Palvelunestohyökkäysten tekniikkaa puolustajille

1 Korkean tason hyökkäystyypit

Palvelunestohyökkäykset voidaan karkeasti jaotella kolmeen tyyppiin:

- **Volumetrisiin hyökkäyksiin**, joissa liikennemäärällä on tarkoitus ylittää palvelulle varattu kaistanleveys. Volumetrisiä hyökkäyksiä ovat mm. UDP- tai ICMP-tulvat.
- **Protokollahyökkäyksiin**, joissa kulutetaan esimerkiksi palvelinten, palomuurien tai kuormanjakajien resursseja. Protokollahyökkäykset ovat mm. SYN-tulva tai Ping of Death.
- **Sovellustason hyökkäyksiin**, joissa esimerkiksi hyvin hitailla kyselyillä, GET/POST-tulvalla tai haavoittuvuuksia hyödyntämällä saadaan kohde kaatumaan.

2 Kaista tukkoon liialla liikenteellä

Verkkoresursseja kuluttavat hyökkäykset pyrkivät kuluttamaan kaiken saatavilla olevan kaistan uhrin verkkoyhteydeltä käyttäen suurta määrää liikennettä. Tyypillisesti tällaisten hyökkäysten lähteenä on bottiverkko.

Hyökkäystekniikasta riippumatta palvelu kuin palvelu saadaan lamautettua, mikäli sen verkkoyhteys saadaan tukittua. Viestintävirasto on vuosien varrella käsitellyt lukuisia tapauksia, joissa verkkoyhteys on saturoitunut, koska kohteeseen suuntautuva liikenne on kasvanut suuremmaksi kuin verkon on suunniteltu kestävän. Hyökkäysliikenteen määrästä riippuen häiriöstä on kärsinyt kohteena oleva yksittäinen palvelu, koko palveluntuotantoverkko, teleyrityksen asiakasliittymä tai jopa teleyrityksen runkoverkko.

Yleisimpiä tulvatyyppisiä eli volumetrisiä hyökkäyksiä kuvaillaan alla olevassa taulukossa.

