Skanowanie portów

Autorzy: Jakub Sorys, Dorota Szczpanik IVFDS

STRESZCZENIE

W niniejszej pracy wyjaśniamy podstawowe pojęcia oraz techniki związane z zagadnieniem skanowania sieci, fingerprintingu i podobnych. Omawiamy poszczególne metody, ich wady i zalety, zakres stosowania oraz sposoby obrony przed nimi.

SPIS TREŚCI

1. SKANOWANIE

Skanowanie komputera lub hosta pozwala nam określić:
- czy dany komputer jest aktywny,
- określić listę usług na nim dostępnych,
- poznać rodzaj i wersję sytemu operacyjnego, na którym pracuje host,

Bardziej zaawansowane techniki pozwalają także na:
- poznanie topologii sieci w której pracuje host,
- poznanie ilości komputerów dostępnych w sieci,
- odszukanie istniejących zapór ogniowych.

Skanowanie jest pierwszym krokiem przeprowadzanym przez hakera, pozwalającym mu zebrać informacje potrzebne do przeprowadzenia udanego ataku na hosta/sieć.

Podstawowe techniki skanowania sieci:

- Ping Sweeps,
- Port Scans,
- Fingerprinting.

Ping Sweeps

Są to jedne z podstawowych technik. Dzięki nim można określić, czy dany host działa. Należą do nich:
- ICMP sweeps,
- Broadcast ICMP,
- TPC sweep,
- UDP Sweep.

ICMP sweeps - polega na wysłaniu pakietu ICMP Echo request, czyli zwykłego pinga. Brak odpowiedzi oznacza, że host jest niedostępny. Może też oznaczać, że odpowiedź na pakiety ICP echo request jest celowo zablokowana przez skanowany system na firewallach lub routerach.
Broadcast ICMP – jest to odmiana poprzedniej metody, polegająca na wysłaniu pinga na adres rozgłoszeniowy sieci. Można w ten sposób nawet ustalić liczbę komputerów w sieci. Systemy Microsoftu nie reagują na taki pakiet.
TCP sweep
Polega na wykorzystaniu pakietu TCP jako pakietu ping, korzystając z właściwości nawiązywania połączenia. TCP, jako protokół połączeniowy, wymaga zestawienia połączenia z

trójpoziomowym potwierdzeniem (three-way handshake) – wymieniane są 3 segmenty kontrolne.
Host nawiązujący połączenie wysyła segment z ustawionym bitem SYN (czyli numer sekwencji synchronizującej). Informuje to odbiorcę, że nadawca chce nawiązać połączenie oraz przekazuje numer sekwencji przesyłanych danych (czyli przekazuje numer pakietu, pozwala na ustawienie danych w kolejności).
Odbiorca odpowiada wysyłając segment z ustawionymi bitami SYN i ACK (bit potwierdzenia), potwierdzając odbiór i informując od jakiego numeru sekwencyjnego będzie odliczał wysłane przez siebie dane. Jeśli port nie jest aktywny, wysyła segment z flagą RESET.
Nadawca wysyła segment potwierdzający odbiór ACK, zawierający już pierwsze dane. Dzięki tej wymianie nadawca wie, że odbiorca jest gotowy do odbioru danych.
Po zakończeniu transmisji jest ona zrywana wymianą 3 segmentów z ustawionym bitem FIN.
Pakiety TCP Sweep są przeważnie wysyłane na porty: 21, 22, 23, 25, 80 – czyli typowe usługi, których pakiety nie są blokowane na zaporach. Ochrona przed takim skanowaniem jest prosta – wystarczy w firewallu podmienić adres źródłowy pakietów RESET. [3]

UDP Sweep
Skanowanie UDP korzysta z faktu, że wysłanie pakietu UDP na zamknięty port powoduje odpowiedź ICMP PORT UNREACHABLE. Jeśli port jest otwarty nie jest wysyłana żadna odpowiedź. Metoda ta jest stosowana do skanowania wysokich portów, na których nie ma usług UDP.
Wady metody:
Większość routerów blokuje pakiety UDP na innych portach niż 53 (DNS);
Firewalle też zwykle blokują pakiety UDP inne od zapytań DNS i łatwo je wykrywają;
Dużo systemów nie reaguje prawidłowo;
Limitowana ilość pakietów błędu ICMP – np. Linux wysyła nie częściej niż co 250 ms. [6]

Skanowanie portów.

Po zidentyfikowaniu, czy dany cel jest osiągalny należy określić jakie usługi są uruchomione na sprawdzanym hoscie i nasłuchują na połączenie. Na podstawie zidentyfikowanych portów można określić konfigurację różnych serwisów i wersje oprogramowania obsługującego daną usługę. Dzięki takiej wiedzy, znając słabe punkty oprogramowania można przeprowadzić skuteczny atak na host w celu zdobycia dostępu do systemu.

Techniki skanowania portów: [1]
TCP connect,
TCP SYN,
Techniki Stealth.

