TEHNIKA I INFORMATIKA U OBRAZOVANJU

Konferencija
32000 Čačak
9-11. Maja 2008.

UDK: 004 Pregledni rad

BEZBEDNOST RAČUNARSKIH MREŽA NA DRUGOM SLOJU OSI REFERENTNOG MODELA

Slaviša Popravak [1]

***Rezime**: Proces zaštite računarskih mreža je kontinuiran, ali mora biti i sveobuhvatan u cilju postizanja željenih rezultata, visokog nivoa bezbednosti i pune funkcionalnosti računarske mreže i mrežnih sistema u njoj. Pažnja ovog rada je usmerena na bezbednost računarskih mreža na drugom sloju OSI nivoa, na kome se i dešava većina napada čije je poreklo iz unutrašnjosti kompanije. Zbog obimnosti problematike, u radu je prezentiran samo deo mogućih brojnih napada i adekvatnih mera zaštite na drugom OSI sloju – samo onih najčešćih i najznačajnijih.*

***Ključne reči:** OSI, referentni model, sloj, zaštita*

COMPUTER NETWORKS SECURITY ON SECOND LAYER OF OSI REFERENCE MODEL

***Summary**: Process of protecting computer networks is continous, but have to be allround to reach optatice results, high level of security and full funcionality of computer network and computer systems existing in it. The aim of this project is securing computer networks at the second level of OSI, where most attack is taking place sourceing from inside of company. Because of largeness of the topic, in this project will be presented only a small part of existing attack and adequate prevention measurement at the second OSI level – only the most often and the most important.*

***Key words:** OSI, reference model, level, security*

1. UVOD

Zaštita na drugom sloju OSI modela, je od izuzetnog značaja i nipošto ne sme biti zanemarena, jer bez te zaštite bi se moglo reći da zaštita uopšte ni ne postoji. Ne vredi

[1] Slaviša Popravak, dipl. inž., M-Rodić d.o.o, Temerinski put 50, Novi Sad, E-mail: slavisa.popravak@mercator-rodic.com

mnogo što je data kompanija uložila novac i ljudske resurse u implementaciju pametnih kartica za autentifikaciju na mrežu, implementaciju IPSec VPN infrastrukture za udaljeni pristup, dobar mehanizam prava pristupa bazama podataka i korisničkim dokumentima i sl., ako ta zaštita nije sveobuhvatna i nije implementirana na svim OSI slojevima.

Treba napomenuti da svi napadi na drugom OSI sloju podrazumevaju da napadač ima lokalni pristup mreži, jer ovi napadi ne prelaze preko rutera. To mogu biti zaposleni koji u kompaniji obavljaju neke ne-IT poslove, a bivaju plaćeni od strane konkurencije da špijuniraju datu kompaniju i sl. Ti korisnici su hladno ili vatreno oružje zamenili računarima i softverom, a krajnji cilj je isti: naneti drugome štetu i/ili ostvariti dobit. Ovi napadi imaju različite ciljeve, od izazova ili nadmetanja hakera pojedinaca ili organizacija, preko nastojanja da se dođe do poslovnih tajni koje se mogu iskoristiti od strane konkurencije, pa sve do napada čiji je jedini cilj uništenje podataka.

2. NAPAD I ZAŠTITA NA DRUGOM SLOJU OSI MODELA

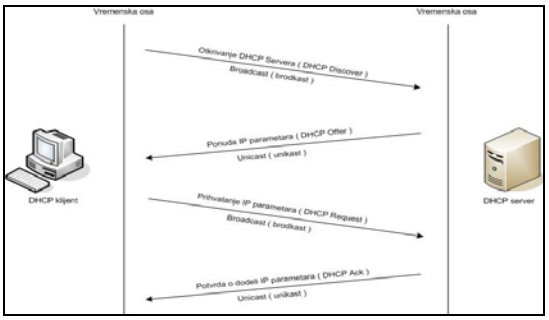
Najznačajniji i najčešće korišćeni napadi koji, u potpunosti ili jednim svojim delom, funkcionišu na drugom sloju OSI referentnog modela (ili mehanizam zaštite koji može da ih spreči funkcioniše na drugom OSI sloju) su:

