LAUREA AMMATTIKORKEAKOULU Uuden edellä

Palvelunestohyökkäysten torjunta

Seuri, Jan

2011 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Palvelunestohyökkäysten torjunta

Jan Seuri
Turvallisuusosaaminen
ylempi amk
Opinnäytetyö
Toukokuu, 2011

Laurea-ammattikorkeakoulu Tiivistelmä
Laurea Leppävaara
Turvallisuusosaamisen ylempi ammattikorkeakoulututkinto

Jan Seuri

Palvelunestohyökkäysten torjunta

Vuosi 2011 Sivumäärä 62

Ympäröivä yhteiskunta on yhä enemmän ja enemmän riippuvainen Internetistä. Verkkokaupan osuus kasvaa, pankit ohjaavat asiakkaitaan verkkopalveluihinsa ja myös viranomaiset siirtävät ainakin osittain palvelujaan verkkoon. Monen yrityksen asiakkaat ovat kaikki verkossa eli nämä yritykset ovat täysin riippuvaisia verkkopalveluidensa toimivuudesta. Vastuunsa tunteva verkkokauppaa harjoittava yritys pystyy varmistamaan tietoturvan CIA-kolmijalasta (Confidentiality – luottamuksellisuus, Integrity – Eheys, Availability – saatavuus) tiedon luottamuksellisuuden ja eheyden ainakin tiettyyn tasoon asti, mutta tiedon saatavuuden varmistaminen on näinä päivinä haastavampaa.

Opinnäytetyön punaisena lankana on uhkien eli eri palvelunestohyökkäystyyppien suhde teoreettisiin ja käytännöllisiin vastatoimiin ja toisaalta kaupallisiin ratkaisuihin. Ideaalitilanteessa kaikkiin palvelunestohyökkäystyyppeihin löytyy vastatoimet, jotka ovat myös toteuttamiskelpoisia, jolloin myös vastaavat kaupalliset ratkaisut ovat niitä tarvitsevien organisaatioiden hankittavissa.

Tässä työssä muodostetaan tehokkaan puolustuksen vaatimusluettelo palvelunestohyökkäyksiä vastaan. Se on hyvä työkalu kaikille organisaatioille, jotka harkitsevat torjuntatuotteen hankintaa.

Palvelunestohyökkäyksen uhka luultavasti vain kasvaa jatkossa. Internetiin liitettyjen koneiden määrä lisääntyy jatkuvasti, toisin sanoen verkossa on enemmän potentiaalisia agentteja ja myös hyökkäyksen kohteita. Internet-yhteydet muuttuvat koko ajan nopeammiksi, jolloin yksi agentti pystyy generoimaan enemmän hyökkäysliikennettä. Lisäksi ohjelmistot muuttuvat yhä vain monimutkaisemmiksi. Monimutkaisten ohjelmistojen haavoittuvuuksia voidaan hyödyntää paitsi agenttien hankkimisessa myös itse palvelunestohyökkäyksissä.

Laurea University of Applied Sciences
Laurea Leppävaara
Master´s Programme in Security Management

Abstract

Jan Seuri

Prevention of denial of service attacks

Year 2011 Pages 62

The surrounding society is becoming more and more dependent on the Internet. E-commerce is growing, the banks are guiding their clients to online services, and the authorities will transfer at least some services online. Customers of many companies are all online so these companies are totally dependent on Internet. A responsible e-commerce can safeguard, at least to certain level, confidentiality and integrity of the three feet information security CIA model (Confidentiality, Integrity, Availability), but securing availability is more challenging these days.

Central theme of this thesis is a threat of different types of denial of service attacks and their relationship to different theoretical and practical counter-measures and to commercial solutions. Ideally all types of denial of service attacks have their counter-measures. If they are also feasible, then corresponding commercial solutions are available for organizations to obtain.

The requirement list of effective defense of denial of service attacks is built in this work. It is a good tool for all organizations that are considering the acquisition of prevention product.

Denial of service threat will probably only grow in the future. The number of machines connected to the Internet continues to increase, in other words, the network has more potential agents and also targets to attack. Internet connections are changing faster all the time, so that one agent will be able to generate more attack traffic. In addition to the software are becoming only more complex. Complex software has potentially more vulnerabilities that can be exploited not only to obtain agents but also in denial of service attacks itself.

SISÄLLYSLUETTELO

1. Johdanto

Ympäröivä yhteiskunta on yhä enemmän ja enemmän riippuvainen Internetistä. Verkkokaupan osuus kasvaa, pankit ohjaavat asiakkaitaan verkkopalveluihinsa ja myös viranomaiset siirtävät ainakin osittain palvelujaan verkkoon. Monen yrityksen asiakkaat ovat kaikki verkossa eli nämä yritykset ovat täysin riippuvaisia verkkopalveluidensa toimivuudesta. Vastuunsa tunteva verkkokauppaa harjoittava yritys pystyy varmistamaan tietoturvan CIA-kolmijalasta (Confidentiality – luottamuksellisuus, Integrity – Eheys, Availability – saatavuus) tiedon luottamuksellisuuden ja eheyden ainakin tiettyyn tasoon asti, mutta tiedon saatavuuden varmistaminen on näinä päivinä haastavampaa.

Syynä ovat erilaiset palvelunestohyökkäykset. Sotilaallinen, poliittinen tai taloudellinen motiivi ovat kaikki tavallaan järkeviä motiiveja palvelunestohyökkäykselle, mutta hyökkääjän motiivina voi olla myös pelkästään näyttämisen halu tai kiusanteko. Kun myös helppokäyttöisiä hyökkäystyökaluja on julkisesti saatavilla ja Internetissä voi myös vuokrata hyökkäykseen käytettäviä saastuneiden koneiden verkkoja, on palvelunestohyökkäyksen kohteeksi joutuminen yhä sattumanvaraisempaa.

Teoreettisia palvelunestohyökkäyksen torjuntakeinoja on tutkittu paljon. Näitä esitellään luvuissa 6 ja 7. Myös kaupallisten tuotteiden ominaisuuksien vertailuja löytyy Internetistä ja alan lehdistöstä. Näiden kahden erilaisen katsantokannan välistä suhdetta tarkastelevaa materiaalia en ole kuitenkaan löytänyt. Tämä tutkielma pyrkii täyttämään tätä aukkoa.

Tutkielman tarkoituksena on selvittää löytyykö erilaisten (hajautettujen) palvelunestohyökkäysten torjumiseksi hyvään teoriaan pohjautuvia käytännön ratkaisuja.

Ensin käyn läpi ongelmakenttää, mm. julkisuudessa olleita palvelunestohyökkäyksiä. Lähteinä esim. kansallisen tietoturvaviranomaisen CERT-FI:n ja Euroopan verkko- ja tietoturvaviranomaisen ENISA:n www-sivut. Lisäksi analysoin palvelunestohyökkäysten motiiveja (esim. kiristys).

Tämän jälkeen käsittelen palvelunestohyökkäysten peruskäsitteistöä ja erilaisia hyökkäystyyppejä sekä muutamia julkisesti saatavilla olevia työkaluja palvelunestohyökkäysten toteuttamiseen.

Teoreettisia ja käytännöllisiä vastatoimia eri hyökkäystyyppeihin tarkastelen mm. IEEE:n ja ACM:n dokumenttien pohjalta. Löytyykö kaikkiin hyökkäystyyppeihin edes teoreettisia vastatoimia (siis muuta kuin kapasiteetin rajaton lisääminen)?

Luvun 6 (Vastatoimia) pohjalta olen muodostanut luvussa 7 esitetyn tehokkaan puolustuksen vaatimusluettelon.

Sitten vertaan em. vaatimusluetteloa Gartnerin Magic Quadrant for Network IPS -dokumentissa mainittujen palvelunestohyökkäysten torjuntaan profiloituneiden kaupallisten ratkaisujen ominaisuuksiin. Ajatuksena on selvittää kyseisten kaupallisten tuotteiden

ominaisuuksia tutkimalla löytyykö teoreettisille ja käytännöllisille vastatoimille kaupallisia ilmentymiä. Jos vastatoimi on kustannustehokkaasti toteutettavissa, niin silloin siitä syntyy myös kaupallinen ratkaisu.

Opinnäytetyön punaisena lankana on uhkien eli tässä tapauksessa eri palvelunestohyökkäystyyppien suhde teoreettisiin ja käytännöllisiin vastatoimiin ja toisaalta kaupallisiin ratkaisuihin. Ideaalitilanteessa kaikkiin palvelunestohyökkäystyyppeihin löytyy vastatoimet, jotka ovat myös toteuttamiskelpoisia, jolloin myös vastaavat kaupalliset ratkaisut ovat niitä tarvitsevien organisaatioiden hankittavissa.

Tässä työssä muodostetaan tehokkaan puolustuksen vaatimusluettelo palvelunestohyökkäyksiä vastaan. Se on hyvä työkalu kaikille organisaatioille, jotka harkitsevat torjuntatuotteen hankintaa. Tehokkaan puolustuksen vaatimusluettelo ja sitä edeltävä Vastatoimia-luku tarjoavat tiiviin tietopaketin kaikille niille, jotka haluavat ymmärtää paremmin palvelunestohyökkäysten logiikkaa ja niiden torjuntaa.

2. Opinnäytetyön tavoitteet ja menetelmät

Luvussa 3 esitetyt esimerkit palvelunestohyökkäyksistä ja niiden motiiveista ovat vain pieni osuus julkisuudessa olleista tapauksista. Uhka on siis todellinen ja sitä esiintyy ainakin seuraavilla tasoilla: yksittäinen palvelu, teleoperaattori, valtio ja kansainvälinen yritys. Tämän opinnäytetyön tavoitteena on muodostaa tehokkaan puolustuksen vaatimuslista. Listan vaatimukset täyttämällä yritys pystyy pienentämään merkittävästi palvelunestohyökkäyksen muodostamaa uhkaa www-palvelulleen. Myös teleoperaattori pystyy vaatimukset huomioimalla suojaamaan paremmin asiakkaitaan.

Työ on toteutettu käyttäen konstruktiivisen tutkimusmenetelmän prosessia, mikä on kuvattu seuraavassa [MOR09]:

1. Mielekkään ongelman etsiminen
2. Syvällisen teoreettisen ja käytännöllisen tiedon hankinta tutkimuksen ja kehittämisen kohteesta
3. Ratkaisujen laatiminen
4. Ratkaisun toimivuuden testaus ja konstruktion oikeellisuuden osoittaminen
5. Ratkaisussa käytettyjen teoriakytkentöjen näyttäminen ja ratkaisun uutuusarvon osoittaminen
6. Ratkaisun soveltamisalueen laajuuden tarkastelu

Tässä opinnäytetyössä toteutettiin vastaavat konstruktiivisen tutkimusmenetelmän osaprosessit seuraavasti:

1. Ongelma, mihin pyrittiin löytämään ratkaisu, on yritys A:n verkkokaupan elokuussa 2010 halvaannuttanut hajautettu palvelunestohyökkäys.
2. Tietoa hankittiin eri hyökkäystyypeistä ja -työkaluista. Lisäksi tutkittiin teoreettisia protokollatason parannusehdotuksia sekä käytännön vastatoimia.

3. Käytännön vastatoimista muodostettiin tehokkaan puolustuksen vaatimuslista, jollaista ei ennen ollut saatavilla ainakaan julkisista lähteistä. Vaatimuslistaa verrattiin markkinoilla olevien tuotteiden ominaisuuksiin.
4. Yhtä tehokkaan puolustuksen vaatimukset täyttävää tuotetta testattiin kattavasti ennen ostopäätöstä.
5. Hankittu tuote on toiminut käytännössä moitteetta. Tehokkaan puolustuksen vaatimuslista on toimiva ainakin nykyisiä hyökkäystyyppejä vastaan.
6. Tehokkaan puolustuksen vaatimuslistaa voi soveltaa yksittäisen www-palvelun suojaamisessa, mutta se skaalautuu myös teleoperaattoreiden tarpeisiin.

3. Ongelmakenttä

Tässä luvussa esitellään ensin amerikkalaisen tietotekniikka-alan tutkimusyhtiö Gartnerin kahta raporttia, joissa käsitellään palvelunestohyökkäyksiä nimenomaan uhkan suuruuden näkökulmasta. Tämän jälkeen käsitellään lyhyesti julkisuudessa olleita palvelunestohyökkäyksiä ja niihin liittyviä motiiveja.

3.1. Gartner

Gartner, Inc jakaa raportissaan Gartner 2008 IT Security Threat Projection Timeline (26.8.2008) ICT-uhat kolmeen kategoriaan: nykyinen uhkaympäristö, keskipitkän aikavälin ja pitkän aikavälin uhkaympäristö. Hajautettu palvelunestohyökkäys kuuluu nykyiseen uhkaympäristöön, johon Gartnerin mukaan niiden, jotka ovat riippuvaisia www-palvelunsa jatkuvuudesta, pitäisi reagoida heti. Uhkan vakavuus (severity) on Gartnerin mukaan 7,7 10-portaisella asteikolla.

Myös raportissa Hype Cycle for Infrastructure Protection, 2009 (28.7.2009) Gartner toteaa, että suojautumisen palvelunestohyökkäyksiä vastaan pitäisi olla normaali osa Internet-yhteyden hankkimista organisaatioille, jotka ovat riippuvaisia siitä, että heidän www-palvelunsa on saatavilla suunnitellusti. Gartner toteaa myös, että ainoastaan isojen organisaatioiden, joilla on lisäksi monimutkainen tietoliikenneverkko www-palveluaan tuottamassa, tulisi hankkia itselle laitteisto palvelunestohyökkäyksiä vastaan. Muiden tulisi harkita tietoliikenteen tarkkailu- ja suodatuspalvelujen hankkimista Internet-palveluntarjoajaltaan.

3.2. Julkisuudessa olleita palvelunestohyökkäyksiä ja niiden motiiveja

Microsoft

Tammikuussa 2001 Microsoftin online-palvelut hävisivät verkosta. Syyksi raportoitiin ensin väärin konfiguroitua verkkoa, mikä tavallaan pitikin paikkansa. Myöhemmin kävi ilmi, että Microsoftin kaikki nimipalvelimet olivat sijainneet yhden reitittimen takana samassa verkkosegmentissä. Hyökkääjät onnistuivat ”kaatamaan” tämän yhden reitittimen, jolloin Microsoftin kaikki online-palvelut olivat tavoittamattomissa. Microsoft hajautti nopeasti nimipalvelunsa maantieteellisesti lisäten samalla redundanssia. Näin yllämainitun kaltaisen

hyökkäyksen toteuttaminen tuli huomattavasti vaikeammaksi. [MDD05]

Huomionarvoinen seikka on, että kaikille yrityksille nimipalvelun suojaaminen Microsoftin tavoin ei ole mahdollista tai ainakaan taloudellisesti järkevää. [MDD05]

Microsoftin nimipalveluun kohdistuneen hyökkäyksen motiivina lienee ollut yleinen Microsoftin vastaisuus ja näyttämisen halu.

Eesti

Viestintävirastossa toimiva kansallinen tietoturvaviranomainen CERT-FI uutisoi 4.5.2007, että Eestin hallintoa vastaan suunnatut palvelunestohyökkäykset jatkuvat edelleen. Suurimman osan liikenteestä aiheutti saastuneiden koneiden verkot eli botnetit, joita hyökkääjät komensivat. Osa liikenteestä oli peräisin Internetin keskustelupalstoilla levitetyistä erilaisista komentosarjoista. [Cer01]

Samassa yhteydessä CERT-FI pyysi suomalaisten verkkojen ylläpitäjiä ilmoittamaan liikenteestä, joka koostuu pääosin ICMP Echo Request- ja TCP SYN –paketeista, ja joka suuntautuu seuraavaan verkkolohkoon [Cer01]:

- AS 8240 / ASO Autonomous System
- Inetnum 195.80.96.0 - 195.80.111.255
- BGP Prefix 195.80.96.0/19

Euroopan verkko- ja tietoturvaviranomainen ENISA kertoi lehdistötiedotteessaan 24.5.2007, että hyökkäysten kohteena olivat olleet erityisesti Eestin hallituksen ja poliisin sivustot. Myös yksityinen pankkisektori ja mediatalot olivat olleet hyökkäyksen kohteena. Eesti joutui estämään ulkomaan liikenteen hyökkäyksen kohteena olleille sivustoille useaksi päiväksi, jotta ne pystyivät palvelemaan kotimaan tarpeita. [Eni01]

ENISA painottaa lehdistötiedotteessaan ennakkovarautumisen ja yhteistyön tärkeyttä. Tässä Eestin tapauksessa yhteistyö sujui erinomaisesti eri CERT-toimijoiden välillä Euroopassa ja Euroopan ulkopuolella. [Eni01]

InfraGard on Yhdysvaltain liittovaltion poliisin FBI:n ja yksityisen sektorin yhteistyöohjelma, jonka tavoitteena on suojella Yhdysvaltain infrastruktuuria. InfraGard toimii FBI:n kenttätoimistojen yhteydessä. [FBI01]

Alabaman osavaltiossa toimiva Birmingham InfraGard on tutkinut Eestin palvelunestohyökkäystä ja esittää yksiselitteisesti poliittista motiivia hyökkäykselle. Birmingham InfraGardin kirjallisessa tuotoksessa ”Estonia vs. Russia, The DDOS War” hyökkäyksen taustalla nähdään pronssosoturin siirtohanke Tallinnassa ja syyttävä sormi osoittaa nimenmaan Venäjää ja Eestin venäläisvähemmistöä. [FBI02]

Veikkaus

Kansallisen rahapeliyhtiö Veikkauksen nettipelipalveluun kohdistui hajautettu

palvelunestohyökkäys 15.8.2009. Suuri määrä lähinnä ulkomailta tulleita yhteydenottoja kuormitti Veikkauksen palvelimia klo 15:30–18:10 haitaten sivujen normaalia käyttöä. Veikkaus kertoi varautuneensa hyökkäyksiin jo ennalta, ja ongelma saatiinkin rajattua jo lauantai-iltana. [Tie01]

Hyökkäykset jatkuivat tämänkin jälkeen, mutta ei enää palvelua häiriten. CERT-FI:n mukaan hyökkäys oli Suomen oloissa harvinaisen raju. [Tk_01]

Nopealla yhteistyöllä oman Internet-palveluntarjoajan sekä CERT-FI:n kanssa on oleellinen merkitys, kun halutaan rajoittaa tehokkaasti hyökkäyksen vaikutuksia. Jos organisaation toiminta riippuu merkittävästi verkkopalveluista, tarvittavista varautumistoimenpiteistä tulee sopia palveluntarjoajan kanssa jo etukäteen. [Cer02]

CERT-FI sai kansainvälisen yhteistyön ansiosta hyökkäykseen käytetyn botnetin komentopalvelimen selville noin tunti sen jälkeen, kun se oli saanut ilmoituksen hyökkäyksestä. Näin rajoittavat toimenpiteet voitiin aloittaa nopeasti. CERT-FI myös varoitti saman botnetin kohteena olleita ulkomaisia tahoja. Komentopalvelimia saatiinkin siivottua eri puolilta maailmaa. [Cer03]

Peliyhtiöitä vastaan suunnatuille palvelunestohyökkäyksille on usein esitetty taloudellista motiivia kiristyksen muodossa. Näin ei tässä tapauksessa ainakaan Veikkauksen osalta ollut. Kohteena oli tosin muitakin peliyhtiöitä, mm. Tanskan valtiollinen peliyhtiö Danske Spil. [Tk_02]

15.8.2009 oli urheilussa merkittävä päivä kahdessakin mielessä. Se oli Englannin Valioliigan alkamispäivä ja myös Yleisurheilun mm-kisojen avajaispäivä. Hyökkäyksen motiivina olikin ehkä vain voimannäyttö tai sitten hyökkäyksen pääkohde oli ulkomailla ja muut kohteet vain hämäystä.

