MAANPUOLUSTUSKORKEAKOULU

PALVELUNESTOHYÖKKÄYKSILTÄ SUOJAUTUMINEN JA NIIDEN TORJUMINEN

Kandidaatintutkielma

Kadetti
Juuso Oinasmaa

98. Kadettikurssi
Maasotalinja

Huhtikuu 2013

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
98. kadettikurssi	Maasotalinja
Tekijä: Kadetti Juuso Oinasmaa	
Tutkielman nimi: **PALVELUNESTOHYÖKKÄYKSILTÄ SUOJAUTUMINEN JA NIIDEN TORJUMINEN**	
Oppiaine, johon työ liittyy: Sotatekniikka	Säilytyspaikka: Kurssikirjasto (MPKK:n kirjasto)
Aika huhtikuu 2014	Tekstisivuja 30 Liitesivuja

TIIVISTELMÄ

Kybersodankäynnin merkitys on kasvanut viime vuosina merkittävästi, ja yhtenä kybersodankäynnin välineenä voidaan käyttää palvelunestohyökkäyksiä. Tässä tutkimuksessa selvitän millä menetelmillä palvelunestohyökkäyksiltä voidaan suojautua ja miten niitä voidaan torjua. Tutkimuksen pääkysymyksenä on: *Millä menetelmillä voidaan suojautua palvelunestohyökkäyksien vaikutukselta?* ja alakysymyksiä ovat: Mikä on palvelunestohyökkäys ja miten se toimii? Mitä erilaisia palvelunestohyökkäyksiä on olemassa? Miten eri palvelunestohyökkäykset vaikuttavat? Miten palvelunestohyökkäys havaitaan? Tutkielman lähteinä on käytetty pääasiassa aihealuetta käsitteleviä ja sitä sivuuttavia tutkimuksia.

Palvelunestohyökkäyksellä (Denial of Service, DoS) tarkoitetaan Internet-palveluun tai muuhun tietotekniseen palveluun oikeutettujen käyttäjien palvelun käyttämisen estämistä tai huomattavaa hidastamista kuormittamalla joko tietoliikennettä tai itse kohdejärjestelmää. Palvelunestohyökkäykset ovat keskeytyshyökkäyksiä, joilla toisin kuin muilla kyberhyökkäyksillä ei yleensä pyritä varastamaan tietoa tai asentamaan haittaohjelmia, vaan pelkästään estämään palvelun tai järjestelmän käyttö siihen oikeutetuilta käyttäjiltä.

Tutkielman tuloksista selviää, että palvelunestohyökkäyksiä vastaan taisteleminen voidaan jakaa kolmeen osaan: hyökkäysten estämiseen, niiden havaitsemiseen sekä hyökkäyksen torjumiseen. Tärkeintä palvelunestohyökkäysten välttämisessä on niiden ennaltaehkäisy. Hyväksi havaittu yleinen tapa ennaltaehkäistä hyökkäyksiä ja parantaa tietoturvallisuutta on pitää tietoverkko yksinkertaisena, hyvin organisoituna ja hyvin ylläpidettynä sekä päivitettynä. Jokaiseen eri palvelunestohyökkäystyyppiin löytyy kyllä suojautumis- ja torjuntakeinot, mutta niiden tehokkuutta hyökkäyksen pysähtymiselle ei voida taata. Vaikeimpia palvelunestohyökkäyksiä suojautumisen ja torjumisen suhteen ovat hajautetut palvelunestohyökkäykset, koska niitä ei voida suodattaa IP-osoitteen perusteella.

AVAINSANAT

palvelunestohyökkäys, hajautettu palvelunestohyökkäys, IPS, IDS, DDoS, tulvitus, tietoturva, kybersodankäynti, bottiverkko, ennaltaehkäisy, suojautuminen, torjunta

PALVELUNESTOHYÖKKÄYKSILTÄ SUOJAUTUMINEN JA NIIDEN TORJUMINEN

SISÄLLYS

PALVELUNESTOHYÖKKÄYKSILTÄ SUOJAUTUMINEN JA NIIDEN TORJUMINEN

1 JOHDANTO

Kybersodankäynnin merkitys on kasvanut viime vuosina merkittävästi, ja aihe on hyvin ajankohtainen. Yhtenä kybersodankäynnin välineenä voidaan käyttää palvelunestohyökkäyksiä, ja esimerkiksi Yhdysvaltojen armeija on jo vuonna 2008 suunnitellut oman botnetin rakentamista vihollisen tietoliikenneyhteyksien lamauttamiseksi [1, s. 10]. Tässä tutkimuksessa selvitän millä menetelmillä palvelunestohyökkäyksiltä voidaan suojautua ja miten niitä voidaan torjua. Tutkimukseni tarkoituksena on ottaa selvää, miten eri palvelunestohyökkäysten tyypit eroavat toisistaan niin toteutuksen kun etenkin suojautumisen osalta. Ideaalitilanteessa kaikkiin palvelunestohyökkäystyyppeihin on olemassa toteuttamiskelpoiset vastatoimet, jolloin myös vastaavat kaupalliset ratkaisut ovat niitä tarvitsevien organisaatioiden hankittavissa [2, s. 2].

Järvisen [3, s. 14] mukaan tehokas, Suomea varten räätälöity laajamittainen palvelunestohyökkäys saisi maan polvilleen muutamassa tunnissa ilman, että laukaustakaan tarvitsisi ampua. Palvelunestohyökkäyksiltä suojautumisen menetelmien tunteminen on erityisen tärkeää Puolustusvoimissa, koska kyberturvallisuusstrategiassa käsketään Puolustusvoimat suojaamaan omat järjestelmänsä siten, että se kykenee suoriutumaan lakisääteisistä tehtävistään huolimatta kybertoimintaympäristön uhkista [2, s. 8, 28]. Kybertoimintaympäristössä suojautuminen ei ole kuitenkaan aina yksinkertaista, sillä monimutkaisia ja kehittyneitä haittaohjelmia vastaan on vaikea suojautua. Erityispiirteenä kyberhyökkäyksissä on hyökkääjien vaikea tunnistaminen tai heidän olinpaikkansa löytäminen. [2, s. 18]

Tammikuussa 2013 valmistunut Suomen kyberturvallisuusstrategia sekä vuonna 2012 valmistunut turvallisuuspoliittinen selonteko asettavatkin yhdeksi merkittäväksi uhaksi Suomen turvallisuudelle juuri kyberuhkat [4; 5]. Kyberuhkat muodostavatkin laaja-alaisen ja merkittävän haasteen kokonaisturvallisuudelle. Kybertoimintaympäristöön kohdistuvat uhkat ovat muuttuneet vaikutuksiltaan vaarallisemmiksi koko yhteiskunnan kannalta, ja niitä voidaan käyttää

myös poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona muiden perinteisten sotilaallisten voimakeinojen ohella. [3, s. 94; 5, s. 1, 28] Siksi kybertoimintaympäristöä kuvataankin usein neljäntenä sodankäynnin elementtinä maan, ilman ja meren lisäksi.

1.1 Tutkimuksen tarkoitus

Tutkimukseni tarkoituksena on selvittää lähdemateriaalin avulla, millaisia palvelunestohyökkäyksiä on tällä hetkellä olemassa, miten ne voidaan havaita ja miten niiltä voidaan suojautua tai miten ne voisi torjua. Tavoitteena on tarkastella yleisimpien palvelunestohyökkäyksien toimintaperiaatteita sekä keinoja suojautua niiltä tai torjua ne. Tutkielman on tarkoitus luoda kattava yleiskatsaus aiheeseen ilman syventymistä tarkkoihin teknisiin yksityiskohtiin.

Tutkimuksen pääkysymyksenä on: *Millä menetelmillä voidaan suojautua palvelunestohyökkäyksien vaikutukselta?*

Alakysymyksiä tutkimuksessani ovat:

- Mikä on palvelunestohyökkäys ja miten se toimii?
- Mitä erilaisia palvelunestohyökkäyksiä on olemassa?
- Miten eri palvelunestohyökkäykset vaikuttavat?
- Miten palvelunestohyökkäys havaitaan?

Tutkielma on osa Maanpuolustuskorkeakoulun kyberturvallisuutta tutkivaa ryhmätutkimusta. Joe Lindberg tutkii tässä ryhmätutkimuksessa myös palvelunestohyökkäyksiä, mutta hän paneutuu laajemmin palvelunestohyökkäyksien toimintaperiaatteisiin, ja itse keskityn niiltä suojautumiseen.

1.2 Tutkimusmenetelmän valinta

Toteutan tutkimukseni laadullisena kirjallisuuskatsauksena. Tutkimuksessani käytän aiheesta aikaisemmin tehtyjä tai sitä sivuuttavia tutkimuksia ja yhdistän niistä aihealueeseeni liittyvän tiedon. Tutkimusmenetelmä valittiin, koska aihealuetta on varsin laajalti tutkittu, ja näin pystytään etsimään laajin ja yhtenäisin tieto liittyen nimenomaisesti tutkielman aihealueeseen. Tutkielman lähteinä on käytetty pääasiassa aihealuetta käsitteleviä ja sitä sivuuttavia tutkimuksia.

1.3 Tutkimuksen rakenne ja aiemmat tutkimukset

Tutkimukseni koostuu neljästä pääluvusta, joista luvut kaksi ja kolme ovat varsinaisia tutkimuslukuja. Ensimmäisessä tutkimusluvussa kerron lyhyesti erilaisista palvelunestohyökkäyksistä ja niiden vaikutuksista. Ensimmäisessä tutkimusluvussa keskitytään tutkimuksen alakysymyksiin ”*Mikä on palvelunestohyökkäys ja miten se toimii*?”, ”*Mitä erilaisia palvelunestohyökkäyksiä on olemassa*?” sekä ”*Miten eri palvelunestohyökkäykset vaikuttavat*?”. Toisessa tutkimusluvussa selvitän, kuinka erilaisilta palvelunestohyökkäyksiltä voidaan suojautua. Toisessa tutkimusluvussa keskityn tutkielman alakysymykseen: ”*Miten palvelunestohyökkäys havaitaan*?” sekä pääkysymykseen: *Millä menetelmillä voidaan suojautua palvelunestohyökkäyksien vaikutukselta?* Johtopäätöskappaleessa tiivistän vielä tutkimuksen tulokset ja havainnot. Tutkimuksen tärkeimpänä lukuna on luku kolme, jossa vastataan tutkimuksen pääkysymykseen.

Aihealueesta on tehty useampi aikaisempi tutkimus. Aihealuetta käsittelee etenkin Jyri Björkmanin opinnäytetyö ”Palvelunestohyökkäykset ja niiltä suojautuminen (2012)”, Ari Keräsen seminaaritutkielma ”Palvelunestohyökkäykset (2003)”, Jukka Koskisen toimittama seminaariraportti ”Palvelunestohyökkäyksen havaitseminen ja torjuminen (2005)” sekä Jan Seurin opinnäytetyö ”Palvelunestohyökkäysten torjunta (2011)”. Tutkielmassani olen kerännyt ja yhdistänyt tiedon eri vuosina tehdyistä tutkimuksista yhtenäiseksi tutkielmaksi keskittyen omaan rajaukseeni. Tarkoitukseni on myös pitää koko ajan sotilaallinen viitekehys mielessä, koska tämä tutkimus laaditaan Maanpuolustuskorkeakoulussa.

1.4 Tärkeimmät käsitteet ja rajaus

Olen rajannut tutkimukseni käsittelemään etenkin palvelunestohyökkäyksiltä suojautumista ja niiden torjumista. Rajaukseen päädyin siksi, että kybersodankäynnissä puolustuksellisessa doktriinissa on tärkeintä tietää kuinka ennaltaehkäistä mahdollinen hyökkäys ja kuinka toimia hyökkäyksen tapahtuessa. Tärkeimpiä käsitteitä ovat:

palvelunestohyökkäys - Palvelunestohyökkäyksellä (Denial of Service, DoS) tarkoitetaan Internet-palveluun tai muuhun tietotekniseen palveluun oikeutettujen käyttäjien palvelun käyttämisen estämistä tai huomattavaa hidastamista kuormittamalla joko tietoliikennettä tai itse kohdejärjestelmää [6, s. 10; 7, s. 1].

hajautettu palvelunestohyökkäys – Hajautetussa palvelunestohyökkäyksessä (DDoS, distributed denial of service) käytetään hyökkäyksen toteuttamiseen useampaa tietokonetta. Tyypillisesti nämä koneet ovat virusten tai erilaisten haittaohjelmien avulla kaapattuja kotitietokoneita, eli ts. agentteja. [1, s. 4-5]

IP-osoite – Tietyn päätelaitteen Internetissä yksilöivä numerosarja. On olemassa versiot 4 ja 6, jotka tunnetaan lyhenteillä IPv4 ja IPv6. [1]

ICMP – Internet Control Message Protocol. Erilaisia kontrolli- ja virheviestejä internetissä välittävä protokolla. [1]

TCP – Transmission Control Protocol. Internetissä yleisimmin käytetty yhteydellinen tiedonvälityksen protokolla. [1]

UDP – User Datagram Protocol. Yhteydetön protokolla, jolla esimerkiksi pyydetään tietoja nimipalvelimelta. [1]

PDR, Packet Delivery Rate – PDR tarkoittaa onnistuneesti perille lähetettyjen ja virheenkorjauksen jälkeen lukukelpoisten pakettien suhdetta niihin paketteihin, jotka eivät menneet virheettä perille, mutta jotka kuitenkin tunnistettiin saapuneiksi paketeiksi. [9, s. 81]

802.11 – standardi langattomille WLAN-lähiverkoille (Wireless Local Area Network) [9]

2 PALVELUNESTOHYÖKKÄYKSET

Tässä luvussa selvitän erilaisten palvelunestohyökkäysten vaikutusmekanismit pintapuolisesti, jotta voin seuraavassa luvussa tarkemmin selvittää, kuinka niiltä voidaan suojautua ja kuinka ne pystytään torjumaan. Palvelunestohyökkäyksellä (Denial of Service, DoS) tarkoitetaan Internet-palveluun tai muuhun tietotekniseen palveluun oikeutettujen käyttäjien palvelun käyttämisen estämistä tai huomattavaa hidastamista kuormittamalla joko tietoliikennettä tai itse kohdejärjestelmää [6, s. 10; 7, s. 1]. Palvelunestohyökkäykset ovat keskeytyshyökkäyksiä, joilla toisin kuin muilla kyberhyökkäyksillä ei yleensä pyritä varastamaan tietoa tai asentamaan haittaohjelmia, vaan pelkästään estämään palvelun tai järjestelmän käyttö siihen oikeutetuilta käyttäjiltä [6, s. 10; 7, s. 2]. Hyökkäystapoja on useita ja niiden torjumiseen tarvittavat toimenpiteet vaihtelevat hyökkäystavan mukaan.

