HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nedostaci preklapanih mreža

CCERT-PUBDOC-2002-07-03

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Postoje mnogi alati za zaštitu postojećih okruženja, ali isto tako postoji mnogi alati za napade na ista ta okruženja. Svi oni se razlikuju po svojim svojstvima i mogućnostima. Neki od tih alata su strogo specijalizirani u svojoj namjeni, dok su drugi općenitiji i koriste više blokova za izradu kompleksnijih alata. Jedan od takvih alata je i alat za praćenje mrežnog prometa (*engl. sniffer*). Praćenje mrežnog prometa u svom najopćenitijem obliku podrazumijeva presretanje okvira iz mreže i pregledavanja njihova sadržaja. Takva mogućnost korištenja u širokoj je uporabi, te se time služe mnogi, od mrežnih administratora (koji pokušavaju pronaći i eliminirati probleme), do zlonamjernih napadača (koji pokušavaju doći do povjerljivih informacija).

Sve do nedavno mogućnosti praćenja mrežnog prometa u preklapanim mrežama nisu bile poznate širim krugovima. Kroz napore sigurnosne zajednice (ili anti-sigurnosne, ovisno o stajalištu) razvijeni su alati koji omogućavaju praćenje mrežnog prometa i na preklapanim mrežama. Da bi se lakše mogao razumjeti način njihovog funkcioniranja biti će ukratko objašnjeno kako funkcioniraju ne-preklapane mreže i kako se njihov promet može pratiti. U nastavku će biti opisano funkcioniranje preklapanih mreža, te načini kako se njihov promet može pratiti. Na kraju će biti dane smjernice kako je najbolje štititi promet u preklapanim i ne-preklapanim mrežama.

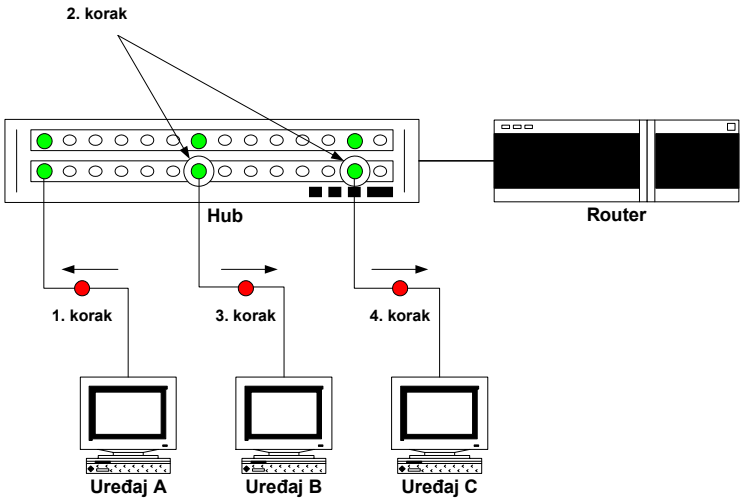
2. Praćenje prometa na ne-preklapanim mrežama

U ne-preklapanom mrežnom okruženju temelj je koncept segmenta mreže. Segment predstavlja mrežnu arhitekturu koja se nalazi iza *routera*, premosnika, *huba* ili preklopnika. U takvom okruženju okviri se odašilju korištenjem *broadcast* metode. Odnosno, kad jedan uređaj pošalje jedan okvir, on je vidljiv svim ostalim uređajima na segmentu. Svaki uređaj po redu pregledava okvir da utvrdi da li je namijenjen njemu, ukoliko nije okvir se odbacuje. Ukoliko je pak okvir namijenjen uređaju on se prihvaća za obradu. Za potrebe ovog dokumenta, uređaj B će služiti kao agent za praćenje mrežnog prometa, dok će uređaji A i C predstavljati uređaje koji međusobno komuniciraju (***Slika 1***).