- *DHCP Attack*
- *STP Attack*
- *ARP Cache Poisoning*
- *CAM Table Flooding*
- *VLAN Hopping*

Zbog izuzetno velike obimnosti materije, u ovome radu će biti detaljno prezentovani samo neki od pomenutih napada i biće detaljno objašnjen princip njihovog funkcionisanja, kao i neophodne mere zaštite koje moraju da se primene da bi se isti napadi sprečili i na taj način sprečilo curenje informacija, omogućen nesmetan rad zaposlenih, sačuvao ugled kompanije i sl. Ako bi se u radu poklonila pažnja svim mogućim napadima i merama zaštite od istih, onda bi rad bio isuviše obiman ili bi se samo površno obratila pažnja na svaki od njih, a to autoru nije cilj.

3. DHCP NAPAD

DHCP (engl. Dynamic Host Configuration Protocol) je protokol koji se koristi za dinamičku dodelu IP parametara radnim stanicama u računarskim mrežama. Ti parametri su IP adresa, mrežna maska, podrazumevajući ruter, ime domena, DNS server i dr. Iako su većina tih parametara parametri trećeg OSI sloja, sam DHCP napad se odvija jednim svojim delom na drugom sloju OSI modela, a mehanizmi zaštite koji mogu da ga spreče su takođe mehanizmi drugog OSI sloja. Princip funkcionisanja protokola prikazan je na slici 1.



Slika 1: *DHCP proces*

DHCP protokol može biti zloupotrebljen za primenu dve vrste napada na korporacijsku računarsku mrežu. Prvi oblik napada je uskraćivanje servisa (engl. Denial of Service – DOS), a drugi se koristi za prisluškivanje saobraćaja preusmeravanjem istog preko napadačeve radne stanice (engl. Man in the Middle). Takođe, je česta i kombinacija ova dva napada – napadač prvo isprazni IP adresni opseg predviđen za dodelu adresa korisnicima, zatim ubacivanjem lažnog DHCP servera, klijentima dodeljuje lažne parametre i na taj način izvršava Man in the Middle Attack.

Prvi način DHCP napada se odvija tako što napadač kontinuirano zahteva od DHCP servera IP parametre sve dok ne isprazni kompletan adresni opseg za koji je dati DHCP server konfigurisan. Taj adresni opseg je najčešće jedna C klasa IP adresa, koja se sastoji od 254 IP adrese koje može da dodeli klijentima. Najčešće je C klasa, bez obzira da li se radi o maloj firmi sa nekoliko desetina računara ili velikoj korporaciji čiju računarsku mrežu sačinjava nekoliko hiljada radnih stanica i servera. Jer u slučaju velikog broja računara date kompanije, zbog povećanja performansi smanjenjem broadcast domena, mreža će najčešće biti segmentirana nekim L3 uređajem kao što je L3 svič ili ruter i na taj način nijedan od segmenata neće imati potrebu za većim brojem IP adresa nego što je jedna C klasa.

Dakle, napad se odvija tako što napadač „iscrpi" DHCP server, menjajući svoju izvorišnu MAC adresu i svaki put od DHCP servera traži IP parametre podmećući mu drugu MAC adresu, a sve dok server ne podeli sve raspoložive adrese. Ovo je izvodljivo bez obira na to koliko IP adresa DHCP server ima na raspolaganju, tj. bez obzira da li se radi o A, B, C klasi ili nekoj podklasi koja se dobija „subnet-ovanjem" neke od pomenutih.Jedan od alata za izvođenje ovakvog napada se može naći na: http://packetstormsecurity.org/DoS/DHCPGobbler.tag.gz.

Alati koji su korišćeni u laboratorijskim uslovima za izradu ovog rada su: „Yersinia" i „DHCPX Flooder". Funkciju DHCP servera je imao Windows Server 2003 Standard Edition, a od mrežne opreme su korišćeni L2/L3 svičevi „Cisco Catalyst 2960 i 3550".

