Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva
ZESOI

IP SPOOFING

Seminarski rad iz predmeta: Sustavi za praćenje i vođenje procesa

Maja Briški
0036397142

Zagreb, lipanj 2006.

Sadržaj:

1. Uvod

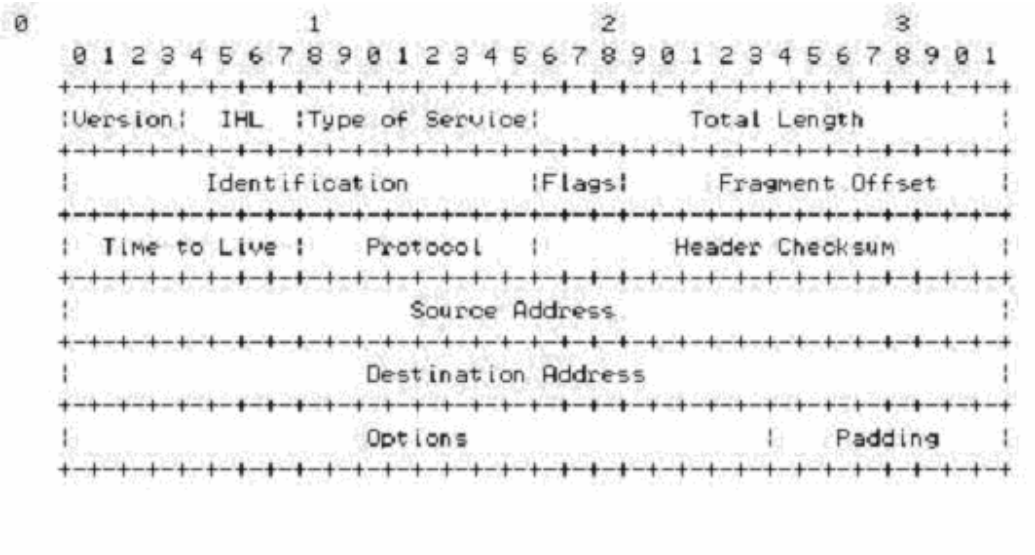
IP spoofing (Internet protocol address spoofing) je pokušaj neautoriziranog entiteta da dobije autoriziran pristup sustavu pretvarajući se da je autoriziran korisnik. Termin se odnosi i na krivotvorenje zaglavlja, ubacivanje lažnog sadržaja u *e-mail* ili *netnews* zaglavlja. Ovo je česta tehnika kojom se služe *spam*-eri s namjerom da prekriju izvor svojih poruka kako bi izbjegli njihovo praćenje.

Inicijalno se koncept *IP spoofing*-a razmatrao u akademskim krugovima u 1980-tim godinama. Iako već poznat neko vrijeme, bio je samo teorija dok nije Robert Morris, čiji je sin napisao prvog internet crva, otkrio slabost u osiguranju TCP protokola poznatu kao slijedno predviđanje (sequence prediction). Steven Bellovin u potpunosti je obradio probleme s TCP/IP protokolom u „Security Problems in the TCP/IP Protocol Suite“. *IP spoofing* još uvijek je moguće izvesti i treba ga prijaviti svim sigurnosnim administratorima.

2. Potrebne informacije

2.1. IP (Internet Protocol)

IP je mrežni protokol koji je implementiran na trećem sloju OSI modela (mrežni). Bespojnog je tipa što znači da se ne vodi računa o tome da li su paketi koji se šalju uopće stigli na odredište.

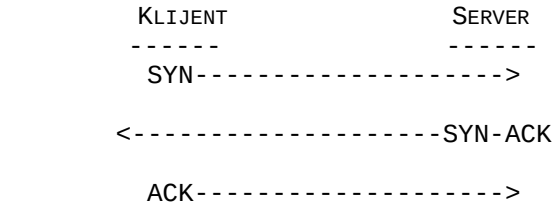


Slika 1. Zaglavlje IP paketa

Ako pogledamo zaglavlje IP paketa (slika 1.), možemo vidjeti da prvih 12B (ili gornja 3 reda zaglavlja) sadrži razne informacije o paketu. Sljedećih 8B (sljedeća dva reda) sadrže izvorišnu i odredišnu IP adresu. Koristeći jedan od nekoliko alata, lako je moguće modificirati adrese, posebno izvorišnu. Važno je primijetiti da se svaki paket šalje nezavisno od drugih.

