HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Zaštita TCP/IP stoga od SYN napada

CCERT-PUBDOC-2003-10-46

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. SYN NAPADI 4

2.1. USPOSTAVA TCP SPOJA 4
2.2. SYN *FLOOD* NAPADI 5
2.2.1. SYN *spoofing* 5
2.3. CILJEVI SYN NAPADA 6

3. MEHANIZMI ZAŠTITE 6

3.1. PODEŠAVANJE TCP/IP PARAMETARA 6
3.2. MEHANIZAM SYN KOLAČIĆA 7

4. ZAŠTITA OD SYN NAPADA 7

4.1. WINDOWS 2000 7
4.1.1. Ugrađeni mehanizmi zaštite 7
4.1.2. Povećanje dimenzija spremnika 8
4.1.3. Smanjenje vremena rukovanja zahtjevom za uspostavu spoja 8
4.2. LINUX 9
4.2.1. Ugrađeni mehanizmi zaštite 9
4.2.2. Povećanje dimenzija spremnika 9
4.2.3. Smanjenje vremena rukovanja zahtjevom za uspostavu spoja 9
4.3. UNIX 10
4.3.1. Povećanje dimenzija spremnika 10
4.3.2. Smanjenje vremena rukovanja zahtjevom za uspostavu spoja 10

5. ZAKLJUČAK 11

6. REFERENCE 11

1. Uvod

Napadi uskraćivanjem usluge (engl. *DoS – denial of service*) vrlo su popularni u današnje vrijeme. Cilj takvih napada nije krađa informacija ili provaljivanje na udaljeni sustav, već isključivo onemogućivanje sustava u obavljanju svoje funkcije, odnosno pružanja usluga. Najpoznatiji i najuočljiviji takvi napadi su napadi na Web poslužitelje, pošto su oni obično najizloženiji, a istovremeno je njihova moguća neraspoloživost vrlo lako uočljiva. Naravno, DoS napada nisu pošteđeni niti poslužitelji ili uređaji drugih namjena.

Jedna od popularnih metoda izvođenja napada uskraćivanjem usluge jesu SYN napadi. Postoji nekoliko inačica takvih napada, no sve se temelje na sličnim načelima. SYN *flood* napadi se izvode otvaranjem brojnih spojeva (engl. *connection*) prema napadnutom poslužitelju i ostavljanjem tako otvorenih spojeva u SYN RECEIVED stanju, dok se odgovarajući spremnik (engl. *backlog queue*) ne prepuni. Poslužitelj ulazi u SYN RECEIVED stanje kada zaprimi zahtjev za otvaranjem spoja, odnosno paket s postavljenom SYN zastavicom. SYN *flood* napadom otvara se velik broj poluotvorenih spojeva tako da se sustav prepuni i ne može prihvaćati daljnje zahtjeve.

Da bi se SYN *flood* napad učinio još efikasnijim, napadač može lažirati adresu IP izvorišta (engl. *source address*). U tom slučaju napadnuti poslužitelj ne može okončati proces inicijalizacije pošto izvorišna IP adresa nije dostupna. Ovakvi napadi nazivaju se SYN *spoofing* napadi.

U ovom dokumentu biti će opisane neke metode kojima se, više ili manje efikasno, mogu umanjiti problemi koji se pojavljuju prilikom SYN napada. Sve metode koje će biti opisane temelje se na modifikacijama TCP/IP stoga u cilju smanjenja utjecaja SYN napada. Konkretni primjeri će pokazati na koje načine se mogu smanjiti posljedice SYN napada na Windows, Unix i Linux sustavima.

2. SYN napadi

Ovo poglavlje opisuje mehanizme TCP/IP komunikacije na temelju kojih se mogu izvoditi SYN napadi. Da bi se moglo razumjeti kako se izvode SYN napadi potrebno je osnovno razumijevanje TCP/IP stoga protokola, odnosno poznavanje mehanizama uspostave TCP spojeva.