„DHCPX Flooder" je prilikom testiranja, svake sekunde uzimao po jednu IP adresu iz opsega, razmenjujući sa serverom sva četiri tipa DHCP paketa neophodnih za

kompletiranje DHCP procesa (dicover, offer, request, ack), dok je „Yersinia" adresni opseg od 200 IP adresa uspela da isprazni za 3 sekunde, s tim da je prilikom tog napada vršena razmena samo prva dva tipa DHCP paketa (discover, offer).

Na ovaj način će DHCP server ostati bez adresa i neće moći da adresira legitimne radne stanice u lokalnoj računarskoj mreži, koje zbog toga neće moći da obavljaju svoju funkciju.

Drugi način napada korišćenjem DHCP servera je malo složeniji i može da se koristiti za prisluškivanje saobraćaja u mreži. Napadač konfiguriše i pušta u produkciju DHCP server na svojoj radnoj stanici ili lap-top računaru. Taj DHCP server se nadmeće sa legitimnim DHCP serverom prilikom dodele IP parametara klijentima (ili prvo uradi DoS napad na legitimni DHCP server(e),a zatim on ostaje jedini DHCP server u mreži). Klijent će da prihvati IP parametre od DHCP servera koji mu prvi odgovori. Međutim parametri koje dodeljuje lažni DHCP server nisu isti kao oni koje dodeljuje legitimni. Napadač najčešće lažira polja DNS servera i podrazumevajućeg rutera (engl. Default Gateway). Lažiranjem ovih parametara, napadač postavlja svoj PC kao podrazumevajući ruter ili DNS server i sav saobraćaj koji napadnute radne stanice razmenjuju sa spoljnim svetom ili drugim virtuelnim lanovima – VLANovima se odvija preko napadačeve radne stanice. Još je neophodno da napadač pokrene neki analizator mrežnog saobraćaja kao što je Ethereal i da prisluškuje saobraćaj iščekujući neko korisničko ime i lozinku poslatu preko mreže u neenkriptovanom obliku, kao što to rade nebezbedni protokoli: Telnet, FTP, HTTP, POP3 i dr. U npr. okruženju gde se koristi terminal server i web interfejs za pristup aplikacija, moguće je u lažnom DNS-u lažirati adresu web interfejsa, podesiti ga da umesto TCP porta 443 koristi TCP port 80 – ako bi se ovakav napad tempirao u vremenu između 7:55 i 8:05 u toku jednog radnog dana, napadač bi mogao da prikupi nekoliko stotina korisničkih imena i lozinki, jer je u tom periodu najveća frekvencija logovanja korisnika.

DHCP DoS napad može da se izvede na dva načina od kojih je jedan starijeg, a drugi novijeg datuma i značajno sofisticiraniji, te je i neophodno implementirati i dodatni sofisticiraniji mehanizam zaštite. Da bi objašnjavanje principa napada i mehanizma zaštite bilo moguće dobro objasniti, neophodna je slika broj 2, koja prikazuje izgled DHCP paketa.

4 Bytes			
Operation Code	Hardware Type	Hardware Length	Hop Count
Transaction ID			
Seconds Elapsed		B (1 Bit)	Flags (15 Bits)
Client IP Address			
Your IP Address			
Server IP Address			
Relay Agent / Gateway IP Address			
Client Hardware Address (16 Bytes)			
Server Host Name (16 Bytes)			
Boot File Name (128 Bytes)			
Options (Variable)			

***Slika 2**: Format DHCP paketa*

Kada se govori o DHCP napadu, onda je ključno polje u DHCP paketu, na koje treba obratiti pažnju, polje „Client Hardware Address".

Prvi i manje sofisticiran DHCP DoS napad funkcioniše tako što napadač radi MAC Spoofing – randomizujući svoju MAC adresu, zatim svaku od njih upisuje u polje „Client Hardware Address" i istu tu MAC adresu upisuje u polje „Source MAC" u zaglavlju Ethernet frejma. Na ovaj način napadač generiše veliku (dovoljnu) količinu DHCP Request paketa koje bradcast-uje na mrežni segment i tako zauzima sve IP adrese koje dati DHCP server ima na raspolaganju. Prilikom izrade ovog rada, za ovu demonstraciju, je korišćen Linux alat „DHCPX Flooder".

