Tallinna Tehnikaülikool
Informaatikainstituut

TCP/IP protokollil baseeruvad rünnakud võrguseadmete vastu

Referaat õppeaines
Kommunikatsioonivõrgud (rakenduslik käsitlus)
IDK3070

Koostaja : Erki Suurjaak
Õpperühm : LAP52
Matrikkel : 970772

Tallinn 1999

Sisukord

Sissejuhatus

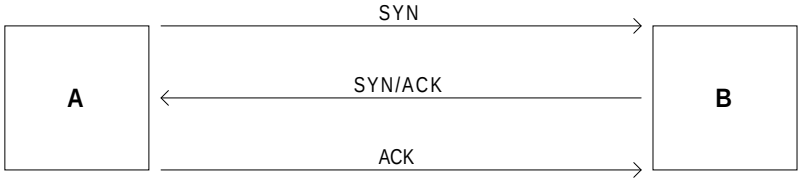
Käesolevas referaadis käsitletakse mõningaid transpordi- ja võrgukihil põhinevaid rünnakuviise võrku ühendatud seadmete (enamjuhul siis arvutite) vastu. Kuigi praeguseks ajaks peaks tsiviliseeritud maailmas enamus alljärgnevatest rünnakuviisidest tõkestatud olema, ei ole neid siiski soovitav järele proovida.

Denial of service

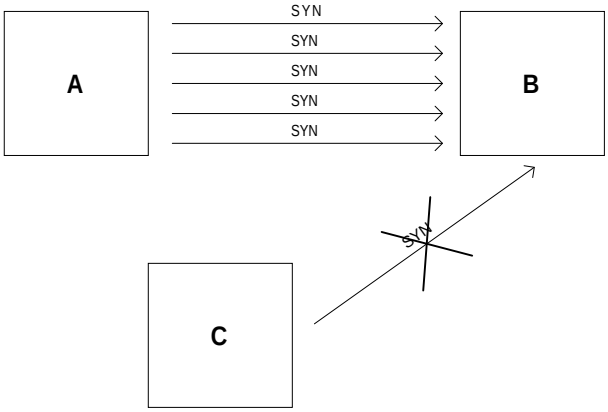
Denial of service on see, kui mingi võrguseade võrgule kättesaamatuks muudetakse, vastavat seadet kas kokku jooksutades või muul viisil ühendust häirides.

SYN-uputus

SYN-uputus (*SYN flood*) põhineb võrgukihi kolmeastmelisel ühenduse loomisel. Ühenduse soovija A saadab B-le *SYN*-paketi, andes märku oma soovist ühendus luua. B vastab *SYN/ACK*-paketiga, millele A saadab vastu *ACK*-paketi. Kui B *ACK*-i kätte saab, on ühendus loodud.



Antud ühenduse loomise viisi võiks võrrelda sellega, kui kodanik N hüüaks kodanik M-ile "Kuule, sina!". Kodanik M küsiks "Kes, mina?". Kodanik N vastaks "Jah, sina." Ja sellega on ühendus kahe kodaniku vahel loodud.



Kui nüüd aga ühenduse looja A enam B poolt saadetud *SYN/ACK*-ile *ACK*-i vastu ei saada, siis jääb B ootama. Ning et igal võrguseadmel on fikseeritud arv poolavatud ühendusi (ühendusi, millel ühenduse loomine pole veel lõppenud), siis niikaua, kuni A-ga pole ühenduse loomine lõpetatud, on B-l üks ressursiosa hõivatud.

Üldjuhul pole sellest hullu, sest ühendus luuakse millisekundites. Et aga võrgus võib ette tulla juhuslikke ummikuid, siis on poolavatud ühendustel üsnagi pikk aegumisaeg - erinevatel süsteemidel oli see algselt 1-3 minutit, *Linuxi* masinatel isegi kuni 20 minutit (*Linuxil* oli kunagi probleeme transpordikihi taimeriga). Kui nüüd võrgus on kasvõi üks pahatahtlik võrguseade, mis saadab igas sekundis B-le 100-200 *SYN*-i, iga paketi kohta võltsides suvalise lähte-IP-aadressi, siis saavad B poolavatud ühenduste puhvrid üsnagi kiiresti täis, ning ühelgi teisel masinal pole võimalik B-ga ühendust saada.