Massapostitettuja palvelunestohyökkäysuhkauksia

CERT-FI ilmoitti 13.8.2010 vastaanottaneensa useita ilmoituksia sähköpostiviesteistä, joissa verkkotunnusten haltijoita on uhattu palvelunestohyökkäyksellä. Kiristysviestit olivat tulleet lähettäjäosoitteen perusteella yahoo.com -domainista. Viestien mukaan palvelunestohyökkäys on vältettävissä maksamalla pieni summa rahaa viesteissä kerrotulla maksumenetelmällä. Samansisältöisiä viestejä oli vastaanotettu eri puolilla maailmaa jo vuoden 2009 puolella. [Cer04]

CERT-FI:n tiedossa ei ole, että maksamatta jättäminen olisi kertaakaan johtanut palvelunestohyökkäykseen viestin vastaanottajaa kohti. CERT-FI suositteli olemaan reagoimatta kyseisiin viesteihin. [Cer04]

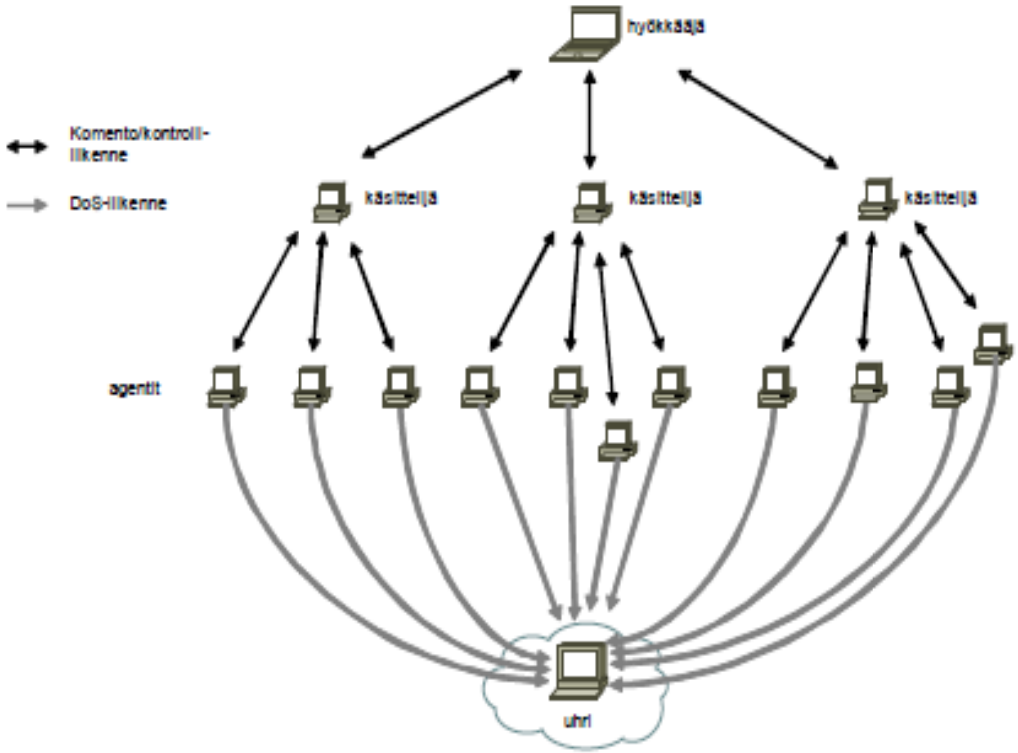
4. Peruskäsitteistöä ja hyökkäystyyppejä

Tässä luvussa esitellään peruskäsitteistöä ja käsitellään erilaisia hyökkäystyyppejä. Yksi ilmeinen palvelunestohyökkäystyyppi on fyysinen, esim. verkkokaapelin katkaisu tai konesalin sytyttäminen tuleen, mutta sitä ei tässä esityksessä tarkastella lähemmin.

4.1. Hyökkäystyyppien jaottelua

Pääjako eri hyökkäystyypeissä on ei-hajautettu palvelunestohyökkäys vs. hajautettu palvelunestohyökkäys. Hajautetuissa palvelunestohyökkäyksissä apuna käytetään useampaa tietokonetta. Tyypillisesti nämä koneet ovat virusten tai erilaisten haittaohjelmien avulla kaapattuja (koti)tietokoneita eli agentteja (bot). Hyökkäysverkkohierarkia käsittää usein varsinaisen hyökkääjän ja agenttien lisäksi käsittelijöitä (master/handler), jotka hallitsevat tiettyä osajoukkoa agenteista. [Möl06]

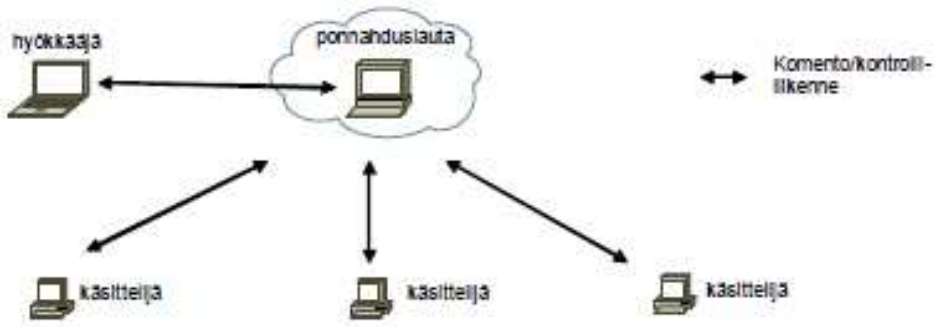
Kuvassa 1 esitetään hyökkääjä/käsittelijä/agentti –arkkitehtuuri. [Tut01]



KUVA 1: Hyökkääjä/käsittelijä/agentti -arkkitehtuuri

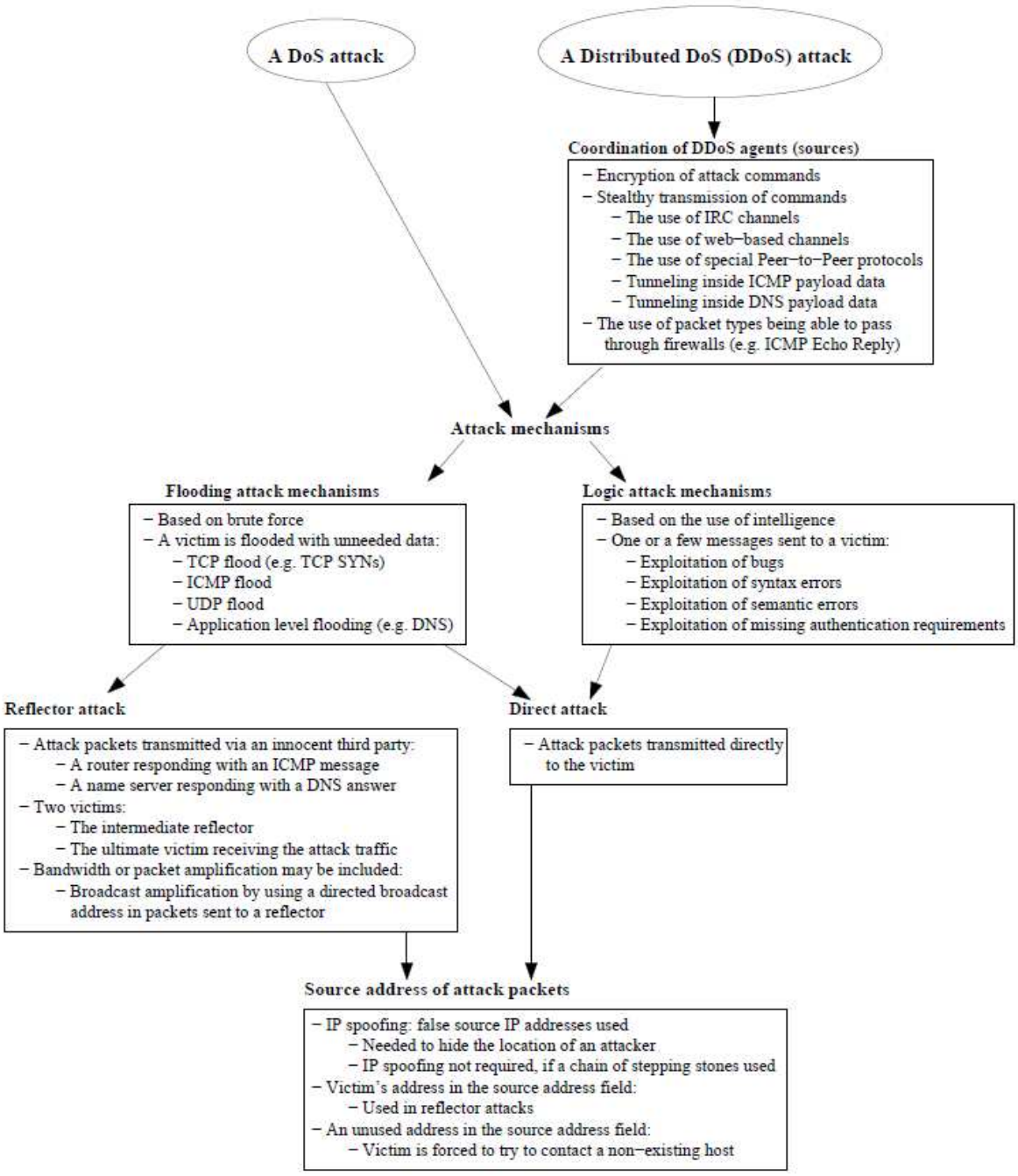
Varsinainen hyökkääjä voi hallita käsittelijöitä yhden tai useamman välikoneen eli ponnahduslaudan (stepping stone) avulla. Ponnahduslautojen tarkoitus on vaikeuttaa varsinaisen hyökkääjän tunnistamista. [Möl06]

Kuvassa 2 esitetään H yökkääjä/ponnahduslauta/käsittelijä –arkkitehtuuri. [Tut01]



KUVA 2: Hyökkääjä/ponnahduslauta/käsittelijä -arkkitehtuuri

Perusjaon eli ei-hajautetun palvelunestohyökkäyksen ja hajautetun palvelunestohyökkäyksen jälkeen hajautetulla puolella on vuorossa agenttien koordinointi. Sitten hyökkäysmekanismit jaetaan loogisiin mekanismeihin ja tulvitukseen (flooding). Vaikka kaikkia hyökkäystyyppejä voi soveltaa sekä ei-hajautettuina että hajautettuina, niin tulvituksessa lähes poikkeuksetta käytetään apuna useampaa tietokonetta eli kyseessä on tällöin raakaan voimaan (brute force) perustuva hajautettu palvelunestohyökkäys. Kuvassa 3 esitetään eräs palvelunestohyökkäystyyppien jaottelu. [Möl06]

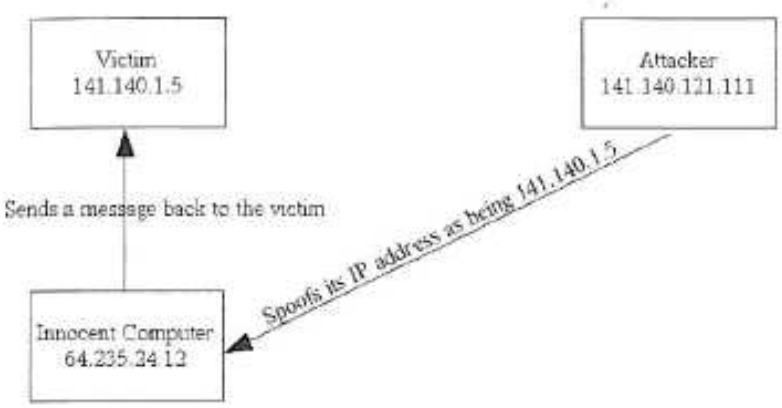


KUVA 3: Eräs palvelunestohyökkäystyyppien jaottelu

Varsinkin jos ponnahduslautoja ei käytetä, hyökkääjä usein haluaa väärentää ip-osoitteensa (ip spoofing) identiteettinsä suojelemiseksi. Jokainen verkossa liikkuva ip-paketti sisältää kontrollitietoa ip-otsikossa (ip header). Yksi ip-otsikon kentistä sisältää paketin lähettäjän ip-osoitteen eli lähdeosoitteen. Tämän kentän sisällön hyökkääjä voi muuttaa mieleisekseen. [MDD05]

Jos hyökkääjä väärentää ip-osoitteensa siten, että se on sama kuin uhrin ip-osoite, on kyseessä smurffi-hyökkäys (smurf attack). Kuvassa 4 esitetään esimerkki smurffi-

hyökkäyksestä. [Cha09]



KUVA 4: Esimerkki smurffi-hyökkäyksestä.

4.2. Haavoittuvuuksien hyödyntäminen

Kohdekoneen haavoittuvuuksia hyödynnetään lähettämällä oikein muotoiltu ip-paketti tai muutama kohdekoneelle, joka tällöin joutuu toimimattomaan tilaan. [MDD05]

Klassinen esimerkki haavoittuvuuksien hyödyntämisestä on kyynelhyökkäys (teardrop). Koska ip-paketin maksimikoko on 65536 tavua, pitää tätä suuremmat sanomat fragmentoida eli jakaa erillisiin ip-paketteihin. Nämä sanoman muodostavat ip-paketit saapuvat kohdekoneelle eri aikaan ja mahdollisesti eri reittiäkin. Kun kaikki ip-paketit ovat saapuneet, kohdekone kokoaa niistä taas loogisen sanoman. Kyynelhyökkäys tehdään siten, että kohdekoneelle lähetetään suuri joukko ip-paketteja, joista kohdekone ei pysty muodostamaan kokonaista sanomaa. Kohdekone pitää kaikki saapuneet paketit muistissa, jolloin sanomapuskuri (message puffer) täyttyy eivätkä muut, oikeat sanomat pääse perille. Aikakatkaisu (timeout) on vastalääke kyynelhyökkäykseen, mutta tällöinkin kohdekone on ollut ainakin jonkin aikaa tavoittamattomissa. [Cha09]

Järjestelmien ohjelmistotasot pitäisi siis olla mahdollisimman tuoreita, jotta haavoittuvuuksia olisi mahdollisimman vähän. Tuotantojärjestelmissä tämä on usein ongelmallista, koska käyttöjärjestelmien ja varusohjelmistojen päivitykset voivat johtaa siihen, että sovelluksen toiminnallisuus kärsii. Muutokset tuotantojärjestelmiin joutuvatkin usein käymään läpi koko testisyklin, ennen lopullista käyttöönottoa, mikä on ristiriidassa sen kanssa, että ohjelmistotasot pitäisi olla mahdollisimman tuoreita. Tämä ristiriita on mahdollista ratkaista sovellustason palomuurilla, joita löytyy nykyään monilta kaupallisilta toimijoilta.

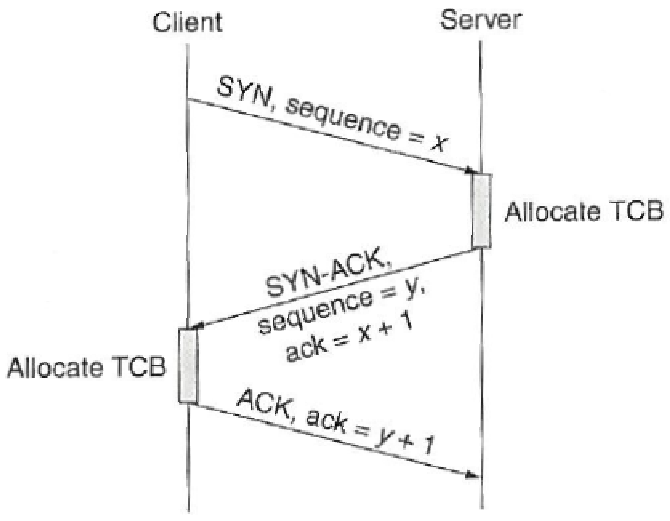
OWASP on ei-kaupallinen toimija, jonka ylläpitämä Top 10 –lista [OWA10] on defacto-

standardi www-palvelun pahimmista haavoittuvuuksista. OWASP:n listaa referoi mm. korttimaksamisen tietoturvastandardi (PCI DSS, Payment Card Industry Data Security Standard), joka hyväksyy Top 10 –listan haavoittuvuuksilta suojautumisen sovellustason palomuurilla. [PCI08]

Vaikka sovellustason palomuuri olisikin käytössä, kannattaa tuotantojärjestelmän ohjelmistotasojen päivitykset testata ja ottaa käyttöön siltä osin kuin mahdollista, jotta sovellustason palomuurista ei muodostuisi ainoaa suojaa (single-point-of-failure), vaan että monikerroksisen suojauksen periaate toteutuisi.

