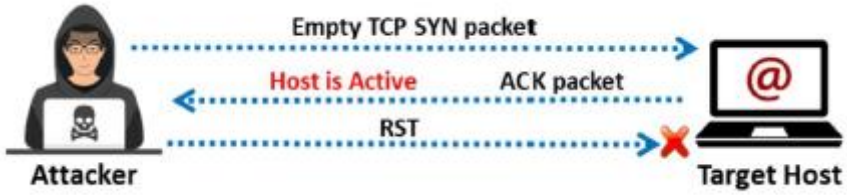
ICMP Address Mask Ping Scan

Polecenie ping maski adresu ICMP to kolejna alternatywa dla tradycyjnego polecenia ping ICMP ECHO, w ramach którego atakujący wysyłają zapytanie o maskę adresu ICMP do hosta docelowego w celu uzyskania informacji związanych z maską podsieci. Jednak odpowiedź maski adresowej z hosta docelowego jest warunkowa i może, ale nie musi, odpowiedzieć z odpowiednią wartością podsieci, w zależności od konfiguracji dokonanej przez administratora na końcu celu. Ten typ metody ping jest również skuteczny w identyfikowaniu aktywnych hostów, podobnie jak ping ICMP ze znacznikiem czasu, zwłaszcza gdy administrator blokuje tradycyjne ping ICMP Echo. W Zenmap opcja -PM jest używana do wykonywania skanowania ping maski adresu ICMP.

Skanowanie pingów TCP SYN

TCP SYN ping to technika wykrywania hostów służąca do sondowania różnych portów w celu określenia, czy port jest w trybie online i sprawdzania, czy napotyka jakiekolwiek zestawy reguł zapory. W tego rodzaju technice wykrywania hostów atakujący używa narzędzia Nmap do zainicjowania trójstronnego uzgadnianie przez wysłanie pustej flagi TCP SYN do hosta docelowego. Po otrzymaniu SYN host docelowy potwierdza odbiór flagą ACK. Po odebraniu flagi ACK atakujący potwierdza, że host docelowy jest aktywny i kończy połączenie, wysyłając flagę RST do docelowego komputera hosta

(ponieważ jego cel wykrycia hosta został osiągnięty). Port 80 jest używany jako domyślny port docelowy. Zakres portów można również określić w tym typie formatu pingowania bez wstawiania spacji między -PS a numerem portu (np. w Zenmap opcja -PS służy do wykonywania skanowania ping TCP SYN.



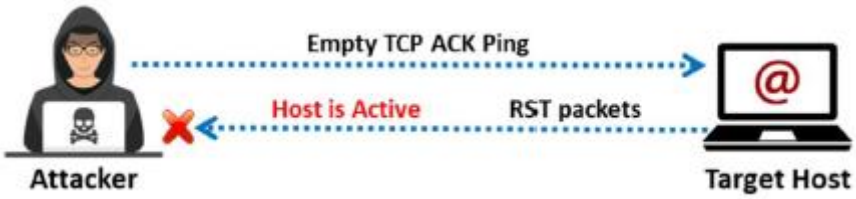
Zalety:

* Ponieważ maszyny mogą być skanowane równolegle, skanowanie nigdy nie powoduje błędu przekroczenia limitu czasu podczas oczekiwania na odpowiedź.

* Ping TCP SYN może być użyty do określenia, czy host jest aktywny bez tworzenia jakiegokolwiek połączenia. W związku z tym dzienniki nie są rejestrowane na poziomie systemu ani sieci, co pozwala atakującemu nie pozostawiać żadnych śladów do wykrycia.

Skanowanie pingów TCP ACK

Ping TCP ACK jest podobny do ping TCP SYN, aczkolwiek z niewielkimi różnicami. TCP ACK ping wykorzystuje również domyślny port 80. W technice TCP ACK ping osoby atakujące wysyłają pusty pakiet TCP ACK bezpośrednio do hosta docelowego. Ponieważ nie ma wcześniejszego połączenia między atakującym a docelowym hostem, po otrzymaniu pakietu ACK docelowy host odpowiada flagą RST, aby zakończyć żądanie. Odbiór tego pakietu RST po stronie atakującego wskazuje, że host jest aktywny. W Zenmap opcja -PA jest używana do wykonywania skanowania ping TCP ACK.



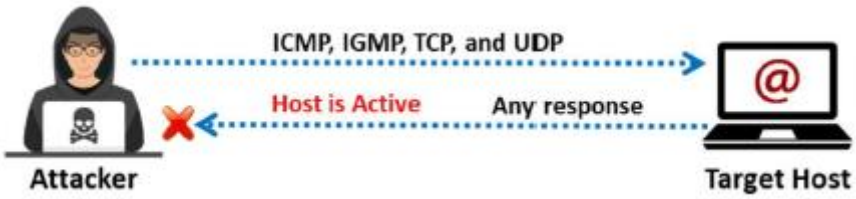
Zalety:

* Zarówno pakiet SYN, jak i pakiet ACK mogą być użyte do maksymalizacji szans na ominięcie zapory. Jednak zapory ogniowe są w większości skonfigurowane do blokowania pakietów ping SYN, ponieważ są one najpowszechniejszą techniką pingowania. W takich przypadkach sonda ACK może być skutecznie wykorzystana do łatwego ominięcia tych zestawów reguł zapory.

IP Protocol Ping Scan

Ping protokołu IP to najnowsza opcja wykrywania hostów, która wysyła pakiety ping IP z nagłówkiem IP dowolnego określonego numeru protokołu. Ma taki sam format jak ping TCP i UDP. Ta technika próbuje wysłać różne pakiety przy użyciu różnych protokołów IP, mając nadzieję na uzyskanie odpowiedzi wskazującej, że host jest online. Wiele pakietów IP dla ICMP (protokół 1), IGMP (protokół 2) i IP-w-IP (protokół 4) jest wysyłanych domyślnie, gdy nie określono żadnych protokołów. Aby skonfigurować domyślne protokoły, zmień DEFAULT PROTO PROBE PORT SPEC w nmap.h podczas kompilacji. Dla określonych protokołów, takich jak ICMP, IGMP, TCP (protokół 6), UDP (protokół 17)

pakiety należy przesyłać z odpowiednimi nagłówkami protokołów, a dla pozostałych protokołów tylko dane nagłówka IP mają być przesyłane z pakiety.



Krótko mówiąc, osoby atakujące wysyłają do docelowego hosta różne pakiety sondujące różnych protokołów IP; każda odpowiedź z dowolnej sondy wskazuje, że host jest online. W Zenmap opcja -PO służy do wykonywania skanowania ping protokołu IP.

Narzędzia pingowania

Narzędzia Ping Sweep pingują cały zakres sieciowych adresów IP w celu identyfikacji działających systemów. Poniżej znajdują się narzędzia ping sweep, które umożliwiają określenie aktywnych hostów w sieci docelowej poprzez wysyłanie wielu żądań ICMP ECHO do różnych hostów w sieci jednocześnie.

Angry IP Scanner

Skaner Angry IP to skaner adresów IP i portów. Może skanować adresy IP w dowolnym zakresie, a także dowolny ich port. Pinguje każdy adres IP, aby sprawdzić, czy jest aktywny; następnie opcjonalnie rozwiązuje swoją nazwę hosta, określa adres MAC, skanuje porty i tak dalej. Ilość gromadzonych danych o każdym hoście wzrasta wraz z wtyczkami. Skaner Angry IP ma dodatkowe funkcje, takie jak informacje NetBIOS (nazwa komputera, nazwa grupy roboczej i aktualnie zalogowany użytkownik Windows), ulubione zakresy adresów IP, wykrywanie serwera WWW i konfigurowalne programy otwierające. Narzędzie umożliwia użytkownikowi zapisywanie wyników skanowania w plikach listy CSV, TXT, XML lub IP-Port. Aby zwiększyć szybkość skanowania, stosuje podejście wielowątkowe: dla każdego skanowanego adresu IP tworzony jest osobny wątek skanowania. Niektóre dodatkowe narzędzia do przeszukiwania ping, których atakujący używa do określenia żywych hostów w sieci są wymienione poniżej:

- Zestaw narzędzi inżyniera SolarWinds (https://www.solorwinds.com)

- NetScanTools Pro (https://www.netscontools.com)

- Narzędzie Colasoft Ping (https://www.colosoft.com)

- Wizualny tester pingu (http://www.pingtester.net)

Wykrywanie portów i usług

Kolejnym krokiem w procesie skanowania sieci jest sprawdzenie otwartych portów i usług w aktywnych systemach. To wykrywanie otwartych portów i usług można przeprowadzić za pomocą różnych technik skanowania portów. Administratorzy często używają technik skanowania portów do weryfikacji zasad bezpieczeństwa swoich sieci, podczas gdy osoby atakujące używają ich do identyfikowania otwartych portów i uruchomionych usług na hoście z zamiarem naruszenia bezpieczeństwa sieci. Co więcej, czasami użytkownicy nieświadomie pozostawiają niepotrzebne otwarte porty w swoich systemach. Atakujący wykorzystuje takie otwarte porty do przeprowadzania ataków. W tej sekcji opisano typowe porty i odpowiadające im usługi, a także różne techniki i narzędzia skanowania portów używane przez atakującego do skanowania portów.

Lista wspólnych portów i usług

Poniżej wymieniono ważne zarezerwowane porty:

Nazwa : Port/Protokół : Opis

echo 7/tcp, udp

discard 9/ tcp, udp sink null

systat 11/tcp Users

daytime 13/ tcp, udp

netstat 15/tcp, udp

qotd 17/tcp, udp Quote

chargen 19/tcp, udp ttytst source

ftp-data 20/tcp ftp data transfer

ftp 21/tcp ftp command

ssh 22/tcp Secure Shell

telnet 23/tcp

SMTP 25/tcp Email server

time 37/tcp, udp Timeserver

rip 39/tcp, udp resource location

domain 53/tcp, udp domain name server

sql*net 66/tcp, udp Oracle SQL*net

bootps 67/udp bootp server

bootpc 68/udp bootp client

tftp 69/udp Trivial File Transfer

gopher 70/tcp gopher server

finger 79/tcp Finger

www-http 80/tcp, udp WWW

www-https 80/tcp WWW

kerberos 88/tcp, udp Kerberos

pop2 109/tcp PostOffice V.2

Pop3 110/tcp PostOffice V.3

sunrpc 111/tcp, udp RPC 4.0 portmapper

auth/ident 113/tcp, udp Authentication Service

audionews 114/tcp, udp Audio News Multicast

nntp 119/tcp Usenet Network News Transfer

ntp 123/udp Network Time Protocol

netbios-ns 137/tcp, udp NETBIOS Name Service

netbios-dgm 138/tcp, udp NETBIOS Datagram Service

netbios-ssn 139/tcp, udp NETBIOS Session Service

imap 143/tcp, udp Internet Message Access Protocol

sql-net 150/tcp, udp SQL-NET

sqlsrv 156/tcp, udp SQL Service

snmp 161/tcp, udp SNMP

snmp-trap 162/tcp, udp

cmip-man 163/tcp, udp CMIP/TCP Manager

cmip-agent 164/tcp, udp CMIP/TCP Agent

ire 194/tcp, udp Internet Relay Chat

at-rtmp 201/tcp, udp AppleTalk Routing Maintenance

at-nbp 202/tcp, udp AppleTalk Name Binding

at-3 203/tcp, udp AppleTalk

at-echo 204/tcp, udp AppleTalk Echo

at-5 205/tcp, udp AppleTalk

at-zis 206/tcp, udp AppleTalk Zone Information

at-7 207/tcp, udp AppleTalk

at-8 208/tcp, udp AppleTalk

ipx 213/tcp, udp Novell

imap3 220/tcp, udp Interactive Mail Access Protocol v3

aurp 387/tcp, udp AppleTalk Update-Based Routing

netware-ip 396/tcp, udp Novell Netware over IP

rmt 411/tcp, udp Remote mt

kerberos-ds 445/tcp, udp Microsoft DS

isakmp 500/udp ISAKMP/IKE

fcp 510/tcp First Class Server

exec 512/tcp BSD rexecd(8)

comsat/biff 512/udp Used by mail system to notify users

login 513/tcp BSD rlogind(8)

who 513/udp whod BSD rwhod(8)

shell 514/tcp cmd BSD rshd(8)

syslog 514/udp BSD syslogd(8)

printer 515/tcp, udp spooler BSD lpd(8)

talk 517/tcp, udp BSD talkd(8)

ntalk 518/udp SunOS talkd(8)

netnews 532/tcp, udp Readnews

uucp 540/tcp, udp uucpd BSD uucpd(8)

klogin 543/tcp, udp Kerberos Login

kshell 544/tcp, udp Kerberos Shell

kremd Kerberos encrypted remote shell

-kfall ekshell 545/tcp

pcserver 600/tcp ECD Integrated PC board srvr

mount 635/udp NFS Mount Service

penfs 640/udp PC-NFS DOS Authentication

bwnfs 650/udp BW-NFS DOS Authentication

flexlm 744/tcp, udp Flexible License Manager

kerberos-adm 749/tcp, udp Kerberos Administration

kerberos 750/tcp, udp kdc Kerberos authentication

kerberos master 751/tcp, udp Kerberos authentication

krb_prop 754/tcp Kerberos slave propagation

applix 999/udp Applixware

socks 1080/tcp,udp Socks Proxy

kpop 1109/tcp Pop with Kerberos

ms-sql-s 1433/tcp,udp Microsoft SQL Server

ms-sql-m 1434/tcp,udp Microsoft SQL Monitor

pptp 1723/tcp,udp Pptp

nfs 2049/tcp,udp Network File System

eklogin 2105/tcp Kerberos encrypted rlogin

rkinit 2108/tcp Kerberos remote kinit

kx 2111/tcp X over Kerberos

kauth 2120/tcp Remote kauth

lyskom 4894/tcp LysKOM (conference system)

sip 5060/tcp Session Initiation Protocol

sip 5060/udp Session Initiation Protocol

6000-6063/tcp, xll udp X Window System

ire 6667/tcp Internet Relay Chat

Techniki skanowania portów

Techniki skanowania portów są dalej kategoryzowane, jak opisano poniżej. Ta kategoryzacja opiera się na typie protokołu używanego do komunikacji w sieci.

Skanowanie TCP:

- Otwórz metody skanowania TCP

o Połączenie TCP/pełne skanowanie

- Metody Stealth TCP Scanning

o Półotwarte skanowanie

o Odwrotne skanowanie flag TCP

• Xmas skan

• Skanowanie FIN

• Skanowanie NULL

• Skanowanie Maimon

o Skanowanie sondy flagowej ACK

• Skanowanie oparte na TTL

• Skanowanie oparte na oknie

- Metody skanowania TCP stron trzecich i sfałszowane

o Skanowanie nagłówka IDLE/IP ID

Skanowanie UDP:

• Skanowanie UDP

Skanowanie SCTP:

• Skanowanie SCTP INIT

• Skanowanie SCTP COOKIE/ECHO

Skanowanie SSDP:

• SSDP i skanowanie list

Skanowanie IPv6:

• Skanowanie IPv6

Połączenie TCP/pełne skanowanie

TCP Connect/Full Open Scan to jedna z najbardziej niezawodnych form skanowania TCP. Podczas skanowania TCP Connect wywołanie systemowe TCP connect ( ) systemu operacyjnego próbuje otworzyć połączenie z każdym interesującym portem na komputerze docelowym. Jeśli port nasłuchuje, wywołanie connect() spowoduje pomyślne połączenie z hostem na tym konkretnym porcie; w przeciwnym razie zwróci komunikat o błędzie informujący, że port jest niedostępny. Skanowanie połączenia TCP kończy trójstronne uzgadnianie z komputerem docelowym. W trójstronnym uzgadnianiu TCP klient wysyła pakiet SYN, który odbiorca potwierdza pakietem SYN+ACK. Następnie klient potwierdza pakiet SYN+ACK pakietem ACK, aby zakończyć połączenie. Po zakończeniu uzgadniania skaner wysyła pakiet RST, aby zakończyć połączenie.

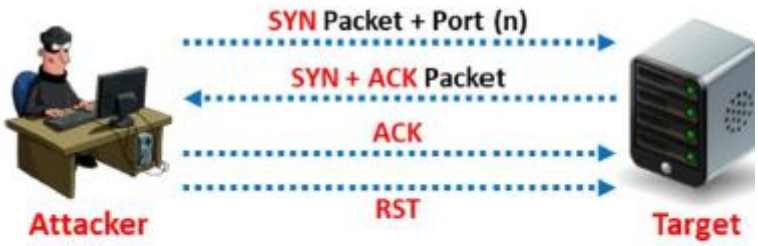
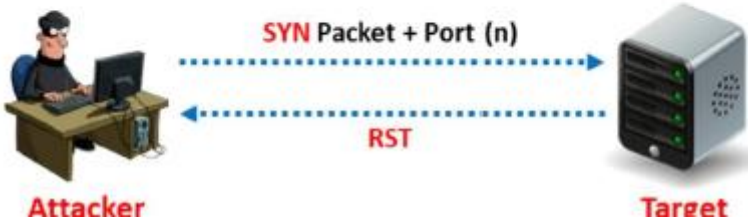


Figure 3.33: Scan result when a port is open



Wykonanie osobnego wywołania connect ( ) dla każdego docelowego portu w sposób liniowy zajęłoby dużo czasu w przypadku wolnego połączenia. Atakujący może przyspieszyć skanowanie, używając wielu równoległych gniazd. Używając nieblokowania, I/O pozwala atakującemu na ustawienie krótkiego limitu czasu i obserwowanie wszystkich gniazd jednocześnie. W Zenmap opcja -ST jest używana do wykonania połączenia TCP/pełnego otwartego skanowania. Wadą tego typu skanowania jest to, że jest ono łatwe do wykrycia i filtrowania. Logi w systemie docelowym ujawnią połączenie. Takie skanowanie nie wymaga uprawnień superużytkownika.

Skanowanie z ukrycia (skanowanie w połowie otwarte)

Skanowanie w ukryciu polega na nagłym zresetowaniu połączenia TCP między klientem a serwerem przed zakończeniem sygnałów trójkierunkowego uzgadniania, co powoduje, że połączenie jest półotwarte. Skanowanie stealth wysyła pojedynczą ramkę do portu TCP bez uzgadniania TCP lub dodatkowych transferów pakietów. Ten typ skanowania wysyła pojedynczą ramkę z oczekiwaniem na pojedynczą odpowiedź. Półotwarte skanowanie częściowo otwiera połączenie, ale zatrzymuje się w połowie. Skanowanie stealth jest również nazywane „skanowaniem SYN”, ponieważ wysyła tylko pakiet SYN. Uniemożliwia to usłudze powiadamianie o połączeniu przychodzącym. TCP SYN lub

półotwarte skanowanie to ukryta metoda skanowania portów. Skanowanie stealth implementuje również metodologię trójstronnego uzgadniania. W ostatnim etapie sprawdza pakiety wchodzące do interfejsu i kończy połączenie przed wyzwoleniem nowej inicjalizacji w celu identyfikacji zdalnych portów. Proces skanowania w ukryciu opisano poniżej.