Analizator mrežnog saobraćaja „Wireshark" je uhvatio mrežni saobraćaj u kome su MAC adresa u CHA polju DHCP paketa i MAC adresa u zaglavlju Ethernet frejma identične. Alat koji je korišćen je „Yersinia" korišćena sa MAC spoofing-om:

Mehanizam koji je dovoljan da bi se sprečio ovaj tip DHCP DoS napada je „Port Security", koji podržavaju svi vodeći proizvođači mrežne opreme. Autor ovog rada je koristio mrežnu opremu kompanije „Cisco Systems". Treba napomenuti da ovaj mehanizam nije podrazumevajuće implementiran na svičevima, već da mrežni inženjeri i administratori, zaduženi za bezbednost, moraju da znaju za moguće L2 napade i da poznaju koje od njih i na koji način može da spreči „Port Security". Sama implementacija je prilično jednostavna i na Cisco svičevima se realizuje pomoću nekoliko komandi, prikazanih na slici 3.

```
Switch#configure terminal
Switch(config)#interface range fastethernet 0/1 - 24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 2
Switch(config-if-range)#switchport port-security violation shutdown
```

Slika 3: *Port Security*

Na ovaj način će port na sviču, na koji je napadač povezan, biti automatski ugašen nakon što se na njemu pojavi više od 2 MAC adrese (maksimalan broj MAC adresa je mogao biti postavljen da dozvoli samo jednu MAC adresu, ali u okruženju gde se koristi IP telefonija i gde je IP telefon povezan na svič, a radna stanica na mrežu povezana preko IP telefona – na datome portu na sviču će se pojaviti 2 MAC adrese) i time potencijalni napad sprečen. Da bi napad mogao uspešno da se izvrši, napadač bi morao moći generisati znatno veći broj MAC adresa i DHCP Request paketa (bar nekoliko desetina ili stotina).

Postoji nekoliko mogućih reakcija koje će svič da primeni u slučaju prekoračenja dozvoljenog broja MAC adresa na datome portu i one su:

3550(config-if-range)#switchport port-security violation ?

protect Security violation protect mode

restrict Security violation restrict mode

shutdown Security violation shutdown mode

Autor ovoga rada preferira „shutdown" datoga porta, iako to zahteva kasniju administraciju u vidu ponovnog aktiviranja datoga porta na sviču, ali s druge strane dati korisnik (potencijalni napadač) će morati sam da prijavi da mu nešto nije u redu sa mrežnom konekcijom – a to će administratoru zaduženom za bezbednost računarskih komunikacija skrenuti pažnju i usmeriti ga da dodatno ispita uzroke narušavanja postavljenih bezbednosnih pravila.

Drugi tip DHCP DoS napada je novijeg datuma i napravljen je da bi izbegao „Port Security" koji je eventualno podešen na mrežnim svičevima. Napad funkcioniše tako što napadač randomizuje polje „Client Hardware Address" u DHCP Request paketu, ali ne radi MAC Spoofing na nivou Ethernet frejma, već u polje „Source MAC" u frejmu uvek upisuje svoju stvarnu MAC adresu. Na ovaj način napadač prazni DHCP opseg datoga servera, jer DHCP server proverava samo polje „Client Hardware Address" u DHCP Request paketu i za tu MAC adresu vezuje dodeljenu IP adresu. Ovde je takođe korišćena „Yersinia", ali bez uključenog MAC spoofing-a. Analizator mrežnog saobraćaja pokazuje različite MAC adrese u polju CHA DHCP paketa i u polju Source MAC u zaglavlju Ethernet frejma.

Testiranje prilikom izrade ovoga rada je vršeno na DHCP serveru podignutom na Windows Serveru 2003 Standard Edition. Moguće je da postoje implementacije DHCP servera koje vrše poređenenje polja „Client Hardware Address" iz DHCP paketa i polja „Source MAC" iz zaglavlja Ethernet frejma – i na taj način sprečavaju ovakav vid napada.