Palvelunestohyökkäykset voidaan jakaa eri kategorioihin usealla eri tavalla. Yksi jaottelu perustuu palvelunestohyökkäyksen lähteen perusteella hajautettuun palvelunestohyökkäykseen (DDoS, distributed denial of service) ja yksittäisestä lähteestä tapahtuvaan palvelunestohyökkäykseen (ei-hajautettu palvelunestohyökkäys) [1, s. 3; 7, s. 1]. Hyökkäysmekanismin mukaan palvelunestohyökkäykset voidaan jakaa myös kahteen eri luokkaan: *loogisiin hyökkäyksiin* ja *tulvitushyökkäyksiin*. Loogisessa palvelunestohyökkäyksessä suhteellisen pienellä määrällä tarkoituksellisesti muokattuja paketteja käytetään hyväksi jotain tietoturva-aukkoa ohjelmistossa tai protokollan toiminnassa ja saadaan järjestelmä hidastumaan tai jopa kaatumaan kokonaan. Loogiset palvelunestohyökkäykset perustuvat sovellusohjelmissa, käyttöjärjestelmissä ja protokollissa olevien haavoittuvuuksien, ohjelmointi- ja konfigurointivirheiden sekä tietoturva-aukkojen hyödyntämiseen tavalla, joka johtaa järjestelmän hidastumiseen, kaatumiseen tai uudelleenkäynnistymiseen. Sen sijaan tulvituksessa käytetään hyväksi internetin erinomaista tehokkuutta pakettien välittämisessä ja hukutetaan kohde valtavaan määrään turhia paketteja, joiden käsittely kuluttaa kohteen resurssit loppuun. Toisin kuin looginen palvelunestohyökkäys tulvitushyökkäys perustuu valtavaan lähetettyjen pakettien määrään joilla valittu kohde hukutetaan suuren pakettitulvan alle. Paketteja ei ole muokattu älykkäästi, vaan ne ovat hyvin toistensa kaltaisia eivätkä juuri eroa normaalista tietoliikenteestä ja muista uhrin saamista paketeista. [9, s. 69-71]

Luokittelu vaihtelee hieman lähteestä riippuen. Tässä tutkielmassa olen jakanut palvelunestohyökkäykset vaikutusmekanisminsa puolesta hajautettuihin palvelunestohyökkäyksiin, verkkokapasiteetin kuluttamiseen perustuviin palvelunestohyökkäyksiin, resurssien kyllästämiseen

perustuviin palvelunestohyökkäyksiin ja langattomissa verkoissa vaikuttaviin palvelunestohyökkäyksiin [1, s. 3; 7, s. 1]. Jotkin palveluestohyökkäykset vaikuttavat useisiin erityyppisiin järjestelmiin samanaikaisesti, minkä johdosta niitä voidaan kutsua geneerisiksi. Tavallisesti nämä hyökkäykset kuuluvat kaistaleveyden ja resurssien kyllästämisen kategorioihin. Yhteistä edellä mainitun tyyppisille hyökkäyksille on protokollien manipulointi. [7, s. 11]

Erilaisten palvelunestohyökkäysten vaikutus ja laajuus vaihtelevat. Ne voivat joko kohdistua yksittäiseen palvelimeen tai useampaan palvelimeen samanaikaisesti. Ne voivat häiritä ja hidastaa palvelun käyttöä, tai ne voivat jopa kaataa koko järjestelmän ja estää täysin sen käytön. Pahimmassa tapauksessa palvelunestohyökkäys voi tehokkaasti lamaannuttaa tietoliikenneyhteyksistä riippuvaisen yrityksen tai organisaation toiminnan kokonaan. [7, s. 2]

2.1 Hajautettu palvelunestohyökkäys (DDoS)

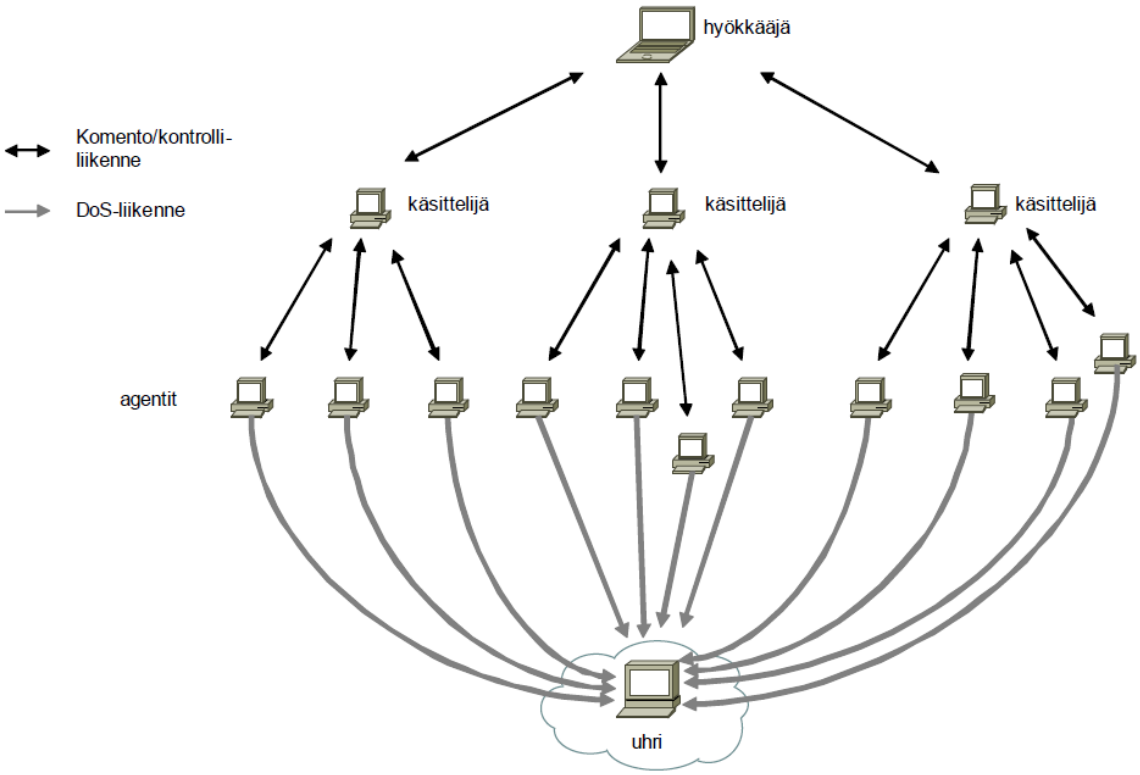
Hajautetussa palvelunestohyökkäyksessä käytetään hyökkäyksen toteuttamiseen useampaa tietokonetta. Tyypillisesti nämä koneet ovat virusten tai erilaisten haittaohjelmien avulla kaapattuja kotitietokoneita, eli ts. agentteja. Haittaohjelman asentaminen onnistuu hyödyntämällä jotain tietoturva-aukkoa tai haavoittuvuutta. Kaapatusta tietokoneesta käytetään usein myös nimitystä zombikone. Haittaohjelman saastutettua tietokoneen se etsii uuden uhrin, johon tartuttaa itsensä. Tällaisesta verkosta, jossa on mukana useampi saastunut tietokone, käytetään nimitystä bottiverkko (botnet). [1, s. 4-5; 2, s. 6-9; 6, s. 13; 7, s. 6-7; 9, s. 73; 10, s. 56-60]

Hyökkäysverkkohierarkia sisältää paljastumisen välttämiseksi varsinaisen hyökkääjän ja agenttien lisäksi käsittelijöitä (handler). Käsittelijä on isäntäkone, johon on onnistuttu tunkeutumaan ja johon on asennettu erityinen ohjelma. Käsittelijät voi olla myös mitä tahansa palvelimia, ja kukin käsittelijä kykenee kontrolloimaan samanaikaisesti useita agentteja. Käsittelijät pyritään sijoittamaan verkkopalvelimille tai reitittimiin, jotka pystyvät käsittelemään suuriakin liikennemääriä, jotta hyökkääjältä käsittelijöille kulkeva liikennemäärä pysyy kohtuullisena ja käsittelijöiden lukuisille boteille lähettämä liikenne hukkuu niiden isäntäkoneen muutenkin suureen tietoliikenteen määrään. [1, s. 4-5; 2, s. 6-9; 6, s. 13; 7, s. 6-7; 9, s. 73; 10, s. 56-60]

Samalla myös jokainen agentti on isäntäkone, johon on tunkeuduttu ja johon myös on asennettuna erityinen ohjelma. Käsittelijä- ja agenttikoneille on asennettu erilaiset haittaohjelmat, jotka mahdollistavat informaation välittämisen. Hyökkääjä kontrolloi agenttikoneita käsittelijäkoneiden avulla. Tämä arkkitehtuuri tekee hyökkääjän paljastumisesta epätodennäköisempää.

Hyökkääjä voi edelleen vaikeuttaa jäljittämistään ns. ponnahduslautojen avulla (ks. 3.5). [1, s. 4-5; 2, s. 6-9; 6, s. 13; 7, s. 6-7; 9, s. 73; 10, s. 56-60]

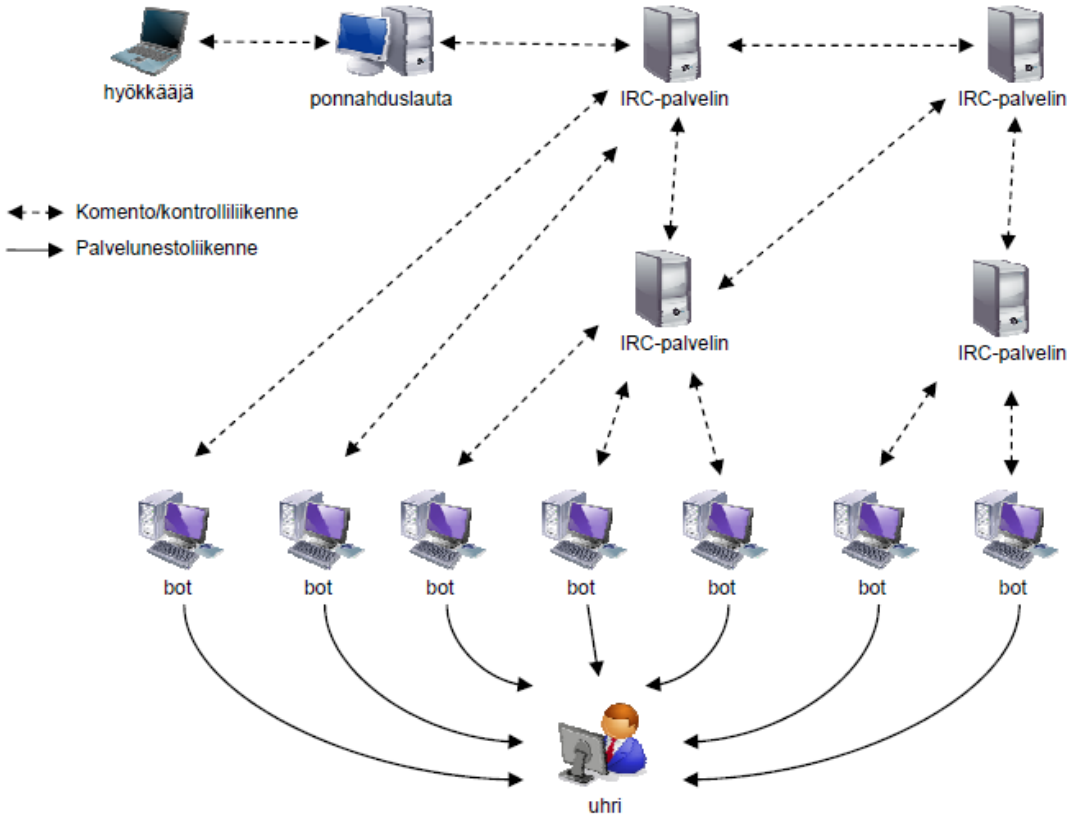
Hajautettu palvelunestohyökkäys jakaantuu kahteen vaiheeseen. Hyökkäyksen ensimmäisessä vaiheessa tavoitteena on saada riittävän suuri määrä haavoittuvia koneita hallintaan. Tässä vaiheessa hyökkääjä etsii verkosta haavoittuvia koneita ja kaappaa ne hallintaansa käyttääkseen niitä hyökkäysvälineinään. Haavoittuvien koneiden etsiminen voidaan toteuttaa manuaalisesti, puolimanuaalisesti tai automaattisesti esimerkiksi skriptien avulla [6, s. 13]. Tämän jälkeen hyökkääjä siirtyy hyökkäysvaiheeseen, jonka tavoitteena on estää uhrikoneita tai -verkkoja tarjoamasta palveluita laillisille käyttäjilleen. Hajautettu palvelunestohyökkäys on esitetty kuvassa 2.1.1. [1, s. 4-5; 2, s. 6-9; 6, s. 12-13; 7, s. 6-7]



Kuva 2.1.1 Hajautetun palvelunestohyökkäyksen toteutus [8, s. 5].