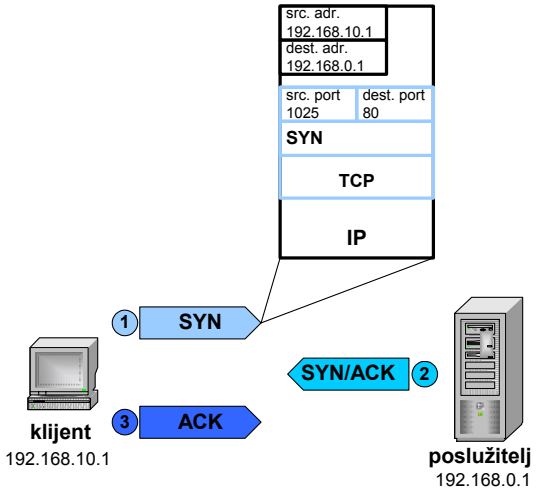
2.1. Uspostava TCP spoja

TCP protokol služi za uspostavu virtualnih spojeva na razini transportnog sloja. Svaki TCP paket posjeduje zaglavlje i podatkovni dio. Zaglavlje TCP paketa sadrži parametre bitne za uspostavu i održavanje spoja, a između ostalog tu su zastavice (engl. *flag bits*) koje specificiraju namjenu svakog paketa. Paket s postavljenom SYN (engl. *synchronize*) zastavicom koristi se pri inicijaciji spoja između pošiljatelja i primatelja, a generira ga pošiljatelj. Paket koji ima postavljenu ACK (engl. *acknowledge*) zastavicu služi kao potvrda primljenih informacija i šalje ga primatelj. Konačno, paket koji ima postavljenu FIN zastavicu (engl. *finish*) koristi se za terminiranje spoja između pošiljatelja i primatelja.

Sama inicijacija, odnosno uspostava TCP spoja, obično zahtjeva razmjenu tri paketa između pošiljatelja i primatelja, a taj postupak se naziva trostruko rukovanje (engl. *three-way handshake*). Slika 1 prikazuje uobičajeni postupak uspostave TCP spoja.

Klijent inicira spoj s poslužiteljem slanjem SYN paketa. U tom paketu specificirani su brojevi portova na klijentskoj (obično neki visoki port – >1023) i poslužiteljskoj strani (npr. port 80 ukoliko se radi o Web poslužitelju). Osim toga, na razini mrežnog sloja, odnosno u IP paketima, moraju biti definirane IP adrese klijenta i poslužitelja.

Kada poslužitelj zaprimi SYN paket na otvorenom TCP portu on odgovara slanjem SYN/ACK paketa. Razlog slanja paketa s postavljenim SYN/ACK zastavicama leži u tome što, unatoč činjenici da su TCP spojevi dvosmjerni, svaki smjer mora biti iniciran i upravljan neovisno. Da bi se izbjeglo slanje dva različita TCP paketa; jedan za potvrdu primljenog paketa, a drugi za otvaranje TCP spoja u drugom smjeru, generira se paket s postavljenim SYN i ACK zastavicama. Brojevi portova i odgovarajuće IP adrese primatelja i pošiljatelja su zamijenjene u odnosu na inicijalno poslani SYN paket. Zaprimanjem takvog paketa klijentu je potvrđeno da postoji (virtualni) put između klijenta i poslužitelja, te da poslužitelj prihvaća uspostavu spoja. U slučaju da poslužitelj ne može prihvatiti spoj, klijentu odgovara slanjem RST/ACK paketa (engl. *reset*) ili ICMP *port unreachable* paketom.

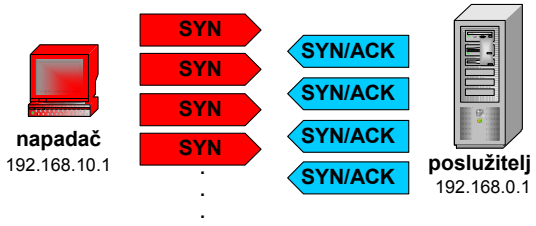


Slika 1: Uspostava TCP spoja

Kada klijent primi poslužiteljski SYN/ACK paket odgovara slanjem ACK paketa poslužitelju. U tom trenutku za klijenta je uspostavljen dvosmjerni TCP spoj i razmjena podataka može započeti. Na isti način poslužitelj primanjem ACK paket koji je poslao klijent smatra TCP spoj uspostavljenim.

2.2. SYN *flood* napadi

SYN *flood* napadi direktna su posljedica nedostataka u samoj implementaciji rukovanja TCP spojem. Nakon što je zaprimio SYN paket, poslužitelj se priprema za uspostavu spoja, odnosno kasnije zaprimanje klijentskog ACK paketa. To podrazumijeva alociranje memorijskih spremnika za slanje i primanje podataka, te pohranu raznih detalja o samom spoju što uključuje klijentsku IP adresu i broj porta. Ukoliko poslužitelj iz nekog razloga, u određenom vremenskom periodu, ne zaprimi klijentski ACK paket, poslužitelj može ponovno poslati SYN/ACK paket pretpostavljajući da paket nije isporučen (Slika 2).