Näide *SYN*-uputuse kohta : 1996. aastal pommitas keegi pahatahtlik inimene *SYN*-pakettidega firma *Panix* serverit viis päeva järjest, mille jooksul oli *Panix* muust maailmast täiesti ära lõigatud - ükski masin ei saanud *Panixiga* ühendust, samuti ei liikunud e-post. Kui rünnak oleks veel jätkunud, oleks *Panix* võinud pankrotti minna.

Antud näide avaldas mõju ainult ühele arvutile. Kui aga keegi pommitaks *SYN*-pakettidega mingeid tähtsaid servereid - näiteks suuremaid domeeninimeservereid (*DNS*-e), on võimalik veebiühendusi tugevalt häirida - inimesed peaksid siis opereerima IP-aadresside kaudu (mida üldjuhul kellelgi peas ei ole), sest nimeserver ei suuda nime IP-aadressiks tõlkida - ta on hõivatud.

SYN-rünnakute vastu efektiivset kaitset ei ole. Üks asi, mida võib teha (ja on ka tehtud), on seada poolavatud ühenduste maksimaalset arvu suuremaks (algselt oli see üldjuhul vähem kui sada; soovitav oleks vähemalt 1024) ning aegumisaega väiksemaks (umbes 30 sekundi peale). See leevendab mõneti probleemi, aga kaitset taoliste rünnakute vastu ei anna. Näiteks kräkkimiseks ülespandud *Linuxi* arvuti (asus kunagi aadressil crack.linuxpcc.com) pidas *SYN*-rünnakutele vastu ainult kuus päeva.

Samuti on igal alamvõrgu administraatoril soovitav konfigureerida oma võrguosa lüüs laia maailma selliselt, et see ei laseks läbi pakette, mille lähte-IP-aadress ei kuulu antud alamvõrku. Sedasi saab garanteerida, et vähemalt antud võrguosast ei tule *SYN*-rünnakuid.

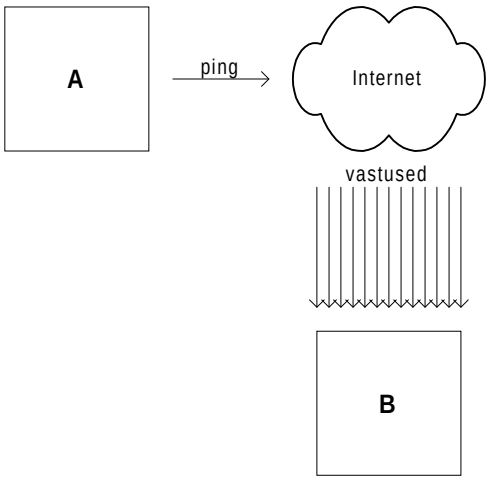
Land-rünnak

Land-rünnak (*land.c* oli algse programmi nimi, mida levitati 1997. aastal ja millega sai antud rünnakut tekitada) on oma olemuselt samuti *SYN*-rünnak, ainult selle vahega, et *SYN*-paketi lähte-IP-aadress võltsitakse adressaadi enda IP-aadressiks, pannes niiviisi võrguseadet iseendaga rääkima. Üllatavalt paljud operatsioonisüsteemid (*BeOS, FreeBSD 3.0, IRIX 5.2, Windowsi* perekond, ..) ja võrguseadmed (*Apple LaserWriter*, mitmed *Cisco* ruuterid, ..) olid *land*-rünnaku suhtes haavatavad. Mõned isegi hangusid (*Windows95*).

Land-rünnaku vastu on kaitset kerge implementeerida - tuleb lihtsalt välja filtreerida halva lähte-IP-aadressiga paketid. Ja alamvõrkude lüüsid on viisakas konfigureerida nii, et ei lasta läbi pakette, mille lähte-IP-aadress ei kuulu antud alamvõrku.

Smurf-rünnak

Smurf-rünnak ei tee iseenesest midagi kurja, ta ainult ummistab süsteemi mõttetute pakettidega. Rünnaku põhimõte - A saadab välja mitme alamvõrgu leviaadressiga (*broadcast*) *ping*-paketi (*ICMP echo*). Paketi lähte-IP-aadress on võltsitud B nimele. Adresseeritud alamvõrgud vastavad *ping*ile, sedaviisi ummistades nii enda võrku kui ka B-d.



Smurf-rünnaku vastu saab alamvõrke kaitsta nii, et lüüsist ei lubata sisse leviaadressiga pakette. Samuti on viisakas mitte lubada lüüsil väljapoole saata leviaadressiga pakette.