Mehanizam zaštite od ovakvog načina DHCP napada, koji je patentirala kompanija „Cisco Systems" se naziva „DHCP Snooping". Dve najznačajnije stvari koje ovaj mehanizam uvodi su: „deep DHCP packet inspection" i „trusted" i „untrusted" portovi na sviču. Prva od njih podrazumeva da svič „pogleda" u DHCP paket i napravi poređenje MAC adrese u polju „Client Hardware Address" sa MAC adresom u zaglavlju Ethernet frejma. Ukoliko se ove dve MAC adrese razlikuju, to ukazuje da je potencijalni DHCP napad u toku i svič će da odbaci takve pakete ili da ugasi dati port i na taj način sprečiti DHCP DoS napad.

Drugi pojavni oblik DHCP napada „DHCP Man in the Middle Attack", čiji cilj nije samo da spreči rad legitimnih korisnika u datoj računarskoj mreži, već da se iskoristi za prikupljanje informacija (prvenstveno korisničkih imena i lozinki, a zatim drugih informacija koje su od značaja napadaču ili konkurenciji date kompanije koja ga je eventualno angažovala) ne može da se spreči korišćenjem ranije pomenutog mehanizma „Port Security", jer se lažni DHCP server uvek javlja sa jedne MAC adrese. Ovakav napad može da se izvodi sam ili u kombinaciji sa DHCP DoS napadom, tako što napadač prvo onesposobi postojeće DHCP servere u mreži, a zatim podigne lazni DHCP server koji će da dodeljuje parametre DHCP klijentima.

Mehanizam zaštite od ovakvog tipa DHCP napada, koji omogućava „DHCP Snooping" se omogućava uvođenjem dva tipa portova na svičevima: „trusted" i „untrusted". Svi portovi na svim svičevima u mreži, na koje su povezane radne stanice je neophodno definisati kao „untrusted" (što je i podrazumevajuća vrednost prilikom implementiranja „DHCP

Snooping-a"). S obzirom da dhcp klijent nema potrebe da šalje „DHCP Offer" i „DHCP Ack" pakete (to su unicast paketi koje šalje isključivo DHCP server) DHCP Snooping onemogućava dolazak ovog tipa DHCP paketa preko „untrusted" porta. Ovakvi tipovi DHCP paketa su dozvoljeni samo sa „trusted" portova koje je mrežni administrator definasao kao „trusted" portove, jer zna da su na njih povezani legitimni DHCP serveri. Tkođe se odnosi i na trunk portove.

Dakle, vidi se da samo jedan od dva pomenuta mehanizma zaštite nije dovoljan, jer je pokazano da može da se zaobiđe i jedan i drugi. Ali implementacijom oba pomenuta mehanizma zaštite: „Port Security" i „DHCP Snooping" se u potpunosti može izbeći „DHCP Denial of Services" i „DHCP Man in the Middle Attack".

Važno je napomenuti da je do pre par godina za zaštitu od DHCP napada bio dovoljan samo „Port Security", ali pojavom novijh alata kao što je „Yersinia" (koju je autor koristio prilikom izrade rada) uveden je sofisticiraniji način DHCP napada koji se zasniva na randomizaciji „Client Hardware Address" polja u DHCP paketu. Poenta je – ono što se danas smatra dovoljnom zaštitom od nekog tipa napada ne mora da znači da će i „sutra" biti dovoljno da datu računarsku mrežu zaštiti. Stalno se otkrivaju novi propusti u protokolima i razvijaju alati koje te propuste znaju da iskoriste.

4. TROVANJE ARP MEMORIJE

Trovanje ARP memorije (engl. ARP cache poisoning) je jedna ot tehnika koja se koristi za prisluškivanje saobraćaja u računarskim mrežama zasnovanim na svičevima, a ne na habovima.