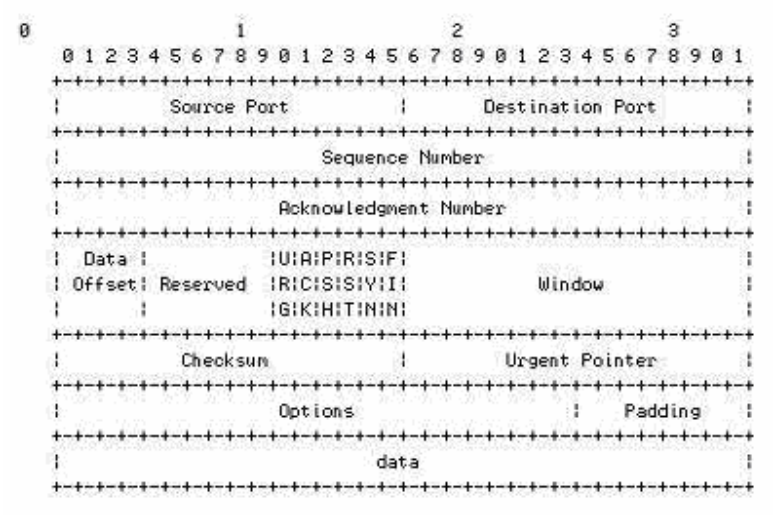
2.2. TCP (Transmission Control Protocol)

Prijenosni sloj (sloj iznad mrežnog) ima implementiran TCP koji je connection-oriented. To znači da sudionici u TCP prijenosu prvo moraju uspostaviti vezu i uskladiti je (SYN-SYN/ACK-ACK, vidi sliku 2.).



Slika 2. Sinkronizacija

Na slici 3. može se vidjeti da se TCP zaglavlje bitno razlikuje od IP zaglavlja.



Slika 3. Zaglavlje TCP paketa

Problematični su prvih 12B koji sadrže izvorišni i odredišni port, slijedni (sequence) i potvrdni (acknowledgement) broj. Kao i IP podatkovni paket, TCP paketi se mogu softeverski manipulirati. Izvorišni i odredišni portovi ovise o mrežnoj aplikaciji koja se koristi (npr. HTTP preko porta 80). Slijedni i potvrdni brojevi su važni za razumijevanje *IP spoofing*-a. Podaci sadržani u tim poljima imaju informaciju o potvrdi primljenih paketa i njihovom pravilnom poretku. Slijedni broj je broj prvog byte-a u trenutnom paketu, koji je važan za tok podatak. Potvrdni broj sadrži vrijednost sljedećeg očekivanog slijednog broja u prijenosu. Vezom se potvrđuje na oba kraja da su primljeni ispravni paketi.

3. Spoofing napadi

Postoji nekoliko tipova napada koji uspješno koriste *IP spoofing*. Iako su neki već zastarjeli, drugi još uvijek predstavljaju prijetnju za sadašnje sigurnosne postupke.

3.1. Spoofing na viđeno (non-blind)

Ovaj napad se odvija kad je napadač na istoj strani podmreže (subnet) kao i žrtva. Slijedni i potvrdni brojevi mogu se „njuškati“, pri tome eleminirajući potencijalne poteškoće koje se javljaju za njihovo točno izračunavanje. Otimanje sesije (razdoblje razmjene podataka) je najveća prijetnja ovog tipa *spoofing*-a. Radi se na taj način da se pokvari prijenos podataka već uspostavljene veze te ponovo uspostavi veza bazirana na točnim slijednim i potvrdnim brojevima sa stranom koja napada. Pomoću ove tehnike, napadač je u stanju zaobići bilo koju mjeru utvrđivanja vjerodostojnosti koje se koriste pri uspostavi veze.

3.2. Spoofing na neviđeno (blind)

Ovo je sofisticiraniji napad jer su nedostupni slijedni i potvrdni brojevi. Kako bi se to izbjeglo, pošalje se nekoliko paketa s namjerom prikupljanja slijednih brojeva. Prije su se koristile osnovne tehnike za generiranje slijednih brojeva. Bilo je jednostavno otkriti formulu za generiranje ako su se samo promatrali paketi i TCP veze. Danas većina operacijskih sustava ima implementirano nasumično generiranje slijednih brojeva pa ih je teško predvidjeti. Prije nekoliko godina mnogo je uređaja koristilo tzv. Rlogin - autorizaciju na središnjem računalu (host-based authentication service). Napadom su se dodavali potrebni podaci u sustav (npr. novi korisnički račun) naslijepo, omogućavajući potpuni pristup napadaču koji se pretvarao da je autorizirani korisnik.

3.3. Čovjek u sredini (man in the middle attack, MITM)

Oba tipa napada malo prije opisana su oblici kršenja sigurnosnih pravila poznatih kao MITM. U ovim napadima, zlonamjerna strana presreće zakonitu komunikaciju između dvije prijateljske strane. Upadač tada kontolira protok podataka i ima mogućnost odstraniti ili izmijeniti informacije koje šalju originalni sudionici, a bez ikakvog znanja

pošiljaoca ili primatelja kojima je informacija namjenjena. U tom slučaju, napadač može lako prevariti žrtvu da mu otkrije povjerljive informacije.

3.4. "Denial-of-service" napad, DoS

IP spoofing se najčešće koristi za napad protiv kojeg se najteže braniti, a to je DoS. Ne mora se voditi briga o pravilnoj primopredaji i transakciji, već samo o opsegu korisnika i izvorima. Zapravo, radi se na tome da se žrtva poplavi sa što je moguće više paketa kratkom vremenu. Kako bi se prolongirala učinkovitost napada, prikrije se izvorišna IP adresa i postaje nemoguće pratiti i zaustaviti DoS.