* Klient wysyła pojedynczy pakiet SYN do serwera na odpowiednim porcie.

* Jeśli port jest otwarty, serwer następnie odpowiada pakietem SYN/ACK.

* Jeśli serwer odpowiada pakietem RST, to zdalny port jest w stanie „zamknięty”.

* Klient wysyła pakiet RST w celu zamknięcia inicjacji przed nawiązaniem połączenia.

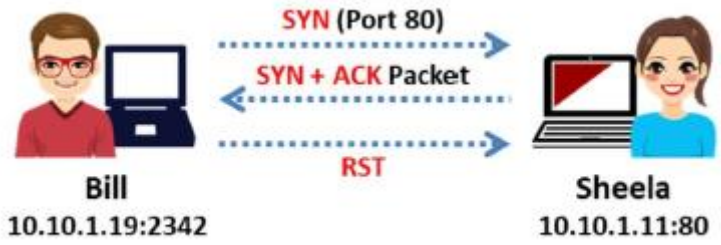
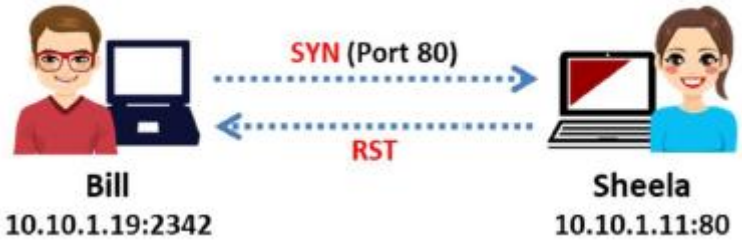


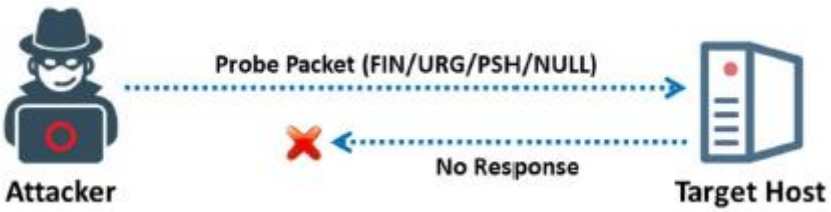
Figure 3.36: Port is open

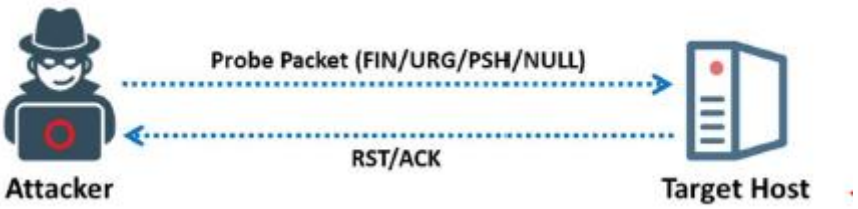


Atakujący używają technik skanowania z ukrycia, aby ominąć reguły zapory sieciowej i mechanizmy rejestrowania, i jak zwykle ukrywają się pod ruchem sieciowym. W Zenmap opcja -sS jest używana do wykonywania skanowania w ukryciu/półotwartego skanowania TCP.

Odwrotne skanowanie flag TCP

Atakujący wysyłają pakiety sondujące TCP z ustawioną flagą TCP (FIN, URG, PSH) lub bez flag. Gdy port jest otwarty, atakujący nie otrzymuje żadnej odpowiedzi od hosta, natomiast gdy port jest zamknięty, otrzymuje komunikat RST od hosta docelowego.





Mechanizmy bezpieczeństwa, takie jak zapory ogniowe i IDS, wykrywają pakiety SYN wysyłane do wrażliwych portów docelowych hostów. Programy takie jak Syslog są dostępne do rejestrowania prób skanowania flagi SYN w połowie otwartej. Czasami pakiety sondujące włączone z flagami TCP mogą przechodzić przez filtry niewykryte, w zależności od zainstalowanych mechanizmów bezpieczeństwa. Odwrócona technika polega na sondowaniu celu przy użyciu na wpół otwartej flagi SYN, ponieważ zamknięte porty mogą tylko odesłać odpowiedź. Zgodnie z RFC 793 pakiet RST/ACK jest wysyłany w celu zresetowania połączenia, gdy host zamyka port. Atakujący wykorzystują tę funkcję do wysyłania pakietów próbnych TCP do każdego portu docelowego hosta z ustawionymi różnymi flagami TCP. Typowe konfiguracje flag używane dla pakietu sondującego obejmują:

* Sonda FIN z ustawioną flagą FIN TCP

* Sonda świąteczna z ustawionymi flagami TCP FIN, URG i PUSH

* Sonda NULL bez ustawionych flag TCP

* Sonda SYN/ACK

Wszystkie zamknięte porty na docelowym hoście wyślą odpowiedź RST/ACK. Ponieważ systemy operacyjne, takie jak Windows, całkowicie ignorują standard RFC 793, nie można zobaczyć odpowiedzi RST/ACK po podłączeniu do zamkniętego portu hosta docelowego. Technika ta jest jednak skuteczna w systemach operacyjnych opartych na systemie UNIX.

Zalety

Unika wielu systemów IDS i rejestrowania; bardzo skryty

Wady :

* Wymaga surowego dostępu do gniazd sieciowych i uprawnień superużytkownika

* Głównie skuteczne przeciwko hostom używającym stosu TCP/IP pochodzącego z BSD (nieskuteczne przeciwko

* W szczególności hosty Microsoft Windows).

Uwaga: Skanowanie odwrotnej flagi TCP jest znane jako skanowanie FIN, URG i PSH w oparciu o flagę ustawioną w pakiecie sondy. Jeśli nie ma ustawionej flagi, jest to znane jako skanowanie NULL. Jeśli ustawiona jest tylko flaga FIN, nazywa się to skanowaniem FIN, a jeśli wszystkie FIN, URG i PSH są ustawione, nazywa się to skanowaniem Xmas.

Xmas skan

Xmas scan to rodzaj odwrotnej techniki skanowania TCP z flagami FIN, URG i PUSH ustawionymi na wysyłanie ramki TCP do zdalnego urządzenia. Jeśli cel otworzył port, nie otrzymasz odpowiedzi ze zdalnego systemu. Jeśli cel zamknął port, otrzymasz odpowiedź zdalnego systemu z RST. Możesz użyć tej techniki skanowania portów, aby przeskanować duże sieci i dowiedzieć się, który host działa i jakie

usługi oferuje. Ta technika opisuje wszystkie zestawy flag TCP. Kiedy wszystkie flagi są ustawione, niektóre systemy zawieszają się; stąd flagi są często ustawiane w nonsensownym wzorcu URG-PSH-FIN. Atakujący używają skanowania TCP Xmas w celu ustalenia, czy porty na docelowej maszynie są zamknięte za pośrednictwem pakietu RST. To skanowanie działa tylko wtedy, gdy systemy są zgodne z implementacją protokołu TCP/IP opartą na RFC 793. Nie będzie działać z żadną bieżącą wersją systemu Microsoft Windows.

Figure 3.41: Xmas scan when the port is open

Kod sieciowy BSD

Ta metoda opiera się na kodzie sieciowym BSD. Dlatego możesz użyć tego tylko dla hostów UNIX; nie obsługuje systemu Windows NT. Jeśli użytkownik przeskanuje dowolny system Microsoft, pokaże, że wszystkie porty na hoście są otwarte.

Przesyłanie pakietów

Możesz zainicjować wszystkie flagi podczas przesyłania pakietu do zdalnego hosta. Jeśli system docelowy zaakceptuje pakiet i nie wyśle żadnej odpowiedzi, oznacza to, że port jest otwarty. Jeśli system docelowy wyśle flagę RST, oznacza to, że port jest zamknięty.

Zalety

Pozwala uniknąć trójstronnego uzgadniania IDS i TCP.

Wady :

* Działa tylko na platformie UNIX.

W Zenmap opcja -sX jest używana do wykonywania skanowania Xmas, podczas gdy opcje -sF i -sN są używane odpowiednio do wykonywania skanowania FIN i skanowania NULL

Skanowanie TCP Maimon

Ta technika skanowania jest bardzo podobna do skanowania NULL, FIN i Xmas, ale używana tutaj sonda to FIN/ACK. W większości przypadków, aby określić, czy port jest otwarty, czy zamknięty, należy wygenerować pakiet RST jako odpowiedź na żądanie sondy. Jednak w wielu systemach BSD port jest otwarty, jeśli pakiet zostanie odrzucony w odpowiedzi na sondę. Nmap interpretuje port jako otwarty|filtrowany, gdy nie ma odpowiedzi od sondy skanującej Maimon, nawet po wielu retransmisjach. Port jest zamykany, jeśli sonda otrzyma odpowiedź w postaci pakietu RST. Port jest filtrowany, gdy z hosta docelowego zwracany jest błąd ICMP unreachable (typ 3, kod1, 2, 3,9,10 lub 13). W Zenmap opcja -sM służy do wykonywania skanowania TCP Maimon.

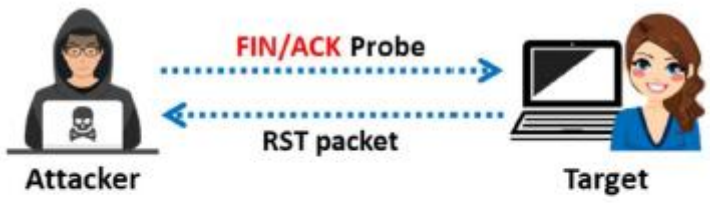
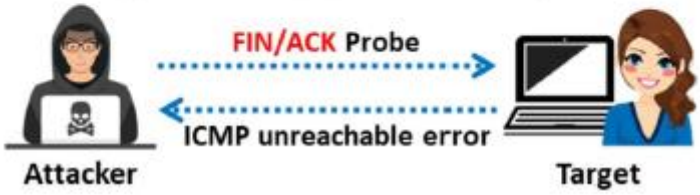


Figure 3.45: TCP Maimon scan result of closed port



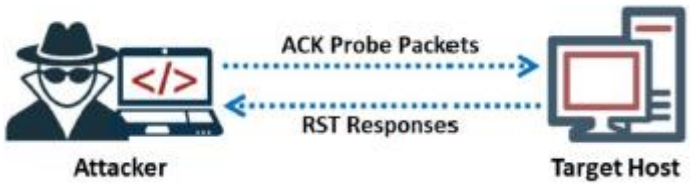
ACK Flag Probe Scan

Atakujący wysyłają pakiety próbne TCP z ustawioną flagą ACK do zdalnego urządzenia, a następnie analizują informacje nagłówkowe (pole TTL i WINDOW) odebranych pakietów RST, aby dowiedzieć się, czy port jest otwarty, czy zamknięty. Skanowanie flagi ACK wykorzystuje luki w stosie TCP/IP pochodzącym z BSD. Dlatego takie skanowanie jest skuteczne tylko w tych systemach operacyjnych i platformach, na których BSD wyprowadza stosy TCP/IP.

Kategorie skanowania sondy flagowej ACK obejmują:

• Skanowanie sondy flagowej ACK w oparciu o TTL

W tej technice skanowania należy najpierw wysłać pakiety próbne ACK (kilka tysięcy) do różnych portów TCP, a następnie przeanalizować wartość pola TTL odebranych pakietów RST. W Zenmap składnia nmap -ttl [czas] [cel] jest używana do wykonywania skanowania opartego na TTL.



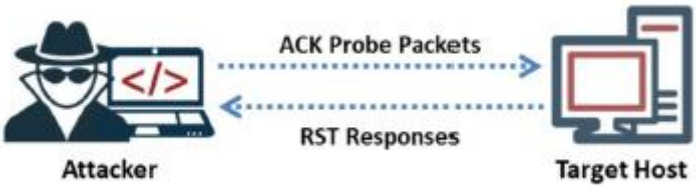
Jeśli wartość TTL pakietu RST na określonym porcie jest mniejsza niż wartość graniczna 64, port ten jest otwarty. Poniżej przedstawiono przykładowy log pierwszych czterech odebranych pakietów RST:

```
1: host 10.2.2.11 port 20: F:RST -> ttl: 80 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 80 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 50 win: 0
4: host 10.2.2.11 port 23: F:RST -> ttl: 80 win: 0
```

W tym przykładzie port 22 zwrócił wartość TTL równą 50, czyli mniejszą niż 64; wszystkie inne porty zwróciły wartość TTL równą 80, czyli większą niż 64. W związku z tym port 22 jest otwarty.

Skanowanie Window-Based ACK Flag Probe

W tej technice skanowania należy najpierw wysłać pakiety próbne ACK (kilka tysięcy) do różnych portów TCP, a następnie przeanalizować wartość pola okna odebranych pakietów RST. Użytkownik może użyć tej techniki skanowania, gdy wszystkie porty zwracają tę samą wartość TTL. W Zenmap opcja -sW służy do skanowania okien.



Jeśli wartość okna pakietu RST na określonym porcie jest różna od zera, to ten port jest otwarty. Poniżej przedstawiono przykładowy log pierwszych czterech odebranych pakietów RST:

```
1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512
4: host 10.2.2.12 port 23: F:RST -> ttl: 64 win: 0
```

Powyższy rysunek pokazuje, że wartość TTL zwracana dla każdego pakietu jest taka sama; w związku z tym nie można wykonać skanowania sondy flagowej ACK w oparciu o TTL w celu znalezienia otwartych portów. Dlatego, gdy obserwujesz wartość okna, trzeci pakiet ma niezerową wartość okna, co oznacza, że port jest otwarty. Gdy zwrócona wartość RST wynosi zero, port jest zamknięty. Jeśli nie ma odpowiedzi nawet po wielu retransmisjach i zwracany jest błąd ICMP unreachable (typ 3, code1, 2, 3, 9, 10 lub 13), port jest uznawany za port filtrowany.

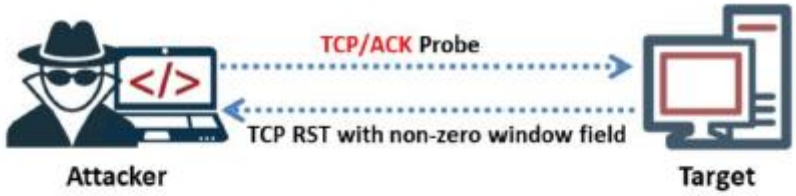


Figure 3.52: TCP Window scan result of an open port

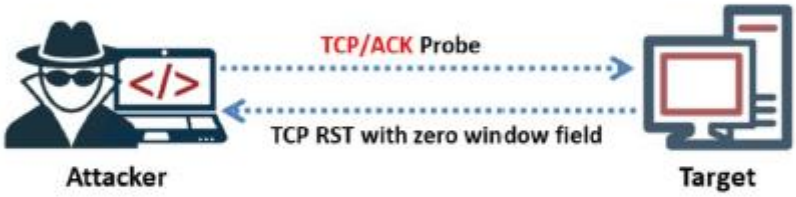
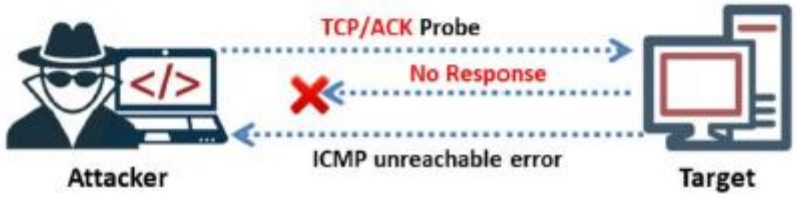


Figure 3.53: TCP Window scan result of a closed port



Zalety:

Ten typ skanowania może w większości przypadków ominąć system IDS.

Wady:

Jest bardzo powolny i może wykorzystywać tylko starsze systemy operacyjne z podatnymi na ataki stosami TCP/IP pochodzącymi z BSD.

Sprawdzanie systemów filtrowania sieci docelowych

Technika skanowania sondy flagowej ACK pomaga również w sprawdzaniu systemów filtrujących sieci docelowych. Atakujący wysyła pakiet sondujący ACK, aby sprawdzić mechanizm filtrowania (zapory ogniowe) pakietów wykorzystywanych przez sieć docelową. Wysłanie pakietu sondy ACK z losowym numerem sekwencyjnym i brak odpowiedzi od celu oznacza, że port jest filtrowany (obecna zapora stanowa); odpowiedź RST od celu oznacza, że port nie jest filtrowany (brak firewalla).

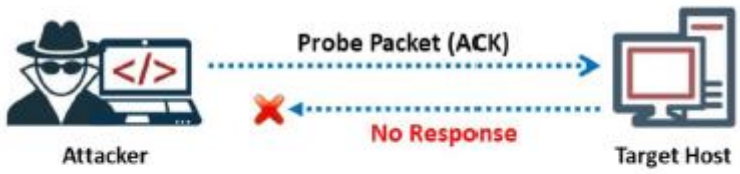
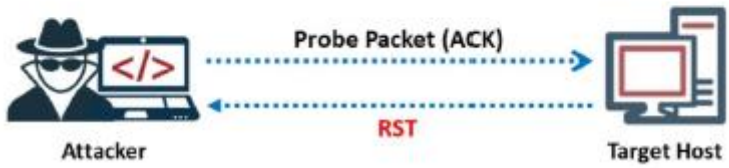
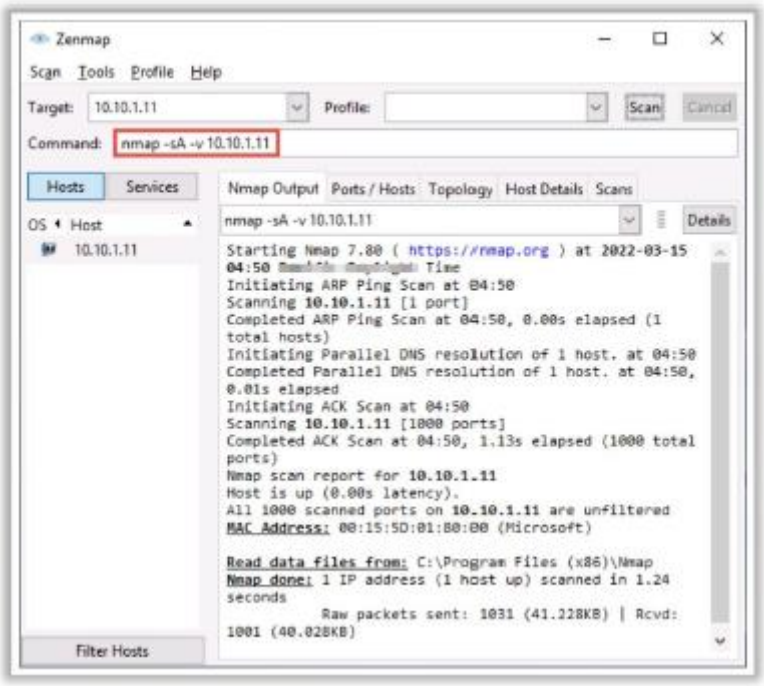


Figure 3.55: Stateful Firewall is present



Skanowanie sondy z flagą ACK przy użyciu Nmap

W Zenmap opcja -sA jest używana do wykonania skanowania sondy flagi ACK.



