SKENIRANJE PORTOVA

Skener portova je program konstruisan da ispita Server ili Host (domaćina) za otvorene portove. Često je korišćen od strane Mrežnih administratora kako bi proverili bezbednost njihovih mreža i preko napadača identifikovali upaljene servise na hostu.

Skeniranje portova (*port scan* ili *portscan*) se moze definisati kao napad koji hostu šalje zahteve klijenata na niz adresa portova servera sa ciljem pronalaženja aktivnog porta i ugrožavanjem poznate slabosti tog servisa, iako većina korišćenja tog programa nisu napadi vec jednostavna ispitivanja dostupnih servisa na udaljenom računaru.

Portsweep ili **Pretraživanje portova** se koristi kako bi se skeniralo više hostova za određeni otvoreni port. Kasnije se najčesce koristi za traženje određenog servisa, na primer, SQL-baziran računarski crv može pretraživati portove za kompatabilnim hostom na TCP portu 1433.

TCP/IP - osnovno znanje

Dizajn i rad Interneta je baziran na Internet protokolima, često nazivanim TCP/IP. U ovom sistemu, hostovi i usluge hostova su označene korišćenjem dve komponente: adrese i broja porta. Postoji 65536 različitih i upotrebljivih brjeva porta. Većina servisa koristi ograničen opseg brojeva.

Neki skeneri portova mogu skenirati samo najučestalije brojeve porta, ili portove najčešće povezane sa ranjivim servisima na datom hostu.

Rezultat skeniranja portova je najčešće genaralizovan u jednu od tri kategorije:

1. *Open (Otvorena)* ili *Accepted (Prihvaćena)*: Host šalje odgovor koji ukazuje da je servis kompatabilan na portu.
2. *Closed (Zatvoren)* ili *Denied (Odbijen)* ili *Not listening (Ne sluša)*: Host šalje odgovor koji ukazuje da će konekcija na portu biti odbijena.
3. *Filtered (Filtriran)*, *Dropped (Pao)* ili *Blocked (Blokiran)*: Nije dobijen odgovor od hosta.

Otvoreni portovi prikazuju dve slabe tačke zbog kojih Administratori moraju biti oprezni:

1. Zabrinutost za bezbednost i stabilnost povezana sa programom odgovornim za dostavljanje servisa - Otvoreni portovi.
2. Zabrinutost za bezbednost i stabilnost povezana sa operativnim sistemom koji je aktivan na hostu - Otvoreni ili zatvoreni portovi.

Filtrirani portovi ne teže da prikazuju ranjivost.

Pretpostavke skeniranja portova

Svi oblici skeniranja portova oslanjaju se na pretpostavci da je označeni host kompatibilan sa RFC793 - Transmission Control Protocol (Protokolom kontrole slanja). Iako je tako u većini slučajeva, postoji šansa da host može poslati nazad čudne pakete ili čak generisati lažno pozitivne kada je TCP/IP stek hosta ne-RFC-kompatabilan ili je promenjen. Ovo posebno važi za manje uobičajene tehnike skeniranja koje su zavisne od operativnih sistema (FIN skeniranje , na primer). TCP/IP stack fingerprinting metoda se takođe oslanja na ovakve tipove različitih mrežnih reakcija od specifičnog stimulansa da pogodi tip operativnog sistema koji je aktivan na hostu.

Tipovi skeniranja portova

TCP skeniranje

Najjednostavniji skeneri portova koriste funkcije mrežnog operatvnog sistema i generalno je sledeća opcija da se nastavi kada SYN nije izvodjliva opcija (opisano u nastavku). Nmap naziva ovaj metod povezivanje connect scan (povezivanje skeniranja), nazvan po Unix povezivanju sistemskog poziva. Ako je port otvoren, operativni sistem završava TCP trostruko rukovanje, i skener portova odmah zatvara konekciju kako bi izbegao izvršavanje Denial-of-service napada (Uskraćivanje servisa). Inače kod greške se vraća. Ovaj režim skeniranja ima prednost da korisnik ne zahteva posebne privilegije. Međutim, korišćenjem funkcija operativnog sistema mreže sprečava se nizak nivo kontrole, pa je ovaj tip skeniranja ređi. Ovaj metod je "bučniji", posebno ako je "*portsweep*": servisi mogu da zabeleže IP adresu pošiljaoca i sistem detekcije upada može pokrenuti alarm.

SYN skeniranje

SYN skeniranje je još jedan oblik TCP skeniranja. Radije nego da koristi funkcije operativnog sistema mreže, skener portova generiše neobradjene pakete sam i traga za odgovorima. Ovaj tip skeniranja je takođe nazvan kao "half-open (polu otvoreno) skeniranje", zato sto zapravo nikad ne otvara celu TCP konekciju. Skener portova generiše SYN paket. Ako je označeni port otvoren, on ce odgovoriti sa SYN-ACK paketom. Skener host odgovara sa RST paketom, zatvarajući konekciju pre nego što je rukovanje završeno. Ako je port zatvoren nefiltriran, cilj ce odmah odgovoriti sa RST paketom.

