TARTU ÜLIKOOL

MATEMAATIKA-INFORMAATIKATEADUSKOND

Arvutiteaduste instituut

Informaatika eriala

Erki Vaino

Teenusetõkestusründed ja kaitse lahendused

Bakalaureusetöö (6 EAP)

Juhendaja: Meelis Roos

Autor: ……... „……“ jaanuar 2015

Juhendaja: ……... „……“ jaanuar 2015

Lubada kaitsmisele

Professor: ……... „……“ mai 2015

TARTU 2015

Teenusetõkestusründed ja kaitse lahendused

Teenusetõkestusründed on aja jooksul muutunud üha keerulisemaks ning populaarsemaks ründajate seas. Kuna hetkel puuduvad head materjalid eesti keeles selle teema kohta, siis selle tööga tuuakse välja üldist infot teenusetõekestusrünnakute kohta: mis põhjusel neid tehakse ja kuidas saab neid klassifitseerida. Põhirõhk on erinevate rünnakute kirjeldustel ehk täpsemalt: kuidas nad töötavad ja milliseid nõrkuseid nad ära kasutavad. Töö teises osas on välja toodud lahendusi, kuidas peatatakse rünnakud või kuidas saab nende mõju vähendada. Viimasena on välja toodud erinevate firmade riistvaralisi ja tarkvaralisi lahendusi ja antud igast lahendusest lühiülevaade.

Märksõnad:

Teenusetõkestusrünne, hajus ummistusrünne, kaitselahendused, rünnete mõju vähendamine, rünnete klassifitseerimine, veebiserver, LAND, Christmas tree, Teardrop, Ping of Death, ROSE, New dawn, Smurf attack, Fraggle, DNS, UDP, SSL, HTTP, Slowloris, RUDY, Socetstress, HashDos, Cisco systems, F5 Networks, CloudFlare, Check Point, Radware, Arbor Networks.

Denial of Service Attacks and Defense Solutions

Over time denial of service attacks have become more sophisticated and a popular method amongst attackers. This document will provide overview of different attacks and defense solutions against them. Although there are many great resources about the subject in English, there are very few of them in Estonian. Firstly there is a general overview of the attacks how they can be classified. Then descriptions of how different attacks work and which vulnerabilities or mechanics they use to stop the victim for providing service. In the last part there are descriptions how these attacks can be stopped or mitigated and also which products and solutions companies currently provide on the market at the moment. Each product is described briefly and info given how it helps to protect the network.

Keywords:

Denial of service attack (DoS), distributed denial of service attack (DDoS), classification of attacks, mitigating attacks, LAND, Christmas tree, Teardrop, Ping of Death, ROSE, New dawn, Smurf attack, Fraggle, DNS, UDP, SSL, HTTP, Slowloris, RUDY, Socetstress, HashDos, Cisco systems, F5 Networks, CloudFlare, Check Point, Radware, Arbor Networks.

Sisukord

Sissejuhatus

Viimastel aastatel on teenusetõkestusründed muutunud üha tavalisemaks nähtuseks. Suurimad ründed on ületanud juba 100 Gbps piiri ja on igapäevased nähtused. Eestis jäävad tavaliselt märgatavad ründed 1-10GBbps suurusjärku (Vt. Lisa 1). Lisaks on välja arendatud ründeid, mis ei vaja kahju tekitamiseks suurt mahtu ja mida saab teostada tavalise sülearvutiga, kasutades ära viga protokollis või süsteemis. Igale võrguadministraatorile on oluline, et ta tunneks erinevaid ründeid ja oskaks neile vastavalt reageerida.

Tegemist on referatiivse tööga, kus kasutatakse ründe- ja kaitsemeetodite jaotamiseks raamatut „Network Security“ ning rünnete täpsemaks kirjeldamiseks erinevaid materjale, mis on Internetis vabalt kättesaadavad. Töö teema sai valitud, kuna teenusetõkestusrünnakute kohta on eesti keeles vähe materjali ja puudub ülevaatlik uurimus erinevatest rünnakutest ja kaitselahendustest. Lisa 1 all on ka intervjuu kahe spetsialistiga, kes jagasid oma teadmisi.

Töö on suunatud Tartu Ülikooli matemaatika-informaatika tudengitele ja inimestele, kes soovivad laiendada oma silmaringi teenusetõkestusrünnete osas. Töö eesmärk on eesti keeles tuua välja erinevate rünnete liigid ja kuidas neid kasutatakse. Lisaks ka erinevad meetodid, mida saab kasutada kaitsmiseks ning milliseid tooteid on loodud erinevate firmade poolt rünnete mõju vähendamiseks.

Esimeses peatükis on kirjeldatud teenusetõkestusründeid üldiselt: kuidas neid saab jaotada ja üldised tunnusjooned. Järgnevas neljas peatükis on kirjeldatud erinevaid ründeid vastavalt sellele, millist nõrkust nad efekti saavutamiseks ära kasutavad. Viimases peatükis kirjeldatakse meetodeid, kuidas on rünnete eest võimalik kaitsta. Lisaks on välja toodud ka erinevate firmade tarkvaralised ja riistvaralised lahendused teenusetõkestusrünnete peatamiseks. Töö praktilise osana viisin läbi kaks intervjuud inimestega, kes jagasid oma teadmisi rünnakute kohta - küsimused ja vastused on näha Lisa 1 all.

1. Teenusetõkestusrünnetest üldiselt

Teenusetõkestusrünneteks loetakse tegevust, kus pahatahtlik kasutaja sihilikult blokeerib arvutisüsteemi või võrgu ressursse niimoodi, et teised kasutajad ei saa neid kasutada. Sellised ründed on muutunud Internetis väga populaarseks ja neid kasutatakse iga päev pankade, firmade ja riigiasutuste vastu.

Ründe idee seisneb selles, et tarvitatakse ära erinevad ressursid, näiteks protsessori jõudlus, vahemälu, võrgu läbilaskevõime ning veebiserveri ühendused, nii et teised kasutajad ei saa enam ohvri pakutavaid teenuseid kasutada.

Peamised ründajate motiivid on raha väljanõudmine, poliitiline vastuseis ja *online* protesteerimine (Vt. Lisa 1). Teenusetõkestusründed on muutunud tavaliseks mooduseks, mille abil pressitakse raha välja. Näiteks: organisatsioonile saadetakse kiri, milles öeldakse, et kui nad ei kanna raha ründaja kontole, siis võetakse firma pakutav teenus maha, põhjustades sellega suuremat finantsilist kahju kui see, mida ründaja nõuab.

Näide poliitilisest vastuseisust on 2007. aastal toimunud pronksiöö, pärast mida sattusid Eesti riigiasutuste, pankade ja uudisteportaalide leheküljed teenusetõkestusrünnete alla. Selle tulemusena oli nende veebilehtede külastamine ja kasutamine häiritud.

Lisaks on viimastel aastatel levima hakanud ka *online* protesteerimine. Rühmitus Anonymous on läbi viinud suuri ründeid selliste firmade vastu nagu MasterCard, PayPal, Visa ja Amazon. Nad protesteerisid selle vastu, et antud organisatsioonid lõpetasid WikiLeaksi toetamise. Selle ründe eripäraks oli see, et mitmed tuhanded inimesed osalesid selles vabatahtlikult, väljendades sellega oma meelepaha.

Eraldi tooks välja väga populaarse teenusetõkestuse ründe liigi - hajusad teenusetõkestusrünnakud (*Distributed Denial of Dervice*) [1]. Nendega saab põhjustada suurt kahju võrkudele ja organisatsioonidele. Üks võimalus hajusaks teenusetõkestusründeks on kasutada robotvõrke, mis koosnevad mitmetest tuhandetest arvutitest. Teine lahendus rünnete võimendamiseks on kasutada ära kolmandatele osapooltele kuuluvaid nõrkusega võrke ja süsteeme.

1.1 Rünnete klassifitseerimine

Ründeid saab jaotada erinevatel viisidel ja siinkohal ongi välja toodud peamised klassifikatsioonid.

Üks võimalikest viisidest jaotada on vastavalt rünnaku protokolli tasemele.

- Võrguseadme tasemel ründed tarbivad ära võrguseadme vabad ressursid või kasutavad ära vigu seadme tarkvaras.
- Operatsioonisüsteemi tasemel ründed kasutavad ära selle, kuidas süsteemid protokolle realiseerivad, näiteks Ping of Death.
- Rakenduse tasemel ründed kasutavad ära nõrkusi rakendustes, põhjustades ohvri ressursside väärkasutamist. Teine võimalus on leida suure algoritmilise keerukusega viga rakendusest.
- Andmete ummistusrünnete korral saadetakse võimalikult palju andmeid ohvri võrku, kasutades sellega ära kogu vaba ribalaiuse. Parimateks näideteks on Smurf ja Fraggle rünnakud.
- Protokolli omaduse rünnete korral kasutatakse ära kindlat protokolli omadust. Kõige lihtsam näide on IP-aadressi võltsimine.

Hajusaid teenusetõkestusründeid saab jaotada ründe intensiivsuse järgi [2]:

- Pideva vooga rünne
- Muutuva vooga rünne
    - Kasvavad
    - Kõikuvad

Pideva vooga ründe puhul kasutab ründaja kõiki oma ressursse, et tekitada koheselt võimalikult palju kahju. Selle meetodi miinuseks on see, et ohver saab rünnakust kiiresti teada ja saab koheselt reageerida. Kasvava võimsusega ründe puhul alustatakse aeglaselt, püüdes jääda märkamatuks võimalikult kauaks ja aja jooksul suurendatakse võimsust, kasutades ära kõik vabad ressursid. Kõikuva võimusega rünnete puhul muudab ründaja võimsust vastavalt sellele, kuidas ohver reageerib: hoides võimsust madalana, jäädes nii märkamatuks või suurendades võimsust, et tarbida võimalikult palju vabu ressursse. Selle kontrollimine nõuab head arusaama ohvri süsteemist. Korralikult teostatud rünnaku puhul võib rünnak jääda märkamatuks kauaks ajaks.

Võib ka jaotada vastavalt sellele, kuidas ründaja kontrollib ründeseadmeid hajusate rünnete korral.

- Manuaalne
- Poolautomaatne
    - Otsene
    - Kaudne
- Täisautomaatne

Varem pidi ründaja otsima endale sobivad masinad, murdma neisse sisse ja seadistama manuaalselt ründekoodi ja sealt seda käivitama. Poolautomaatsete rünnete korral on ründajal olemas vahelüli tema ja rünnet teostavate seadmete vahel. Otsese suhtluse korral peavad ründaja ja vahelüli üksteist teadma. Sellisel juhul on tavaliselt vahelülidel teada ründaja IP-aadress. Peamine probleem on see, et kui tuvastatakse vahelüli, siis on kergem tuvastada ründajat. Kaudse suhtluse korral on ründaja tuvastamine keerulisem, sest otsest suhtlust ei toimu. Üks näide sellest on IRC serverite kasutamine, eesmärgiga kontrollida rünnakuid. Täisautomaatse ründe korral ei pea olema suhtlust ründaja ja ründeseadme vahel, mis vähendab riski vahele jääda. Ründe meetod, kestvus ja ohver seadistatakse eelnevalt ja enamasti on tegemist ühe käsuga. Sellised ründed on aga üsnagi piiratud.

Ründe mõju ohvrile saab jaotata ründed kaheks. Esimene on täielik segav mõju, mille tulemusena tekib ohvril koheselt teenusetõkestus. Teine võimalus on häirida teenuste pakkumist aeglasemalt, vältides sellega kohest ründe avastamist ohvri poolt.

Viimane rünnete jaotamise viis on vastavalt sellele, millist nõrkust ära kasutatakse [2]:

- Vigaste pakettide ründed
- Ummistusründed
- Võimendusründed
- Ründed, mis kasutavad ära nõrkusi protokollis

Vigaste pakettide rünnete korral valmistab ründaja spetsiaalseid pakette, mis põhjustavad ohvrisüsteemide hangumist ja kokku jooksmist. Ummistusrünnete korral saadetakse ohvrile

võimalikult palju andmeid, nii et kasutatakse ära kogu vaba ribalaius. Võimendusrünnete korral kasutatakse peegeldajaid, et võimendada rünnakut kordades suuremaks. Lisaks veel ründed, mis kasutavad nõrkusi protokollides. Selle jaotumise järgi on antud töö üles ehitatud: igas peatükis on kirjas erinevad ründed ja nende täpsem kirjeldus.

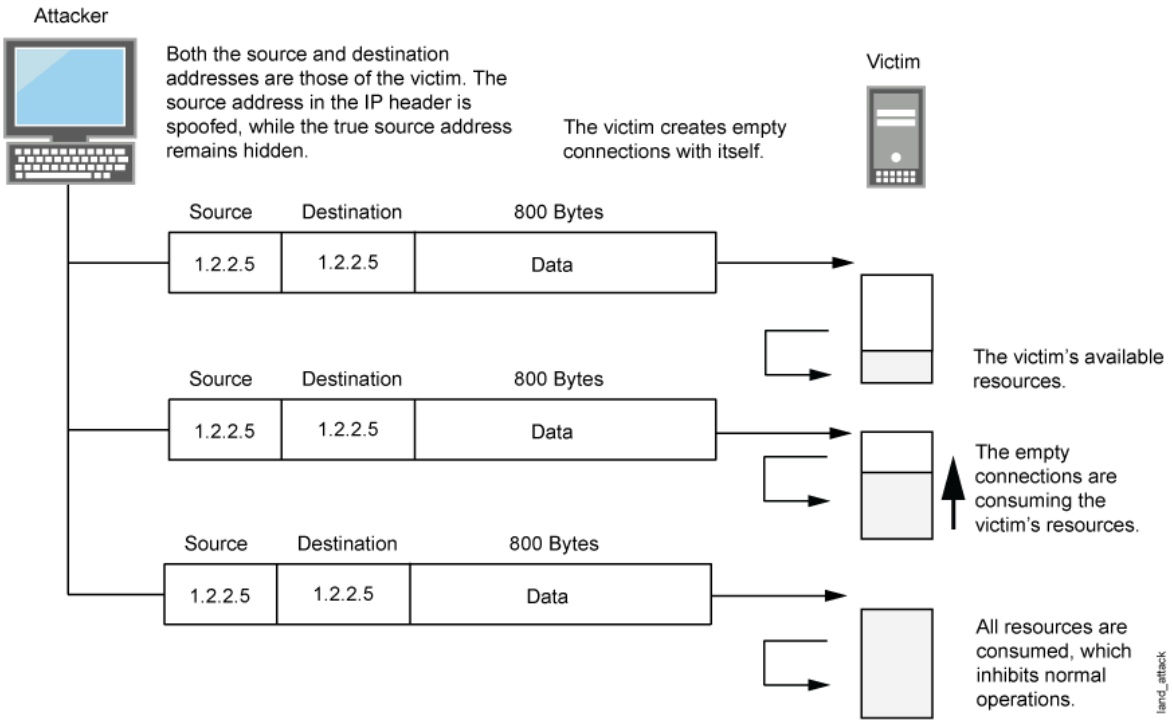
2. Vigaste pakettide ründed

Sellised ründed põhinevad ideel, et ründaja genereerib vigase paketi, mis saadetakse ohvrile ja mis põhjustab süsteemide ebanormaalset käitumist. Teenusetõkestusrünne tekib näiteks siis, kui arvuti või server hangub või teeb taaskäivituse. Näiteks LAND (*Local Area Network Denial*) ja *Christmas tree* rünnete puhul tekitab teenusetõkestuse see, milliseid andmeid kirjutatakse paketti.