4.3. Protokollaa vastaan hyökkääminen

TCP-sessio alkaa asiakkaan ja palvelimen välisellä neuvottelulla sessioparametreista. Asiakas lähettää TCP SYN –paketin palvelimelle pyytäen jonkin TCP-portin palvelua (service). SYN-paketin otsikkotiedoissa asiakas kertoo palvelimelle oman yhteyskohtaisen numeronsa (initial sequence number), jonka avulla palvelin tunnistaa juuri tämän asiakkaan palvelimelle lähettämän datan. Palvelimen vastaanottaessa SYN-paketin se varaa samalla lähetyskontrollilohkon (transmission control block, TCB), johon se tallentaa tiedot asiakkaasta. Sitten palvelin vastaa asiakkaalle SYN-ACK –viestillä, että palvelupyyntöön on suostuttu. Lisäksi palvelin kuittaa asiakkaan ilmoittaman yhteyskohtaisen numeron ja kertoo oman yhteyskohtaisen numeronsa. Vastaanottaessaan SYN-ACK –viestin asiakas varaa myös lähetyskontrollilohkon. Tämän jälkeen asiakas vastaa ACK-viestillä palvelimelle, mikä päättää yhteyden avaamisen. Tätä yhteyden avaavaa viestinvaihtoa sanotaan kolmivaiheiseksi kättelyksi (three-way handshake) ja se on esitetty kuvassa 5. [MDD05]



KUVA 5: TCP-yhteyden avaava kolmivaiheinen kättely.

TCP-yhteyden avaavaa kolmivaiheista kättelyä hyödyntäen on mahdollista tehdä TCP SYN –tulvitushyökkäys. Siinä asiakas ei lähetäkään yhteyden avaamisen päättävää ACK-viestiä

sitä odottavalle palvelimelle. Kun näitä hajautettuun palvelunestohyökkäykseen osallistuvia asiakkaita on satoja tai tuhansia, joutuu palvelin varaamaan jokaiselle yhteydelle lähetyskontrollilohkon. Vaikka aikakatkaisu vapauttaakin lähetyskontrollilohkoja, saadaan palvelimen tietyssä portissa oleva palvelu toimimattomaan tilaan ainakin joksikin aikaa. [Cha09]

Puolustautuminen protokollahyökkäystä vastaan on erittäin hankalaa, jos hyökkäys hyväksikäyttää protokollan heikkouksia. Tällöin puolustautuminen voi vaatia muutoksia protokollan määritelmään, minkä muuttaminen on, jos se yleensäkään onnistuu, pitkä prosessi. [MDD05]

4.4. Loogiset hyökkäykset

Looginen hyökkäys voi kohdistua myös algoritmiin, jossa on haavoittuvuus. Algoritmi voi olla esimerkiksi tiivistefunktio (hash function). Hyökkääjän lähettäessä dataa, minkä prosessointi hyödyntää tiivistefunktion haavoittuvuutta, saattaa esim. perättäisten syötteiden prosessointiaika muuttua lineaarisesta eksponentiaaliseksi. Tällöin prosessorikuorma saadaan nousemaan tasolle, joka vaikuttaa palvelutasoon. [MDD05]

Edellä mainitun kaltaiselta hyökkäykseltä voi puolustautua poistamalla haavoittuvuus algoritmista. Tämä edellyttää että ongelma eli palvelun hitauden syy pitää ensin paikallistaa, mikä ei aina ole helppoa. Näin varsinkin jos hyökkääjä on löytänyt ns. nollapäivähaavoittuvuuden. Voi myös olla, ettei hyökkäyksen kohde voi haavoittuvuutta itse poistaa, vaan ongelman korjaus edellyttää algoritmin valmistajan päivitystä, mikä voi olla saatavissa vasta viiveellä. Jos algoritmi ei ole ehdottoman tarpeellinen, sen voi tietysti poistaa väliaikaisesti käytöstä. [MDD05]

Myös tietokantakyselyt voivat sisältää loogisen hyökkäyksen mahdollisuuden. Jos esimerkiksi www-palvelussa käyttäjälle annetaan mahdollisuus tehdä tietokantakyselyjä, kannattaa niihin liittyvät proseduurit suunnitella huolella. Lisäksi jos on tiedossa raskaita ja usein toistuvia tietokantahakuja, kannattaa nämä haut tehdä mahdollisuuksien mukaan jo etukäteen ja tarjota vastaus käyttäjille ilman, että joka kyselyn yhteydessä tehtäisiin raskas tietokantahaku.

4.5. Sovellusta vastaan hyökkääminen

Sovellusta vastaan hyökkäämisestä on kyse esimerkiksi silloin, kun www-palvelimella on määritelty maksimipyyntömäärä, johon palvelin vastaa sekunnissa, ja hyökkääjä ylittää tarkoituksella tämän maksimimäärän botnetin avulla. [MDD05]

Myös virusten, matojen ja muiden haittaohjelmien avulla voidaan hyökätä sovellusta vastaan häiriten sen toimintaa tai pahimmassa tapauksessa estäen sen toiminnan kokonaan. [Cha09]

4.6. Resurssien varaaminen

Jos hyökkääjän tavoitteena on vain hyökkäyksen kohteen kaikkien resurssien varaaminen, niin tämä tehdään yleensä raa’alla voimalla (brute force). Hyökkäyksessä voi olla mukana tuhansien agenttien verkko ja sen tavoitteena on estää palvelimen tai palvelun normaali

käyttö. [Cha09]

Riippuen hyökkäyksen kohteen Internet-kaistan leveydestä voi olla että raa'alla voimalla tehty hyökkäys täyttää uhrin koko tietoliikennekapasiteetin. Tällöin mitkään toimenpiteet varsinaisessa kohdejärjestelmässä eivät auta. Jos hyökkäyksen kohde hallinnoi isoa verkkoa, voi olla että jotkin verkkotekniset toimet auttavat hyökkäyksen torjunnassa. Normaalitilanteessa joudutaan kuitenkin turvautumaan Internet-palveluntarjoajan (Internet Service Provider, ISP) apuun. Internet-palveluntarjoaja on luultavasti hyökkäystilanteen jo havainnut, ainakin reititinverkossa, joka on yhteydessä hyökkäyksen kohteen verkkoon. Hyökkäyksen torjunnan tavoitteena on tunnistaa hyökkäysliikenne ja suodattaa se pois. Joskus hyökkäysliikenne on helppo tunnistaa ja joskus vaikeaa tai miltei mahdotonta. [MDD05]

5. Hyökkäystyökaluja

Tässä luvussa esitellään erilaisia yleisesti saatavilla olevia työkaluja, joita voi käyttää erityyppisiin palvelunestohyökkäyksiin. Usein hyökkäyksissä käytetään myös itse tehtyjä ohjelmistoja tai tässä esitellyistä ohjelmista muokattuja versioita.

- Trinoo

  Trinoo käyttää hyväkseen botnet-arkkitehtuuria siten, että hyökkääjä lähettää käskyjä käsittelijöille TCP:llä ja käsittelijät kommunikoivat puolestaan UDP:lla kukin omassa komennossaan olevien agenttien kanssa. Sekä käsittelijät että agentit voi suojata salasanalla, ettei joku toinen hyökkääjä kaappaa niitä. Trinoossa lähetetään UDP-paketteja satunnaisiin portteihin ja hyökkäykseen käytettävän UDP-paketin kokoa pystyy säätämään. Samanaikaisia kohdeosoitteita voi olla useampia ja hyökkäyksen keston voi valita. [MDD05]

- Tribe Flood Network (TFN)

  TFN:ssa hyökkääjä käyttää hyväkseen yhtä käsittelijää, jonka avulla käskytetään kaikkia agentteja. Käskytys tapahtuu komentoriviltä. Hyökkääjä voi ottaa yhteyden käsittelijään lukuisilla eri tavoilla, mm. SSH:lla tai Telnetillä. Kaikki komennot käsittelijältä agenteille lähetetään ICMP Echo Reply –paketeissa. Paketit ovat koodattuja, eivät siis selväkielisiä, mikä vaikeuttaa niiden havaitsemista. TFN2K:n avulla voidaan hyökätä käyttämällä UDP-, TCP SYN- tai ICMP Echo -tulvaa. Myös smurffi-hyökkäys on mahdollinen. Hyökkäys voi kohdistua määrättyihin tai satunnaisiin portteihin uhrikoneessa. [MDD05]

- Tribe Flood Network 2000 (TFN2K)

  TFN2K on parannettu versio Tribe Flood Networkista. Uudet ominaisuudet liittyvät enimmäkseen siihen, että TFN2K-liikenne olisi vaikeampaa havaita ja suodattaa. [MDD05]

- Stacheldraht

  Stacheldrahtissa on Trinoon ja TFT:n ominaisuuksia. Lisäksi TCP-liikenne

hyökkääjän ja käsittelijöiden välillä on salattua. Käsittelijöiden ja agenttien välinen liikennöinti tapahtuu TCP:llä tai ICMP:llä. Toinen lisäominaisuus on kyky päivittää automaattisesti agenteissa olevaa hyökkäysohjelmistoa. Tuetut hyökkäystyypit ovat samat kuin TFN:ssä. [MDD05]

- Shaft

  Shaftissa on Trinoon, TFT:n ja Stacheldrahtin ominaisuuksia. Shaft pystyy myös vaihtamaan lennossa käsittelijän ja agentin käyttämiä tietoliikenneportteja, mikä vaikeuttaa sen havaitsemista tunkeutumisenestojärjestelmien (Intrusion Detection System, IDS) avulla. Liikennöinti käsittelijöiden ja agenttien välillä tapahtuu UDP:lla. Hyökkääjä kontrolloi käsittelijöitä tavallisten Telnet-istuntojen avulla. [MDD05]

  Shaft käyttää erikoista tiketöintijärjestelmää. Jokainen komento, minkä käsittelijä lähettää agentille, sisältää salasanan ja tiketin. Salasana on suojattu yksinkertaisella Caesar-salauksella. Sekä salasanan että tiketin numeron pitää olla oikein, jotta agentti suorittaisi halutun komennon. [MDD05]

  Shaftissa on myös erityisiä tilastointiominaisuuksia. Käsittelijät voivat lähettää agenteille komennon, millä kerätään tilastotietoa jokaisen agentin generoimasta hyökkäysliikenteestä. Näin saadaan tietoa agenttiverkon ja hyökkäyksen tehokkuudesta. [MDD05]

  Agentit voivat generoida UDP-, TCP SYN- tai ICMP-tulvaa, ja myös yhtä aikaa näitä kaikkia. Tulvitus tapahtuu sadan IP-paketin purskeissa per agentti. IP-pakettien lukumäärä ei ole parametri, vaan se on kovakoodattu työkaluun. Lähdeportti ja -osoite ovat satunnaisia. [MDD05]

- HTTP-palvelimiin kohdistettu palvelunestohyökkäystyökalu ja rajoituskeinot

  Viestintävirastossa toimiva kansallinen tietoturvaviranomainen CERT-FI uutisoi yo. otsikolla uudesta palvelunestohyökkäystyökalusta 23.6.2009. Työkalu vaikuttaa haitallisimmin Apache 1.x, Apache 2.x, dhttpd, GoAhead WebServer -HTTP-palvelimiin ja Squid HTTP-välityspalvelimeen niiden ollessa oletuskonfiguraatiossaan. [Cer05]

  Työkalu toimii lähettämällä HTTP-palvelimille vaillinaisia HTTP GET tai HTTP POST -viestejä, jolloin HTTP-yhteys jää avoimeksi ja palvelin jää varaamaan resursseja yhteyden ylläpitämiseksi. Joidenkin palvelimien oletusasetuksissa resurssit varataan minuuttien ajaksi, jolloin palvelunestotila saadaan aikaan suhteellisen pienellä määrällä HTTP-pyyntöjä. [Cer05]

  CERT-FI:n sivulla on myös linkki ISC SANS:n blogiartikkeliin, jossa otsikolla Apache HTTP DoS tool mitigation mainitaan kaksi rajoituskeinoa työkalua vastaan, kun kyseessä on Apache HTTP –palvelin: TimeOut-direktiivin pienentäminen ja yhdestä IP-osoitteesta samanaikaisesti luotujen yhteyksien määrän rajoittaminen. [Cer05]

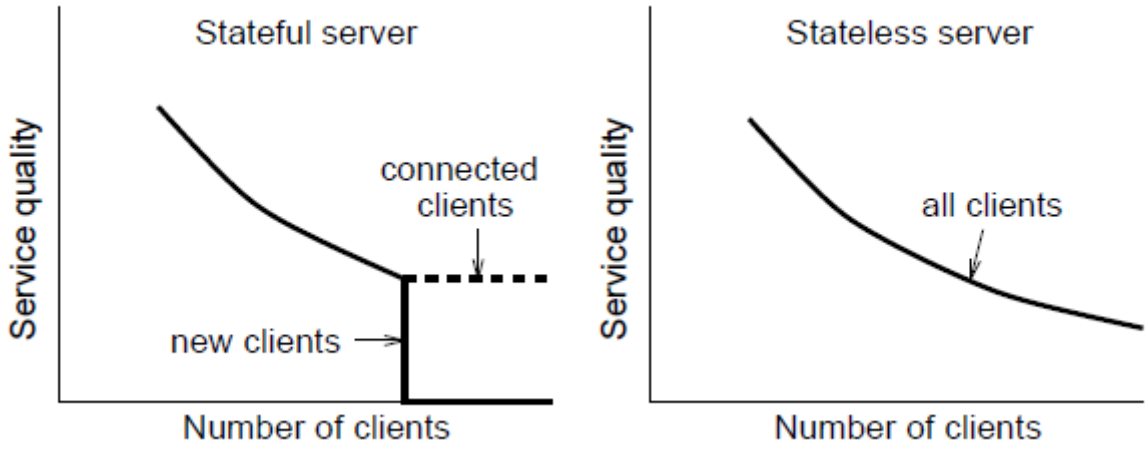
6. Teoreettisia protokollatason parannusehdotuksia

Tässä luvussa tarkastellaan kolmea erilaista protokollatason parannusta, joilla pyritään estämään palvelunestohyökkäyksiä tai lieventämään niiden vaikutuksia.

6.1. Tilattomat yhteydet

Tilatietoisen palvelimen heikkous on se, että se pystyy käsittelemään vain rajallisen määrän yhtäaikaisia yhteydenottoja. Tämä raja voi ylittyä paitsi palvelunestohyökkäyksen myös normaalin ruuhkahuipun aikana.

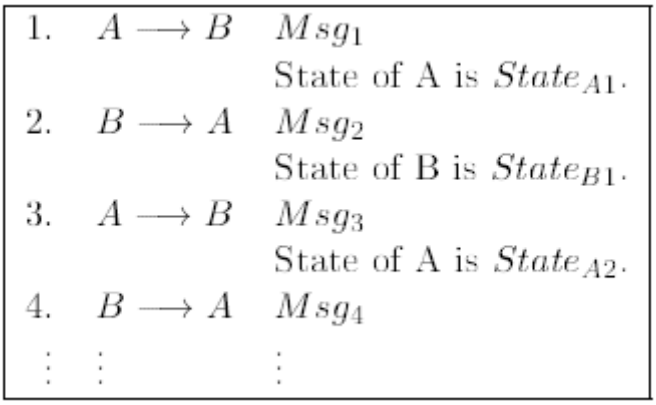
Aura ja Nikander [AuN97] ovat ehdottaneet tilattomia yhteyksiä (stateless connection) vastalääkkeeksi resursseja varaavaa palvelunestohyökkäystä vastaan. Päinvastoin kuin tilatietoinen protokolla tilaton yhteysprotokolla on immuuni hyökkäyksille, jotka jättävät yhteyden muodostamisen puoliavoimeen tilaan. Tilaton palvelin reagoi kasvavaan kuormaan laskemalla hitaasti palvelutasoa, kun taas tilatietoiselle palvelimelle on tyypillistä palvelutason yhtäkkinen romahdus kuorman ylittäessä tietyn rajan. Tämä käy ilmi kuvasta 6, jossa vertaillaan tilatietoisen ja tilattoman palvelimen palvelulaatua (QoS, Quality of Servise) asiakasmäärien kasvaessa. Tilaton palvelin myös toipuu nopeammin palvelunestohyökkäyksestä.



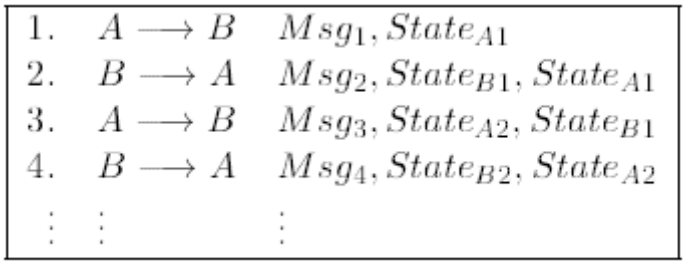
KUVA 6: Tilatietoisen ja tilattoman palvelimen palvelulaadun kehitys asiakasmäärien kasvaessa.