Korišćenje sirove mreže ima nekoliko prednosti, davajući skeneru potpunu kontrolu nad poslatim paketima kao i vremenskim rokom za odgovore i omogućava detaljne izveštaje odgovora. SYN skeniranje ima tu prednost da pojedini servisi nikada ne prihvataju konekciju. Međutim, RST tokom rukovanja može uzrokovati probleme za neke mrežne stekove, posebno kod jednostavnih uređaja kao sto su štampači. Ne postoje uverljivi argumenti bilo kako.

UDP skeniranje

UDP skeniranje je takođe moguće, iako postoje tehnički izazovi. UDP (User Datagram Protocol) je protokol bez konekcije tako da ne postoji ekvivalent za TCP SYN paket. Međutim, ako se šalje UDP paket na port koji nije otvoren, sistem ce odgovoriti sa ICMP (Internet Control Message Protocol) porukom nedostupnog porta. Većina UDP skenera portova koristi ovaj metod skeniranja i koriste odsustvo odgovora da zaključe da je port otvoren. Međutim, ako je blokiran od strane Firewall-a (Zaštitnog zida), ovaj metod ce lažno izveštavati da je port otvoren. Ako je poruka nedostupnog porta blokirana, svi portovi će se pojaviti otvoreni. Ova metoda takođe utiče na ICMP ograničavanje stopa.

Alternativni pristup je da pošalje UDP pakete određene aplikacije, nadajući se da će generisati odgovor aplikacionog sloja. Na primer, slanjem DNS upita portu 53 će rezultovati odgovorom, ako je DNS server prisutan. Ova metoda je mnogo pouzdanija u identifikovanju otvorenih portova. Međutim, ona je ograničena na skeniranje portova sa kojih je specificni probni paket aplikacije dostupan. Neke alatke (npr. nmap) generalno imaju probe za manje od 20 UDP servisa, dok neke komercijalne alatke (npr. Nessus) imaju cak 70. U nekim slučajevima, servisi mogu slušati port, ali nije konfigurisan da odgovori na određeni probni paket.

Da bi se izborio sa različitim ograničenjima svakog pristupa, neki skeneri nude hibridni metod. Na primer, koristeci nmap sa -sUV opcijom počeće koristiti ICMP metod nedostupnog porta, praveći sve portove "zatvorenim" ili "otvorenim|filtriranim". Otvoreni|filtrirani portovi su probni za odgovor aplikacije i oznaceni kao "otvoreni" ako je bar jedan primljen.

ACK skeniranje

ACK skeniranje je jedan od više jedinstvenih tipova skeniranja, jer on ne utvrđuje tačno da li je port otvoren ili zatvoren, nego da li je port filtriran ili ne. Ovo je posebno dobro kada pokušava da ispita postojanje zaštitnog zida i njegovih pravila. Jednostavnim filtriranjem paketa će omogućiti uspostavljanje veze , dok kod prisustva kompleksnijeg firewall-a možda neće.

Skeniranje prozora

Retko se koristi zbog svoje zastarele prirode, skeniranje prozora je prilično neupouzdano u određivanju da li je port otvoren ili zatvoren. On generiše isti paket kao ACK skeniranje, ali proverava da li je polje prozora paketa promenjeno. Kada paket stigne na odredište, mana u dizajnu pokušava da napravi prozor veličine paketa ako je port otvoren, obeležavajuci polje prozora paketa sa 1 pre nego sto se vraća pošiljaocu. Korišćenjem ove tehnike skeniranja sa sistemima koji ne podržavaju ovu primenu, vracaju 0 za polje prozora, obeležavanjem otvorenih portova kao zatvorene.

FIN skeniranje

Pošto SYN skeniranja nisu dovoljno prikrivena, firewall-ovi skeniraju blokirane pakete u vidu SYN paketa. FIN paketi mogu da prođu firewall bez promene svoje svrhe. Zatvoreni portovi odgovaraju FIN paketu sa odgovarajućim RST paketom, dok otvoreni portovi ignorišu paket "na ruci". Ovo je tipično ponašanje zbog prirode TCP, i na neki način neizbežan pad.

Ostali tipovi skeniranja

Postoje jos neki neuobičajeni tipovi skeniranja. Oni imaju različita ograničenja i nisu u širokoj upotrebi. Nmap podržava većinu njih.

- X-mas i Null Skeniranje - su slični sa FIN skeniranjem
    - X-mas šalje pakete sa FIN, URG i PUSH oznakama uključenim kao novogodisnja jelka
    - Null šalje paket bez TCP oznaka na sebi
- Protokol skeniranje - određuje šta je od IP nivoa protokola (TCP, UDP, GRE (Generic Routing Encapsulation), itd.) omugućeno.
- Proksi skeniranje - proksi (SOCKS ili HTTP) su korišćeni za izvršavanje skeniranja. Meta ce videti proksijevu IP adresu kao izvor. Ovo takođe moze biti učinjeno korišćenjem FTP (File Transfer Protocol) servera
- Idle skeniranje - jos jedan način skeniranja bez otkrivanja nečije IP adrese, iskorišćavajuci predvidljivu IP ID manu
- Cat skeniranje - Provera port u potrazi za pogrešnim paketima
- ICMP (Internet Control Message Protocol) skeniranje - odredjuje da li host reaguje na ICMP zahteve, kao sto su eho (ping), netmask, itd.