Teine suurem variatsioon vigaste pakettide rünnetest kasutab ära nõrkust fragmenteeritud pakettide kokku panemisel. Kuna üks osa võrguseadmeid ei saa suurte pakettide käsitlemisega hakkama, siis jaotatakse pakettides olev info väiksematesse pakettidesse ja saadetakse üle võrgu. Sihtpunktis olev seade võtab need paketid vastu ja paneb andmed uuesti kokku ning annab edasi kõrgema kihi rakendusele. Ründaja saadab modifitseeritud pakette, mis võivad süsteemi kokku jooksutada ning põhjustada süsteemi mittetavapärast käitumist. Selle tagajärjel tekibki teenusetõkestus, sest süsteemid ei saa teenindada teisi kasutajaid.

2.1 LAND rünne

Tuntud ründemeetod, kus ründaja saadab ohvri masinale eriliselt loodud TCP SYN paketi. IP lähteaadress võltsitakse ja määratakse samaks, mis on rünnatava masina aadress. Selle tulemusena hakkab masin iseendale vastama ja tekib lõpmatu tsükkel, mis kasutab ära kogu protsessori jõudluse. Tänapäeval on kõigil operatsioonisüsteemidel olemas turvapaik selle nõrkuse vastu. Lisaks viskavad marsruuterid ja jagajad sellised paketid kohe minema ega lase neil võrgus edasi liikuda [3][4][5][6].



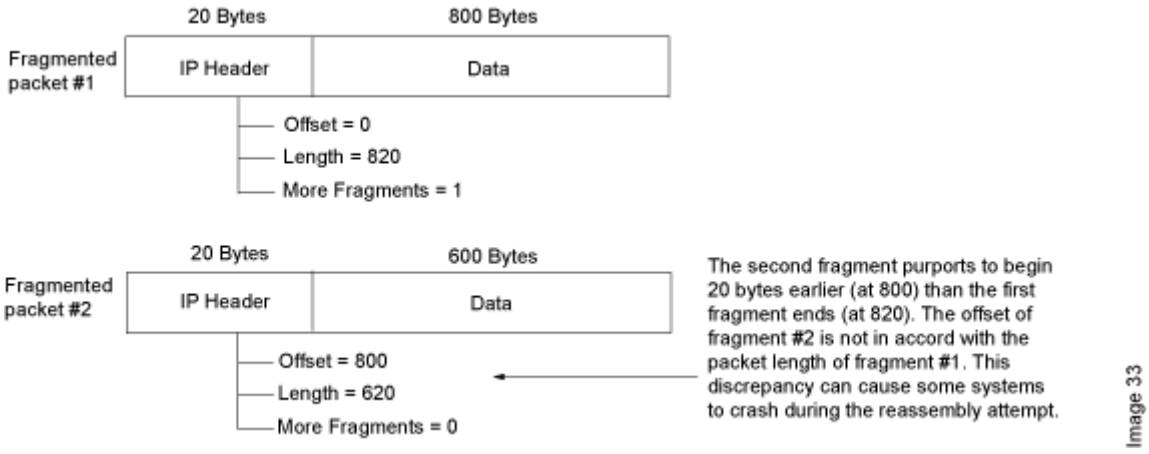
Joonis 1: LAND ründe seletus [4]

2.2 Christmas tree rünne

Christmas tree ründe puhul saadab ründaja ohvrile pakette, mille kõikvõimalikud protokolli lipud on määratud tõeseks, näiteks FIN, PSH ja URG [5]. Kuna paljud operatsioonisüsteemid reageerivad sellistele pakettidele erinevalt, siis kasutatakse seda rünnet tuvastamaks, milline on rünnatav süsteem. Kuna aga selliste pakettide protsessimine nõuab palju ressursse, siis saab kasutada seda ka kui teenusetõkestusrünnet [7].

2.3 Teardrop rünne

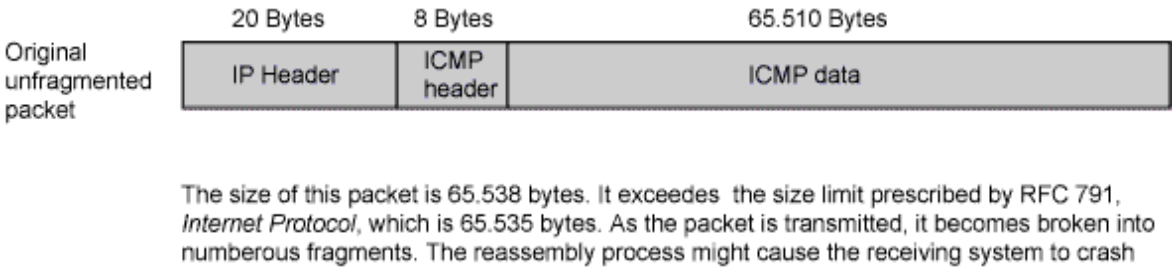
Teardrop on rünne, kus ründaja moodustab sellised fragmenteeritud paketid, milles olev info kattub. Näiteks esimene pakett ütleb, et temas olev info jätkub keset teist paketti ja teine pakett ütleb, et temas olev info algas juba esimeses paketis. Vanemates operatsioonisüsteemides, mis kasutasid veel koodiveaga TCP/IP fragmentide kokkupanemist, tekitasid sellised pakettid segadust ja tihti jooksid operatsioonisüsteemid kokku või tegid iseseisva taaskäivituse [8][9].



Joonis 2: Fragmenteeritud pakettide kattumise rünne [8]

2.4 Ping of Death

RFC 791 (*Internet protocol*) määrab selle, et suurim IPv4 pakett võib olla 65535 baiti. IP paketi päis on 20 baiti ja ICMP *echo request* 8 baiti pikk. Seega võib ICMP *echo* paketi kehas olla 65507 baiti andmeid. Ping of Death ründe puhul loob ründaja aga ICMP paketti, kus on lubatust rohkem andmeid. Selliseid fragmenteeritud pakette kokku pannes hangusid paljud vanad operatsioonisüsteemid. See rünne on tuntud ning tänapäeval viskavad operatsioonisüsteemid sellised paketid minema. Selliste pakettide saatmine viitab ründele ning tulemüürid kirjutavad logifailidesse, et toimub kahtlane võrguliiklus [10][11].



Joonis 3: Näide Ping of Death paketist [11]

2.5 ROSE rünne

Selle ründe puhul saadetakse fragmenteeritud paketi paar esimest ja viimast baiti. Ohvri arvuti puhver jääb ootama andmeid paketi keskelt, aga neid tegelikult kunagi ei saadetagi. Kui selliseid väikseid pakette saadetakse piisavalt palju, siis fragmentidele eraldatud mälu täitub ning see ei saa enam uusi pakette vastu võtta ja töödelda. Lisaks võib rünne ära kasutada kogu vaba ribalaiuse [12].

2.6 New Dawn

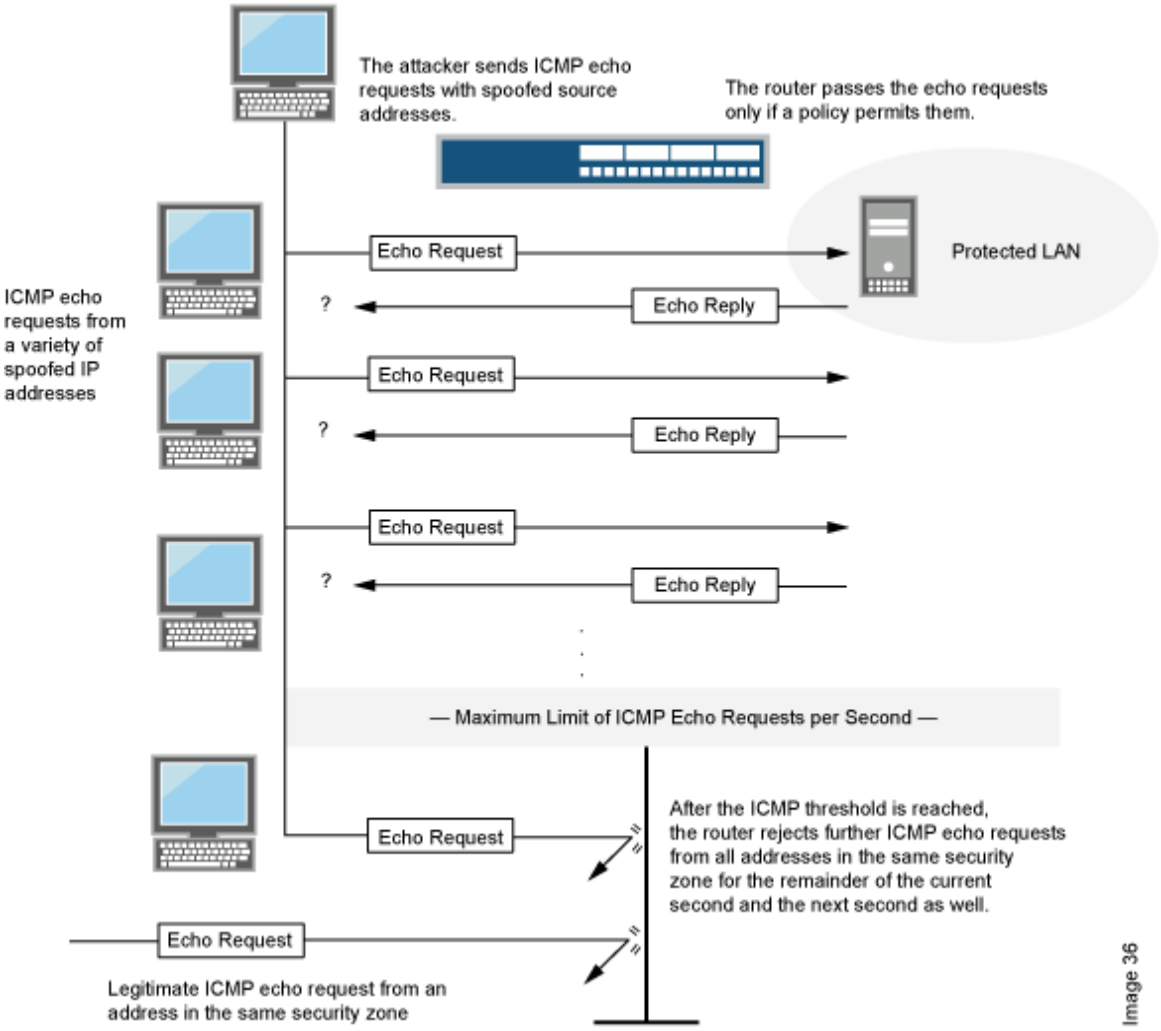
New Dawni näol on tegemist Rose ründe edasiarendusega. Algul saadetakse fragmendi alguse pakett ja siis hakatakse saatma järjest väikseid osasid, aga vahelt jäetakse ära osad paketid ning terve pakett ei jõuagi kunagi kohale. Lõpuks pannakse korduvalt teele fragmendi viimast paketti. Selle peale üritab ohvri arvuti protsessor korduvalt sõnumit kokku panna, mis ei õnnestu, sest osa fragmentidest ei jõua üldse kohale [12].

3. Ummistusründed

Ummistusrünnete puhul saadetakse ohvrile väga palju võrguliiklust, mille läbitöötamine nõuab ressursse. Osad sellised ründeid ummistavad sidekanali ja tekib suur paketikadu, mistõttu ei pääse läbi ka õigete kasutajate andmevood. Osad ründed aga koormavad sihtarvutit ennast, segades selle tööd. Kõiki selliseid ründeid saab robotivõrku kasutades muuta veelgi efektiivsemaks.