Skanowanie nagłówka IDLE/IPID

Skanowanie nagłówka IDLE/IPID to metoda skanowania portów TCP, której można użyć do wysłania sfałszowanego adresu źródłowego do komputera w celu określenia dostępnych usług. Oferuje pełne skanowanie w ciemno zdalnego hosta. Większość serwerów sieciowych nasłuchuje na portach TCP; na przykład serwery WWW nasłuchują na porcie 80, a serwery poczty nasłuchują na porcie 25. Port jest uważany za „otwarty”, jeśli aplikacja nasłuchuje na porcie. Jednym ze sposobów ustalenia, czy port jest otwarty, jest wysłanie do portu pakietu „SYN” (ustanowienia sesji). Maszyna docelowa zwraca pakiet „SYN|ACK” (potwierdzenie żądania sesji), jeśli port jest otwarty, lub pakiet „RST” (reset), jeśli port jest zamknięty. Maszyna, która otrzymuje niezamówiony pakiet SYN|ACK, odpowiada komunikatem RST. Niezamówione RST jest ignorowane. Każdy pakiet IP w Internecie ma „identyfikator IP” (IPID), który jednoznacznie identyfikuje fragmenty oryginalnego datagramu IP. System operacyjny zwiększa IPID dla każdego wysłanego pakietu. Zatem sondowanie IPID ujawnia atakującemu liczbę pakietów wysłanych od ostatniego sondowania. W Zenmap, opcja -si jest używana do wykonywania skanowania IDLE.

Atakujący przeprowadza to skanowanie, podszywając się pod inny komputer za pomocą spoofingu. Atakujący nie wysyła pakietu ze swojego adresu IP; zamiast tego używają innego hosta, często nazywanego „zombie”, do skanowania zdalnego hosta i identyfikowania otwartych portów. W tym ataku atakujący oczekuje numerów sekwencyjnych hosta zombie, a jeśli zdalny host sprawdza adres IP strony skanującej, wyświetlany jest adres IP maszyny zombie.

Skanowanie bezczynności

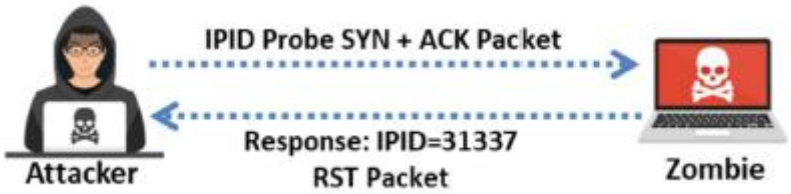
Krok 1

Pierwszym krokiem w bezczynnym skanowaniu jest określenie odpowiedniego zombie. Zombie, który przyrostowo przypisuje pakiety IPID w skali globalnej, jest odpowiednim lub bezczynnym zombie

wykonywanie skanów bezczynności. Im krótszy odstęp czasu na żądanie/odpowiedź między atakującym-zombie a zombie-celem, tym szybsze jest skanowanie.

Wybierz „Zombie” i sprawdź jego aktualny numer identyfikacyjny IP (IPID).

W pierwszym kroku pakiet SYN+ACK jest wysyłany do maszyny zombie w celu zbadania jej numeru IPID. W tym przypadku pakiet SYN+ACK jest wysyłany w celu zbadania numeru IPID, a nie ustanowienia połączenia TCP (trójkierunkowe uzgadnianie).



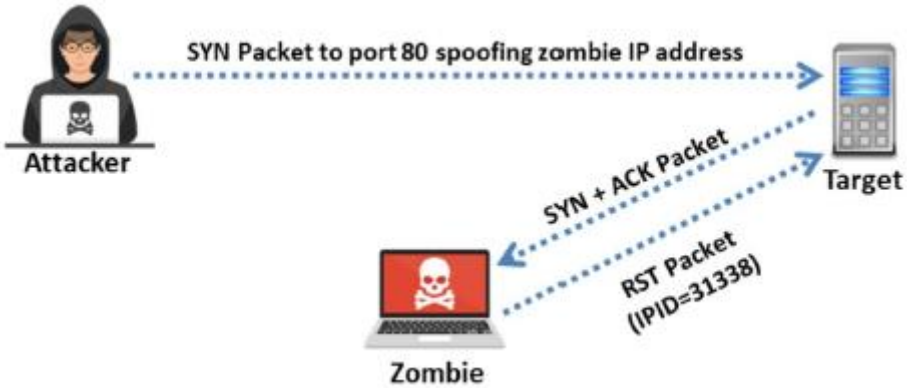
Ponieważ zombie nie oczekuje pakietu SYN+ACK, odrzuca połączenie, zwracając pakiet RST. Pakiet RST wysłany przez maszynę zombie jest analizowany w celu wyodrębnienia IPID. Jak pokazano na rysunku, zakładamy, że zombie odpowiada IPID=31337. Ponadto zakładamy, że IPID to X.

Krok 2

Atakujący wysyła pakiet SYN do docelowej maszyny na porcie 80, podszywając się pod adres IP zombie.

Skanowanie w trybie bezczynności: krok 2.1 (otwarty port)

Jeśli port jest otwarty, cel wysyła pakiet SYN+ACK do zombie (ponieważ adres IP został sfałszowany), aby kontynuować uzgadnianie trójstronne. Ponieważ zombie nie oczekiwał pakietu SYN+ACK od maszyny docelowej, odpowiada pakietem RST.



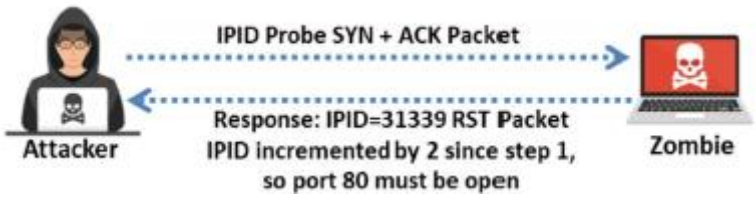
Ponieważ każdy pakiet IP ma IPID, który zwiększa się o jeden dla każdej transmisji pakietu, zombie używa teraz następnego dostępnego IPID, tj. 31338 (X +1).

Skanowanie bezczynności: krok 2.2 (zamknięty port)

Załóżmy, że port w miejscu docelowym jest zamknięty. Następnie, po otrzymaniu pakietu SYN od atakującego, cel odpowiada pakietem RST, po czym zombie pozostaje bezczynny.

Krok 3

Teraz ponownie wykonaj krok 1, aby sprawdzić numer IPID.

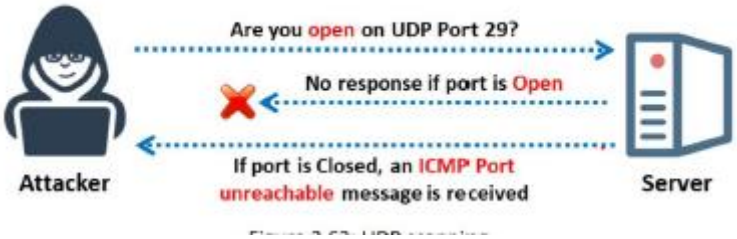


Wyślij pakiet SYN+ACK do zombie, a on odpowie pakietem RST zawierającym IPID. Zakładając, że port na celu był otwarty i że zombie wysłał już pakiet RST do celu, numer IPID jest zwiększany o 1. Teraz zombie odpowiada atakującemu pakietem RST, używając swojego następnego IPID, tj. 31339 (X + 2). W rezultacie IPID jest zwiększany o 2, co oznacza, że port na komputerze docelowym był otwarty. W ten sposób, używając skanowania bezczynności, osoba atakująca może zidentyfikować otwarte porty i usługi na docelowej maszynie, podszywając się pod jej adres IP z adresem IP zombie.

Skanowanie UDP

Nieosiągalne skanowanie portu UDP Raw ICMP

Skanery portów UDP używają protokołu UDP zamiast TCP. Podczas skanowania UDP nie ma trójstronnego uzgadniania. Protokół UDP może być trudniejszy w użyciu niż skanowanie TCP, ponieważ możesz wysłać pakiet, ale nie możesz określić, czy host jest żywy, martwy lub przefiltrowany. Można jednak użyć jednego protokołu ICMP, który sprawdza otwarte lub zamknięte porty. Jeśli wyślesz pakiet UDP do portu bez powiązanej z nim aplikacji, stos IP zwróci pakiet ICMP port unreachable. Jeśli jakikolwiek port zwróci błąd ICMP, zostanie zamknięty, pozostawiając porty, które nie odpowiedziały, jeśli są otwarte lub filtrowane przez zaporę.



Dzieje się tak, ponieważ otwarte porty nie muszą wysyłać potwierdzenia w odpowiedzi na sondę, a zamknięte porty nie są nawet wymagane do wysłania pakietu błędu.

Pakiety UDP

Gdy wysyłasz pakiet do zamkniętego portu UDP, większość hostów wysyła błąd ICMP_PORT_UNREACH. W ten sposób można określić, czy port jest otwarty, jeśli nie ma gwarancji, że dotrą pakiety UDP lub błędy ICMP. Dlatego skanery UDP tego typu muszą implementować retransmisję pakietów, które wydają się utracone. Skanery UDP interpretują utracony ruch jako otwarte porty. W Zenmap opcja -su służy do wykonywania skanowania UDP. Ponadto ta technika skanowania jest powolna, ponieważ ogranicza liczbę komunikatów o błędach ICMP jako formę rekompensaty dla maszyn stosujących RFC 1812 sekcja 43.2.8. Zdalny host będzie wymagał dostępu do surowego gniazda ICMP w celu odróżnienia portów zamkniętych od portów nieosiągalnych.

UDP RECVFROM () i WRITE () Skanowanie

Chociaż użytkownicy inni niż root nie mogą bezpośrednio odczytywać błędów nieosiągalnego portu, Linux informuje cię pośrednio, gdy otrzymuje komunikaty.

Przykład:

Na przykład drugie wywołanie zapisu ( ) do zamkniętego portu zwykle kończy się niepowodzeniem. Różne skanery, takie jak Netcat i Pluvial pscan.c, wykonują recvfrom( ) na nieblokujących gniazdach UDP i zwykle zwracają EAGAIN("Spróbuj ponownie", errno 13), jeśli błąd ICMP nie został odebrany lub ECONNREFUSED("Połączenie odmówiono," errno 111) inaczej. Ta technika jest używana do określania otwartych portów, gdy użytkownicy inni niż root używają - u (UDP). Użytkownicy root mogą również użyć opcji -l (lamer UDP scan), aby wymusić ten proces.

Zalety :

Skanowanie UDP jest mniej nieformalne w odniesieniu do otwartego portu, ponieważ nie ma narzutu związanego z uzgadnianiem TCP. Jeśli jednak protokół ICMP odpowiada na każdy niedostępny port, łączna liczba ramek może przekroczyć liczbę ze skanowania TCP. Systemy operacyjne firmy Microsoft zwykle nie implementują żadnych ograniczeń szybkości ICMP; w związku z tym to skanowanie działa bardzo wydajnie na urządzeniach z systemem Windows.

Wady:

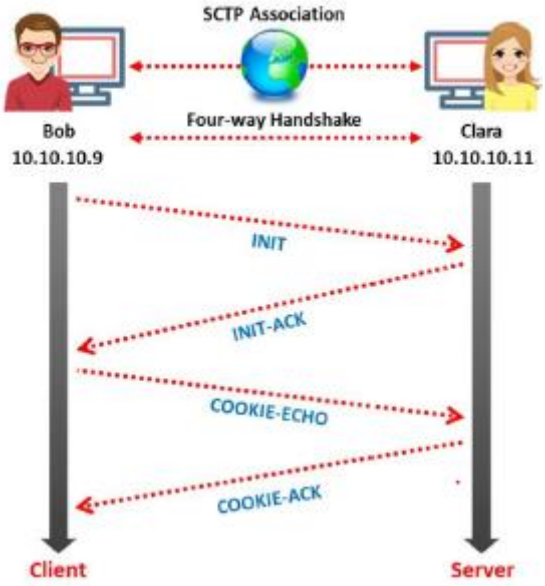
Skanowanie UDP dostarcza tylko informacji o porcie. Jeśli potrzebne są dodatkowe informacje o wersji, skanowanie musi zostać uzupełnione skanowaniem w celu wykrycia wersji (-sv) lub opcją pobierania odcisków palców systemu operacyjnego (-o).

Skanowanie UDP wymaga uprzywilejowanego dostępu; dlatego ta opcja skanowania jest dostępna tylko w systemach z odpowiednimi uprawnieniami użytkownika.

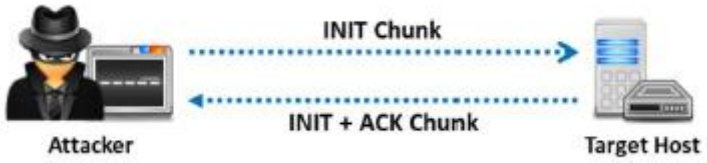
Większość sieci ma ogromne ilości ruchu TCP; w rezultacie wydajność skanowania UDP jest niska. Skanowanie UDP zlokalizuje otwarte porty i dostarczy kierownikowi ds. bezpieczeństwa cennych informacji umożliwiających zidentyfikowanie udanych inwazji hakerów na otwarte porty UDP z powodu aplikacji spyware, koni trojańskich i innego złośliwego oprogramowania.

Skanowanie SCTP INIT

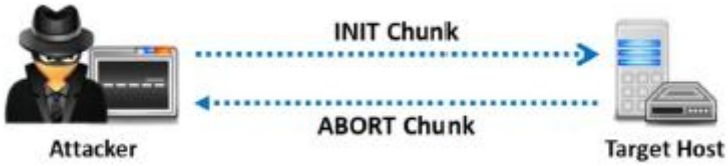
Stream Control Transport Protocol (SCTP) to niezawodny zorientowany na komunikaty protokół warstwy transportowej. Jest używany jako alternatywa dla protokołów TCP i UDP, ponieważ jego charakterystyka jest podobna do protokołów TCP i UDP. SCTP jest specjalnie używany do wykonywania działań multi-homing i multi-streaming. Niektóre aplikacje SCTP obejmują wykrywanie usług VoIP, telefonii IP i Signaling System 7/SIGnaling TRANsport (SS7/SIGTRAN). Powiązanie SCTP obejmuje czterokierunkową metodę uzgadniania, jak pokazano na zrzucie ekranu poniżej.



W protokole SCTP skanowanie INIT odbywa się szybko, skanując tysiące portów na sekundę w szybkiej sieci niezakłóconej przez zaporę ogniową, co zapewnia większe poczucie bezpieczeństwa. Skanowanie SCTP INIT jest bardzo podobne do skanowania TCP SYN; stosunkowo, jest również niewidoczny i dyskretny, ponieważ nie może ukończyć powiązań SCTP, przez co połączenie jest półotwarte. Atakujący wysyłają porcję INIT do hosta docelowego. Jeśli port nasłuchuje lub jest otwarty, wysyła potwierdzenie jako porcję INIT+ACK.



Jeśli cel jest nieaktywny i nie nasłuchuje, wysyła potwierdzenie jako porcję ABORT.



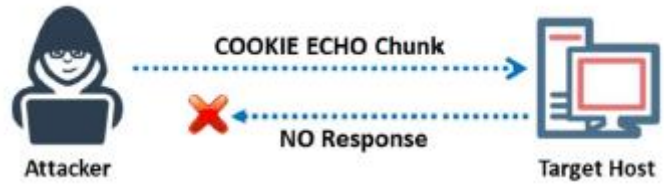
Po kilku retransmisjach, jeśli nie ma odpowiedzi, port jest oznaczony jako filtrowany. Port jest również wskazany jako port filtrowany, jeśli serwer docelowy odpowiada wyjątkiem nieosiągalności ICMP (typ 3, kod 0,1, 2, 3, 9, 10 lub 13). W Zenmap opcja -SY jest używana do wykonania skanowania SCTP INIT.

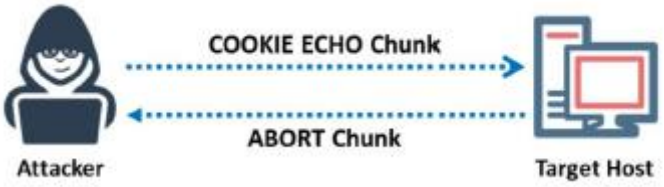
Zalety:

Skanowanie INIT może wyraźnie rozróżnić różne porty, takie jak otwarte, zamknięte i filtrowane stany

SCTP COOKIE ECHO Skanowanie

Skan SCTP COOKIE ECHO to bardziej zaawansowany typ skanowania. W tym typie skanowania atakujący wysyłają fragment COOKIE ECHO do celu, a jeśli docelowy port jest otwarty, po cichu upuszcza pakiety na ten port i nie otrzymasz żadnej odpowiedzi od celu. Jeśli cel odsyła odpowiedź ABORT chunk, port jest traktowany jako port zamknięty. Fragment COOKIE ECHO nie jest blokowany przez niestanowe zestawy reguł zapory sieciowej, jak w przypadku skanowania INIT. Tylko zaawansowany IDS może wykryć skanowanie SCTP COOKIE ECHO. W Zenmap opcja -sz jest używana do wykonania skanowania SCTP COOKIE ECHO





Zalety:

Skanowanie portów nie jest tak widoczne jak skanowanie INIT.

Wady :

Skan SCTP COOKIE ECHO nie może wyraźnie rozróżnić otwartych i filtrowanych portów i pokazuje dane wyjściowe jako otwarte|filtrowane w obu przypadkach.