UDP-uputus

UDP-uputus (*UDP flood*) hõlmab kaht süsteemi. Pahatahtlik süsteem C seob, enda poolt saadetud pakettide lähte-IP-aadressi võltsides, süsteemi B *UDP* (*User Datagram Protocol*) teenuse *chargen* (*character-generating service*, saadab iga vastuvõetud paketi kohta mingi jada sümboleid) ja süsteemi A *UDP* teenuse *echo* (saadab tagasi iga vastuvõetud sümboli), sedaviisi pannes kaks süsteemi omavahel mõttetut informatsiooni vahetama.

UDP-uputuse vastu mingit korralikku kaitset ei ole.Võib keelata alamvõrgu lüüsil lasta sissepoole *UDP* teenuse soove.

Surmaping

Surma*ping* (*ping of death*) põhineb sellel, et paljud süsteemid on haavatavad lubatud suurusest suurema paketiga. *RFC-791* seab IP-pakettide maksimumsuuruseks 65535 baiti. Kui aga fragmenteerida *ping*-pakett nii, et fragmente tervikuks liites tuleb paketi suurus üle 2^{16} baidi, siis mitmed süsteemid kas annavad veateate (*HP3000 MPE/iX, Windows 3.11 with Trumpet Winsock*), hanguvad (*Minix, Convex*

SPP-UX, *Apple Mac*, *Windows95*-e perekond), teevad alglaadimise (*Solaris 2.4*) või veel midagi muud.

Surma*ping*i vastu ainus korralik lahendus on operatsioonisüsteemi parandamine - alamvõrgu lüüsis ping-pakettide keelamine on ajutine lahendus, sest antud probleem ei puuduta ainult *ping*i, vaid kõike, mis IP-paketti kasutab.

Teardrop-rünnak

Teardrop-rünnak (*teardrop.c* oli algse programmi nimi, mida levitati 1997. aastal ja millega sai rünnakut sooritada) kasutab ära operatsioonisüsteemi viga - mitmed operatsioonisüsteemid (*Linux, Windowsi* perekond) ei kontrolli IP-pakettide defragmenteerimisel valesid fragmendiväärtusi, mistõttu, kui fragmendiväärtused on valitud nii, et fragmendisuurus kokku tuleb väiksem kui null, siis üritab operatsioonisüsteem kopeerida liiga palju informatsiooni, mille tulemusena operatsioonisüsteem võib hanguda või alglaadimise teha.

Teardrop-rünnaku vastu ainus mõistlik kaitse on parandatud operatsioonisüsteem.

IP-fragmenteerimise rünnak

Antud rünnak kasutab ära seda, et IP-pakette on võimalik fragmenteerida, kui pakett on liiga suur alumise OSI kihi jaoks. Rünnak võimaldab mööda pääseda alamvõrgu tulemüürist.

Üliväikese fragmendi rünnak

IP-paketi fragment valitakse nii väike, et transpordikihi päis poolitatakse kahe fragmendi vahel nii, et transpordikihi pordi number jääb teise fragmenti.

Alamvõrgu tulemüür ei defragmenteeri pakette ise, vaid saadab need edasi lõppvastuvõtjale, kes fragmendid kokku paneb. Kui tulemüür on pandud mingeid konkreetseid porte tõkestama, siis niiviisi on võimalik sellest võimalik pääseda.

Fragmendi ülekattumise rünnak

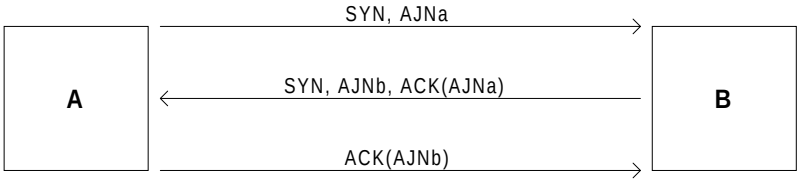
Antud rünnaku eesmärk on analoogne eelmisega, selle vahega, et esimeses fragmendis on mingi lubatud port (näiteks 80, veeb) ja teises fragmendis on mingi

keelatud port (näiteks 23, *telnet*). Teise fragmendi nihe (*offset*) on valitud nii, et esimeses fragmendis olev pordinumber 80 kirjutatakse üle pordinumbriga 23.