3.1 Ping pakettide ummistus

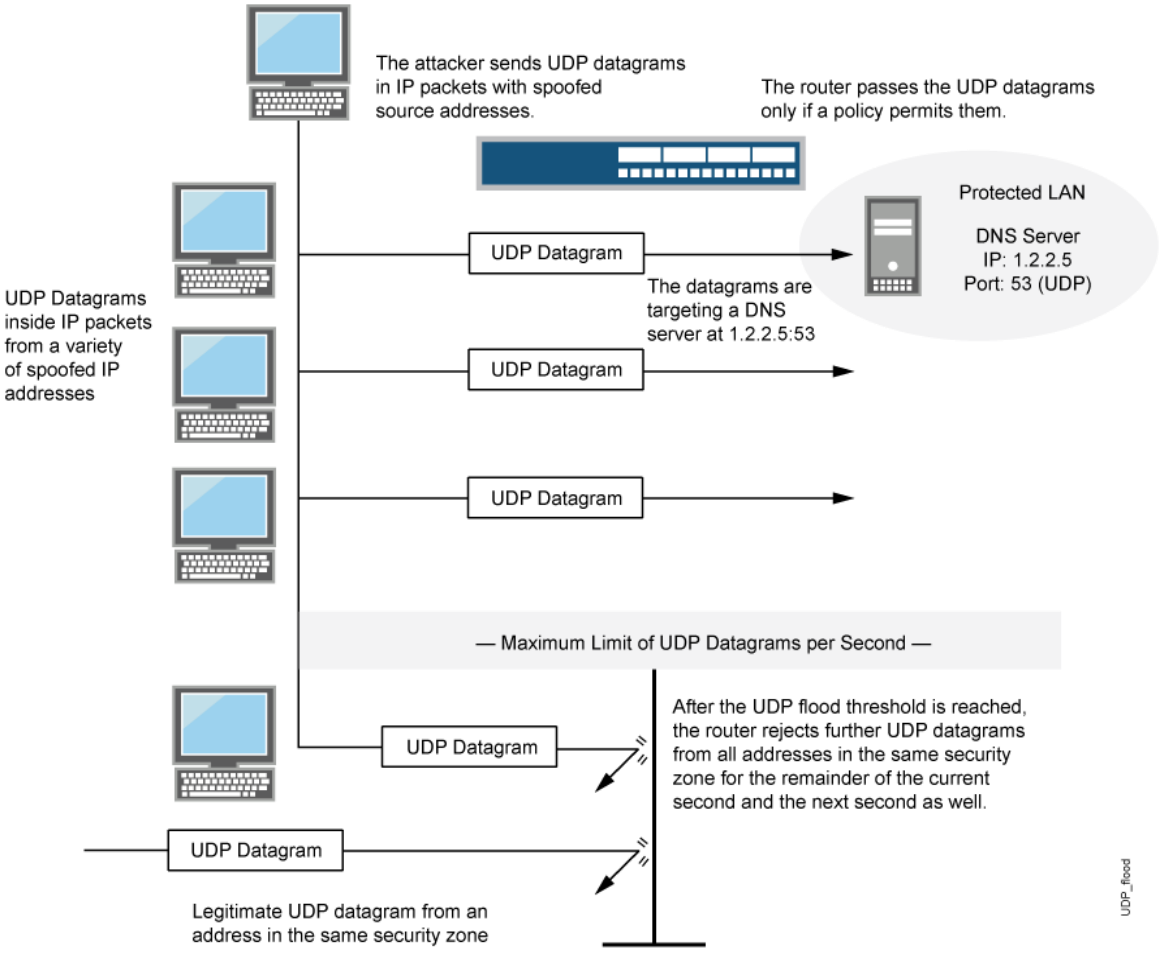
Ping kasutab ICMP (*Internet Control Message Protocol*) protokolli, et kontrollida, kas võrgus olevad seadmed on kättesaadavad. Sihtkohas olevale masinale saadetakse ICMP *echo request*, mille peale vastatakse *echo reply*. Rünnak seisneb selles, et ründaja saadab võimalikult kiiresti väga palju ping pakette. Ohver tavaliselt vastab kõigile neile, kasutades selleks oma protsessorit ja üleslaadimise kiirust. Kuna ICMP ei loo ühendust kahe arvuti vahel, siis võib ründaja võltsida IP tagastusaadressi [13].



Joonis 4: Ping pakettide ummistus [13]

3.2 UDP ummistus

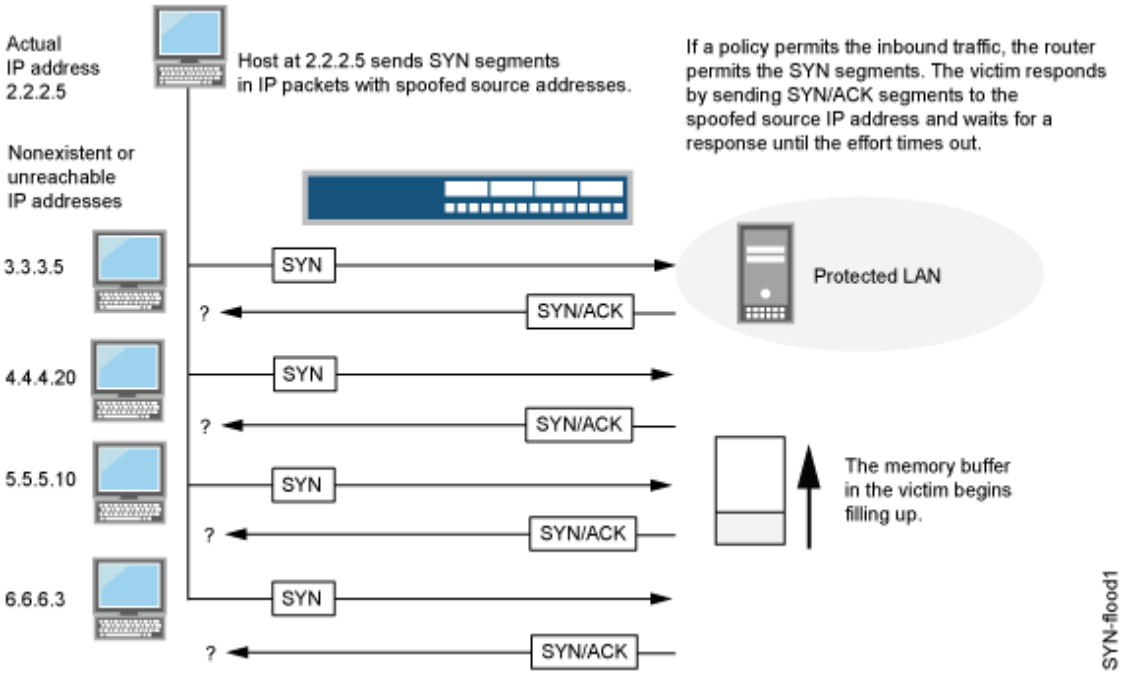
UDP (*User Datagram Protocol*) uputusründega on tegemist siis, kui ohvrisüsteemile saadetakse palju UDP-pakette. Praegusel hetkel on see ründeliik üks populaarsemaid (Vt. Lisa 1). Sellega kasutatakse ära vaba ribalaius ning tekib võrguliikluse küllastus. Lisaks peab ohver genereerima ICMP-paketi teatega „*destination unreachable*“ ja selle tagasi saatma. Teenuse tõkestus tekib siis, kui ohvri arvuti ei suuda enam teenindada teisi kasutajaid, sest on hõivatud ICMP-pakettide genereerimise ja saatmisega. Ründaja saab ründe ajal anonüümseks jääda, sest UDP ei loo ühendust kahe arvuti vahel ja seega saab võltsida lähteaadressi, kust paketid pärinevad [14][15].



Joonis 5: UDP ummistusründe seletus [15]

3.3 SYN ummistus

Kahe arvuti vahelise ühenduse loomiseks kasutatakse TCP *three-way-handshake*'i. Klient saadab näiteks serverile SYN-paketti, server vastab kliendile saates SYN-ACK paketi ja jääb vastust ootama. Peale seda, kui klient vastab omaltpoolt ACK-paketiga, avatakse täisühendus kahe masina vahel ja hakatakse üksteisele saatma andmeid. Ründaja aga ei saada kunagi tagasi viimast ACK-paketti, mille tulemusena hoiab server ühendust mõnda aega poolavatud seisundis. Kui ründaja suudab luua poolavatuid ühendusi kiiremini, kui need jõuavad aeguda, siis tekib teenusetõkestusrünne, sest uusi ühendusi teistelt kasutajatelt ei võeta enam vastu. Tänapäeval kasutavad mitmed operatsioonisüsteemid SYN *cookies* mehhanismi, mis paneb SYN-paketiga kaasa ühenduse info ja kui tegemist on päris ühenduse algatusega, siis saavad SYN-ACK vastusega selle info tagasi [16][17].



Joonis 6: SYN ummistusründe seletus [17]

3.5 RA ummistus

Router Advertisement ummistus on väga spetsiifiline rünne, mis toimib ainult OSI-mudeli teise kihi kohtvõrgu piires. Kuna IPv6 toetab väga suurt aadresside hulka, siis saab kasutada seda teenusetõkestusründeks. Ründaja genereerib palju RA-pakette erinevate MAC aadresside ja IPv6 eesliidetega. Arvutid, millel on automaatne olekuseisundi seadistamine lubatud, hakkavad IPv6 eesliiteid välja arvutama ja oma marsruuditabeleid uuendama. See põhjustab omakorda protsessori 100 %-list kasutamist, mille tagajärjel süsteemid enam ei toimi ja vajavad enamasti taaskäivitamist [18][19].

4. Võimendusründed

Tavaliste ummistusrünnete korral üritab ründaja saata piisavalt võrguliiklust, et tekitada teenusetõkestusrünne. Tänapäeval aga suudavad enamus arvutivõrkude kaitsesüsteeme sellised ründed kas lihtsalt peatada või ära taluda ning nüüd on kasutusele võetud võimendusründed.

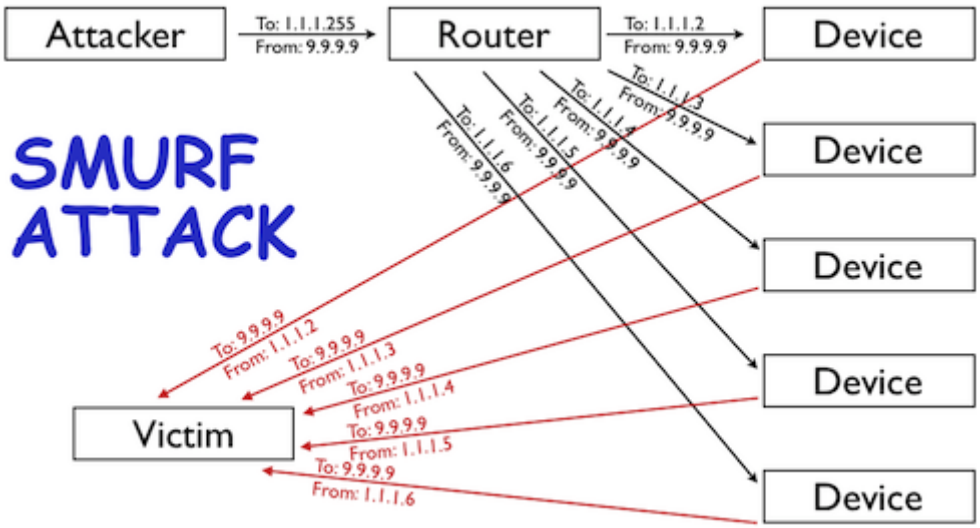
Vahelülisid ründaja ja ohvri vahel nimetatakse peegeldajateks, paketi saamisel nad vastavad suurema hulga pakettidega. Veebiserverid, DNS-serverid ja marsruuterid on peegeldajad, sest peale SYN või teiste TCP-pakettide saamist, vastavad nad SYN-ACK või *Reset connection* (RST) paketiga.

Klassikaliste võimendusrünnete puhul kasutab ründaja ära marsruuteritel olevat IP leviedastusaadressi võimalust – marsruuterid edastavad leviedastusaadressile saadetud paketid kõigile seadmetele, mis kuuluvad sihtvõrku.

Ründe ajal saadab ründaja peegeldajatele vastustnõudvaid võltsitud pakette. Pakettide lähteaadress võltsitakse ja asendatakse ohvri aadressiga. Pärast pakettide saamist vastavad peegeldajad ja saadavad paketid seejärel ohvrile edasi. Ohvri seisukohalt on ründe teostajateks peegeldajad, sest neilt pärineb andmevoog. Peegeldajatele jääb mulje, et ohver ründab neid, sest päringud tulevad ohvri IP-aadressiga.

4.1 Smurf rünne

Smurf rünne on tavalise ping ummistusründe edasiarendus, kus ründaja saadab ICMP *echo request* pakette võltsitud ohvri lähteaadressiga võrgu marsruuteri leviedastusaadressile, mis siis omakorda edastab need paketid kõigile seadmetele selles võrgus. Seadmed vastavad ping päringule ja saadavad ohvrile vastused. Tänapäeval on selliseid ründeid raske teostada, sest enamus marsruutereid on seadistatud mitte edastama ICMP päringuid leviedastusaadressil [1].



Joonis 7: Smurf rünne [22]

4.2 Fraggle rünne

Fraggle rünne on UDP ummistusründe edasiarendus, kus ründaja saadab peegeldajale palju UDP-pakette. Marsruuter edastab paketid oma sisevõrku ja seal olevad masinad vastavad ICMP *destination unreachable* paketiga ründaja võltsitud läheaadressile ehk siis ohvrile [20].

4.3 SMTP rünne

SMTP ründe korral saadab ründaja Internetis asuvale halvasti seadistatud STMP (*Simple Mail Transfer Protocol*) serverile ettevalmistatud meili. Server võtab kirja vastu ja tuvastab, et sellise kasutajanimega kirja vastuvõtjaid ei ole. Iga CC: ja BCC: päistes olev kehtetu kasutaja kohta genereeritakse NDN (*non-delivery notification*) sõnum ehk *bounce* ja saadetakse see kirja lähtekohta tagasi. Kuna aga lähteaadress on ründaja poolt võltsitud, siis saadetakse veateated ohvri SMTP serverile. Olenevalt sellest, kuidas vahelüli moodustab NDN sõnumi, võivad edastatavad kirjad olla väga suured, omades näiteks originaalsõnumit, kirjale kaasa pandud lisasid ja SMTP serveri omaveateadet. NDN sõnumi moodustamise kohta ei ole kindlat protokolli, nii et iga SMTP server moodustab selle nii, nagu see on seadistatud [21].

Tänapäeval korralikud seadistatud SMTP serverid selliseid kirju enam vastu ei võta ja annavad veateate juba SMTP seansi ajal.

4.4 DNS ummistusrünne.

Selle ründe peegeldajateks on DNS (*Domain Name System*) serverid. Ründaja teeb päringu DNS serverile ohvri aadressiga, server genereerib vastuse ja saadab selle ohvrile. Ründaja üritab küsida DNS serverilt võimalikult palju andmeid, et võimendusefekt oleks võimalikult suur. Kuna ründaja päringu pakett on väiksem kui DNS serveri vastus, siis saab ründaja väikse vaevaga väga efektiivse tulemuse. Probleemiks on avatud DNS serverid, mis on halvasti konfigureeritud ja vastavad kõigile päringutele. Kui DNS server toetab DNSSEC signatuure ja ründaja neid küsib, siis saab rünnakut veel suuremaks võimendada, sest vastusepaketid on DNSSEC signatuuride ja linkimisinfo võrra suuremad [1][22][23].

5. Ründed protokolli nõrkuste pihta

5.1 SSL ründed

SSL/TLS on protokoll, mis võimaldab ühenduse teist osapoolt autentida ning andmeid edastada krüpteeritult ja tervikluskontrolliga. TLS ühendusel on kaks faasi: esimene on ühenduse loomine (*handshake*) ja teine on andmete saatmine. Esimene neist on üldjuhul teisest arvutuslikult kallim ja peamise osa arvutusest peab tegema veebiserver, mitte klient. Seda nõrkust kasutataksegi teenusetõkestuste tegemiseks.

