HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Tehnike zaobilaženja vatrozidne zaštite

CCERT-PUBDOC-2005-02-109

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 4

2. VRSTE VATROZIDOVA 5

3. SIGURNOST VATROZIDNIH SUSTAVA 5

4. PROPUSTI *PACKET FILTER* VATROZIDA 6

4.1. OTKRIVANJE LOKACIJE VATROZIDA 6
4.2. PREGLEDAVANJE PORTOVA IZA VATROZIDA 7
4.3. ZAOBILAŽENJE VATROZIDA U LOKALNOJ MREŽI 8
4.4. IZLAZNA ACL PRAVILA TEMELJENA NA ODREDIŠNOM MREŽNOM PORT 9
4.5. ZAOBILAŽENJE VATROZIDA NAKON OSTVARENOG PRISTUPA UNUTAR MREŽE 9

5. SIGURNOST *PROXY* POSLUŽITELJA 10

6. ZAKLJUČAK 11

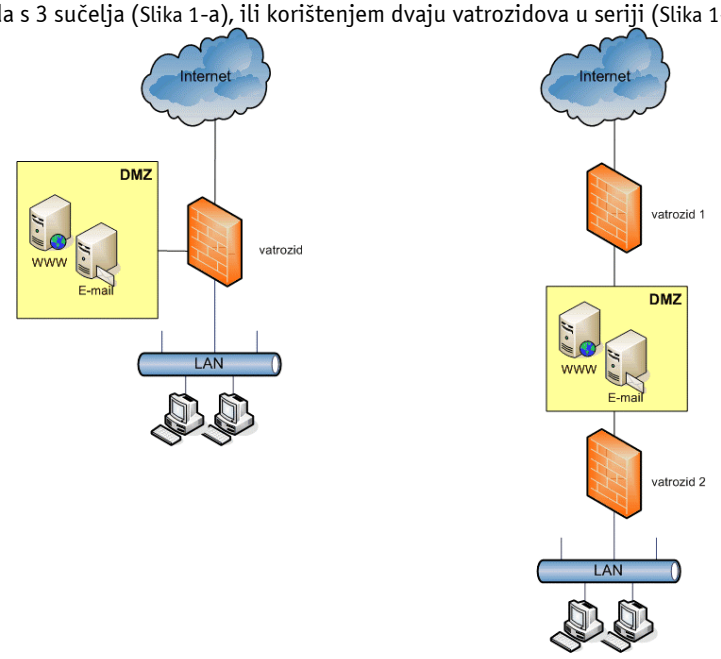
7. REFERENCE 11

1. Uvod

Moderna zaštita računalnih i mrežnih resursa podrazumijeva korištenje različitih sigurnosnih mehanizama. Među brojnim metodama zaštite mrežnih sustava, a unazad zadnjih nekoliko godina i pojedinačnih klijentskih računala, vatrozidi (eng. *firewall*) predstavljaju tehnologiju bez koje je nemoguće osigurati sigurnost sustava.

Bez obzira radi li se o zaštiti klijentskog računala na Internetu, zaštiti privatne mreže, zaštiti B2B komunikacijskog kanala ili zaštiti pristupa privatnoj mreži s Interneta, jedino ispravno postavljena vatrozidna zaštita može osigurati odgovarajuću razinu sigurnosti.

Uz pojam vatrozida vrlo usko je vezan i pojam DMZ-a, odnosno demilitarizirane zone (eng. *demilitarized zone*). Demilitariziranu zonu čine računala, mrežna oprema i čvorovi koji se nalaze iza vatrozida, a izvan privatne mreže. Ovisno o implementaciji, DMZ se može implementirati korištenjem jednog vatrozida s 3 sučelja (Slika 1-a), ili korištenjem dvaju vatrozidova u seriji (Slika 1-b).



Slika 1: Mogućnosti implementacije DMZ-a

U ovom dokumentu ukratko će biti opisani osnovni tipovi mrežnih vatrozida i njihovih osnovnih karakteristika, a poseban naglasak dan je na tehnikama koje neovlašteni korisnici mogu iskoristiti u svrhu njihovog zaobilaženja.