TCP/IP võltsimine

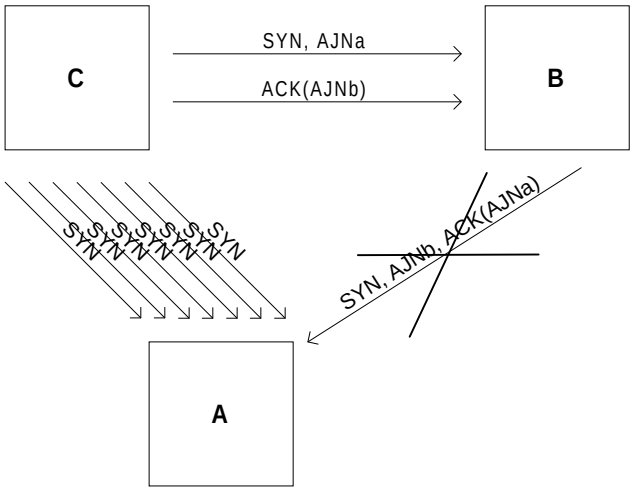
Antud rünnakus kasutatakse ära seda, et paljud süsteemid on konfigureeritud usaldama teatud konkreetseid süsteeme ja aktsepteerima nendelt süsteemidelt tulevaid ühendusi.

Näide ühenduse loomise kohta A ja B vahel :



A saadab B-le ühendusesoovi, algse järjekorranumbriga (AJN) *a*. B saadab samuti ühendusesoovi, algse järjekorranumbriga *b*, kviteerides järjekorranumbrit *a*. A saadab kviteeringu järjekorranumbriga *b*.

Rünnak näeb välja järgmiselt : pahatahtlik ründaja C saadab usaldatud süsteemi A nimel süsteemile B ühendusesoovi (*SYN*-paketi), algse järjekorranumbriga *a*. Samal ajal pahatahtlik C ründab usaldatud süsteemi A *SYN*-uputusega - vastasel juhul, kui A saab B-lt kviteeringu paketile, mida A ei ole



saatnud, siis A taipab, et midagi on korrast ära, ja saadab B-le *RST*-paketi, loodavat ühendust katkestades. Kui nüüd B saadab süsteemile A *SYN/ACK*-paketi, algse järjekorranumbriga *b*, siis A ei ole võimeline sellele reageerima, sest ta on juba *SYN*-pakettidest üle ujutatud. A asemel saadab ründaja C *ACK*-paketi

järjekorranumbriga *b* süsteemile B, jällegi usaldatud süsteemi A nimel. Ja sellega ongi C-lt loodud ühendus B, kus tal on usaldatud süsteemi A õigused.

Ründaja C saab järjekorranumbri *b* teada järgmiselt :

- võtab kümnest ühendusest statistilise keskmise
- paljud süsteemid valivad uue järjekorranumbri kindla korra järgi. Kui nüüd C loob mingi legitiimse ühenduse B-ga ja saab teada B poolt antud

järjekorranumbri selle ühenduse jaoks, siis võib ta üsna kindlalt oletada, milline järjekorranumber valitakse järgmise ühenduse jaoks.

Selle rünnaku moraal on see, et usaldatud süsteemide olemasolu on suur turvarisk. Ainus aktsepteeritav usaldatavus on krüpteeritud ühenduste loomine.

Kokkuvõte

Nagu näha, on TCP/IP protokolli kasutavad võrguseadmed üllatavalt haavatavad mitmesuguste rünnakute poolt. Ainus korralik võimalus turvalisuse saavutamiseks on implementeerida kõikjal piisaval määral paranoiat - mitte kedagi usaldada, mitte midagi eeldada ja igale võrku ühendatud seadmele sättida peale selline turva, nagu hakataks seda seadet iga päev ründama. Sest Internetis ei ole kaitsmata seadme puhul juttu sellest, KAS rünnatakse, vaid MILLAL rünnatakse, nagu üsna paljud firmad on oma kurbuseks tõdenud.

Kasutatud kirjandus

1. *Denial of Service on the Internet*, http://www.info-sec.com/denial/infosece.html-ssi
2. *Ping of Death*, http://www.insecure.org/sploits/ping-o-death.html
3. *The LAND attack (IP DOS)*, http://www.insecure.org/sploits/land.ip.DOS.html
4. *Linux and Windows IP fragmentation (Teardrop) bug*, http://www.insecure.org/sploits/linux.fragmentation.teardrop.html
5. *RFC-791*
6. Dr. Bill Hancock *Securing the Firewall*
7. *Firewall Attacks*
8. Steve Bellovin *Sequence Attack*, ftp://ftp.research.att.com/dist/internet_security/seqattack.txt
9. *IP Spoofing*, http://home.earthlink.net/~gitan617/ipspoof.html