Palvelunestohyökkäykset

Ari Keränen

Helsinki 20. huhtikuuta 2003
Tietoturvallisuus nykyaikaisessa liiketoimintaympäristössä – seminaari
Seminaaritutkielma
HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Palvelunestohyökkäykset

Ari Keränen

Tietoturvallisuus nykyaikaisessa liiketoimintaympäristössä – seminaari
Seminaaritutkielma
Tietojenkäsittelytieteen laitos
Helsingin yliopisto
20. huhtikuuta 2003, 21 sivua

Tässä tutkielmassa tarkastellaan palvelunestohyökkäyksiä, joiden tarkoituksena on kuluttaa jokin tietokonejärjestelmän tai tietoverkon rajallinen resurssi loppuun niin, etteivät palvelun käyttöön oikeutetut käyttäjät pääse käyttämään palvelua, tai sitten palvelun käyttö hidastuu ja hankaloituu huomattavasti. Aluksi hahmotellaan erilaisia yleisiä hyökkäystyyppejä, joilla pyritään vaikuttamaan normaalin tietoliikenteen esteettömään ja turvalliseen kulkuun. Seuraavaksi tarkastellaan tietoturvarikkomuksia koskevaa tutkimustietoa.

Sitten tarkastellaan palvelunestoon pyrkivien hyökkäysten toteuttamistapoja. Palvelunesto-hyökkäykset jakautuvat useaan perustyyppiin, jotka ovat kaistanleveyden loppuunkuluttaminen, resurssien loppuunkuluttaminen, ohjelmointivirheiden hyödyntäminen, reitittimiin ja nimi-palvelimiin kohdistuvat hyökkäykset ja tietoverkkojen komponenttien fyysinen tuhoaminen tai muuttaminen.

Viimeisessä kappaleessa tarkastellaan tapoja, joilla palvelunestohyökkäyksiltä voidaan suojautua. Turvallisuus Internetissä on yhteinen asia ja se on sidoksissa Internetin yleiseen turvallisuuteen. Oleellisinta on se, että yhden osapuolen laiminlyönnit turvallisuuden suhteen vaarantavat myös muiden osapuolten turvallisuuden, vaikka hyökkäys ei vahingoittaisi turvatoimenpiteet laiminlyönyttä tahoa, niin se voi aiheuttaa huomattavia vahinkoja ulkopuolisille. CERT kehoittaa lisäksi noudattamaan eräitä yksityiskohtaisia toimenpiteitä hyökkäyksiltä suojautumiseksi. Lisäksi hyökkäyksiltä suojautumiseksi voidaan käyttää eräitä protokollien yleisiä suunnitteluperiaatteita.

Aiheluokat (Computing Reviews 1998): C 2.0, K 6.5

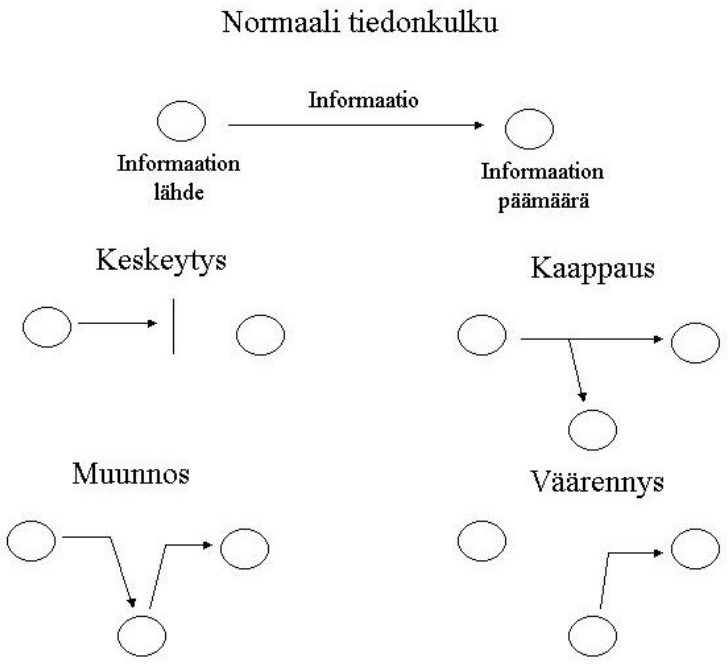
Avainsanat: Palvelunestohyökkäykset, tietoturva

SISÄLLYSLUETTELO

1. Johdanto

Tietoverkkojen käyttö yritysten, organisaatioiden ja yksityishenkilöiden keskeisen kommunikoinnin välineenä on kasvanut 1990-luvulta lähtien räjähdysmäisesti. Samoin on käynyt myös tietoverkkoihin liittyvien rikosten ja rikkomusten osalta. Tietoverkkoihin liittyvät väärinkäytösten uhat eivät ole vähentyneet. Vaikka järjestelmät ja ohjelmistot kehittyvät, ovat myös hyökkäysmenetelmät kehittyneet koko ajan samoin, kuin niiden vaikutusten laajuus.

Tietoturvaan kohdistuvia hyökkäyksiä voidaan tarkastella katsomalla tietokonejärjestelmää informaation tuottajana. Normaali tietovirta kulkee häiriöttä lähteestä päämäärään. Tähän tietovirtaan kohdistuvia hyökkäystapoja voidaan yleisesti hahmotella kuvan 1. mukaisesti.



Kuva 1. Normaaliin tiedonkulkuun kohdistuvia hyökkäystapoja [Sta99].

Keskeytyshyökkäys kohdistuu järjestelmän käytettävyyteen. Tällöin järjestelmän käyttö estetään tukkimalla jokin sen resurssi. Kaappauksessa kolmas taho onnistuu sieppaamaan viestin sen kulkiessa normaalisti verkossa päämääräänsä, jolloin viestin luottamuksellisuus vaarantuu. Muunnoshyökkäyksessä kolmas taho kaappaa viestin kokonaan sen kulkiessa verkossa ja muuntaa sen sisältöä, ennen kuin lähettää sen uudelleen lopulliselle vastaanottajalle, jolloin