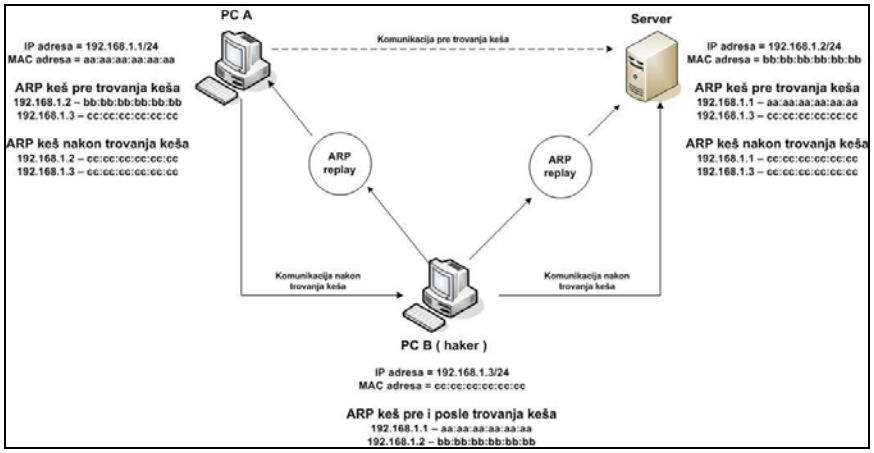
Svičevi su napravljeni da bi se ubrzala mrežna komunikacija smanjenjem veličine kolizionog domena (mikrosegmentacija – jedan port na sviču i radna stanica povezana na taj port čine jedan kolizioni domen), a ne da bi se povećala bezbednost u mrežnoj komunikaciji. Pored pomenute tehnike za prisluškivanje mrežnog saobraćaja u mreži zasnovanoj na svičevima, postoje i druge tehniku koje imaju istu svrhu. Neke od njih su:

- CAM table flooding
- Switch port stealing

Tehnika trovanja arp memorije je zasnovana na ARP protokolu (engl.Address ResolutionProtocol). Kada računar " A " želi da komunicira sa serverom, on će poslati ARP zahtev (*engl*. ARP request). ARP zahtev se šalje kao brodkast na drugom sloju OSI modela i primiće ga svi aktivni računari na datom mrežnom segmentu. Server će, takođe, primiti ARP zahtev, tj. zahtev za razrešenjem IP adrese u MAC adresu i zatim će računaru " A " poslati ARP odgovor (*engl.* ARP replay), iz kojega će računar " A " saznati MAC adresu servera i pomoću koje će se odvijati kasnija komunikacija. Računar " B " može da počne sa trovanjem ARP keša računara " A " i servera, konstantnim slanjem ARP odgovora na njihove adrese (npr.: svakih 30 sekundi). ARP protokol je dizajniran tako da će računar prihvatiti ARP odgovor iako nije poslao ARP zahtev, te će računar "A" u svome ARP kešu mapirati IP adresu servera sa MAC adresom računara "B". Server će u svoj ARP keš

mapirati IP adresu računara "A" sa MAC adresom računara "B", tako da će se stvarna komunikacija, između njih, odvijati preko računara "B", a da oni toga neće biti svesni, što je prikazano na slici 4.

Jedino što još korisnik računara "B" treba da uradi je da pokrene neki softver za analizu i praćenje mrežnog saobraćaja na svome računaru i prebaci mrežnu karticu u promiskuitetni režim rada. Tako će uhvatiti sav saobraćaj između dva ciljna računara, neometajući njihovu komunikaciju. Postoje već razvijeni softveri koji mogu da rade i trovanje ARP keša i praćenje mrežnog saobraćaja. Jedan od njih je "Ethercap".



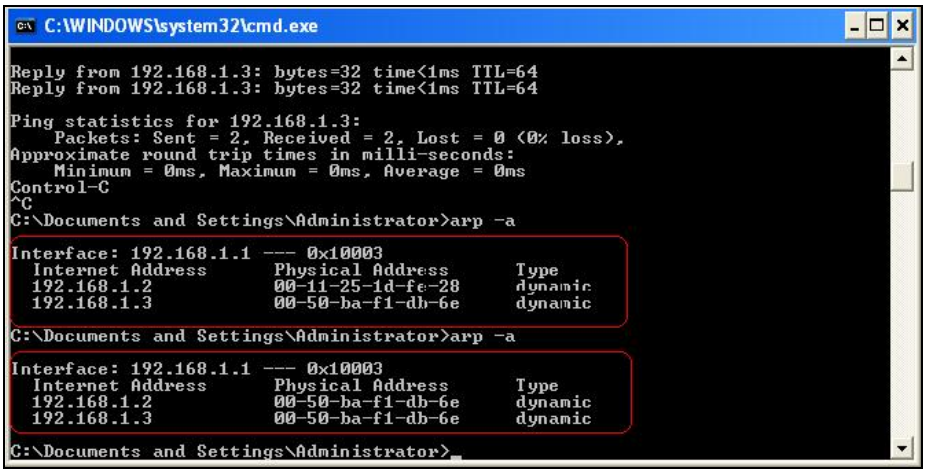
Slika 4: *Ttrovanje ARP memorije (ARP cache poisoning)*