Skanowanie SSDP i listy

Skanowanie SSDP

Simple Service Discovery Protocol (SSDP) to protokół sieciowy, który ogólnie komunikuje się z maszynami podczas wysyłania do nich zapytań za pomocą rutowalnych adresów multiemisji IPv4 lub IPv6. Usługa SSDP steruje komunikacją dla funkcji Universal Plug and Play (UPnP). Na ogół działa, gdy maszyna nie jest zabezpieczona zaporą ogniową; jednak czasami może działać przez zaporę ogniową. Usługa SSDP odpowie na zapytanie wysłane przez adresy rozgłoszeniowe IPv4 lub IPv6. Ta odpowiedź zawiera informacje o powiązanej z nią funkcji UPnP. Atakujący używa skanowania SSDP do wykrywania luk w zabezpieczeniach UPnP, które mogą pozwolić mu na uruchomienie przepełnienia bufora lub ataków DoS Atakujący może użyć narzędzia do wykrywania informacji UPnP SSDP M-SEARCH, aby

sprawdzić, czy maszyna jest podatna na ataki UPnP. Narzędzie do wyszukiwania informacji UPnP SSDP M-SEARCH zbiera informacje z systemów obsługujących UPnP.

Skanowanie listy

Podczas skanowania listy wykrywanie aktywnego hosta sieciowego jest pośrednie. Skanowanie listy po prostu generuje i drukuje listę adresów IP/nazw bez faktycznego pingowania lub skanowania hostów. W rezultacie skanowanie listy pokazuje wszystkie adresy IP jako „nieskanowane" (0 hostów w górę). Domyślnie Nmap nadal przeprowadza odwrotne rozpoznawanie DNS na każdym hoście, aby poznać ich nazwy. W Zenmap opcja -SL służy do skanowania listy.

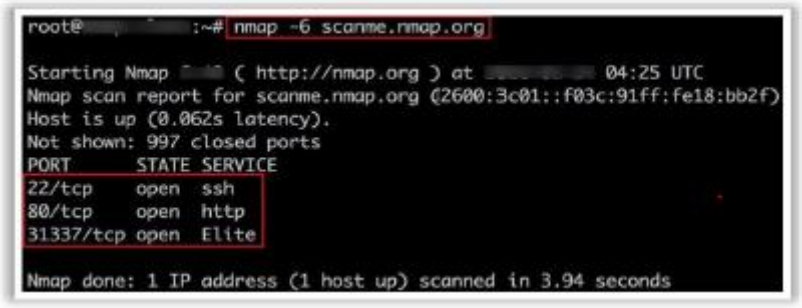
Zalety:

* Skanowanie listy może przeprowadzić dobrą kontrolę poprawności.

* Skanowanie listy wykrywa nieprawidłowo zdefiniowane adresy IP w wierszu poleceń lub w pliku opcji. Przede wszystkim naprawia wykryte błędy, aby uruchomić dowolne „aktywne" skanowanie.

Skanowanie IPv6

IPv6 zwiększa rozmiar przestrzeni adresowej IP z 32 bitów do 128 bitów, aby obsługiwać wyższe poziomy hierarchii adresowania. Tradycyjne techniki skanowania sieci są mniej wykonalne pod względem obliczeniowym ze względu na większą przestrzeń wyszukiwania (64 bity przestrzeni adresowej hosta lub 264 adresy) zapewnianą przez protokół IPv6 w podsieci. Skanowanie sieci IPv6 jest trudniejsze i bardziej złożone niż w przypadku IPv4. Ponadto wiele narzędzi skanujących nie obsługuje testów ping w sieciach IPv6. Atakujący muszą przechwytywać adresy IPv6 z ruchu sieciowego, zarejestrowanych dzienników lub „Otrzymano od" i innych linii nagłówka w zarchiwizowanych wiadomościach e-mail lub wiadomościach Usenet, aby zidentyfikować adresy IPv6 w celu późniejszego przeskanowania portów. Jednak skanowanie sieci IPv6 zapewnia dużą liczbę hostów w podsieci; jeśli atakujący może skompromitować jeden host podsieci, może sondować lokalny adres multiemisji łącza „wszystkich hostów", jeśli numery hostów są sekwencyjne lub używają dowolnego zwykłego schematu. Osoba atakująca musi przeanalizować 264 adresy, aby sprawdzić, czy na hoście w tej podsieci działa określona otwarta usługa. Przy konserwatywnym tempie jednej sondy na sekundę, takie skanowanie zajęłoby około 5 miliardów lat. Atakujący mogą używać Nmap do skanowania IPv6. W Zenmap opcja -6 służy do wykonywania skanowania IPv6.



Wykrywanie wersji usługi

Każdy port ma przypisaną określoną usługę, a każda usługa ma swoją własną wersję. Niektóre wersje protokołów są niepewne i mogą pozwolić atakującemu na złamanie zabezpieczeń maszyny poprzez wykorzystanie tej luki. Wykrywanie wersji usług pomaga atakującym uzyskać informacje o uruchomionych usługach i ich wersjach w systemie docelowym. Uzyskując dokładne numery wersji usługi, osoba atakująca może określić, na jakie luki w zabezpieczeniach jest narażony system docelowy.

Technika wykrywania wersji to nic innego jak badanie portów TCP i UDP. Sondy z bazy danych service-probes Nmap są używane do wysyłania zapytań do różnych usług i dopasowywania wyrażeń w celu rozpoznawania i analizowania odpowiedzi. W Zenmap opcja -sv służy do wykrywania wersji usługi.

Techniki redukcji czasu skanowania Nmap

W Nmap wydajność i dokładność mają wysoki priorytet, a można to osiągnąć jedynie poprzez skrócenie długiego czasu skanowania. Ważne techniki skracania czasu skanowania są następujące:

- Pomiń testy niekrytyczne

Podczas wykonywania skanowania Nmap złożoność czasową można zmniejszyć za pomocą następujących metod:

o Unikanie intensywnego skanowania, jeśli wymagana jest tylko minimalna ilość informacji,

o Liczbę skanowanych portów można ograniczyć za pomocą określonych poleceń.

o Skanowanie portów (-sn) można pominąć wtedy i tylko wtedy, gdy trzeba sprawdzić, czy hosty są online, czy nie.

o Można uniknąć zaawansowanych typów skanowania (-sc, -sv, -o, —traceroute i -A),

o Rozpoznawanie DNS powinno być włączane tylko wtedy, gdy jest to konieczne.

- Zoptymalizuj parametry rozrządu

Aby kontrolować aktywność skanowania, Nmap udostępnia opcję -T do skanowania w zakresie od wysokiego do niskiego poziomu agresywności czasowej. Może to być niezwykle przydatne do skanowania silnie filtrowanych sieci.

- Oddziel i zoptymalizuj skanowanie UDP

Ponieważ wiele wrażliwych usług korzysta z protokołu UDP, skanowanie protokołu UDP jest niezbędne i powinno być skanowane oddzielnie, ponieważ skanowanie TCP ma różne wymagania dotyczące wydajności i charakterystyki czasowej. Co więcej, skanowanie UDP jest bardziej podatne na ograniczenie stopy błędów ICMP w porównaniu ze skanowaniem TCP.

- Zaktualizuj Nmapa

Zawsze zaleca się używanie zaktualizowanej wersji Nmapa, ponieważ zawiera ona wiele poprawek błędów, ważne ulepszenia algorytmiczne i funkcje o wysokiej wydajności, takie jak skanowanie sieci lokalnej ARP.

- Wykonaj współbieżne instancje Nmap

Uruchamianie Nmapa w całej sieci zwykle powoduje, że system jest wolniejszy i mniej wydajny. Nmap obsługuje równoległość i można go również dostosować do konkretnych potrzeb. Staje się bardzo wydajny, gdy uzyskuje się wyobrażenie o niezawodności sieci podczas skanowania większej grupy. Ogólną szybkość skanowania można poprawić, dzieląc je na wiele grup i uruchamiając je jednocześnie.

- Skanuj z korzystnej lokalizacji sieciowej

Zawsze zaleca się uruchamianie Nmapa z sieci lokalnej hosta do miejsca docelowego w sieci wewnętrznej, ponieważ zapewnia to dogłębną ochronę. Skanowanie zewnętrzne jest obowiązkowe

podczas testowania firewalla lub gdy sieć powinna być monitorowana z punktu widzenia zewnętrznego atakującego.

- Zwiększ dostępną przepustowość i czas procesora

Zwiększając dostępną przepustowość lub moc procesora, można skrócić czas skanowania Nmap. Można to zrobić, instalując nową linię danych lub zatrzymując uruchomione aplikacje. Nmap jest kontrolowany przez własne algorytmy kontroli przeciążenia, dzięki czemu można zapobiec zalewaniu sieci. Poprawia to jego dokładność. Wykorzystanie przepustowości Nmapa można przetestować, uruchamiając go w trybie szczegółowym –v

Wykrywanie systemu operacyjnego (przechwytywanie banerów/odcisk palca systemu operacyjnego)

Osoba atakująca wykorzystuje techniki wykrywania systemu operacyjnego lub przechwytywania banerów w celu zidentyfikowania hostów sieciowych, na których działają aplikacje i wersje systemu operacyjnego ze znanymi exploitami. W tej sekcji zapoznasz się z chwytaniem banerów, jego rodzajami i narzędziami do chwytania banerów.

Wykrywanie systemu operacyjnego/przechwytywanie banerów

Przechwytywanie banerów lub „odcisk palca systemu operacyjnego" to metoda używana do określenia systemu operacyjnego działającego w zdalnym systemie docelowym. Jest to ważna metoda skanowania, ponieważ atakujący będzie miał większe prawdopodobieństwo sukcesu, jeśli znany jest system operacyjny systemu docelowego (wiele luk jest specyficznych dla systemu operacyjnego). Atakujący może następnie sformułować strategię ataku w oparciu o system operacyjny systemu docelowego. Istnieją dwie metody przechwytywania banerów: wykrycie banera podczas próby połączenia z usługą, taką jak witryna FTP, oraz pobranie pliku binarnego/bin/ls w celu sprawdzenia architektury systemu. Bardziej zaawansowana technika pobierania odcisków palców polega na odpytywaniu stosu, które przesyła pakiety do hosta sieciowego i ocenia je na podstawie odpowiedzi. Pierwsza metoda stosu zapytań zaprojektowana w odniesieniu do trybu komunikacji TCP ocenia odpowiedź na żądania połączenia. Następna metoda, znana jako analiza początkowego numeru sekwencyjnego (ISN), identyfikuje różnice w generatorach liczb losowych znajdujących się w stosie TCP. Analiza odpowiedzi ICMP to kolejna metoda używana do odcisku palca systemu operacyjnego. Polega na wysyłaniu komunikatów ICMP do zdalnego hosta i ocenie odpowiedzi. Poniżej opisano dwa rodzaje technik przechwytywania banerów:

Aktywne przechwytywanie banerów

Aktywne przechwytywanie banerów opiera się na zasadzie, że stos IP systemu operacyjnego ma unikalny sposób reagowania na specjalnie spreparowane pakiety TCP. Dzieje się tak z powodu różnych interpretacji stosowanych przez dostawców podczas wdrażania stosu TCP/IP w określonym systemie operacyjnym. Podczas aktywnego przechwytywania banerów atakujący wysyła do zdalnego hosta różne zniekształcone pakiety, a odpowiedzi są porównywane z bazą danych. Odpowiedzi z różnych systemów operacyjnych różnią się ze względu na różnice w implementacji stosu TCP/IP. Na przykład narzędzie do skanowania Nmap wykorzystuje serię dziewięciu testów w celu określenia odcisku palca systemu operacyjnego lub przechwytywania banerów. Testy wymienione poniżej dostarczają pewnych informacji na temat aktywnego ataku przechwytywania banerów, jak opisano na stronie www.packetwatch.net:

o Test 1: Pakiet TCP z włączonymi flagami SYN i ECN-Echo jest wysyłany do otwartego portu TCP.

o Test 2: Pakiet TCP bez włączonych flag jest wysyłany do otwartego portu TCP. Ten typ pakietu jest pakietem NULL.

o Test 3: Pakiet TCP z włączonymi flagami URG, PSH, SYN i FIN jest wysyłany do otwartego portu TCP.

o Test 4: Pakiet TCP z włączoną flagą ACK jest wysyłany do otwartego portu TCP,

o Test 5: Pakiet TCP z włączoną flagą SYN jest wysyłany do zamkniętego portu TCP,

o Test 6: Pakiet TCP z włączoną flagą ACK jest wysyłany do zamkniętego portu TCP.

o Test 7: Pakiet TCP z włączonymi flagami URG, PSH i FIN jest wysyłany do zamkniętego portu TCP.

o Test 8 PU (Port nieosiągalny): Pakiet UDP jest wysyłany do zamkniętego portu UDP. Celem jest wydobycie komunikatu „ICMP port nieosiągalny" z maszyny docelowej.

o Test 9 TSeq (test zdolności sekwencji TCP): ten test ma na celu określenie wzorców generowania sekwencji początkowych numerów sekwencyjnych TCP (znanych również jako próbkowanie ISN TCP), numerów identyfikacyjnych IP (znanych również jako próbkowanie IPID) oraz znacznika czasu TCP liczby. Wysyła sześć pakietów TCP z włączoną flagą SYN do otwartego portu TCP.

Celem tych testów jest znalezienie wzorców w początkowej sekwencji liczb, które wybrały implementacje TCP, odpowiadając na żądanie połączenia. Można je podzielić na grupy, takie jak tradycyjne 64K (wiele starych systemów UNIX), losowe przyrosty (nowsze wersje Solaris, IRIX, FreeBSD, Digital UNIX, Cray i wiele innych) lub prawdziwie losowe (Linux 2.0.*, OpenVMS , nowszy system AIX itp.). Skrzynki systemu Windows wykorzystują model „zależny od czasu", w którym numer ISN jest zwiększany o stałą wartość dla każdego wystąpienia.

Pasywne przechwytywanie banerów

Podobnie jak aktywne przechwytywanie banerów, pasywne przechwytywanie banerów również zależy od różnicowej implementacji stosu i różnych sposobów, w jakie system operacyjny reaguje na pakiety. Flowever, zamiast polegać na skanowaniu docelowego hosta, pasywne pobieranie odcisków palców przechwytuje pakiety z docelowego hosta poprzez wąchanie w celu zbadania charakterystycznych znaków, które mogą ujawnić system operacyjny.

Pasywne przechwytywanie banerów obejmuje:

o Przechwytywanie banerów z komunikatów o błędach: komunikaty o błędach dostarczają informacji, takich jak typ serwera, typ systemu operacyjnego i narzędzia SSL używane przez docelowy system zdalny.

o Sniffowanie ruchu sieciowego: przechwytywanie i analizowanie pakietów z celu umożliwia atakującemu określenie systemu operacyjnego używanego przez system zdalny.

o Pobieranie banerów z rozszerzeń strony: Wyszukiwanie rozszerzenia w adresie URL może pomóc w ustaleniu wersji aplikacji. Na przykład .aspx => serwer IIS i platforma Windows.

Cztery obszary, które zwykle określają system operacyjny, podano poniżej:

o TTL (czas życia) pakietów: co system operacyjny ustawia jako czas życia pakietu wychodzącego?

o Rozmiar okna: Jaki jest rozmiar okna ustawiony przez system operacyjny?

o Czy ustawiony jest bit DF (nie fragmentuj): Czy system operacyjny ustawia bit DF?

o TOS (rodzaj usługi): czy system operacyjny ustawia TOS, a jeśli tak, to jakie to ustawienie?

Pasywne pobieranie odcisków palców nie jest ani w pełni dokładne, ani ograniczone do tych czterech podpisów. Flowever, można poprawić jego dokładność, patrząc na kilka podpisów i łącząc informacje. Poniżej znajduje się analiza przechwyconego pakietu opisana przez Lance'a Spitznera w jego artykule na temat pasywnego pobierania odcisków palców:

```
04/20-21:41:48.129662 129.142.224.3:659 -> 172.16.1.107:604
TCP TTL:45 TOS:0x0 ID:56257
***F**A* Seq: 0x9DD90553
Ack: 0xE3C65D7 Win: 0x7D78
```

Zgodnie z czterema kryteriami wyróżnia się:

o TTL: 45

o Rozmiar okna: 0x7D78 (lub 32120 dziesiętnie)

o DF: Bit DF jest ustawiony

o TOS: 0x0

Porównaj te informacje z bazą sygnatur.

TTL: TLL z analizy wynosi 45. Oryginalny pakiet przeszedł 19 przeskoków, aby dotrzeć do celu, więc ustawia oryginalny TTL na 64. Na podstawie tego TTL wygląda na to, że użytkownik wysłał pakiet z systemu Linux lub FreeBSD box (jednak do bazy danych należy dodać więcej sygnatur systemowych). Ten TTL potwierdza to, wdrażając traceroute do zdalnego hosta. Jeśli śledzenie musi być wykonane potajemnie, TTL traceroute (domyślnie 30 przeskoków) można ustawić na jeden lub dwa przeskoki mniej niż zdalny host (opcja -m). Ustawienie traceroute w ten sposób ujawnia informacje o ścieżce (w tym dostawcę nadrzędnego) bez faktycznego kontaktowania się ze zdalnym hostem.

Rozmiar okna: W tym kroku porównywane są rozmiary okien. Rozmiar okna to kolejne skuteczne narzędzie do dokładnego określania, jaki rozmiar okna jest używany i jak często jest zmieniany. W poprzedniej sygnaturze rozmiar okna jest ustawiony na 0x7D78, co jest domyślnym rozmiarem okna używanym przez Linuksa. Ponadto FreeBSD i Solaris mają tendencję do utrzymywania tego samego rozmiaru okna przez całą sesję. Jednak routery Cisco i rozmiary okien systemu Microsoft Windows NT stale się zmieniają. Rozmiar okna jest dokładniejszy, gdy jest mierzony po początkowym uzgadnianiu trójstronnym (ze względu na powolny start TCP).

Bit DF: Większość systemów używa zestawu bitów DF; stąd ma to ograniczoną wartość. Ułatwia to jednak identyfikację kilku systemów, które nie używają flagi DF (takich jak SCO lub OpenBSD).

