Nmap 4.0

 Nedavno je Fyodor izdao novu inačicu ovog inače nezamjenjivog alata za sve sistem-administratore, mrežare, sigurnosne entuzijaste i ine. Prisjetimo se, ovo je Nmap **[1]**-ova osma godina postojanja - te se tijekom vremena razvio u glavnu aplikaciju (za Windows OS, te Unixoide i Linux) za mrežno mapiranje, odnosno identifikaciju otvorenih portova na pojedinoj IP adresi u kakvoj mreži. To je alat kako za sistemce - tako i za crackere i hackere diljem svijeta.

Nmap iskusnom pojedincu omogućava niz načina pregleda dotičnih portova i cijelog računala kroz mrežu - čak omogućavajući nevidljivost te lažiranje izvorišne adrese. U osnovi, Nmap koristi IP pakete sa posebnim sadržajem i omogućava:

- otkrivanje aktivnih računala: detekcija koja su računala upaljena a koja nisu,
- skeniranje portova: koji su TCP i UDP portovi otvoreni, a koji nisu,
- detekcija verzije mrežnih servisa: koje su aplikacije (odnosno tipovi aplikacija) aktivne i koja im je radna verzija,
- detekciju verzije operacijskog sustava odnosno tipa uređaja.

U svojoj 4.0 inačici Nmap je doživio niz velikih promjena i poboljšanja. Uz poboljšanu dokumentaciju **[2]**, izrazito se mnogo radilo na doradivanju detekcije verzija softvera i operacijskih sustava - te je ugrađena baza porasla u svojoj veličini čak triput (na ukupnih 3153 potpisa za čak 381 protokol). Nmap sada standardno u komandnoj liniji interaktivno skenira, što će reći da očitava tipkovnicu: primjerice, tipka v uključuje i isključuje detaljni pregled događaja za vrijeme rada, a tipka p prikazuje tok paketa, odnosno ujedno gasi prikaz toka paketa. Sam dio aplikacije "ispod haube" je znatno promijenjen, te sada aplikacija radi znatno brže, koristeći osjetno manje radne memorije nego prije. U grupnom skeniranju sada se standardno skenira više računala uporedo, kao i više portova na pojedinom računalu odjednom.

Za one koji koriste Nmap na lokalnoj Ethernet mreži, isti sada podržava novi tip skeniranja (koji se automatski uključuje ako je zadovoljen preduvjet da se skenira lokalna mreža), tzv. ARP scan. U takvom slučaju Nmap osluškuje ARP odgovore, pa više nije potrebno koristiti ICMP echo prema računalima. Interesantna je i pojava nove --badsum opcije koja omogućava slanje IP paketa sa krivim TCP odnosno UDP zaštitnim sumama. U slučaju da računalo odgovara na takve pakete, riječ je o vatrozidu koji uopće nije provjeravao sume, već je prema odgovarajućim pravilima odlučio poduzeti nekakve akcije. Jasno, obična računala takve pakete uvijek odbacuju, zbog detektirane greške u njima. Od ostalih promjena, spomenimo mogućnost slanja čistih Ethernet okvira (naravno moguće je i lažirati izvornu MAC adresu) s IP paketima, naspram dosadašnjeg slanja paketa kroz "sirove" portove. Osim već spomenutog povećanja potpisa za različite protokole i servise, povećala se znatno i baza potpisa operacijskih sustava za udaljeno prepoznavanje istih (na 1684 potpisa). Ima naravno još niz manjih poboljšanja i dorada, umjesto trivijalnog i beskorisnog nabrajanja svih mogućih izmjena, radije preporučamo čitanje prilično osvježene dokumentacije **[2]** i pripadnih manual **[3]** stranica.

Pokažimo stoga radije na nekoliko primjera tipičnu upotrebu Nmap naredbe. Primijetite da je Nmap inače standardni konzolski program koji za veliku većinu tipova skeniranja nužno zahtijeva root ovlasti.

TCP SYN skeniranje

Koristi se samo za identifikaciju TCP-baziranih servisa na udaljenom računalu, a specificira se parametrom -sS. Tijekom procesa prikupljanja informacija ne ostvaruje se potpuno trostepeno rukovanje, već se veza prekida čim se ustvrdi otvoreni port. Ovakav tip skeniranja podrazumijeva se ako se Nmap koristi pod administratorskim ovlastima. Primjer korištenja: skeniramo sva računala u mreži 192.168.0.0/24 s detaljnim ispisom informacija (-v parametar) i još namjerno ugasimo provjeru jesu li sva računala iz tog prostora živa (dakle gasimo ping provjeru s -P0) i to izrazito agresivnom brzinom (-T Insane) što obično dovodi do vrlo povišenog mrežnog prometa na mreži, kao i mogućih grešaka u rezultatima (nepotpunih rezultata):

nmap -P0 -T Insane -sS -v "192.168.0.*"

TCP connect() skeniranje

Ovakav tip skeniranja koristi se uglavnom samo kad korisnik nema administratorske ovlasti, a specificiramo ga parametrom -sT. Pri skeniranju se ostvaruju potpune veze, što je nezgodno budući da će sama aplikacija koja se pregledava na pojedinom portu obično zabilježiti pokušaj spajanja. U primjeru ćemo nasumično (--randomize_hosts parametar), a ne sekvencijalno skenirati cijelu klasu računala koristeći "puno spajanje":

nmap --randomize_hosts -sT 192.168.0.0/24

Skriveno skeniranje

Riječ je o nekoliko podtipova skeniranja:

- FIN skeniranju: koristi se -sF,
- Xmas Tree skeniranju: koristi se -sX,
- Null skeniranju: koristi se -sN.