5.1.1 SSL käepigistuste ummistus

SSL käepigistuste ummistus on olemuselt lihtne rünne, kus ründaja avab serveriga palju turvalisi ühendusi. Kuna iga ühenduse loomine nõuab kliendilt 10-15 korda vähem arvutusi ja andmetöötlust kui serverilt, siis saab väga kiiresti tekitada serverile teenusetõkestuse. Sellel ajal kui protsessor tegeleb ründaja ühenduste arvutamisega, ei ole võimalik teenindada teisi kasutajaid. Keskmine server suudab teha 150-300 käepigistust sekundis, samas klient võib nõuda üle 1000 käepigistuse sama aja jooksul. Ründe teeb efektiivseks see, et klient ise teeb väga vähe ja server peab kasutama väga palju ressursse [57].

5.1.2 SSL renegotian rünne

SSL-i üks võimalus on see, et iga ühendus sees võib korduvalt nõuda uue käepigistuse tegemist. Seega saab ründaja ühe ühenduse abil pidevalt nõuda, et server teeks arvutused uuesti. Arvutamine omakorda kasutab palju protsessori jõudlust ja muudab serveri aeglaseks [23][24][25][57].

Lahenduseks oleksid süsteemid, mis sunnivad klienti tegema teatud lisaarvutusi. Kui klient peab serveriga tegema sama palju arvutusi, siis kaob ründe mõte ära. Rünnet on raske avastada, sest välised teenusetõkestusrünnete mõju vähendajad näevad ainult ühte TCP ühendust.

5.2 HTTP ründed

HTTP ründed on suunatud veebiserverite pihta. Sellised ründed on tulemuslikud sellepärast, et nad on kõrgema kihi ründed ja 4. kihi teenusetõkestusrünnete kaitsemeetodid neid ei peata. Need on populaarsed, sest neid on lihtne teostada, vajavad ründaja poolt vähe arvutusliku jõudu ja tihti on neid keeruline tuvastada. Nad loovad täieliku TCP ühenduse ja jätavad

mulje, et tegemist on täiesti tavalise ühendusega. Selliste rünnete jaoks ei ole vaja suurt robotivõrku, saab hakkama ka tavalise sülearvutiga [26][27].

5.2.1 Slowloris

Slowloris on programm, mille abil saab teostada nn. aeglase ja varjatud ründe veebiserveri pihta. Erinevalt ummistusrünnetest ei proovita pakettidega ära uputada tervet võrku, vaid rünnatakse ainult veebiserverit, jättes teised teenused kasutuskõlblikuks. Slowloris hoiab ühenduse serveriga avatuna, saates osalisi HTTP päiseid iga teatud aja tagant, nii et server ei saaks ühendust sulgeda. Klient peab ootama, kuni veebi sokkel vabaneb, et seda kasutada. Kui tegemist on populaarse leheküljega, siis võib aega minna enne, kui kõik veebisoklid vabanevad.

Slowlorise teeb varjatud ründeks see, et esiteks saab serverile saata erinevaid kliendi päiseid. Teine põhjus on aga see, et logidesse ei kirjutata enne ühenduse lõppemist midagi. Kui rünne lõppeb või sessioon lõpetatakse, siis ilmub veebiserveri logidesse veateateid „400 *bad request*“.

Tegemist ei ole TCP-l põhineval rünnakul, sest luuakse terviklikke TCP ühendusi, aga selle asemel tehakse poolikud HTTP ühendused. Slowloris lubab väga kiiresti veebiserveril minna tagasi normaalsesse seisundisse, vabastades veebisoklid teistele kasutajatele.

Kuna selle ründe edukus sõltub serveri tarkvarast, siis kasutatakse ründe mõju vähendamiseks sellist lahendust, kus haavatavate serverite kaitsmiseks pannakse püsti vähem haavatavad serverid. Näiteks nginx abil kaitsti Apachet [28][29][30][31].

5.2.3 R-U-DEAD-YET (RUDY)

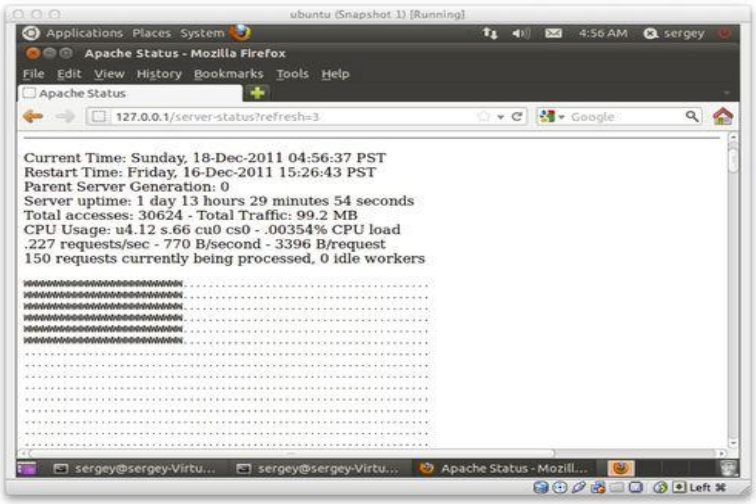
RUDY rünnet on sarnaselt Slowlorise rünnakule raske tuvastada ja peatada, sest pakette luuakse vähe ja aeglaselt ning sel ründel puudvad klassikalised ummisturünde tunnused. Kui kasutaja täidab veebilehel vormi, siis serverile saatmiseks kasutatakse HTTP POSTi. Server töötleb need andmed ära ja valmis saades sulgeb ühenduse, misjärel hakkab teiste külastajate päringuid töötlema. Kui aga kasutatakse RUDY ründeprogrammi, siis saadetakse HTTP päis, kuhu pannakse kirja „*content-length*“ ja seejärel saadetakse HTTP sõnumi andmed serverile ühe baiti kaupa. Server peab seetõttu ühenduse lahti hoidma ja sellega raiskab oma ressursse. Selleks, et server liiga vara ühendust ei sulgeks, saadetakse ründepakette kindlate intervallide tagant, millega simuleerib ründaja aeglase Internetiühendusega kasutajaid.

Sellise ründe peatamiseks on vaja määrata mõistlik *timeout* päringute lugemiseks veebiserveris [30][32][33][34].

5.2.4 Slow READ, socketstress

Slow READ-i puhul on tegemist ründega, mis kasutab TCP akna suurust. Selle ründe puhul hoiab ründaja serveri ühendusi lahti, lugedes serveri poolt saadetud andmeid väga aeglaselt. Kui server hakkab andmeid saatma, siis küsitakse kliendi käest, kui suur on hetkel tema paketi kättesaamise akna suurus. Ründaja vastab, et akna suurus on 0 baiti. Selle peale hoiab server ühenduse avatuna ja küsib teatud aja pärast uuesti kliendi akna suurust. Kui ründaja avab mitu ühendust serveriga ja sunnib ühendusi lahti hoidma, siis tekib teenusetõkestus teistele kasutajatele, sest serveril ei ole piisavalt vabu ühendusi ja mälu, et teisi veebilehe külastajaid teenindada. Tegemist on ründega TCP tasandil.

Teine võimalus tekitada teenusetõkestusrünne on vastata serverile, et akna suurus on 4 baiti, mis sunnib serverit kogu andmete hulga jagama väikestesse pakettidesse, kasutades sellega ära kogu oma vaba mälu [35][36][37].



Joonis 8: Apache server, mis Slow READ ründe all [37]

5.2.5 Keep-alive rünne

Keep-Alive rünne on HTTP/1.1 protokolli osa ja lubab ühe TCP ühenduse ajal teha palju päringuid. Selle tulemusena saab teha palju päringuid, ilma et süsteemi kaitsemehhanismid aktiveeruksid. Ründajale on see hea, sest iga ühenduse avamine nõuaks ründaja enda ressursse, aga ühe ühenduse lahti hoidmiseks ei ole palju vaja. Kui tavaliselt saadab veebilehitseja GET või POST päringuid, siis server saadab kliendile tagasi andmeid ja ründaja enda võrguriba laius saab otsa. Lahenduseks kasutatakse HEAD-i. See sunnib

serverit päringut tegema, aga ei saada tulemust tagasi ründajale. Kuna see rünne kasutab ära veebiserveri CPU ja RAM-i, siis kasutatakse seda rünnet nendel lehekülgedel, mille genereerimine nõuab palju ressursse, näiteks otsingud [38].

5.2.6 HTTP GET rünne

HTTP GET-rünne on klassikaline rünne, kus ründaja laseb oma robotivõrgul ohvri veebilehelt alla laadida väga suuri faile, näiteks videoid. Server koormatakse päringutega üle, mistõttu muutub aeglaseks, häirides sellega teiste kasutajate veebikülastusi. See ei ole tänapäeval kuigi efektiivne, sest sellise ründe filtreerimine on väga lihtne [39].

5.3 P2P rünne

P2P (*peer-to-peer*) tehnoloogiat kasutatakse failide jagamiseks üle võrgu ilma keskse infrastruktuurita. Kuna neid süsteeme kasutavad paljud inimesed, siis on leitud ka moodus, kuidas kasutada suurt hulka inimesi tõkestusrünnete tegemiseks. Peamine ründe meetod kasutab indeksfaili "mürgitamist".

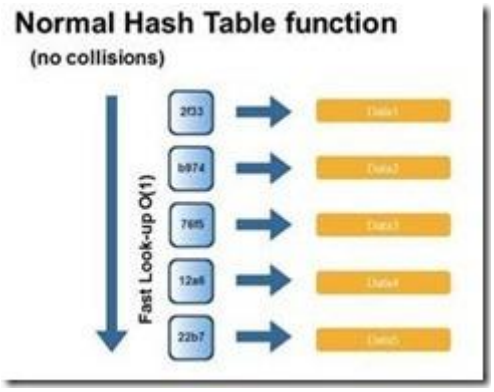
Paljud P2P süsteemid kasutavad indeksfaili, kus on kirjas teatud väärtused ja nende asukohad. Näiteks Skype indeksfailis on kirjas kasutajanimi ja tema aadress. Torrentvõrgud kasutavad samasugust süsteemi, omades infot selle kohta, kes ja kui palju omab allalaetavat faili.

Ründaja "mürgitab" indeksfaili tekitades näilise olukorra justkui oleks võimalik populaarset filmi või raamatut ohvri aadressilt leida. Kui teised võrgu kasutajad otsivad seda populaarset faili, siis indeks annab neile teada, et see fail on kättesaadav ohvri aadressil. Iga klient loob ohvriga TCP ühenduse ja üritab faili alla laadida, aga kuna ohver ei saa nõutava päringuga, siis ta lihtsalt vastab veateatega ja sulgeb TCP ühenduse [40][51].

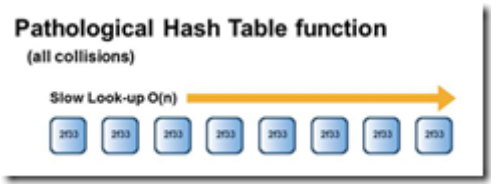
5.4 HashDos

HashDog puhul on tegemist ründega paisktabelite pihta. Paisktabeleid kasutatakse selleks, et luua kiire ligipääsuga andmestruktuur, mille abil saavad arendajad mugavalt infot kasutada. Modernsed veebirakendused sisaldavad tavaliselt veebivorme, kus moodustatakse võtmeväärtuste ja andmete paarid, mis saadetakse rakendusele. Enamasti pannakse need väärtused sõnastikku (*dictionary*). Sõnastikud kasutavad andmete hoidmiseks paisktabeleid. Ründaja loob palju sama andmevõtmega väärtusi ja laseb need sisestada paisktabelitesse. Kui küsitakse võtmeväärtusega andmeid, siis kuna neid väärtusi on hästi palju, siis tekivad võtme kollisioone. Teenusetõkestus tekib sellest, et ründaja saadab hulga spetsiaalselt

valitud objekte, mis põhjustavad kollisioone ja seega põhjustavad rohket lisaahelate läbimist. [41][42].



Joonis 9: Normaalne räsitabelite kasutamine [64]



Joonis 10: Kui ründaja tekitab palju võtmeväärtuse kokkupõrkeid, siis kulub otsimiseks aega O(n) [64]

6. Kaitsemeetodid

Kuna teenusetõkestusründed on populaarsed, siis on suurenenud ka vajadus nende eest ennast kaitsta. Selles peatükkis uuritakse, kuidas saab kaitset klassifitseerida, millised on tehnikad erinevate rünnakute vastu ning milliseid toodetega on firmad tulnud, et kaitsta rünnakute eest (Vt. Lisa 1).

Kaitsemeetodid teenusetõkestuse rünnakute jaoks saab jagada neljaks [2].

- Ründe peatamine
- Ründe avastamine
- Ründele reageerimine
- Ründe mõju vähendamine

Parim lahendus teenusetõkestusrünnete vastu on nende peatamine enne, kui nad jõuavad kahju tekitada. Näiteks globaalsed filtrid peatavad ründe enne, kui see jõuab ohvri sisevõrku. Lisaks tasub jälgida, et kõigil süsteemidel oleksid uusimad turvapaigad, sest see aitab ära hoida vigaste pakettide rünnakud. Mittevajalike teenuste sulgemine aitab vähendada vektoreid, mille abil saab teosta ründeid. Kahtlase võrguliikluse suunamine *Honeypot'*idesse ja koormusjaotur võrgus aitab sellega, et ohvril oleks rohkem aega ründele reageerida.

Mida kiiremini avastatakse rünne, seda kiiremini saab sellele reageerida ja vähendada selle mõju. Tuvastamiseks on kaks peamist meetodit: esimene neist on eelnevate kogemuste põhjal moodustatud signatuurid ja teine on kahtlase või suurenenud võrguliikluse tuvastamine süsteemis. Võrgusüsteemide jälgimisel saab luua standardseisundi ning kui tekivad muudatused, siis võib olla tegemist teenusetõkestusründega.

Ründe mustreid teades on võimalik rünnet võrguliiklust jälgides hõlpsasti tuvastada. Signatuuride omamine on üks väga efektiivne kaitsemeetod. Probleemiks on teenusetõkestusrünnete pidev muutumine ning erinevate kombinatsioonide kasutamine. See omakorda eeldab signatuuride andmebaasi pidevat uuendamist. Uute mustrite lisamine ja haldamine on keerukas ja ajamahukas töö.

Kui tuvastatakse rünne, on kõige tähtsam tagada teenuse toimimine. Edasi on vaja uurida, kust rünne pärineb ja alustada blokeerimistöid. Üheks lahenduseks on IP tagasijälitus, mille puhul üritatakse rünnet jälitada selle alguspunkti, tuvastades sellega ründaja identiteedi. Kuna IP-aadresse on võimalik võltsida, siis on ründe päritolu raske tuvastada. Teiseks võimaluseks on võrguliikluse analüüs, kasutades selleks logisid tulemüüridest ja serveritest või *honeypot'e* ja võrguliikluse pealtkuulajaid. Need aitavad tuvastada ründe karakteristikud ja omadused. Tulemusi saab kasutada näiteks võrguliikluse koormusjaoturis või rakendada uusi filtreerimistehnikaid tulemüürides.