2. Vrste vatrozidova

Prema načinu rada i razini zaštite koju pružaju, a donekle i u skladu s povijesnim razvojem, vatrozidove je moguće podijeliti na nekoliko vrsta:

- Vatrozidovi koji filtriraju mrežne pakete (*eng. packet filters*). Filtriranje se bazira na ACL (*eng. Access Control List*) listama koje definiraju koji se mrežni promet propušta, a koji blokira.
- Vatrozidovi koji filtriraju mrežne pakete i prate stanje mrežnih sjednica (*eng. stateful inspection firewalls*). Ova vrsta vatrozida je samo napredniji tip prije navedene skupine s obzirom da posjeduju mogućnost praćenja stanja pojedinih mrežnih sjednica (npr. praćenje sekvencijalnih brojeva TCP sjednice, samog sadržaja mrežnih paketa i sl.). Ovakav način rada omogućuje im znatno pouzdanije filtriranje mrežnog prometa u odnosu na klasične ACL vatrozide.
- *Proxy* poslužitelji koji određenoj grupi računala (u nekim slučajevima bilo kome) pružaju mogućnost pristupa mrežnim servisima izvan, ili unutar mreže na kojoj su postavljeni. *Proxy* poslužitelji temelje se na posebnoj *proxy* programskoj podršci, a njihova uporaba uglavnom je ograničena na pojedine tipove mrežnih servisa (npr. HTTP ili FTP).
- Aplikacijski *gateway* poslužitelji su naprednija verzija ranije spomenutih *proxy* poslužitelja, budući da uglavnom analiziraju mrežni promet koji prolazi kroz njih te provjeravaju da li je on u skladu s definiranim pravilima. Uglavnom se radi o provjerama mrežnog prometa s ciljem detekcije potencijalnih neovlaštenih aktivnosti i sl.

Popularni komercijalni vatrozidovi uglavnom su hibridi između nekih od upravo opisanih vrsta vatrozidova. Također, vatrozidovi mogu biti implementirani sklopovski, odnosno na posebnoj *hardware* platformi ili programski, na nekom od operacijskih sustava (npr. Windows, Linux, Unix).

Neki od poznatijih vatrozidova namijenjenih osobnoj uporabi su *Zone Alarm*, *Kerio Personal Firewall*, dok su u mrežnim okruženjima popularni *Linux iptables*, *Linux ipchains*, *OpenBSD ip-filter*, *CheckPoint FW-1*, *NetScreen*, *PIX* itd.

Od *proxy* poslužitelja i aplikacijskih *gateway* poslužitelja popularni su *Squid*, *WinGate*, *TIS Firewall toolkit*, razni `SOCKS` poslužitelji, itd.

3. Sigurnost vatrozidnih sustava

Razina sigurnosti koju vatrozid pruža ovisi o njegovoj konfiguraciji, načinu implementacije i sigurnosti samog vatrozida, te o sigurnosti mreže i servisa kojima vatrozid dopušta pristup. Čest problem s vatrozidovima je neispravna konfiguracija računalne mreže na kojoj se vatrozid nalazi i pogrešno definirana sigurnosna politika na temelju koje se provodi filtriranje mrežnog prometa. Također, sigurnosni propusti u samim vatrozidnim sustavima vrlo su važan aspekt, budući da kompromitiranje vatrozidne zaštite automatski ugrožava i sigurnost cijelog sustava kojeg vatrozid štiti. Sigurnosni propusti (npr. prepisivanje spremnika ili *format string* ranjivosti) vezani su uglavnom za *proxy* poslužitelje i aplikacijske *gateway* poslužitelje, iako su poznati i kod brojnih drugih tipova vatrozida.

Važno je napomenuti da je većina programski implementiranih vatrozidova na Windows operacijskim sustavima imala sigurnosne propuste, od kojih su neki omogućavali i potpuno kompromitiranje računala na kojem se vatrozid nalazi. Neispravno i površno podešeni vatrozidni sustavi ponekad mogu sami po sebi biti sigurnosni problem. Ovo je posebno slučaj kod *proxy* poslužitelja koji korisnicima računalne mreže omogućavaju pristup servisima na javnom Internetu. Ukoliko je *proxy* poslužitelj neispravno podešen, neovlašteni korisnik izvan računalne mreže kojoj je taj *proxy* poslužitelj namijenjen ponekad može ostvariti neautorizirani pristup internoj mreži organizacije. Takvi slučajevi su prilično česti. Primjer neispravno podešenog *proxy* poslužitelja je medijski razvikana provala u računalni sustav New York Timesa, kada je Adrian Lamo preko neispravno podešenog *proxy* poslužitelja ostvario pristup internoj mreži organizacije.

Propusti vatrozidova koji se baziraju na filtriranju mrežnih paketa (*eng. packet filters i stateful filters*) uglavnom su nedovoljno dobro definirane ACL liste koje neovlaštenim korisnicima omogućavaju zaobilaženje vatrozidne zaštite te pristup nekom od servisa kojeg vatrozid štiti. Također, dodavanjem

novih funkcionalnosti u moderne vatrozide (kao što je npr. VPN servis putem kojeg se udaljenim korisnicima omogućuje pristup internoj mreži organizacije) sve su češći sigurnosni propusti vezani uz greške u programskom kodu vatrozida (*buffer overflow* ranjivosti i sl.). Pregledavanjem javnih baza ranjivosti moguće je naći velik broj sigurnosnih propusta za mnoge komercijalne i besplatne vatrozidne sustave, koji potencijalnom napadaču omogućuju preuzimanje potpune kontrole nad vatrozidom, a samim time i neograničeni pristup internoj računalnoj mreži koju vatrozid štiti.