Hyökkääjät käyttävät erilaisia haittaohjelmia toteuttaakseen hajautetun palvelunestohyökkäyksen. Tällaisia ohjelmia ovat mm. Trinoo, TFN, TFN2K ja Stacheldraht [7, s. 6]. Yksi yleinen kanava hajautetun palvelunestohyökkäyksen toteuttamiselle on IRC (Internet Relay Chat). IRC-kanavien välityksellä uhrit löytää helposti ja hyökkäys on helppo toteuttaa. IRC-kanavia voidaan käyttää käsittelijöiden sijasta yhteydenpitoon bottien ja hyökkääjän välillä, ja hyökkäyskomennot voidaan suorittaa IRC-palvelinten kautta. IRC-palvelimilla on normaalistikin runsaasti liikennettä ja hyökkääjän aiheuttama liikennemäärä peittyy helposti muun liikenteen

joukkoon. Myöskään käsittelijöiden ylläpitämää listaa sen hallinnoimista boteista ei enää tarvita, sillä hyökkääjä voi selvittää botit kirjautumalla oikealle kanavalle. Useasta IRC-botista luodulla bottiverkolla palvelunestohyökkäys toteutetaan hajautettuna usealta koneelta. IRC-pohjaisen palvelunestohyökkäyksen tapauksessa käsittelijöinä toimivat siis IRC-palvelimet ja agentteina IRC-botit (kuva 2.1.2). [6, s. 15; 8, s. 73-74; 9, s. 73-74]



Kuva 2.1.2 Hajautetun palvelunestohyökkäyksen toteutus IRC-palvelinten kautta [6, s.15].

2.2 Verkkokapasiteetin kuluttaminen

Tietoverkoilla on aina omat rajansa verkkoliikenteessä. Verkon liikennemäärä riippuu mm. verkon nopeudesta, laitteiden tyypistä ja suorituskyvystä. Verkkokapasiteetin kuluttamiseen pyrkivä palvelunesto toteutuu, kun verkon koko kapasiteetti on käytössä. Palvelunestohyökkäykset, joiden tavoitteena on verkkokapasiteetin kuluttaminen pyrkivät käyttämään kohteen koko verkkokapasiteetin niin tehokkaasti, että joko oikeat pyynnöt palvelimelle tai vastaukset pyyntöihin eivät pääse perille. Hyökkäyksen ei välttämättä tarvitse edes estää pyyntöjä kokonaan. Toisinaan riittää, että pyyntöjä hidastetaan riittävästi. Mikäli pyyntöön ei vastata kymmenessä sekunnissa tai sivun latautuminen kestää kauemmin kuin 10 sekuntia, palvelin koetaan käyttökelvottomaksi ja palvelu estyy. [1, s. 3] Tällöin verkkoon ei pystytä enää lähettämään uutta dataa [6, s. 16]. Tämän tyyppiset hyökkäykset perustuvatkin siihen, että hyökkää-

jillä on käytössään enemmän kaistanleveyttä kuin uhrilla. Tämä onnistuu joko hyökkääjän käytössään olevalla suuremmalla kaistanleveydellä tai yleisemmin vahvistamalla palvelunestohyökkäystä käyttämällä useita palvelimia tulvittamaan uhrin verkon. [7, s. 7] Palvelu on estynyt kuitenkin vain niin kauan, kun koko kaistanleveys on käytössä [6, s. 16].

Verkkokapasiteetin kuluttamiseen löytyy useita eri tapoja. Hyökkäykset toteutetaan usein protokollapohjaisilla tekniikoilla, joissa verkkokaistaa kulutetaan lähettämällä tarkoitukseen suunniteltua dataa. Näitä ovat muun muassa ICMP-tulvitus (Internet Control Message Protocol) ja UDP-tulvitus (User Datagram Protocol). Ns. Ping of Death-hyökkäyksessä eli ICMP-tulvituksessa hyökkääjä lähettää uhrille suuria määriä ICMP echo request –paketteja, joihin on väärennetty lähettäjän osoitteeksi uhrin kohdekoneen osoite. Tällöin kohde vastaa itselleen tuplaten näin verkkoliikenteensä määrän. Hyökkääjä voi lähettää echo request - pakettinsa myös välikätenä käytettävän verkon yleislähetysosoitteeseen, jolloin se välittyy reitittimen ohjaamana kaikille verkon koneille. Kun jokainen kone lähettää vastauksensa uhrille, on yksi hyökkääjän lähettämä paketti tuottanut uhrille monikertaisen määrän paketteja. Tällaista hyökkäystä kutsutaan smurfing-hyökkäykseksi, ja sen avulla vaatimatonkin verkkokaista saadaan moninkertaistettua. [1, s. 3-4; 6, s. 16; 7, s. 11-14; 9, s. 69-72; 12, s. 26]

TCP/IP-protokolla sallii paketin maksimikooksi 65536 tavua, ja ICMP-paketit kapseloidaan IP-pakettien sisään. Monet ping-toteutukset lähettävät oletusarvoisesti 8 tavun kokoisia ICMP-paketteja, mutta ne sallivat kuitenkin käyttäjän määritettäväksi kooltaan suurempia paketteja, jolloin niitä voidaan käyttää palvelunestohyökkäyksiin. Jotkut järjestelmät reagoivat ennalta arvaamattomalla tavalla saadessaan liian suuren IP-paketin; ne voivat esimerkiksi kaatua, hyytyä tai käynnistyä uudelleen. Näin voidaan yhdelläkin paketilla saada hyökkäys toteutettua. [1, s. 3-4; 6, s. 16; 7, s. 11-14; 9, s. 69-72]

Toinen kaistanleveyttä hyödyntävä hyökkäysmuoto perustuu verkkoon liitettyjen järjestelmien ja laitteiden reagointiin. Verkon kaikki koneet voidaan saada reagoimaan samanaikaisesti, jolloin ne käyttävät kaiken saatavilla olevan verkkokapasiteetin. UDP-tulvituksessa periaate on sama kuin ICMP-tulvituksessa, mutta ICMP-pakettien sijaan hyödynnetään UDP-protokollaa käyttäen suuria määriä paketteja, esimerkiksi väärennettyjä DNS-pyyntöjä (ns. Fraggle-hyökkäys). [1, s. 3-4; 7, s. 11-14] Hyökkääjä voi myös saada DNS-palvelimen tallettamaan väärää tietoa, jolloin asiakkaiden pyyntöihin vastataan väärillä tiedoilla [8, s. 12]. Hyökkääjällä on kuitenkin oltava valjastettuna riittävän suuri määrä agentteja, jotta verkon kaistan kulut-

taminen onnistuu [8, s. 13]. Useimmat palvelunestohyökkäyksiin tarkoitetut ohjelmat (Trinoo, TFN, TFN2K ja Stacheldraht) käyttävät TCP-, UDP- tai ICMP-paketteja hyökkäyksiin [7, s. 6].

2.3 Resurssien kyllästäminen

Resurssien kyllästämisellä on tarkoitus kuluttaa kohteen fyysiset resurssit, kuten muisti tai kiintolevytila loppuun. Resurssien kyllästäminen toteutetaan usein tulvittamalla, ja sen tarkoituksena on kasvattaa kohteelle tulevien pakettien määrä niin suureksi, että se joutuu käyttämään ylettömästi resursseja, kuten CPU-aikaa ja muistia, niiden käsittelemiseen. [9, s. 71-72] Jokaisella verkolla ja tietokoneella on rajallinen määrä resursseja (esim. muisti, levytila, prosessoriteho), ja kun yksi tai useampi näistä resursseista on kokonaan käytetty, tapahtuu resurssien kyllästyminen. Resurssien loppuun kuluttamiseen perustuvat palvelunestohyökkäykset yleensä johtavat järjestelmän kaatumiseen, levytilan täyttymiseen tai prosessien hyytymiseen. [6, s. 17; 7, s. 8]. Yleisin resursseja kyllästävä sovellustason hyökkäys on hajautettu palvelunestohyökkäys. Toteuttamalla palvelunestohyökkäyksen sovellustasolla hyökkääjä voi kohdistaa hyökkäyksen suoraan sellaiseen porttiin, jota organisaation tai käyttäjän palomuuri ei ole suojannut. [10, s. 53]

Yleinen esimerkki resurssien kyllästämishyökkäyksestä on niin sanottu SYN-tulvitushyökkäys, jolla pyritään avaamaan lyhyessä ajassa niin paljon puoliavoimia yhteyksiä, että kohdekoneen muisti loppuu kesken ja palvelin kaatuu. Www-palvelimella avattaessa http-yhteyttä asiakas lähettää palvelimelle SYN-paketin. Kun palvelin vastaa, se lähettää takaisin SYN-ACK-paketin. Tämän jälkeen asiakaskone lähettää vielä yhden ACK-paketin, jonka jälkeen yhteys aukeaa. SYN-tulvitushyökkäyksessä hyökkääjä jättää TCP-yhteydet puoliksi avatuiksi, eli hyökkääjä ei vastaa SYN ACK –viestiin ACK-viestillä. Lähettäjän IP-osoite on väärennetty, joten lopullista vastausta ei koskaan saada. Hyökkäysohjelma väärentää lähdeosoitteen valiten joko satunnaisen IP-osoitteen, samaan aliverkkoon kuuluvan naapurin IP-osoitteen tai hyökkäyksen kohteena olevan uhrin IP-osoitteen. Satunnainen IP-osoite saattaa olla epäpätevä, jolloin sitä kantava paketti saattaa kaataa tai jumiuttaa reitittimen. Tätä kutsutaan IP-spoofingiksi. Hyökkääjän väärentäessä paketit ei www-palvelin pysty enää käsittelemään uusia yhteyksiä ja joutuu odottamaan väärennettyjen yhteyksien aikakatkaisua. Www-palvelin kykenee yleensä käsittelemään suuren määrän pyyntöjä, koska pyyntöjen suoritusaika on usein hyvin lyhyt ja pyyntöjä saapuu yksi kerrallaan. Mikäli yhteyspyyntöjä tulee kuitenkin nopeammin kuin mitä palvelin ehtii hylkäämään, palvelimen TCB-muisti (transmission control block) alkaa täyttyä, eikä laillisiin yhteyspyyntöihin kyetä enää vastaamaan. Hyökkäys pystytään siksi toteuttamaan suhteellisen pienellä määrällä SYN-paketteja (esim. 10kpl/min

riittää). Lopputuloksena SYN-tulva estää palvelinta vastaanottamasta uusia yhteyksiä ylittämällä palvelimen käyttämän portin yhteyksien maksimimäärän. Mikä tahansa järjestelmä, joka tarjoaa verkkopalveluja, kuten verkkopalvelin, FTP-palvelin tai postipalvelin, ovat tämän hyökkäystyypin mahdollisia uhreja. Toinen TCP:tä hyödyntävä hyökkäystyyppi on TCP SYN-hyökkäys, jossa hyökkääjä lähettää suuren määrän TCP SYN -paketteja satunnaisiin portteihin kuluttaen uhrin verkkoresurssit, eikä niinkään TCB-muistia. [1, s. 5; 6, s. 15-17; 7; s. 12; 8, s. 10-11]

Yksinkertaisimmillaan resurssien kyllästämiseen perustuva palvelunestohyökkäys onnistuu sähköpostitilin tai webhotellin levytilan loppuun kuluttamisella. Tämä onnistuu lähettämällä palvelimelle tai sähköpostiosoitteeseen suuri määrä suuria tiedostoja. Tällöin laillisen datan kulku muilta käyttäjiltä estyy. [1, s. 5] Sähköroskapostissa (spamming) sähköpostiviestejä lähetetään lukuisille käyttäjille (tai listoille, jotka kattavat erittäin suuria käyttäjämääriä). Vaikutus pahenee, mikäli vastaanottajat vastaavat viestiin, jolloin kaikki alkuperäiset osoitelistassa olleet osoitteet saavat vastausviestin. Tämä voi tapahtua täysin käyttäjän ymmärtämättömyydestä siitä, että viestiin vastaaminen aiheuttaa viestin monistumisen tuhansille käyttäjille. Sähköroskapostia on melkein mahdotonta estää, koska kuka tahansa käyttäjä, jolla on toimiva sähköpostiosoite voi lähettää roskapostia mille tahansa toimivalle sähköpostiosoitteelle. On myös hyvin yksinkertaista päästä sisään suurille postituslistoille tai tietolähteisiin, jotka sisältävät suuria määriä sähköpostiosoitteita ja käynnistää hyökkäyksiä näiden avulla. [7, s. 15]

2.4 Palvelunestohyökkäykset langattomissa 802.11-verkoissa

Langaton verkko on kaapeliverkkoa alttiimpi palvelunestohyökkäyksille, koska radioaallot leviävät joka suuntaan ympäristöönsä ja jokainen kantaman sisällä oleva voi kuunnella tai häiritä muiden lähettämiä viestejä. Toisaalta tästä johtuen myös hyökkääjän on oltava suhteellisen lähellä, kantaman päässä. Langattoman 802.11-verkon tiedonsiirtokapasiteetti on myös huomattavasti kaapeloitua lähiverkkoa ja internetiä pienempi, joten se kärsii helpommin ruuhkasta. Kolmas 802.11-verkkoa palvelunestohyökkäyksille altistava tekijä on todennuksen ja salauksen puute MAC-kerroksen kehyksistä, sillä ainoastaan datakehysten data on salattua. [9, s. 78]

Palvelunestohyökkäyksiä voidaan tehdä langattomaan verkkoon usealla eri tavalla. Esimerkiksi koko siirtotien lähetys/vastaanottokaista voidaan tukkia erittäin voimakkaalla lähettimellä. Vaarallisimmat palvelunestohyökkäykset langattomissa 802.11-verkoissa perustuvat joko ra-

diohäirintään, yksittäisten lähetysten heikkoon todentamiseen tai suurella lähetysmäärällä tulvittamiseen. [9]