Kui rünnakut ei saa koheselt peatada, siis kõige olulisem on ründe mõju vähendamine, et tagada teenuse pakkumine. Kuna üldjuhul ei saa rünnet otseselt peatada, siis peavad olema kasutuses süsteemid, mis tagaksid selle, et klientidele oleks võimalus kasutada süsteeme. Üks võimalus on tõrkekindlus ehk olulised võrguteenused ja süsteemid dubleeritakse. See tagab, et ohver saab jätkata tegevust ka siis, kui üks osa süsteemidest ei ole kasutatav. Kuna rünnakud saavad maha võtta ka tagavarasüsteemi, siis on peamiseks meetodiks kujunenud QoS (*Quality of Service*) süsteemide rakendamine. Need klassifitseerivad võrguliikluse ja tagavad selle, et prioriteediga liiklus saab võrgu läbida enne, kui teised andmevood ja tagavad selle, et isegi ründe all olles suudavad võrk ja teised olulised süsteemid tagada teenuste pakkumist oma kasutajatele.

Vastavalt sellele, kus kaitsemeetodeid rakendatakse, saab neid jaotada järgnevalt

- Ohvri võrgus
- Ründaja ja ohvri vahelises võrgus
- Ründe allika võrgus

Enamus lahendusi ja süsteeme rakendatakse ohvri võrgus, sest see kannatab ründe korral kõige rohkem ja üldiselt on see ohvri enda vastutusel. Ohvrist ülesvoolu olevatele võrkudele saab ka rakenda kaitsemeetodeid ja nende efektiivsus on väga hea, kuid kuna need võrgud üldiselt ei ole rünnakutest mõjutatud, siis ei kasutada väga palju kaitsemeetodeid. Kui ründe allika juures olevatel võrkudel on rakendatud kaitsemeetodeid, siis võib peatada ründe enne, kui see jõuab Interneti tuumani välja, lisaks saab ründaja kiiremini tuvastada. Ainuke probleem selle süsteemi juures on olukord, kui ei suudeta korrektselt rünnet tuvastada - siis võidakse piirata tavainimeste Interneti kasutust.

6.1 Kaitsemeetmeid vastavalt rünnetele

Enamus vigaste pakettide ründeid on hõlbus peatada, kuna selliste pakettide avastamine on väga lihtne. Tulemüürid ja teenusetõkestusrünnete peatamise süsteemid viskavad ründepaketid minema enne, kui need jõuavad sisevõrku: näiteks Ping of Death, Christmas Tree ja LAND-paketid filtreeritakse võrguliiklusest kohe välja. Tänapäeval suudavad tulemüürid panna fragmenteeritud paketid tagasi kokku ja alles siis rakendavad neile filtreerimist.

Ummistusrünnete peatamine on keerulisem, kuna ohvril pole tihti selliste rünnete peatamiseks tavaliselt piisavalt vabu ressursse. Kõige tavalisem lahendus on määrata andmevoogudele limiidid, kuid tihti ei ole sellest kasu ning kõige parem lahendus oleks osta vastav seade, mis suudab filtreerida pakete või kasutada kolmanda osapoole rünnete mõju vähendamise teenuseid.

SYN ummistusründe vastu on aja jooksul välja kujunenud erinevad kaitsetehnikad. Esimene neist on SYN proksi kaitse, mida leidub paljudes kaasaegsetes tulemüürides. Proksi aeglustab TCP ühendusi ja filtreerib välja ründeühendusi. Teine lahendus on SYN puhver, mis optimeerib mälutabeleid, et mahutada rohkem ühendusi. Kolmas lahendus on SYN küpsiste kasutamine. Selleks luuakse krüpteeritud järjendite numbreid, et filtreerida välja kehtetud sessioonid. Süsteemid panevad SYN-paketiga kaasa ühenduse info ja kui tegemist on päris ühenduse algatusega, siis saavad SYN-ACK vastusega selle info tagasi.

RA uputuse korral on kõige lihtsam lahendus lõpetada IPv6 kasutamine, kuid selle kasutamine on varsti vajalik, sest IPv4 on vananemas. Lihtsam lahendus on keelata *Router Discovey* võimalus. Kuna mõlemad lahendused ei ole kõikides süsteemides võimalikud, siis parim viis ründe peatamiseks on keelata tulemüüris võlts *Router Advertisments* ja lubada teateid ainult autoriseeritud võrguväravatelt. Turul on nüüd saadaval ka kommutaatorid, mis blokeerivad RA uputused. Ka tavaline võrgumonitooring võib avastada isehakanud ruutereid ja DHCP servereid.

Võimendusrünnete mõju ja kasutamist vähendab see, kui sulgeda nõrkused peegeldajates. Näiteks Smurf ja Fraggle rünnete puhul peaksid võrguadministraatorid sulgema marsruuteri võimaluse edastada päringuid leviedastusaadressile. See tagab selle, et võrku ei kasutada rünnete teostamiseks. Ohvri seisukohalt tuleb üles seada süsteemid, mis jälgivad võrguliiklust ja määrata vastavatele andmevoogudele piirid. Juhul kui piirist minnakse üle, siis visatakse paketid minema.

SMTP rünnete piiramiseks tuleb seada piirangud, näiteks genereerida vähe ja väiksema mahuga veateateid - see vähendab võimenduse mõju. Samuti aitab, kui määrata ära, millised kasutajad võivad kirju saata ja paika panna ülim piir, kui palju võib olla kirja saajaid ühe saatmissessiooni ajal. Tänapäeval ei võta SMTP serverid selliseid kirju vastu ja annavad veateate juba SMTP seansis [21].

DNS võimendusrünnete puhu on lahenduseks piirata, millistele päringutele DNS serverid vastavad. Probleemiks on see, et paljud hoiavad nimeserverid avatuna ja nad vastavad kõigile päringutele (tsoonide pädevad nimeserverid muidugi peavadki seda tegema). Lahendus on lubada päringuid teha ainult usaldusväärsetelt võrkudelt [22][63].

SSL *renegotiation* ründe puhul ei aita selle võimaluse ära keelamine, sest siis muudetakse rünne ümber tavaliseks SSL käepigistusummistuseks. Lahenduseks on SSL arvutuste liigutamine serverilt teised süsteemide peale, näiteks võrguliikluse koormusjaotur või spetsiaalsed SSL arvutussüsteemid.

Aeglaste HTTP rünnete korral tuleb ära määrata lubatud agressiivsete piirangute arv:

- Määrata limiidid päistele ja sõnumi osadele, vastavalt oma süsteemi eripäradele.
- Kindel aegumine ühendustele: valides liiga lühikese aja, piiratakse õigeid kasutajaid; valides liiga pika aja, ei saada kaitset ründe eest.
- Lisada serverile süsteem, mis toetab pooleliolevate ühenduste salvestamist ja alles hiljem vastamist.
- Määrata minimaalne sissetulev andmevoo suurus ühenduse kohta

Üks võimalus on ka süstida JavaScript koodi veebilehtedesse. Sellega saab eraldada robotvõrgu robotid õigetest kasutajatest [62].

Tavalise GET ummistuse korral tuleb määrata piirangud vastavalt serveri jõudlusele. Lisaks ka piirangud, kui palju ühendusi võib tulla ühelt IP-aadressilt ning kui palju võib kindlat veebiressurssi alla laadida.

P2P ründe üheks peatamise võimaluseks on enne kontrollida, kas indeksfailis reklaamitav aadress kuulub P2P võrku. Enamasti ohver ei kuulu P2P võrku ja selle abil saab kiiresti eemaldada väärad aadressid. Teine võimalus on krüpteerida võrguliiklus ja lubada vaid

sõlmedel ennast reklaamida P2P võrgule. Ohvri lahenduse kaitseks on visata paketid P2P võrgust minema [40][61].

HashDoS rünnet saab peatada signatuuriga. Kui avastatakse POST, mis sisaldab palju võtmeväärtusi või millel on liiga palju andmeid kaasas, siis visatakse pakett minema, nii et andmebaasid ei pea seda kasutama. Osad programmeerimiskeeled on selle probleemi juba lahendanud, kasutades suvalist sõna ja XOR sissetulevate andmete puhul. Teine võimalus on piirata sissetulevate andmete kogust programmeerimiskeele tasemel [42].

6.2 Teenusetõkestusründe allika tuvastamine

Rünnete allika tuvastamine on parim viis, kuidas peatada teenusetõkestusrünne. Kahjuks on allika jälitamine väga keerukas. Kindlasti tuleb teha koostööd Interneti-teenuse pakkujaga - nad saavad filtreerida andmevoogusid enne, kui need jõuavad ohvrini, vähendades seeläbi ründe mõju.

Teenusetõkestusrünnete jälitamine võrgus on keeruline ja aeganõudev töö. Kõige tavalisem lahendus on tuvastada, milline marsruuter saadab ründepakette ülesvoolu. Tavaliselt kuuluvad need Internetiteenuse pakkujale, kellega tuleb ühendust võtta ja lasta neil seadistada filter, mis eemaldab ründepaketid.

Üks võimalus teenusetõkestusründe peatamiseks on tuvastada isik, kes saab kasu sellest, et ohvri võrk või veebileht ei ole kättesaadav. Nendeks võivad olla kas endine pahatahtlik töötaja, konkurent või kuritegelik rühmitus. Põrandaaluste foorumite ja jututubade jälgimine, kus toimub robotvõrkude rentimine ja rünnete arutamine, võib anda infot, kes soovib halba. Selline uurimistöö nõuab kogemustega inimesi ja palju koostööd, kuid ründaja tuvastamine annab kohese efekti.

Kuna IP-aadressid on võltsitavad, siis on väga raske tuvastada, kust ründed pärinevad. Siiski on välja arendatud tehnikad, mille abil saab vähendada rünnete mõju, kasutades selleks filtreerimist ülesvoolu marsruuterites.

Üks lahendus teenusetõkestusründe jälitamiseks on manuaalne ACL (*Access Control List*) tagasijälitus. Interneti-teenuse pakkuja määrab marsruuteris algul üldiste parameetritega ACL ja mida rohkem saadakse teada ründe kohta, seda spetsiifilisemaks muudetakse parameetrid, kuni lõpuks saadakse teada, millised on ründavate andmevoogude karakteristikud. Selle info abil saab määrata ülesvoolu oleva marsruuteri allikaliidese ja MAC aadressi. Siis peab seadmes kordama sama protseduuri, kuni jõutakse ründe allikani.

See on aga ajakulukas ja kui tegemist on hajusa teenusetõkestusründega, siis hargneb jälitustöö ülesvoolu olevates marsruuterites mitmeks.

Teine võimalus on hajusjälitus. Internetiteenuse pakkuja ääremarsruuterid tuvastavad ründevood ja viskavad need paketid minema, genereerides sellega ICMP *unreachable* paketti ja saadavad need tagasi võltsitud IP-ga aadressidele. Kui aga *sinkhole* marsruuter reklaamib era- või kasutamata aadressiruumi, siis need ICMP-paketid suunatakse lõpuks sinna seadmesse. Siis jälgitakse, millised marsruuterid genereerivad neid pakette ja saadakse teada IP-d [58][59][60].

6.3 Pakutavad tooted ja teenused

Paljud firmad on turule tulnud oma süsteemidega ja teenustega, mis kaitsevad teenusetõkestusrünnete eest. Üks võimalustest on soetada riistvaraline lahendus, mis jälgib ja puhastab võrguliiklust enne, kui see lubatakse sisevõrku (Vt. Lisa 1). Teine lahendus on osta kaitseteenust sisse. Praeguseks on välja kujunenud firmasid, mis suudavad pakkuda monitoormist, kaitset ja rünnaku mõju vähendamist. Kuna turul pakutavad tooted ja teenused on erinevad, siis siin peatükkis toon välja mõned neist ning annan ülevaate, kuidas nad toimivad.

6.3.1 Cisco Systems

Cisco Systems on üks suurimaid võrguseadmete tootjaid ning ta pakub kahte erinevat süsteemi teenusetõkestusrünnete tõrjumise jaoks. Esimene on Cisco Traffic Anomaly Detector XT [43], mille ülesandeks on passiivselt võrku jälgida ja anomaaliate tekkimisel teavitada sellest koheselt teist seadet Cisco Guard XT [44], mis alustab võrguliikluse analüüsimist ja filtreerimist. Kui tuvastatakse ründaja saadetud paketid, siis kaotatakse need koheselt ja teiste kasutajate paketid suunatakse edasi õigesse sihtpunkti.

Cisco Guard XT kasutab rünnete vastu viie-astmelist MVP (*Multiverification*) struktuuri [45].

- Pakettide filtreerimine on esimene moodul struktuuris. Kasutatakse lihtsaid staatilised filtreid, mis blokeerivad mittevajaliku võrguliikluse jõudmist kasutajani. Filtrid on Cisco poolt juba eelnevalt seadistatud. Juhul kui tuvastatakse pahatahtliku andmevoo eripära, siis saavad dünaamilised filtrid oma reeglistiku teistelt moodulitelt.

- Aktiivse tõendamise mooduli ülesandeks on avastada võltsitud aadressiga pakette. Lisaks leidub erinevaid mehhanisme, mis tagavad selle, et andmevoost eemaldatakse ainult ründepaketid.

- Anomaalia tuvastamise moodul jälgib eelmisi moodulid läbinud võrguliiklust ja võrdleb seda varem salvestatud nn. normaalse võrguliikluse tunnustega. Kuna ründe andmevood erinevad teatud aspektides tavaliste kasutajate omadest, siis saab võrdluse teel eemaldada kahtlased paketid.

- Protokolli analüüs - antud moodul analüüsib rünnete tuvastamiseks seda liiklust veelgi täpsemalt. Kasutatakse selleks, et tuvastada ründed, mis kasutavad kindlaid protokolle, näiteks HTTP.

- Andmevoogude piiramine on viimane moodul ja selle abil analüüsitakse liialt kasutaja ressursse kasutavaid andmevooge, mis aeglustavad kasutaja ligipääsu sisevõrgule.

6.3.2 F5 Networks

F5 Networks töötab välja ja müüb võrguseadmeid. Nende lipulaev BIG-IP oli alguses tavaline võrguliikluse koormusjaotur, mis aitas ka rünnakute vastu, kuid hiljem on täiendavat funktsionaalsust juurde lisatud, et efektiivsemalt vähendada teenusetõkestusrünnete mõju. Välja kujunenud on oma Application Delivery Controller (ADC) [46].