4. Propusti *packet filter* vatrozida

Kao što je već napomenuto, vatrozidovi koji mrežni promet propuštaju ili blokiraju na temelju mrežnih paketa baziraju se na ACL listama u kojima je opisano koji se mrežni promet propušta, a koji blokira. Vatrozidovi imaju različite ACL liste za ulazni (eng. *incoming*) i izlazni (eng. *outgoing*) mrežni promet. ACL pravila za ulazni mrežni promet uglavnom su puno rigoroznija od onih za izlazni mrežni promet, budući da se izlazni promet generira iz privatne mreže ili DMZ-a, pa se pretpostavlja da je taj promet legitiman. Takve pretpostavke često vode do sigurnosnih incidenata. Postoje neke specifične situacije u kojima mrežni administrator želi korisnicima lokalne mreže omogućiti pristup samo određenim servisima izvan lokalne mreže (npr. samo HTTP i HTTPS), no takve zabrane je vrlo jednostavno zaobići. Sigurnost vatrozida može se promatrati sa perspektive ulaznog i izlaznog mrežnog prometa.

Zaobilaženje ulaznih ACL pravila uglavnom je najzanimljivije udaljenim neovlaštenim korisnicima s obzirom da uspješno zaobilaženje ulaznih ACL pravila vatrozida uglavnom vodi do daljnjeg kompromitiranja privatne računalne mreže. U nastavku dokumenta su opisane neke tehnike otkrivanja vatrozidova i zaobilaženja ulaznih i izlaznih ACL pravila.

4.1. Otkrivanje lokacije vatrozida

Prije nego što pokuša iskoristiti sigurnosni propust u postavkama vatrozida ili u samom vatrozidu, neovlašteni korisnik mora otkriti njegovu točnu lokaciju. U nekim slučajevima jednostavnih mrežnih topologija s malim brojem računala, ova zadaća je trivijalna, no u slučaju većih računalnih mreža s velikim brojem računala i mrežnih uređaja to može biti iznimno složen zadatak. Kvaliteta i učinkovitost pojedinih vatrozidnih sustava ovisi o njihovim projektantima i programerima. Vatrozidni sustavi mogu se otkriti pregledavanjem pojedinih IP adresa i analizom njihovog odstupanja od standarda definiranih RFC dokumentima. Konkretno, traže se razlike u ponašanju mrežnog stoga od onog koje bi trebao imati klasični mrežni stog operativnog sustava. Najviše takvih odstupanja može se pronaći u funkcijama vatrozida koje služe za obradu transportnog sloja ISO/OSI referentnog modela. Vatrozidni sustavi često odgovaraju na mrežne pakete koje operativni sustavi s kompletnim mrežnim stogom odbacuju. Također, vatrozidi često mogu biti otkriveni zbog odgovaranja na TCP pakete koje bi u pravilu trebali odbaciti. Npr. TCP paketi u zaglavlju imaju *checksum* polje koje osigurava integritet paketa prenošenih preko mreže. Ukoliko se dio TCP paketa iz nekog razloga izmijeni tijekom prolaza kroz mrežne čvorove, TCP *checksum* više ne odgovara sadržaju paketa i kada pristigne na odredišnu IP adresu, paket bi se trebao odbaciti. Veliki broj vatrozidova odgovara na pakete s pogrešno postavljenim *checksumom*, što se može iskoristiti za njihovo otkrivanje. Navedena tehnika opisana je u `Phrack 60` magazinu, s priloženom zakrpom za `nmap` koja omogućava primjenu te tehnike. Vatrozidne sustave uglavnom je puno jednostavnije otkriti kombinacijom `nmap` i `traceroute` programa. `Traceroute` program služi za praćenje putanje mrežnih paketa do njihovog odredišta. Ukoliko neki mrežni čvorovi ne odgovaraju na pakete koje šalje `traceroute`, postoji vjerojatnost da se prije njih nalazi vatrozid. U nastavku je prikazana putanja mrežnih paketa do poslužitelja `www.cert.hr`:

```
ljuranic@xxx:~$ traceroute www.cert.hr
traceroute to shash.cert.hr (161.53.160.69), 30 hops max, 38 byte packets
 1  161.53.120.254 (161.53.120.254)  0.241 ms  0.166 ms  0.141 ms
 2  193.198.231.65 (193.198.231.65)  1.814 ms  2.032 ms  1.957 ms
 3  193.198.231.1 (193.198.231.1)  2.116 ms  1.993 ms  1.999 ms
 4  193.198.229.9 (193.198.229.9)  2.038 ms  2.011 ms  2.003 ms
 5  * * *
 6  * * *
```