Radiohäirinnällä tarkoitetaan laitteiden yhteisesti jakaman siirtotien käyttämisen tai sille pääsyn fyysistä häiritsemistä, ja se käyttää hyväksi radioaalloilla tapahtuvan tiedonsiirron perusrajoitusta: siirtotiellä voi olla vain yksi lähettäjä kerrallaan. Häirintäsignaalia on hyvin helppo muodostaa, ja sitä voidaan tuottaa joko täysin käytetystä protokollasta mitään tietämättä tai sitten älykkäästi ajoittamalla häirintä vain tiettyihin tarkoin valittuihin protokollan kohtiin. Häirintäsignaalin perusteella radiohäirintää käyttävät palvelunestohyökkäykset voidaan jakaa kahteen pääluokkaan, *tyhmään radiohäirintään* ja *älykkääseen radiohäirintään* sen perusteella onko hyökkääjä tietoinen verkossa käytettävästä siirtotien vuoronvarausprotokollasta. [9]

Tyhmässä radiohäirinnässä hyökkääjän ei tarvitse olla tietoinen käytetystä protokollasta. Tyhmällä radiohäirinnällä aiheutetaan joko muiden lähettämien signaalien sotkeutuminen lukukelvottomaksi lähettämällä samanaikaisesti omaa häirintäsignaalia tai estetään muita saamasta siirtotietä käyttöönsä sen ollessa koko ajan varattuna. Häirintäsignaali voi olla joko oikeita kelvollisia paketteja tai pelkkiä satunnaisia bittejä. Häirintäsignaalin energian on oltava tarpeeksi suuri, jotta häirintä tuottaa täydellisen palvelunestohyökkäyksen, jolloin yksikään lähetys ei pääse virheettömänä perille. [9]

Tyhmä radiohäirintä voidaan jakaa edelleen *jatkuvaan*, *pulssimaiseen* ja *reagoivaan* radiohäirintään. Kaikkein yksinkertaisin radiohäirintä on jatkuva verkon toimintataajuudella lähetettävä signaali, jolloin siirtotien ollessa jonkin muun laitteen käytössä hyökkäyksen käynnistyessä hyökkäys sotkee lähettäjän signaalin täysin eivätkä vastaanottajat saa siitä mitään selvää virheenkorjauksesta huolimatta. Mikäli taas siirtotie on vapaana hyökkäyksen alkaessa, eivät muut laitteet yritä päästä siirtotielle havaitessaan sen olevan koko ajan varattuna. Jatkuvan häirintäsignaalin sijaan hyökkääjä voi tehdä pulssimaista radiohäirintää lähettämällä lyhyehkön signaalin säännöllisin väliajoin. Pulssimainen hyökkäys ei näytä täysin säännölliseltä ja sitä on vaikeampaa havaita. Hyökkääjä voi myös tehdä pulssimaista häirintää, joka reagoi siirtotien vapauteen. Tällöin hyökkääjä lähettää häirintäsignaalia havaittuaan siirtotien olevan vapaana DIFSin (DCF Interframe Space) mittaisen ajan, jolloin häirintäsignaali joko sotkee jonkun toisen laitteen lähettämän datakehyksen, tai estää muita laitteita lyhentämästä omaa odotusaikaansa kilpailuikkunassa. Reagoivassa radiohäirinnässä hyökkääjä kuuntelee siirtotietä, ja vasta havaitessaan siirtotiellä jonkun muun lähettämää signaalia, aloittaa häirinnän. Hyök-

kääjä lähettää lyhyen ajan häirintäsignaalia ja sotkee toisen lähetyksen, jonka jälkeen hiljentyy kuuntelemaan siirtotietä. [9]

Älykkäällä radiohäirinnällä pyritään saavuttamaan tyhmän radiohäirinnän edut, mutta välttämään sen ongelmia, kuten suurta energiankulutusta ja helppoa havaittavuutta. Älykäs hyökkäys voidaan kohdistaa tarkemmin vain tiettyyn laitteeseen. Älykkäässä radiohäirinnässä hyökkääjän on tiedettävä onko verkossa käytössä siirtotien varaukseen ja käyttöön liittyvät CSMA/CA (Carrier Sense Multiple Access With Collision Avoidance) tai RTS/CTS:llä (Request to Send / Clear to Send) -protokollat, minkä lisäksi hyökkääjän on seurattava liikennettä ja ajoitettava hyökkäyksensä tiettyihin protokollan vaiheisiin. Hyökkäyksessä voidaan sotkea verkossa liikkuvia kehyksiä, mutta häirintä ajoitetaan tiettyihin data- tai kontrollikehyksiin. Datakehysten sijasta hyökkääjä voi myös sotkea kuittaukset, jolloin hyökkääjä seuraa verkon liikennettä ja sotkee häirintäsignaalillaan datakehyksen jälkeen tulevan ACK:n. [9]

Myös 802.11-verkoissa voidaan tehdä palvelunestohyökkäystä tulvittamalla. Tulvitus voidaan suorittaa mm. probe request, authentication request sekä association request -kehyksillä. Tulvoi onnistua myös reassociation request- ja PS-Poll-kehyksillä, mutta niiden käyttöä ei ole tutkittu. Tulvitushyökkäys kohdistuu 802.11-verkoissa aina tukiasemaan ja perustuu yhteyden muodostuksen eri osapuolilta vaatimaan epätasaiseen resurssien kulutukseen. Hyökkääjä voi lähettää helposti valtavan määrän sopivia hallintakehyksiä väärennetyllä MAC-osoitteella, jolloin runsas hallintakehysten tulvitus kuluttaa tukiaseman resursseja niin paljon, ettei tukiasema voi enää palvella muita asemia. [9]

Langattomien 802.11-lähiverkon kehityksessä huomio on keskittynyt vuosien varrella lähinnä vain datan salaukseen, luotettavaan osapuolten väliseen todennukseen ja kehysten eheyteen, minkä takia saatavuuden varmistaminen on jäänyt tietoturvaa parannettaessa vähemmälle huomiolle ja sitä uhkaavat erityisesti palvelunestohyökkäykset. Langattomat 802.11-verkot on suojattu joko WEP, WPA tai WPA2-salausmenetelmillä. WEP-salaus on kohtuullisen helppo murtaa jopa kotikäyttäjän toimesta, minkä takia suurin osa 802.11-verkoista on nykyään suojattu WPA/WPA2-salauksella. WPA:n huonona puolena pidetään kuitenkin sen tapaa suojautua DDoS-hyökkäyksiltä. Kun palvelunestohyökkäys havaitaan, WPA sulkee koko verkon minuutiksi, jolloin myös verkon lailliset käyttäjät jäävät ilman verkkoa. [9, s. 78; 12, s. 17-21]

3 PALVELUNESTOHYÖKKÄYKSIEN HAVAITSEMINEN JA TORJUMINEN

Palvelunestohyökkäyksiltä suojautumista edesauttaa oman tietoverkon tunteminen ja organisointi. Mikäli yleiset haittaohjelmilta suojaavat keinot kuten virustorjunta, palomuuri ja päivitykset eivät riitä suojaamaan järjestelmää, on etsittävä muita suojautumiskeinoja. Tässä kappaleessa selvitän, miten voidaan ennaltaehkäistä hyökkäys ja torjua se, mikäli hyökkäys on onnistunut jo vaikuttamaan.

Palvelunestohyökkäyksiä vastaan taisteleminen voidaan jakaa kolmeen osaan: hyökkäysten estämiseen, niiden havaitsemiseen sekä hyökkäyksen torjumiseen [9, s. 75]. Palvelunestohyökkäyksien havaitseminen on kiinteässä yhteydessä niiden torjumiseen. Havaitseminen itsessään on harvoin vaikeaa, mutta siihen liittyy monia asioita, joilla on vaikutusta torjunnan onnistumiseen. [8, s. 1] Mikäli epäilee joutuneensa palvelunestohyökkäyksen kohteeksi, on suotavaa heti ottaa yhteyttä verkko-operaattoriin ja selvittää tilanne heidän kanssaan. Myös palvelimen, palomuurin tai muun verkkolaitteen lokitiedoista voi selvitä paljon hyökkäyksen laadusta. Näin voidaan varmistua siitä, että kyseessä on palvelunestohyökkäys eikä esimerkiksi laitevika tai asetusvirhe. [6, s. 24]

Hyökkääjät etsivät yleensä koneita, joista löytyy laajakaistayhteys, hyvät resurssit ja jotka ovat huonosti ylläpidettyjä. Kun hyökkääjä löytää haavoittuvan koneen, täytyy sen ensin murtautua kyseille koneelle. Yleensä tämä hoituu kyseessä olevaa haavoittuvuutta hyväksi käyttäen. [8, s. 5-7] Sen takia on tärkeää puuttua näihin haavoittuvuuksiin ennaltaehkäisevästi.

3.1 Palvelunestohyökkäyksen havaitseminen ja tunnistaminen

Palvelunestohyökkäys voidaan havaita seuraamalla mm. sisään tulevaa verkkoliikennettä, ulkopuolisten käyttäjien lukumäärää, käyttäjien käyttäytymistä, palvelimien kuormitusta sekä käytettyjä resursseja. Hajautettujen DDoS-hyökkäysten havaitseminen ei ole helppoa, sillä ne muistuttavat erehdyttävästi normaalia liikennettä, joten on vaikea erottaa onko kasvanut liikenne normaalia vai hyökkäyksestä aiheutuvaa. DDoS-hyökkäysten havaitsemiseen on kaksi tapaa: joko hyökkäys havaitaan kullekin DDoS-hyökkäykselle tyypillisistä erityispiirteistä tai mallinnetaan verkon toimintaa normaaliaikana, jolloin hyökkäyksen aiheuttamat muutokset voidaan havaita. [6, s. 24; 9, s. 75-76]

Kun palvelunestohyökkäys on havaittu, tulee se aina tunnistaa vaikutusmekanismin puolesta. Vaikutusmekanismit on esitelty kappaleessa 2. Palvelunestohyökkäyksen tyypin tunnista-

minen helpottaa sen torjumista oleellisesti. Hyökkäys voidaan torjua joko suodattamalla se tai kaistanrajoittamisella. Valinta näiden kahden välillä riippuu liikenteen luokittelun tarkkuudesta. Mikäli hyökkäystyyppi saadaan tarkasti tunnistettua, voidaan tämä häiriöliikenne suodattaa kokonaan pois. Suodattamalla saadaan poistettua kaikki epäilyttävät paketit liikenteen luokittelun perusteella. Sen sijaan kaistanrajoituksella vahvistetaan tietty kaista epäilyttäville paketeille. [6, s. 24]

Mikäli palvelunestohyökkäyksen lähde on organisaation sisäisen verkon kone, voidaan tällainen hyökkäys havaita seuraamalla ulospäin suuntautuvaa liikennettä. Myös lähdeosoitteen väärentämisen havaitseminen antaa viitteitä verkon hyväksikäytöstä. Havaitsemisen jälkeen on tärkeää suodattaa ulospäin menevää liikennettä uhrikohteisiin ja yrittää tunnistaa hyökkäyskoneet. Kun hyökkäyskoneet saadaan tunnistettua, kaapatut koneet voidaan poistaa verkosta, ottaa kovalevyistä kopiot, tutkia hyökkäyskoodi ja lopulta puhdistaa koneet. Kone tulee aina puhdistaa huolellisesti, sillä haitallinen koodi voi olla hyvin piilotettu. [6, s. 24]

Palvelunestohyökkäykset voidaan havaita myös määrittämällä verkon ulkorajan tilanne normaalitilanteessa. Yksi tapa jonkin tietyn hyökkäyksen havaitsemiseksi on seurata verkkoliikennettä jollain mittarilla ja etsiä hyökkäyksen aiheuttamaa muutosta, esimerkiksi TCP-protokollassa SYN-pakettien suhdetta FIN- ja RST-paketteihin. Tällä tavoin voidaan havaita SYN-paketeilla tapahtuvan hyökkäyksen aiheuttama epätavallisen suuri SYN-pakettien suhde muihin paketteihin. Volyymimittarilla voidaan selvittää pitkän aikavälin normaalivolyymi, jonka jälkeen on määritettävä riittävän oikea-aikaiset kynnysarvot, jotka ylittyessään kertovat, että tilanne ei ole enää normaali. Hyökkääjä voi kuitenkin harhauttaa lähettämällä SYN-paketin lisäksi sopivasti FIN- tai RST-paketteja, jotta liikenne vaikuttaisi normaalilta. [11; 9, s. 76]

3.2 Yleiset ennaltaehkäisevät suojautumismenetelmät

Vaikka ennaltaehkäisevät toimenpiteet eivät suojaisikaan verkkoa täydellisesti, kohtuullisen korkea suojaus voi turhauttaa hyökkääjän luopumaan aikeistaan tai etsimään uhreikseen helpompia kohteita. Hyvin moni palvelunestohyökkäys käyttää hyväkseen tunnettuja tietoturva-aukkoja ja ohjelmointivirheitä. Perussuojautumismenetelminä voidaankin pitää ennaltaehkäisevää toimintaa päivittämällä ja korjaamalla ohjelmistoista tunnistetut tietoturva-aukot, huonojen protokollien rakenteet sekä kehittämällä resurssien hallintaa. Siksi suojautumisessa onkin ensisijaisen tärkeää, että ohjelmistojen ja käyttöjärjestelmien valmistajien uusimmat korjauspäivitykset on asennettuna järjestelmään [1, s. 38; 6, s. 22; 7, s. 18]. Yleisesti hyväksi havaittu

tapa parantaa tietoturvallisuutta on pitää tietoverkko yksinkertaisena, hyvin organisoituna ja hyvin ylläpidettynä. [6, s. 22; 8, s. 16-17]

Ennaltaehkäisyyn kuuluu myös olennaisesti haavoittuvuuksien kartoittaminen. Verkkopalveluille tulisi tehdä aika ajoin oikeanlaista kapasiteettitestausta. Testauksessa tulisi käydä läpi palvelun koko ketju edustasta taustajärjestelmiin asti ja selvittää palvelun pullonkaulat. Tämä ei merkittävästi eroa normaalista kuormitustestauksesta. Kuitenkin valitettavan usein testataan vain yhtä järjestelmän osaa kerrallaan, mikä ei vastaa kokonaiskuvaa. [11] Useat erilaiset tulvitushyökkäykset sekä resurssien kyllästämiseen perustuvat hyökkäykset kyetään helposti mallintamaan ja toteuttamaan käytännössä, minkä perusteella voidaan löytää verkkopalveluiden pullonkaulat turvallisesti ennen mahdollista ”kovaa” palvelunestohyökkäystä.