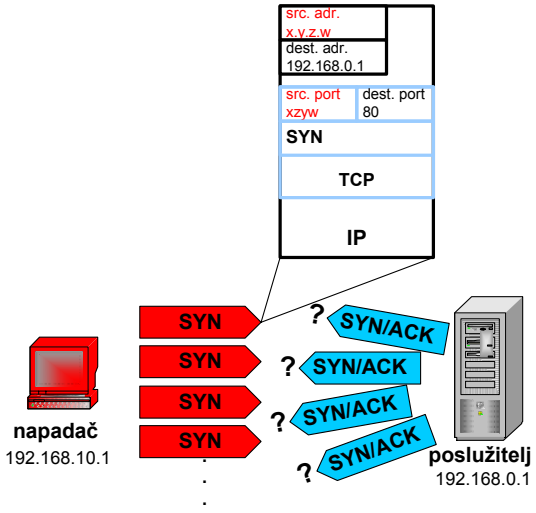


Slika 2: SYN flood napad

Ovdje postaje očigledno da alokacija resursa koju provodi poslužitelj znači da broj poluotvorenih TCP spojeva koje poslužitelj može održavati mora biti ograničen. Zlonamjerni napadač može slanjem velikog broja SYN paketa iskoristiti taj nedostatak i onemogućiti poslužitelj da dalje zaprima SYN zahtjeve. Na taj način poslužitelj je efektivno doveden u DoS stanje, u kojem on uskraćuje usluge drugim klijentima.

2.2.1. SYN *spoofing*

Iskorištavanje nedostataka u uspostavi TCP komunikacije opisano u prethodnom poglavlju može se i unaprijediti korištenjem lažiranih podataka (engl. *spoofing*) u TCP i IP zaglavljima. Zlonamjerni klijent (napadač) može u SYN paketu koji šalje poslužitelju lažirati IP adresu i broj porta. Poslužitelj ponovno alocira nužne resurse i odgovara slanjem SYN/ACK paketa na lažiranu adresu (**Slika 3**).



Slika 3: SYN spoofing

U idealnom slučaju poslužitelj će dobiti RST paket kojim ga druga strana informira da nije zatražila uspostavu spoja, no postoji velika šansa da na tako specificiranoj IP adresi i portu uopće ne postoji računalo odnosno servis. Isto kao i u prethodnom slučaju, poslužitelj nakon nekog vremena ponavlja SYN/ACK paket vjerujući da prethodni paket nije isporučen klijentu. Na taj način, napadač može još efikasnije dovesti poslužitelj do stanja u kojem on više ne može prihvaćati dolazne spojeve.

2.3. Ciljevi SYN napada

SYN napadi mogu se razlikovati prema cilju koji se želi postići. Obzirom na to mogući su SYN (DoS) napadi na poslužitelje (uređaje) ili na komunikacijske kanale (engl. *bandwidth consumption*). SYN napadi na komunikacijske kanale obično se izvode kao distribuirani DoS napadi (engl. DDoS – *distributed denial of service*). Ovakvi napadi često provode se sinkronizirano, s više različitih lokacija, i cilj im je onesposobiti komunikacijski kanal. Za zaštitu i smanjivanje utjecaja takvih napada se koriste metode kao što su npr. filtriranje paketa na usmjerivačima te druge metode koje nisu predmet ovog dokumenta.

SYN napadi na poslužitelje predstavljaju tipičniju vrstu napada i ograničeni su na pojedine poslužitelje (uređaje). Postoji nekoliko vrsta zaštitnih mehanizama ugrađenih u operacijske sustave kojima se može smanjiti utjecaj, a samim time i posljedice takvih napada.

3. Mehanizmi zaštite

Postoje razni mehanizmi zaštite od SYN napada koji su implementirani na razne načine na Windows, Unix i Linux sustavima. Prvi način zaštite moguće je uspostaviti podešavanjem TCP/IP parametara na razini operacijskog sustava. Drugi pristup je korištenje mehanizma SYN kolačića (engl. *SYN cookies*).