BIG-IP Local Traffic Manager süsteem peatab vigaste pakettide ründed. Selle süsteemi osadeks on:

- *Packet Velocity Accelerator* – eraldi disainitud riistvara protsessor, mis aitab BIG-IP LTM vähendada klassikaliste ummistusrünnete mõju.

- Täisproksi arhitektuur – tagab turvalisuse sellega, et klientidelt tulev võrguliiklus analüüsitakse enne, kui see saadetakse rakenduskihile.

- Protokolli kontroll – jälgitakse, et võrku ei siseneks valesti määratud lippude või puudulike andmetega pakette. Peatab lihtsad *FRAG* ja *Christmas tree* ründed.

BIG-IP Global Traffic Manager – kaitseb hajusate teenusetõkestusrünnete eest ja DNS Express kontrollib üle kõik DNS päringud enne võrku lubamist.

BIG-IP Advanced Firewall Manager – AFM abil saavad võrguadministraatorid kiiresti ja efektiivselt luua spetsiaalseid turvareeglistike. Lisaks jälgitakse ja antakse teada, kui teenusetõkkerünne toimub.

BIG-IP Application Security Manager – peatab seitsmenda kihi ründed. Oskab eristada inimeste ja robotite ründeid. Süstib veebilehtedesse JavaScript *redirect* koodi, eemaldades sellega robotivõrgustiku orjad. Kui avastab, et tegemist on ründega, siis määrab ka kiirusepiirangud andmevoogudele.

Lisaks on F5-l ka oma skriptimiskeel iRules, mis laseb võrguadministraatoritel luua kiiresti ja tõhusaid turvareegleid. Seda kasutatakse BIG-IP masinates ning see on paindlik, lubades kirjutada skripte, mis vastavad vajadustele ja süsteemi eripäradele.

6.3.3 Check Point

Check Point on rahvusvaheline firma, mis pakub erinevaid tarkvaralisi ja riistvaralisi infoturbe lahendusi oma klientidele [49].

SmartEvent Blade – kasutatakse ründaja profiili ründe mustrite kiireks tuvastamiseks.

SmartLog funktsioon – analüüsib logisid erinevatelt süsteemidelt

Firewall Software Blade – sisse ehitatud süsteemid teenusetõkestusrünnete peatamiseks.

- Agressiivne vananemine – ühendused, mis on avatud kauem kui algselt määratud, suletakse ja kustutatakse võrguvärava tabelitest. See meetod kaitseb aeglaste HTTP rünnete vastu.
- Võrgu kvoot – määrab ära, kui palju ühendusi võib ühelt IP-aadressilt olla. Kui avatakse lubatust rohkem ühendusi, siis kas keelatakse uute avamine või jälgitakse täpsemalt andmevoogu.
- Blokeeritakse ICMP/UDP – sellised ründepaketid visatakse võrgu perimeetril minema.
- Olekuga ühenduste inspekteerimine – vähendatakse aega, kui kaua võib mõni ühendus olla avatud. Toimib rünnete vastu, mis on aeglased ja nõuavad palju ressursse.

IPS Software Blade – täiendavad kaitsemeetodid teenusetõkestusrünnete vastu.

- Riikide kaupa blokeerimine – blokeeritakse võrguliiklus riikidest, kust pärineb palju rünnakuliiklust.
- Ussipüüdjate signatuurid – blokeeritakse URL-id, mida kasutatakse ründeks.
- TCP akna suuruse määramine – tagab kaitse ründe vastu, mis pahatahtlikult kasutab TCP akna suuruse muutmist, et põhjustada tõkestus.
- SYN ummistusrünnete kaitse – käivitatakse siis, kui võrku siseneb üle 200 SYN paketi 5 sekundi jooksul.
- HTTP ummistusrünnete kaitse – käivitatakse siis, kui tehakse rohkem kui 10000 päringut 10 sekundi jooksul.

Check Point DDoS protector [50] – riistvaraliselt kiirendatud ja spetsiaalse tarkvaraga süsteem, mis paigaldatakse väljapoole võrgu perimeetrit. Tuvastab ja peatab teenusetõkestusründed enne, kui need jõuavad sisevõrku.

- Võrgu ummistusrünnete kaitse – jälgitakse, millised on tavapärased võrguliikluse mustrid ja ebatavalise andmevoo avastamisel alustatakse filtreerimisega.
- Serveri ummistuskaitse – genereerib igale ühendusele unikaalse signatuuri, jälgimaks ühendusi - ründe korral need peatatakse.
- Rakenduskihi kaitse – blokeerib automaatsed tööriistade ründed ja võltskasutajad, kasutades selleks väljakutse/vastuse tehnikat. Samal ajal suunatakse tavakasutajad edasi oma sihtpunkti.

6.3.4 Radware

Radware pakub rakenduse kättetoimetamise, võrgu turvalisuse ja võrguliikluse koormusjaotur lahendusi. Radware DefensePro [52] on seade, milles on ühendatud IPS (*Intrusion Prevention System*), NBA (*Network Behavioral Analysis*), *DoS Protection* ja *Reputation Engine*. Koostöös suudavad need neli süsteemi peatada erinevaid sissetungi ründed. Teenusetõkestusrünnete avastamiseks kasutatakse ründe signatuuride tuvastamist [52][53].

DoS Mitigation Engine (DME) on riistvaraline lahendus hajusate teenusetõkestusrünnete vastu. Omades kuni 40Gbps läbilaskevõimet suudab see tuvastada ja peatada teenusetõkestusründeid.

Network Behavioral Analysis moodul kasutab signatuuridel põhinevad kaitsetehnikat. Teenusetõkestusrünnete puhul süstitakse reaalaja signatuur otse DME riistvarasse, vabastades sellega seadme protsessori ja jättes kogu töö DME teha.

Denial-of-service Protection moodul kasutab erinevaid tehnoloogiaid teenusetõkestusrünnete peatamiseks. Näiteks signatuuride tuvastamine, käitumispõhised reaalaja signatuurid ja SYN *cookies* mehhanism, mis esitavad väljakutse enne, kui uued ühendused saavad luua seansi serveriga.

6.3.5 Arbor Networks

Arbor Network on tarkvarafirma, mis müüb võrguturbe ja võrguseire tarkvara. Koostöös firmadega Cisco, IBM ja Juniper Networks on välja töötatud erinevaid lahendusi robotvõrkude, võrgusideme ja teenusetõkestusrünnete vastu.

Peakflow SP Threat Management System (TMS) vähendab teenusetõkestusrünnete mõju, eemaldades ründe andmevoo tavaliste kasutajate omadest. Süsteemi ülesandeks on see, et kõik võrku läbivad andmevood saab ründe korral suunata TMS-i, mis eemaldab ründepaketid ja suunab puhtad paketid tagasi võrku.

Teadaolevate ohuallikate blokeerimiseks kasutatakse musti ja valgeid nimekirju. HTTP-põhiste rünnete peatamiseks on veel lisaks IP-põhised piirangud. Eemaldatakse vigased paketid ja piiratakse andmevoogusid, mis tahavad kasutada liiga palju ressursse.

Peakflow SP TMS õpib automaatselt, millised on normaalsed võrguliikluse mustrid ja kohandab oma reegleid vastavalt sellele. Kui vaja, siis võib need ka ümber seadistada vastavalt vajadusele ning see lubab kasutada TMS süsteemi koheselt karbist välja võttes [55][56].

6.3.6 CloudFlare

CloudFlare on sisuedastusvõrk (CDN) ja hajus domeeninimede teenus (DNS). Firmal on kogu maailmas 23 andmebaaside ja serverite klastrit, mis tagavad selle, et klientide lehed oleksid kiiresti kättesaadavad. Selleks et veebikülastaja DNS-i päring jõuaks temale

lähimasse CloudFlare serverite klastrisse, kasutatakse *Anycast* tehnoloogiat. Seal asuv puhverdatud veebileht saadetakse veebikülastajale. Kõik DNS päringud tasakaalustatakse kõigi 23 klastri vahel ning see on üldjuhul väiksemate hajusate rünnete puhul juba piisav, et kliendi veebileht jääks kättesaadavaks. Isegi kui mõni klaster muudetakse ründe tulemusena töövõimetuks, saavad ülejäänud andmebaasid ja klastrid külastajaid teenindada. Lisaks puhastatakse igas klastris täiendavalt andmevoogusid. Näiteks visatakse minema kõik DNS vastused, sest CloudFlare ei tee ühtegi DNS päringut.

Rakenduskihi rünnete jaoks on loodud eraldi teenus: „*I'm under attack*", mis lisab täiendava kihi turvalisust HTTP rünnete vastu. Veebikülastajale näidatakse vahelehekülge, mis käitub kui automaatne CAPTCHA ja selle taustal tehakse täiendavad testid ja analüüsid, kontrollimaks, kas tegemist on ründaja või tavalise külastajaga [47][48].

CloudFlare küll otseselt ei paku kaitset teenusetõkestusrünnakute vastu, kuid oma disaini poolest on suuteline vähendama nende mõju. Kuna on olemas ka tasuta versioon, siis on ta suurepärane tavakasutajatele, näiteks blogid, mis saavad üleöö populaarseks ja vajavad rohkem ressurssi, et toime tulla suurenenud liiklusega veebilehele.

6.3.7 Prolexic

Prolexic on üks suurimates teenusetõkestus rünnakute peatamisele orienteeritud firmadest. Omades globaalset rünnaku mõju vähendamise võrku suudab ta pakkuda kaitset rünnakut suurfirmadele üle kogu maailma.

Spetsialiseerunud ja hea väljaõppega töötajad pakkuvad kohest tehnilist tuge ja nõu rünnakul all olevatele firmadele. Lisaks on olemas ka eraldi rünnakuid uuriv meeskond, kelle ülesandeks on jälgida ja analüüsida rünnakuid. Kord kvartalis antakse välja raport, kus hinnatakse viimase nelja kuu jooksul ründe trende.

Lahendusena suunatakse kogu Internetist tulev liiklus Prolexicu võrku, kus toimub võrguliikluse puhastamine. Sarnaselt Cloudflare'ile on Prolexicul on nn puhastusjaamu üle kogu maailma, et tagada regionaalne võrguliikluse tasakaalustamine. Pärast seda suunatakse puhas liiklus tagasi kliendini.

Kuna pakutakse väga võimsaid lahendusi, siis on ka hinnad vastavad ning Prolexicut saavad endale lubada suurfirmad.

6.4 Nõuandeid enda kaitsmiseks

Enne rünnakut

Küsige endalt järgmisi küsimusi:

- Mis juhtub, kui teie pakutav teenus ei ole klientidele kättesaadav 5 minutit, 1 tund, 3 tundi, 1 päev?
- Kas sellel on rahaline kahju, kas kaotate klientide usalduse?
- Kas te võite olla sihtmärk?
- Kas te tegelete ebaseaduslike või „hallis alas“ olevate tegevustega?

Kui tegelete finantsteenuste pakkumisega, siis olete ka tõenäolisemalt kurjategijate huviobjektiks. Näiteks peavad riigiasutused ja meediasektoris olevad asutused olema valmis „meelsusrünneteks“. Võib sattuda ka nn mittetahtliku rünnaku ohvriks ehk saada lihtsalt suurtes kogustes võrguliiklust.

Madala riskitasemega – Siia alla kuuluvad peamiselt üksikindiviidid ja väiksed firmad, kellel ei teki tõsist finantsilist kahju, kui teenusetõkestusrünnak piirab teenust. Kuna Eestis väga palju sihtmärke ei ole, siis on tegu väikse riskiga ja sel puhul tasub lihtsalt olla teadlik ohust ja kui vähegi on oht olemas, siis on vaja teada, kellega vajadusel kontakteeruda, et saada abi ning nõu.

Keskmise riskitasemega – Siia alla kuuluvad keskmise suurusega firmad ning „hallis sektoris“ tegelevad ettevõtted. Tuleb jälgida ja mõista oma süsteemi; tuvastada varakult kitsaskohad oma süsteemides; omada plaani, kuidas käituda ja kellega kontakteeruda, kui rünnak peaks toimuma.

Kõrge riskitasemega – Suurfirmad ja rahaga tegelevad asutused (peamiselt pangad). Tuleb aktiivselt planeerida ja paika panna kaitselahendusi; pidevate rünnakute korral soetada võrguliiklust puhastavaid seadmeid või võimalusel osta seda teenust sisse. Mõningaid lahendusi on toodud välja kaitsemeetodite peatükis. Lisaks peaks omama jälgimissüsteeme, mis tuvastavad kahtlast liiklust või anomaaliad võrgus. Tõsiselt tuleks võtta klientide kaebusi, kui öeldakse, et teenus on kättesaamatu. Oluline oleks omada automatiseeritut monitooringut sõltumatust võrgust, et näha teenuste kättesaadavust kliendi vaatepunktist.

Rünnaku ajal

Kui tuvastatakse rünnak, siis tuleb koheselt võtta ühendust võrguspetsialistiga ja seletada olukorda. Kindlasti anda teada ka oma internetiteenusepakkujale, sest siis saavad ka nemad alustada uurimist ja võimalusel vähendada rünnaku mõju. Rakendada rünnaku mõju leevendamise süsteeme, kui need on olemas.

- Määra rünnaku võimsus, millised teenused on kättesaamatud ja millised töötavad.
- Ründeliikluse identifitseerimine. Millistelt IP-delt tuleb rünnak, mis sorti liiklusega on tegemist, kas see on suunatud millegi kindla pihta?

Jätke tööle ainult teenuse pakkumiseks vajalikud süsteemid; sulgege teised, et vähendada koormust võrgus.

Pärast rünnakut

Peale rünnakut on vaja aru saada, mis olid võrgus kitsaskohad. Firmades oleks vaja koostada rünnakut kirjeldav raport ja seletada ülemustele ja töötajatele, mis juhtus. Kindlasti tuleks arutada ja paika panna lahendused, et vältida ja vähendada rünnete mõju edaspidi.

Kui on tuvastatud probleemsed kohad, siis võimalusel need elimineerida: parandada ja muuta võrgustruktuuri, et see oleks kindlam. Kui rünnak oli spetsiifilise teenuse pihta, näiteks veebirakendused, siis peaks elimineerima kitsaskohad.

Kokkuvõte

Töö alguses on kirjeldatud üldiselt teenusetõkestusründeid, kuidas neid klassifitseerida ja jaotada. Vastavalt sellele, millist nõrkust ära kasutatakse, on ründed jaotatud neljaks ja igas peatükis on kirjeldatud erinevaid selle jaotuse ründeid. Refereerimiseks on kasutatud Internetis vabalt kättesaadavaid materjale.