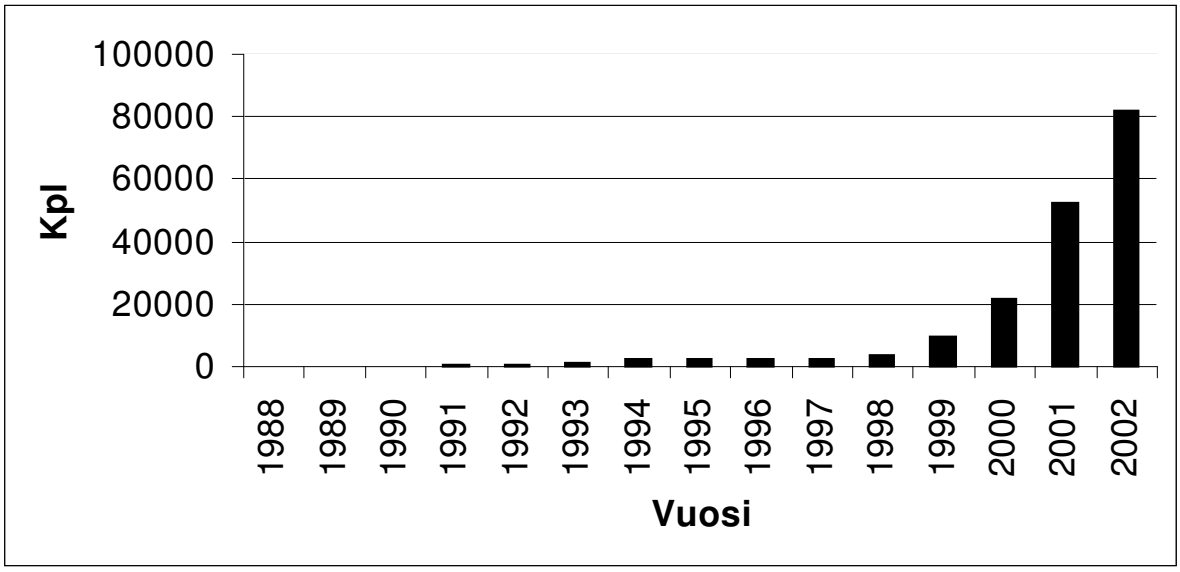
viesti eheys vaarantuu. Väärennöksessä jokin ulkopuolinen taho esiintyy viestin lähettäjänä muiden nimissä. Tämä on mahdollista, jos viestien todennus on toteutettu puutteellisesti.

Palvelunestohyökkäykset ovat keskeytyshyökkäyksiä, jotka kohdistuvat jonkin järjestelmän käytettävyyteen ja niiden tarkoituksena on estää jonkin palvelun oikeutettuja käyttäjiä käyttämästä kyseistä palvelua. Hyökkäystapoja on useita {CER01]. Hyökkääjät voivat tulvittaa verkon suurilla datamäärillä ja estää näin verkkoliikenteen. Kahden isäntäkoneen välinen yhteys voidaan yrittää katkaista. Hyökkääjät voivat yrittää estää jonkin tietyn yksittäisen henkilön pääsyn palveluun. He voivat myös yrittää häiritä jonkin tietyn järjestelmän palvelujen käyttöä. Palvelunestohyökkäykset voivat myös olla osana jotakin toista laajempaa hyökkäystä. Jonkin palvelun laiton käyttö voi myös johtaa palvelun käytön estoon. Järjestelmään tunkeutunut ulkopuolinen voi esimerkiksi käyttää loppuun levytilan kapasiteetin ja estää näin sen laillisen käytön.

Palvelunestohyökkäysten vaikutus ja laajuus vaihtelee. Ne voivat kohdistua yksittäiseen palvelimeen tai sitten useampaan palvelimeen samanaikaisesti. Ne voivat häiritä ja hidastaa palvelun käyttöä, tai sitten ne voivat kaataa koko järjestelmän ja estää täysin sen käytön. Niitä voidaan käynnistää pienin resurssein laajoja ja monimutkaisia järjestelmiä vastaan. Ne voivat tehokkaasti lamaannuttaa tietoliikenneyhteyksistä riippuvaisten yritysten tai organisaatioiden toimintaa.

2. Tutkimustietoa tietoturvatapauksista

CERT/CC:n tilastoraportti vuosilta 1998-2002 [CER03] kuvaa raportoitujen tietoturvarikkomusten vuosittaista määrää (Kuva 2.1). Tietoturvarikkomus on mitä tahansa tietoverkkoon liittyvää toimintaa, josta aiheutuu tietoturvan vaarantuminen. Raportoitujen rikkomusten määrä on ollut suhteellisen tasaista 1990-luvun loppupuolelle asti, jonka jälkeen rikkomusten määrä on lähtenyt räjähdysmäiseen kasvuun. Vuoden 2002 aikana raportoitujen rikkomusten määrä on noussut jo yhteensä 82.094 tapaukseen. Kukin tapaus voi koskea yhtä tai useita, jopa tuhansia, palvelimia. Jotkut tapaukset voivat olla luonteeltaan toimintaa, joka on jatkunut pitkiä ajanjaksoja. Todellisia tapauksia on huomattavasti raportoituja tapauksia enemmän, sillä monet organisaatiot pelkäävät tapausten raportoinnin saattavan aiheuttaa negatiivista mainetta ja useinkin rikkomusta ole edes onnistuttu havaitsemaan.



Vuosi	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002
Kpl	6	132	252	406	773	1334	2340	2412	2573	2134	3734	9859	21756	52658	82094

Kuva 2.1 CERT/CC:lle raportoitujen tietoturvarikkomusten määrät [CER03].

CSI:n ja FBI:n vuonna 2002 tekemässä Computer Crime and Security Survey:ssä [CSI02] saatiin vastaukset 503 organisaatiolta, joiden joukossa oli Yhdysvaltalaisia yrityksiä,

hallintovirastoja, rahoituslaitoksia, lääketieteellisiä instituutioita ja yliopistoja. Nämä organisaatiot olivat kooltaan pääosin suuria. Tutkimus vahvisti, että tietokonerikosten ja muiden tietoturvarikkomusten määrä ei ole vähentynyt ja niiden taloudelliset vaikutukset ovat jatkuvasti kasvussa.

Tutkimuksessa 90% vastaajista oli havainnut tietoturvarikkomuksia edellisen 12 kuukauden aikana. Näistä oli aiheutunut 80%:lle taloudellisia menetyksiä. Taloudellisten menetysten suuruutta halusi ja/tai kykeni määrittelemään 44%:ia. Arvioitujen vahinkojen yhteissumma kohosi 455.848.000 dollariin. Vastaajista 74% ilmoitti Internet-yhteytensä olevan pääsääntöinen hyökkäyskohta, kun taas 33 % ilmoitti sisäisen järjestelmänsä olevan pääsääntöinen hyökkäyskohta. Tutkimuksessa havaittu yleisin tietoturvatapaus oli virus, jonka 85% vastanneista oli havainnut järjestelmässään. Järjestelmään tunkeutuminen ulkopuolelta (44%) ja palvelunestohyökkäys (40%) olivat myös hyvin yleisiä (Taulukko 2.2.).

Vastanneista havainnut	**%**
Virus	85
Tunkeutuminen järjestelmään ulkopuolelta	44
Palvelunestohyökkäys	40

Taulukko 2.2. Järjestelmässä havaitut tietoturvatapaukset [CSI02].