Tilaton palvelin ei pidä yhteyden tilatietoa muistissaan, vaan lähettää sen asiakkaalle. Asiakas palauttaa tilatiedon seuraavan pyyntönsä yhteydessä. Näin asiakas pystyy ylläpitämään yhteyttä tilattoman palvelimen kanssa. Tilatiedon edestakainen lähetys vaatii luonnollisesti jonkun verran lisätietoliikennekaistaa.

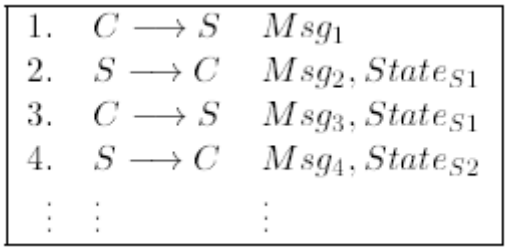
Kuvassa 7 esitetään kahden osapuolen tilatietoinen protokolla ja kuvassa 8 vastaava tilaton protokolla. Kuvassa 9 esitetään tilaton palveluprotokolla.



KUVA 7: Kahden osapuolen, A ja B, tilatietoinen protokolla. Yhteyden osapuolet pitävät tilatiedon muistissaan.



KUVA 8: Kahden osapuolen, A ja B, tilaton protokolla. Yhteyden osapuolet eivät pidä tilatietoa muistissaan. Yhteyden osapuoli palauttaa vastapuolen tilatiedon oman pyyntönsä yhteydessä, mikä mahdollistaa yhteyden ylläpidon.



KUVA 9: Tilaton palveluprotokolla. C = asiakas, S = palvelin. Vain palvelin on tilaton.

Tilatiedon eheys ja luottamuksellisuus voidaan taata symmetrisellä salauksella. Tilatietopaketit sisältävät viestin todennuskoodin, joka voidaan laskea vain palvelimen tietämällä salaisella avaimella. Sessioavaimet ja muu luottamuksellinen tilatieto kryptataan niin ikään salaisella avaimella. Myös yhteysdata voidaan suojata ja liittää oikeisiin tilatietopaketteihin.

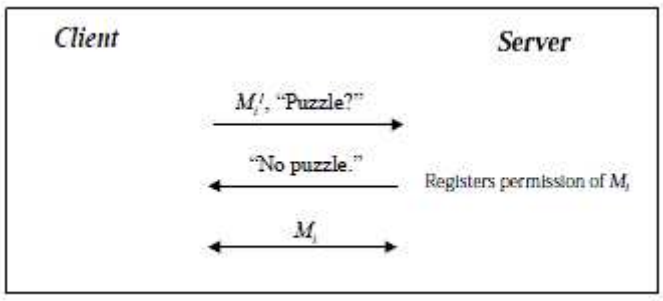
Aura ja Nikander ehdottavat todentamisen suunnitteluperiaatteeksi sitä, että yhteyden pitäisi olla aina tilaton, kunnes asiakas on tunnistettu tai hänen on jollain muulla tavoin todettu olevan aikeissa käyttää palvelua asiallisesti. Asiakkaan todentamisen jälkeen palvelin voi muuttaa yhteyden tilatietoiseksi.

Koska vastaanottajalla ei ole tilatietoa aikaisemmista viesteistä, tilaton yhteys saattaa mahdollistaa uuden hyökkäystekniikan. Siinä yhteydenottaja lähettää saman tilan sisältävää viestiä yhä uudelleen ja uudelleen. Tämä voi kuluttaa palvelimen kapasiteettia, mutta legitiimien asiakkaiden yhteydet kuitenkin säilyvät. Tämä on huomattava ero verrattuna tilatietoiseen protokollaan, missä palvelunestohyökkäystilanteessa nimenomaan legitiimit asiakkaat kärsivät.

6.2. Asiakasarvoitus

Juels ja Brainard [JuB99] ovat esittäneet asiakasarvoitusprotokollaa (client puzzle protocol) vastalääkkeeksi resursseja varaavaa palvelunestohyökkäystä, esimerkiksi TCP SYN – tulvitusta vastaan. Protokolla sopii erityisesti tilanteisiin, joissa hyökkääjä pystyy lähettämään yhteyspyyntöjä nopeassa tahdissa tai kun hyökkääjä käyttää resurssi-intensiivistä yhteysprotokollaa kuten SSL. Asiakasarvoitusprotokollan periaate on esitetty kahdessa seuraavassa kuvassa.

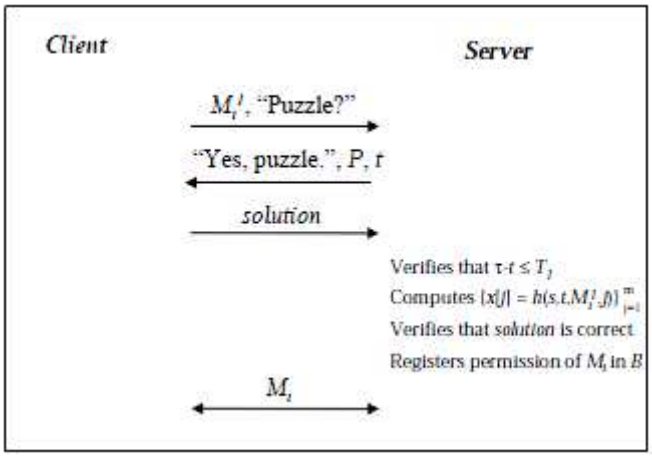
Kuvassa 10 asiakas ehdottaa palvelimelle protokolla M:n käyttöönottoa ja samalla kysyy tarjoaako palvelin asiakasarvoitusta. Koska palvelin ei ole palvelunestohyökkäyksen kohteena, se ilmoittaa asiakkaalle, että se ei lähetä asiakasarvoitusta ja samalla rekisteröi aloituksen (initiation) M_i. Asiakas ja palvelin aloittavat liikennöinnin protokollalla M.



KUVA 10: Asiakasarvoitusprotokolla normaalitilanteessa

Kuvassa 11 palvelin on palvelunestohyökkäyksen kohteena, minkä johdosta se lähettää

asiakkaalle arvoituksen (Puzzle, P) ja aikaleiman (timestamp, t). Kun asiakas lähettää arvoituksen ratkaisun (solution), palvelin tarkastaa ensin että vastaus on tullut ajoissa ($\tau - t \leq T_1$, T_1 = vastaukselle varattu aika, τ = nykyinen aika, t = aikaleima) ja sitten että ratkaisu on oikein. Väärä ratkaisu luonnollisesti torjuttaisiin. Palvelin rekisteröi aloituksen M_i palvelimen muistiin B. Huomioitava seikka on, että palvelimen tulee varmistaa jollain mekanismilla, ettei hyökkääjä käytä samaa ongelman ratkaisua useamman aloituksen M_i rekisteröimiseen.



KUVA 11: Asiakasarvoitusprotokolla, kun palvelin on palvelunestohyökkäyksen kohteena

6.3. Formaali kehikko ja arviointimenetelmä palvelunestohyökkäykselle

Meadows [Mea99] ehdottaa lääkkeeksi resursseja varaavaa palvelunestohyökkäystä vastaan sitä, että protokollan jokainen viesti tulisi todentaa. Kuitenkin siten, että laskentakapasiteetin säästämiseksi todennus voisi olla protokollan alussa heikompi ja vahventua jatkossa. Palvelimen muodostama eväste, mikä asiakkaan pitää palauttaa, on esimerkki heikosta todennuksesta, mikä voisi aloittaa yhteyden.

Meadowsin formaali kehikko ja palvelunestohyökkäyksen arviointimenetelmä perustuu Gongin ja Syversonin konseptiin fail-stop-protokollista. Fail-stop-protokolla on sellainen, minkä suoritus lopetetaan heti, kun väärä tai epäilyttävä viesti havaitaan. [GoS98]

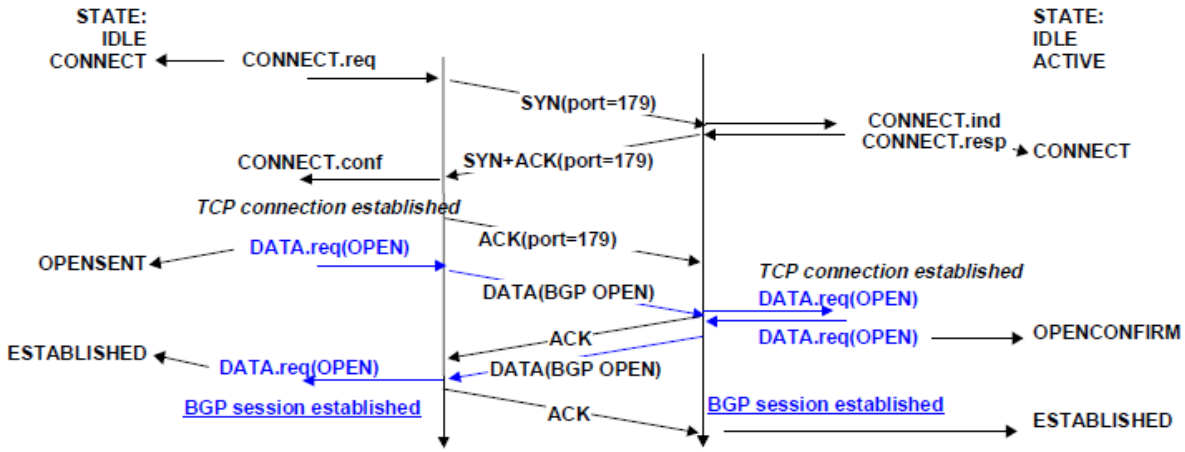
7. Vastatoimia

Tässä luvussa käsitellään erilaisia toimia, joilla palvelunestohyökkäyksiä voidaan estää tai niiden vaikutuksia lieventää. Ensin käsitellään palvelunestohyökkäyksen tyrehdyttämistä BGP:n avulla ja sitten muita käytännöllisiä vastatoimia lähinnä ACM:ssä ja IEEE:ssä olevien artikkelien pohjalta.

7.1. Palvelunestohyökkäyksen tyrehdyttäminen BGP:n avulla

Autonomisten järjestelmien (Autonomous Systems, AS) väliseen reititykseen tarkoitettu BGP on Internetin tärkein reititysprotokolla. BGP on ulkoinen reititysprotokolla, joka ei välitä tietoa autonomisten järjestelmien sisäisestä rakenteesta keventäen näin reititysprosessia eri autonomisten järjestelmien välillä. BGP mahdollistaa erilaisten poliitikoiden käyttämisen paikallisen verkon (autonominen järjestelmä) reuna-alueilla. BGP-reitittimet vaihtavat reititystietoa keskenään sanomien avulla. Tärkeimmät sanomat ovat UPDATE, joka välittää tiedot uusista verkoista, jotka ovat saavutettavissa kyseisen naapurin kautta, ja WITHDRAW, joka poistaa verkot, jotka eivät enää ole saavutettavissa. [MIT09]

Kuvassa 12 on esitetty BGP-session muodostaminen reititysinformaation siirtoa varten. [TKK06]



KUVA 12: BGP-session muodostaminen sovellusporttia 179 hyödyntäen.

Varsinkin Suomessa on usein tilanne, jossa halutut www-palvelun käyttäjät ovat pääasiassa suomalaisia, mutta palvelunestohyökkäyksen lähde on kuitenkin ulkomailla. BGP:tä voidaan tällöin käyttää ulkomaan liikenteen estämiseen seuraavasti:

a) Internet-palveluntarjoaja (ISP, Internet Service Provider) merkitsee kotimaan AS-verkkojen reititysmainostuksensa tagilla 41808:32921.
b) Www-palvelun tuottajan reitittimellä otetaan vastaan vain ao. tagilla mainostuvat reitit. Reititys muihin verkkoihin tapahtuu default-reitin mukaan.
c) Kun ulkomaanliikenne halutaan estää, poistetaan www-palvelun tuottajan reitittimeltä default-reitti, jolloin lähtevät ip-paketit eivät enää löydä perille muihin kuin kotimaisiin verkkoihin.
d) Asetetaan Internet-palveluntarjoajan suuntaan mainostuvalle www-palvelun tuottajan osoitealueelle tietty tag, jolloin kyseinen osoitealue ei mainostu enää maailmalle Internet-palveluntarjoajan kautta, eivätkä ip-paketit löydä enää perille www-palveluun muualta kuin kotimaasta

Edellä mainittu edellyttää, että www-palvelun tuottaja hallinnoi myös BGP-reitittimiä, mikä rajaa tämän puolustautumiskeinon suhteellisen suuriin organisaatioihin.

Voidaan myös sopia ISP:n kanssa, että he estävät www-palvelun tuottajan verkkoon tulevan ulkomaanliikenteen jo oman verkkonsa reunalla. Kotimainen Internet-palveluntarjoaja pystyy helpommin erottamaan kotimaan ja ulkomaan liikenteen toisistaan kuin monikansallinen Internet-palveluntarjoaja.

Ulkomaisen liikenteen estäminen ei toimi sataprosenttisesti. On suomalaisia käyttäjiä, joilla on esim. amerikkalaisen yrityksen amerikkalainen ip-osoite työnsä puolesta. Suomessa on myös Internet-palveluntarjoajia, joilla on käytössään, ainakin osittain, ruotsalaisia ip-avaruuksia. Lisäksi esim. ulkomailla eri syistä olevat suomalaiset eivät pääse www-palveluun, kun ulkomaan liikenne estetään.

7.2. Muita käytännöllisiä vastatoimia

Tässä luvussa käsitellään muita käytännöllisiä vastatoimia lähinnä ACM:ssä ja IEEE:ssä olevien artikkelien pohjalta.

Yhteysmäärän rajoittaminen ja yhteyksien vanheneminen

Ei-hajautetun palvelunestohyökkäyksen voi estää rajoittamalla yhdestä ip-osoitteesta tulevien yhteyksien määrää. Tämä vastatoimi on tehokas hajautetussa palvelunestohyökkäyksessäkin, jos hyökkäysliikennettä tulee kohtuullisen rajatusta määrästä ip-osoitteita. Jos hyökkäys on tarpeeksi hajautettu, yhdestä lähteestä tulevien yhteyksien määrän rajoittaminen ei toimi. Se ei toimi myöskään, vaikka hyökkääjiä olisi vain yksi, jos tämä väärentää ip-osoitteensa ja vaihtaa sitä hyökkäyskoodissa jatkuvasti.

Myös suurten operaattorien välityspalvelimet (www-proxy) ovat ongelmallisia, jos yhdestä osoitteesta tulevia yhteysmääriä rajoitetaan. Välityspalvelimien takaa tulee paljon yhteyksiä ja lähdeosoitteena on tällöin välityspalvelimen ip-osoite. Toisin sanoen suurella joukolla käyttäjiä on sama lähdeosoite. Voisi tietysti ajatella, että suurten operaattorien välityspalvelimet sijoitetaan sallittujen listalle (white list), jolloin niistä tuleva liikenne pääsee ilman tarkistuksia läpi. Mutta entä jos hyökkäys tuleekin oikeasti välityspalvelimien takaa, tai jos hyökkääjä väärentää lähdeosoitteensa välityspalvelimen ip-osoitteeksi?

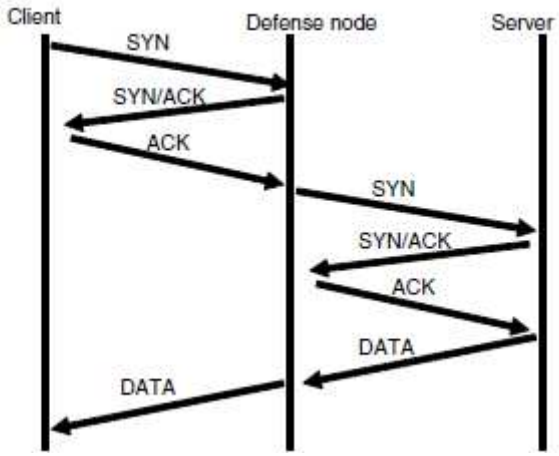
Perustavaa laatua oleva suojautumiskeino palvelunestohyökkäystä vastaan on myös käyttämättömien (idle) yhteyksien aikakatkaisu säädettävän session TTL (Time-To-Live) –arvon perusteella. Kyseisen arvon pienentäminen voi auttaa hyökkäystilanteessa.

SYN-välityspalvelin

Ohsita, Ata ja Murata ovat esitelleet TCP SYN –tulvitusta vastaan hajautetun

puolustusmekanismin, joka käyttää eräänlaista kerrosverkkotekniikkaa (overlay network). Siinä puolustussolmut on sijoitettu suojauksen kohteena olevan verkon reunalle. Kukin puolustussolmu on yhteydessä yhteen tai useampaan toiseen puolustussolmuun siten, että ne muodostavat keskenään verkon.

Tunnistaakseen lailliset SYN-paketit puolustussolmut toimivat SYN-välityspalvelimina (SYN proxy) palauttaen SYN ACK –paketin kohdepalvelimen asemesta. Vasta kun puolustussolmu vastaanottaa ACK-paketin vastauksena lähettämäänsä SYN ACK –pakettiin, SYN-paketti välitetään kohdepalvelimelle, joka lähettää dataa asiakkaalle (kuva 13). [OAM05]



KUVA 13: Puolustussolmun toimiminen SYN-välityspalvelimena.