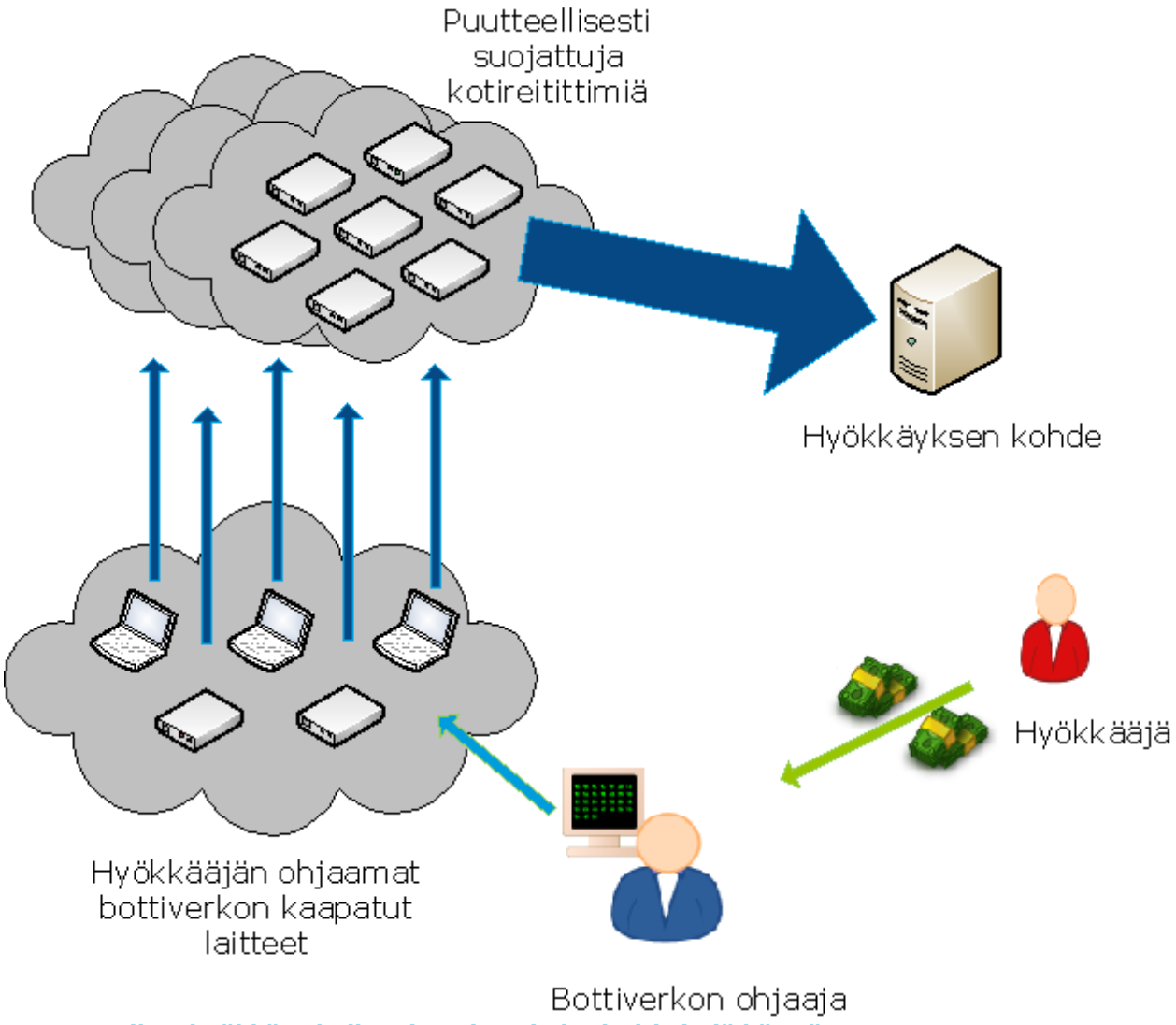
Taulukko 1 Yleisimpiä tulvatyyppisiä (volumetrisiä) palvelunestohyökkäyksiä

Hyökkäys	Kuvaus	Suojautumistapa
UDP-tulva (UDP flood)	UDP-tulva koostuu suuresta määrästä UDP-paketteja, jotka on lähetetty todennäköisimmin väärennetyistä lähdeosoitteista kohdepalvelimelle satunnaisiin portteihin. Kun tietty liikennemäärä/raja ylittyy, kohdepalvelin ei kykene käsittelemään kaikkia sille saapuvia pyyntöjä. UDP-tulva mitataan siirtonopeutena (Mbps) ja paketteina sekunnissa (pps).	• Vastauksena lähetettävien ICMP-vastausten määrän rajoittaminen • Internet-operaattorin tai palveluntarjoajan pakettipesurit
ICMP-tulva (ICMP flood)	ICMP-tulva toimii samalla tapaa kuin UDP-tulva. Liikenne muodostuu ICMP-paketeista, kuten ping-komennon echo request tai echo reply -viesteistä. Esimerkiksi Smurf -hyökkäys toteutetaan lähettämällä väärennetyllä lähdeosoitteella varustettuja ICMP-paketteja verkon broadcast-osoitteeseen, jolloin kaikki kyseisen verkon laitteet saavat kyselyn ja mahdolliset vastaukset menevät väärennettyyn, hyökkäyksen kohteena olevaan osoitteeseen. Kohteen kannalta paketit näyttävät tulevan eri osoitteista, jolloin hyökkäyksen torjuminen IP-osoitteen perusteella ei onnistu. Hyökkääjän osoitetta paketeissa ei näy.	• Internet-operaattorin tai palveluntarjoajan pakettipesurit
DNS-tulva (DNS flood)	DNS-tulvalla tarkoitetaan vastaavasti suurta määrää DNS-kyselyitä, jotka lähetetään tietylle palvelimelle samanaikaisesti esimerkiksi bottiverkon avulla.	• Internet-operaattorin tai palveluntarjoajan pakettipesurit • DNS-vastausten määrän ja timeouttien muokkaaminen ja tiettyjen DNS-pakettien suodatus: http://blog.fortinet.com/post/10-simple-ways-to-mitigate-dns-based-ddos-attacks