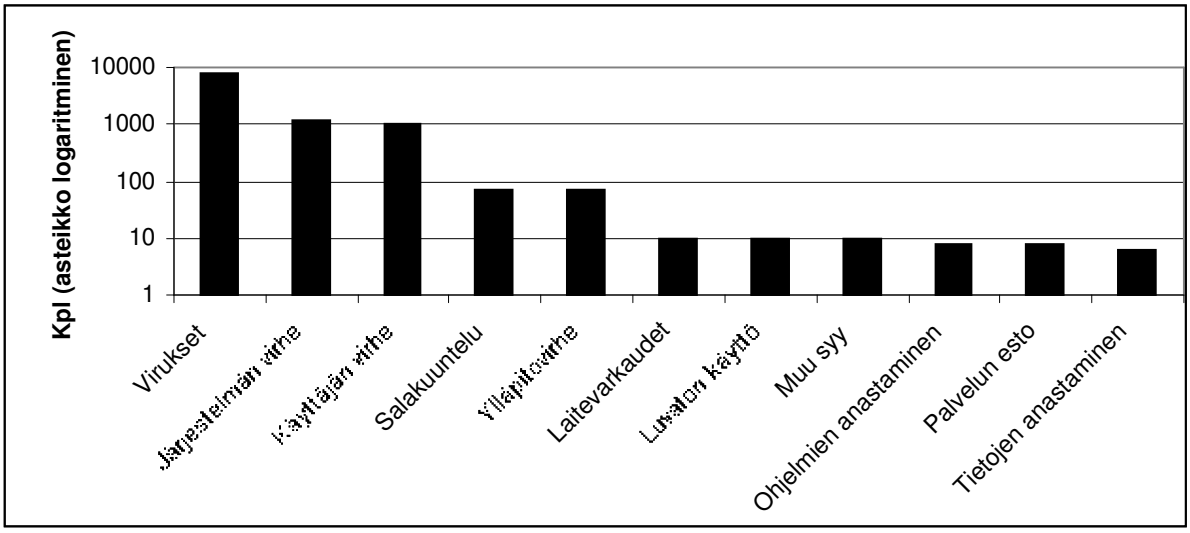
Tutkimuksessa tarkasteltiin myös sähköistä kaupankäyntiä. Lähes kaikilla vastanneista oli Internet-sivusto ja noin puolet harjoitti sivuillaan sähköistä kaupankäyntiä. Yleisin tietoturvatapaus oli erilainen ilkivalta, jota 70 %:ia vastanneista oli havainnut. Palvelunestohyökkäykset olivat seuraavaksi yleisin tapauslaji 55 %:lla. (Taulukko 2.3.).

Vastanneista havainnut	**%**
Ilkivalta	70
Palvelunestohyökkäys	55
Tietovarkaus	12
Tal. petos tai väärennös	6

Taulukko 2.3. Havaitut tietoturvatapaukset sähköisessä kaupankäynnissä [CSI02].

Suomessa tehtiin syksyllä 2000 tutkimus tietoturvatapauksista yhteistyössä Tampereen yliopiston ja Tietoturva ry:n kanssa [Paa00]. Kysely tehtiin n. 1300 yritykselle eri puolella Suomea. Hyväksyttäviä vastauksia saapui 178 kappaletta, jolloin vastausprosentti jäi niinkin

alhaiseksi kuin 13,7 %. Kuvassa 2.4 ovat tutkimuksessa ilmenneiden todennettujen tietoturva-tapauksien määrät (huom. asteikko on logaritminen). Ylivoimainen enemmistö tapauksista oli virusten aiheuttamia. Varmasti havaittujen palvelunestohyökkäysten määrä tutkimuksessa, 9 kappaletta, oli suhteessa hyvin pieni.

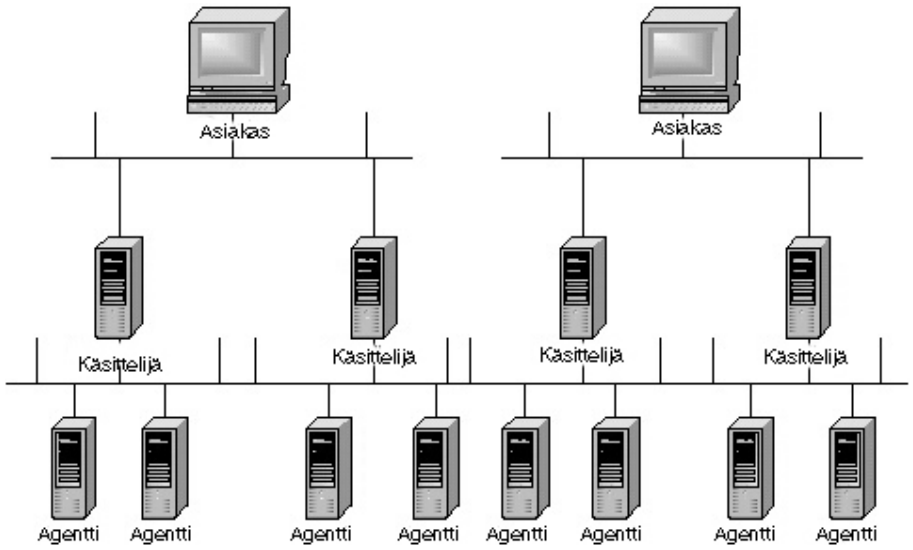


Kuva 2.4. Todennettujen tietoturvatapausten määrä Suomessa [Paa00].

Näiden tutkimusten pohjalta voidaan havaita, että tietoverkkoihin ja liittyvät uhat eivät ole vähentyneet ja erilaisten tietoturvarikkomusten määrät ovat räjähdysmäisessä kasvussa. Vaikka palvelunestohyökkäykset ovat Suomessa suhteellisen harvinaisia, niin CSI:n Yhdysvalloissa tekemässä tutkimuksessa ilmene, että peräti 40%:ia vastaajista oli havainnut palvelunesto-hyökkäyksiä ja määrä kasvoi jopa 55%:iin niiden organisaatioiden osalta, jotka harjoittivat tietoverkossa sähköistä kaupankäyntiä.

3. Palvelunestohyökkäystyypit

Palvelunestohyökkäys voidaan toteuttaa yhdeltä koneelta, tai sitten se voidaan käynnistää hajautetusti useilta koneilta samanaikaisesti. Hajautettu hyökkäystapa on esitetty kuvassa 3.1.



Kuva 3.1 Hajautettu palvelunestohyökkäys [CIS00].

Jokaisen asiakaskoneen (Client) taustalla on henkilö, joka järjestelee hyökkäyksen [CIS00]. Käsittelijä (Handler) on isäntäkone, johon on onnistuttu tunkeutumaan ja johon on asennettu erityinen ohjelma. Kukin käsittelijä kykenee kontrolloimaan useita agentteja. Kukin agentti on myös isäntäkone, johon on tunkeuduttu ja johon myös on asennettu erityinen ohjelma. Kukin agentti tuottaa IP-pakettivirran, joka on kohdistettu valittuun uhriin, kun hyökkäys käynnistetään. Hyökkääjien tiedetään käyttävän neljää ohjelmaa, jotka kulkevat nimellä Trinoo, TFN, TFN2K ja Stacheldraht, hajautettujen palvelunestohyökkäysten toteuttamiseksi. Nämä ohjelmat käyttävät TCP-, UDP- ja ICMP-paketteja hyökkäyksiin.