Ovi tipovi skeniranja koriste posebno generirane pakete (obično šalju samo jedan paket s namjerno manipuliranim zastavicama) koji uzrokuju obično paket s RST zastavicom kao odgovor u slučaju da je port zatvoren - odnosno nikakav odgovor u slučaju da na njemu postoji aktivni servis. Nažalost, u ovakvim je metodama nemoguće razlikovati stanje između otvorenog porta i namjerno odbačenih paketa koristeći vatrozid. Primijetite, ovi tipovi pregleda omogućavaju identifikaciju samo TCP portova i nužno zahtijevaju administratorske ovlasti.

Ping skeniranje

Ovo je vjerojatno najjednostavniji tip pregleda (samo dva razmijenjena paketa po pojedinom računalu) koji ne služi identifikaciji portova, već isključivo pronalaženju aktivnih računala ili uređaja po pojedinim IP adresama. Pri pregledu se koristi ICMP echo upit i odgovor, a takav tip skeniranja omogućujemo parametrom -sP:

nmap -sP -v 192.168.0.0/24

Skeniranje verzija

Riječ je o pregledu koji pokušava ustanoviti verzije aplikacija na pojedinim računalima i pripadnim portovima. Ovaj tip skeniranja omogućava se parametrom -sV, a prikazat ćemo u primjeru skeniranje samo jednog računala i pri tome ćemo pregledati samo portove koje se nalaze između 20 i 30, uključno 139 i sve iznad 60000:

nmap -sV -p 20-30,139,60000- -v 192.168.0.10

Postoji još jedna varijanta ovog testa, a to je -A. Naime, dotični napredni tip testiranja uključuje i test verzija -sV kao i identifikaciju udaljenog operacijskog sustava -O. Jasno, svaki od tih parametara moguće je koristiti i odvojeno, ne mora se podrazumijevati skupno korištenje. U primjeru, pokažimo napredno testiranje verzija na već spomenutom računalu:

nmap -A -v 192.168.0.10

Ovaj tip testiranja generira vrlo mnogo prometa po mreži. Također, ispravna detekcija se može omesti korištenjem naprednijih tehnika filtriranja paketa, a pri tome udaljeni servis niti ne mora imati zabilježen potpis u Nmap bazi.

UDP skeniranje

Ovaj tip skeniranja relativno je jednostavan budući da nema potrebe za rukovanjima - paketi se šalju i primaju, odnosno odbacuju. Ovaj tip pregleda se koristi parametrom -sU. Problem kod ovakvog tipa skeniranja je da većina TCP/IP stogova ima implementiranu kontrolu brzine primanja/slanja ICMP poruka, pa će poruke o neaktivnim portovima uzrokovati uglavnom znatna usporenja. Primjer korištenja je sljedeći:

nmap -sU -v 192.168.0.10

Ostali tipovi skeniranja

Postoji još niz relativno naprednih tipova pregleda koji zahtijevaju nešto višu razinu poznavanja TCP/IP protokola, implementacije mrežnih stogova i implikacija koje donose otkrivene informacije. Takva skeniranja su primjerice sljedeća:

- skeniranje IP protokola -sO koje utvrđuje postojanje različitih dodatnih IP protokola koji su možda u upotrebi na udaljenom računalu (EGP, IGP, itd),
- ACK skeniranje -sA koje se koristi prvenstveno za utvrđivanje da li se određeni paketi odnosno portovi filtriraju ili ne,
- skeniranje pomičnim prozorima -sW koristi se za istu namjenu kao i ACK skeniranje, ali daje i informacije da li je nešto aktivno na portu - no nažalost ovaj tip skeniranja radi na sve manjem broju uređaja i računala,
- RPC skeniranje -sR koje služi pregledu i identifikaciji registriranih RPC servisa,
- IdleScan -sI koje koristi tzv. zombi računala za udaljeno skeniranje koje se pojavljuje kao da dolazi od zombi računala,
- FTP bounce skeniranje -b koje omogućava korištenje nekog FTP servisa na nekom trećem računalu kao zombija za skeniranje - no ovaj potonji tip radi na sve manjem broju FTP poslužitelja.

uto, 2006-04-11 16:11 - Uredništvo**Vijesti:** Sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/2

Links
[1] http://nmap.org/
[2] http://nmap.org/docs.html
[3] http://nmap.org/book/man.html
[4] https://sysportal.carnet.hr/taxonomy/term/13