3.1. Podešavanje TCP/IP parametara

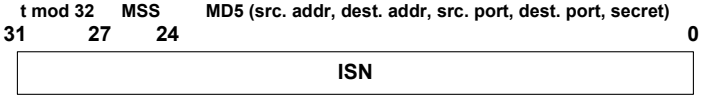
U cilju podizanja otpornosti sustava na SYN napade moguće je podešavati razne parametre TCP/IP stoga. Između ostalog moguće je povećati spremnik za poluotvorene spojeve (u SYN *received* stanju). Na nekim operacijskim sustavima taj spremnik je predefinirano malog kapaciteta i često sami proizvođači preporučaju povećanje veličine spremnika u slučaju SYN napada. Povećanje veličine spremnika zahtijeva dodatne memorijske resurse, što u slučaju nedostatka memorije može imati negativan utjecaj na ukupne performanse sustava.

Također, moguće je smanjiti predefinirani period u kojem se poluotvoreni spojevi zadržavaju u spremniku. To se postiže na dva načina. Prvi način je smanjenje vremenskog perioda ponovnog slanja SYN/ACK paketa, a drugi je smanjenje ukupnog broja slanja SYN/ACK paketa ili kompletno

isključivanje ponovnog slanja paketa. Na ovaj način se ubrzava uklanjanje spojeva u SYN *received* stanju iz spremnika, te se brže otvara prostor za prihvaćanje novih spojeva.
Kod podešavanja ovih parametara treba biti vrlo oprezan pošto postavljanje prevelikih ograničenja može imati utjecaja i na legitimne servise. Ukoliko spomenuti parametri nisu dobro postavljeni, može se dogoditi da poslužitelj počne odbijati i legitimne zahtjeve za uslugom, pogotovo u okruženjima gdje se koriste komunikacijski kanali male propusnosti.

3.2. Mehanizam SYN kolačića

Mehanizam SYN kolačića kreiran je upravo u cilju eliminacije SYN napada. SYN kolačići predstavljaju specifični odabir TCP sekvencijalnih brojeva prilikom iniciranja spoja. U normalnim uvjetima TCP sekvencijalni brojevi, odnosno inicijalni sekvencijalni brojevi (engl. *ISN – initial sequence number*) su pseudoslučajni brojevi koje generira sustav. Kod korištenja mehanizma SYN kolačića taj broj se ne generira na slučajni način već predstavlja *hash* vrijednost funkcije IP adresa odredišta i izvorišta, portova odredišta i izvorišta, te dodatnih (tajnih) parametara.
Slika 4 prikazuje način generiranja SYN kolačića, pri čemu t označava 32-bitni brojač koji se povećava svake 64 sekunde, MSS je enkodirani poslužiteljski MSS (engl. *maximum segment size*) kao odgovor na klijentski MSS, a MD5() je 25bita rezultata MD5 *hash* funkcije nad odredišnim i izvorišnim adresama, portovima i tajno generiranim brojem. Ovi podaci su okvirni, i mogu varirati u raznim implementacijama.



Slika 4: Generiranje SYN kolačića

Prilikom SYN napada sustav na SYN pakete odgovara slanjem SYN/ACK paketa s generiranim SYN kolačićem, unatoč tome da li je spremnik poluotvorenih spojeva pun. Kad poslužitelj zaprimi ACK paket on provjerava vrijednost kolačića, te u slučaju ispravne vrijednosti otvara spoj, bez obzira da li u spremniku poluotvorenih spojeva postoji odgovarajući zapis.
Može se uočiti da mehanizam SYN kolačića uopće ne koristi spremnik poluotvorenih spojeva. Zbog toga i nekih drugih razloga, neki napadaju taj mehanizam tvrdeći da narušava pravila TCP/IP protokola (RFC1323, RFC2018), no bez obzira na to pokazuje se da u praksi može poslužiti kao efikasna metoda zaštite od SYN napada.