Hajautettujen hyökkäysten helpottamiseksi hyökkääjät tarvitsevat käyttöönsä useista sadoista useisiin tuhansiin isäntäkoneita, joihin on onnistuttu tunkeutumaan. Nämä koneet ovat tavallisesti Linux- ja Sun-koneita, vaikkakin ohjelmat voidaan muokata myös muille alustoille sopiviksi. Isäntäkoneeseen tunkeutuminen ja ohjelman asentaminen on automatisoitu. Tämä prosessi voidaan jakaa seuraaviin vaiheisiin. Aluksi hyökkääjä aloittaa kartoitusvaiheen (scan), jossa suuri joukko isäntäkoneita, joita voi olla 100.000 tai enemmänkin, tutkitaan tunnettujen heikkouksien suhteen. Suojaamattomaan isäntäkoneeseen tunkeudutaan ja siihen asennetaan

ohjelma. Murrettua konetta käytetään uusien kartoitusten tekoon ja uusiin koneisiin tunkeutumiseen. Koska prosessi on automatisoitu, voidaan ohjelma asentaa murrettuun koneeseen alle 5 sekunnissa, jolloin tuhansia koneita voidaan manipuloida alle tunnissa.

Palvelunestohyökkäykset jakautuvat useaan perustyyppiin, joita voidaan yleisesti luokitella seuraavasti: kaistanleveyden loppuunkuluttaminen, resurssien loppuunkuluttaminen, ohjelmointivirheiden hyödyntäminen, reitittimiin ja nimipalvelimiin kohdistuvat hyökkäykset ja tietoverkkojen komponenttien fyysinen tuhoaminen tai muuttaminen. [McC01][CER01].

3.1. Verkon kaistanleveyden kuluttaminen

Hyökkääjien pyrkimyksenä on kuluttaa kaikki käytettävissä oleva verkon kaistanleveys loppuun [McC01]. Kohteena on tavallisesti jokin tietty verkonosa. Tämä hyökkäys voidaan toteuttaa paikallisessa verkossa, mutta yleensä hyökkäys toteutetaan jostakin etäällä olevasta verkonosasta. Pelkästään käytettävissä olevaan suurempaan kaistanleveyteen perustuvia hyökkäyksiä voidaan toteuttaa kahdella tavalla.

3.1.1. Tulvitus suuremman kaistanleveyden avulla

Hyökkäys voi perustua siihen, että hyökkääjillä on käytössään enemmän kaistanleveyttä, kuin uhrilla, jolloin he voivat tulvittaa uhrin verkkoyhteyden. Esimerkiksi hyökkääjällä voi olla käytettävissä T1 (1.544 Mbps) tai nopeampi yhteys, jolloin hän voi helposti tulvittaa uhrin 56 Kbps tai 128 Kbps nopeuksisen verkkolinkin. Tämänkaltainen hyökkäystapa ei rajoitu vain hitaisiin verkkoyhteyksiin. On todettu tapauksia [McC01], joissa hyökkääjät on saavuttaneet pääsyn verkkoihin, joiden käytettävissä oleva kaistanleveys on yli 100 Mbps. Tällöin hyökkääjät ovat onnistuneet käynnistämään palvelunestohyökkäyksiä palvelimiin, joiden yhteyden kaistanleveys on T1 ja onnistuneet tulvittamaan täysin uhrin verkkoyhteyden.

3.1.2 Tulvitus useiden palvelimien avulla

Hyökkääjät voivat myös vahvistaa (amplify) palvelunestohyökkäyksensä useiden palvelimien avulla ja siten tulvittaa uhrin verkkoyhteyden [McC01]. Esimerkiksi hyökkääjä, jolla on käytettävissä vain 56 Kbps yhteys voi täysin tulvittaa T3 (45 Mbps) yhteyden omistavan uhrin verkon käyttämällä useita muita palvelimia hyökkäyksen

vahvistamiseen. Onnistuakseen hyökkääjän on kyettävä saamaan vahvistava palvelin lähettämään paketteja uhrin verkkoon. Tämä saattaa olla usein aika helppoa.

3.2. Resurssien loppuun kuluttaminen

Rajallisten resurssien loppuun kuluttaminen kohdistuu tietokoneiden ja tietoverkon käytön ja toiminnan kannalta kriittisiin osiin, joita ilman ne eivät voi toimia[CER01]. Tällaisia tekijöitä ovat mm. verkkoyhteydet, isäntäkoneen muisti, levytila ja prosessoriaika, ohjelman tietorakenteet ja eräät ympäristötekijöihin liittyvät resurssit, kuten sähkövirta ja viileä ilma.

Monissa järjestelmissä on käytettävissä rajallinen määrä tietorakenteita prosessi-informaation säilyttämiseen [CER01]. Nämä tietorakenteet voivat sisältää prosessin tunnisteita ja prosessi-taulu merkintöjä. Hyökkääjä voi onnistua kuluttamaan nämä rajalliset resurssit loppuun kirjoittamalla yksinkertaisen ohjelman tai skriptin, jonka ainoa tehtävä on vain tuottaa jatkuvasti kopioita itsestään. Lisäksi esimerkiksi UNIX:issa jokainen saapuva TCP-yhteys poikii (fork) uuden prosessin [Mar01]. Ottamalla useita yhteyksiä hyökkääjä voi täyttää järjestelmän prosessitaulun. Kun taulu on täynnä, ei uusia prosesseja voida enää käynnistää, joten järjestelmällä ei voida tehdä enää mitään.

Mitä tahansa palvelua, joka sallii tiedon kirjoittamisen levylle voidaan käyttää myös palvelunestohyökkäykseen, jos kirjoitetun datan määrälle ei ole asetettu rajoitteita. Useat uudenaikaiset käyttöjärjestelmät sisältävät kiintiörajoja, jotka suojaavat tällaiselta hyökkäystavalta, mutta kaikissa ei ole tällaista ominaisuutta. Vaikka kiintiörajoja olisi käytettävissä, niin siltikin suuri määrä prosesseja ja vaihdot näiden välillä saattavat kuluttaa huomattavasti CPU-aikaa.

Usein hyökkääjillä on laillinen oikeus käyttää järjestelmä resursseja rajoitetussa määrin [McC01]. Kuitenkin hyökkääjä voi väärinkäyttää tätä oikeutta kuluttamalla resursseja yli sallitun määrän, jolloin järjestelmältä tai muilta laillisilta käyttäjiltä riistetään oikeus osuutensa resursseista. Resurssien loppuunkuluttamiseen pyrkivät palvelunestohyökkäykset yleensä johtavat järjestelmän kaatumiseen, levytilan täyttymiseen tai prosessien hyytymiseen.

3.3. Ohjelmointivirheiden hyödyntäminen

Palvelunestohyökkäyksiä voidaan toteuttaa myös tunnettujen ohjelmointivirheiden avulla [McC01]. Näiden virheiden johdosta sovellus, käyttöjärjestelmä tai logiikkapiiri ei kykene selviytymään aiheutuneesta poikkeuksellisesta tilanteesta. Usein hyökkääjä lähettää omituisia RFC-normeista poikkeavia paketteja kohdejärjestelmään selvittääkseen, onnistuuko sen verkkopino (network stack) selvittämään tämän poikkeuksen vai johtaako se järjestelmän kaatumiseen.

Jotkut sovellukset on ohjelmoitu luottamaan käyttäjän syötteisiin. Tällöin hyökkääjä voi lähettää sovellukselle syötteen, joka ei vastaa odotettua. Esimerkiksi, jos sovellus käyttää kiinteän mittaista puskuria, vaikkapa 128 tavua, voi hyökkääjä saada puskurin vuotamaan yli lähettämällä ylisuuren määrän dataa, jolloin sovellus kaatuu.