Puolustussolmu tutkii SYN- ja ACK-paketeista yhteyskäytännön (protocol), lähde- ja kohde-ip-osoitteen sekä tietoliikenneportin. Kun nämä ovat samat, kyse on laillisesta liikenteestä, joka välitetään kohdepalvelimelle. [OAM05]

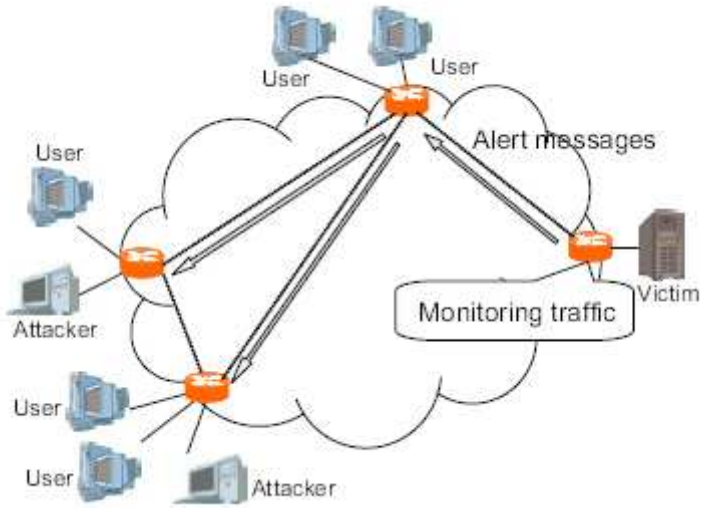
Jotta puolustuksesta ei tulisi pullonkaulaa suorituskyvylle, on tarpeen tunnistaa vain ne ip-paketit, mitkä ovat menossa hyökkäyksen kohteena olevaan palveluun. Tämän takia puolustusmekanismi on jaettu kahteen vaiheeseen [OAM05]:

- hyökkäyksen havaitsemisvaihe (kuva 14)
- puolustusvaihe (kuva 15)

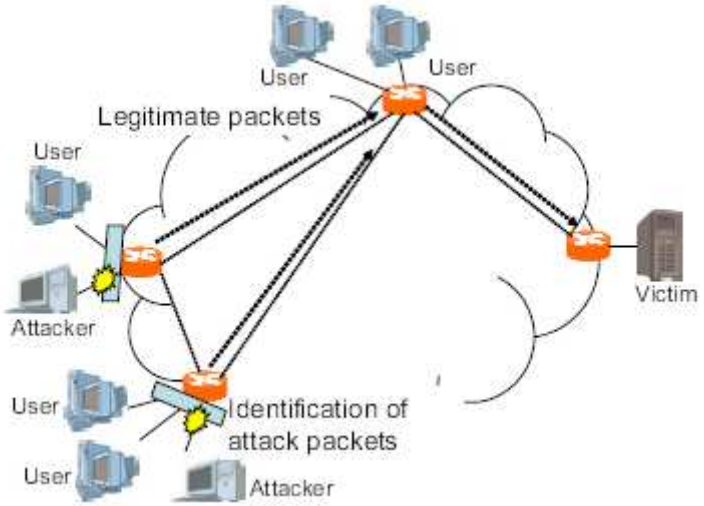
Hyökkäyksen havaitsemisvaiheessa puolustussolmut (merkitty kuvissa punaisella) monitoroivat suojauksen kohteena olevasta verkosta ulospäin tulevia ip-paketteja ja tarkastavat samalla onko saapuva liikenne hyökkäysliikennettä vai ei. Jos puolustussolmu havaitsee hyökkäysliikennettä, se lähettää varoituksena hyökkäyksen kohteena olevan ip-osoitteen siihen yhteydessä oleville toisille puolustussolmuille, jotka lähettävät tiedon edelleen.

Kun puolustussolmu vastaanottaa hyökkäyksen kohteena olevan ip-osoitteen, se siirtyy

puolustusvaiheeseen koskien kyseiseen ip-osoitteeseen menevää liikennettä. Puolustusvaiheessa puolustussolmut toimivat hyökkäyksen kohteena olevan ip-osoitteen SYN-välityspalvelimina tunnistaen laillisen liikenteen ja estäen hyökkäysliikenteen. Puolustusvaihe kestää kunnes hyökkäys on ohi.

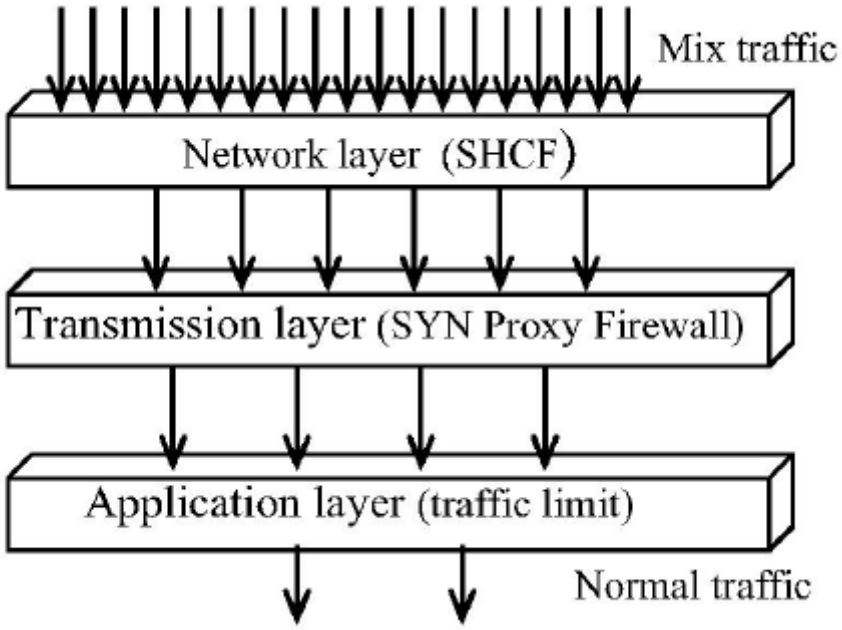


KUVA 14: Hyökkäyksen havaitsemisvaihe - TCP SYN –hyökkäyksestä varoittaminen kerrosverkossa



KUVA 15: Puolustusvaihe - laillisen liikenteen läpi päästäminen ja haittaliikenteen estäminen

Zhijun ja Zhifeng ovat esitelleet oman ehdotuksensa kolmikerrospuolustusmekanismiksi palvelunestohyökkäyksiä vastaan. Perusideana on suojella laillista liikennettä suuren hyökkäysliikennemassan seassa (kuva 16). [ZhZ06]



KUVA 16: Kolmikerrospuolustusmekanismi palvelunestohyökkäyksiä vastaan.

Ensimmäisessä puolustustasossa eli verkkokerroksessa SHCF-algoritmilla (Simplified Hop Count Filtering) pyritään estämään väärennetyn ip-osoitteen käyttö. Algoritmin teho perustuu siihen, että suurimmassa osassa ip-paketeista, joissa on väärennetty lähdeosoite, hop count –arvo ei vastaa kyseistä ip-osoitetta.

Toisessa puolustustasossa eli kuljetuskerroksessa (transmission layer) on SYN-välityspalvelin, joka toimii palomuurina päästäen vain validit SYN-paketit eteenpäin.

Jos hyökkääjät toimivat oikeilla ip-osoitteillaan, kolmannen puolustustason sovelluskerroksessa pystytään rajoittamaan kuinka paljon liikennettä tietystä ip-osoitteesta voi lähettää per aikayksikkö. Jos määrä ylittyy, asiakkaan katsotaan olevan hyökkääjä. [ZhZ06]

Tietoliikenteen poikkeavuuksien havaitseminen

Sekä Silveira ja Diot että Kim ja Reddy ovat kehitelleet tilastollisia menetelmiä, joilla voidaan tunnistaa verkkoliikenteen poikkeavuuksia. Silveiran ja Diotin menetelmä perustuu

aikasarjojen käyttöön, kun taas Kim ja Reddy tutkivat ip-pakettien otsikkotietoja (packet header data) etsiessään poikkeavuuksia. Kim ja Reddy etsivät siis protokolla-anomaliaa. Molemmat menetelmät perustuvat siihen, että ensin liikennettä tutkitaan riittävä ajanjakso, jotta voidaan määritellä ns. normaaliliikenne (baseline). Kun liikennevirrassa tämän jälkeen havaitaan poikkeavuuksia, niin nämä poikkeavuudet voivat olla merkkejä palvelunestohyökkäyksestä. [KiR08] [SiD07]

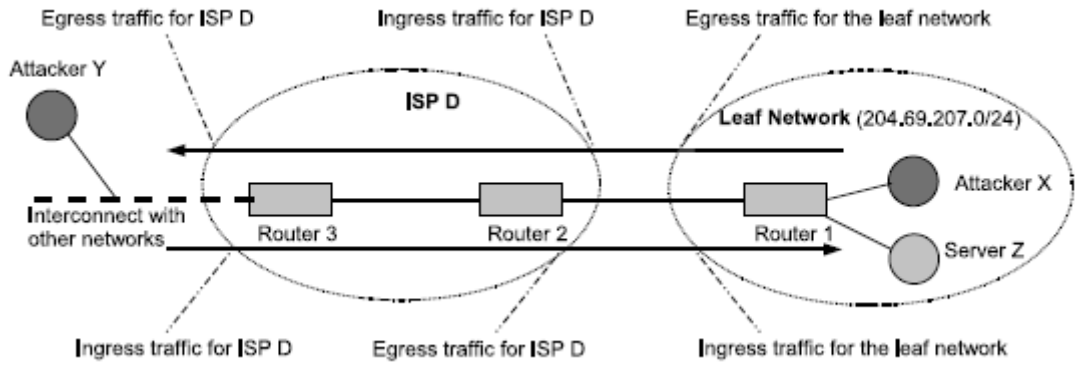
Tavallinen tilanne on, että palvelunestohyökkäys havaitaan vasta, kun kohteena olevan palvelun palvelutaso alkaa laskea. Tilastolliset menetelmät voivat auttaa havaitsemaan palvelunestohyökkäyksen jo aikaisemmin, mikä on tehokkaan torjunnan kannalta tärkeää.

Schuhmann ja Volker ovat tutkineet reititysprotokollan poikkeavuuksia. Poikkeavuus viestin järjestysnumerossa (Sequence Number Anomalies, SNA) merkitsee usein sitä, että lähettäjän ip-osoite on väärennetty. Kun on vastaanotettu vähintään kaksi ip-pakettia, joissa on sama lähettäjäosoite, voidaan havaita seuraavia poikkeavuuksia [ScV08]:

- Viestin järjestysnumero kasvaa liian nopeasti
- Viestin järjestysnumero pienenee
- Kahdella erisisältöisellä viestillä on sama järjestysnumero
- Vastaanotetaan viesti, jossa lähettäjäosoitteena on oma ip-osoite, mutta järjestysnumero on liian korkea.

Kaistanhallinta

Kuvassa 17 esitetään tyypillinen organisaation verkkomalli. Organisaatiolla (Leaf Network) on yhteys Internet-palveluntarjoajaan (ISP D), jota kautta on yhteys maailmalle. Kuvaan on merkitty myös eri verkkojen sisääntulo- ja ulosmenoliikenteen (ingress/egress) suodatuspisteet. Koska yhden verkon ulosmenoliikenne on toisen verkon sisääntuloliikennettä, on termejä käytettäessä oltava tarkkaan selvillä, missä on referenssipiste. [PLR07]



KUVA 17: Sisääntulo- ja ulosmenoliikenteen suodatuspisteet tyypillisessä verkkomallissa.

Jos sisääntulo- ja ulosmenopisteissä tehdään esim. liikennemääriin perustuvaa suodatusta, ja liikennemäärät vaihtelevat esim. viikonpäivän tai vuorokauden ajan mukaan, on syytä käyttää mukautuvaa kynnysarvoa (adaptive threshold). [DPV06]

Kiinteällä kynnysarvolla (fixed threshold) rajoitetaan esimerkiksi yhdestä ip-osoitteesta tulevien yhteyksien määrää. [ZhZ06]

Porttiskannauksen esto

Ennen palvelunestohyökkäystä hyökkääjä haluaa usein tutustua paremmin tulevaan kohteeseen. Eräs työkalu, jota hyökkääjä voi käyttää, on Nessus.

Nessus on haavoittuvuusskanneri, jolla voi mm.

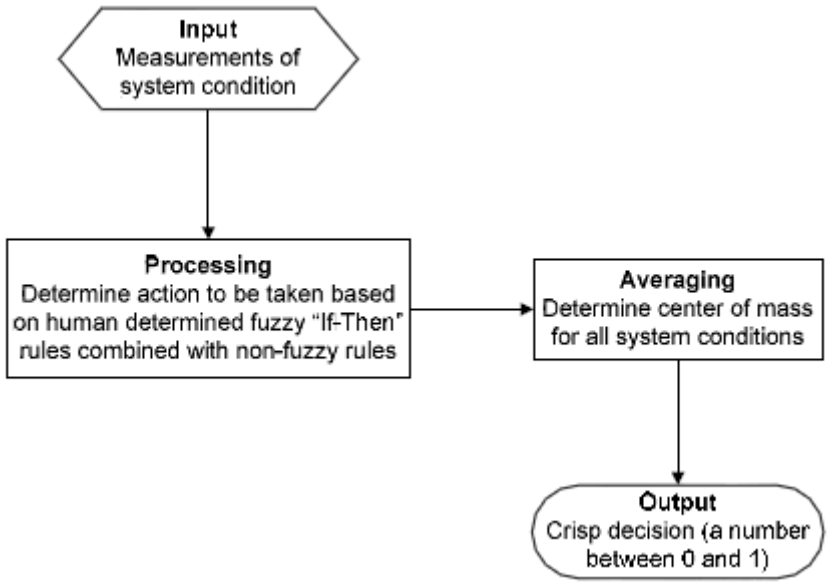
- selvittää kohdejärjestelmän auki olevat tietoliikenneportit (porttiskannaus)
- tehdä haavoittuvuusskannauksen
- tarkistaa Windowsin ja useimpien Unix-järjestelmien softatasot ja konfiguroinnin
- tehdä web-sovelluksen haavoittuvuustestauksen
- tarkistaa SQL-tietokannan ja Ciscon reitittimen konfiguroinnin
- luetteloida käytössä olevat ohjelmistot Windowsissa ja Unix-järjestelmissä
- saada tietoa antivirus-asennuksen tilasta

Koska hyökkääjä todennäköisesti joutuu käyttämään Nessusta julkisesta verkosta, jolloin mm. palomuuri suojaa kohdejärjestelmää, Nessus saa selville vain osajoukon edellä olevan listan asioista, mutta joka tapauksessa kyseessä on tehokas työkalu. [Nes01]

Huomattakoon, että Suomen oikeuskäytännössä porttiskannaus tulkitaan tietomurron yritykseksi, mikä on rangaistava teko. [Lex01]

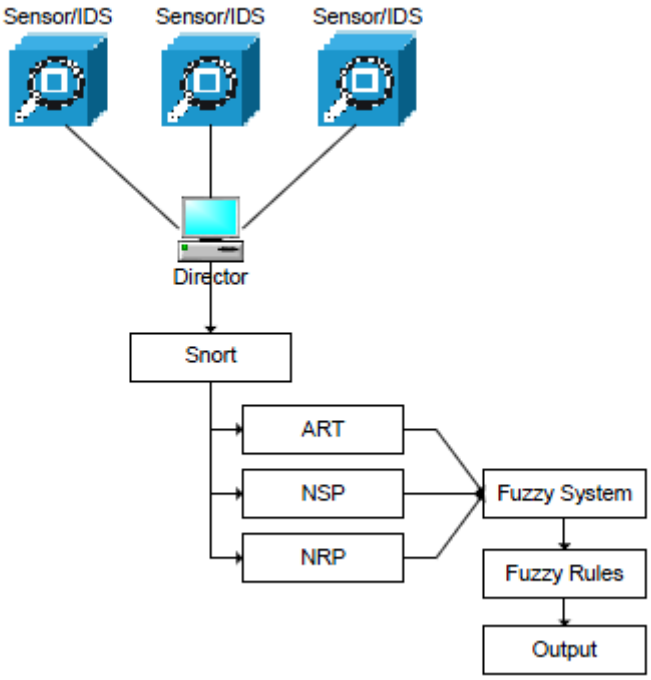
Snort on avoimen koodin verkkotunkeutumisen havaitsemis- ja estämistyökalu (Intrusion Detection/Prevention System, IDS/IPS), jolla pystyy havaitsemaan mm. Nessuksen käytön. Snort havaitsee hyökkäyksiä sekä valmiiden sääntöjen pohjalta (signature) että etsien poikkeavuuksia (anomalies) tietoliikennevirrasta. [Sno01]

El-Hajj, Aloul, Trabelsi ja Zaki ovat edelleen kehittäneet avoimen koodin Snort-ohjelmistoa lisäämällä siihen sumeaa logiikkaa. Kehittäjien mukaan tunkeutumisen havaitsemisessa, missä pitää yhdistää ja analysoida erilaisia tietoliikenneparametreja, on nimenomaan hyötyä sumeasta logiikasta. Sumea logiikka vähentää sekä vääriä negatiivisia että vääriä positiivisia hälytyksiä. Kuvassa 18 on sumean logiikan ohjain (controller), jonka avulla saadaan tietty täsmällinen johtopäätös ja ratkaisu, joka perustuu epäselvään, epämääräiseen tai osittain puuttuvaan syötteeseen. [EAT08]



KUVA 18: Sumean logiikan ohjain ja sen komponentit. Syötteen ja lopputuloksen välissä on prosessointia sumeiden ja ei-sumeiden sääntöjen avulla ja keskimääräistämistä.

Kuvassa 19 näkyy miten kehittäjät ovat yhdistäneet sumean logiikan ohjaimen ja Snortin. FB-Snortissa (Fuzzy-Based Snort) Snortin Directorin alaisuudessa toimivat IDS-sensorit toimivat syötteinä. Sumean logiikan ohjaimelle syötetään kolme Snortin parametria: ART, NSP ja NRP. ART tarkoittaa keskimääräistä aikaa kohteen vastaanottamien ip-pakettien välillä., NSP-parametri on lähteen lähettämien ip-pakettien lukumäärä ja NRP tarkoittaa kohteen vastaanottamien ip-pakettien lukumäärää. Edellä mainitut parametrit syötetään sumean logiikan ohjaimelle ja lopputuloksena saadaan nollan ja ykkösen välillä oleva hyökkäystaso. Jos hyökkäystaso on 0, tarkoittaa se sitä, että mitään palvelunestohyökkäykseen viittaavaa ei ole havaittu, kun taas 1 tarkoittaa varmaa palvelunestohyökkäystä. [EAT08]



KUVA 19: FB-Snort-arkkitehtuuri

Botnet-esto

Palvelunestohyökkäyksen mahdollisimman aikainen havaitseminen on ensiarvoisen tärkeää tehokkaan suojautumisen kannalta. Jos botnetin tuottama tietoliikenne pystyttäisiin tunnistamaan, tämä olisi hyvä keino havaita hyökkäys aikaisessa vaiheessa. Feily, Shahrestani ja Ramadass ovat tutkineet botnet-liikenteen havaitsemista.