3 Peilaamalla vahvistusta heikosti suojatuista palveluista

Vahvistinhyökkäys (amplification attack) tai peilaushyökkäys (reflection attack) tarkoittavat hyökkäystä, jossa hyväksikäytetään verkosta löytyviä UDP-protokollaa hyödyntäviä palveluita kuten DNS , NTP, SNMPv2 tai SSDP. UDP on yhteydetön protokolla, eli liikenteen lähettämiseksi ja vastaanottamiseksi osapuolien ei ensin tarvitse neuvotella yhteyden parametreista. Vastaanottaja ei myöskään tarkista, onko lähettäjän IP-osoite aito vai väärennetty.

Peilattu palvelunestohyökkäys toimii siten, että hyökkääjän ohjaama bottiverkko etsii internetistä koneita, joissa on puutteellisesti suojattu avoin UDP-pohjainen palvelu, esimerkiksi SNMP. Botit lähettävät näille koneille pienikokoisen SNMP-kyselyn, jossa lähdeosoitteeksi on väärennetty uhrin IP-osoite. Välikappaleena toimiva palvelu lähettää vastaukset uhrille eikä boteille (katso Kuva 1).



Kuva 1 Peilaushyökkäys heikosti suojattuja kotireitittimiä käyttäen.

Eri protokollilla on erikokoisia vahvistuskertoimia, jotka perustuvat siihen, että palvelimen tiettyyn kyselyyn antama vastaus saattaa olla huomattavasti suurempi kuin itse kysely.

Joissakin verkoissa verkon reunalla oleva reititin tai palomuuri ei tarkista, onko lähtevän liikenteen osoite väärennetty, mikä mahdollistaa tämäntyyppiset hyökkäykset.

US-CERT kartoitti peilaushyökkäyksille alttiita protokollia, määritti niiden antamat vahvistuskertoimet ja selvitti komennot, joilla peilaushyökkäyksessä käytetty haitallinen liikenne saadaan muodostettua. Niitä esitellään seuraavassa taulukossa.

Taulukko 2 Vahvistinhyökkäysten vahvistuskertoimia ja toteutustapoja

Protokolla	**Liikenteen vahvistuskerroin**	**Haitallisen liikenteen mahdollistava komento**
DNS	28 - 54	Avoimiin nimipalvelimiin kohdistetut kyselyt; ks. https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2013/03/ttn201303251530.html ja http://www.us-cert.gov/ncas/alerts/TA13-088A
NTP	556,9	Monlist -kysely; ks. https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2013/12/ttn201312301707.html
SNMPv2	6,3	GetBulk -kysely
NetBIOS	3,8	Toimialueen nimikysely
SSDP	30,8	SEARCH -kysely
CharGEN	358,8	Character generation -kysely; ks. https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2013/10/ttn201310071710.html ja http://www.us-cert.gov/ncas/alerts/TA13-088A
QOTD	140,3	Quote -kysely
BitTorrent	3,8	File search
Kad	16.3	Peer list -vaihto
Quake Network Protocol	63,9	Server info -vaihto
Steam Protocol	5,5	Server info -vaihto
Multicast DNs (mDNS)	2 - 10	Unicast-kysely
RIPv1	131,24	Väärin muotoiltu kysely
Portmap (RPCbind)	7 - 28	Väärin muotoiltu kysely

Taulukossa esitetty vahvistuskerroin kuvastaa annetun kyselyn koon suhdetta palvelimen lähettämään vastaukseen. Esimerkiksi NTP-protokollan osalta aikapalvelimelle lähetettyyn sopivasti muotoiltuun kyselyyn annettu vastaus on lähes 600 kertaa alkuperäistä kyselyä suurempi. Lisätietoa on US-CERT:n tiedotteessa https://www.us-cert.gov/ncas/alerts/TA14-017A.