Kao što je vidljivo iz primjera, nakon četvrtog čvora, nema odgovora na mrežne pakete koje šalje `traceroute`. Iz tog razloga pretpostavljamo da se na IP adresi 193.198.229.9 provodi filtriranje mrežnog prometa. Pregledavanjem portova na računalima iza potencijalnog vatrozida moguće je ustvrditi da li se stvarno radi o vatrozidu.
Neke vatrozide također je moguće vrlo lako identificirati na temelju otvorenih mrežnih portova koji su dostupni s javnog Interneta. Npr. Checkpoint fw1 vatrozid moguće je vrlo lako prepoznati na temelju otvorenih TCP/264 i TCP/265 mrežnih portova, budući da su oni specifični za ovaj tip uređaja. Jednostavnim pregledavanjem mrežnih portova napadač može identificirati o kojem se tipu vatrozida radi te na taj način preciznije usmjeriti svoje maliciozne aktivnosti.

4.2. Pregledavanje portova iza vatrozida

Sigurnosna politika vatrozidnog sustava može blokirati pristup resursima na internoj računalnoj mreži ili DMZ zoni, no u kombinaciji s nekim drugim postavkama neovlašteni korisnik može ipak ostvariti pristup određenim servisima. Vatrozidni sustavi propuštaju određenu vrstu prometa koja je bitna za funkcioniranje određenih mrežnih operacija, a ponekad ta funkcionalnost može rezultirati kompromitiranjem ulaznih pravila vatrozida. Vatrozidovi često propuštaju TCP (*eng. Transmission Control Protocol*) pakete s izvorišnim portom 20 (`FTP-DATA`) koji se koristi za prijenos podataka te pakete s izvorišnim portom 53 (`DNS`) koji može biti TCP ili UDP (*eng. User Datagram Protocol*), a služi za tzv. DNS *zone-transfer* operacije. Ukoliko ACL pravila za te operacije nisu strogo definirana, neovlašteni korisnik ih može iskoristiti u svrhu pristupa servisima iza vatrozida. U tom slučaju, za pristup servisima iza vatrozida, neovlašteni korisnik za izvorišni port paketa koje šalje treba postaviti port 20 ili 53. Normalno konfigurirani vatrozid sustavi propuštaju mrežni promet s izvornog porta 20 na portove iznad 1024 (visoki portovi), što neovlaštenom korisniku i dalje omogućava pristup velikom broju potencijalno ranjivih mrežnih servisa (npr. `MySQL`). Pomoću popularnog `nmap` programa za pregledavanje portova moguće je ustvrditi postavke nekog vatrozida i njegova ACL pravila što je prvi korak u analizi sigurnosti vatrozidne zaštite.
U nastavku je prikazano pregledavanje portova iza vatrozida iskorištavanjem navedene pogrešne konfiguracije vatrozida pomoću `nmap` programa za pregledavanje portova:

```
[root@t-rex FW]# nmap -sS -p 22 192.168.0.3
Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2005-02-24
13:55 EST
Interesting ports on 192.168.0.3:
PORT    STATE    SERVICE
22/tcp filtered ssh
MAC Address: 00:10:A4:02:61:49 (Xircom)

Nmap run completed -- 1 IP address (1 host up) scanned in 0.385 seconds
```

Kao što je vidljivo iz primjera, nakon pregledavanja TCP porta 22 (`SSH`), `nmap` je prijavio da je port filtriran, što znači da `nmap` vjerojatno nije primio `ICMP` (*eng. Internet Control Message Protocol*) poruku tipa 13 da je mrežni port nedostupan (*eng. port unreachable*). Navedena poruka upućuje da je pristup TCP portu 22 zaštićen vatrozidom. Pregledavanje porta 22 je ipak moguće, zbog propusta u vatrozidu koji dopušta sve TCP pakete s izvorišnim portom 53 kao što je prikazano u nastavku.

```
[root@t-rex FW]# nmap -g 53 -sS -p 22 192.168.0.3

Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2005-03-24 13:55 EST
Interesting ports on 192.168.0.3:
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:10:A4:02:61:49 (Xircom)

Nmap run completed -- 1 IP address (1 host up) scanned in 0.389 seconds
```