Töö teises pooles on kirjeldatud kaitsemeetmeid ning nende jaotust. Lisaks on välja toodud ka teoreetilised lahendused erinevatele rünnetele. Lõpuks on kaitsemeetodite illustreerimiseks toodud välja ka erinevate firmade tooteid ja lahendusi, mis on loodud rünnete tuvastamiseks ja mõju vähendamiseks. Samuti on kirjeldatud nende ülesehitust. Lisaks spetsialistide Marko ja Tarko intervjuud aitavad mõista, kuidas teenusetõkesturünnakud Eestis reaalselt toimuvad ja kuidas nendega praktikas tegeletakse.

Tulevikus võiks seda tööd edasi arendada, näiteks uurides rakenduskihis teostatavaid ründeid. Kuna selliseid ründeid arendatakse tõenäoliselt tulevikus rohkem välja, siis on mõistlik olla nendega kursis. Teiseks uurimisobjektiks võiks olla robotvõrgud – kuidas neid kontrollitakse, kuidas leitakse uusi lülisid võrku ja kuidas neid kasutatakse rünnete teostamiseks.

Denial of Service Attacks and Defense Solutions

Bachelor's Thesis (6 ECTS)

Erki Vaino

Summary

Over the last years denial of service attacks have been gaining a lot of popularity amongst hackers and activists. New more sophisticated methods of attack have been developed and used against users across Internet. Idea behind the attack is to consume enough victims resources that he is no longer able to serve other legitimate users. In the beginning there is a short overview of DoS attacks and how can they be classified.

DoS attacks by exploited vulnerability:

1. Malformed packet attacks
2. Flooding attacks
3. Amplification attacks
4. Protocol exploit attack

This method of classification is used to segment different attacks in to groups.

Early days of DoS attacks consisted mostly of malformed packet attacks and attacks that flooded networks with a lot of data. On today's network these attacks have little effect because packets with faulty data will be dropped by routers and switches before any damage can be done.

10-15 years ago flooding attacks were serious problems to victims. But because of today's powerful computers simple flooding attacks have lost their effect on networks. Distributed denial of serve attacks are much more powerful and will cause serious damage to networks and systems. DNS server and unprotected networks are used to amplify the attacks and can cause serious outage to networks. Hackers can also easily rent botnets to do attacks on the victim.

More sophisticated attacks are used on application layer. These attacks don't require a large botnet to do damage. A simple laptop will be able to take a webserver offline with Slowlorise or RUDY attack. These attacks are hard to detect and mitigate.

Popular P2P technologies are also used in denial of service attacks because of their large user base, who can be used as attackers without them even knowing.

Due to SSL requiring a lot of computation power from the server some attacks have been developed to use that in attackers advantage.

Second half of the work is to give a overview of defense methods. Organizations need to understand that DoS attacks can cause serious financial and reputation loss. Over the years defense methods and solutions have been created to combat the rising threat of DDoS attacks.

DDoS defense mechanism by activity [2]

1. Intrusion prevention
2. Intrusion detection
3. Intrusion response
4. Intrusion tolerance and mitigation

Preventing attacks even getting to the network is the best kind of defense, but not always possible, since some application layer DoS attacks can be stealthy and go unnoticed until it is too late, detecting attacks is really important. Also reacting to attacks needs to be considered, having a plan, and response should be considered by IT departments. Since DoS attacks are really hard to stop completely, mitigating and tolerating the effects is the best solution.

Many companies have developed solutions against attacks. Cisco, F5 and Check Point have developed special hardware and software products against denial of service attacks.

CloudFlare is Content Delivery Network and due to its distributed nature can easily protect against layer 3 and 4 flooding attacks. In addition CloudFlare have developed solutions against higher level attacks and are able to keep websites up, even during serious DDoS attacks.

Viited

1. CloudFlare advanced DDoS protection https://www.cloudflare.com/ddos (03.01.2015)
2. Christos Douligeris ja Dimitrios N. Serpanos, Network Security Current Status and Future Directions, 2007
3. LAND Attacks http://www.imperva.com/resources/glossary/land_attacks.html (03.01.2015)
4. Understanding Land Attacks http://www.juniper.net/techpubs/software/junos-security/junos-security96/junos-security-swconfig-security/land-attacks-understanding.html#land-attacks-understanding (03.01.2015)
5. LAND Attack http://security.radware.com/LAND-attack.aspx (03.01.2015)
6. The LAND attack (IP DOS) http://insecure.org/sploits/land.ip.DOS.html (03.01.2015)
7. Christmas Tree Attacks http://www.aries.net/home/demos/Security/chapter2/2_1_4.html (03.01.2015)
8. Understanding Teardrop Attacks http://www.juniper.net/techpubs/software/junos-es/junos-es93/junos-es-swconfig-security/understanding-teardrop-attacks.html (03.01.2015)
9. Teardrop Attack http://security.radware.com/knowledge-center/DDoSPedia/teardrop-attack/ (03.01.2015)
10. Stelios Antoniou, The PING of Death and Other DoS Network attacks http://www.trainsignal.com/blog/ping-of-death-and-dos-attacks (03.01.2015)
11. Understanding Ping of Death Attacks http://www.juniper.net/techpubs/software/junos-security/junos-security96/junos-security-swconfig-security/id-64486.html#id-64486 (03.01.2015)
12. Rose Frag Attack Explained http://www.digital.net/~gandalf/Rose_Frag_Attack_Explained.txt (03.01.2015)
13. Understanding ICMP Flood Attacks http://www.juniper.net/techpubs/software/junos-security/junos-security96/junos-security-swconfig-security/id-25581.html#id-25581 (03.01.2015)
14. CERT Advisory ca-1996-01 UDP Port Denial-of-Service Attack http://www.cert.org/advisories/CA-1996-01.html (03.01.2015)
15. Understanding UDP Flood Attacks http://www.juniper.net/techpubs/software/junos-security/junos-security96/junos-security-swconfig-security/id-60351.html#id-60351 (03.01.2015)

16. TCP SYN Flooding Attacks and Common Mitigations http:/tools.ietf.org/html/rfc4987 (03.01.2015)

17. Understanding SYN Flood Attacks http://www.juniper.net/techpubs/software/junos-security/junos-security96/junos-security-swconfig-security/id-34128.html#id-34128 (03.01.2015)

18. Layer 7 DoS Attacks and Defenses http://www.youtube.com/watch?v=7zQ8lcgxeZk&list=PL23099A7D790EA725 (03.01.2015)

19. ICMPv6 Router Announcement flooding http://www.mh-sec.de/downloads/mh-RA_flooding_CVE-2010-multiple.txt (03.01.2015)

20. How to Prevent Denial of Service Attack http://www.ids-sax2.com/articles/PreventDosAttacks.htm (03.01.2015)

21. Stefan Frei,Ivo Silvestri, Gunter Ollamann, Mail Non Delivery Message DDoS Attacks http://www.techzoom.net/Papers/Mail_Non_Delivery_Notice_Attacks_%282004%29.pdf (03.01.2015)

22. Matthew Prince, Deep Inside a DNS Amplification DDoS Attack http://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack (03.01.2015)

23. THC-SSL-DOS Attack Tool, http://www.youtube.com/watch?v=Ex2xz0ZOKKs (03.01.2015)

24. SSL/TLS and Computational DoS http:/www.educatedguesswork.org/2011/10/ssltls_and_computational_dos.html (03.01.2015)

25. TLS Renegotiation and Denial of Service Attacks https://community.qualys.com/blogs/securitylabs/2011/10/31/tls-renegotiation-and-denial-of-service-attacks (03.01.2015)

26. Sergey Shekyan, New Open-Source Tool for Slow HTTP DoS Attack Vulnerabilities https://community.qualys.com/blogs/securitylabs/2011/08/25/new-open-source-tool-for-slow-http-attack-vulnerabilities (03.01.2015)

27. Sean Michael Kerner, Denial of Service Attacks Get more Sophisticated http://www.esecurityplanet.com/trends/article.php/3921156/Denial-of-Service-Attacks-Get-more-Sophisticated.htm (03.01.2015)

28. Slowloris HTTP DoS http://ha.ckers.org/slowloris/ (03.01.2015)

29. Slowloris HTTP DoS http://ha.ckers.org/blog/20090617/slowloris-http-dos/ (03.01.2015)

30. ModSecurity Advanced Topic of the Week: Mitigating Slow HTTP DoS Attacks http://blog.spiderlabs.com/2011/07/advanced-topic-of-the-week-mitigating-slow-http-dos-attacks.html (03.01.2015)

31. Sergey Shekyan, Identifying Slow HTTP Attack Vulnerabilities on Web Applications https://community.qualys.com/blogs/securitylabs/2011/07/07/identifying-slow-http-attack-vulnerabilities-on-web-applications (03.01.2015)

32. r-u-dead-yet https://code.google.com/p/r-u-dead-yet/ (03.01.2015)

33. R-U-Dead-Yet, RUDY DDoS Attack Tool http://www.youtube.com/watch?v=k1o9Ya8qxlU (03.01.2015)

34. Kelly Jackson Higgins, Researchers To Demonstrate New Attack That Exploits HTTP http://www.darkreading.com/attacks-breaches/researchers-to-demonstrate-new-attack-th/228000532 (03.01.2015)

35. Windows TCP/IP Denial of Service Attacks (Sockstress) http://www.checkpoint.com/defense/advisories/public/announcement/090809-tcpip-dos-sockstress.html (03.01.2015)

36. Kelly Jackson Higgins, New Denial-Of-Service Attack Cripples Web Servers By Reading Slowly http://www.darkreading.com/attacks-breaches/new-denial-of-service-attack-cripples-we/232301367 (03.01.2015)

37. Are you ready for slow reading? http://shekyan.typepad.com/blog/2012/01/are-you-ready-for-slow-reading.html (03.01.2015)

38. LetDown and HTTP DoS attacks http://securityadventures.wordpress.com/2011/09/21/letdown-and-http-dos-attacks/ (03.01.2015)

39. Lori MacVittie, Layer 4 vs Layer 7 DoS Attack https://devcentral.f5.com/blogs/us/layer-4-vs-layer-7-dos-attack (03.01.2015)

40. Naoum Naoumov ja Keith Ross, Exploiting P2P Systems for DDoS Attacks, https://302326fe-a-a28aa00e-s-sites.googlegroups.com/a/nyu.edu/keithross/Exploiting%20P2P%20Systems%20for%20DDoS%20Attacks.pdf?attachauth=ANoY7cp36UiqxK5f_nrOaTtKrkF4eVtH850Q71L7TRWz2KWUVHGV_wg_9HAeetDPZpE7y0jdpcGHvVoOf0HmzQnZkV9rqua1tFiR6zHdcJm3zHfan1rkBSWw7Nvg9tQaBmqCnjE0Kap0Bu3yltFnJsF92lb3MPekVQBojHeijNnZMidReUySKpP6bSJq37UT-OpXMHurRoJ0sYofRMHU-9TGiMgEB3lQyGipuRftHmn5XKYFIW3yU0I%3D&attredirects=0 (03.01.2015)

41. Denial of Service through hash table multi-collisions http://www.readbag.com/nruns-downloads-advisory28122011 (03.01.2015)

42. David Holmes, HashDos – The Post of Doom Explained https://devcentral.f5.com/blogs/us/hashdos-ndash-the-post-of-doom-explained (03.01.2015)

43. Cisco Traffic Anomaly Detector XT 5600 http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5887/product_data_sheet0900aecd800fa552.html (03.01.2015)

44. Cisco Guard XT 5650
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/product_data_sheet0900aecd800fa55e.html (03.01.2015)

45. Defeating DDOS Attacks
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/prod_white_paper0900aecd8011e927.html (03.01.2015)

46. Mitigating DDoS Attacks with F5 Technology http://www.f5.com/pdf/white-papers/mitigating-ddos-attacks-tech-brief.pdf (03.01.2015)

47. CloudFlare security http://www.cloudflare.com/features-security (03.01.2015)

48. CloudFlare: How does CloudFlare work? http://www.quora.com/CloudFlare/How-does-CloudFlare-work# (03.01.2015)

49. Dos Attacks: Response Planning and Mitigation
http://www.motiv.nl/documenten/whitepapers/check-point-ddos-whitepaper
(03.01.2015)

50. Check Point DDoS Protector Appliances
http://www.checkpoint.com/products/ddos-protector/ (03.01.2015)

51. Rich Miller, P2P Networks Hijacked for DDoS Attacks
http://news.netcraft.com/archives/2007/05/23/p2p_networks_hijacked_for_ddos_attacks.html (03.01.2015)

52. DefensePro: All-in-One Attack Protection with IPS, NBA, DoS Protection and Reputation Services
http://www.radware.com/Products/ApplicationNetworkSecurity/DefensePro.aspx
(03.01.2015)

53. DefensePro DDoS Protection
http://www.radware.com/Products/ApplicationNetworkSecurity/DDoS_Attack_Protection.aspx (03.01.2015)

54. Ipv6-ra-flood http://nmap.org/nsedoc/scripts/ipv6-ra-flood.html (03.01.2015)

55. Peakflow SP Threat Management System
http://www.arbornetworks.com/products/peakflow/tms (03.01.2015)

56. Peakflow SP Solution
http://www.icraft21.com/kor/image/Peakflow%20Datasheet.pdf (03.01.2015)

57. DDoS and Security Reports: The Arbor Networks Security Blog
http://ddos.arbornetworks.com/2012/04/ddos-attacks-on-ssl-something-old-something-new/ (03.01.2015)

58. Convery Sean, Network Security Architectures, Cisoc Press, 2004

59. Service Provider Security,
http://www.cisco.com/web/about/security/intelligence/sp_infrastruct_scty.html#14
(03.01.2015)

60. Matthew Tanase, Closing the Floodgates: DDoS Mitigation Techniques http://www.symantec.com/connect/articles/closing-floodgates-ddos-mitigation-techniques (03.01.2015)

61. Sam Bowne, Win 7 DoS by RA Packets, http://samsclass.info/ipv6/proj/flood-router6a.htm (03.01.2015)

62. Sergey Shekyan, How to Protect Against Slow HTTP Attacks https://community.qualys.com/blogs/securitylabs/2011/11/02/how-to-protect-against-slow-http-attacks (03.01.2015)

63. Dave Pisicitello, Do More to Prevent DDNS DDoS Attacks http://blog.icann.org/2013/04/do-more-to-prevent-dns-ddos-attacks/ (03.01.2015)

64. David Holmes, VU#903934 Post of doom https://devcentral.f5.com/blogs/us/vu-903934-ndash-post-of-doom (03.01.2015)

Lisad

Lisa 1: Intervjuud

Töö praktilises osa intervjueerisin kahte oma ala spetsialisti, kes oma töös teenusetõkestusrünnakutega kokku puutuvad. Mõlemad intervjueeritavad said enne töö avaldamist näha korrigeeritud vastuseid ja kinnitasid, et seda infot võib avalda.