TOS: TOS ma również ograniczoną wartość, ponieważ wydaje się być bardziej oparty na sesji niż na systemie operacyjnym. Innymi słowy, to nie system operacyjny, ale używany protokół w dużym stopniu determinuje TOS. Korzystając z informacji uzyskanych z pakietu, a konkretnie TTL i rozmiaru okna, można porównać wyniki z bazą sygnatur iz pewną dozą pewności określić system operacyjny (w tym przypadku jądro Linuksa 2.2.x). Pasywne pobieranie odcisków palców, podobnie jak aktywne pobieranie odcisków palców, ma pewne ograniczenia. Po pierwsze, aplikacje budujące własne pakiety (np. Nmap, Hunt, Nemesis itp.) nie będą używać tych samych sygnatur, co system operacyjny. Po drugie, zdalnemu hostowi stosunkowo łatwo jest dostosować ustawienia TTL, rozmiaru okna, DF lub TOS na pakietach. Pasywne pobieranie odcisków palców ma kilka innych zastosowań. Na przykład osoby atakujące mogą wykorzystać ukryte odciski palców do określenia systemu operacyjnego

potencjalnego celu, takiego jak serwer WWW. Użytkownik musi tylko zażądać strony internetowej z serwera, a następnie przeanalizować ślady sniffera. Omija to potrzebę używania aktywnego narzędzia, które mogą wykryć różne systemy IDS. Pasywne pobieranie odcisków palców pomaga również w identyfikowaniu zdalnych zapór proxy. Możliwe może być zidentyfikowanie zapór proxy na podstawie sygnatur, jak omówiono powyżej, po prostu dlatego, że zapory proxy odbudowują połączenia dla klientów. Podobnie pasywnego pobierania odcisków palców można używać do identyfikowania nieuczciwych systemów.

Uwaga: Pasywne przechwytywanie banerów omówimy w późniejszych modułach.

Dlaczego przechwytywanie banerów?

Atakujący wykorzystuje przechwytywanie banerów, aby zidentyfikować system operacyjny używany na docelowym hoście, a tym samym określić luki systemowe i exploity, które mogą działać w tym systemie w celu przeprowadzenia dalszych ataków.

Jak zidentyfikować docelowy system operacyjny

Identyfikacja docelowego systemu operacyjnego jest jednym z ważnych zadań atakującego w celu skompromitowania docelowej sieci/maszyny. W sieci wdrażane są różne standardy, aby umożliwić komunikację między różnymi systemami operacyjnymi. Standardy te regulują funkcjonowanie różnych protokołów, takich jak IP, TCP, UDP itp. Analizując określone parametry/pola w tych protokołach, można odkryć szczegóły systemu operacyjnego. Parametry, takie jak czas życia (TTL) i rozmiar okna TCP w nagłówku IP pierwszego pakietu w sesji TCP, pomagają zidentyfikować system operacyjny uruchomiony na komputerze docelowym. Pole TTL określa maksymalny czas, przez jaki pakiet może pozostawać w sieci, a rozmiar okna TCP określa długość zgłaszanego pakietu. Te wartości różnią się w zależności od systemu operacyjnego, jak opisano w poniższej tabeli:

Operating System	Time To Live	TCP Window Size
Linux	64	5840
FreeBSD	64	65535
OpenBSD	255	16384
Windows	128	65,535 bytes to 1 Gigabyte
Cisco Routers	255	4128
Solaris	255	8760
AIX	255	16384

Atakujący mogą używać różnych narzędzi do wykrywania systemu operacyjnego na docelowej maszynie, w tym Wireshark, Nmap, Unicornscan i Nmap Script Engine. Atakujący mogą również zastosować metodę odcisków palców IPv6, aby przechwycić szczegóły docelowego systemu operacyjnego.

Wykrywanie systemu operacyjnego za pomocą Wireshark

Aby zidentyfikować docelowy system operacyjny, sniffuj/przechwytuj odpowiedź wygenerowaną z maszyny docelowej do maszyny pochodzącej z żądania za pomocą narzędzi do wąchania pakietów, takich jak Wireshark itp., i obserwuj pola rozmiaru okna TTL i TCP w pierwszym przechwyconym

pakiecie TCP. Porównując te wartości z wartościami w powyższej tabeli, możesz określić docelowy system operacyjny, który wygenerował odpowiedź.

Wykrywanie systemu operacyjnego za pomocą Nmap i Unicornscan

Wykrywanie systemu operacyjnego za pomocą Nmap

Aby wykorzystać cel, bardzo ważne jest zidentyfikowanie systemu operacyjnego działającego na docelowym komputerze. Atakujący mogą wykorzystywać różne narzędzia, aby uzyskać szczegółowe informacje o systemie operacyjnym celu. Nmap jest jednym ze skutecznych narzędzi do wykonywania czynności związanych z wykrywaniem systemu operacyjnego. W Zenmap opcja -o służy do wykrywania systemu operacyjnego, który wyświetla szczegóły systemu operacyjnego maszyny docelowej.

Wykrywanie systemu operacyjnego za pomocą Unicornscan

W Unicornscan system operacyjny docelowej maszyny można zidentyfikować, obserwując wartości TTL w uzyskanym wyniku skanowania. Aby wykonać Unicornscan, używana jest składnia #unicornscan ctarget IP address>. Jak pokazano na zrzucie ekranu, wartość tti uzyskana po skanowaniu wynosi 128; stąd system operacyjny to prawdopodobnie Microsoft Windows.

Wykrywanie systemu operacyjnego przy użyciu silnika skryptów Nmap

Nmap Scripting Engine (NSE) w Nmap może być używany do automatyzacji szerokiej gamy zadań sieciowych, umożliwiając użytkownikom pisanie i udostępnianie skryptów. Skrypty te mogą być wykonywane równolegle z taką samą wydajnością i szybkością jak Nmap. Atakujący mogą również używać różnych skryptów w Nmap Script Engine do wykrywania systemu operacyjnego na docelowej maszynie. Na przykład w Nmap, smb-osdiscovery jest wbudowanym skryptem służącym do zbierania informacji o systemie operacyjnym na maszynie docelowej za pośrednictwem protokołu SMB. W Zenmap, NSE można generalnie aktywować za pomocą opcji -sc. Jeśli mają zostać określone niestandardowe skrypty, osoby atakujące mogą użyć opcji —script. Wyniki NSE zostaną wyświetlone zarówno z normalnymi, jak i XML danymi wyjściowymi Nmap.

Wykrywanie systemu operacyjnego za pomocą odcisków palców IPv6

Odcisk palca IPv6 to kolejna technika używana do identyfikacji systemu operacyjnego działającego na komputerze docelowym. Posiada te same funkcjonalności co IPv4, takie jak wysyłanie sond, oczekiwanie i zbieranie odpowiedzi oraz dopasowywanie ich do bazy danych odcisków palców. Różnica między odciskami palców IPv6 i IPv4 polega na tym, że IPv6 wykorzystuje kilka dodatkowych zaawansowanych sond specyficznych dla IPv6 wraz z oddzielnym silnikiem wykrywania systemu operacyjnego dla IPv6. Nmap wysyła prawie 18 sond w następującej kolejności, aby zidentyfikować docelowy system operacyjny przy użyciu metody odcisków palców IPv6.

* Generowanie sekwencji (S1-S6)

* echo ICMPv6 (IE1)

* echo ICMPv6 (IE2)

* Zapytanie o informacje o węźle (Nl)

* Nagabywanie sąsiada (NS)

* UDP (UL)

* Wyraźne powiadomienie o przeciążeniu TCP (TECN)

* TCP (T2-T7)

W Zenmap opcja -6 wraz z opcją -o jest używana do wykrywania systemu operacyjnego przy użyciu metody odcisków palców IPv6.

składnia: # nmap -6 -O <cel>

Skanowanie poza IDS i Firewall

Systemy wykrywania włamań (IDS) i zapory ogniowe to mechanizmy bezpieczeństwa, których celem jest uniemożliwienie atakującemu dostępu do sieci. Jednak nawet systemy IDS i zapory ogniowe mają pewne ograniczenia dotyczące bezpieczeństwa. Atakujący próbują przeprowadzić ataki, aby wykorzystać te ograniczenia. Ta sekcja opisuje różne techniki unikania IDS/firewall, takie jak fragmentacja pakietów, routing źródłowy, fałszowanie adresu IP itp.

Techniki unikania IDS/zapór sieciowych

Chociaż zapory ogniowe i system IDS mogą zapobiegać przedostawaniu się złośliwego ruchu (pakietów) do sieci, osoby atakujące mogą wysyłać do celu zamierzone pakiety, które omijają system IDS/zaporę sieciową, stosując następujące techniki:

* Fragmentacja pakietów

* Routing źródłowy

* Manipulacja portem źródłowym

* Wabik adresu IP

* Fałszowanie adresu IP

* Fałszowanie adresu MAC

* Tworzenie niestandardowych pakietów

* Losowa kolejność hostów

* Wysyłanie złych sum kontrolnych

* Serwery proxy

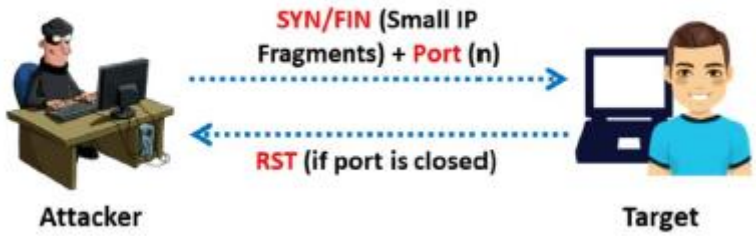
* Anonimizatory

Fragmentacja pakietów

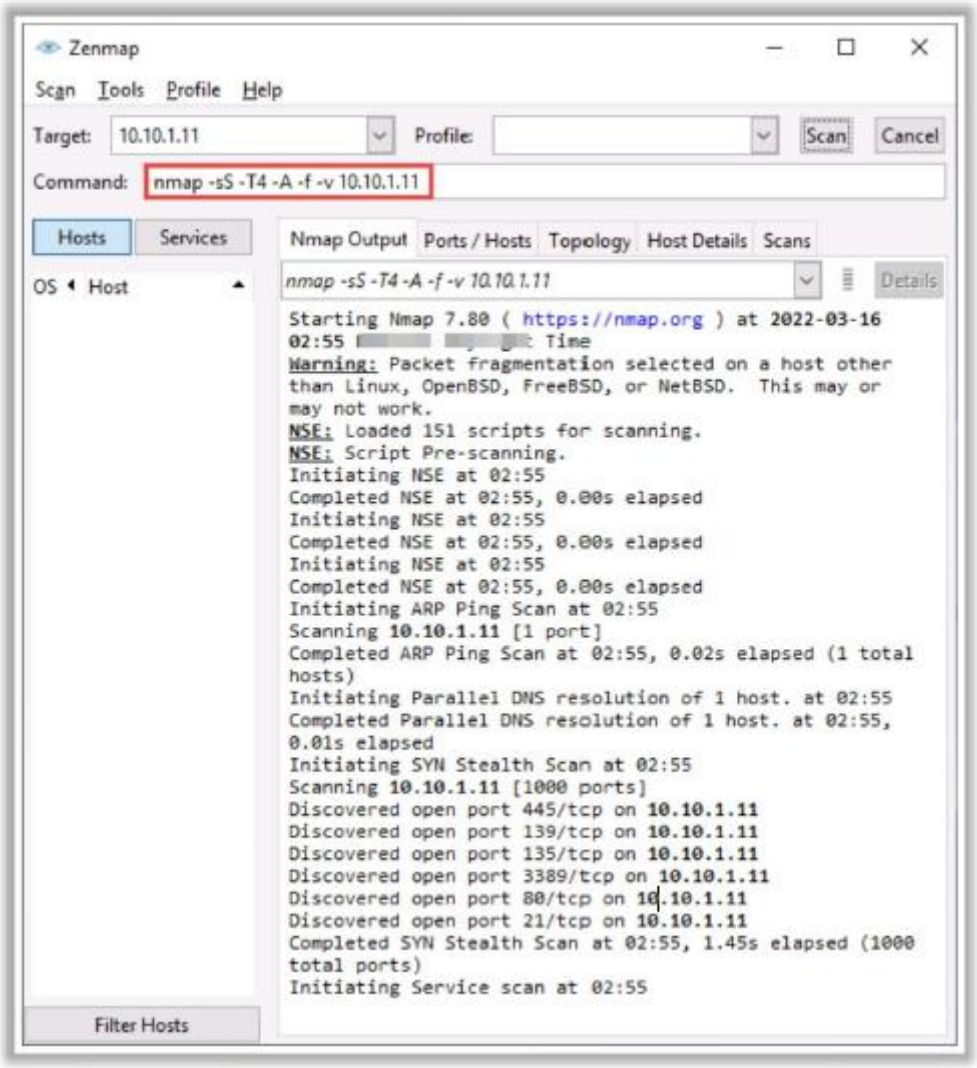
Fragmentacja pakietów odnosi się do dzielenia pakietu sondującego na kilka mniejszych pakietów (fragmentów) podczas wysyłania go do sieci. Kiedy te pakiety docierają do hosta, IDS i zapory sieciowe stojące za hostem generalnie umieszczają je wszystkie w kolejce i przetwarzają jeden po drugim. Ponieważ jednak ta metoda przetwarzania wiąże się z większym zużyciem zasobów procesora i sieci, konfiguracja większości systemów IDS powoduje, że pomijają one pofragmentowane pakiety podczas skanowania portów. Dlatego osoby atakujące używają narzędzi do fragmentacji pakietów, takich jak Nmap i fragroute, w celu podzielenia pakietu sondującego na mniejsze pakiety, które omijają techniki skanowania portów stosowane przez system IDS. Gdy te fragmenty dotrą do docelowego hosta, są ponownie składane, tworząc pojedynczy pakiet.

Skanowanie SYN/FIN przy użyciu fragmentów IP

Skanowanie SYN/FIN przy użyciu fragmentów IP nie jest nową metodą skanowania, ale modyfikacją poprzednich technik. Ten proces skanowania został opracowany w celu uniknięcia fałszywych alarmów generowanych przez inne skany z powodu urządzenia filtrującego pakiety w systemie docelowym. Nagłówek TCP jest dzielony na kilka pakietów, aby ominąć filtr pakietów. W przypadku każdej transmisji każdy nagłówek TCP musi mieć port źródłowy i docelowy dla pakietu początkowego (8-oktet, 64-bit). Zainicjowane flagi w następnym pakiecie umożliwiają zdalnemu hostowi ponowne złożenie pakietów po odebraniu przez moduł protokołu internetowego, który wykrywa pofragmentowane pakiety danych przy użyciu równoważnych pól wartości źródła, miejsca docelowego, protokołu i identyfikacji.

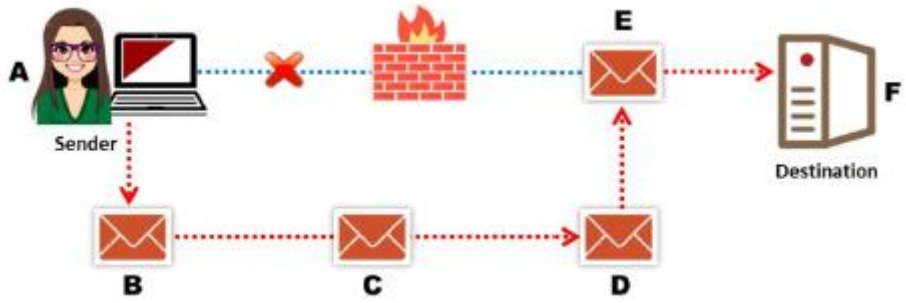


Podczas tego skanowania system dzieli nagłówek TCP na kilka fragmentów i przesyła je przez sieć. Jednak ponowne składanie adresów IP po stronie serwera może skutkować nieprzewidywalnymi i nieprawidłowymi wynikami, takimi jak fragmentacja danych nagłówka IP. Niektóre hosty mogą nie analizować i ponownie składać pofragmentowanych pakietów, co może prowadzić do awarii, restartów, a nawet zrzutów monitorowania urządzeń sieciowych. Niektóre zapory mogą mieć zestawy reguł, które blokują kolejki fragmentacji IP w jądrze (np. opcja CONFIG_IP_ALWAYS_DEFRAG w jądrze Linuksa), chociaż nie jest to powszechnie wdrażane ze względu na niekorzystny wpływ na wydajność. Ponieważ wiele IDS używa metod opartych na sygnaturach do wskazywania prób skanowania nagłówków IP i/lub TCP, użycie fragmentacji często pozwala uniknąć tego typu filtrowania i wykrywania pakietów, co skutkuje dużym prawdopodobieństwem spowodowania problemów w sieci docelowej. Atakujący używają metody skanowania SYN/FIN z fragmentacją adresów IP, aby uniknąć tego typu filtrowania i wykrywania. Poniższy zrzut ekranu pokazuje skanowanie SYN/FIN za pomocą narzędzia Zenmap.



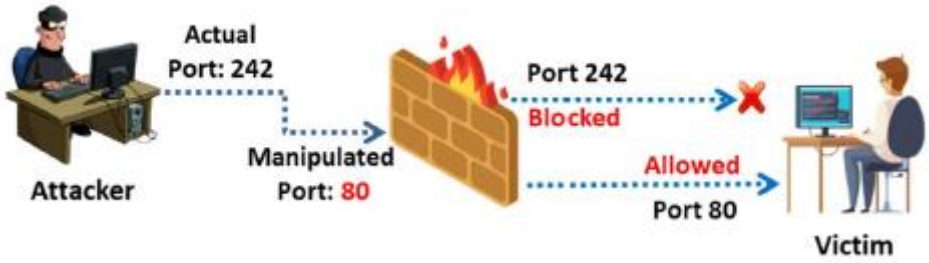
Routing źródłowy

Datagram IP zawiera różne pola, w tym pole opcji IP, w którym przechowywane są informacje o routingu źródłowym oraz lista adresów IP, przez które pakiet dociera do miejsca docelowego. Gdy pakiet przechodzi przez węzły w sieci, każdy router sprawdza docelowy adres IP i wybiera następny przeskok, aby skierować pakiet do miejsca docelowego. Kiedy atakujący wysyłają do celu źle sformułowane pakiety, pakiety te przeskakują przez różne routery i bramy, aby dotrzeć do miejsca docelowego. W niektórych przypadkach routery na ścieżce mogą zawierać skonfigurowane zapory i systemy IDS, które blokują takie pakiety. Aby ich uniknąć, atakujący wymuszają luźny lub ścisły mechanizm routingu źródła, w którym manipulują ścieżką adresu IP w polu opcji IP, tak aby pakiet podążał ścieżką zdefiniowaną przez atakującego (bez routerów skonfigurowanych zaporą sieciową/IDS), aby dotrzeć do miejsca docelowego , unikając w ten sposób zapór ogniowych i systemów IDS. Poniższy rysunek przedstawia routing źródłowy, w którym nadawca dyktuje ostateczną trasę ruchu.



Manipulacja portem źródłowym

Manipulowanie portem źródłowym to technika używana do omijania IDS/firewall, gdzie rzeczywiste numery portów są manipulowane wspólnymi numerami portów w celu obejścia pewnych reguł IDS i firewalla. Główne błędne konfiguracje zabezpieczeń występują z powodu ślepego zaufania do numeru portu źródłowego. Administrator najczęściej konfiguruje zaporę ogniową, przepuszczając ruch przychodzący z dobrze znanych portów, takich jak HTTP, DNS, FTP itp. Zapora ogniowa może po prostu przepuszczać ruch przychodzący z pakietów wysyłanych przez atakujących za pomocą takich wspólnych portów.