Eräs yksinkertainen ja yleinen haavoittuvuus on heikko salasana. Aivan liian usein hyökkääjä kykenee löytämään tai selvittämään käyttäjätunnus/salasana -parin ja saa näin järjestelmän luvatta käyttöönsä. [8, s. 5-7] Kun hyökkääjä on päässyt järjestelmään käsiksi admin–oikeuksilla, kykenee hän muuttamaan järjestelmän ja verkkoympäristön asetuksia ja siten joko helpottamaan ulkopuolisen palvelunestohyökkäyksen toteuttamista tai luomaan palvelunestohyökkäyksen sisältä käsin. Salasanojen suhteen onkin noudatettava tarkkoja varotoimenpiteitä, etenkin silloin, kun kyseessä ovat pääkäyttäjän oikeudet.

3.3 Suojautuminen organisoinnilla

Tietoverkon organisointi vaikuttaa merkittävästi siihen, kuinka helposti palvelunestohyökkäys voi onnistua kyseisessä verkossa. Organisaation tulisi tarkkailla resurssiensa käyttöä sekä järjestelmän suorituskykyä ja määriteltävä tasot normaalikäytölle, kuten kappaleessa 3.2 selvisi. Näin voidaan havaita poikkeuksellinen levyn ja keskusmuistin käyttö sekä epätavallinen verkkoliikenne. Lisäksi verkon kriittiset palvelut on tunnistettava, ja niihin on kohdistettava erityistoimenpiteitä, joihin kuuluu mm. verkkolaitteiden ja järjestelmien huolellinen konfigurointi. Mikäli konfigurointitiedoissa havaitaan muutoksia, viestii se palvelunestohyökkäyksestä. Muutokset konfigurointitiedoissa tai muissa tiedostoissa voidaan havaita sopivilla ohjelmistotyökaluilla. Verkkokonfigurointitietojen on syytä olla vikasietoisia, ja niistä on aina syytä olla varmuuskopioita. Säännöllisten varmuuskopiointien ylläpito edistää tehokkaasti palvelunestohyökkäyksien vaikutuksien torjumista. [6, s. 22; 7, s. 17-18]

Hajauttaminen on yksi erittäin toimiva ja yksinkertainen tapa vähentää hyökkäyksen vaikutuksia. Organisaation palvelut kannattaakin hajauttaa usealle eri palvelimelle [1, s. 7]. Tietoverkko tulisi

organisoida siten, että kriittiset sovellukset ovat jaettu usealle eri palvelimelle, jotka sijaitsevat eri aliverkoissa. Kun oman verkon infrastruktuuripalvelut ovat pois varsinaisen verkkopalvelun läheltä, ne eivät kaadu yhtä aikaa. Siksi organisaation ei tulisi käyttää palvelimia, joilla on useita tehtäviä. Jokaisella palvelimella tulisi olla vain yksi tehtävä ja tarkoin määritelty toiminnallisuus. Myös laskentakapasiteettia tulisi hajauttaa oman verkon sisällä ja varata varmuudeksi lisäkapasiteettipalveluita toisaalta verkkoavaruudesta. Hyvin organisoidussa verkossa hyökkäyksen kohteeksi joutuneet palvelimet voidaan tunnistaa, eristää ja lopuksi korvata toimivilla ilman palvelutason heikkenemistä. Tämä luo tietoverkolle kestävyyttä ja nopeuttaa toipumista hyökkäykseltä. [6, s. 22-23; 11]

3.4 Suojautuminen hankkimalla lisää resursseja

Suojautuminen palvelunestohyökkäyksiltä hankkimalla lisää resursseja lienee tehokkain, mutta samalla kallein menetelmä ennaltaehkäistä hyökkäykset. Hankkimalla lisää resursseja voidaan tietoverkon kestävyyttä lisätä joko staattisesti ostamalla lisää resursseja tai dynaamisesti hankkimalla hajautetusti organisaation tietoverkon ulkopuolisia palvelimia ja toisintamalla kohdepalvelimet. Kapasiteetin lisääminen on yksinkertainen, mutta kallis tapa vaikeuttaa palvelunestohyökkäyksen onnistumismahdollisuuksia. Palvelinkapasiteettia voidaan ostaa sisällön hajauttamispalveluita tarjoavilta organisaatioilta. Palvelunestohyökkäyksen varalta tulisi suosia palveluita, joissa lisäkapasiteetin ostaminen käy nopeasti [11]. [6, s. 23] Kapasiteetin ylimitoittamisessa on kuitenkin muistettava, että verkon eri osien on oltava tasapainossa keskenään, sillä muuten muodostuu pullonkaula eikä ylimitoittamisella saavuteta käytännön hyötyä [1, s. 6].

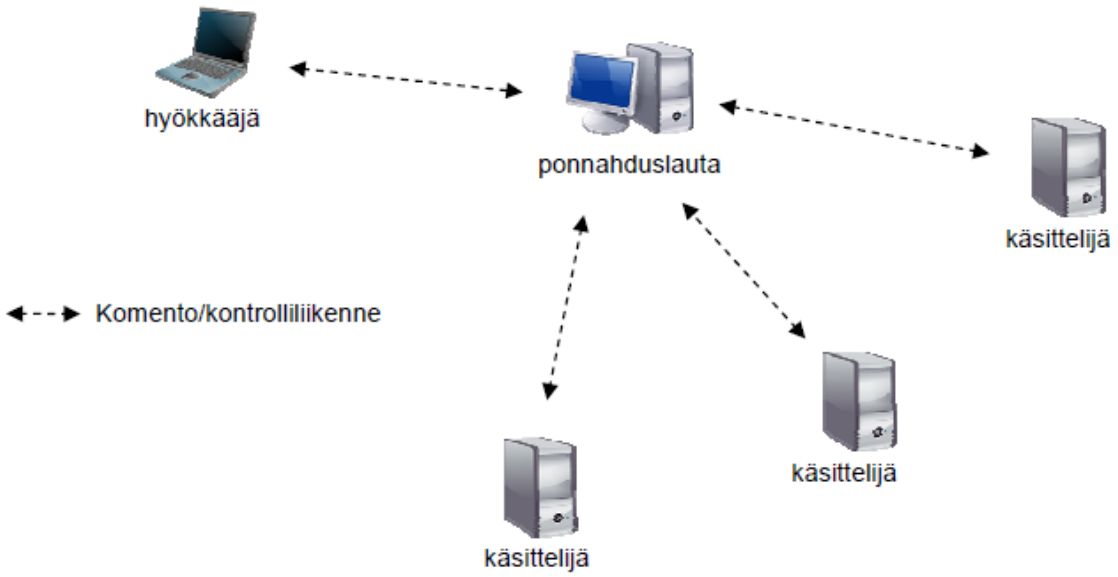
3.5 Suojautuminen hajautetulta palvelunestohyökkäykseltä

Mikäli palvelunestohyökkäys tulee yksittäisestä IP-osoitteesta, on se helppo suodattaa pois. Hajautetussa palvelunestohyökkäyksessä suojautuminen on paljon vaikeampaa, koska yksittäisten IP-osoitteiden suodattaminen ei ole hyödynnettävissä. [1, s. 4] Hyökkääjän kannalta IP-osoitteen väärentäminen eli IP-spoofing ei ole tarpeellista tulvahyökkäyksissä, kun agentteja on huomattavan paljon (yli 10 000) [8, s. 11]. Jotta hyökkäyksen vaikutuksia saadaan vähennettyä, on tärkeää eristää ulospäin näkyvät palvelut omaan IP-avaruuteen, jotta hyökkäykset eivät estä esimerkiksi sähköpostin ja VPN-yhteyksien toimintaa. [6, s. 22]

Bottiverkon tuhoamiseksi yleensä paras tapa on hallintapalvelimien sulkeminen. Näitä hallintapalvelimia sulkevat oikeusviranomaiset, kuten kansainväliset tietoturvaviranomaiset, CERT-it (Computer Emergency Response Team). Hallintapalvelimien sulkeminen estää bottiver-

kon ohjaajaa käskyttämästä botteja. [10, s. 60] Hajautetussa palvelunestohyökkäyksessä hyökkääjän jäljittäminen on kuitenkin hankalaa. Hyökkääjä voi käyttää hyökkääjäkoneen ja käsittelijöiden välillä ”ponnahduslautaa” (kuva 3.2), jolloin hyökkääjä kirjautuu useisiin koneisiin peräkkäin ennen käsittelijään kirjautumista. Jos ponnahduslaudat valitaan eri maista ja eri mantereilta, on jälkien seuraaminen hankalaa. Jotta hyökkääjän jälkiä voidaan seurata, tarvitsee jäljittäjän saada käyttöönsä eri maissa olevia lokitietoja. Tähän vaaditaan kyseessä olevien maiden poliisin lupa, eikä se ole kaikissa maissa edes mahdollista. Mikäli ponnahduslaudat valitaan maista, joissa lokitietojen välittäminen jäljittäjille ei ole mahdollista, on jäljittäminen mahdotonta. EU-maiden välillä lokitiedot välitetään poliisien välillä heti, ja tutkintapyyntö tehdään vasta perässä, mikä nopeuttaa jäljittämistä merkittävästi. [6, s. 14; 8; s. 4]

On myös keino, jolla saadaan selvitettyä koko bottiverkko pelkästään yhden hyökkäykseen osallistuvan koneen perusteella. Hajautetussa palvelunestohyökkäyksessä viestit (komennot) hyökkääjän, käsittelijöiden ja agenttien välillä voivat olla kryptaamattomia (selkokielisiä), kryptattuja tai binäärimuotoisia. Suorien komentojen sarja generoi normaalista poikkeavaa liikennettä, joka voidaan havaita verkon liikennettä tarkkailemalla ja analysoida sen jälkeen. Käsittelijän ja agentin välisten viestien analysoinnilla voidaan saada tietoa haittaohjelmasta näkemättä itse haittaohjelmaa. Koska käsittelijöiden täytyy pitää agenttien tiedot tallessa ja agentin pitää tieto käsittelijästään tallessa, saattaa hyökkäyksen tutkija saada koko DDoS-verkon selville saadessaan ”kaapatuksi” yhden hyökkäykseen osallistuvan koneen. [8, s. 8]



Kuva 3.2. Ponnahduslautojen käyttö hajautetussa palvelunestohyökkäyksessä [6, s. 14].

3.6 Suojautuminen verkkokapasiteetin kuluttamiselta

Mikäli hyökkääjä tulvittaa uhrin verkon ICMP- tai UDP-paketeilla, ei uhri voi yksin suojautua siltä, koska lailliset paketit hukkuvat jo verkossa. Tulvitushyökkäykset näyttävätkin usein vain tavalliselta, runsaan liikenteen aiheuttamalta ruuhkalta, ja siksi niiden torjuminen on loogisia hyökkäyksiä vaikeampaa [9, s. 71]. Siksi uhri tarvitseekin Internet-palveluntarjoajan (Internet Service Provider, ISP) tukea. Joissakin tapauksissa hyökkäysliikenne voidaan tunnistaa ja ISP voi suodattaa sen pois. [8, s. 13] Vaihtoehtoina on tällöin kaksi pääkeinoa: suodatus ja kaistanrajoitus. Suodatuksella poistetaan kaikki epäilyttävät paketit liikenteen luokittelun perusteella. Kaistanrajoituksella taas vahvistetaan tietty kaista epäilyttäville paketeille. Valinta näiden kahden välillä riippuu liikenteen tunnistamisen perusteella. [6, s. 24] Helposti tunnistettavaa hyökkäysliikennettä ovat esim. suuret UDP-paketit lähetettyinä tuntemattomiin portteihin. Tunnistaminen on tässäkin avainasemassa, sillä muuten ISP voi joutua suodattamaan kaiken asiakkaalle kohdennetun liikenteen, jolloin asiakkaan laillinenkin liikennöinti estyy. [8, s. 13]

Smurfing- ja fraggle-hyökkäyksien vastatoimenpiteenä tulee suunnattu monilähetystoiminto olla poiskytkettynä rajareitittimessä (border router). Lisäksi käyttöjärjestelmä pitää konfiguroida siten, että se estää koneita vastaamasta IP-monilähetysosoitteista lähetettyihin ICMP- tai UDP-paketteihin. Pakettien suodatus tulee asettaa reitittimissä siten, että paketit, joiden lähtöosoite on muualla kuin kyseisessä verkossa hylätään. Tämä auttaa myös estämään tällaisen hyökkäyksen käynnistymistä hyökkäyksen lähtöpisteessä. [7, s. 11; 8, s. 72]

IP-spoofingilla voidaan kuitenkin yrittää ohittaa puolustus UDP-pohjaisissa hyökkäyksissä. Mikäli puolustus päästää verkkoon liikennettä vain tietyistä IP-osoitteista, hyökkääjä voi käyttää sallittuja osoitteita. Puolustus voi myös perustua asiakkaiden tasavertaiseen kohteluun, jolloin hyökkääjä vaihtelee käyttämäänsä lähdeosoitetta. IP-spoofingia vastaan on vaikea puolustautua, sillä sitä ei voida estää päätelaitteiden TCP/IP API:ssa, koska ominaisuutta tarvitaan mm. mobile IP:ssä. Samasta aliverkosta väärennettyjä lähdeosoitteita voidaan kuitenkin estää tutkimalla reitittimissä pakettien MAC-osoitteita, mutta tämä on ylläpidon ja reitittimien kannalta erittäin työlästä. [8, s. 11]