Ohjelmointivirheisiin liittyvät tapaukset ovat myös yleisiä logiikkapiireissä. Esimerkiksi Pentium f00f-palvelunestohyökkäyksen mahdollisti se, että käyttäjämoodissa oleva prosessi saattoi kaataa käyttöjärjestelmän suorittamalla ei-validin komennon 0xf00fc7c8 [McC01].

3.4. Reitittimiin ja nimipalvelimiin kohdistuvat hyökkäykset

Reitittimeen kohdistuvat palvelunestohyökkäykset perustuvat siihen, että hyökkääjät onnistuvat manipuloimaan reititystaulujen kirjauksia (entry) estääkseen oikeutettujen järjestelmien tai verkonosien pääsyn palveluun [McC01]. Useimmat reititysprotokollat, kuten RIP (Routing Information Protocol) v1 ja BGP (Border Gateway Protocol) v4, ovat suojaamattomia tai sitten niiden autentikointi on heikolla tasolla. Usein tätä autentikointimahdollsuutta ei edes sovelleta implementointivaiheessa. Nämä heikkoudet antavat hyökkääjille mahdollisuuden muuttaa reitittimien kirjauksia, joiden avulla palvelun käyttö voidaan estää. Kirjausten muutoksiin liittyy usein myös osoiteväärennös. Tällaisen hyökkäyksen uhrin liikenne reititetään joko hyökkääjän verkon kautta tai sitten liikenne ohjataan mustaan aukkoon, eli verkon osaan, jota ei ole olemassa.

Useimmat nimipalvelimiin kohdistuvat palvelunestohyökkäykset edellyttävät, että palvelin saadaan tallentamaan väärää osoitetietoa. Kun nimipalvelin sitten suorittaa osoitteen selvitystä,

niin hyökkääjät voivat ohjata sen haluamalleen palvelimelle, tai mustaan aukkoon. On todettu useita nimipalvelimiin liittyviä palvelunestohyökkäyksiä, joissa suuria palvelimia on saatu tavoittamattomiksi pitkiksi ajoiksi [McC01].

3.5. Verkon komponenttien fyysinen tuhoaminen tai muuttaminen

Laitteistojen fyysinen turvallisuus on merkittävä, mutta usein vähemmälle huomiolle jäänyt tekijä. Tietokoneet, reitittimet, verkon kaapelointikaapit, verkon runko-osat, virta-asemat ja muut verkon kriittiset osat ovat haavoittuvia ulkopuolisten fyysisille hyökkäyksille. Onnistunut hyökkäys voi lamaannuttaa laitteet ja verkon, jolloin palveluiden käyttö voidaan estää [CER01].

4. Geneeriset palvelunestohyökkäykset

Eräät palveluestohyökkäykset kykenevät vaikuttamaan useisiin erityyppisiin järjestelmiin, jonka johdosta niitä voidaan kutsua geneerisiksi [McC01]. Tavallisesti nämä hyökkäykset kuuluvat kaistaleveyden ja resurssien loppuunkulutuksen kategorioihin. Yhteinen tekijä näille hyökkäyksille on protokollien manipulointi. Erilaisia hyökkäystapoja on monia, jonka johdosta tässä kappaleessa käsitellään vain kaikkein keskeisimpiä.

4.1. Smurf

Smurf-hyökkäys hyödyntää suunnattuja monilähetyksiä ja se vaatii vähintään kolme tahoa: hyökkääjän, vahvistavan verkon ja uhrin [McC01]. Hyökkääjä lähettää väärennettyjä ICMP ECHO-paketteja vahvistavan verkon monilähetysosoitteeseen. Pakettien lähdeosoite on väärennetty siten, että se on uhrin omassa verkossa, jolloin vaikuttaa, että alkuperäinen pyyntö on tullut täältä. Koska ECHO-paketti lähetettiin monilähetysosoitteeseen, niin kaikki vahvistavan verkon järjestelmät vastaavat uhrille. Esimerkiksi, jos vahvistavassa verkossa on 100 järjestelmää, niin yhden paketin lähettäminen monilähetysosoitteeseen tuottaa 100 pakettia. Tätä voidaan kutsua vahvistumisasteeksi.

Fraggle on Smurf-hyökkäyksen variantti, jossa ICMP-pakettien sijaan käytetään UDP-paketteja. Hyökkääjät voivat lähettää osoiteväärennettyjä paketteja vahvistavan verkon monilähetysosoitteeseen. Kohteena on tyypillisesti echo-portti. Jokainen vahvistavan verkon järjestelmä, jonka echo-palvelu on päällä, vastaa uhrin koneelle tuottaen suuren määrän liikennettä. Vaikka echo-palvelu olisi kytketty pois päältä joltakin vahvistavan verkon järjestelmältä, niin se generoi kuitenkin ICMP määränpää tavoittamaton viestin ja kuluttaa silti kaistanleveyttä.

Vastatoimenpiteenä näille hyökkäyksille tulee suunnattu monilähetystoiminto olla poiskytkettynä rajareitittimessä (border router) [CER00c]. Lisäksi käyttöjärjestelmä tulee konfiguroida siten, että se estää koneita vastaamasta ICMP- tai UDP-paketteihin, jotka on lähetetty IP-monilähetysosoitteisiin. Pakettien suodatus reitittimissä siten, että hylätään paketit, joiden lähtöosoite on muualla kuin kyseisessä verkossa auttaa myös estämään tällaista hyökkäystapaa hyökkäyksen lähtöpisteessä.

4.2. SYN-tulvitus

Useimmiten palvelunestohyökkäykset kohdistuvat verkkoyhteyksien muodostukseen [CER01]. Hyökkääjän tavoitteena on estää isäntäkoneita tai verkonosia kommunikoimasta keskenään. Tyypillinen tähän tavoitteeseen pyrkivä hyökkäystapa on SYN-tulvitushyökkäys. Tässä hyökkäystavassa hyökkääjä aloittaa prosessin ottamalla yhteyden uhrin isäntäkoneeseen lähettämällä tälle yhteyden aloittamisesta kertovan datagrammin, jonka SYN-bitti on asetettu päälle, jolloin isäntäkone varaa uudelle yhteydelle tarvittavat tietorakenteet ja jää odottamaan aloittajan suorittavan yhteyden avaamiseen liittyvät toimet loppuun, joita tämä ei tule tekemään. Hyökkäystapa perustuu siihen, että uhrin koneen yhteysjonon pituus on rajallinen, eikä siihen mahdu muutamaa kymmentä puoliavointa yhteyttä enempää. Lisäksi uhrin sovellus yleensä jää odottamaan yli minuutiksi, että yhteyden aloittamiseen liittyvä koneiden välinen kolmin-kertainen kädenpuristus saatettaisiin loppuun. Näin hyökkääjä pystyy, lähettämällä useita yhteyden aloituspyyntöviestejä väärennetyillä IP-osoitteilla tai muiden koneiden nimissä, joihin on onnistuttu murtautumaan, ja tukkimaan uhrin järjestelmän estäen näin sen käytön.
Mikä tahansa järjestelmä, joka on liitetty Internet-verkkoon ja joka tarjoaa verkkopalveluja, kuten verkkopalvelin, FTP-palvelin tai postipalvelin, ovat tämän hyökkäystyypin potentiaalisia uhreja [CER00b]. Tällainen hyökkäys voidaan kohdistaa myös reitittimiin ja muihin verkkopalvelin-järjestelmiin, jos nämä laitteet mahdollistavat muita TCP-palveluja (esim.echo).