4. Zaštita od SYN napada

4.1. Windows 2000

4.1.1. Ugrađeni mehanizmi zaštite

Najvažniji mehanizam zaštite na Windows 2000 (i Windows Server 2003) sustavima jest `SynAttackProtect` parametar. Podešavanjem tog parametra operacijskih sustav može efikasnije obrađivati TCP spojeve. Ovaj parametar moguće je definirati korištenjem `Regedit.exe` alata, odnosno modifikacijom *registry* datoteke tako da se u sljedeći ključ datoteke (engl. *registry key*) doda `SynAttackProtect` vrijednost koju je potrebno definirati kao DWORD tip:

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

Ovaj parametar mijenja ponašanje TCP/IP stoga prilikom detekcije SYN napada. Na taj način operacijski sustav može prihvatiti veći broj SYN zahtjeva. Postavljanjem ovog parametra onemogućuju se neke *socket* opcije, definiraju dodatni intervali za indikaciju spoja i mijenjaju vrijednosti isticanja zahtjeva za uspostavom spoja.
Vrijednost parametra `SynAttackProtect` je moguće postaviti na vrijednost 1 ili 2. Ukoliko je odabrana vrijednost 1 smanjuje se broj ponovnih slanja SYN/ACK paketa, a *cache* zapis se ne kreira dok god se spoj potpuno ne uspostavi. Ako se pak vrijednost parametra postavi na 2, što je i preporučena

vrijednost proizvođača, indikacija spoja *socket* sloju dok se ne dojavljuje dok se ne uspostavi potpuni spoj, odnosno dok se trostruko rukovanje ne obavi uspješno. Tijekom napada, rukovanje spojevima se poboljšava onemogućavanjem nekih parametara koje obično koristi sustav prilikom otvaranja novih spojeva. `TCPInitialRTT` parametar, koji označava vrijeme prvog ponavljanja SYN/ACK paketa, se zanemaruje, a također je onemogućeno definiranje proizvoljnih prozora.
Bitno je naglasiti da podešavanjem `SynAttackProtect` parametra ne mijenja ponašanje sustava u normalnim uvjetima. Zaštita se aktivira tek ukoliko se detektira SYN napad, odnosno ukoliko dođe do prekoračenja vrijednosti parametara opisanih u tablici (Tablica 1). Parametre je potrebno definirati unutar istog *registry* ključa kao i `SynAttackProtect`.

Parametar	Opis	Preporučena vrijednost
`TcpMaxHalfOpen`	maksimalni broj spojeva u SYN RECEIVED stanju koji istovremeno mogu biti prihvaćeni	100 (Windows 2000 Server) 500 (Windows 2000 Advanced Server)
`TcpMaxHalfOpenRetried`	maksimalni broj poluotvorenih spojeva za koje je barem jednom ponovljen SYN/ACK paket	80 (Windows 2000 Server) 400 (Windows 2000 Advanced Server)
`TcpMaxPortsExhausted`	maksimalni broj odbačenih SYN zahtjeva	5

Tablica 1: Parametri za detekciju SYN napada

4.1.2. Povećanje dimenzija spremnika

Osim ranije opisanih parametara `TcpMaxHalfOpen` i `TcpMaxHalfOpenRetried`, broj poluotvorenih spojeva na Windows 2000 sustavima moguće je definirati i podešavanjem dinamičkog spremnika (engl. *dynamic backlog*). Konfiguraciju dinamičkog spremnika moguće je provesti podešavanjem `AFD.SYS` upravljačkog programa. `AFD.SYS` je upravljački program na razini jezgre koji koriste Windows *socket* aplikacije poput FTP-a i Telnet-a. Za podešavanje broja poluotvorenih spojeva `AFD.SYS` definira četiri *registry* vrijednosti koje se mogu podesiti unutar sljedećeg *registry* ključa:

```
HKLM\System\CurrentControlSet\Services\AFD\Parameters
```

Tablica 2 opisuje parametre za podešavanje broja poluotvorenih spojeva.

Parametar	Opis	Preporučena vrijednost
`EnableDynamicBacklog`	maksimalni broj spojeva u SYN RECEIVED stanju koji istovremeno mogu biti prihvaćeni	1
`MinimumDynamicBacklog`	maksimalni broj poluotvorenih spojeva za koje je barem jednom ponovljen SYN/ACK paket	20
`MaximumDynamicBacklog`	maksimalni broj odbačenih SYN zahtjeva	20000
`DynamicBacklogGrowthDelta`	broj slobodnih spojeva koje treba kreirati kada su novi spojevi nužni	10

Tablica 2: Parametri za upravljanje poluotvorenim spojevima

4.1.3. Smanjenje vremena rukovanja zahtjevom za uspostavu spoja

Na Windows 2000 sustavima predefinirano vrijeme za prvo ponavljanje SYN/ACK paketa je 3000 milisekundi (3 sekunde), no ta vrijednost može se proizvoljno podešavati preko parametra `TcpInitialRtt` unutar *registry* datoteke za svako mrežno sučelje. Ukupan broj ponovljenih slanja SYN/ACK paketa također se može podesiti u *registry* datoteci korištenjem parametra