Kuvassa 20 on esitetty tyypillisen botnet-verkon elinkaari [FSR09]:

- Alustava tartunta

  Hyökkääjä kartoittaa (scan) kohdealiverkkoa ja tartuttaa uhrikoneet, joista löytyy haavoittuvuuksia, erilaisilla hyväksikäyttömenetelmillä

- Toissijainen tartunta

  Tartunnan saaneet uhrikoneet suorittavat shell-code –skriptin, joka noutaa ftp:llä, http:llä tai jollain vertaisverkkoprotokollalla varsinaisen agenttibinäärikoodin. Binäärikoodi asentaa itsensä ja uhrikoneesta tulee agentti, joka pystyy osallistumaan hajautettuun palvelunestohyökkäykseen. Agenttiohjelma käynnistyy automaattisesti aina kun uhrikonekin käynnistetään.

- Yhteysvaihe

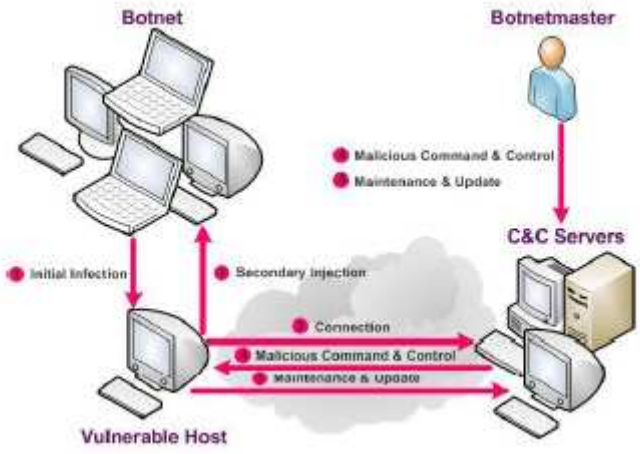
  Agenttiohjelma luo komento- ja kontrollikanavan sekä yhdistää uhrikoneen komento- ja kontrollipalvelimelle. Uhrikoneesta on tullut osa hyökkääjän botnettiä.

- Vahingolliset komennot ja kontrolli

  Hyökkääjä käyttää komento- ja kontrollikanavaa komentojen lähettämiseen botnetin agenteille. Uhrikoneiden agenttiohjelmat suorittavat hyökkääjän lähettämät komennot. Hyökkääjä pystyy kontrolloimaan komento- ja kontrollikanavan avulla suurta joukkoa agentteja, jotka voivat hajautetun palvelunestohyökkäyksen lisäksi suorittaa muitakin laittomia toimia, esimerkiksi lähettää roskapostia.

- Ylläpito ja päivitys

  Elinkaaren viimeisessä vaiheessa hyökkäysverkkoa ja sen agentteja ylläpidetään ja päivitetään. Agenttibinäärikoodin päivityksille voi olla useita syitä, esimerkiksi uuden botnetin havaitsemistekniikan väistäminen tai uusien hyökkäysominaisuuksien lisääminen agentteihin. Joskus koodin päivitys liittyy palvelinmigraatioon, toisin sanoen agentit siirretään toisen komento- ja kontrollipalvelimen alaisuuteen, minkä tarkoituksena on hankaloittaa botnetin löytymistä. Dynaamisen nimipalvelun (Dynamic DNS, DDNS) avulla komento- ja kontrollipalvelinta voidaan vaihtaa lennossa. Tällöin agenttikoodissa viitataan tiettyyn isäntänimeen (host name), ja dynaamisen nimipalvelun avulla vastaava ip-osoite ja samalla komento- ja kontrollipalvelin saadaan vaihdettua hetkessä. Uusi komento- ja kontrollipalvelin voi olla vaikka eri mantereella kuin vanha.



KUVA 20: Tyypillisen botnet-verkon elinkaari.

Botnetin havaitsemisessa ja jäljittämisessä on kaksi lähestymistapaa. Ensimmäinen on hunajaverkon (honeynet) pystyttäminen. Siinä annetaan haavoittuvuuksia sisältävien koneiden joutua osaksi botnetiä, jolloin päästään tutkimaan botnetin toimintaa ja ominaisuuksia. Jos halutaan tietää, onko oma järjestelmä botnetin kohteena, tulee käyttää toista lähestymistapaa; passiivista liikenteen monitorointia ja analysointia. Botnetin havaitseminen passiivisen liikenteen monitoroinnin ja analysoinnin avulla jaetaan neljään

luokkaan [FSR09]:

- Sääntöpohjainen havaitseminen

  Sääntöpohjaisesti voidaan tunnistaa jo tunnettuja hyökkäysverkkotyyppejä, mutta uusien botnettien havaitseminen ei onnistu. Suurin osa IDS-ohjelmistoista toimii sääntöpohjaisesti, jolloin problematiikka on samankaltaista kuin virustorjunnalla ns. nollapäivävirusten eli uusien ja tuntemattomien virusten suhteen.

- Poikkeavuuteen perustuva havaitseminen

  Poikkeavuuteen perustuvassa havaitsemisessa tutkitaan mm. verkkoviivettä, liikennemäärien äkillistä kasvua, liikennettä epätavallisiin tietoliikenneportteihin tai ylipäätään tietoliikenteellisiä poikkeavuuksia normaalitilanteeseen (baseline) nähden.

- Nimipalveluun (DNS) perustuva havaitseminen

  Nimipalveluun perustuva botnetin havaitseminen on myös poikkeavuuteen perustuvaa havaitsemista siinä mielessä, että siinä tutkitaan botnetin aiheuttamia poikkeavia nimipalvelukyselyitä. Kuten aikaisemmin todettiin, komento- ja kontrollipalvelimia suojataan usein dynaamisen nimipalvelun avulla. Tähän liittyen agenttien tekemiä nimipalvelukyselyjä voidaan jäljittää.

- Tiedon louhintaan (mining) perustuva havaitseminen

  Komento- ja kontrollipalvelimen tietoliikenne on hyvä tapa botnetin tunnistamiseen. Toisaalta komento- ja kontrollipalvelimen tietoliikennettä on vaikea havaita, koska siinä käytetään normaaleja yhteyskäytäntöjä eikä sitä ole määrällisesti paljon. Toisin sanoen siinä ei ole mitään poikkeavaa, vaan se muistuttaa normaalia verkkoliikennettä. Tiedon louhinnan on havaittu olevan tehokas keino komento- ja kontrollipalvelimen tietoliikenteen tunnistamiseen. Tiedon louhinta –tekniikoista voidaan käyttää ainakin koneoppimista (machine learning), luokittelua (classification) ja klusterointia.

Hyökkäyslähteen identifiointi ja esto

Hajautetun palvelunestohyökkäyksen torjunnassa on tärkeää tunnistaa lähteet, toisin sanoen mistä ip-osoitteista hyökkäysliikennettä generoidaan. Tavallinen vastalääke IP-osoitteen väärentämiseen on IP-pakettien merkitseminen (Packet Marking). Siinä reitittimet jättävät jälkensä IP-paketteihin ja palvelunestohyökkäyksen kohde voi tämän avulla rekonstruoida hyökkäyspolun ja jäljittää (traceback) näin ollen hyökkääjän, IP-osoitteen väärentämisestä huolimatta. [PDB07]

IP-pakettien merkitsemistekniikat voidaan jakaa kahteen kategoriaan [PDB07]:

- Todennäköinen merkitseminen (Probabilistic Packet Marking - PPM)
  IP-paketit merkataan jollain todennäköisyydellä, yleensä 1/25. Hyökkäyspolun rekonstruointi vaatii yleensä 500-1000 IP-pakettia tällä tekniikalla.

- Deterministinen merkitseminen (Deterministic Packet Marking - DPM)
  Jokainen IP-paketti merkataan. Ongelmaksi voi tällöin muodostua rajallinen tila IP-otsikossa (IP Header)

Paruchuri, Durresi ja Barolli ovat kehittäneet FAST-nimisen (Fast Autonomous System Traceback) DPM-tekniikan. Siinä ei rekonstruoida IP-polkua, vaan hyökkäyspolku selvitetään AS-tasolla (Autonomous System). AS-reunareitittimet lisäävät jokaiseen IP-pakettiin tunnisteen ja hyökkäyksen kohde pystyy rekonstruoimaan hyökkäyspolun nopeasti vastaanotettuaan vain pienen joukon IP-paketteja. Vain AS-reunareitittimien pitää siis osallistua merkitsemiseen, mikä on etu siinäkin mielessä, että rajallinen tila IP-otsikossa ei muodostu ongelmaksi niin kuin yleensä deterministisissä tekniikoissa. [PDB07]

Zhaoyang ja Chunfeng ovat kehittäneet jäljitysalgoritmin, joka perustuu FAST-yhteyskäytäntöön eroten siitä siten, että se tarvitsee ainoastaan lähimmän IP-paketin reitillä olleen AS-reunareitittimen valitakseen satunnaisesti yhden tiivistefunktion neljästä mahdollisesta. Muut AS-reunareitittimet ottavat huomioon kaksi viimeistä bittiä edellisen reitittimen laskemasta tiivisteestä. Heidän menetelmänsä perustuu siis myös autonomisiin järjestelmiin (autonomous system, AS) ja se jakaantuu kahteen vaiheeseen [ZhC08]:

- Ensimmäisessä vaiheessa autonomiseen järjestelmään perustuvalla deterministisellä paketin merkkaajalla (Deterministic Packet Marking based on AS, ASDPM) selvitetään AS, mistä hyökkäys on lähtöisin.
- Toisessa vaiheessa ei-toistettavaa todennäköistä paketin merkkaajaa (Non-Repeated Probabilistic Packet Marking, NRPPM) käytetään varsinaisen hyökkäyslähteen tunnistamiseen kyseisessä AS:ssa.

Verrattuna aikaisempiin menetelmiin Zhaoyangin ja Chunfengin algoritmi kuluttaa vähän tietoliikennekaistaa, konvergenssi on nopeaa, se on laskennallisesti kevyt ja se tuottaa vähän vääriä tuloksia (false positive). Se rekonstruoi hyökkäyspolun tehokkaasti tehden mahdolliseksi hyökkäyslähteiden reaaliaikaisen selvittämisen. [ZhC08]

Liikenteen torjuminen ja jakaminen eri kohteisiin erilaisin perustein

Jun, Ping ja Peiguo korostavat ip-osoitteen väärentämisen olevan erityisen vaarallisen piirteen tämän päivän palvelunestohyökkäyksissä. He ovat luokitelleet osoiteväärennökset kuuteen eri kategoriaan, jotta niitä voitaisiin paremmin analysoida, tunnistaa ja torjua [JPP10]:

- Kategoria H0 (dark addresses)

  Hyökkäyksessä käytetty lähdeosoite on julkinen ip-osoite, jota ei ole rekisteröity kenellekään tai joka ei ole aktiivisessa käytössä. Myös yksityiset osoitteet (private address) ja silmukka osoite (loop address) kuuluvat tähän kategoriaan.

- H1

  Hyökkääjä käyttää kohteen ip-osoitetta.

- H2

  Hyökkääjä käyttää ip-osoitetta, mikä on samassa aliverkossa kuin kohde.

- H3

Hyökkääjä käyttää ip-osoitetta, mikä on samassa aliverkossa kuin hänen oikea osoitteensa.

- H4

  Hyökkääjä käyttää jonkun hänen ja kohteen välissä olevan verkkolaitteen ip-osoitetta.

- H5

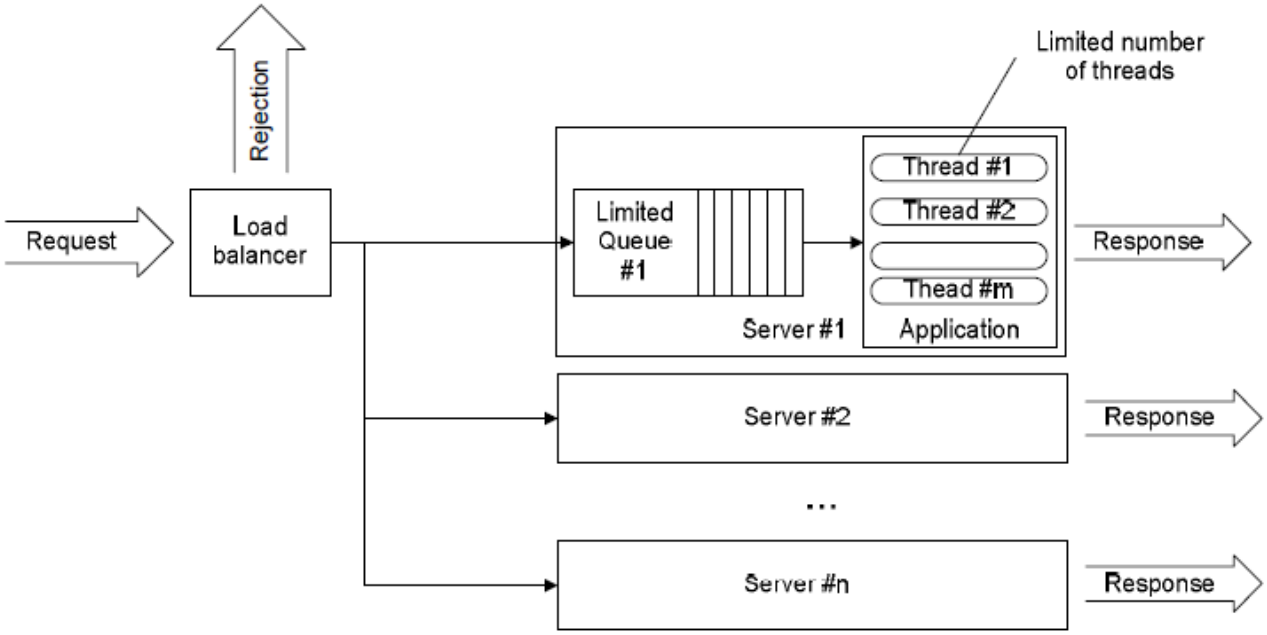
  Hyökkääjä käyttää ip-osoitetta, mikä ei ole missään topologisessa suhteessa hänen omaansa tai kohteen osoitteeseen.

Huomattakoon että, jos hyökkääjä ja hyökkäyksen kohde sijaitsevat samassa aliverkossa, kategoriat H2 ja H3 ovat yhteneväiset.

Kuvassa 21 on perinteinen kuormanjakomalli. Samalla tapaa kuin kuormanjakaja jakaa kuormaa eri palvelimille voidaan liikennettä jakaa myös muilla perustein, esimerkiksi lähdeosoitteen perusteella. Edelleen tällaisessa jakajassa voi olla käytössä musta- ja valkolistat, jolloin mustalla listalla olevista ip-osoitteista tulevaa liikennettä ei jaeta ollenkaan, vaan se hylätään, samoin kuin muilla tavoin hyökkäysliikenteeksi tunnistettu tietoliikenne (kuvan 15 rejection-nuoli). [THT08]

Mustalle listalle kerätään lähdeosoitteita, jotka on tunnistettu hyökkäysliikennettä lähettäviksi osoitteiksi. Mustia listoja voi tehdä itse tai niitä voi hankkia julkisista ja kaupallisista lähteistä. Myös roskapostin torjuntaan on omia mustia listoja, jotka sijoitetaan tyypillisesti postipalomuurille. [THT08]

Mustat listat eivät toimi, jos hyökkääjä väärentää osoitteensa sellaiseksi, mitä ei listalta löydy. Eräs vastatoimi tähän on valkolistan käyttö. Valkolistalle kerätään normaalitoiminnan aikana palvelun vakiokäyttäjien lähdeosoitteita. Jos joudutaan hyökkäyksen kohteeksi, otetaan valkolista käyttöön, jolloin vain valkolistan lähdeosoitteista pääsee palveluun. Hyökkäys tyrehtyy, mutta uudet käyttäjät eivät pääse palveluun. Samoin vakiokäyttäjän pääsy estyy, jos hän pyrkii palveluun eri lähdeosoitteesta kuin normaalisti. [THT08]



KUVA 21: Perinteinen kuormanjakomalli

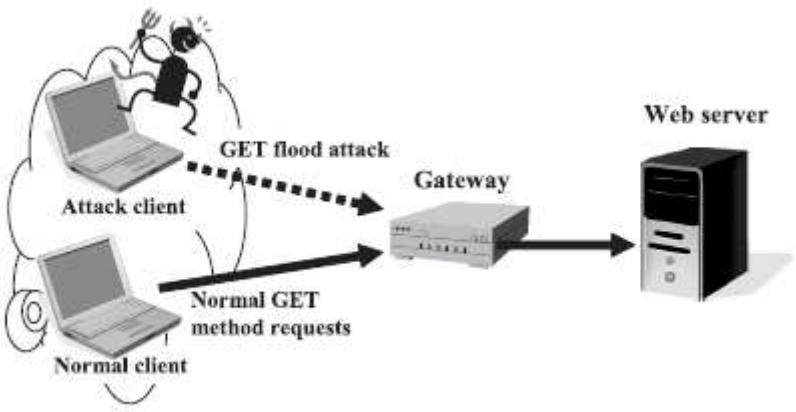
Jos hyökkäyksen kohteena oleva www-palvelu vaatii sisään kirjautumisen ja jos liikennettä pystytään jaottelemaan sen mukaan, onko kyseessä jo tunnistettu käyttäjä vai ei, pystyvät palvelussa jo sisällä olevat käyttäjät jatkamaan palvelun käyttämistä hyökkäystilanteessa. Näin siinä tapauksessa, että muu liikenne estetään. Tällöin luonnollisesti myös uusien laillisten käyttäjien sisään kirjautuminen estyy.