Vastatoimina hyökkäyksen kohden voi koettaa selvittää, onko järjestelmä hyökkäyksen kohteena antamalla netstat-komennon, jos käyttöjärjestelmä tukee tätä komentoa [McC01]. Jos tuloksena ilmenee, että useat yhteydet ovat SYN_RECV-tilassa, niin tämä voi viitata siihen, että järjestelmä on hyökkäyksen kohteena. Tällöin voidaan kasvattaa yhteysjonon kokoa ja vähentää yhteydenmuodostuksen timeout-ajastimen arvoa. Käytettävissä on myös ohjelmistovalmistajien tuotteita, joiden avulla voidaan havaita ja kiertää mahdolliset SYN-hyökkäykset. Käytettävissä on myös IDS (Intrusion Detection System) - työkaluja, joiden avulla voidaan havaita ja vastata SYN-hyökkäyksiin. IDS-ohjelma voi lähettää hyökkäyksen kohteena olevalle järjestelmälle RST-paketteja, jotka vastaavat alkuperäisiä SYN-pyyntöjä. Tämä voi auttaa järjestelmän yhteysjonon elvyttämisessä.

4.3. Land

Land-hyökkäyksessä valmistetaan SYN-paketti, jonka lähde- ja kohdeosoite on sama [Mar01]. Lisäksi tämä osoite sijaitsee hyökkäyksen kohteena olevalla koneella. Joissakin vanhemmissa järjestelmissä tämä aiheuttaa järjestelmän lukkiutumisen, jolloin järjestelmä täytyy käynnistää uudelleen. Vain yksi paketti tarvitaan tämän hyökkäyksen suorittamiseksi.

4.4. UDP-myrsky

Tällä hyökkäystavalla saadaan kaksi saman järjestelmän konetta hyökkäämään toistensa kimppuun [Mar01]. Perusajatuksena on se, että on olemassa joukko portteja, jotka saadessaan paketin reagoivat siihen lähettämällä vastauspaketin. Tällaisia portteja ovat echo (portti 7) ja chargen (portti 19). Echo lähettää takaisin vastaanottamansa paketin ja chargen tuottaa vastaukseksi joukon merkkejä. Jos ajatellaan tilannetta, jossa UDP paketin lähtöportti on 7 ja kohdeportti on 19, niin silloin vastaanotettu paketti generoi joukon merkkejä kohdekoneelta. Nämä merkit on osoitettu lähettäjäkoneen echo-porttiin. Lähdekone kaiuttaa nämä paketit takaisin, joka taas generoi lisää paketteja, jne. Lopulta kumpikin kone käyttää kaiken aikansa lähettelemällä paketteja edestakaisin, kunnes jompikumpi niistä kaatuu. Sillä välin nämä kaksi konetta kuluttavat loppuun kaiken verkon kaistanleveyden välillään [CER96]. Näin voidaan mahdollisesti estää kaikkien verkon koneiden verkkoyhteydet tai jommankumman kohteena olevan koneen verkkoyhteydet. Jokainen, jolla on verkkoyhteys, voi käynnistää tällaisen hyökkäyksen, joko laillisesti joltakin verkon koneelta tai osoiteväärennöksen avulla, joka useimmiten on hyökkäyksen taustalla.

Vastatoimenpiteenä on syytä kytkeä pois käytöstä chargen- ja echo-palvelut, sekä samoin myös kaikki käyttämättömät UDP-palvelut [CER96]. Jos tarvitaan pääsyä ulkopuolelta johonkin UDP-palveluun, niin voidaan käyttää proxy-palvelinta palvelun suojaamiseksi väärinkäytöltä. Tällöin on lisäksi syytä seurata verkkoa mahdollisen väärinkäytön suhteen. Koska tähän hyökkäystapaan tyypillisesti liittyy osoiteväärennös, niin on syytä ryhtyä toimenpiteisiin myös osoiteväärennösten estämiseksi.

4.5. Ping O' Death

Joskus hyökkääjä voi onnistua kaatamaan järjestelmän tai saattamaan sen epävakaaseen tilaan lähettämällä siihen verkon yli odottamatonta dataa [CER97]. TCP/IP spesifikaatio sallii paketin maksimikooksi 65536 tavua. On osoittautunut, että jotkut järjestelmät reagoivat ennalta arvaamattomalla tavalla saadessaan liian suuren IP-paketin. Järjestelmät voivat kaatua, hyytyä tai käynnistyä uudelleen (rebooting). Tämä on voitu saavuttaa ICMP (Internet Control Message Protocol) - paketeilla, joita ovat ICMP ECHO_REQUEST ja ICMP ECHO_RESPONSE, käyttäen "ping"-komentoa, jolla voidaan selvittää onko etäjärjestelmä tavoitettavissa verkon kautta. ICMP-paketit kapseloidaan IP-pakettien sisään. Monet ping toteutukset lähettävät oletusarvoisesti 8 tavun kokoisia ICMP-paketteja, mutta ne sallivat käyttäjän määritettäväksi kooltaan suurempia paketteja, jolloin niitä voidaan käyttää palvelunestohyökkäyksiin. Yksi paketti riittää hyökkäyksen toteuttamiseksi [Mar01].

4.6. Targa3

Tässä hyökkäystavassa hyökkääjä lähettää uhrin koneelle laittomia paketteja [Mar01]. Nämä väärinmuodostetut paketit saavat jotkin järjestelmät kaatumaan ja myös ne järjestelmät, joita kyseiset paketit eivät vahingoita, joutuvat käyttämään resurssejaan näiden pakettien käsittelyyn. Näille paketille on ominaista yksi tai useampi piirre seuraavista: väärä fragmentointi, protokolla, paketin koko tai IP-otsakkeen arvot. Lisäksi optiot, segmentit ja reititysliput saattavat olla normin vastaisia.

Hyökkäykseltä voidaan suojautua tarkastamalla kaikkien saapuvien pakettien laillisuus. Kaikkien mahdollisten väärinmuodostettujen pakettien listaamista ja tarkistamista ei tarvita.

4.7. Teardrop

Tämä hyökkäystapa perustuu siihen, että eräät vanhemmat TCP/IP toteutukset eivät osaa käsitellä oikealla tavalla limittyviä segmenttejä [Mar01]. Hyökkääjä lähettää joukon huolellisesti työstettyjä paketteja, jotka vaikuttavat tavallisilta paketeilta, mutta jotka on fragmentoitu siten, että osat olematta erillisiä menevätkin päällekkäin. Tämän johdosta vastaanottava kone kaatuu.