TCP connect polega na próbie zestawienia połączenia z danym portem za pomocą funkcji systemowej connect . Procedura nawiązywania połączenia przez protokół TCP została opisana powyżej. Jest to technika łatwa do wykrycia, zapory ogniowe skutecznie je blokują. Zaletą tych technik jest ich duża szybkość

Podobną metodą jest technika TCP SYN – czyli tzw. Technika półotwarcia. Procedura inicjowania połączenia nie jest wykonywana do końca. Po wysłaniu pakietu SYN odczytywana jest odpowiedz odbiorcy. Jeśli odebrano RESET to oznacza, że sprawdzany port jest zamknięty. Jeśli w odpowiedzi odebrano SYN/ACK to oznacza, że port jest otwarty. W takim przypadku nadawca wysyła pakiet RESET kończący natychmiast połączenie.
Częściowe połączenie przeważnie nie jest rejestrowane przez system, co jest niewątpliwie zaletą tej metody. Jest ona szybsza od TCP connect. Do jej wad zalicza się to, że większość zapór ogniowych odnotowuje je oraz blokuje.

Techniki Stealth

Stealth, czyli skanowanie ukryte. Ma na celu:
ominięcie reguł filtrów pakietów,
ukrycie faktu skanowania.

Do technik stealth zaliczmy: [1]
SYS/ACK;
FIN;
XMAS;
NULL.
RESET;
FTP Bounce Scanning;
Reverse Ident Scanning.

Wszystkie korzystają z faktu, że zamknięty port powinien odpowiedzieć pakietem RST na pakiety niezgodne z kolejnością zestawiania połączenia TCP

SYS/ACK
Polega na wysłaniu na dany port pakiety SYS/ACK, który jest drugim etapem zestawiania połączenia. Wartość ACK odnosi się do nieistniejącego połączenia. Jeśli badany host odbierze go na otwartym porcie (nasłuchującym) to zignoruje go, uznając za zniekształcony. Jeśli zostanie odebrany na porcie zamkniętym system powinien wysłać pakiet RST informujący, że żądany port jest zamknięty.

Większość zapór ogniowych blokuje pakiety SYN kierowane na zabronione porty. Ponadto istnieją programy pozwalające na wykrywanie tego typu skanowania.

FIN

Technika podobna do poprzedniej, tylko że w tym przypadku na badany port wysyłany jest pakiet z flagą FIN, kończącą połączenie. I tak jak poprzednio, otwarty port zignoruje pakiet a zamknięty odpowie RST.
Jest to metoda trudna do wykrycia jak i do zablokowania. Niektóre systemy są odporne na ten typ skanowania (np. Windows) [6]

XMAS

Christmas Tree, czyli choinka. Nazwa wzięła się stąd, że pakiet który jest wysyłany ma ustawione wszystkie flagi (bity kontrolne) i przez to jest nazywany pakietem choinkowym:
URG pilny wskaźnik;
ACK potwierdzenie;
PSH: funkcja przepychania;
RST: resetowanie połączenia;
SYN: synchronizacja numeru sekwencji;
FIN zakończenie pobierania danych.
Odpowiedź powinna być identyczna jak w przypadku SYS/ACK i FIN. Także Windows powinien udzielić prawidłowej odpowiedzi.
Podobną techniką jest wysłanie pakietu pustego, nie zawierającego żadnej flagi, czyli pakietu NULL. Host po odebraniu takiego pakietu na zamkniętym porcie, zgodnie ze specyfikacją TCP powinien odpowiedzieć pakietem RST. Jednak nie wszystkie systemy mają prawidłową implementację TCP/IP i np. Windows, Cisco odpowiedzą RST nawet na otwartym porcie. [1]

RESET

Celem tej metody jest sprawdzenie topologii sieci, określenie hostów pracujących w danej podsieci. Router, po odebraniu pakietu przeznaczonego dla nieistniejącego celu wysyła w odpowiedzi pakiet ICMP HOST UNREACHABLE lub TIME EXCEEDED. Jeśli zostanie użyty typowy pakiet, np. ACK czy ICMP ECHO REQUEST to zostanie to odnotowane. Jeśli natomiast zostanie użyty pakiet RST z dowolnym numerem ACK to nie zostanie on odnotowany, a system wyśle odpowiedni komunikat.

FTP Bounce Scanning

Technika ta wykorzystuje typowy serwer FTP jako serwer proxy, ponieważ serwer FTP może wysyłać dane do hosta o innym adresie niż źródłowy. Polega na użyciu komendy PORT, precyzującej port docelowy. Po wydaniu polecenia LIST FTP wynik zostanie przesłany do klienta.

Komunikat 150 lub 226 oznacza, że transfer zakończono powodzeniem, czyli że podany port jest otwarty. Natomiast komunikat 425 oznacza, że port jest zamknięty.
Do zalet tej metody należą wysoka skuteczność i ukrycie adresu atakującego. Niestety, jest to technika wolna. Poza tym nie wszystkie serwery FTP mają aktywna funkcję proxy.