Korištenjem `nmap` opcije „`-g`“, postavljen je port 53 kao izvorišni port TCP paketa, što omogućava zaobilaženje vatrozida i `nmap` prijavljuje da je port 22 otvoren. Pregledavanjem porta otkriveno je da je port otvoren. Za spajanje na navedeni port potrebno je za izvorišni TCP postaviti port 53. U nastavku je prikazano zaobilaženje vatrozida i spajanje na navedeni port pomoću programa `NetCat`. Izvorišni TCP port postavlja se opcijom „`-p`“.

```
[root@t-rex FW]# nc 192.168.0.3 22
(UNKNOWN) [192.168.0.3] 22 (ssh) : Connection refused
```

```
[root@t-rex FW]# nc -p 53 192.168.0.3 22
SSH-1.99-OpenSSH_3.1p1

Protocol mismatch.
[root@t-rex FW]#
```

4.3. Zaobilaženje vatrozida u lokalnoj mreži

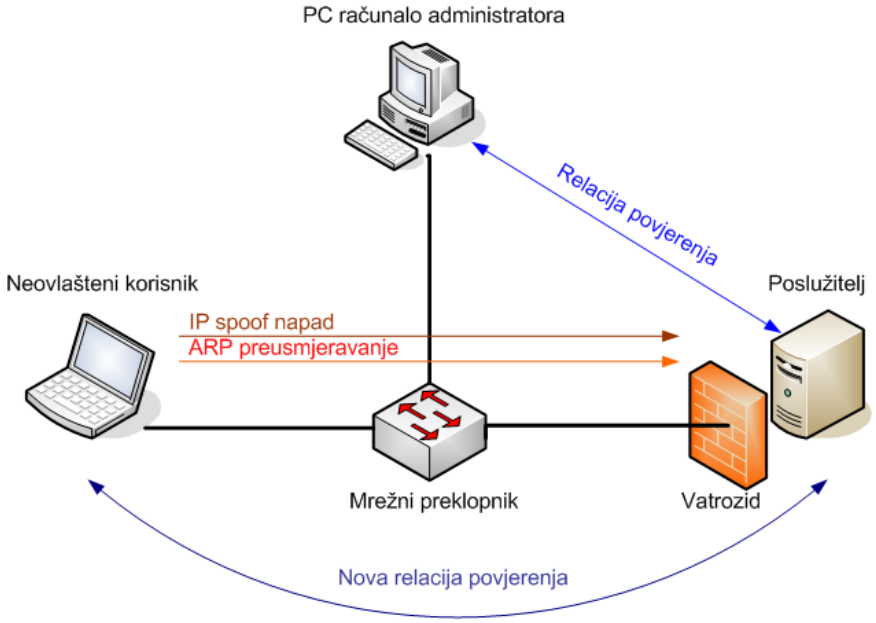
Ukoliko lokalna mreža općenito ima nisku razinu sigurnosti, moguće je uz kombinaciju nekoliko specifičnih tehnika potpuno zaobići vatrozidnu zaštitu. Uvjeti potrebni za potpuno zaobilaženje vatrozida mogu se pronaći u otprilike 70% računalnih mreža. Potpuno zaobilaženje vatrozida moguće je kombinacijom poznatih tehnika napada ARP (*eng. Address Resolution Protocol*) preusmjeravanja (*eng. redirect*) i IP lažiranja (*eng. IP spoofing*). ARP protokol koristi se u `Ethernet` mrežama i služi za razlučivanje MAC (*eng. Media Access Control*) adrese nekog računala na mreži na temelju njegove IP adrese. Da bi računalo u `Ethernet` mreži moglo poslati mrežni paket nekom drugom računalu, ono mora znati MAC adresu mrežnog sučelja na tom drugom računalu. Za otkrivanje MAC adrese nekog drugog računala na mreži, računalo šalje *broadcast* ARP `WHO-HAS` paket u kojem je navedena IP adresa traženog računala svim računalima u tom mrežnom segmentu. Računalo koje ima traženu IP adresu odgovara sa *unicast* ARP `REPLY` paketom i mrežna komunikacija može započeti. Informacije o MAC adresama i pripadajućim IP adresama nalaze se u ARP *cache* tabeli na svakom mrežnom računalu posebno. Problem kod ARP protokola je da taj da ne sadrži nikakvu autentikaciju koja bi osigurala da samo tražena računala odgovaraju na ARP `WHO-HAS` pakete. Računalo koje dobije ARP `REPLY` paket osvježava svoju ARP *cache* tablicu s podacima iz dobivenog paketa, čak i ako ono nije ni slalo ARP `WHO-HAS` paket. Neovlašteni korisnik može bilo kojem računalu u mreži poslati ARP `REPLY` paket kojim će se ARP *cache* tablica osvježiti pogrešnim podacima. Na taj način neovlašteni korisnik ubacuje MAC adresu vlastitog mrežnog sučelja i IP adresu nekog legitimnog računala (npr. poslužitelja). Idući puta kada žrtvino računalo pokuša komunicirati sa poslužiteljem, mrežni paketi će biti poslani na mrežno sučelje neovlaštenog korisnika.