Normalni tok prometa na ne-preklapanoj mreži odvija se na sljedeći način:

1. Uređaj A šalje okvir uređaju C.
2. *Hub* šalje okvir na svaki aktivni port.
3. Uređaj B prima okvir i provjerava adresu okvira. Nakon što je utvrdio da to nije njegova adresa, uređaj B odbacuje okvir.
4. Uređaj C također prima okvir i provjerava adresu. Nakon što je utvrdio da je okvir namijenjen njemu, uređaj ga prihvaća za daljnju obradu.

U načeli koraci 3 i 4 mogu se i zamijeniti, obzirom na to koji će uređaj primiti ranije okvir, što izlazi iz okvira ovog dokumenta. Zbog praktičnih razloga može se pretpostaviti da se oni događaju istovremeno.



Slika 1

Da bi se pojedini uređaj mogao koristiti kao agent za praćenje mrežnog prometa, njegovo mrežno sučelje mora biti podešeno u "*promiscuous*" način rada. Ovaj način rada može podesiti samo korisnik sa administratorskim ili *root* ovlastima. U tom načinu rada uređaj više ne odbacuje okvire koji su adresirani za druge uređaje. Umjesto toga okvir se prosljeđuje višim slojevima u očekivanju da postoji programska podrška koja će ga obrađivati. U odnosu na sliku 1, koraci ovog procesa bili bi sljedeći:

1. Uređaj A šalje okvir uređaju C.
2. *Hub* šalje okvir na svaki aktivni port.
3. Uređaj B prima okvir i prihvaća ga jer je mrežno sučelje podešeno u "*promiscuous*" način rada. To mrežnom sučelju omogućava prihvaćanje bilo kakvih okvira, bez obzira na MAC (Media Access Control) adresu u okviru. Iako sučelje prihvaća okvir, potrebno je postojanje programske podrške na višoj razini koja će obraditi podatke.
4. Uređaj C također prima okvir i obrađuje ga kako je i potrebno. Ne postoji način da uređaj C može znati da je neki drugi uređaj također obradio okvir.

Također i ovdje koraci 3 i 4 mogu biti navedeni obrnutim redoslijedom.

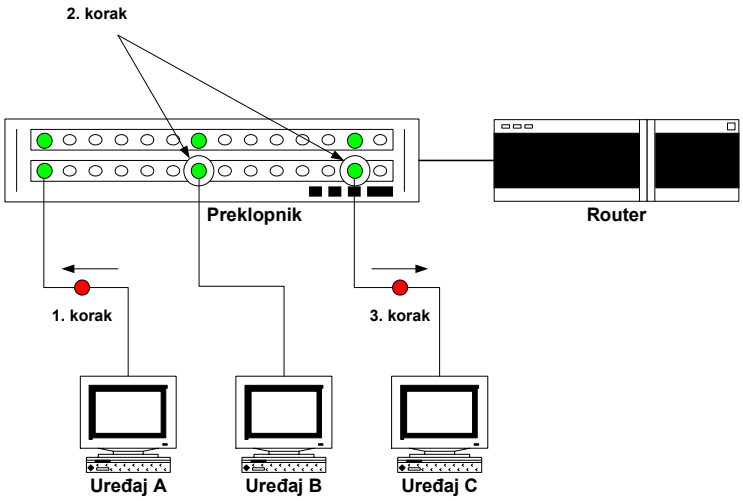
Lako je uočiti da je u ne-preklapanom okruženju praćenje mrežnog prometa vrlo jednostavno. Pošto *hub* pakete šalje na sve aktivne portove, potrebno je samo postaviti odgovarajućeg agenta koji će prihvaćati sav promet. Postoji nekoliko alata koji to omogućavaju, a neki od njih su i javno dostupni alati za praćenje prometa na ne-preklapanim mrežama, kao npr.:

- ADMsniff – alat za Linux ili SunOS2,
- esniff – alat za višestruke platforme,
- linsniffer – specifični Linux ethernet alat,
- sniffer – specijaliziran sa praćenje pojedinih portova, za Windows okruženje,
- sniffit – alat koji radi pod LINUX, SunOS, Solaris, FreeBSD i IRIX sustavima,
- snmpsniff – alat specijaliziran za SNMP promet,
- solsniffer – specifični Solaris ethernet alat,
- sunsniff – specifični SunOS ethernet alat,
- websniff – alat specijaliziran za praćenje login/auth informacija web poslužitelja.