Reverse Ident Scanning

Dla napastnika istotną informacją oprócz listy otwartych portów jest także określenie uprawnień z jakimi dana usługa pracuje. Służy do tego protokół ident. Po połączeniu z daną usługą wysyła się zapytanie do ident o identyfikację połączenia. W odpowiedzi host wysyła nazwę użytkownika z uprawnieniami którego pracuje dana usługa.

2. Fingerprinting

Fingerprinting oznacza metody określania systemu operacyjnego. Ponieważ zabezpieczenia i luki w nich zależą od typu systemu pod jakim pracuje dany host określenie OS jest ważną informacją dla włamywacza.

Do technik fingerprintingu zaliczmy: [1]
Banner grabbing;
Analiza stosu TCP/IP;
Badanie opcji TCP;
SYN Flood Resistance.

Banner Grabbing

Jest to jedna z najprostszych metod. Większość usług wyświetla banery po połączeniu się z nimi. Bardzo często zawierają informację o zainstalowanym systemie i wersji demona obsługującego usługę. Najprościej odczytać baner za pomocą zwykłego telnetu.
Nie jest to pewna metoda, ponieważ baner może zostać usunięty lub sfałszowany przez administratora systemu.

Analiza stosu TCP/IP [1]

Bardzo wiarygodna metoda, ponieważ każda implementacja TCP/IP jest inna i różne systemy różnie reagują na błędne stany, szczególnie nie ujęte w specyfikacji.
Analiza stosu może być pasywna i aktywna. Aktywna jest wtedy, gdy jest sprawdzana reakcja systemu na spreparowane odpowiednio pakiety. Pasywny, gdy sprawdza się zwykłą aktywność danego systemu.
Do analizy stosu należy np. technika skanowania portów FIN. Niektóre nieprawidłowe implementacje TCP na wysłanie pakietu FIN na otwarty port reagują pakietem RST (prawidłowo powinien być brak odpowiedzi). W ten sposób zachowują się: Windows, Cisco, BSDI, HP-UX, MVS, IRIX.

Bogus Flag Probe Test polega na wysłaniu pakietu z nieistniejącą flagą i badaniu odpowiedzi systemu. Przeważnie jest to wartość 64 lub 128 w pakiecie SYN. Niektóre systemy na taki pakiet reagują wysłaniem RST. Linux odsyła pakiet z tą flagą z powrotem do nadawcy. Można dzięki temu wstępnie zidentyfikować system.

ISN Sampling

Jest to metoda znajdywania systemu operacyjnego hosta na podstawie zależności w generowaniu numerów sekwencyjnych ISN (Initial Sequence Number). Są 4 grupy algorytmów generowania ISN:
tradycyjna, oparta na cyklu 64 tysięcy, wykorzystywana w starszych implementacjach UNIX;
pseudolosowe generatory, używane w: FreeBSD, Digital-Ux, IRIX, nowszych dystrybucjach Solarisa;
losowe , spotykane w Linuxie; zależne od kwantu czasu wysłania pakietu to MS Windows;
stałe – zawsze ten sam ISN.

Inna technika opiera się na obecności bitu DF(nie fragmentuj) w odebranym pakiecie. Niektóre systemy operacyjne wysyłają pakiety z ustawionym bitem DF w celu zwiększenia wydajności i dobrania parametrów połączenia.

Testowanie inicjującego rozmiaru okna TCP w odebranym pakiecie także dużo mówi o systemie, ponieważ różne systemy przyjmują różne wartości. [2]

Inną metodą określania systemu operacyjnego jest testowanie wartości pakietu ACK. Różne systemy różnie reagują na błędne sytuacje. Na przykład po odebraniu pakietów z fagami FIN, PSH, URG na zamknięty port TCP niektóre implementacje odsyłają ACK z identycznym ISN, niektóre drukarki odsyłają ACK z ISN zwiększonym o jeden. Windows zachowuje się tu dość nieprzewidywalnie, czasem odsyła ISN identyczny, czasem zwiększony o jeden, czasem jest to zupełnie losowa wartość.

Badanie opcji TCP

Nie są to opcje obowiązkowe i nie wszystkie systemy mają je zaimplementowane. Czasem też mają je nieprawidłowo zaimplementowane. Jeśli opcje są dostępne na danym hoscie to po odebraniu pakietu z aktywnymi opcjami wysyła komunikat o ich obsłudze. Można przeprowadzić cały test tylko za pomocą jednego pakietu.

SYN Flood Resistance

Bardzo brutalna i rzadko stosowana metoda. Bada odporność hosta na zalew pakietami SYN. Jest to metoda łatwa do wykrycia. Wystarczy sprawdzić liczbę połączeń z jednego adresu IP i tego samego portu. Linux jest w stanie obsłużyć 8 takich żądań.

Literatura:

1. Sebastian Sawicki „Techniki skanowania sieci” NetWorld luty 2002
2. http://project.honeynet.org/papers/finger/
3. http://www.linuxpub.pl/man/sif/
4. http://www.networld.pl/artykuly/9927.html
5. http://www.networld.pl/artykuly/9714.html
6. http://www.auditmypc.com/freescan/readingroom/port_scanning.asp