Tehnika lažiranja IP adrese bazira se na slanju IP paketa s izmijenjenom izvorišnom IP adresom u samom zaglavlju paketa, tako da paket izgleda kao da je poslan s nekog drugog računala. IP lažiranje u današnje doba, odnosno na preklapanim mrežama, uglavnom nema smisla ukoliko neovlašteni korisnik nije u mogućnosti praćenja odgovora sa računala na kojeg šalje lažirane pakete Međutim, korištenjem ranije opisane tehnike ARP preusmjeravanja i kod preklapanih mrežama to se može postići.

Navedene tehnike su objašnjene na primjeru lokalne mreže u kojoj su spojena tri računala. Prvo računalo je poslužitelj s osjetljivim podacima na koje zbog konfiguracije vatrozida može pristupiti samo mrežni administrator sa svojeg PC računala. U ovom slučaju je između poslužitelja i administratorskog PC računala uspostavljena tzv. „relacija povjerenja“ (*eng. trust relationship*).

Treće računalo je prijenosno računalo neovlaštenog korisnika koje je s ili bez znanja mrežnog administratora spojeno u preklopnik.

Samo izvođenje napada relativno je jednostavno. Neovlašteni korisnik tehnikom ARP preusmjeravanja ubacuje lažne podatke u poslužiteljsku ARP *cache* tablicu, tako da za IP adresu PC računala mrežnog administratora ubacuje svoju MAC adresu. Svi podaci koji će nadalje biti poslani s poslužitelja prema PC računalu mrežnog administratora završit će na mrežnom sučelju neovlaštenog korisnika. Nakon napada ARP preusmjeravanjem, neovlašteni korisnik šalje lažirane IP pakete, a za izvorišnu IP adresu postavlja adresu administratorskog PC računala. Takvi paketi zbog lažirane izvorišne IP adrese prolaze kroz vatrozid na poslužitelju i otvaraju neovlaštenom korisniku pristup mrežnim servisima tog računala. Zbog prethodno uspješno izvedenog napada ARP preusmjeravanjem, svi odgovori s poslužitelja će, umjesto na legitimno PC računalo mrežnog administratora, biti poslani na mrežno sučelje neovlaštenog korisnika, koji je sada ostvario mrežnu sjednicu sa poslužiteljem iza vatrozida. U prethodnom slučaju vatrozid se nalazi na samom poslužitelju, no napad je na isti način moguće izvesti ukoliko se vatrozid nalazi na posebnom računalu prije poslužitelja. Kompletni prethodno opisani napad i topologija navedene mreže su prikazani na priloženoj slici (Slika 2).



Slika 2: Zaobilaženje vatrozida ARP preusmjeravanjem i IP lažiranjem

4.4. Izlazna ACL pravila temeljena na odredišnom mrežnom portu

Važno je napomenuti da su izlazna ACL pravila većine vatrozida puno labavije definirana od ulaznih, pa ih je samim time i jednostavnije zaobići. Neka mrežna okruženja i postavke vatrozida mrežnim korisnicima onemogućuju korištenje određenih mrežnih servisa izvan lokalne mreže. Vatrozid može biti konfiguriran tako da propušta izlazni promet samo prema određenim servisima. Npr. vatrozid može propuštati izlazni mrežni promet samo prema TCP portovima 80 (HTTP) i 443 (HTTPS), te tako onemogućiti sve servise osim WWW-a. Ukoliko vatrozid analizira mrežni promet samo na temelju odredišnog TCP porta (80 ili 443), takve restrikcije je vrlo lako zaobići. Svaki mrežni servis (npr. FTP, SSH, SMTP) ima svoj standardni mrežni port koji određuje IANA udruga, no određeni mrežni servis ne mora nužno biti na portu koji je određen standardom. Tako se npr. SSH (*eng. Secure Shell*) servis koji se standardno nalazi na TCP portu 22 može pokrenuti i na portu 80. Korisnik s lokalne mreže s prije navedenim mogućnostima pristupa samo WWW servisu može pokrenuti SSH servis na portu 80 na nekom računalu izvan lokalne mreže. Obzirom da vatrozid kontrolira samo mrežni port, a ne sadržaj paketa, korisnik se sada može SSH klijentom spojiti na SSH poslužitelj izvan lokalne mreže. Ovaj način zaobilaženja vatrozida u lokalnoj mreži radi za obične *packet-fiter* vatrozidove koji ne kontroliraju sadržaj paketa upućenih na određene mrežne portove. Moderniji *stateful filter* vatrozidovi koji analiziraju i sam sadržaj mrežnog paketa mogu onemogućiti ovaj način zaobilaženja vatrozida.