3.7 Suojautuminen resurssien kyllästämiseltä

Useat uudenaikaiset käyttöjärjestelmät sisältävät kiintiörajoja, jotka suojaavat resurssien ylikuormittumista, mutta kaikissa järjestelmissä ei ole tällaista ominaisuutta. Jos käyttöjärjestelmä mahdollistaa levykiintiöitä, niin niitä on syytä käyttää kaikkien käyttäjätilien kohdalla ja erityisesti silloin, kun ne käyttävät verkkopalveluja. Resurssien kyllästämiseltä voidaan suojautua myös rajoittamalla käyttäjien oikeutta käyttää järjestelmän resursseja. Usein hyökkääjillä on kuitenkin laillinen oikeus käyttää järjestelmän resursseja rajoitetussa määrin, ja tätä oikeutta voidaan väärinkäyttää kuluttamalla resursseja yli sallitun määrän, jolloin järjestelmältä tai muilta laillisilta käyttäjiltä riistetään oikeus osuutensa resursseista. Tämä korostaakin käyttöjärjestelmien käyttäjien oikeuksien määrittämisen tärkeyttä suojauduttaessa väärinkäytöltä. On myös tärkeää tarkkailla järjestelmän suorituskykyä ja määriteltävä yleiset tasot normaalikäytölle. Tällöin näitä rajoituksia voidaan käyttää poikkeuksellisen levytilan ja keskusmuistin käytön sekä verkkoliikenteen havaitsemiseen. [7, s. 8, 17-18]

Protokolliin kohdistuvat hyökkäykset (esim. TCP SYN –tulva) ovat vaikeita torjua, koska uusi korjattu versio protokollasta täytyy asentaa sekä palvelimelle, että asiakkaille. Toinen tapa torjua hyökkäyksiä on käyttää protokollaa ”älykkäästi”, esim. palvelin voi ottaa käyttöönsä TCP SYN –keksit. [8, s. 12] Mikäli SYN-hyökkäystä epäillään, voidaan se selvittää antamalla ”netstat”-komento (mikäli käyttöjärjestelmä tukee tätä komentoa). Jos tuloksena ilmenee, että useat yhteydet ovat SYN_RECV-tilassa, niin tämä viittaa järjestelmän olevan hyökkäyksen kohteena. Tällöin voidaan vastatoimena kasvattaa yhteysjonon kokoa, rajoittaa yksittäisen kävijän avaamien yhteyksien määrää ja vähentää yhteydenmuodostuksen timeout-ajastimen arvoa. Järjestelmä saadaan myös kestämään SYN-tulvitusta varaamalla yhdelle puoliavoimelle yhteydelle mahdollisimman vähän muistia, jolloin istunnolle ladataan palvelun käyttöön tarvittavat koodit vasta kun yhteys on avattu kokonaan. [1, s. 8]. Ohjelmistovalmistajien tuotteissa on myös tarjolla IDS-työkaluja (Intrusion Detection System), joiden avulla voidaan havaita ja vastata SYN-hyökkäyksiin (tarkemmin kappaleessa 3.8). IDS-ohjelma voi lähettää hyökkäyksen kohteena olevalle järjestelmälle RST-paketteja, jotka vastaavat alkuperäisiä SYN-pyyntöjä. Tämä voi auttaa järjestelmän yhteysjonon elvyttämisessä. [7, s. 12]

UDP-protokollaa käyttävien hyökkäyksien vastatoimenpiteenä tulee kytkeä pois käytöstä kohdekoneen porteista chargen- ja echo-palvelut, sekä samoin myös kaikki käyttämättömät UDP-palvelut. Mikäli ulkopuolelta tarvitaan pääsyä johonkin UDP-palveluun, voidaan käyttää proxy-palvelinta palvelun suojaamiseksi väärinkäytöltä. Koska tähän hyökkäystapaan tyypillisesti

liittyy myös osoiteväärennös, niin on syytä ryhtyä toimenpiteisiin myös niiden estämiseksi. [7, s. 13].

Roskasähköpostin vastatoimenpiteinä voidaan kehittää organisaation sisäisiä työkaluja, joiden avulla tunnistetaan tilanne ja reagoidaan roskapostiin, ja siten minimoidaan toiminnan vaikutusta. Näiden työkalujen avulla paranee valmius havaita ja hälyttää saapuvista ja lähtevistä viesteistä, jotka lähtevät samalta käyttäjältä tai palvelimelta hyvin lyhyellä aikavälillä. Kun toiminta on havaittu, voidaan käyttää muita organisaation sisäisiä työkaluja näiden viestien hylkäämiseen. Sähköpostipalvelimilla voidaan myös estää sähköpostilaatikoiden täyttyminen asettamalla rajoituksia sekä lähtevien, että saapuvien viestien koolle [1, s. 9]. Palomuuri voidaan myös konfiguroida varmistamaan, että ulkopuolelta tulevat SMTP-yhteydet voidaan ottaa vain pääasialliseen sähköpostipalvelimeen, eikä muihin palvelimiin. Vaikka tämä ei estä hyökkäyksiä kokonaan, niin se minimoi kohdekoneiden määrän, joihin ulkopuolinen voi kohdistaa SMTP-pohjaisen hyökkäyksen. Mikäli tarkoituksena on kontrolloida saapuvia SMTP-yhteyksiä suodattamalla tai muilla keinoin, niin tällä tavoin on tarpeen konfiguroida vain pieni määrä laitteita. Sähköpostin käsittelyjärjestelmät voidaan konfiguroida viemään viestit tiedostojärjestelmiin, joissa on käyttäjäkohtaiset kiintiöt. Tämä voi minimoida hyökkäyksen vaikutusta rajaamalla vahingon vain kohteena olevaan käyttäjätiliin, jolloin hyökkäys ei vaikuta koko järjestelmään. Organisaation käyttäjät on aina syytä neuvoa ilmoittamaan välittömästi roskasähköpostista ja olemaan vastaamatta niihin. [7, s. 16]

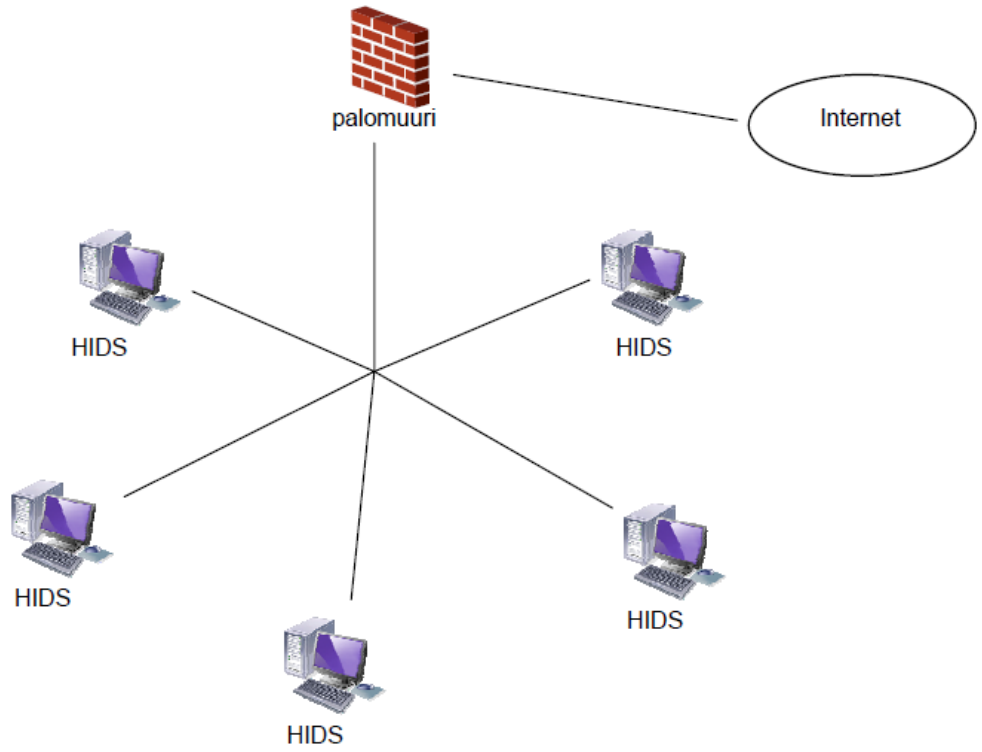
3.8 Suojautuminen tunkeutumisen havaitsemis- ja estojärjestelmillä

Yleensä kaikki tietoverkon läpi kulkeva liikenne menee palomuurin tarkastuksen läpi. Palomuureilla saadaankin rajattua pois suurin osa väärinkäytöksistä ja tunkeutumisyrityksistä, mutta palomuureistakin löytyy aika-ajoin virheitä. Tällaisen virheen paljastuttua on palomuuri mahdollista kiertää tai jopa kaataa se kokonaan palvelunestohyökkäyksellä. Palomuurien jättämiä aukkoja paikkaamaan on kehitetty tunkeutumisen havaitsemisjärjestelmiä. Tunkeutumisen havaitsemisjärjestelmien eli IDS-järjestelmien (Intrusion Detection System) tarkoituksena on valvoa verkkoa ja havaita mahdolliset tunkeutumisyritykset. IDS-järjestelmien toiminta perustuu oletukseen, että haitallinen verkkoliikenne poikkeaa normaalista verkkoliikenteestä. Useat virustorjunta- ja palomuurisovellukset sisältävät valmiiksi IDS:n. IDS-järjestelmät tarjoavat hyvän suojan etenkin tietoverkon sisältä tulevilta hyökkäyksiltä ja uusilta, vielä tuntemattomilta uhilta. Pelkästään IDS-järjestelmä ei kuitenkaan pelasta palvelunestohyökkäykseltä, sillä ne vain varoittavat tunkeutumisesta, eivätkä välttämättä torju sitä. [13; 14]

Tunkeutumisen havaitsemisjärjestelmät toimivat kahdella erilaisella toimintamekanismilla. Toinen perustuu tilastolliseen ja toinen sääntöpohjaiseen havaitsemiseen. Tilastollinen havaitseminen perustuu tietokantaan, johon on tallennettu otos normaalista verkkoliikenteestä. Kun analysoitavaa verkkoliikennettä verrataan tilastollisin menetelmin tietokantaan, voidaan päätellä, onko kyseessä tunkeutuja vai normaali verkkoliikenne. Sääntöpohjainen havaitseminen perustuu puolestaan joukkoon ennalta määriteltyjä sääntöjä, joiden perusteella pyritään tunnistamaan tunkeutujan käyttäytyminen. [13; 14]

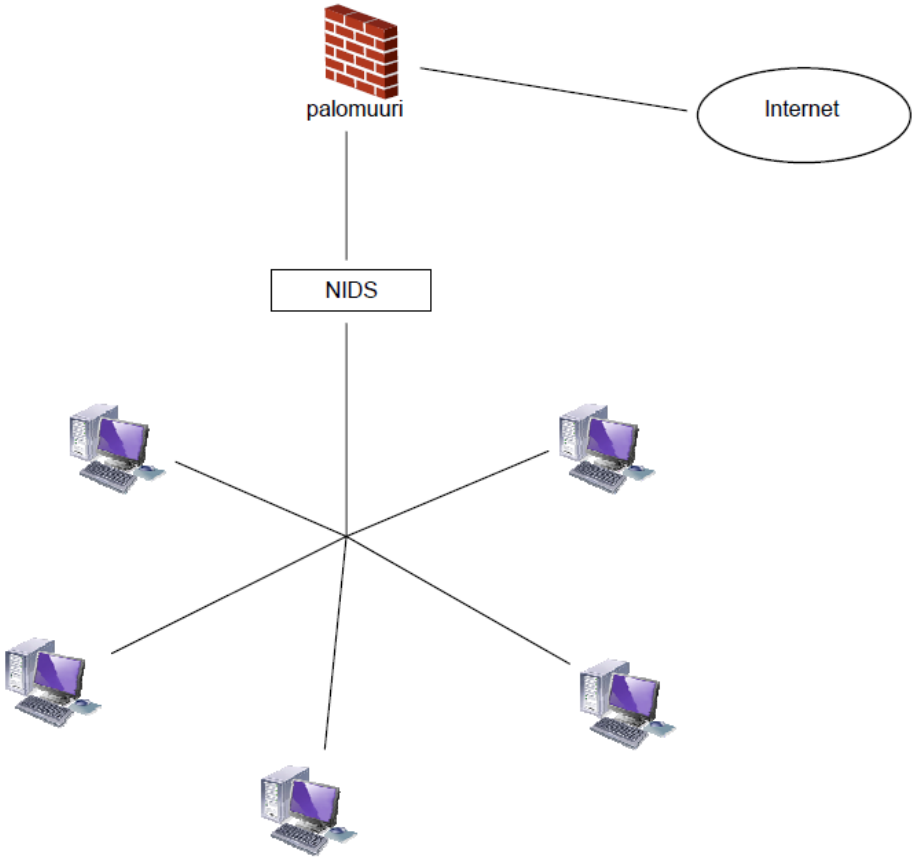
IDS-järjestelmien laajennuksena voidaan pitää tunkeutumisen estojärjestelmiä eli IPS-järjestelmiä (Intrusion Prevention System). IPS-järjestelmä kykenee samoihin tehtäviin kuin IDS-järjestelmäkin, mutta sen tarkoitus on estää mahdolliset tunkeutumiset. On olemassa myös IDP-järjestelmä (Intrusion Detection and Prevention), joka sisältää sekä havaitsemis- että estojärjestelmän. [13; 14]

IDS-järjestelmät voidaan jakaa myös sijaintinsa perusteella verkkoasemakohtaisiin (HIDS) sekä verkkokohtaisiin (NIDS) havaitsemisjärjestelmiin. Verkkoasemakohtaisessa havaitsemisjärjestelmässä (HIDS = Host Intrusion Detection System) IDS-järjestelmä asennetaan koneille, joita halutaan vahtia (kuva 3.9.1). Nimensä mukaisesti HIDS perustuu isäntä- eli laitekohtaisen liikenteen analysointiin. Se on erityisen tehokas verkon sisältä tulevien hyökkäysten havaitsemiseksi. Verkkoasemakohtaisen havaitsemisjärjestelmän heikkoutena on ylläpidon hankaluus, kun hallittavien koneiden lukumäärä kasvaa. IDS-järjestelmä voi myös heikentää kohdekoneen suorituskykyä. Siksi verkkoasemakohtainen havaitsemisjärjestelmä voikin olla kannattavampaa asentaa vain kriittisiin koneisiin. [13; 14]