Chociaż zapory można zabezpieczyć za pomocą serwerów proxy na poziomie aplikacji lub elementów zapory analizujących protokoły, technika ta pomaga atakującemu w łatwym obejściu reguł zapory. Atakujący próbuje manipulować oryginalnym numerem portu za pomocą wspólnych numerów portów, co może łatwo ominąć IDS/firewall. W Zenmap opcja -g lub —source-port służy do manipulowania portem źródłowym.

Wabik na adres IP

Technika wabika adresu IP polega na generowaniu lub ręcznym określaniu adresów IP wabika w celu uniknięcia IDS/zapór sieciowych. Celowi wydaje się, że wabiki i hosty skanują sieć. Technika ta utrudnia systemowi IDS/firewallowi określenie, który adres IP rzeczywiście skanuje sieć, a który jest wabikiem. Narzędzie do skanowania Nmap ma wbudowaną funkcję skanowania zwaną skanowaniem wabików, która maskuje skanowanie za pomocą wabików. Ta technika generuje wiele adresów IP w celu przeprowadzenia skanowania, co utrudnia docelowym mechanizmom bezpieczeństwa, takim jak IDS, zapory ogniowe itp., identyfikację oryginalnego źródła na podstawie zarejestrowanych dzienników. Docelowy IDS może zgłaszać skanowanie z 5-0 adresów IP; nie może jednak odróżnić rzeczywistego adresu IP skanowania od nieszkodliwych adresów IP wabika. Za pomocą Nmap możesz wykonać dwa rodzaje skanów wabików:

* nmap -D RND:10 [cel]

Za pomocą tego polecenia Nmap automatycznie generuje losową liczbę wabików do skanowania i losowo umieszcza prawdziwy adres IP między adresami IP wabików. Były. Załóżmy, że 10.10.10.10 to docelowy adres IP do przeskanowania. Zatem polecenie skanowania wabika Nmap będzie:

nmap -D RND: 10 10.10.10.10

* nmap -D decoyl,decoy2,decoy3,...,ME,... [target]

Za pomocą tego polecenia możesz ręcznie określić adresy IP wabików, aby przeskanować sieć ofiary. Tutaj musisz oddzielić każdy adres IP wabika przecinkiem (,) i możesz opcjonalnie użyć polecenia ME, aby umieścić swój prawdziwy adres IP na liście wabika. Jeśli umieścisz ME na czwartej pozycji polecenia, twoje prawdziwe IP zostanie odpowiednio ustawione na czwartej pozycji. Jest to opcjonalne polecenie, a jeśli nie wymienisz ME w poleceniu skanowania, Nmap automatycznie umieści twoje prawdziwe IP w dowolnej losowej pozycji. Załóżmy na przykład, że 10.10.1.19 to prawdziwy źródłowy adres IP, a 10.10.1.11 to docelowy adres IP do przeskanowania. Następnie polecenie wabika Nmap będzie:

Składnia:

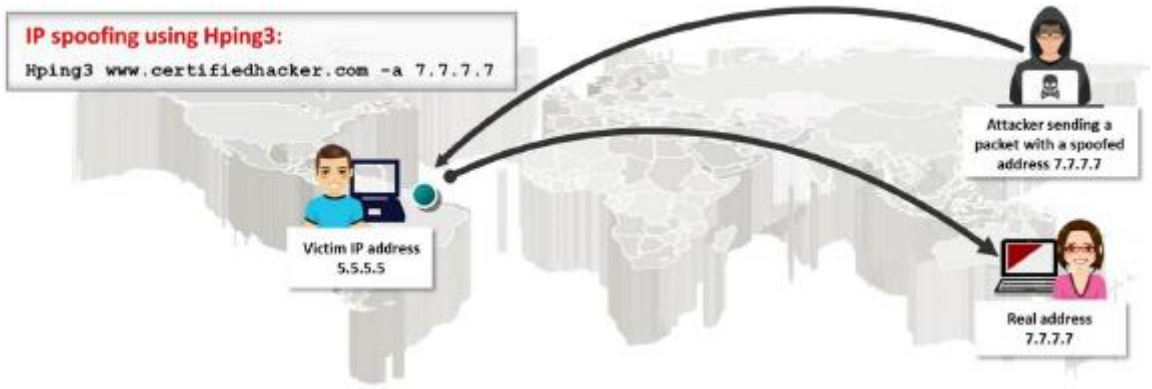
nmap -D 192.168 .0.1172.120 .2.8192.168 .2.8,10.10.1.19,10.10 .1.5

10.10. 1.11

Te wabiki mogą być generowane zarówno podczas początkowych skanów ping, takich jak ICMP, SYN, ACK itp., jak i podczas rzeczywistej fazy skanowania portów. Wabik adresu IP to przydatna technika ukrywania adresu IP. Jednak nie powiedzie się, jeśli cel wykorzystuje aktywne mechanizmy, takie jak śledzenie ścieżki routera, odrzucanie odpowiedzi itp. Ponadto użycie wielu wabików może spowolnić proces skanowania i wpłynąć na dokładność skanowania.

Fałszowanie adresu IP

Większość zapór ogniowych filtruje pakiety na podstawie źródłowego adresu IP. Zapory te sprawdzają źródłowy adres IP i określają, czy pakiet pochodzi z legalnego źródła, czy z nielegalnego źródła. IDS filtruje pakiety z nielegalnych źródeł. Atakujący wykorzystują technikę fałszowania adresów IP, aby ominąć takie IDS/firewalle. Fałszowanie adresu IP to technika przejmowania kontroli, w której osoba atakująca uzyskuje adres IP komputera, zmienia nagłówki pakietów i wysyła pakiety żądań do maszyny docelowej, udając legalnego hosta. Pakiety wydają się być wysyłane z legalnej maszyny, ale w rzeczywistości są wysyłane z maszyny atakującego, podczas gdy adres IP tej maszyny jest ukryty. Kiedy ofiara odpowiada na adres, następuje powrót do sfałszowanego adresu, a nie prawdziwego adresu atakującego. Atakujący najczęściej wykorzystują fałszowanie adresów IP do przeprowadzania ataków DoS. Gdy atakujący wysyła żądanie połączenia do hosta docelowego, host docelowy odpowiada na sfałszowany adres IP. Podszywając się pod nieistniejący adres, cel odpowiada nieistniejącemu systemowi, a następnie zawiesza się do momentu wygaśnięcia sesji, zużywając w ten sposób znaczną ilość własnych zasobów.



Fałszowanie adresów IP przy użyciu Hping3:

Hping3 www.certifiedhacker.com -a 7.7.7.7

Możesz użyć Hping3 do fałszowania adresów IP. Powyższe polecenie pomaga w wysyłaniu dowolnych pakietów TCP/IP do hostów sieciowych.

Uwaga: nie będziesz w stanie zakończyć trójstronnego uzgadniania i otworzyć udanego połączenia TCP ze sfałszowanymi adresami IP.

Fałszowanie adresu MAC

Zapory sieciowe filtrują pakiety na podstawie źródłowego adresu kontroli dostępu do nośnika (MAC). Sprawdzają adres MAC w nagłówku pakietu i określają, czy pakiety pochodzą z legalnego źródła. Zapory ogniowe zezwalają na ruch z określonych źródeł przy użyciu reguł filtrowania adresów MAC i ograniczają pakiety, które nie spełniają reguł filtrowania. Aby uniknąć tych ograniczeń, osoby atakujące wykorzystują techniki fałszowania adresów MAC, w których używają fałszywych adresów MAC i podszywają się pod legalnych użytkowników w celu przeskanowania hostów znajdujących się za zaporą ogniową. Technika fałszowania adresów MAC umożliwia atakującym wysyłanie pakietów żądań do docelowej maszyny/sieci, podszywając się pod legalnego hosta. Atakujący używają narzędzia Nmap do omijania zapór ogniowych poprzez fałszowanie adresów MAC.

Wykonywanie fałszowania adresów MAC w celu skanowania poza IDS i zaporą za pomocą Nmap:

Atakujący używają opcji —spoof-mac Nmap, aby wybrać lub ustawić określony adres MAC dla pakietów i wysłać je do docelowego systemu/sieci.

nmap -sT -Pn --spoof-mac 0 [Docelowy adres IP]

Powyższe polecenie automatycznie generuje losowy adres MAC i dołącza go do pakietów w miejsce oryginalnego adresu MAC podczas skanowania hosta. Tutaj - -spoof-mac 0 reprezentuje randomizację adresu MAC.

*nmap -sT -Pn --spoof-mac [Dostawca] [Docelowy adres IP]

Powyższe polecenie pozwala atakującym wybrać adres MAC od dostawcy i sfałszować go, dołączając go do pakietów w miejsce oryginalnego adresu MAC podczas skanowania. Ten typ skanowania umożliwia atakującym skanowanie w trybie ukrytym, ponieważ oryginalny adres MAC nie jest rejestrowany w dziennikach zapory. --spoof-mac [dostawca] reprezentuje randomizację adresu MAC w oparciu o określonego dostawcę.

* nmap -sT -Pn --spoof-mac [nowy MAC] [Docelowy adres IP]

Powyższe polecenie umożliwia atakującym ręczne wybranie lub ustawienie nowego adresu MAC dla pakietów wysyłanych podczas procesu skanowania. --spoof-mac [nowy MAC] oznacza ręczne ustawienie adresu MAC.

Tworzenie niestandardowych pakietów

Atakujący tworzy i wysyła niestandardowe pakiety w celu przeskanowania zamierzonego celu poza IDS/firewalle. Do tworzenia niestandardowych pakietów wykorzystywane są różne techniki. Niektóre z nich są wspomniane poniżej:

- Tworzenie niestandardowych pakietów za pomocą narzędzi do tworzenia pakietów

Atakujący tworzą niestandardowe pakiety TCP w celu przeskanowania celu z pominięciem zapór ogniowych. Atakujący używają różnych narzędzi do tworzenia pakietów, takich jak kreator pakietów Colasoft (https://www.colasoft.com), NetScanTools Pro (https://www.netscantools.com) itp., aby przeskanować cel znajdujący się poza zaporą ogniową. Narzędzia do tworzenia pakietów tworzą i wysyłają strumienie pakietów (pakiety niestandardowe) przy użyciu różnych protokołów z różnymi szybkościami przesyłania.

o Konstruktor pakietów Colasoft

Colasoft Packet Builder to narzędzie, które umożliwia atakującemu tworzenie niestandardowych pakietów sieciowych i pomaga specjalistom ds. bezpieczeństwa ocenić sieć. Atakujący może wybrać pakiet TCP z dostarczonych szablonów i zmienić parametry w dekoderze, edytorze szesnastkowym lub ASCII, aby utworzyć pakiet. Oprócz budowania pakietów, Colasoft Packet Builder obsługuje zapisywanie pakietów do plików pakietów i wysyłanie pakietów do sieci.

W Konstruktorze pakietów dostępne są trzy widoki: Lista pakietów, Edytor dekodowania i Edytor szesnastkowy.

* Lista pakietów wyświetla wszystkie skonstruowane pakiety. Gdy wybierzesz jeden lub więcej pakietów na Liście pakietów, pierwszy podświetlony pakiet zostanie wyświetlony zarówno w Edytorze dekodowania, jak i Edytorze szesnastkowym do edycji.

* W Hex Editor dane pakietu są reprezentowane jako wartości szesnastkowe i znaki ASCII; znaki niedrukowalne są reprezentowane przez kropkę w sekcji ASCII. Można edytować wartości szesnastkowe lub znaki ASCII.

* Edytor dekodowania umożliwia atakującemu edycję pakietów bez zapamiętywania długości wartości, kolejności bajtów i przesunięć. Możesz wybrać pole i zmienić wartość w polu edycji.

Aby utworzyć pakiet, możesz użyć polecenia dodaj lub wstaw pakiet w menu Edycja lub na pasku narzędzi, aby utworzyć nowy pakiet. Atakujący może wysłać skonstruowany pakiet bezpośrednio do sieci i kontrolować sposób, w jaki Colasoft Packet Builder wysyła pakiety, określając na przykład interwał między pakietami, czasy pętli i opóźnienie między pętlami. Ten konstruktor pakietów przeprowadza audyty sieci i sprawdza ochronę sieci przed atakami i intruzami. Atakujący mogą używać tego konstruktora pakietów do tworzenia pofragmentowanych pakietów w celu ominięcia zapór sieciowych i systemów IDS. Mogą również tworzyć pakiety i zalewać ofiarę bardzo dużą liczbą pakietów, co może skutkować atakami DoS.

Losowanie kolejności hostów i wysyłanie złych sum kontrolnych

Losowa kolejność hostów

Atakujący skanuje liczbę hostów w sieci docelowej w losowej kolejności, aby przeskanować zamierzony cel, który znajduje się za zaporą ogniową. Opcją używaną przez Nmap do skanowania z losową kolejnością hostów jest --randomize-hosts. Ta technika instruuje Nmapa, aby przetasował każdą grupę 16384 hostów przed skanowaniem z opcjami wolnego czasu, dzięki czemu skanowanie jest mniej zauważalne dla systemów monitorowania sieci i zapór ogniowych. Jeśli losowane są większe grupy, należy zwiększyć PING_GROUP_SZ w nmap.h i ponownie skompilować. Można zastosować inną metodę, generując listę docelowych adresów IP za pomocą polecenia list scan -SL -n -ON <nazwa pliku>, a następnie losując ją za pomocą skryptu Perla i dostarczając całą listę do Nmapa za pomocą polecenia -iL.

Wysyłanie nieprawidłowych sum kontrolnych

Atakujący wysyła pakiety ze złymi lub fałszywymi sumami kontrolnymi TCP/UPD do zamierzonego celu, aby uniknąć określonych zestawów reguł zapory. Sumy kontrolne TCP/UPD służą do zapewnienia integralności danych. Wysyłanie pakietów z nieprawidłowymi sumami kontrolnymi może pomóc atakującym w uzyskaniu informacji z niewłaściwie skonfigurowanych systemów poprzez sprawdzanie odpowiedzi. Jeśli jest odpowiedź, to jest ona z IDS lub firewalla, który nie zweryfikował otrzymanej sumy kontrolnej. Jeśli nie ma odpowiedzi lub pakiety są odrzucane, można wywnioskować, że system jest skonfigurowany. Ta technika instruuje Nmapa, aby wysyłał pakiety z nieprawidłowymi sumami kontrolnymi TCP, UDP lub SCTP do hosta docelowego. Opcja używana przez Nmapa to --badsum.

Serwery proxy

Serwer proxy to aplikacja, która może służyć jako pośrednik do łączenia się z innymi komputerami. Używany jest serwer proxy:

- Jako zapora ogniowa i do ochrony sieci lokalnej przed atakami z zewnątrz.

- Jako multiplekser adresów IP, który pozwala kilku komputerom łączyć się z Internetem, gdy masz tylko jeden adres IP (NAT/PAT).

- Aby anonimizować surfowanie po Internecie (do pewnego stopnia).

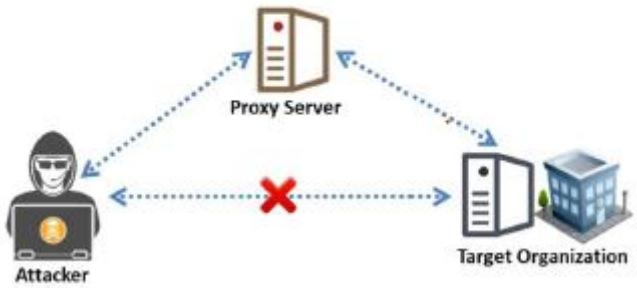
- Aby wyodrębnić niechciane treści, takie jak reklamy lub „nieodpowiednie” materiały (przy użyciu wyspecjalizowanych serwerów proxy).

- Aby zapewnić pewną ochronę przed atakami hakerskimi.

- Aby zaoszczędzić przepustowość.

Jak działa serwer proxy?

Początkowo, gdy korzystasz z serwera proxy, aby zażądać określonej strony internetowej na rzeczywistym serwerze, serwer proxy ją otrzymuje. Serwer proxy następnie wysyła żądanie do rzeczywistego serwera w Twoim imieniu. Pośredniczy między tobą a rzeczywistym serwerem, aby przesłać żądanie i odpowiedzieć na nie, jak pokazano na poniższym rysunku.



W tym procesie serwer proxy odbiera komunikację między klientem a miejscem docelowym aplikacji. Aby skorzystać z serwera proxy, osoba atakująca musi skonfigurować programy klienckie w taki sposób, aby mogły wysyłać swoje żądania do serwera proxy zamiast do miejsca docelowego.

Dlaczego atakujący używają serwerów proxy?

Atakującemu łatwiej jest zaatakować lub zhakować określony system niż ukryć źródło ataku. Dlatego głównym wyzwaniem dla atakującego jest ukrycie swojej tożsamości, tak aby nie można było go namierzyć. W ten sposób atakujący używa serwera proxy, aby uniknąć wykrycia ataku poprzez maskowanie swojego adresu IP. Kiedy osoba atakująca używa serwera proxy do łączenia się z systemem docelowym, dzienniki serwera rejestrują adres źródłowy serwera proxy, a nie adres źródłowy osoby atakującej. Witryny proxy pomagają atakującemu anonimowo przeglądać Internet i uzyskiwać dostęp do zablokowanych witryn (tj. omijać ograniczenia zapory sieciowej). W ten sposób osoba atakująca może anonimowo przeglądać witryny z ograniczeniami bez użycia źródłowego adresu IP.

Atakujący wykorzystują serwery proxy:

* Aby ukryć rzeczywiste źródło skanowania i ominąć pewne ograniczenia IDS/zapory sieciowej.

* Aby ukryć źródłowy adres IP, aby mogli włamać się bez żadnych konsekwencji prawnych.

* Aby zamaskować rzeczywiste źródło ataku, wykorzystując fałszywy adres źródłowy serwera proxy.

* Aby uzyskać zdalny dostęp do intranetu i innych zasobów witryny, które normalnie są niedostępne.

* Aby przerwać wszystkie żądania wysyłane przez użytkownika i przesłać je do trzeciego miejsca docelowego; w związku z tym ofiary będą mogły zidentyfikować jedynie adres serwera proxy.

* Aby połączyć wiele serwerów proxy, aby uniknąć wykrycia.

Darmowe serwery proxy

Niektóre bezpłatne serwery proxy dostępne w Internecie, które mogą pomóc w uzyskaniu dostępu do zastrzeżonych witryn bez ujawniania adresu IP. W wyszukiwarce Google wpisz „Free Proxy Servers”, aby zobaczyć listę takich serwerów. Wybierz jedną z tej listy, pobierz ją i zainstaluj, aby przeglądać anonimowo bez ujawniania swojego prawidłowego adresu IP.