4.5. Zaobilaženje vatrozida nakon ostvarenog pristupa unutar mreže

Nakon kompromitiranja računala zaštićenog vatrozidom, preko mrežnog servisa čiji promet vatrozid dopušta ili pomoću nekog malicioznog programa, neovlašteni korisnici uglavnom ostavljaju stražnje ulaze (eng. *backdoor*) koji im omogućavaju daljnji pristup kompromitiranom računalu. Za takve aktivnosti, neovlašteni korisnici često iskorištavaju propuste u ACL pravilima vatrozida. Određeni protokoli koje vatrozid sustavi propuštaju mogu biti iskorišteni za prenošenje malicioznih naredbi kompromitiranom sustavu. Dobar primjer je ICMP protokol koji u normalnim okolnostima služi za prenošenje mrežnih kontrolnih poruka. Neovlaštenom korisniku ICMP protokol može poslužiti za prenošenje određenih naredbi koje će proći vatrozid i doći do kompromitiranog računala na kojem je pokrenut maliciozni program. Prenošenje potencijalno malicioznih podataka pomoću ICMP protokola detaljnije je objašnjeno u dokumentu „*Stražnji ulazi na Linux operacijskim sustavima*“ koji se može pronaći na adresi http://www.cert.hr/filehandler.php?did=97. UDP protokol također se vrlo često

koristi za postavljanje stražnjih ulaza koji prolaze kroz vatrozid. Važno je napomenuti da je nakon kompromitiranja računala iza vatrozida neovlašteni korisnik u mogućnosti zaobići ACL pravila vatrozida na mnogo načina. Legitimni servisi koje vatrozid omogućava također mogu biti iskorišteni za prenošenje malicioznih naredbi kompromitiranom računalu. To npr. može biti specijalno kreirana skripta na HTTP poslužitelju koja dobivene argumente prosljeđuje u korisničku ljusku, `.forward` datoteka koja po primitku određene poruke u *e-mailu* izvršava niz naredbi i sl.

5. Sigurnost *proxy* poslužitelja

Kao što je već ranije spomenuto, *proxy* poslužitelji omogućavaju pristup raznim servisima unutar ili izvan mreže na kojoj su postavljeni. *Proxy* poslužitelji rade na aplikacijskom nivou ISO/OSI referentnog modela. Razni sigurnosni propusti i pogrešne postavke u samim *proxy* poslužiteljima čest su uzrok sigurnosnih incidenata, pa tako *proxy* vatrozid može biti uzrok kompromitiranja određenog računala ili cijele računalne mreže. Pogrešna konfiguracija ACL pravila *proxy* poslužitelja udaljenom neovlaštenom korisniku može omogućiti pristup internoj mreži za koju je poslužitelj postavljen, a slaba ACL pravila korisnicima unutar mreže mogu omogućiti pristup servisima za koje *proxy* poslužitelj nije predviđen. Neovlašteni pristup internoj mreži preko *proxy* poslužitelja uglavnom je rezultat pogrešno definiranih ili uopće nedefiniranih IP adresa kojima je dozvoljeno korištenje *proxy* poslužitelja. Neovlašteni korisnici takve proxy poslužitelje često koriste za kompromitiranje drugih računalnih sustava izvan organizacije na kojoj je on postavljen.

Zbog mogućnosti HTTP protokola da tunelira i druge protokole, korisnici interne mreže koji putem *proxy* poslužitelja pristupaju servisima izvan lokalne mreže mogu pristupati i drugim servisima kao što su FTP, POP3 i SMTP. U nastavku je prikazano tuneliranje FTP protokola preko HTTP *proxy* poslužitelja. *Proxy* poslužitelj se nalazi na IP adresi 192.168.0.2 na portu 8080, dok se računalo s FTP poslužiteljem nalazi na IP adresi 192.168.0.3 na standardnom portu 21.

```
[root@t-rex FW]# nc 192.168.0.2 8080
CONNECT 192.168.0.3:21 HTTP/1.0

HTTP/1.0 200 Connection established
Proxy-agent: tinyproxy/1.4.3

220 ProFTPD 1.2.10 Server (ProFTPD) [192.168.0.3]
USER ljuranic
331 Password required for ljuranic.
PASS xxxxxxxx
230 User ljuranic logged in.
HELP
214-The following commands are recognized (* =>'s unimplemented):
 CWD     XCWD    CDUP    XCUP    SMNT*   QUIT    PORT    PASV
 EPRT    EPSV    ALLO*   RNFR    RNTO    DELE    MDTM    RMD
 XRMD    MKD     XMKD    PWD     XPWD    SIZE    SYST    HELP
 NOOP    FEAT    OPTS    AUTH    CCC*    CONF*   ENC*    MIC*
 PBSZ    PROT    TYPE    STRU    MODE    RETR    STOR    STOU
 APPE    REST    ABOR    USER    PASS    ACCT*   REIN*   LIST
```