Osim navedenih alata postoje i mnogi drugi.

3. Praćenje prometa na preklapanim mrežama

U preklapanom mrežnom okruženju i dalje se pojavljuje pojam mrežnog segmenta, ali segment se u ovom slučaju odnosi samo na uređaj i preklopnik. Okviri sa podacima direktno se obrađuju, odnosno okviri od uređaja A do uređaja C šalju se samo kroz one dijelove preklopnika koji su nužni sa uspostavu veze između uređaja A i uređaja C. Ovakvu komunikaciju prikazuje ***Slika 2***.



Slika 2

1. Uređaj A šalje okvir uređaju C.
2. Preklopnika ispituje okvir i određuje koji je ciljni uređaj. Nakon toga preklopnik uspostavlja vezu između uređaja A i uređaja C, tako da imaju privatnu vezu.
3. Uređaj C primit će okvir i provjeriti adresu. Nakon što odredi da je on ciljni uređaj dalje će obraditi okvir.

Važno je uočiti da uređaji i dalje provjeravaju ciljnu adresu iako preklopnik osigurava da su oni ciljni uređaj. Iako to može uzrokovati vrlo male suvišne provjere, to je nužno jer uređaji mogu migrirati između preklapanih i ne-preklapanih okruženja (npr. prijenosna računala).

Preklapane mreže donose sljedeća poboljšanja:

- smanjenje mrežnog prometa pošto više nema *broadcasta* svim uređajima,
- smanjenja opterećenja uređaja pošto ne moraju obrađivati okvire koji im nisu namijenjeni.

Osim dobrih strana, tu su i neki nedostaci:

- povećano opterećenje preklopnika pošto on u stvarnom vremenu mora uspostavljati virtualne spojeve između uređaja.

Kako se može vidjeti u preklapanim mrežama nije moguće pratiti mrežni promet kao što je to moguće u ne-prospajanim. Iako to doprinosi sigurnosti, to nije navedeno kao poboljšanje, pošto su preklapane mreža uvedene samo iz razloga poboljšanja performansi (brzine i propusnosti), a ne povećanja razine sigurnosti. Detaljnije razmatranje otkriva nekoliko mogućnosti praćenja mrežnog prometa i na preklapanim mrežama:

- ARP lažiranje,
- MAC preplavljivanje,
- MAC dupliciranje.

Osin tih mogućnosti postoje još neke, no nabrojane mogućnosti mogu poslužiti kao dobar primjer.

3.1. ARP lažiranje

Jedna od osnovnih operacija na kojima se temelji Ethernet protokol jesu ARP (Address Resolution Protocol) upiti i odgovori. Općenito kada uređaj A želi preko mreže komunicirati sa uređajem C on šalje ARP upit. Uređaj C tada šalje ARP odgovor koji uključuje i MAC adresu. Čak i u preklapanom mrežnom okruženju, inicijalni ARP upit šalje se *broadcastom*. Moguće je da uređaj B napravi i pošalje lažni ARP odgovor uređaju A. Takav lažni ARP odgovor će označavati da uređaj B ima MAC adresu uređaja C. Uređaj A će nadalje slati sav promet uređaju B, pošto je on dokazao da ima traženu MAC adresu. Dostupni su razni alati za slanje lažnih ARP odgovora za razne klase uređaja (npr. NFS poslužitelje, HTTP poslužitelje itd.). Jedan od takvih alata je i *dsniff* koji je dobar za praćenje određenih vrsta prometa. Drugi alati osluškuju općenite ARP upite i šalje lažne ARP odgovore u tom trenutku. Program *parasite* spada u tu kategoriju i služi za praćenje čitavih mreža. Da bi ovakva vrst napada bila moguća, potrebna je mogućnost slanja okvira koji se prime uređajima kojima su zaista namijenjeni. Najuobičajeniji načini za postizanje toga jest *IP forwarding*, bilo na razini kernela, bilo na razini aplikacije.