`TcpMaxConnectResponseRetransmissions`. Oba parametra moguće je definirati u sljedećem registry ključu:

```
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

Tablica 3 daje moguće vrijednosti parametra i `TcpMaxConnectResponseRetransmissions` njihovo značenje.

Vrijednost	Vrijeme ponavljanja	Ukupno vrijeme zadržavanja poluotvorenog spoja u spremniku
0	–	3s
1	nakon 3000ms	9s
2	nakon 3000ms i 9000ms	21s
3	nakon 3000ms i 9000ms i 21000ms	45s

Tablica 3: Podešavanje vremena zadržavanja poluotvorenog spoja u spremniku

4.2. Linux

4.2.1. Ugrađeni mehanizmi zaštite

Na RedHat, isto kao i drugim Linux sustavima implementiran je mehanizam zaštite od SYN napada korištenjem SYN kolačića. Mehanizam se aktivira na sljedeći način:

```
# echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

ili

```
# sysctl -w net.ipv4.tcpsyn_cookies=1
```

Ukoliko je potrebno permanentno korištenje SYN kolačića, potrebno je definirati postavljanje ove varijable u nekoj od *startup* datoteka. Isto pravilo vrijedi i za sve ostale varijable opisane u nastavku dokumenta čija vrijednost želi sačuvati i nakon restarta sustava.
Pri tome valja naglasiti da je za funkcioniranje mehanizma SYN kolačića prilikom prevođenja jezgre (engl. *kernel compilation*) potrebno uključiti opciju `CONFIG_SYNCOOKIES`.

4.2.2. Povećanje dimenzija spremnika

Na RedHat Linux sustavima broj poluotvorenih spojeva u spremniku definira varijabla `tcp_max_syn_backlog`. Predefinirani broj poluotvorenih spojeva na RedHat 7.3 sustavima je 256. Podešavanje vrijednosti ove, ali i drugih varijabli moguće je korištenjem `sysctl` ili drugih standardnih naredbi. Vrijednost ovog parametra preporučeno je podesiti na >1024. Sljedeća naredba ilustrira način povećanja dimenzija spremnika.

```
# sysctl -w net.ipv4.tcp_max_syn_backlog="2048"
```

4.2.3. Smanjenje vremena rukovanja zahtjevom za uspostavu spoja

Smanjenje vremena rukovanja zahtjevom za uspostavu spoja postiže se podešavanjem varijable `tcp_synack_retries`. Predefinirana vrijednost na većini Linux sustava je 5 što označava da se poluotvoreni spojevi uklanjaju iz spremnika nakon 3 minute, a maksimalna vrijednost koju parametar može poprimiti je 255. Tablica 4 daje pregled mogućih vrijednosti parametra `tcp_synack_retries` i njihovo značenje.

Vrijednost	Vrijeme ponavljanja	Ukupno vrijeme zadržavanja poluotvorenog spoja u spremniku
1	nakon 3000ms	9s
2	nakon 3000ms i 9000ms	21s
3	nakon 3000ms i 9000ms i 21000ms	45s

Tablica 4: Podešavanje vremena zadržavanja poluotvorenog spoja u spremniku

4.3. Unix

4.3.1. Povećanje dimenzija spremnika

Na Solaris sustavima postoje dva parametra kojima je moguće podešavati dozvoljeni broj spojeva. Jedan parametar (`tcp_conn_req_max_q`) kontrolira broj uspostavljenih spojeva koji čekaju `accept()` poziv od strane aplikacije, a drugi parametar, `tcp_conn_req_max_q0`, definira dozvoljeni broj poluotvorenih spojeva. Predefinirana vrijednost ovog parametra na Solaris 8 sustavima je 1024. Korištenjem `ndd` naredbe vrijednost parametra se može proizvoljno podesiti:

```
# ndd -set /dev/tcp tcp_conn_req_max_q0 2048
```

Na HP-UX sustavima parametar koji definira ukupan broj poluotvorenih spojeva jest `tcp_syn_rcvd_max`, a njegovo podešavanje se izvodi isto kao i na Solaris platformama:

```
# ndd -set /dev/tcp tcp_syn_rcvd_max 2048
```

Predefinirana vrijednost parametra `tcp_syn_rcvd_max` na HP-UX 11.00 sustavima je 500.