Jos käytössä on SSL-salaus, pitää se purkaa palvelun sertifikaatilla ennen kuin päästään tutkimaan, onko käyttäjä jo tunnistettu vai ei. Isommissa installaatioissa tilanne on usein se, että SSL-yhteydet terminoidaan jo ennen www-palvelimia, esim. kuormanjakajilla, jolloin tämä tarkistus voidaan tehdä ennen www-palvelimia selväkielisestä liikenteestä.

HTTP GET –tulvituksen esto

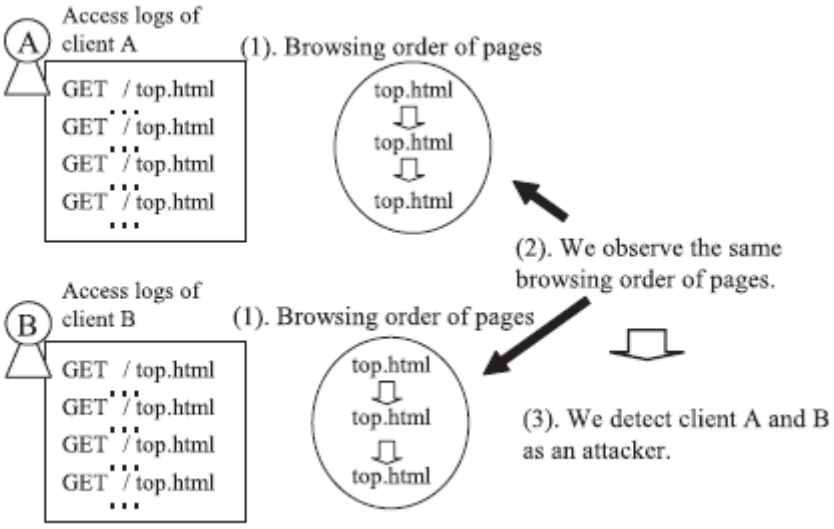
HTTP GET –tulvituksesta on kysymys, kun www-palveluun lähetetään suuria määriä tavallisia HTTP GET –pyyntöjä. Koska pyynnöt ovat täysin normaalin näköisiä, niiden erottaminen laillisista HTTP GET –pyynnöistä, ja siten myös torjunta, on hankalaa. [YIS07]

Yatagai, Isohara ja Sasase ovat tutkineet HTTP GET -tulvituksen havaitsemista sivustokäyttäytymisen (page access behavior) avulla. He ovat kehittäneet kaksi algoritmia, jotka asennetaan yhdyskäytävään kuvan 22 järjestelmämallissa. Järjestelmä toimii siten, että hyökkäysliikenteeksi tunnistetut pyynnöt pysäytetään yhdyskäytävällä ja vain lailliset pyynnöt päästetään www-palveluun. [YIS07]



KUVA 22: Järjestelmämalli HTTP GET –tulvituksen torjuntaan

Kuvassa 23 esitetään ensimmäisen algoritmin periaate. Siinä lokitetaan kustakin ip-osoitteesta tulevat sivupyynnöt. Jos kahdesta tai useammasta osoitteesta, toisin sanoen kahdelta tai useammalta asiakkaalta tulee tietty määrä identtisiä sivupyyntöjä samassa järjestyksessä, voidaan päätellä että asiakkailla on sama agenttiohjelma generoimassa pyyntöjä. Kyseessä on siis hyökkäys ja kyseisistä ip-osoitteista tulevat sivupyynnöt pysäytetään yhdyskäytävällä. [YIS07]

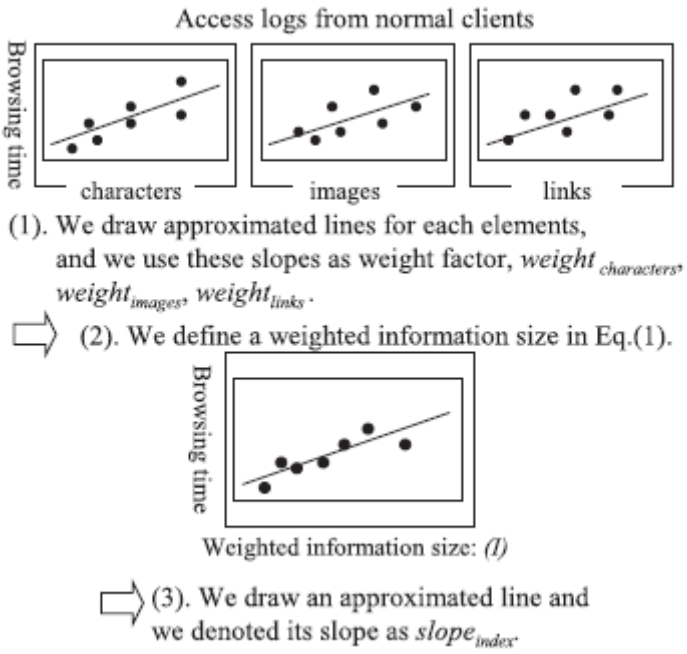


KUVA 23: Algoritmi 1, sivupyyntöjen lokitus ja vertailu

Kuvissa 24 ja 25 esitetään toinen algoritmi, missä verrataan asiakkaan sivustolla viettämää aikaa siirretyn tiedon määrään. [YIS07]

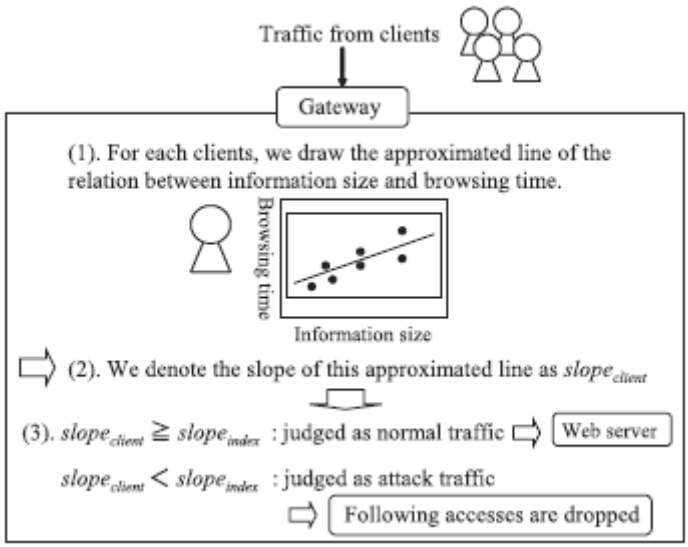
Ensin lasketaan vanhoista lokitiedoista jokaiselle lähde-ip-osoitteelle merkki-, kuva- ja linkkimäärät ajan funktiona. Sitten tehdään kaikille kolmelle estimaattisuora ja lasketaan kulmakertoimet. Nämä yhdistetään, jolloin saadaan jokaiselle lähde-ip-osoitteelle siirretty

tiedon määrä ajan funktiona. Osalla lähde-ip-osoitteista siirretty tiedon määrä ja aika korreloivat huonosti keskenään. Näitä ei oteta huomioon, mutta lopuista lasketaan painotettu indeksikulmakerroin, minkä katsotaan vastaavan normaaliasiakkaan asiointia www-palvelussa. [YIS07]



KUVA 24: Algoritmi 2, indeksikulmakertoimen laskeminen

Toisessa vaiheessa jokaiselle www-palvelussa asioivalle asiakkaalle lasketaan reaaliaikaisesti asiakaskulmakerroin vastaavalla tavalla kuin lähde-ip-osoitteille laskettiin kulmakertoimet vanhoista lokitiedoista. Näin saatua asiakaskulmakerrointa verrataan indeksikulmakertoimeen. Jos asiakaskulmakerroin on suurempi tai yhtä suuri kuin indeksikulmakerroin, kyseessä on normaaliliikenne, joka ohjataan edelleen www-palveluun. Jos asiakaskulmakerroin on pienempi kuin indeksikulmakerroin, kyseisen asiakkaan katsotaan olevan hyökkäysverkon agentti, eikä kyseisestä ip-osoitteesta tulevia pyyntöjä välitetä enää yhdyskäytävältä www-palveluun. [YIS07]



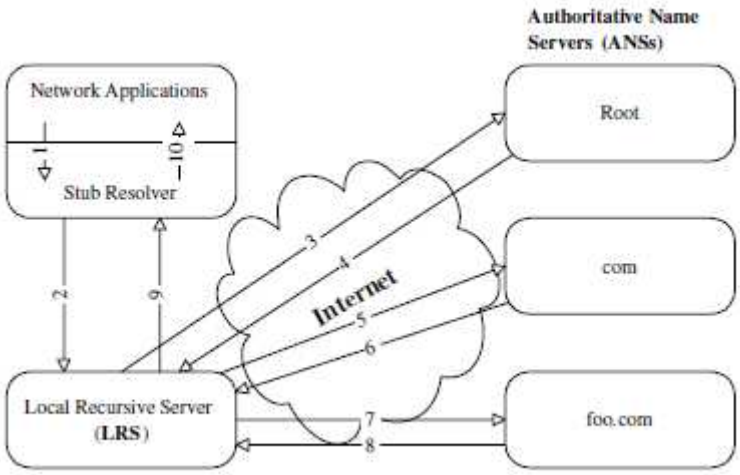
KUVA 25: Algoritmi 2, asiakaskulmakertoimen laskeminen ja vertaaminen indeksikulmakertoimeen

Nimipalvelun suojaaminen

Nimipalvelu (Domain Name System, DNS) on kriittinen elementti Internetin infrastruktuurissa tarjotessaan kyselijöille isäntänimeä vastaavan ip-osoitteen. Nimipalvelu tarjoaa yhä enenevässä määrin palveluita myös muille sovelluksille, esimerkiksi ip-osoitteita vastaavia sijaintitietoja ja hakemistopalveluita perinteisille puhelinsovelluksille. Lisäksi mm. SMTP- ja SIP-yhteyskäytännöt ovat riippuvaisia nimipalvelusta reitittäessään viestejä sovellustason yhdyskäytävien läpi. [PML07]

Koska nimipalvelukyselyt ja –vastaukset perustuvat enimmäkseen yhteydettömään UDP-yhteyskäytäntöön (User Datagram Protocol), on nimipalvelu altis ip-osoiteväärennöksiin perustuviin palvelunestohyökkäyksiin. Viime vuosina hyökkäyksiä on ollutkin. Jo se, että pieni osa nimipalveluinfrastruktuurista on pienen aikaa saavuttamattomissa, häiritsee mahdollisesti koko Internetin toimintaa. [FJT06]

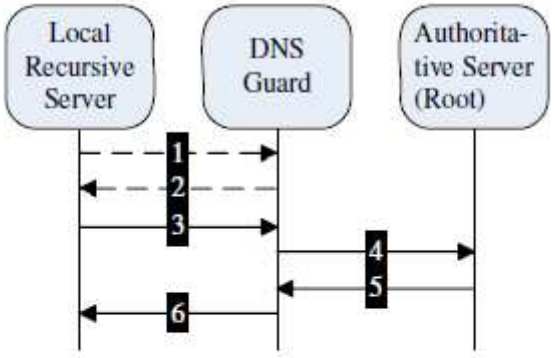
Kuvassa 26 esitetään nimipalveluarkkitehtuuri. Kun verkkosovellus pyytää isäntänimeä vastaavaa ip-osoitetta (name resolution), tyypillisesti samassa koneessa oleva Stub Resolver lähettää rekursiivisen nimipalvelukyselyn yleensä paikalliselle eli oman organisaation nimipalvelimelle (Local Recursive Server, LRS), joka edelleen lähettää yhden tai useamman iteratiivisen kyselyn usealle viralliselle nimipalvelimelle (authoritative name servers, ANS). Paikallinen nimipalvelin pitää välimuistissaan virallisilta nimipalvelimilta saamansa vastaukset ja lähettää uusia kyselyitä vain jos ei löydä vastausta omasta välimuististaan. [FJT06]



KUVA 26: Nimipalveluarkkitehtuuri

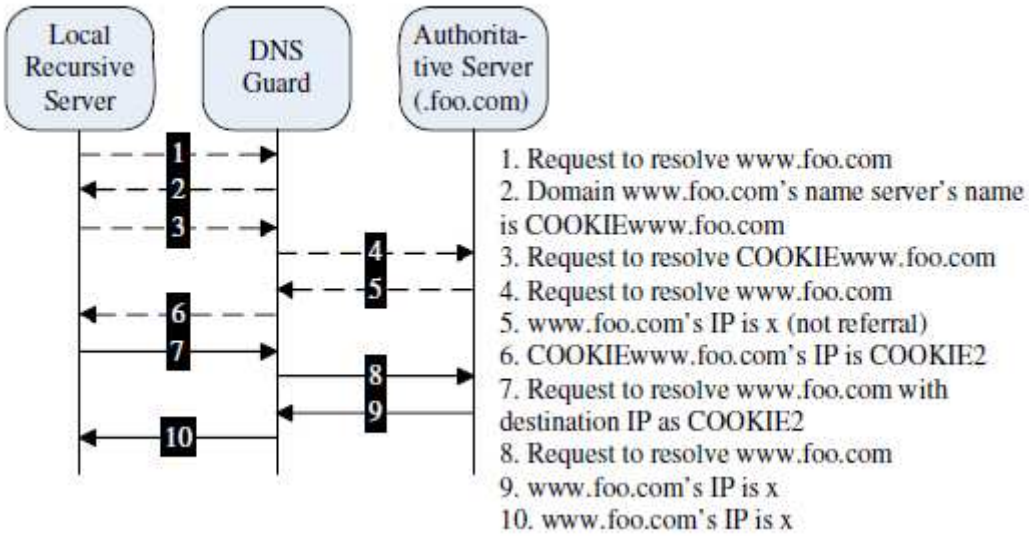
Fanglu, Jiawu ja Tzi-cker ovat kehittäneet paikallisen nimipalvelimen ja virallisen nimipalvelimen väliin asetettavan nimipalvelupalomuurin (DNS Guard), joka evästetekniikalla pyrkii estämään väärän ip-osoitteen käytön nimipalvelukyselyissä. [FJT06]

Kuvassa 27 esitetään evästeen käyttö tapauksessa, jossa nimipalvelin ei tue rekursiota, jolloin se antaa viitteellisen vastauksen (referral answer). Viitteellinen vastaus sisältää lisäresurssitietueita (additional resource record) kyselyn ratkaisemiseksi. [FJT06]



KUVA 27: Evästeen käyttö, kun nimipalvelin antaa viitteellisen vastauksen.

Kuvassa 28 esitetään evästeen käyttö tapauksessa, jossa nimipalvelin tukee rekursiota ja antaa ei-viitteellisen vastauksen. [FJT06]



KUVA 28: Evästeen käyttö, kun nimipalvelin antaa ei-viitteellisen vastauksen.

Kuvissa 27 ja 28 katkoviivat edustavat vaiheita, jotka ovat käytössä vain ensimmäisessä kyselyssä. [FJT06]

Pappasin, Masseyn ja Lixian mukaan nimipalveluarkkitehtuuriin saataisiin huomattavasti enemmän vastustuskykyä palvelunestohyökkäyksiä vastaan tekemällä seuraavat kaksi muutosta [PML07]:

- Nimipalvelutietueiden joukossa on infrastruktuuritietueita. Niissä on tietoa nimipalvelun infrastruktuurikomponenteista ja niitä käytetään nimipalveluhierarkiassa navigoitaessa. Infrastruktuuritietueet muuttuvat huomattavasti harvemmin kuin muut nimipalvelutietueet eli ne ovat suhteellisen staattisia. Jos niille määritettäisiin huomattavasti nykyistä pidempi TTL-aika, tiedot säilyisivät paikallisissa välimuisteissa, millä olisi positiivinen vaikutus palvelunestohyökkäysten torjunnassa.
- Sarja yksinkertaisia tietueiden uusimisperiaatteita käytettäväksi yhdessä yllä mainitun infrastruktuuritietueiden pidemmän TTL-ajan kanssa.

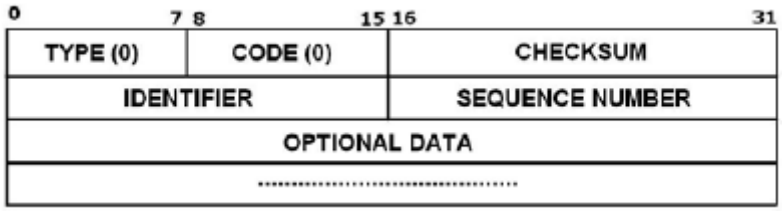
Edellä mainitut muutokset eivät vaadi mitään lisäresursseja tai muutoksia nimipalvelumalliin. [PML07]

ICMP-liikenteen rajoittaminen

ICMP (Internet Control Message Protocol) on yksi Internetin tärkeimmistä protokollista. Verkossa olevien tietokoneiden käyttöjärjestelmät käyttävät sitä pääasiassa virheilmoitusten lähettämiseen, esimerkiksi että pyydetty palvelu ei ole saatavilla. ICMP-protokollaa voidaan

käyttää myös kyselyjen välittämiseen. [UdA09]

Tyypillisesti reititin, isäntä tai käyttäjä käyttää ICMP echo requestia eli ping-komentoa testatakseen toisen järjestelmän saavutettavuutta. Kun järjestelmä vastaanottaa ICMP echo requestin, se vastaa lähettämällä ICMP echo replyn. Näin järjestelmät tietävät toistensa olemassaolosta verkossa. Kuvassa 29 on esitetty ICMP echo request- ja ICMP echo reply –viestien pakettimuoto. TYPE-kentän arvolla määritetään onko kyseessä request (8) vai reply (0). [Kum07]



KUVA 29: ICMP echo request- ja ICMP echo reply –viestien pakettimuoto.