Łańcuch proxy

Łańcuch serwerów proxy pomaga atakującemu zwiększyć jego anonimowość w Internecie. Anonimowość w Internecie zależy od liczby serwerów proxy używanych do pobierania docelowej

aplikacji; im większa liczba używanych serwerów proxy, tym większa jest anonimowość atakującego. Proces łączenia serwerów proxy opisano poniżej:

* Użytkownik żąda zasobu od miejsca docelowego.

* Klient proxy w systemie użytkownika łączy się z serwerem proxy i przekazuje żądanie do serwera proxy.

* Serwer proxy usuwa informacje identyfikacyjne użytkownika i przekazuje żądanie do następnego serwera proxy.

* Ten proces jest powtarzany przez wszystkie serwery proxy w łańcuchu.

* Wreszcie niezaszyfrowane żądanie jest przekazywane do serwera WWW.

Narzędzia proxy

Narzędzia proxy mają na celu umożliwienie użytkownikom anonimowego surfowania po Internecie poprzez ukrywanie ich adresu IP za pośrednictwem łańcucha serwerów proxy SOCKS lub HTTP. Narzędzia te mogą również działać jako serwery proxy HTTP, poczty, FTP, SOCKS, news, telnet i HTTPS.

Przełącznik proxy

Proxy Switcher umożliwia atakującym anonimowe surfowanie po Internecie bez ujawniania ich adresu IP. Pomaga także atakującym uzyskać dostęp do różnych zablokowanych witryn w organizacji. Ponadto pozwala uniknąć wszelkiego rodzaju ograniczeń narzuconych przez witryny docelowe.

CyberGhost VPN

CyberGhost VPN ukrywa adres IP atakującego i zastępuje go wybranym adresem IP, umożliwiając mu anonimowe surfowanie i dostęp do zablokowanych lub ocenzurowanych treści. Szyfruje połączenie i nie prowadzi logów, zabezpieczając w ten sposób dane.

Oprócz narzędzi proxy wymienionych powyżej, istnieje wiele innych narzędzi proxy, których celem jest umożliwienie użytkownikom anonimowego surfowania po Internecie. Poniżej wymieniono niektóre dodatkowe narzędzia proxy:

* Pakiet Burp (https://www.portswigger.net)

* Tor (https://www.torproject.org)

* CCProxy (https://www.youngzsoft.net)

* Tarcza Hotspot (https://www.hotspotshield.com)

Narzędzia proxy dla urządzeń mobilnych

Shadowsocks

Shadowsocks to wysokowydajny, wieloplatformowy, zabezpieczony serwer proxy socks5. Przyjmuje najnowocześniejsze techniki z asynchronicznymi wejściami/wyjściami i programowaniem sterowanym zdarzeniami. To narzędzie jest dostępne na wielu platformach, w tym na komputerach PC, MAC, urządzeniach mobilnych (Android i iOS) oraz routerach (OpenWRT). Jest to narzędzie o niskim zużyciu zasobów, które jest odpowiednie dla urządzeń z niższej półki i urządzeń wbudowanych. Obsługuje implementacje open-source w Pythonie, node.js, golang, C# i czystym C. Shadowsocks pomaga atakującym w prywatnym i bezpiecznym surfowaniu po Internecie.

Poniżej wymieniono niektóre dodatkowe narzędzia proxy dla urządzeń mobilnych:

- ProxyDroid (https://github.com)

- Proxy Manager (https://play.google.com)

- CyberGhost VPN (https://www.cyberghostvpn.com)

- Servers Ultimate (https://icecoldapps.com)

Anonimizatory

Anonimizator to pośredni serwer umieszczony między użytkownikiem końcowym a witryną internetową, który uzyskuje dostęp do witryny w jego imieniu i uniemożliwia śledzenie działań związanych z surfowaniem po sieci. Anonimizatory pozwalają użytkownikom ominąć cenzurę Internetu. Anonimizator usuwa z systemu wszelkie informacje identyfikujące (adres IP) podczas przeglądania Internetu, zapewniając w ten sposób prywatność. Szyfruje dane przesyłane z komputera do dostawcy usług internetowych (ISP). Większość anonimizatorów może anonimizować usługi internetowe (HTTP:), File Transfer Protocol (FTP:) i gopher (gopher:)). Aby anonimowo odwiedzić stronę, możesz odwiedzić preferowaną witrynę anonimizującą i wpisać nazwę docelowej witryny w polu anonimizacji. Alternatywnie możesz ustawić stronę główną przeglądarki tak, aby wskazywała na anonimizator w celu anonimizacji późniejszego dostępu do sieci. Ponadto możesz anonimowo podawać hasła i inne informacje do witryn bez ujawniania żadnych dodatkowych informacji, takich jak adres IP. Atakujący mogą skonfigurować anonimizator jako stały serwer proxy, ustawiając nazwę witryny jako ustawienie opcji HTTP, FTP, Gopher i innych opcji proxy w menu konfiguracji aplikacji, ukrywając w ten sposób swoje złośliwe działania.

Dlaczego warto używać anonimizatora?

Powody korzystania z anonimizatorów obejmują:

* Zapewnienie prywatności: Chroń swoją tożsamość, uniemożliwiając śledzenie działań związanych z nawigacją po sieci. Twoja prywatność jest utrzymywana do momentu ujawnienia swoich danych osobowych w Internecie, na przykład poprzez wypełnienie formularzy.

* Dostęp do treści objętych ograniczeniami rządowymi: większość rządów uniemożliwia swoim obywatelom dostęp do niektórych stron internetowych lub treści uznanych za nieodpowiednie lub wrażliwe. Dostęp do tych witryn można jednak nadal uzyskać za pomocą anonimizatora znajdującego się poza krajem docelowym.

* Ochrona przed atakami online: Anonimizator może chronić Cię przed wszystkimi przypadkami ataków typu pharming online, kierując cały ruch internetowy klientów przez chroniony serwer DNS.

* Omijanie reguł IDS i zapory sieciowej: Zapory ogniowe są zazwyczaj omijane przez pracowników lub uczniów uzyskujących dostęp do stron internetowych, do których nie powinni mieć dostępu. Usługa anonimizatora omija zaporę sieciową Twojej organizacji, konfigurując połączenie między Twoim komputerem a usługą anonimizatora. Dlatego zapory sieciowe widzą tylko połączenie z twojego komputera na adres internetowy podmiotu anonimizującego. Anonimizator następnie połączy się do dowolnej strony internetowej (np. Twittera) za pomocą połączenia internetowego, a następnie przekierować treść z powrotem do Ciebie. W Twojej organizacji system wydaje się być po prostu podłączony do adresu internetowego anonimizatora, ale nie do rzeczywistej witryny, którą przeglądasz.

Oprócz ochrony tożsamości użytkowników anonimizatory mogą być również wykorzystywane do atakowania witryn internetowych bez śledzenia.

Rodzaje anonimizatorów

Istnieją dwa podstawowe typy anonimizatorów: anonimizatory sieciowe i anonimizatory jednopunktowe.

Sieciowe anonimizatory

Anonimizator sieciowy najpierw przesyła Twoje informacje przez sieć komputerów połączonych z Internetem, zanim przekaże je do strony internetowej. Ponieważ informacje przechodzą przez kilka komputerów internetowych, ustanowienie połączenia między tobą a anonimizatorem staje się uciążliwe dla każdego, kto próbuje śledzić twoje informacje.

Przykład: jeśli chcesz odwiedzić dowolną stronę internetową, musisz złożyć wniosek. Żądanie najpierw przejdzie przez komputery internetowe A, B i C, zanim przejdzie do witryny internetowej.

Zaleta: Złożoność komunikacji sprawia, że analiza ruchu jest złożona.

Wada: każda komunikacja sieciowa obejmująca wiele węzłów wiąże się z pewnym ryzykiem naruszenia poufności w każdym węźle.

Jednopunktowe anonimizatory

Anonimizatory jednopunktowe najpierw przesyłają Twoje informacje przez stronę internetową przed wysłaniem ich do docelowej strony internetowej, a następnie przekazują ci informacje zebrane z docelowej strony internetowej za pośrednictwem strony internetowej w celu ochrony Twojej tożsamości.

Zaleta: Komunikacja na odległość ukrywa adres IP i powiązane informacje identyfikacyjne.

Wada: Oferuje mniejszą odporność na wyrafinowaną analizę ruchu.

Narzędzia anonimizujące wykorzystują różne techniki, takie jak SSH, VPN i serwery proxy HTTP, które umożliwiają dostęp do zablokowanych lub ocenzurowanych treści w Internecie z pominięciem reklam.

Whonix

Whonix to system operacyjny dla komputerów stacjonarnych zaprojektowany z myślą o zaawansowanych zabezpieczeniach i prywatności. Łagodzi zagrożenie typowych wektorów ataku przy zachowaniu użyteczności. Anonimowość online jest realizowana za pośrednictwem bezpiecznego, automatycznego i obejmującego cały komputer korzystania z sieci Tor. Składa się z mocno zrekonfigurowanej bazy Debiana, która jest uruchamiana na wielu maszynach wirtualnych, zapewniając znaczną warstwę ochrony przed złośliwym oprogramowaniem i wyciekami adresów IP.

Poniżej wymieniono niektóre dodatkowe anonimizatory:

- Psiphon (https://psiphon.co)

- TunnelBear (https://www.tunnelbeor.com)

- Niewidzialny projekt internetowy (I2P) (https://geti2p.net)

- JonDo (https://ononymous-proxy-servers.net)

Poniżej omówiono różne anonimizatory dla urządzeń mobilnych:

Orbot

Orbot to aplikacja proxy, która umożliwia innym aplikacjom bezpieczniejsze korzystanie z Internetu. Używa Tora do szyfrowania ruchu internetowego, a następnie ukrywa go, odbijając się od szeregu komputerów na całym świecie. Tor to darmowe oprogramowanie, które zapewnia otwartą sieć, która pomaga chronić twój system przed wszelkimi formami nadzoru sieciowego, które mogą naruszyć wolność osobistą i prywatność, a także poufne działania i relacje biznesowe poprzez rodzaj monitorowania bezpieczeństwa państwa znanego jako „analiza ruchu". Orbot tworzy prawdziwie prywatne połączenie internetowe.

Psiphon Pro

Psiphon Pro to narzędzie do obejścia opracowane przez firmę Psiphon, Inc., które wykorzystuje technologię VPN, SSH i proxy HTTP, aby zapewnić otwarty i nieocenzurowany dostęp do treści internetowych. Jednak Psiphon Pro nie zwiększa prywatności w Internecie i nie jest narzędziem bezpieczeństwa online.

Cechy:

o Tryb przeglądarki lub VPN (całe urządzenie): można wybrać, czy tunelować wszystko

lub po prostu przeglądarka internetowa.

o Statystyki w aplikacji: Dzięki temu dowiesz się, z jakiego ruchu korzystasz.

Narzędzia do obchodzenia cenzury

Alkasir

Alkasir to wieloplatformowe, otwarte i solidne narzędzie do obchodzenia cenzury stron internetowych, które również mapuje wzorce cenzury na całym świecie. Alkasir umożliwia atakującym identyfikację ocenzurowanych linków. Informuje ich o linkach, które są nadal blokowane i linkach, które nie są blokowane.

Tails

Tails to działający system operacyjny, który użytkownicy mogą uruchomić na dowolnym komputerze z napędu DVD, pamięci USB lub karty SD. Wykorzystuje najnowocześniejsze narzędzia kryptograficzne do szyfrowania plików, wiadomości e-mail i wiadomości błyskawicznych. Umożliwia atakującym anonimowe korzystanie z Internetu i obejście cenzury. Nie pozostawia śladów na komputerze.

Środki zaradcze skanowania sieciowego

W przypadku hakowania etycznego haker etyczny, znany również jako „tester pióra”, musi wykonać dodatkowe zadanie, którego nie wykonuje zwykły haker (tj. przyjąć środki zaradcze przeciwko odpowiednim lukom ustalonym podczas hakowania). Jest to niezbędne, ponieważ znajomość luk w zabezpieczeniach w Twojej sieci jest bezwartościowa, chyba że zastosujesz środki chroniące ją przed prawdziwymi hakerami. W tej sekcji omówiono różne środki zaradcze chroniące przed atakami polegającymi na skanowaniu sieci.

Środki zaradcze dotyczące skanowania portów

Jak omówiono wcześniej, skanowanie portów dostarcza atakującym dużej ilości przydatnych informacji, takich jak adresy IP, nazwy hostów, otwarte porty i usługi działające na portach. Otwarte porty oferują atakującemu łatwy sposób na włamanie się do sieci. Nie ma jednak powodu do niepokoju, pod warunkiem, że system lub sieć jest zabezpieczona przed skanowaniem portów poprzez zastosowanie następujących środków zaradczych:

* Skonfiguruj reguły zapory sieciowej i systemu wykrywania włamań (IDS) w celu wykrywania i blokowania sond.

* Zapora powinna być zdolna do wykrywania sond wysyłanych przez atakujących za pomocą narzędzi do skanowania portów. Nie powinno przepuszczać ruchu po zwykłym sprawdzeniu nagłówka TCP. Zapora powinna być w stanie zbadać dane zawarte w każdym pakiecie przed zezwoleniem na przejście przez niego ruchu.

* Uruchom narzędzia do skanowania portów na hostach w sieci, aby określić, czy zapora dokładnie wykrywa aktywność skanowania portów.

* Niektóre zapory sieciowe radzą sobie lepiej niż inne, jeśli chodzi o wykrywanie niewidzialnych skanów. Na przykład wiele zapór ma określone opcje wykrywania skanów SYN, podczas gdy inne ignorują skany FIN.

* Upewnij się, że oprogramowanie sprzętowe routera, IDS i zapory jest zaktualizowane do najnowszych wydań/wersji.

* Skonfiguruj komercyjne zapory ogniowe, aby chronić sieć przed szybkim skanowaniem portów i powodziami SYN.

* Hakerzy używają narzędzi takich jak Nmap i przeprowadzają wykrywanie systemu operacyjnego, aby wąchać szczegóły zdalnego systemu operacyjnego. Dlatego ważne jest, aby w takich przypadkach zastosować IDS. Snort (https://www.snort.org) to bardzo przydatna technologia wykrywania włamań i zapobiegania im, głównie dlatego, że sygnatury są często dostępne od autorów publicznych.

* Pozostaw jak najmniej otwartych portów i filtruj resztę, ponieważ intruz może próbować wejść przez dowolny otwarty port. Użyj niestandardowego zestawu reguł, aby zablokować sieć, zablokować niechciane porty na zaporze i odfiltrować następujące porty: 135-159, 256-258, 389, 445, 1080, 1745 i 3268.

* Blokuj niechciane usługi działające na portach i aktualizuj wersje usług.

* Upewnij się, że wersje usług działających na portach nie są podatne na ataki.

* Blokuj przychodzące typy komunikatów ICMP i wszystkie wychodzące komunikaty ICMP typu 3 o nieosiągalności na routerach granicznych ustawionych przed głównym firewallem firmy.

* Atakujący próbują wykonać routing źródłowy i wysłać pakiety do celów, które mogą nie być osiągalne przez Internet, za pomocą hosta pośredniego, który może wchodzić w interakcje z celem. Dlatego konieczne jest upewnienie się, że zapora ogniowa i router mogą blokować takie techniki routingu źródłowego.

* Upewnij się, że mechanizmy używane do routingu i filtrowania odpowiednio na routerach i zaporach ogniowych nie mogą zostać ominięte przy użyciu określonego portu źródłowego lub metod routingu źródłowego.

* Przetestuj przestrzeń adresową IP za pomocą skanowania portów TCP i UDP oraz sond ICMP w celu określenia konfiguracji sieci i dostępnych portów.

* Upewnij się, że skonfigurowano reguły ochrony przed skanowaniem i fałszowaniem.

* Jeśli używana jest zapora komercyjna, upewnij się, że:

o Jest załatany najnowszymi aktualizacjami.

o Posiada poprawnie zdefiniowane reguły antyspoofingowe,

o Jego usługi trybu szybkiego są bezużyteczne.

* Upewnij się, że opakowania TCP ograniczają dostęp do sieci na podstawie nazw domen lub adresów IP.

* Przetestuj, jak zapora sieciowa i IDS zarządzają pofragmentowanymi pakietami, używając fragtest i fragroute.

* Używaj serwerów proxy do blokowania pofragmentowanych lub zniekształconych pakietów.

* Upewnij się, że zapory przekierowują skany otwartych portów do pustych hostów lub honeypotów, aby zadanie skanowania portów było trudne i czasochłonne.

* Zastosuj system zapobiegania włamaniom (IPS) do identyfikowania prób skanowania portów i umieszczania adresów IP na czarnej liście.

Środki zaradcze związane z przechwytywaniem banerów

- Wyłączanie lub zmiana banera

Otwarty port wskazuje, że działa na nim usługa/baner. Kiedy atakujący łączą się z otwartym portem przy użyciu technik przechwytywania banerów, system wyświetla baner zawierający poufne informacje, takie jak system operacyjny, typ serwera i wersja. Wykorzystując zebrane informacje, atakujący identyfikuje określone luki w zabezpieczeniach, które może wykorzystać, a następnie przeprowadza ataki. Środki zaradcze przeciwko atakom polegającym na przechwytywaniu banerów są następujące:

o Wyświetlaj fałszywe banery w celu wprowadzenia w błąd lub oszukania atakujących.

o Wyłącz niepotrzebne usługi na hoście sieciowym, aby ograniczyć ujawnianie informacji,

o Użyj narzędzi do maskowania serwera, aby wyłączyć lub zmienić informacje na banerze.

o Usuń niepotrzebne nagłówki HTTP i dane odpowiedzi oraz zamaskuj serwer, podając fałszywe podpisy. Zapewnia to również możliwość wyeliminowania rozszerzeń plików, takich jak .asp i .aspx, które wyraźnie wskazują, że witryna działa na serwerze firmy Microsoft.

o W przypadku Apache 2.x z modułem mod_headers użyj dyrektywy w pliku httpd.conf, aby zmienić nagłówek informacyjny banera i ustawić serwer jako Nowa nazwa serwera.

o Ewentualnie zmień wiersz ServerSignature na ServerSignatureOff w pliku httpd.conf.

o Wyłącz szczegóły dostawcy i wersji na banerach.

o Zmodyfikuj wartość Server Tokens z Full na Prod w pliku httpd.conf Apache, aby zapobiec ujawnieniu wersji serwera.

o Zmień wartość RemoveServerHeader z 0 na 1 w pliku konfiguracyjnym UrlScan.ini znajdującym się w C: WindowsSystem32inetservUrlscan. Ta metoda zapobiega ujawnieniu wersji serwera.

o Oszukać atakujących, modyfikując wartość AlternateServerName na wartości takie jak xyz lub myserver.

o Wyłącz metody HTTP, takie jak Connect, Put, Delete i Options z serwerów aplikacji internetowych.

o Usuń nagłówek x-Powered-By tylko za pomocą opcji customHeaders w sekcji <system.webServer> pliku web.config.