Ovim načinom tuneliranja drugih protokola unutar HTTP protokola mrežni korisnici često pristupaju servisima koji im u pravilu nisu dozvoljeni od strane mrežnog administratora.

Za *proxy* poslužitelje karakteristično je da promet koji njima prolazi pohranjuju u privremenu memoriju (*eng. cache*). Kada korisnik zatraži određenu Web stranicu, *proxy* poslužitelj je dohvaća i prosljeđuje korisniku te je istovremeno pohranjuje u privremenu memoriju na određeno vrijeme. Svim sljedećim korisnicima koji zatraže istu stranicu u definiranom vremenskom periodu biti će prikazan sadržaj stranice pohranjen u cache memoriji, a ne onaj originalni na Web poslužitelju. Na taj način *proxy* poslužitelji znatno štede mrežne resurse.

Ukoliko se na zatraženoj Web stranici nalazi ranjiva skripta koja u odgovor ubacuje korisnički unos, postoji mogućnost da neovlašteni korisnik ubaci lažne podatke u privremenu memoriju *proxy* poslužitelja što će utjecati na zahtjeve ostalih korisnika prema toj Web stranici. Radi se o tzv. napadu „dijeljenja odgovora“ (*eng. response splitting*) u kojem neovlašteni korisnik ubacuje određene vrijednosti u samo zaglavlje HTTP odgovora kojim odgovara Web servis na kojem se nalazi zatražena stranica. Iako ova vrsta napada nije problem *proxy* poslužitelja već ranjivih Web skripti, „dijeljenje odgovora“ može biti iskorišteno kao dio napada na korisnike određenog *proxy* poslužitelja. Više o

samom napadu može se saznati na adresi http://www.packetstormsecurity.org/papers/general/whitepaper_httpresponse.pdf.

6. Zaključak

Ispravno implementirani i podešeni vatrozidni sustavi mogu znatno pridonijeti podizanju razine sigurnosti mreže na kojoj su postavljeni. No, isto tako neispravno ili površno podešeni sustavi korisniku pružaju lažni privid sigurnosti, što u nekim slučajevima može predstavljati i veći problem od same nesigurnosti.

S ciljem podizanja razine sigurnosti, korisnicima se preporučuje da sigurnosnu politiku vatrozida definiraju strogo i pažljivo, bez nepotrebnih pretpostavki i dozvoljavanja nepotrebnih mogućnosti pristupa koje bi potencijalno mogle ugroziti sigurnost sustava. Također se preporučuje redovito održavanje i praćenje sigurnosnih upozorenja vezanih uz vatrozid koji se koristi, budući da vrlo često i sam vatrozid može biti meta neovlaštenih korisnika. Za vatrozidne sustave koji se instaliraju na određeni operacijski sustav, iznimno je važno voditi računa o sigurnosnim postavkama sustava na kojem je vatrozid instaliran. Sigurnosni propusti platforme na kojoj je vatrozid postavljen mogu u potpunosti ugroziti sigurnost cijelog sustava bez obzira na kvalitetu i pouzdanost vatrozida.

Prilikom implementacije vatrozidne zaštite također treba voditi računa i o njegovoj vidljivosti s javnog Interneta. Uloga vatrozida je isključivo da štiti internu računalnu mrežu od malicioznih aktivnosti s javnog Interneta i nema potrebe da bude vidljiv korisnicima. Informacije o tipu i inačici vatrozida, servisima, adresama pojedinih sučelja i njegovoj lokaciji potrebno je maksimalno zaštiti, budući da vještom napadaču olakšavaju provođenje malicioznih aktivnosti.

7. Reference

[1] Richard Stevens, *"TCP/IP Illustrated, Volume 1"*

[2] Stuart McClure, Joel Scambray i George Kurtz, "*Hacking Exposed*"

[3] Ed3f, „*Firewall spotting with broken CRC*", http://www.phrack.org/show.php?p=60&a=12.

F4] Nmap, http://www.insecure.org/nmap/