Legenda:

..... logička konekcija (način na koji ciljni računari „misle" da komuniciraju, odnosno način na koji komuniciraju pre trovanja ARP keša)

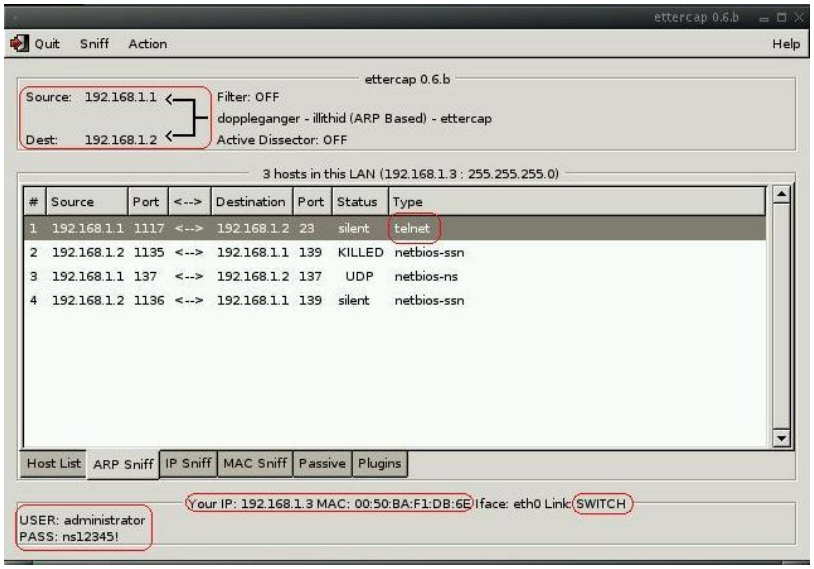
——— stvarna komunikacija

Na slici 5. se vidi izgled arp keša, u normalnim okolnostima i kasnije, nakon primene tehnike "ARP Cache Poisoning". Računar A ima zapamćene, u svojoj arp memoriji, MAC adrese računara B i C, međutim, kasnije na istoj slici se vidi kako računar A ima iste MAC adrese i za B i C. Pošto se stvarna komunikacija u računarskim mrežama odvija pomoću fizičkih MAC adresa, a ne logičkih IP adresa, komunikacija između računara A (192.168.1.1) i računara B (192.168.1.2) će se odvijati preko uljeza, tj. preko računara C (192.168.1.3).



Slika 5: *ARP keš, pre i posle trovanja*

I na kraju slika 6. pokazuje kako računar C, lako dolazi do administatorske lozinke, prilikom Telnet komunikacije između računara A i B.



Slika 6: *Ettercap na delu*

Kao mehanizam zaštite od ovakvog napada se može koristiti, ranije pomenuti, „DHCP Snooping". Na taj način svič poseduje tabelu mapiranja IP-MAC, koju može da iskoristi da utvrdi da li su informacije u ARP replay paketu tačne. Ukoliko nisu, paket jednostavno biva

odbačen. Ova tehnika se naziva dinamička inspekcija ARP-a (Dynamic ARP Inspection – DAI) i može biti dovoljan mehanizam zaštite ukoliko se u mreži koristi isključivo dinamičko adresiranje radnih stanica.

Druga tehnika koja može da se koristi da bi se izbegao ovakav vid napada je ignorisanje bezrazložnih ARP replay paketa (engl. Gratuitous ARP) od strane radnih stanica.