Filtriranje portova preko ISP (internet servis provajdera)

Mnogi internet provajderi ograničavaju mogućnosti svojih korisnika da skeniraju portove van svoje kućne mreže. Ovo je uglavnom pokriveno u uslovima usluge ili u prihvatljivom postupku korišćenja koji korisnik mora da prihvati. Neki internet provajderi sprovode filtere ili transparentne proksije koji sprečavaju odlazne servisne zahteve pojedinim portovima. Na primer, ako jedan internet provajder obezbeđuje transparentni HTTP proxy na portu 80, skeniranje portova bilo koje adrese će pokazati da je port 80 otvoren, bez obriza na trenutnu konfiguraciju ciljnog hosta.

Etika

Informacije koje je prikupilo skeniranje portova ima mnoge koristi uključujući inventor mreže i verifikaciju bezbednosti mreže. Skeniranje portova može, medjutim, biti korišćeno i da ugrozi bezbednost. Mnogi korisnici se oslanjaju na skeniranje portova za traženje otvorenih portova i slanje posebnih obrazaca u pokušaju da aktiviraju stanje poznato kao "butterfly overflow". Takvo ponašanje može da ugrozi bezbednost mreže i računare u okviru nje, što dovodi do gubitka ili izlaganja informacija i mogućnosti za rad.

Nivo pretnje koju izaziva skeniranje portova moze mnogo da varira u zavisnosti od načina koji je korišćen za skeniranje, vrste porta koji je skeniran, njegovog broja, vrednosti ciljnog hosta i administratora koji prati host. Ali, skeniranje portova se uglavnom vidi kao prvi korak u napadu, stoga se ozbiljno uzima u obzir jer moze da otkrije mnogo privatnih informacija o hostu. Uprkos ovome, verovatnoća da će skeniranje porta biti praćena napadom je mala. Verovatnoća napada je mnogo veća kada je skeniranje porta povezano sa skeniranjem ranjivosti.

Pravne posledice

Zbog otvorene i necentralizovane arhitekture interneta, zakonodavci su se borili od njegovog postanka da definišu zakonske granice koje omogućavaju efikasno krivično gonjenje kriminalaca. Slučajevi koji uključuju skeniranje portova su primer teškoća sudskih kršenja. Iako su ovakvi slučajevi retki, većinu vremena pravni proces uključuje dokazivanje da je namera za upad i neovlašćeni pristup postojala, a ne samo skeniranje portova.

- U junu 2003, Izraelac, Avi Mizrahi, je optužen od strane izraelske policije za pokušaj neovlašćenog pristupa računarskom materijalu. On je skenirao portove sajta Mossad. Oslobođen je svih optuzbi 29. Februara 2004. Sudija je rekao da ovakve postupke ne treba obeshrabrivati kada se izvode na pozitivan način.
- 17-godišnji Finac je optužen za pokušaj upada u računar velike finske banke. 9. Aprila 2003. je osuđen od strane vrhovnog suda i naređeno mu je da plati 12000 dolara, za troškove forenzičke analize od strane banke. U 1998, on je skenirao portove mrezže banke, u pokušaju da pristupi zatvorenoj mreži, ali nije uspeo u tom pokusaju.
- U decembru 1999, Scott Moulton je uhapšen od strane FBI i optužen za pokušaj upada u računar pod Georgia's Computer Systems Protection Act. U ovo vreme , njegova IT kompanija je imala trenutni ugovor sa Cherokee, okrugom drzave Georgia da održi i unapredi 911 centar za bezbednost. On je izveo nekoliko skeniranja portova na serverima u Cherokee okrugu da bi proverio njihovu bezbednost i konačno je pronašao jos jedan veb server druge IT kompanije, izazivajući svađu, što je zavrsilo na sudu. Oslobođen je 2000, sudija je rekao da nije doslo do oštećenja u integritetu i dostupnosti mreže.

U 2006, Britanski parlament je izglasao amandman na račun Computer Misuse Act 1990 koji dokazuje krivicu osobe koja "napravi, izmeni, snabdeva ili predloži da snabdeva bilo koji članak za koji se zna da je dizajniran i prilagođen za upotrebu u toku ili u vezi sa prekrsajem iz stava 1 ili 3 (CMA)". Ipak, oblast uticaja ovog amandmana je nejasna, i široko kritikovana od strane bezbednosnih stručnjaka.

Nemačka ima sličan zakon, i Savet EU je izdao saopštenje za javnost u kojoj se navodi da planiraju naprave jedan slični, mada precizniji.