4.3.2. Smanjenje vremena rukovanja zahtjevom za uspostavu spoja

Na Solaris sustavima moguće je podešavanje nekoliko parametara koji su vezani uz vrijeme rukovanja zahtjevom za uspostavu spoja. Parametar `tcp_ip_abort_interval` definira maksimalno vrijeme koje poluotvoreni spojevi mogu provesti u spremniku. Predefinirana vrijednost je 8 minuta, a moguće vrijednosti su od 500 milisekundi do 1193 sata. Parametar `tcp_rexmit_interval_initial` definira inicijalno vrijeme ponavljanja SYN/ACK paketa; predefinirana vrijednost je 3 sekunde, a moguće vrijednosti se kreću od 1 milisekunde do 20 sekundi. Konačno, parametri `tcp_rexmit_interval_min` i `tcp_rexmit_interval_max` definiraju minimalna, odnosno maksimalna vremena ponavljanja SYN/ACK paketa. Promjene tih parametara moraju biti međusobno pažljivo usklađene jer u suprotnom može doći do poteškoća u radu sustava. Proizvođač preporuča da vrijednost parametra `tcp_ip_abort_interval` bude barem četiri puta veća od vrijednosti parametra `tcp_rexmit_interval_max`, čija vrijednost treba pak biti barem osam puta veća od vrijednosti parametra `tcp_rexmit_interval_min`.

Na HP-UX sustavima vrijeme rukovanja zahtjevom za uspostavu spoja može se kontrolirati korištenjem `tcp_ip_abort_cinterval` parametra. Korištenjem `ndd` naredbe moguće je podesiti maksimalno vrijeme koliko će poluotvoreni spoj biti u spremniku. Tablica 5 daje pregled vrijednosti parametra `tcp_ip_abort_cinterval` i njihovo značenje.

Vrijednost	Vrijeme ponavljanja	Ukupno vrijeme zadržavanja poluotvorenog spoja u spremniku
1000	-	1s
5000	nakon 2s	5s
10000	nakon 2s i 5s	10s
60000	nakon 2s, 5s, 11s, 23s i 47s	60s

Tablica 5: Podešavanje vremena zadržavanja poluotvorenog spoja u spremniku

Moguće je i ručno podešavanje vremena prvog ponavljanja korištenjem parametra `tcp_rexmit_interval_initial`, te podešavanje sljedećih ponavljanja parametrima `tcp_rexmit_interval` i `tcp_rexmit_interval_min`.

5. Zaključak

SYN napadi mogu usporiti, pa i potpuno onemogućiti rad sustava. U ovom dokumentu opisane su osnovne tehnike i ciljevi SYN napada, a također su pokazani načini na koje se specifični sustavi mogu djelomično zaštititi od ovakvih napada.

Zaštitu od SYN napada, odnosno DoS napada na komunikacijske kanale nije moguće unaprijediti korištenjem metoda opisanih u ovom dokumentu, no zato je razinu otpornosti pojedinih poslužitelja moguće efikasno podesiti korištenjem spomenutih metoda i ugađanjem navedenih parametara.

Uz standardne metode filtriranja TCP/IP prometa na vatrozidima i usmjerivačima, postupke opisane u ovom dokumentu svakako bi trebalo implementirati na sustavima koji su potencijalno izloženi SYN napadima, no isto tako ih je preporučljivo implementirati i na bilo kojem sustavu kojem se želi podići opća razina sigurnosti. Pri tome uvijek treba biti oprezan da se krivo postavljenim vrijednostima parametara TCP/IP stoga ne bi narušile performanse sustava.

6. Reference

Distributed Reflection Denial of Service, http://grc.com/dos/drdos.htm,

SYN cookies, http://cr.yp.to/syncookies.html,

Hardening the TCP/IP stack to SYN attacks, http://www.securityfocus.com/infocus/1729,

Protecting Against Network DoS Attacks, http://security.uchicago.edu/seminars/DDoS/netprot.shtml,

UNIX IP Stack Tuning Guide v2.7, http://www.cymru.com/Documents/ip-stack-tuning.html,

Sun Product Documentation, http://docs.sun.com/db,

Microsoft Windows 2000 TCP/IP Implementation Details, http://www.microsoft.com/technet/itsolutions/network/deploy/depovg/tcpip2k.asp,

HOW TO: Harden the TCP/IP Stack Against Denial of Service Attacks in Windows 2000, http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315669&sd=tech.