1. **Alustuseks, kes Te olete, ametinimetus ja millised on peamised tööülesanded?**

Marko Veelma, Starmani IP võrgu arendusjuht. Enne seda töötanud 10.a. LinxTelecom-is IP võrgu arhitektina (rahvusvaheline võrk, 12 riiki). Osalenud otseselt nii 2007. aasta pronksiööga seotud DDoS rünnakute vastasel kaitsel kui ka hiljem Gruusia e-teenuste kaitsel.

Tarko Tikan, Eesti Telekomi võrgu ja IT-infrastruktuuri peaarhitekt. Tööülesanneteks on andmesidevõrkude ja IT-infrastruktuuri lahenduste disainimine ja opereerimine.

2. **Kui palju ja kui suuri DDoS-e praktikas tänapäeval tehakse - Eestis ja üldiselt?**

Marko: Tehakse täpselt nii palju kui vaja. Kellel on “jämedamad” torud, nende pihta ka suuremat DDoS-i tehakse. Eestis jäävad numbrid enamasti gigade või isegi kümnete gigade kanti, maailmas ületati sel aastal 300 Gbps piir.

Tarko: Eesti tavapärane DDoS on suurusjärgus 1-2Gbps, harvad ei ole ka 10Gbps suurused rünnakud. Seda eelkõige seetõttu, et Eestis ei ole globaalsel tasemel huvitavaid sihtmärke. Viimase 8 kuu jooksul oleme Elioni infrastruktuuris näinud ~300 rünnakut mahuga alates 1Gbps-st ning kestvusega rohkem kui 5 minutit.

Huvitavate sihtmärkide pihta toimuvad rünnakud mahuga 100Gbps ja rohkem. Näiteks võib tutvuda leheküljega http://www.digitalattackmap.com/ mida tehakse Arbori andmete põhjal (mis omakorda tuleb Arbori süsteemide kasutajate käest). See ei anna kindlasti täit pilti, aga näitab, et rünnak ei ole mingi harv nähtus.

3. **Kui suur DDoS peab praktikas olema, et see märgatav oleks?**

Marko: Täpselt nii suur või natuke suurem, kui on vaja teenuse tõkestamiseks.

Tarko: Alates 1Gbps-st, alla selle ei ole mõtet isegi ühtegi hoiatavat teadet saata.

4. **Mis tüüpi need ründed praktikas on?**

Marko: Enamasti lihtsalt „toru ummistamised“. Harvematel juhtudel ka mingite kindlate rakenduste pihta suunatud rünnakud.

Tarko: 99% on tegu UDP peegeldus tüüpi rünnakutega. Pikka aega kasutati selleks DNS-i, 2014.a. kevadest on liigutud NTP peale, mis võimaldab veelgi suuremat võimendussuhet. Kuna MONLIST-i võimaldavate NTP serverite kinnipanekuga on kõvasti tegeletud, siis viimastel kuudel on jälle ka DNS-i näha.

5. **Kas enamasti on ründed lihtsakoelised ummistus rünnakud või esineb ka väga spetsiifilisi/keerukaid/huvitavaid ründeid?**

Marko: Vt. eelmist vastust.

Tarko: Vt. eelmine punkt. Aga teinekord on ka huvitavaid teemasid. Personaalselt olen tegelenud http://www.f-secure.com/v-descs/allaple_a.shtml tagajärgede likvideerimisega (olime sihtmärk, kui töötasin Starmanis). See oli väga hästi konstrueeritud rakenduste taseme rünne (neljanda kihi HTTP päringud).

6. **Millised rünnaku trendid on praegu välja kujunemas, mida tulevik võib tuua?**

Marko: Kasutatakse ära turvaauke erinevates internetti ühendatud seadmetes, mis ei pruugi olla ainult arvutid. Kui arvutite turvalisuse tagamiseks annab näiteks antiviirustega palju ära teha, siis muud võrku ühendatud seadmed kipuvad tihti mõne aasta pärast toeta jääma. Interneti laienedes suureneb ka selliste seadmete arv ning sellest johtuvalt rünnakut teostavate masinate hulk ainult kasvab.

Tarko: Valdavalt UDP võimendusrünnakud. Järgmine populaarne trend on ilmselt SNMP, kust õiget puud *snmpwalk-ides* (kasutades kõrget *maxrepetitions* väärtust) on võimalik saavutada veelgi paremat võimendust. SNMP puhul tuleb skaneerimisega natuke rohkem vaeva näha, kuna kasutada tuleb ka õiget SNMP *community*-it, aga ilmselt on internetis piisavalt palju seadmeid, kus *community* on jäetud kas *public* või *private*.

7. **Kui kergesti on tuvastatav ründe tellija (näiteks klient on saanud ähvardusi või väljapressimiskirju vms)?**

Marko: Seda peab oskama juba rünnaku alla sattunu öelda. Minul otsest kokkupuudet rünnatavaga pole olnud. Väga tihti korraldatakse "meelsusründeid" näiteks portaalide või meediaväljaannete pihta. Sel juhul on ründaja tuvastamine tihti üsna võimatu. Ettevõtete vastu toime pandud rünnete puhul on kahtlustatavate leidmine lihtsam.

Tarko: Minu kõrvu on viimastel aastatel väljapressimisründeid jõudnud ainult üks (ja see oli meie kliendi vastu). Selles juhtumis ilmselt ei suutnud politsei ründajat tuvastada.

8. **Mis sorti klientide pihta need tavaliselt on?**

Marko: Meedia, „hallis alas" või lausa ebaseadusliku tegevusega tegelevad või neile teenuseid pakkuvad ettevõtted on sagedasemad rünnakuobjektid.

Tarko: Pealtnäha täiesti suvaliste klientide vastu, praktikas sisuteenuste pakkujad ning mängurid.

9. **Mis on levinumad meetmed DDoS vastu praktikas?**

Marko: Tehnilistest meetmetest on kõige lihtsam rünnatava teenuse blokeerimine ehk võrguliikluse nn „musta auku“ suunamine. See on tihti ka ründajate eesmärk, aga samas saab teised sama infrastruktuuri kasutavad teenused “päästa”. Palju kallim lahendus on liikluse nö “pesemine”, mis tähendab kogu ründe vastuvõtmist ja filtreerimist. See eeldab juba palju keerukamat (ja kallimat) tehnikat ning piisava mahu olemasolu. Administratiivsetest meedetest võib mainida kliendist “vabanemist”. Viimast kasutatakse tihti klientide suhtes, kes tavaliselt ka oma tegevusega teenusekasutamise tingimusi rikuvad (nö „hallis alas“ tegelevad ettevõtted nagu näiteks rämpsposti saatjad või neile teenuste pakkujad).

Tarko: ISP kohustus on DDoS kliendini kohale toimetada. ISP sekkub alles siis, kui rünnaku maht on nii suur, et see hakkab mõjutama võrgu enda tööd ja seeläbi teiste klientide teenuste kvaliteeti. Siis kasutatakse tavaliselt rünnaku sihtmärgi pihta suunduva liikluse blokeerimise taktikat (st sihtmärk jääb ilma netiühenduseta).

10. **Kui sageli õnnestub ründajat panna rünnet lõpetama (olgu sees siis identifitseerimise kaudu või temale vale pildi tekitamise kaudu või kuidas iganes)?**

Marko: Selle kohta mul adekvaatne info puudub.

Tarko: Praktiliselt mitte kunagi. Ründaja pakub samamoodi teenust, tegelik ründe tellija on keegi kolmas isik.

11. **Mis on levinumad kitsaskohad võrkudes (ribalaius kanalis, ruuteri jaks, ruuteri valesti seadistamine a la *connection tracking*, lõppserverite ülekoormamine, miski muud?)**

Marko: Ebaturvalised seadmed (näiteks turvapaikade puudumine) ja saatja-aadressi võltsimise võimaldamine on suur teene ründajatele. Võrgu suutlikkusega seda probleemi ei lahenda, sest suutlikum võrk suudab ka paremat DDoS rünnet edastada.

Tarko: Ruuteri jaks ei ole tänapäeval probleem. Vähegi tõsiseltvõetava võrgu puhul ei ole seoses liikluse mahtudega nagunii võimalik kasutada tarkvara ruutereid - kogu suunamine toimub raudvara tasemel. Õigesti valitud seadmete puhul ei oma ka PPS mingit rolli.

Ruuterid *conntracki* ei tee - see on tulemüüride teema. See, kes oma avaliku teenuse ette *stateful* müüri paneb, on rumal. Kui muidu on mingigi lootus, et *backend* peab vastu või seda õnnestub vajadusel kiirelt horisontaalselt skaleerimine, siis tulemüüri kaasamisel kukub see kindlasti kõige esimesena kokku. Kõige levinum on siiski sihtmärgi kanali täitumine ja serverite jõudlus.

12. **Mismoodi need ründe leevendamise „kastid“ toimivad?**

Marko: Põhimõtteliselt tegelevad need “hea” ja “halva” liikluse eristamisega erinevate tunnuste alusel ning siis vastavalt filtreerimise või kiiruse piiramisega. Spetsiaalselt rakenduste kaitseks mõeldud kastid töötavad *proxy*-dena ning teavad, mismoodi vastavaid teenuseid kasutatakse ja vastavalt kas vahendavad liiklust või blokeerivad selle.

Tarko: On kaks eraldi osa. Esiteks ründe tuvastamine ja siis selle blokeerimine/filtreerimine.

Tuvastamine toimub üldiselt *netflow* andmete järgi. Kõrgtasemel: lahendusele on selgeks õpetatud, et näiteks IP 1.2.3.4 normaalne võrguliiklusmuster on ~50Mbps ning ~1Mbps allika kohta IP suurenemisega kuni 15Mbps. Vastavalt ka PPS. Kui nüüd koguliiklus või mingi allika IP ületab talle määratud piirid, loetakse see rünnakuks ja liigutakse blokeerimise faasi.

Blokeerimiseks süstitakse näiteks BGP-ga võrku marsruut 1.2.3.4/32 IP kohta, mis tõmbab liikluse filtreerimise kastidesse. Seal omakorda üritatakse blokeerida pakette, mis pole teenusega otseselt seotud (nt HTTP teenus ei vaja UDPd jne). Puhas liiklus suunatakse tagasi

võrku ning tuleb kasutada erinevaid võtteid, et see lõpuks ikka sihtmärgini jõuaks (ilma et võrku süstitud marsruut seda liiklust uuesti filtrisse suunaks).

See on väga kõrgtasemeline jutt - praktikas on kogu ülesseadmine umbes 10x keerulisem.

13. **Millal neist „kastidest“ kasu on ja millal mitte?**

Marko: Kasu on juhul, kui need on piisavalt “targad” ning kui kasti siseneva liikluse maht jääb mõistlikkuse piiridesse ega ummista sisenevat ühendust. Kui rünnak on suunatud otseselt teenuse vastu ning ei kasutata lihtsat võrgu ummistamist, on kastidest kindlasti kasu.

Tarko: Kasu on praktikas ainult ummistusrünnakute korral. Kuna nende näol on tegemist 99% juhtudel UDP peegeldusega, siis on sihtmärkide kaitsmiseks muid meetodeid - HTTP serveritel ei ole UDP-d vaja, rekursiivsed DNS serverid ei pea olema väljaspool oma võrku kättesaadavad jne.

Kuna antud turul on ainus tõsiseltvõetav pakkuja Arbor, siis on nende hinna/kvaliteedi suhe väga paigast ära. Praktikas on võimalik ise mõeldes saavutada palju paremaid tulemusi.

Oma teenuseid tasub hoida normaalsete operaatorite juures, mitte aga koduse ühenduse taga. Operaator omakorda peab olema valmis filtreerimisega tegelema (ning omama selleks piisavalt laiu kanaleid) mitte lihtsalt rünnaku all olevat teenust katkestama. Eraldi võimaluseks on veel oma teenuse CDN-i panemine - viimastest juhtumitest tuleb meelde e-Kooli kolimine CloudFlare CDN taha.

14. **Kuidas käib nn *workflow* ründe korral Teil firmas(Kas klient võtab ühendust, süsteemi monitoorijad annavad alerdi, kas spetsialistid konfigureerivad uusi reegleid, aktiveeritakse leevendamise süsteeme)?**

Marko: See on vägagi konkreetse rünnaku põhine. On nii proaktiivset monitoorimist ja spetsiaalset konfiguratsiooni kui ka rünnaku ajal reageerimist ning tegutsemisplaane.

Tarko: Kuna tegu on firmasisese konfidentsiaalse infoga, ei soovitud kommenteerida.

15. **Midagi lõppsõnaks? Huvitavaid olukordi/rünnakuid?**

Marko: Viimasel ajal pole suurte ja huvitavate rünnakutega ise kokku puutunud. Kõige suurem kogemus tuli 2007-2009 aastatel. Edasine on olnud üsna ühetooniline robotvõrkude rünnakute tõrjumine. Üldiselt on edukas rünnakute tõrjumine väga kallis tegevus. Kindlasti tasub tegeleda erinevate meetmetega rünnakute vältimiseks sh mitte tegeleda "kahtlaste" asjadega. Niisama heast peast kedagi naljaviluks üldiselt ei rünnata. Samas olles pank või mõni muu atraktiivne sihtmärk, ei ole kahjuks taoliste asjade täielik vältimine võimalik. Olemas on erineva efektiivsuse ja hinnaklassiga lahendusi, mille seast parima(te) väljavalimise oskus ongi oluline.

Tarko: Teenuste pakkujad kasutagu usaldusväärseid firmasid kodu- või välismaalt. DDoS ei ole midagi erilist ja kuigi numbrid tunduvad jahmatavad, on ründajad enamasti siiski lihtsameelsed tainapead ☺ ja rünnakud väga lihtsasti filtreeritavad.

Lisa 2: Lihtlitsents

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina_____Erki Vaino_____

(*autori nimi*)

(sünnikuupäev: _____29.06.1989_____)

annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

_____Teenusetõkestusründed ja kaitse lahendused_____,

(*lõputöö pealkiri*)

mille juhendaja on _____Meelis Roos_____,

(*juhendaja nimi*)

reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, 03.01.2015