Treća tehnika je implementacija sistema za detekciju napada (engl. Intrusion Detection System – IDS), koji može da proveri ispravnost IP-MAC mapiranja u ARP saobraćaju.

Statičko održavanje ARP memorije može biti efikasno, ali bi zahtevalo suviše veliko angažovanje, te se ne preporučuje kao vid zaštite od ovog tipa napada.

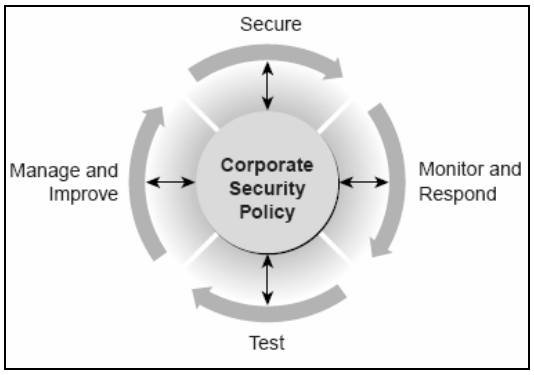
5. ZAKLJUČAK

Zaštita računarskih mreža mora biti sveobuhvatan i kontinuiran proces. Sveobuhvatnost se ogleda u adekvatnoj zaštiti na svakom sloju OSI referentnog modela. Takođe, proces zaštite mora biti kontinuiran, tj. stalno se mora testirati i unapređivati.

Sa pojavom svičeva se smatralo da je onemogućeno prisluškivanje saobraćaja u mreži, što je u početku i bilo tačno, ali se odnosilo na dotadašnje analizatore mrežnog saobraćaja i njihov princip funkcionisanja. Vremenom su se razvili noviji alati, koji su se prilagodili principima funkcionisanja svičeva u odnosu na habove.

Isto tako se do skora smatralo da je zaštita na nivou porta na sviču dovoljan mehanizam da se data računarska mreža zaštiti od DHCP napada. Vremenom su se pojavili mehanizmi koji mogu da zaobiđu ovaj nivo zaštite, o čemu je u radu i bilo reči.

Kontinuiranost procesa zaštite računarskih mreža bi se mogla posmatrati kao točak koji se stalno okreće, a ilustrovan na slici 7.



Slika 7: Točak bezbednosti

Točak definiše četiri faze implementacije bezbednog sistema i održavanja istog u

bezbednom stanju:

- Nakon detaljnog proučavanja sistema – isti treba zaštititi na adekvatan način, korišćenjem određenih tehnologija (neke od njih su pomenute u prethodnom delu rada)
- Nadgledanje sistema podrazumeva konstantno praćenje aktivnosti sa aspekta bezbednosti – praćenje logova, korišćenje alata za monitoring i sl., a sve to radi pravovremenog uočavanja eventualnih propusta i pokušaja napada na mrežne sisteme.
- Testiranje sistema može da obuhvata testiranje novih tehnologija i procesa da bi se utvrdilo da li zadovoljavaju politiku bezbednosti, testiranje postojećih procesa da bi se utvrdilo da li su i dalje na zadovoljavajućem nivou bezbednosti.
- Unapređenje nivoa bezbednosti treba da bude produkt prethodne dve faze. Konstantno unapređenje mora da se sprovodi, da bi se trenutno bezbedan sistem, održao bezbednim i u budućnosti

6. LITERATURA

[1] „LAN Switch Security – What Hackers know about yur Switches";Erick Vyncke and Christopher Paggen;isco Press
[2] „Network Security Fundamentals"; Gert De Laet, Gert Schauwers; Cisco Press 2004
[3] „Penetration Testing and Network Defence"; Andrew Whitaker, Daniel P. Newman; Cisco Press 2005
[4] „Network Security Architectures"; Sean Convery; Cisco Press 2004
[5] „CCSP Complete Study Guide"; Wade Edwards, Todd Lammle; Sybex 2005
[6] „OSI referentni model – problemi bezbednosti u korporacijskim računarskim mrežama"; Slaviša Popravak; seminarski rad – Tahnički fakultet Čačak, 2007