4.8. Sähköpostipommitus

Hyökkääjän tavoitteena on yrittää kuluttaa koneen levytilaa tuottamalla suuria määriä sähköpostiviestejä [CER02]. Sähköpostipommitus on luonteeltaan toimintaa, jossa hyökkääjä lähettää jatkuvasti sähköpostiviestejä samaan osoitteeseen uhriksi joutuneelle palvelimelle (site). Viestit koostuvat useissa tapauksissa mielivaltaisesta datasta ja niiden koot ovat suuria. Pyrkimyksenä on muiden järjestelmä- ja verkkoresurssien loppuun kuluttaminen. Kohteena voi olla kohdepalvelimella useampia käyttäjätilejä, jolloin palvelunestovaikutus kasvaa.

Sähköroskaposti (spamming) on pommituksen variantti, jossa sähköpostiviestejä lähetetään sadoilletuhansille käyttäjille (tai listoille, jotka kattavat näin suuria käyttäjämääriä). Vaikutus pahenee, jos vastaanottajat vastaavat viestiin, jolloin kaikki alkuperäiset osoitteet saavat vastausviestin. Tämä voi tapahtua täysin tietämättä siitä, että viestiin vastaaminen aiheuttaa viestin monistumisen tuhansille käyttäjille.

Sähköpostipommitukseen ja sähköroskapostiin voi liittyä myös osoiteväärennös, jolloin alkuperäisen lähettäjän selvittäminen on hyvin vaikeaa, ellei mahdotonta. Jos tarjoat sähköpostipalveluja käyttäjäyhteisölle, niin käyttäjäsi ovat haavoittuvia sähköpostipommitukselle ja sähköroskapostille. Sähköroskapostia on melkein mahdotonta estää, koska käyttäjä, jolla on toimiva sähköpostiosoite voi lähettää roskapostia mille tahansa toimivalle sähköpostiosoitteelle, uutisryhmälle tai ilmoitustaulu (bulletin-board) - palvelulle. Kun suuria sähköpostimääriä kohdistuu yhdelle palvelimelle, tai ne kulkevat saman palvelimen kautta, niin tämän johdosta palvelimen toimintakyky voi estyä. Seurauksena voi olla ylikuormitettut verkkoyhteydet tai verkkoyhteyksien menettäminen, järjestelmäresurssien menettäminen, levytilan täyttyminen monista postituksista johtuvien syslog-kirjausten takia tai järjestelmän kaatuminen.

Tällaiset hyökkäystavat voidaan havaita siitä, että sähköpostijärjestelmä muuttuu hitaaksi tai vaikuttaa, että viestit eivät lähde tai saavu. Tällöin syynä voi juuri olla, että postipalvelin yrittää käsitellä suuria määriä viestejä. Nykyisin ei ole olemassa tapaa estää sähköpostipommitusta tai sähköroskapostia, paitsi kytkeytymällä irti Internetistä ja lisäksi on mahdotonta ennalta tietää seuraavan hyökkäyksen lähdettä. On hyvin yksinkertaista päästä sisään suurille postituslistoille tai tietolähteisiin, jotka sisältävät suuria määriä sähköpostiosoitteita ja käynnistää hyökkäyksiä näiden avulla. Vastatoimenpiteinä voidaan kuitenkin kehittää organisaation sisäisiä työkaluja,

joiden avulla voidaan tunnistaa tilanne ja reagoida pommituksiin ja roskapostiin, ja siten minimoida toiminnan vaikutusta. Näiden työkalujen avulla pitäisi voida parantaa valmiutta 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 tahojen lähettämien viestien hylkäämiseen.

Jos järjestelmässä on vain pieni määrä postipalvelimia, niin palomuuri voidaan konfiguroida varmistamaan, että ulkopuolelta tulevat SMTP yhteydet voidaan ottaa vain pää sähköposti-palvelimeen, eikä muihin palvelimiin. Vaikka tämä ei estä hyökkäyksiä, niin se minimoi koneiden määrän, joihin ulkopuolinen voi kohdistaa SMTP-pohjaisen hyökkäyksen. Jos halutaan kontrolloida saapuvia SMTP-yhteyksiä suodattamalla tai muilla keinoin, niin näin on tarpeen konfiguroida vain pieni määrä laitteita.

Organisaation sähköpostin käsittelyjärjestelmät voidaan konfiguroida viemään viestit tiedostojärjestelmiin, joissa on käyttäjäkohtaiset kiintiöt. Tämä voi minimoida pommitus-hyökkäyksen vaikutusta rajaamalla vahingon vain kohteena olevaan käyttäjätiliin, jolloin hyökkäys ei vaikuta koko järjestelmään. Organisaation sisäiset käyttäjät on syytä neuvoa informoimaan pommituksista ja roskapostista. Roskapostin vaikutusta ei myöskään ole syytä edistää jatkamalla eteenpäin viestejä tai vastaamalla niihin.

4.9. Useat sisäänkirjautumisyritykset

Monissa järjestelmissä on ominaisuus, joka lukitsee käyttäjätilin, kun tietty määrä virheellisiä sisään kirjoittautumisyrityksiä on tehty [CER01]. Tavallisesti lukkiutuminen tapahtuu 3-5 epäonnistuneen yrityksen jälkeen. Hyökkääjä voi käyttää tätä järjestelmän ominaisuutta estääkseen laillista käyttäjää kirjautumasta sisään järjestelmään. Joskus näin voidaan estää jopa pääkäyttäjän sisäänpääsy järjestelmään.

Tähän hyökkäystapaan voidaan varautua siten, että on olemassa tapa päästä sisään järjestelmään hätätapauksissa. Tietoa löytyy yleensä käyttöjärjestelmän manuaaleista tai järjestelmän toimittaneelta taholta.

5. Palvelunestohyökkäysten torjuminen

Turvallisuus Internetissä on yhteinen asia ja se on sidoksissa Internetin yleiseen turvallisuuteen [CER00]. Yhden osapuolen laiminlyönnit turvallisuuden suhteen vaarantavat myös muiden osapuolten turvallisuuden, vaikka hyökkäys ei vahingoittaisi turvatoimenpiteet laiminlyönyttä tahoa, niin se voi aiheuttaa huomattavia vahinkoja ulkopuolisille. Lisäksi laitteet, jotka eivät ole osa keskitettyä laskentajärjestelmää ja joilla ei ole strategista merkitystä organisaation järjestelmässä voivat osaamattomasti ja huonosti ylläpidettyinä joutuessaan ulkopuolisten manipuloimiksi aiheuttaa huomattavaa vahinkoa kolmansille tahoille. On tärkeää, että turva-asioista vastaavat tahot ovat kaikkialla tietoisia uhkaavista vaaroista. Palvelunestohyökkäyksiä toteutetaan yleensä hyvin tunnettujen järjestelmien ja ohjelmien heikkouksien kautta. On tärkeää, että laitteisto- ja ohjelmistovalmistajien uudet turvapäivitykset otetaan aikailematta käyttöön.