3.2. MAC preplavljivanje

Pošto su preklopnici odgovorni za uspostavu virtualnih spojeve od jednog uređaja prema drugom, oni moraju čuvati tabelu koja sadrži koje adrese (MAC adrese) pripadaju kojim fizičkim portovima. Memorija koja je namijenjena za tu tabelu je ograničena. Ta činjenica omogućava da preklopnik bude iskorišten za potrebe praćenja mrežnog prometa. Neke preklopnike moguće je preplaviti sa zlonamjernim podacima o MAC adresama. Preklopnik ne znajući kako da obradi te suvišne podatke će početi raditi kao *hub* i napraviti *broadcast* svih mrežnih okvira na sve portove. U tom slučaju će se omogućiti rad generičkih alata za praćenje mrežnog prometa.

3.3. MAC dupliciranje

Pošto se svi okviri na mreži usmjeravaju prema svojoj MAC adresi, nije teško zamisliti lažno da se može iskoristiti mogućnost lažnog predstavljanja adresom drugog uređaja. To je osnovna ideja MAC dupliciranje. Uređaj B konfigurira tako da ima istu MAC adresu kao i uređaj čiji se promet želi pratiti (na Linux operacijskim sustavima to je moguće ukoliko je dozvoljen pristup *ifconfig* naredbi). Ovo je

različito od ARP lažiranja, pošto se ARP lažiranje služi metodom modifikacije ARP *cache*-a. Korištenjem MAC dupliciranja prijevara se radi na preklopniku, pošto preklopnik tada misli da dva porta imaju istu MAC adresu. Pošto podaci moraju biti proslijeđeni na oba porta, nužno je korištenje IP *forwardinga*.

4. Zaštita

Postoji nekoliko načina zaštite od ranije opisanih napada. Neke od tih metoda mogu se primijeniti na preklapana i ne-preklapana mrežna okruženja.

4.1. IP filtriranje

Omogućavanjem IP filtriranja na preklopniku moguće je direktno specificirati koji promet je dozvoljen prema i od svakog porta. Ovo je ponekad prilično teško za implementaciju, posebno u dinamičkim okruženjima.

4.2. Sigurnost portova

Ukoliko *hub* ili preklopnik imaju mogućnost postavljanja sigurnosnih parametara portova, to se može iskoristiti za zaštitu od napada korištenjem MAC preplavljivanja ili MAC lažiranja. Ova opcija efikasno štiti *hub* ili preklopnik od prepoznavanja više od jedne MAC adrese na fizičkom portu. Kao i ostale sigurnosne procedure, ova opcija ograničava okruženje i povećava potrebu za procesima upravljanja i praćenja.

4.3. Sigurnost usmjeravanja

Usmjeravanje mogu vršiti samo za to namijenjeni usmjerivači, što znači da ni jedna radna stanica ne smije imati dozvole za pokretanja *routing* protokola, pošto radne stanice mogu biti kompromitirane. Također je upravljanje svakim od mrežnih uređaja potrebno vršiti korištenjem sigurnih konekcija, a ne korištenjem *telnet* sjednica koje administrativne *login/password* podatke šalju kao otvoreni tekst.

5. Zaključak

Svrha ovog dokumenta je bila pokazati da je zaštitu mreža potrebno provoditi na svim razinama. Mreže su infrastruktura koja omogućava obavljanje raznih funkcija. Iako se često koriste na taj način, mreže koje se koriste općenito nikad nisu bile osmišljene kao sigurnosni parametri. Osiguravanje nadgledane mrežne infrastrukture je ključna komponenta osiguranja sigurnosti.
Kompromitacija pojedinog računala može napadaču omogućiti pristup nekolicini sustava, dok mogućnost praćenja mrežnog prometa, odnosno korisničkih imena i zaporki za nekolicinu uređaja efektivno kompromitira čitavu mrežu. Mrežni administratori moraju biti svjesni da imaju dvije opcije. Mogu upravljati mrežom na odgovarajući način, te pokušati osigurati okolinu ili mogu konfigurirati okolinu tako da se sama održava, što uglavnom dovodi do sigurnosnih nedostataka.