- Ukrywanie rozszerzeń plików na stronach internetowych

Rozszerzenia plików ujawniają informacje o podstawowej technologii serwera, której osoba atakująca może użyć do przeprowadzenia ataków. Środki zaradcze przeciwko takim atakom polegającym na przechwytywaniu banerów są następujące:

o Ukryj rozszerzenia plików, aby zamaskować technologię internetową.

o Zamień mapowania aplikacji, takie jak .asp, na .htm, .foo itp., aby ukryć tożsamość serwerów.

o Użytkownicy Apache mogą używać dyrektyw mod_negotiation.

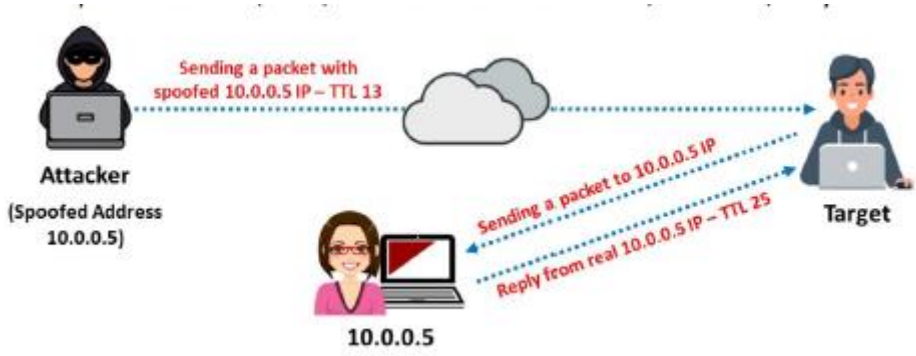
o Użytkownicy IIS mogą używać narzędzi takich jak PageXchanger do zarządzania rozszerzeniami plików.

Uwaga: Lepiej w ogóle nie używać rozszerzeń plików.

Techniki wykrywania fałszowania adresów IP

• Bezpośrednie sondy TTL

W tej technice początkowo wysyłasz pakiet (żądanie ping) do legalnego hosta i czekasz na odpowiedź. Sprawdź, czy wartość TTL w odpowiedzi odpowiada wartości sprawdzanego pakietu. Oba będą miały ten sam TTL, jeśli używają tego samego protokołu. Chociaż początkowe wartości TTL różnią się w zależności od używanego protokołu, powszechnie stosuje się kilka początkowych wartości TTL. W przypadku protokołu TCP/UDP wartości to 64 i 128; dla ICMP są to 128 i 255.

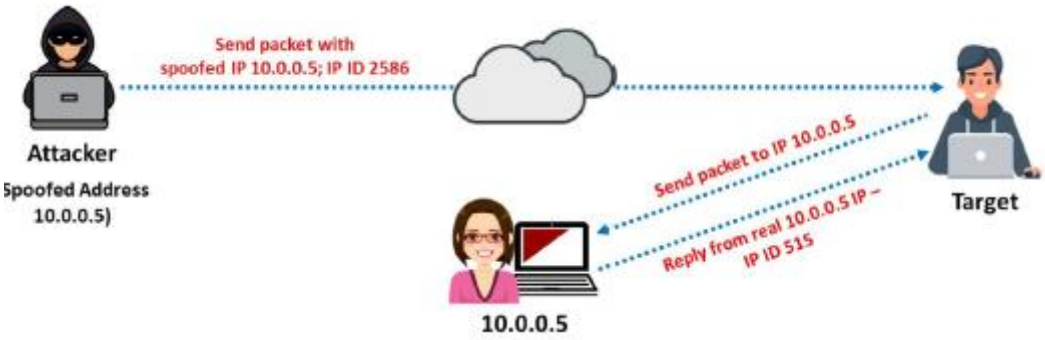


Jeśli odpowiedź pochodzi z innego protokołu, należy sprawdzić rzeczywistą liczbę przeskoków, aby wykryć sfałszowane pakiety. Odejmij wartość TTL w odpowiedzi od początkowej wartości TTL, aby określić liczbę przeskoków. Pakiet jest sfałszowanym pakietem, jeśli TTL odpowiedzi nie pasuje do TTL pakietu. Bardzo łatwo będzie przeprowadzić atak, jeśli atakujący zna liczbę przeskoków między źródłem a hostem. W takim przypadku wynik testu jest fałszywie ujemny. Ta technika jest skuteczna, gdy atakujący znajduje się w innej podsieci niż ofiara.

Uwaga: normalny ruch z jednego hosta może różnić się wartościami TTL w zależności od wzorców ruchu.

Numer identyfikacyjny IP

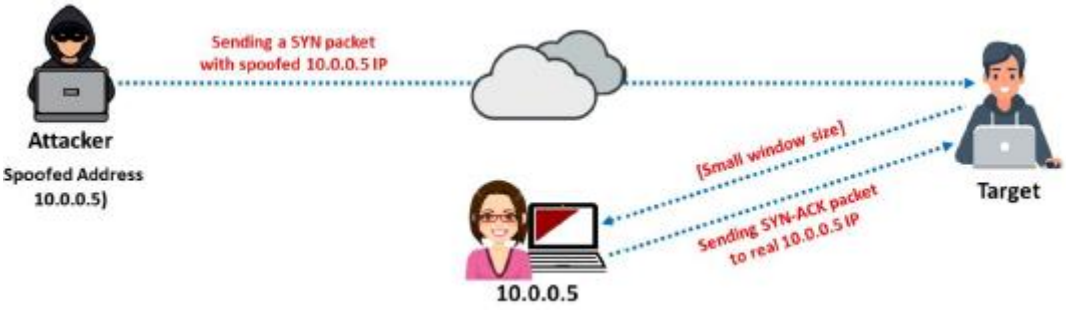
Użytkownicy mogą identyfikować sfałszowane pakiety, monitorując numer identyfikacyjny IP (IPID) w nagłówkach pakietów IP. IPID zwiększa się stopniowo za każdym razem, gdy system wysyła pakiet. Każdy pakiet IP w sieci ma unikalny numer „identyfikujący IP", który jest zwiększany o jeden przy każdej transmisji pakietu. Aby sprawdzić, czy pakiet jest sfałszowany, wyślij pakiet sondujący na źródłowy adres IP pakietu i zwróć uwagę na numer IPID w odpowiedzi. Wartość IPID w pakiecie odpowiedzi musi być zbliżona do wartości IPID pakietu sondującego, ale nieco większa. Adres źródłowy pakietu IP jest sfałszowany, jeśli IPID pakietu odpowiedzi nie jest zbliżony do adresu pakietu sondującego. Ta metoda jest skuteczna nawet wtedy, gdy atakujący i cel znajdują się w tej samej podsieci.



Metoda kontroli przepływu TCP

Dzięki swojemu algorytmowi protokół TCP może zoptymalizować kontrolę przepływu zarówno po stronie nadawcy, jak i odbiorcy. Algorytm realizuje kontrolę przepływu przy użyciu zasady przesuwanego okna. Użytkownik może kontrolować przepływ pakietów IP za pomocą pola rozmiaru okna w nagłówku TCP. To pole reprezentuje maksymalną ilość danych, które odbiorca może otrzymać, oraz maksymalną ilość danych, które nadawca może przesłać bez potwierdzenia. Zatem to pole pomaga kontrolować przepływ danych. Nadawca powinien przestać wysyłać dane, gdy rozmiar okna jest ustawiony na zero. W ogólnej kontroli przepływu nadawca powinien zaprzestać wysyłania danych

po wyczerpaniu początkowego rozmiaru okna. Atakujący, który nie zna pakietu ACK zawierającego informacje o rozmiarze okna, może kontynuować wysyłanie danych do ofiary. Jeśli ofiara otrzyma pakiety danych przekraczające rozmiar okna, są to sfałszowane pakiety. Aby zapewnić skuteczną kontrolę przepływu i wczesne wykrycie fałszowania, początkowy rozmiar okna musi być bardzo mały. Większość ataków polegających na fałszowaniu ma miejsce podczas uzgadniania, ponieważ utworzenie wielu fałszywych odpowiedzi z poprawnym numerem kolejnym jest trudne. Dlatego do uzgadniania należy zastosować metodę wykrywania sfałszowanych pakietów kontroli przepływu. Podczas uzgadniania TCP host wysyłający początkowy pakiet SYN czeka na SYN-ACK przed wysłaniem pakietu ACK. Aby sprawdzić, czy otrzymujesz żądanie SYN od prawdziwego klienta, czy sfałszowanego, ustaw SYN-ACK na zero. Jeśli nadawca wysyła ACK z jakimikolwiek danymi, oznacza to, że nadawca jest sfałszowany. Dzieje się tak dlatego, że gdy SYN-ACK jest ustawiony na zero, nadawca musi odpowiedzieć na niego tylko pakietem ACK, bez dodatkowych danych.



Atakujący wysyłający sfałszowane pakiety TCP nie otrzymają pakietów SYN-ACK celu. Osoby atakujące nie mogą reagować na zmiany rozmiaru okna przeciążenia. Gdy odbierany ruch jest kontynuowany po wyczerpaniu rozmiaru okna, najprawdopodobniej pakiety są sfałszowane.

Środki zaradcze związane z fałszowaniem adresów IP

Jak wspomniano wcześniej, fałszowanie adresów IP to technika stosowana przez hakerów w celu włamania się do sieci docelowej. Dlatego też, aby chronić sieć przed hakerami zewnętrznymi, w ustawieniach bezpieczeństwa sieci należy zastosować środki zaradcze polegające na fałszowaniu adresów IP. Niektóre środki zaradcze związane z fałszowaniem adresów IP, które można zastosować, są następujące:

• Unikaj relacji opartych na zaufaniu

Nie polegaj na uwierzytelnianiu opartym na protokole IP. Atakujący mogą podszywać się pod zaufanych hostów i wysyłać złośliwe pakiety. Jeśli te pakiety zostaną zaakceptowane przy założeniu, że są „czyste", ponieważ pochodzą od zaufanego hosta, system zainfekowany zostanie złośliwym kodem. Dlatego zaleca się testowanie wszystkich pakietów, nawet jeśli pochodzą od zaufanego hosta.

Tego problemu można uniknąć, wdrażając uwierzytelnianie hasłem wraz z zaufaniem uwierzytelniania oparteg na relacjach.

Używaj zapór ogniowych i mechanizmów filtrujących

Jak wspomniano powyżej, wszystkie pakiety przychodzące i wychodzące powinny być filtrowane, aby uniknąć ataków i utraty poufnych informacji. Zapora ogniowa może ograniczać przedostawanie się złośliwych pakietów do sieci prywatnej i zapobiegać poważnej utracie danych. Listy kontroli dostępu (ACL) mogą służyć do blokowania nieautoryzowanego dostępu. Jednak istnieje również możliwość ataku wewnętrznego. Atakujący z wewnątrz mogą wysyłać poufne informacje o firmie do konkurencji,

co może prowadzić do strat finansowych i innych problemów. Innym ryzykiem pakietów wychodzących jest to, że atakujący może pomyślnie zainstalować złośliwy program podsłuchowy działający w trybie ukrytym w sieci. Programy te zbierają i wysyłają wszystkie informacje o sieci do atakującego bez żadnego powiadomienia po odfiltrowaniu pakietów wychodzących. Dlatego skanowaniu pakietów wychodzących należy przypisać taką samą wagę jak pakietom przychodzącym.

Użyj losowych początkowych numerów sekwencji

Większość urządzeń wybiera swoje początkowe numery sekwencyjne (ISN) na podstawie liczników czasowych. Dzięki temu numery ISN są przewidywalne, ponieważ osoba atakująca może łatwo określić koncepcję generowania numeru ISN. Osoba atakująca może określić numer ISN następnego połączenia TCP, analizując numer ISN bieżącej sesji lub połączenia. Jeśli atakujący może przewidzieć numer ISN, może ustanowić złośliwe połączenie z serwerem i przechwycić ruch sieciowy. Aby uniknąć tego ryzyka, używaj losowych numerów ISN.

Filtrowanie wejściowe

Filtrowanie ruchu przychodzącego zapobiega przedostawaniu się sfałszowanego ruchu do Internetu. Jest stosowane w routerach, ponieważ zwiększa funkcjonalność routerów i blokuje sfałszowany ruch. Konfigurowanie i używanie list ACL odrzucających pakiety z adresem źródłowym spoza zdefiniowanego zakresu to jedna z metod implementacji filtrowania ruchu przychodzącego.

Filtrowanie wychodzące

Filtrowanie ruchu wychodzącego to praktyka, której celem jest zapobieganie fałszowaniu adresów IP poprzez blokowanie pakietów wychodzących z adresem źródłowym z zewnątrz.

Użyj szyfrowania

Aby zmaksymalizować bezpieczeństwo sieci, stosuj silne szyfrowanie dla całego ruchu przesyłanego na nośnikach transmisyjnych bez uwzględniania jego rodzaju i lokalizacji. Jest to najlepsza metoda zapobiegania atakom polegającym na fałszowaniu adresów IP. IPSec może być wykorzystany do drastycznego zmniejszenia ryzyka fałszowania adresów IP, ponieważ zapewnia uwierzytelnianie, integralność i poufność danych. Sesje szyfrowania powinny być włączone na routerze, aby zaufane hosty mogły bezpiecznie komunikować się z hostami lokalnymi. Atakujący mają tendencję do skupiania się na celach, które są łatwe do skompromitowania. Jeśli atakujący chce włamać się do zaszyfrowanej sieci, musi odszyfrować całą masę zaszyfrowanych pakietów, co jest trudnym zadaniem. W związku z tym osoba atakująca prawdopodobnie przejdzie dalej i spróbuje znaleźć inny cel, który można łatwo skompromitować lub po prostu przerwać próbę. Ponadto korzystaj z najnowszych algorytmów szyfrowania, które zapewniają silne bezpieczeństwo.

Środki zaradcze przeciw powodziom SYN

Środki zaradcze przeciwko atakom typu SYN flooding mogą również pomóc w uniknięciu ataków polegających na fałszowaniu adresów IP.

Inne środki zaradcze związane z fałszowaniem adresów IP

o Zwiększenie integralności i poufności stron internetowych poprzez migrację z IPv4 do IPv6 podczas tworzenia.

o Zaimplementuj mechanizmy uwierzytelniania za pomocą certyfikatów cyfrowych, takie jak weryfikacja domeny i certyfikatu uwierzytelniania dwukierunkowego.

o Korzystaj z bezpiecznej sieci VPN podczas uzyskiwania dostępu do wszelkiego rodzaju publicznych usług internetowych, takich jak bezpłatne Wi-Fi i hotspoty.

o Zastosuj urządzenia łagodzące specyficzne dla aplikacji, takie jak płuczki Behemoth do głębokiego poziomu badania pakietów z dużą prędkością prawie 100 milionów pakietów/s.

* Zaimplementuj dynamiczną zmianę adresu IPv6 za pomocą losowego generatora adresów, aby skrócić czas aktywnej luki w zabezpieczeniach.

* Skonfiguruj routery, aby wysyłały zakodowane informacje o pofragmentowanych pakietach wchodzących do sieci.

* Skonfiguruj routery, aby weryfikowały pakiety danych za pomocą ich podpisów, przechowując przychodzące skróty pakietów danych.

* Skonfiguruj routery, aby ukryć hosty intranetu przed siecią zewnętrzną, wprowadzając modyfikacje translacji adresów sieciowych (NAT).

* Skonfiguruj wewnętrzne przełączniki, aby wyświetlały statyczne adresy DHCP w celu filtrowania złośliwego, sfałszowanego ruchu.

Narzędzia do wykrywania i zapobiegania skanowaniu

Specjaliści ds. bezpieczeństwa używają różnych zaawansowanych narzędzi, takich jak ExtraHop i Splunk Enterprise Security, do wykrywania aktywnych sieci i prób skanowania portów zainicjowanych przez atakujących.

• Dodatkowy przeskok

ExtraHop zapewnia pełną widoczność, wykrywanie w czasie rzeczywistym i inteligentną reakcję na złośliwe skanowanie sieci. To narzędzie umożliwia specjalistom ds. bezpieczeństwa automatyczne wykrywanie i identyfikowanie każdego urządzenia i jego słabych punktów, w tym niezarządzanych urządzeń Internetu rzeczy (IoT) w sieci. Co więcej, to narzędzie pozwala specjalistom ds. bezpieczeństwa analizować wszystkie interakcje sieciowe w czasie rzeczywistym, w tym wszystkie transakcje w chmurze i ruch zaszyfrowany SSL/TLS, aby zapewnić pełny wgląd w obwód sieci. ExtraHop pomaga również w automatycznym wykrywaniu i klasyfikacji każdego urządzenia w sieci, za pomocą którego zespoły ds. bezpieczeństwa mogą analizować całą komunikację.

Poniżej wymieniono niektóre dodatkowe narzędzia do wykrywania i zapobiegania skanowaniu:

- Splunk Enterprise Security (https://www.splunk.com)

- Scanlogd (https://github.com)

- Vectra Cognito Detect (https://www.vectro.ai)

- IBM Security QRadar XDR (https://www.ibm.com)

- Cynet 360 (https://www.cynet.com)

Podsumowanie modułu

W tym module omówiono sposób, w jaki osoby atakujące określają aktywne hosty na podstawie zakresu adresów IP, wysyłając różne żądania skanowania ping do wielu hostów. Opisano również, w jaki sposób osoby atakujące wykonują różne techniki skanowania w celu określenia otwartych portów, usług, wersji usług itp. w systemie docelowym. Ponadto wyjaśniono, w jaki sposób osoby atakujące

wykonują przechwytywanie banerów lub pobieranie odcisków palców systemu operacyjnego w celu określenia systemu operacyjnego działającego w zdalnym systemie docelowym. Zilustrowano również różne techniki skanowania, które atakujący mogą zastosować, aby ominąć reguły IDS/zapory sieciowej i mechanizmy rejestrowania oraz jak zwykle ukryć się pod ruchem sieciowym. Ostatecznie zakończyła się szczegółową dyskusją na temat środków zaradczych skanowania sieci w celu obrony przed atakami skanowania sieci. W następnym module szczegółowo omówimy, w jaki sposób atakujący, a także etyczni hakerzy i pentesterzy wykonują wyliczanie w celu zebrania informacji o celu przed atakiem lub audytem.