Peilaushyökkäykseltä voi suojautua mm. seuraavilla tavoilla:

- Sulje tarpeettomat palvelut.
- Päivitä palvelinohjelmistot. Haavoittuvuudet protokollatoteutuksessa tai tilakoneessa voivat mahdollistaa palvelunestohyökkäyksen.
- Tunnista ja tee hälytys isoista UDP-paketeista yläportteihin - ne voivat olla merkki vahvistushyökkäyksestä. Suodata tarvittaessa.
- Tunnista ja tee hälytys sellaisista UDP-paketeista, jotka eivät vaikuta kuuluvan mihinkään yhteyteen. Suodata tarvittaessa. Katso tarkemmin US-CERT:n ohjeesta https://www.us-cert.gov/ncas/alerts/TA14-017A

4 Alimitoitetut resurssit palvelimella tai verkkolaitteissa

Sen lisäksi, että yhteyksille varattu tietoliikenneyhteyden kaistanleveys on alimitoitettu, myös palvelimen tai verkkolaitteiden resurssit voivat olla riittämättömät.

Palvelimen resursseja kuluttavat hyökkäykset pyrkivät aiheuttamaan jollekin palveluketjussa olevalle laitteelle niin paljon prosessointikuormaa tai kuluttamaan muistia, että palvelu hyytyy siihen. Monet hyökkäyksistä hyväksikäyttävät TCP-protokollan heikkouksia.

Palvelujen tai ohjelmistojen resursseja kuluttavat hyökkäykset voivat kohdistua myös sovelluskerroksen protokollien, kuten HTTP, SMTP tai FTP, heikkouksiin. Palvelutason hyökkäyksiä eritellään seuraavassa taulukossa.

Taulukko 3 Palvelutason hyökkäysten tekniikkaa ja suojautumistapoja

Hyökkäys	Kuvaus	Suojautumistapa
TCP SYN -tulva (puoliavoin kättely)	TCP SYN -tulvahyökkäyksessä väärinkäytetään yhteydellisen TCP-protokollan kolmivaiheista kättelyä. Kohteena olevaan osoitteeseen lähetetään paljon TCP-protokollan yhteydenmuodostuspaketteja (SYN), joihin kohdepalvelin vastaa. Tässä vaiheessa ensimmäisen koneen tulisi viimeistellä kättely, jolloin koneiden välille muodostuu looginen yhteys. Hyökkäyksessä kättely kuitenkin jätetään tahallaan viimeistelemättä ja kohdepalvelin jää turhaan odottelemaan yhteyden valmistumista. Puoliksi muodostuneet yhteydet varaavat resursseja palvelimelta, palomuurilta ja muiltakin verkkolaitteilta. SYN-pakettien lähettäjän IP-osoite voi olla väärennetty, sillä hyökkääjähän ei ole edes kiinnostunut vastauspaketeista. SYN flood ei tavallisesti näy sovellustason lokeissa.	• SYN cookieiden käyttöönotto (katso lisää https://www.incapsula.com/ddos/attack-glossary/syn-flood.html) • DoS Protection -palvelut
TCP RST -hyökkäys	RST-pakettien lähettäjän IP-osoite voi olla väärennetty.	• RST cookieiden käyttöönotto (katso lisää https://www.incapsula.com/ddos/attack-glossary/syn-flood.html) • DoS Protection -palvelut
TCP PSH+ACK -tulva		
HTTP-tulva	HTTP-tulvalla tarkoitetaan hyökkäystä, jossa esimerkiksi tietyn www-palvelun etusivua haetaan suurella joukolla tietokoneita mahdollisimman samanaikaisesti, jolloin pyyntöjen käsittely kuluttaa palvelun resurssit loppuun. Jos esimerkiksi www-sivu rakennetaan palvelimella jokaiselle	• Palvelun hajautus useille palvelimelle ja kuormanjakajan käyttö • Raskaiden tai hitaiden operaatioiden määrän rajoittaminen ajanjaksoa ja IP:tä kohti • Riittävän kaistanleveyden varaaminen perustuen