Kuva 3.9.1 Verkkoasemakohtainen havaitsemisjärjestelmä (Host Intrusion Detection System) [6]

Verkkokohtainen havaitsemisjärjestelmä NIDS (Network Intrusion Detection System) sen sijaan vahtii verkkoliikennettä. Sen toiminta perustuu siihen, että verkossa on haluttu määrä koneita, jotka tarkkailevat verkkoliikennettä. Kone, joka toimii verkkomonitorina, pyrkii nappaamaan kaiken verkossa liikkuvan datan ja tutkimaan sen sisällön etsien mahdollisia tunkeutumisyrityksiä (kuva 3.9.2). Verkkokohtaisen havaitsemisjärjestelmän toteutuksessa yleensä verkkokortti asetetaan ns. promiscuous-tilaan eli se ei suodata mitään pois, ei edes viallista informaatiota. Jokainen kehys lähetetään IDS-prosessin analysoitavaksi. Verkkokohtainen havaitsemisjärjestelmä on ylläpidon kannalta helpompi ottaa käyttöön ja ylläpitää kuin verkkoasemakohtainen havaitsemisjärjestelmä. Tässä järjestelmässä valvottavien koneiden teho ei kulu IDS-prosesseihin, ja verkkomonitoriksi voidaan valita tähän tarkoitukseen riittävän tehokas tietokone. Verkkokohtaisen havaitsemisjärjestelmän heikkoudeksi jää verkkomonitorina toimivan koneen mahdollinen tehottomuus, jolloin valvontakoneen resurssit eivät riitä käsiteltävän datan tehokkaaseen valvontaan. Ratkaisuna verkkoa joudutaan osittamaan pienempiin segmentteihin, joilla jokaisella on oma valvontakone. [13; 14]



Kuva 3.9.2 Verkkokohtainen havaitsemisjärjestelmä NIDS (Network Intrusion Detection System) [6]

3.9 Suojautuminen reitittimellä

Nykyisin paras menetelmä suojautua palvelunestohyökkäyksiltä on asentaa verkkoon suodattava reititin. Reitittimissä on syytä käyttää erityisiä reititinsuodattimia, joiden avulla voidaan vähentää verkkoon saapuvien ja sieltä lähtevien osoitevääränettyjen IP-pakettien määrää, vaikkei niitä voidakaan nykyisellä IP-protokollan teknologialla täysin eliminoida. Suodattava reititin ei päästä verkon sisään paketteja, joiden lähettäjäosoite on samassa verkossa eikä verkosta ulos paketteja, joiden lähettäjäosoite ei ole saman verkon sisällä. Nämä suodattimet eivät kuitenkaan pysäytä kaikkia hyökkäyksiä, sillä ulkopuoliset hyökkääjät voivat väärentää osoitteen missä tahansa ulkopuolella olevassa verkonosassa ja verkon sisältä tapahtuvassa hyökkäyksessä hyökkääjä voi edelleen väärentää minkä tahansa verkon sisäisen osoitteen. [7, s. 17]

3.10 Palvelunestohyökkäysten havaitseminen ja torjunta 802.11-verkoissa

Tyhmää radiohäirintää käyttävän hyökkäyksen havaitsemisessa vaikeutena voi olla sen erottaminen verkon muusta epätavallisesta käyttäytymisestä, kuten ruuhkasta, akun loppumisesta tai jonkin verkkolaitteen rikkoutumisesta. Häirintä voidaan kuitenkin tunnistaa ja erottaa luo-

tettavasti muusta verkon toiminnasta seuraamalla samanaikaisia muutoksia pakettien lähetyssuhteessa (Packet Delivery Rate, PDR) ja siirtotiellä havaitun signaalin voimakkuudessa. Toinen mahdollisuus tyhmän radiohäirinnän havaitsemiseksi on seurata sen aiheuttamia muutoksia siirtotiellä havaittujen signaalien voimakkuuksiin. Tällöin siirtotiellä havaitusta radiosignaalista tehdään useita mittauksia, joiden perusteella lasketaan joko signaalin keskimääräinen voimakkuus tai signaalien kokonaisenergia. Tavoitteena on selvittää näiden arvot normaalioloissa ja saada vertailuarvot, joita sitten verrataan oletetun radiohäirinnän aikana mitattuihin arvoihin. Näitä kahta (PDR ja signaalin voimakkuuksien tasot) yhtä aikaa seuraamalla voidaan erottaa tyhmä radiohäirintä muista verkon tietoliikenteen poikkeustilanteista. Kun PDR pienenee eli entistä vähemmän paketteja pääsee virheettä perille, niin normaalisti tähän on jokin luonnollinen syy, jolloin myös signaali heikkenee. Normaalisti siis PDR:n laskemiseen liittyy aina myös signaalin selkeä lasku. Tyhmän radiohäirinnän aikana PDR alenee huomattavasti, mutta signaali ei kuitenkaan heikkene, vaan pysyy luonnottoman korkeana johtuen hyökkääjän siirtotielle syöttämästä energiasta. [9, s. 81-82] Havaitsemisen jälkeen tulee aloittaa toimenpiteet häirinnän torjumiseksi. Radiohäirinnän torjuminen on melko vaikeaa, mutta sitä voidaan yrittää muutamilla keinoilla. Jossain määrin lähetystehon kasvattaminen tai kanavan vaihtaminen voi auttaa, mutta usein torjuntakeinoksi jäävät fyysiset toimenpiteet, kuten suunnatun antennin käyttäminen, etäisyyden kasvattaminen hyökkääjään tai hyökkääjän lähettimen vaientaminen. [9, s. 107]

Tulvitushyökkäystä on vaikea torjua millään kehysten todentamiseen liittyvällä menetelmällä, sillä todentaminen perustuu usein johonkin yhteiseen salaiseen tietoon aseman ja tukiaseman välillä ja tällainen syntyy vasta onnistuneen todennuksen ja nelivaiheisen kättelyn jälkeen (WPA:ssa ja WPA2:ssa). Tulvituksen torjuntaan on kuitenkin useita tehtäviin perustuvia tapoja. Niissä hyökkääjä joutuu jokaista lähettämäänsä tulvituskehystä kohti suorittamaan ensin jonkin resursseja kuluttavan tehtävän. Voidakseen tehdä tulvitusta tällaisia tehtäviä on ratkaistava useita, mikä rajoittaa tulvituksen suorittamista. Tehtävät perustuvat tiivistefunktioiden käyttöön, jolloin tukiasema voi nopeasti sekä muodostaa että tarkistaa tehtävän. Tulvitus voidaan torjua myös kehysten sekvenssinumeroiden avulla. Niitä on aiemmin käytetty vain purkukehysten havaitsemiseen, mutta ne soveltuvat myös tulvituksen torjuntaan. Purkukehysten havaitsemisessa hyökkäyksen paljastaa sekvenssinumeroiden poikkeavuus säännönmukaisesta sarjasta. Tulvituksessa tilanne on päinvastainen: eri MAC-osoitteista tulevien kehysten sekvenssinumeroiden säännönmukainen kasvaminen paljastaa hyökkääjän, kun taas niiden satunnainen jakaantuminen kertoo vain normaalista ruuhkasta. [9]

3.11 VoIP-palvelujen suojaaminen

Puolustusvoimien kiinteän verkon suojaamisessa kyetään käyttämään hyväksi edellä mainittuja puolustusmekanismeja, mutta puolustusvoimilla on käytössä myös taktisen tason johtamisjärjestelmässä palvelunestohyökkäyksille alttiita osia. Yksi esimerkki tällaisesta on VoIP eli IP-puhe. VoIP tarkoittaa puheen välittämistä IP-protokollan avulla IP-verkossa, ja sen avulla voidaan siirtää ääntä ja videota pakettimuotoisesti IP-verkossa [15, s. 1]. VoIP:ssa analoginen puhe ja videokuva muunnetaan digitaaliseen muotoon ja siirretään paketeissa verkon yli. VoIP:lla voidaan soittaa tavalliseen lanka- tai matkapuhelinverkkoon erillisen yhdyskäytävän kautta. [15, s. 1]

Koska VoIP perustuu tavanomaisiin palvelimiin, ovat ne muiden palvelimien tavoin alttiita palvelunestohyökkäyksille. Yhdysvaltalaisen SANS-instituutin vuonna 2006 tekemän tutkimuksen mukaan VoIP-palvelimet ja -puhelimet ovat verkkolaitteet kategoriassa ensimmäisellä sijalla puhuttaessa potentiaalisista hyökkäyskohteista, ja tästä johtuen ne tulisikin suojata huolellisesti. [15, s. 21] Suojautumisessa palvelunestohyökkäyksiltä sisäverkon suojaaminen luvattomilta käyttäjiltä on tärkeää. Mikäli organisaation sisäverkkoon pääsy on helppoa, johtaa se pääsyyn verkon resursseihin, salakuunteluun tai palvelunestohyökkäykseen VoIP-verkossa. Työaseman tai IP-puhelimen liittäminen suojaamattomaan VoIP-verkkoon voi antaa pääsyn LAN:iin tai puheverkkoon, ja tämä kaikki tulee estää. [15, s. 31]

Välttääkseen tunkeilun, on syytä liittää kaikki käyttämättömät portit käyttämättömään VLAN:iin (Virtual LAN). Tämä toimenpide estää luvattoman pääsyn VLAN:iin niin fyysisesti kuin loogisestikin. Myös IP-puhelimien käyttämättömät portit tulisi ottaa pois käytöstä, mikäli niitä ei tarvita. VoIP-päätelaitteen pääsy VoIP-palveluihin tulisi aina perustua yksilölliseen tarpeeseen ja lupaan ottaa yhteys verkkoon. Kun lupa on tarkastettu, varmistetaan laitteen ohjautuminen oikeaan VLAN:iin. Toisen tason pääsynhallintaan ja VLAN:in ohjaukseen voidaan käyttää seuraavia tapoja: port security –ominaisuus, porttikohtainen autentikointi 802.1x sekä VLAN Management Policy –palvelin (VMPS). [15, s. 31]

Port security-ominaisuus on useimmissa kytkimissä, ja siinä käytetään MAC-suodatusta kytkimen portteihin, jolloin kytkin antaa pääsyn vain sen asetuksiin määriteltyjen laitteiden MAC-osoitteille. Port security-ominaisuudella voidaan siis estää luvattomien laitteiden kytkentä VoIP-verkkoon. Porttikohtainen autentikointi 802.1x-tekniikka mahdollistaa asiakkaan tunnistautumisen, autentikoitumisen ja pääsyn sisään verkkoon kirjautuessa.verkkoon. Sen tarkoituksena on estää luvattoman asiakaslaitteen pääsy verkkoon lähiverkon liityntäpisteen

kautta. VMPS on taas erityinen kytkin, joka käyttää laitteen MAC-osoitetta tunnistaakseen laitteen ja pistääkseen tämän oikeaan VLAN:iin. Vaikka MAC-osoitteiden väärentäminen onkin suhteellisen helppoa, on näillä työkaluilla mahdollisuus parantaa VoIP:n turvallisuutta. [15, s. 31-32]

VoIP:n turvallisuutta voidaan parantaa myös rajoittamalla dataverkon liikennettä VoIP-verkkoon. Ideaalitilanteessa VoIP- ja data-VLAN:ien välistä liikennettä ei olisi ollenkaan, mutta sen on oltava ainakin suodatettua. Mikäli VoIP- ja data-VLAN:ien välistä dataliikennettä on, pakettisuodatus tulee hoitaa sisäisellä palomuurilla tai vähintään 3-tason kytkimien ja reitittimien pääsylistoilla. Näin voidaan rajoittaa portteja ja osoitteita, joille sallitaan pääsy näiden verkkojen välillä. [15, s. 32]

4 JOHTOPÄÄTÖKSET

Palvelunestohyökkäyksen torjumisessa tulisi aina tietää *mitä* puolustetaan. Organisaation sisällä on siksi ymmärrettävä hyvin, miten organisaation tietoverkko toimii ja miten se on organisoitu. Tämä auttaa tunnistamaan tietoverkon mahdolliset heikkoudet, jotka voivat olla alttiina hyökkäykselle. Suojautumisen tulisikin aina perustua huolelliseen uhkien kartoitukseen ja riskianalyysiin. Siksi oikeanlainen suunnittelu on avain onnistumiseen. Hyvin suunnitellut järjestelmät kestävät paremmin hyökkäyksiä eivätkä kaadu hyökkäyksistä aiheutuviin virhetilanteisiin. Olen jakanut keskeiset tulokset ennaltaehkäisyn, havaitsemisen ja suojautumisen kokonaisuuksiin.

Palvelunestohyökkäyksiin ja muihin tunkeutumisyrityksiin on syytä varautua etukäteen. Paras suojautumiskeino on ennaltaehkäisy. Hyväksi havaittu yleinen tapa ennaltaehkäistä hyökkäyksiä ja parantaa tietoturvallisuutta on pitää tietoverkko yksinkertaisena, hyvin organisoituna ja hyvin ylläpidettynä. Palvelunestohyökkäyksien ennaltaehkäisyä tulee tehdä aina yhteistyössä organisaation, sen tietotekniikan toimittajan ja verkko-operaattorin kanssa. Kuitenkin hyökkäyksen tapahtuessa, yrityksen on myös osattava reagoida tarpeellisin keinoin. Siksi tietoturvasuunnittelua tehtäessä on selvitettävä aina mistä, ja millaisella aikataululla asiantuntija-apua on saatavilla. Asiantuntijoiden työtä helpottaakseen on häiriötilanteiden hallinnassa tärkeää, että häiriötilanteen hallitsemiseksi käynnistetyt toimenpiteet kirjataan ja analysoidaan mahdollisimman kattavasti. Myös niin sanottujen ”läheltä piti” -tilanteiden analysointi on liitettävä osaksi tätä seurantaa, erityisesti uhkien ja riskien ennaltaehkäisemiseksi. Järjestelmälokien mahdollisimman tarkka kirjaaminen sekä velvoite luovuttaa lokitietoja viranomaisten määräämille selvittäjille epäiltäessä verkkohyökkäystä nopeuttaa palvelunestohyökkäyksien havaitsemista ja tunnistamista.