3.5. Detekcija IP spoofing-a

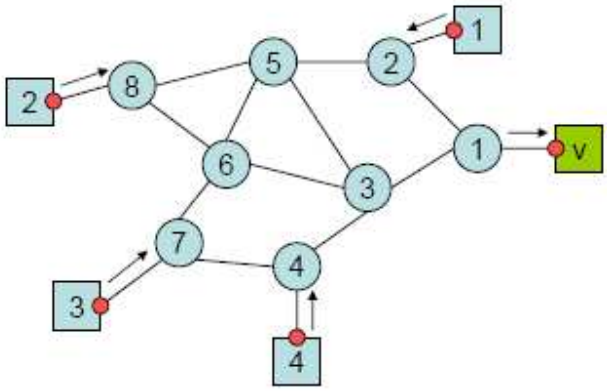
Postoji mogućnost softverskog praćenja paketa. Indikacija *IP spoofing*-a su paketi na vanjskom sučelju koji imaju i izvorišnu i vanjsku adresu u lokalnoj domeni. Drugi način detekcije je uspoređivanje procesa logiranja između sustava na unutarnjoj mreži. Ako napad *spoofing*-om uspije, može se dobiti podatak o ulogiravanju na žrtvinom računalu, ali s udaljenim pristupom.

4. Kako se braniti protiv IP spoofinga?

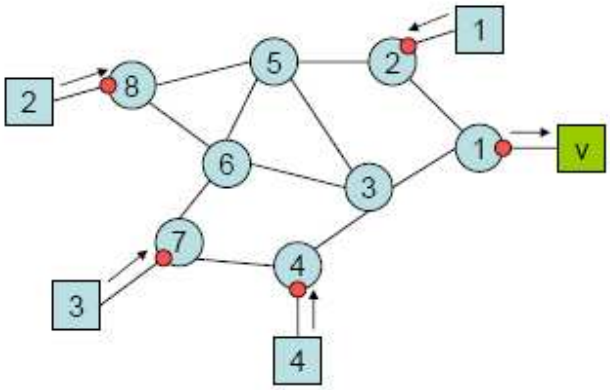
Postoji nekoliko mjera predostrožnosti koje ograničavaju IP spoofing na mreži, kao što su:

4.1. Filtriranje kod router-a

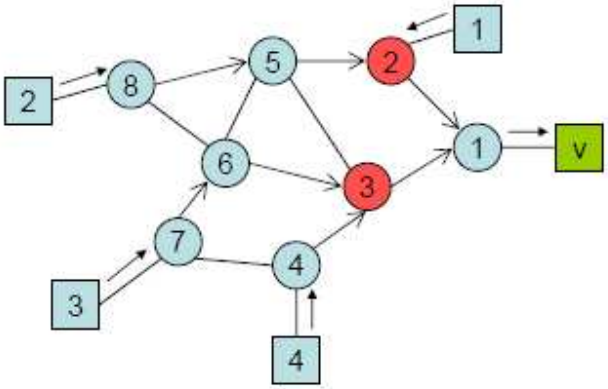
Borbu protiv *spoofing*-a dobro je početi implementiranjem ulaznih (ingress) i izlaznih (egress) filtra na usmjerivače (router) (slike 4.,5.,6.). Potrebno je implementirati listu dopuštenih pristupa (ACL-access control list) koja blokira privatne IP adrese na sučelju od mreže prema računalu. Dodatno, ovakvo sučelje ne smije prihvatiti adrese koji se nalaze unutar vlastitog dometa mreže što je česta tehnika za zaobilaženje vatrozida. Na sučelju od računala prema mreži potrebno je ograničiti izvorišnu adresu izvan važećeg dometa što će spriječiti nekoga unutar mreže da šalje podatke *spoofing* tipa prema Internetu.



Slika 4. Izlazno filtriranje: filtrira se promet prema vanjskom usmjerivaču



Slika 5. Ulazno filtriranje



Slika 6. Ulazno filtriranje: selektivni filter

4.2. Enkripcija i autorizacija

Implementiranje zaštitnog kodiranja (enkripcije) i provjere autentičnosti također se reducira prijetnja od *spoofing*-a. Oba elementa uključena su u Ipv6. Treba također eliminirati autorizaciju koja dolazi od središnjeg računala, što uobičajeno imaju računala na istoj podmreži.

5. Zaključak

IP spoofing je problem koji nema jednostavnog rješenja pošto je svojstven dizajnu TCP/IP protokola. Razumijevanje kako i zašto se koriste IP spoofing napadi, u kombinaciji s nekoliko jednostavnih metoda, omogućuje zaštitu naših mreža od zlonamjernih *cloak* i *crack* tehnika.

6. Literatura

[1] www.securityfocus.com/infocus/1674

[2] http://en.wikipedia.org/wiki/Internet_protocol_spoofing

[3] http://www.iss.net

[4] http://dokumentacija.linux.hr/Sigurnost-KAKO.html#toc12