CERT kehottaa noudattamaan seuraavia toimintatapoja palvelunestohyökkäysten torjuntaan [CER01]. Reitittimissä on syytä käyttää erityisiä reititinsuodattimia, joiden avulla voidaan vähentää verkkoon saapuvien ja sieltä lähtevien osoiteväärennettyjen IP-pakettien määrää, vaikkei niitä voidakaan nykyisellä IP-protokollan teknologialla täysin eliminoida [CER00b]. Nykyisin paras menetelmä on asentaa verkkoon suodattava reititin, joka ei päästä verkkoon sisään paketteja, joiden lähettäjäosoite on tässä samassa verkossa ja joka ei päästä verkosta ulos paketteja, joiden lähettäjäosoite ei ole tämän 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. On syytä kytkeä pois käytöstä kaikki käyttämättömät tai tarpeettomat verkkopalvelut, sillä tämä voi rajoittaa hyökkääjän kykyä hyödyntää näitä palveluja palvelunestohyökkäysten suorittamiseksi.

Ohjelmistojen ja käyttöjärjestelmien valmistajien uusimmat korjauspäivitykset tulee asentaa järjestelmään. On syytä ottaa käyttöön käyttöjärjestelmän tarjoamat kiintiöjärjestelmät, jos niitä on käytettävissä. Esimerkiksi, jos käyttöjärjestelmä mahdollistaa levykiintiöitä, niin näitä on syytä käyttää kaikkien käyttäjätilien kohdalla ja erityisesti silloin kun ne käyttävät verkkopalveluja. On tarkkailtava järjestelmän suorituskykyä ja määriteltävä tasot normaalikäytölle. Tällöin näitä voidaan käyttää poikkeuksellisen levyn ja keskusmuistin käytön, ja verkkoliikenteen havaitsemiseen.

Rutiininomaiset fyysiseen turvallisuuteen kohdistuvat tarkastukset ovat tarpeen, jolloin voidaan havaita poiketaanko sen hetken tarpeista. Tarkastuskohteita ovat palvelimet, reitittimet, ilman valvontaa olevat päätteet, verkkoon pääsypisteet, kaapelointikaapit, ympäristötekijät, kuten sähkövirta ja ilma, sekä muut verkon kriittiset komponentit. On tarpeen käyttää sopivia ohjelmistotyökaluja, että voidaan havaita, jos konfigurointitiedoissa tai muissa tiedostoissa on tapahtunut muutoksia. On tarpeen pitää varalla nopeasti käyttöönotettavissa olevia koneita, jos vastaavanlainen kone tulee toimintakyvyttömäksi. Verkkokonfigurointitietojen on syytä olla vikasietoisia ja niistä on syytä olla kopioita. On tarpeen kehittää ja ylläpitää säännöllisiä varmuuskopiointitoimintoja. Salasanojen suhteen on noudatettava tarkkoja varotoimenpiteitä, etenkin silloin, kun kyseessä ovat pääkäyttäjän oikeudet.

Edellisten toimien lisäksi voidaan käyttää myös joukkoa yleisiä suunnitteluperiaatteita kehitettäessä palvelunestohyökkäyksiltä suojaavia verkkoprotokollia [LAN00]. Resursseja ei tulisi sitoa tietoliikenneyhteyteen, ennen kuin asiakas on autentikoinut itsensä. Koska useimmat palvelunestohyökkäykset perustuvat osoitevääränn ökseen, on muistin allokoimista mielivaltaisen asiakkaan pyynnöstä on siten voitava välttää. Asiakkaan autentikointiin tulee ryhtyä vasta sitten, kun helpommat tavat havaita hyökkäys on loppuun suoritettu, koska autentikointi on toimenpide, joka kuluttaa paljon laskentatehoa. On olemassa tehokkaita tapoja, joilla voidaan havaita yritykset tehdä uudelleenlähetykseen perustuvia hyökkäyksiä väärentämällä IP-osoitetiedot.

Asiakkaan työtaakan tulisi aina olla palvelimen työtaakkaa suurempi. Tällöin voidaan asiakkaalta eliminoida hänen kykynsä käynnistää useita hyökkäyksiä, koska suurempi työtaakka kuluttaa loppuun hänen hyökkäyksen käynnistämiseksi tarvittavat resurssit. Asiakkaan työtaakan tulisi kasvaa lineaarisesti, kun taas palvelimen työtaakan tulisi säilyä niin vakioisena, kuin mahdollista ja tämän työtaakan tulisi olla asiakkaan työtaakasta riippumatonta.

Asiakkaan työtaakan tulisi olla parametrisoitavissa ja palvelimen tulisi kyetä helposti muuttamaan sitä. Tämä mahdollistaisi protokollien modifioimisen erilaisille sovellus-skenaarioille ja asiakaan laitteistoille. Lisäksi mahdollisuus muuttaa asiakkaan työtaakkaa mahdollistaa verkkoliikenteeseen reagoimisen ja puuttumisen. Jos epäillään hyökkäystä, niin protokollan vaikeusastetta voitaisiin vähitellen kasvattaa, jotta voitaisiin taata järjestelmän

toimintakyky epäillystä hyökkäyksestä huolimatta vähentämättä kuitenkaan huomattavissa määrin järjestelmän palvelujen saatavuutta laillisille käyttäjille.

Lähteet

CER03 CERT/Coordination Center Statistics 1988-2002, January 21 2003.
http://www.cert.org/stats/cert_stats.html

CER02 CERT Coordination Center: Email Bombing and Spamming, August 14, 2002.
http://www.cert.org/tech_tips/email_bombing_spamming.html

CER01 CERT Coordination Center: Denial of Service Attacks, June 4, 2001.
http://www.cert.org/tech_tips/denial_of_service.html

CER00 CERT/CC and FedCIRC: CERT Advisory CA-2000-01 Denial-of-Service Developments, January 3, 2000.
http://www.cert.org/advisories/CA-2000-01.html

CER00b CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks, November 29, 2000.
http://www.cert.org/advisories/CA-1996-21.html

CER00c CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks, March 13, 2000.
http://www.cert.org/advisories/CA-1998-01.html

CER97 CERT Advisory CA-1996-26 Denial-of-Service Attack via ping, December 5, 1997.
http://www.cert.org/advisories/CA-1996-26.html

CER96 CERT Advisory CA-1996-01 UDP Port Denial-of-Service Attack, September 24, 1997
http://www.cert.org/advisories/CA-1996-01.html

CIS00 Cisco Systems Inc: Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks, February 17, 2000.
http://www.cisco.com/warp/public/707/newsflash.html

CSI02 2002 Computer Crime and Security Survey, April 7 2002.
http://www.gocsi.com/press/20020407.html

LAN00 Leiwo, Aura, Nikander: "Towards network denial of Service resistant protocols". IFIP TC11 16th Annual Working Conference on Information Security, 2000.

Mar01 Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint, Springer-Verlag, 2001.

McC01 Stuart McClure, Joel Scambray, George Kurtz: Hacking Exposed: Network Security Secrets and Solutions, Third edition, Osborne/McGraw-Hill, 2001.

Paa00 Paavilainen, J, Tietoturva 2000: Tietoturvan kyselytutkimus, Tampereen yliopisto, 2000.
http://www.tietoturva.org/TituKysely2.pdf

Sta99 Stallings,W, Cryptography and network security: Principles and practises, Prentice-Hall, 1999.