Hyökkäys	Kuvaus	Suojautumistapa
	käyttäjälle erikseen, voidaan palvelin saada jumiin suhteellisen pienelläkin määrällä yhteyksiä. Samoin on vaara, mikäli www-sivun tuottamiseen liittyy raskaita tietokantahakuja tai muita järjestelmää kuormittavia tapahtumia. Yksinkertaisimmillaan palvelunestohyökkäykseen on pyritty kehottamalla ihmisiä ottamaan yhtä aikaa toistuvia yhteyksiä kohteena olevaan palveluun. Tällainen hyökkäys ei ole välttämättä kovin tehokas. Monet suositut palvelut ovat kuitenkin tukkiutuneet ilman varsinaista hyökkäystarkoitustakin kun käyttäjiä on yhtäkkiä tullut odottamattoman paljon. Jo pelkästään www-osoitteen ilmoittaminen vilkkailla keskustelufoorumeilla tai chat-kanavilla voi aiheuttaa yllättävän kuormituspiikin.	arvioon palvelun suodatuksesta • Pakettipesurin käyttö • Rajoitus palomuurilla, jos hyökkäyksen lähteiden määrä on rajattu. Vaarana myös laillisen liikenteen suodattaminen.
"Low and slow"	"Low and slow" -tyyppisellä palvelunestohyökkäyksellä pyritään saamaan kohdepalvelu palvelunestotilaan ilman suurta liikennemäärää heikkouksia hyväksikäyttämällä. Esimerkiksi Slowloris- tai R.U.D.Y (R U Dead Yet?) -hyökkäystyökalujen avulla voidaan tuottaa protokollan mukaisia paketteja, jotka hitaan lähetysvälinsä vuoksi ohittavat suojausmekanismit, mutta jotka toisin keinoin kuluttavat kohdepalvelimen resursseja. Esimerkiksi hitaasti lähetettyjen HTTP GET -pyyntöjen avulla on mahdollista täyttää palvelun tilataulu ja saattaa se sitä kautta palvelunestotilaan. "Low and slow" -tyyppiset hyökkäykset voivat kohdistua joko palvelimen tai siinä ajettavan palvelun resursseihin.	• Palvelinohjelmiston valinta: kaikki palvelinohjelmistot eivät ole yhtä haavoittuvia esimerkiksi Slowlowrikselle • Timeout-arvojen konfigurointi palvelimella • Kuormanjakajan käyttö, joka hyväksyy vain täydelliset HTTP-pyynnöt • Palvelinkohtaiset suojaustoimet: esimerkiksi Apachen mod_antiloris-moduuli

Joissakin tapauksissa sovelluksen toimintaa voi häiritä edellä kuvattua kolmivaiheista kättelyä vastaavalla tavalla, mutta sovellusprotokollan puitteissa. Esimerkiksi sähköpostipalvelimia voi kuormittaa avaamalla suuri määrä SMTP-yhteyksiä, joiden kautta ei kuitenkaan lähetetä mitään.

Sähköpostipalvelimien kuormitusta on myös havaittu tehtävän siten, että niiden kautta on toistuvasti lähetetty viestejä olemattomille vastaanottajille tai lähettämällä paljon suurikokoisia, pakattuja liitetiedostoja, jotka ovat kuormittaneet vastaanottajan virusskanneria.