Mikäli ennaltaehkäisevistä toimenpiteistä huolimatta palvelunestohyökkäys tapahtuu, on hyökkäyksen havaitseminen ja tunnistaminen avainasemassa. Sen tekee haasteelliseksi verkkoyhteyden kuluttamiseen käytettyjen pakettien erittäin hankala erotettavuus muusta liikenteestä. Hyökkääjät voivat lisäksi käyttää tyypiltään vaihtelevia paketteja, jotka sulautuvat muun liikenteen joukkoon sekä väärentää pakettien osoitetietoja ehkäistäkseen agenttien jäljittämisen. Siksi puolustusmekanismit eivät usein pysty prosessoimaan jokaista tulevaa pakettia liikenteen erittäin suuren määrän takia. Lisäksi hajautettua palvelunestohyökkäystä vastaan on hyvin vaikea suojautua, sillä jopa tunnistetun haitallisen liikenteen suodattaminen on vaikeaa,

koska sitä ei voida suodattaa IP-osoitteen perusteella. Siksi DDoS-hyökkäyksiin ei olekaan mitään yhtä ainoaa jokaiseen tilanteeseen ja ympäristöön toimivaa ratkaisua.

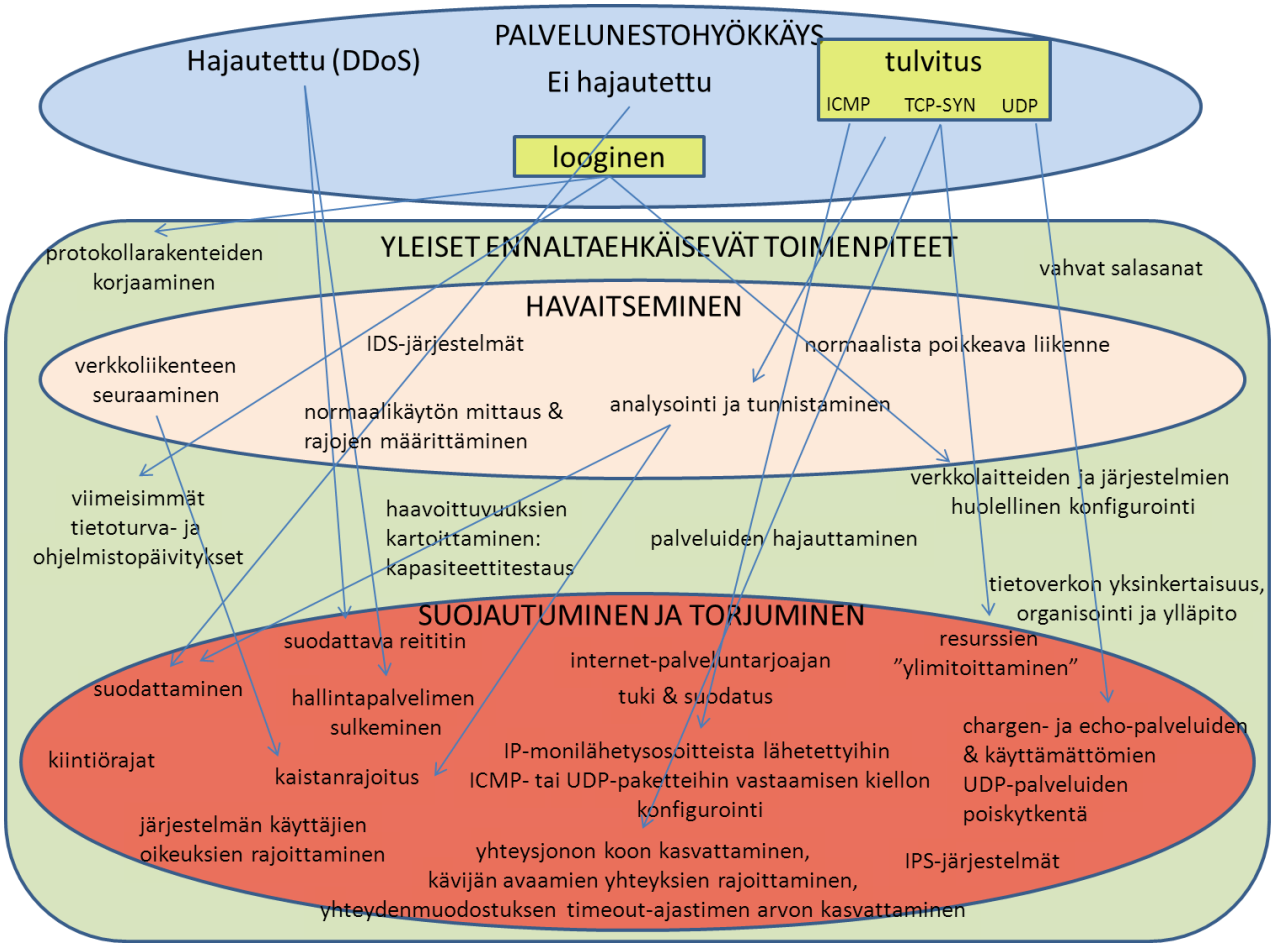
Valitettavasti on hyväksyttävä tosiasia, että hajautettu palvelunestohyökkäys voi saada polvilleen lähes kenet tahansa, mutta siihen, miten pitkään palvelukatko kestää, voidaan vaikuttaa paljon. Paras keino varautua tähän on järjestelmien ja verkkoyhteyksien ylimitoittaminen. Ylimitoittaminen voi kuitenkin tulla kalliiksi, eikä sekään välttämättä pelasta massiiviselta hyökkäykseltä. Siksi organisaation on riskianalyysinsä pohjalta mietittävä, onko kannattavampaa panostaa enemmän palvelunestohyökkäykseen reagoimiseen kuin siltä suojautumiseen, mikäli hyökkäyksiä tapahtuu erittäin harvoin. Reagoinnin tehokkuus riippuu aina hyökkäyksen havaitsemisen tarkkuudesta ja puolustautuminen tulisi tapahtua mahdollisimman nopeasti hyökkäyksen havaitsemisen jälkeen.

Internetin turvallisuus on loppujen lopuksi yhteinen asia ja se on sidoksissa Internetin yleiseen turvallisuuteen. Siksi yhden osapuolen laiminlyönnit turvallisuuden suhteen vaarantavat myös muiden osapuolten turvallisuuden, ja vaikka hyökkäys ei välttämättä vahingoittaisi turvatoimenpiteet laiminlyönyttä tahoa, niin se voi aiheuttaa huomattavia vahinkoja ulkopuolisille. Palvelunestohyökkäykset toteutetaan yleensä hyvin tunnettujen järjestelmien ja ohjelmien heikkouksien kautta, ja siksi on tärkeää, että kaikilla on laitteisto- ja ohjelmistovalmistajien uusimmat turvapäivitykset käytössä. Palvelunestohyökkäyksien torjunnan tulisikin olla kollektiivista, koska tällöin haavoittuvien koneiden löytäminen palvelunestohyökkäyksen toteuttamiseksi vaikeutuisi huomattavasti. Tätä kollektiivista tietoturvallisuutta parantaisivat tietoturvallisuusohjeet, joissa tulisi määrätä, miten tietoturvapäivityksistä ja virustentorjunnasta huolehditaan.

Yksi tärkeä kehitysaskel olisi myös viranomaisten yhteistoiminta hyökkääjän jäljittämisvaiheessa niin kansallisesti kuin kansainvälisestikin. Operaattoreilla ja viranomaisilla tulisi olla oikeus, velvollisuus ja tekninen mahdollisuus sulkea tietojärjestelmä pois tietoverkosta silloin, kun järjestelmä aiheuttaa haittaa verkkoliikenteelle. Julkisessa verkossa suodatusvastuu tulisi olla erityisesti operaattoreilla ja organisaatioiden järjestelmien ylläpitäjillä, jolloin haitallinen tietoliikenne saataisiin karsittua mahdollisimman varhaisessa vaiheessa. Kansainvälisen lainsäädännön yhteistyötä tulisi kehittää siten, että käytännöt olisivat mahdollisimman yhtenäisiä.

Olen laatinut tiivistelmäkaavion yksityiskohtaisempana yhteenvetona yleisimmistä suojautumis- ja torjuntakeinoista palvelunestohyökkäyksiä vastaan (kuva 4.1). Kaavio noudattaa kes-

keisten tulosten osalta jo edellä mainittua jakoa ennaltaehkäisyn, havaitsemisen ja suojautumisen asiakokonaisuuksiin Tiivistelmä on laadittu kappaleen 3 pohjalta.



Kuva 4.1 Yhteenvetokaavio

Kuvan yhteenvedosta nähdään, että yleisiksi ennaltaehkäiseviksi toimenpiteiksi voidaan lukea mm. vahvat salasanat ja viimeisimpien tietoturva- ja ohjelmistopäivityksien asentamisen. Ennaltaehkäisyä saadaan edelleen tehostettua organisoimalla tietoverkko yksinkertaiseksi ja hyvin ylläpidetyksi sekä hajauttamalla palvelut. Ennaltaehkäisyssä olisi myös syytä kartoittaa haavoittuvuudet kapasiteettitestauksella ja korjata heikkoja protokollarakenteita. Kuvasta voidaan myös havaita, että tulvitushyökkäysten havaitsemisessa analysointi ja tunnistaminen ovat avainasemassa. Onnistuneen analysoinnin ja tunnistamisen perusteella suodattamalla haitallinen liikenne tai rajoittamalla kaistanleveyttä voidaan hyökkäys usein pysäyttää. Koska loogiset palvelunestohyökkäykset perustuvat sovellusohjelmissa, käyttöjärjestelmissä ja protokollissa olevien haavoittuvuuksien, ohjelmointi- ja konfigurointivirheiden sekä tietoturva-aukkojen hyödyntämiseen, korostuu niiden torjumisessa tietoturva- ja ohjelmistopäivitysten asentaminen sekä verkkolaitteiden, järjestelmien ja protokollarakenteiden huolellinen konfigurointi.

LÄHTEET

[1] Björkman, J. *Palvelunestohyökkäykset ja niiltä suojautuminen*. Opinnäytetyö. Helsinki, 2011. Haaga-Helia ammattikorkeakoulu, Tietotekniikan koulutusohjelma. 43 s.

[2] Seuri, J. *Palvelunestohyökkäysten torjunta*. Opinnäytetyö. Leppävaara, 2011. Laurea ammattikorkeakoulu, Turvallisuusosaamisen ylempi ammattikorkeakoulututkinto. 62 s.

[3] Järvinen, P. *Arjen tietoturva*, 1. painos. Jyväskylä: Docendo, 2012. 323 s. ISBN 978-951-038948-5.

[4] *Suomen turvallisuus- ja puolustuspolitiikka 2012. Valtioneuvoston selonteko*. Valtioneuvoston kanslian julkaisusarja 5/2012. Helsinki: Edita Prima, 2013. 122 s. ISBN 978-952-287-003-2.

[5] *Suomen kyberturvallisuusstrategia*. Helsinki: Forssa print, 2013. 44 s. ISBN 978-951-25-2434-1.

[6] Juppi, E & Juppi E. *Palvelunestohyökkäykset ja muut yrityksen tietoturvauhat*. Opinnäytetyö. Kajaani, 2008. Kajaanin ammattikorkeakoulu, Tietojenkäsittelyn koulutusohjelma. 43 s.

[7] Keränen, A. *Palvelunestohyökkäykset*. Seminaaritutkielma. Helsinki, 2003. Helsingin yliopisto, Tietojenkäsittelytieteen laitos. 21 s.

[8] Koskinen, J., Komssi, T., Peltotalo J., Peltotalo S. & Viitanen T. P*alvelunestohyökkäyksen havaitseminen ja torjuminen*. Seminaariraportti. Tampere, 2005. Tampereen teknillinen yliopisto, Tietoliikennetekniikan laitos. 43 s.

[9] Hallenberg, S. *Langattoman IEEE 802.11 -lähiverkon tietoturva*. Pro gradu –tutkielma. Helsinki, 2012. Helsingin yliopisto, Tietojenkäsittelytieteen laitos. 117 s.

[10] Lillbacka, J. *Informaatiosodankäynti – tietoverkkojen vaarat*. Opinnäytetyö, Tampere, 2012. Tampereen ammattikorkeakoulu, Tietoliikennetekniikka ja tietoverkot. 69 s.

[11] Fiskari, J ym. Nixu Oy: Palvelunestohyökkäykseltä suojautuminen, diasarja, Espoo, 2013

[12] Tuominen, T. *WLAN tietoturva*. Tutkintotyö. Tampere, 2005. Tampereen ammattikorkeakoulu, Tietotekniikan koulutusohjelma. 42 s.

[13] Häkkinen, N. *Tunkeutumisen esto- ja havainnointijärjestelmien soveltuvuus verkkopalveluiden suojaamiseen*. Kandidaatintutkielma. Jyväskylä, 2012. Jyväskylän yliopisto, Tietojärjestelmätiede. 25 s.

[14] Koskinen, J., Linden, M., Kari, J., Peltotalo, J., Peltotalo, S. & Viitanen T. *Tunkeutumisen havaitseminen*. Seminaariraportti. Tampere, 2004. Tampereen teknillinen yliopisto, Tietoliikennetekniikan laitos. 53 s.

[15] Viitala, J. *VoIP:n tietoturva ja soveltuvuus julkishallintoon*. Opinnäytetyö. Lahti, 2007. Lahden ammattikorkeakoulu, Tietotekniikan koulutusohjelma. 77 s.