ICMP-tulvitusta voidaan käyttää myös palvelunestohyökkäyksessä. Yleensä tätä torjutaan rajoittamalla ICMP-protokollalle varattua tietoliikennekaistaa, mikä voi johtaa siihen, että joskus tietoliikennekaistaa on liikaa ja joskus liian vähän siten, että laillinenkin ICMP-liikenne estyy. [UdA09]

Udhayan ja Anitha ovat kehittäneet ICMP-ikkunanrajoitusjärjestelmän (Window restriction scheme) ICMP-protokollalle varattavan tietoliikennekaistan parempaan määrittelemiseen. Vaadittava tietoliikennekaista Б lasketaan seuraavasti [UdA09]:

Vaadittava tietoliikennekaista Б = (N * β) pps = β pps

N = Ikkunoiden (komentorivien) lukumäärä, mikä tarvitaan ICMP-vuoropuheluun

Koska yksi ikkuna riittää lailliseen ICMP-vuoropuheluun, niin N = 1

β = ICMP-vuoropuhelujen määrä sekunnissa

pps (packets per second) = ip-paketteja sekunnissa

Udhayanin ja Anithan suorittamien testien mukaan ikkunanrajoitusjärjestelmän käyttö sallii edelleen laillisen ICMP-liikenteen, mutta se tyrehdyttää ICMP-tulvitushyökkäyksen siten, että generoitua hyökkäysliikennettä tarvitaan kymmenen kertaa enemmän, jotta saavutetaan sama hyökkäysteho. [UdA09]

8. Tehokkaan puolustuksen vaatimuksia ja kaupallisia tuotteita

Tässä luvussa esitellään ensin vaatimuksia, jotka täyttämällä voidaan estää palvelunestohyökkäyksiä tai ainakin vähentää niiden vaikutuksia.

Tämän jälkeen käsitellään erilaisia kaupallisia vaihtoehtoja palvelunestohyökkäysten torjuntaan.

8.1. Tehokkaan puolustuksen vaatimuslista

Listan vaatimukset on johdettu tämän esityksen aikaisemmista luvuista, erityisesti luvussa 7 käsitellyistä vastatoimista.

1. Connection limit – yhteysmäärien rajoitus, estää yhdestä lähteestä tulevat hyökkäykset

2. Connection reset/aging (mahdollisuus resetoida idle-yhteydet, session TTL)

3. Syn proxy – tekee tcp-kättelyn, estää syn flood-hyökkäykset
   SynFlood käsittelykyky min. 1Msyns/sek

4. Käytösanalyysi ja näkymä liikenteeseen (reaaliaikainen ja historia, baseline)

5. Protokolla-anomalioiden tunnistaminen (http, https header)

6. Tila-anomalioiden tunnistaminen (syn-ack tilat, Syn proxy, sekvenssinumeromuutokset)

7. Adaptiivinen kaistanhallinta (liikenteen mukaan muuntuvat thresholdit), Ingress, Egress

8. Kiinteä kaistanhallinta (fixed thresholds) (L3 Frag,src/dst IP, L4 tcp/udp port, icmp, syn)

9. Porttiskannauksen esto (madot yms.)

10. Botnet/DDoS-esto (heuristiikka, algoritmit, riittävä suorituskyky)

11. Source tracking – hyökkäyslähteen identifiointi ja esto

12. Dark addresses-esto (julkiset ip-alueet, joita ei rekisteröity kenellekään tai eivät aktiivisessa käytössä)

13. Mahdollisuus ohjata liikennettä eri vipeille source-osoitteen perusteella -> vlan ja/tai dst ip

14. White/black-listaukset (päästetään läpi ilman muita tarkistuksia/estetään/ohjataan eri vipille)

15. Autentikointi voimassa / ei voimassa ja ohjaus sen mukaan (jos mahdollista https-paketissa)

16. HTTP GET Flood (L7) –esto

17. DNS-palvelun suojaaminen flooding-hyökkäyksiltä

18. ICMP-liikenteen rajoittamismahdollisuus

Lisäksi raja-arvoja ja tietoliikenteeseen ja suorituskykyyn liittyviä vaatimuksia:

- Kaksi 1 Gbit kupariporttia, joiden läpi liikenne kulkee (in-line)
- Liikenteen käsittelykyky 1 Gbps
- HA/Stateful failover
- Joko sisäänrakennettu tai erikseen saatavilla oleva bypass-switch, jolla voidaan suojauslaitteisto ohittaa vikatilanteessa automaattisesti ja manuaalisesti esim. etäyhteydellä
- Yhtäaikaisten yhteyksien maksimimäärä vähintään 300k
- Uusia yhteyksiä 50k/sek minimi
- HTTP Idle timeout 300 sek (DDos) – 360 sek palomuuri (säädetään tarpeen mukaan)
- HTTPS idle timeout 1800 sek (DDos) – 1860 sek palomuuri (säädetään tarpeen mukaan)
- HTTP connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
- HTTPS connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
- Poispudotetun liikenteen ohjaamismahdollisuus liikenneanalysaattorille (span/mirror tms.)
  Reitittimillä Black holeen/nulliin ohjattavan liikenteen ohjaaminen ja monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
- DDos-laitteistolla ”roskiin” ohjatun liikenteen monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
- Lokien ja hälytysten ohjaaminen lokivalvontajärjestelmälle esim. syslogilla

8.2. Kaupallisia tuotteita

Tässä luvussa käsitellään ensin sitä vaihtoehtoa, että suojaa palvelunestohyökkäyksiä vastaan ostetaan palveluna.

Tämän jälkeen esitellään kaupallisia tuotteita, jotka Gartner mainitsee raporteissaan Gartner 2008 IT Security Threat Projection Timeline ja Magic Quadrant for Network Intrusion Prevention System Appliances. Gartnerin mukaan nyt käsiteltävät tuotteet soveltuvat hyvin palvelunestohyökkäysten torjuntaan.

Tuotteiden ominaisuuksia peilataan tehokkaan puolustuksen vaatimuslistaa vasten. Tuotteiden tiedot on kerätty lähinnä valmistajien www-palveluista. Lisätietoja ja tarkennuksia on kysytty sekä sähköpostilla valmistajilta että suomalaisilta tuotteiden jälleenmyyjiltä. Tiedot on kerätty syksyllä 2010 ja keväällä 2011. Lopuksi todetaan, että

kaksi tuotetta erottuu joukosta.

Palvelunestohyökkäyksiltä suojautuminen palveluna

Gartner ennakoi Selecting the Right Targets for Security as a Service -raportissaan (14.11.2007), että suojauksen hankkiminen palvelunestohyökkäystä vastaan palveluna ei tule suosituksi vaihtoehdoksi. Gartner ennustaa, että loppuvuoden 2007 1%-tasosta noustaisiin ainoastaan 3%:iin vuoteen 2013 mennessä. Tämä 3%:n siivu olisi käytännössä Internet-palveluntarjoajilla.

Arbor Networks

Arbor Networks on johtava toimittaja verkkouhkien havainnointi- ja torjuntatuotteissa. Tarjolla on lähinnä teleoperaattoritason ratkaisuja, joten laitteiden suorituskyky on erittäin hyvällä tasolla. Arbor Networks ylläpitää myös ATLAS-palvelua (Global Network Threat Analysis) osoitteessa http://atlas.arbor.net/.

http://www.arbornetworks.com/

Ratkaisu: Arbor TMS

Arbor TMS täyttää erittäin hyvin sekä toiminnallisuuteen että tietoliikenteeseen ja suorituskykyyn liittyvät tehokkaan puolustuksen vaatimukset (ks. liite).

Cisco

Cisco on maailman johtava verkkotuotteiden toimittaja. Palvelunestohyökkäysten torjuntaan on tarjolla Catalyst 6500 -reitittimeen optiona liitettävä Anomaly Guard –moduuli.

http://www.cisco.com/

Ratkaisu: Cisco Guard

Cisco Guardilla on selkeitä puutteita sekä toiminnallisuuteen että tietoliikenteeseen ja suorituskykyyn liittyen (ks. liite).

Juniper Networks

Juniper Networks on amerikkalainen tietoliikennetuote- ja teknologiatoimittaja. Tarjolla oleva ratkaisu on uuden sukupolven yhdyskäytävätuote tietoverkon suojaamiseen ja liikenteenvälitykseen keskikokoisille ja suurille yrityksille.

http://www.juniper.net/

Ratkaisu: IDP, Juniper SRX 3400

IDP, Juniper SRX 3400 täyttää hyvin sekä toiminnallisuuteen että tietoliikenteeseen ja suorituskykyyn liittyvät tehokkaan puolustuksen vaatimukset (ks. liite).

Radware

Radware on israelilainen tietoliikennetoimittaja. Defence Pro -ratkaisu on Radwaren lippulaivatuote palvelunestohyökkäysten torjuntaan. Kyseessä on laite, joka käyttää tekoälyä ennestään tuntemattomien uhkien torjuntaan.

http://www.radware.com/

Ratkaisu: Radware Defense Pro

Radware Defense Pro täyttää melko hyvin sekä toiminnallisuuteen että tietoliikenteeseen ja suorituskykyyn liittyvät tehokkaan puolustuksen vaatimukset (ks. liite).

TippingPoint

Hewlett-Packard osti TippingPoint-yhtiön keväällä 2010. TippingPoint on kuitenkin säilynyt tuotenimenä. Palvelunestohyökkäysten torjuntaan soveltuva tuote koostuu TippingPoint Security Management System -hallintalaitteesta ja IPS1200E hyökkäysten estolaitteesta.

http://www.hp.com/

Ratkaisu: TippingPoint IPS

TippingPoint IPS:llä on selkeitä puutteita sekä toiminnallisuuteen että tietoliikenteeseen ja suorituskykyyn liittyen (ks. liite).

Top Layer Security

Top Layer Security on amerikkalainen IPS-järjestelmiin (Intrusion Prevention Systems) erikoistunut tietoliikennetoimittaja. Ei edustusta Suomessa. IPS 5500 on Top Layer Securityn edistynein tuoteperhe.

http://www.toplayer.com/

Ratkaisu: Top Layer IPS 5500

Top Layer IPS 5500 täyttää melko hyvin sekä toiminnallisuuteen että tietoliikenteeseen ja suorituskykyyn liittyvät tehokkaan puolustuksen vaatimukset (ks. liite).

F5 Networks

F5 Networks on amerikkalainen tietoliikennetoimittaja, joka on tunnettu mm. järeistä BIG-IP –kuormanjakajistaan. Viprion on modulaarinen ratkaisu, johon voidaan lisätä erilaisia toiminnallisuuksia, esimerkkinä ssl-yhteyksien terminointi.

http://www.f5.com/

Ratkaisu: F5 BIG-IP Viprion

F5 BIG-IP Viprion täyttää erittäin hyvin sekä toiminnallisuuteen että tietoliikenteeseen ja suorituskykyyn liittyvät tehokkaan puolustuksen vaatimukset (ks. liite).

Tuoteanalyysi

Edellä käsitellyt tuotteet ovat kalliita. Hinnoista puhuttaessa kyse on ennemmin sadoista tuhansista kuin kymmenistä tuhansista euroista. Hinnat ovat kuitenkin siinä mielessä kohdillaan, että mitä enemmän on valmis maksamaan, sen paremman suojan palvelunestohyökkäyksiä vastaan saa.

Tuotteiden ominaisuustaulukkoja katsomalla kaksi tuotetta nousee ylitse muiden: Arbor Networksin TMS ja F5 Networksin Viprion.

Arbor Networksin tuotteet sopivat suorituskykynsä puolesta myös teleoperaattoreille, ja tämä näkyy myös tuotteiden ja ratkaisujen hinnoittelussa.

F5 Networks on erikoistunut kuormanjakamiseen, ja tästähän palvelunestohyökkäysten torjunnassakin on kyse. Siis raskaasta tietoliikennekuormasta, joka tietyin perustein ohjataan eri osoitteisiin. Palvelunestohyökkäystilanteessa laillinen liikenne pyritään ohjaamaan haluttuun palveluun normaalisti ja hyökkäysliikenne pyritään torjumaan.

9. Yhteenveto ja johtopäätökset

Lukuisat esimerkit tänä päivänä todistavat, että palvelunestohyökkäyksen uhka erilaisten palveluiden jatkuvuudelle on todellinen. Uhkaa ei siis sovi aliarvioida, muttei myöskään yliarvioida. Kunkin organisaation pitää analysoida riskin suuruus normaalin riskienhallinnan keinoin. Riski määritellään arvioimalla toisaalta sen todennäköisyys ja toisaalta sen vaikutukset. Jotkut organisaatiot painottavat riskiä arvioidessaan enemmän todennäköisyyttä, toiset taas vaikutuksia riskin toteutuessa. Mitä korkeampi profiili yrityksellä on, sitä todennäköisemmin se joutuu laajamittaisen palvelunestohyökkäyksen kohteeksi.

Suojaustoimenpiteiden pitää olla oikein mitoitettuja ja kustannustehokkaita. Esimerkiksi verkkokauppa pystyy laskemaan euroissa, kuinka paljon rahaa menetetään, jos www-palvelu on päivän asiakkaiden saavuttamattomissa. Tällöin mittavatkin panostukset palvelunestohyökkäyksen torjuntakykyyn eli palvelun jatkuvuuteen ovat perusteltavissa. Verkkokaupan tapauksessa on myös vaarana, että asiakkaat menetetään pysyvästi kilpailijalle, jos asiakas ei saa haluamaansa palvelua juuri haluamanaan ajankohtana. Toisaalta tilanteessa, jossa organisaation www-palvelu toimii vain tiedotuskanavana, kannattaa miettiä, paljonko suojaustoimenpiteisiin kannattaa euroja sijoittaa.
Vaikkei www-palvelun alhaalla olon kustannuksia pystyisikään euroissa laskemaan, on se organisaatiolle kuitenkin aina imagotappio.

Tässä työssä käsitellään ensiksi julkisuudessa olleita palvelunestohyökkäyksiä, peruskäsitteistöä ja yleisiä, vapaasti saatavilla olevia hyökkäystyökaluja.

Tämän jälkeen tarkastellaan joitakin teoreettisia protokollatason parannusehdotuksia. Siis sellaisia IP-protokollan parannuksia, joiden avulla olisi helpompi varautua erityyppisiin

palvelunestohyökkäyksiin. Internetin yleinen ongelmahan on se, että tekninen perusta on luotu aikana, jolloin nykyisiä uhkakuvia, mm. palvelunestohyökkäyksiä, ei voitu kuvitellakaan. Miten nämä teoreettiset protokollatason parannusehdotukset vaikuttaisivat luvun 6 käytännöllisten vastatoimien tarpeellisuuteen? Jos siis päästäisiin suunnittelemaan Internetin liikennöintiä ikään kuin puhtaalta pöydältä, olisiko palvelunestohyökkäyksiin liittyvä ongelmakenttä poispyyhkäisty? Osittain kyllä, mutta ei kokonaan. Esimerkiksi Auran ja Nikanderin tilattomat yhteydet ratkaisevat kyllä sen ongelman, että tilatietoinen palvelin pystyy käsittelemään vain rajallisen määrän yhtäaikaisia yhteydenottoja, mutta ongelmaksi jää edelleen se, että hyökkääjä voi lähettää saman tilan sisältävää viestiä yhä uudelleen ja uudelleen. Juelsin ja Brainardin asiakasarvoitusprotokolla tarjoaa lääkkeen TCP SYN –tulvitusta vastaan, mutta siinäkin pitäisi jollain mekanismilla ratkaista se, ettei hyökkääjä käytä samaa ongelman ratkaisua useamman aloituksen rekisteröimiseen. Kyse on samantapaisesta kilpavarustelusta kuin virusten tekijöiden ja virusten torjujien välillä; vaikka protokollatason parannuksia saataisiin laajalti käyttöön, epäilemättä niitäkin vastaan keksittäisiin uusia hyökkäystapoja.

Käytännöllisistä vastatoimista käsiteltiin ensiksi BGP:tä. Jos organisaatio ylläpitää itse BGP-reitittimiä, voidaan niitä käyttää kuvatulla tavalla ulkomaan liikenteen suodattamiseen. Jos www-palvelun halutut käyttäjät ovat suomalaisia, niin kuin Suomessa tilanne usein on, niin tämä on tehokas tapa tyrehdyttää palvelunestohyökkäys, jos hyökkäysliikenne tulee ulkomailta. Vaikkei organisaatio ylläpitäisikään omia BGP-reitittimiä, niin tietoliikenneoperaattorin kanssa voi sopia etukäteen ulkomaan liikenteen suodattamiseen tähtäävistä toimista organisaation joutuessa palvelunestohyökkäyksen kohteeksi.

Seuraavaksi tarkasteltiin lähinnä IEEE:n ja ACM:n artikkeleiden pohjalta käytännöllisiä vastatoimia erilaisiin hyökkäystyyppeihin. Käsitellyistä toimenpiteistä on koottu tehokkaan puolustuksen vaatimuslista, joka tarjoaa kattavat vastatoimet erilaisiin hyökkäystyyppeihin.

Käytännönläheisyyteen on pyritty myös siinä mielessä, että teorian lisäksi käydään läpi kaupallista tarjontaa, toisin sanoen mitä tuotteita on tarjolla palvelunestohyökkäysten torjuntaan. Tuotteiden ominaisuuksia verrataan tehokkaan puolustuksen vaatimuslistaan. Siitä, perustuuko tuotteessa oleva torjuntaominaisuus tässä työssä esiteltyyn ratkaisuun, ei ole tietoa. Joissakin tapauksissa tämän voisi ehkä saada selville, mutta luultavasti useimmissa tapauksissa vedottaisiin liikesalaisuuteen, eikä kerrottaisi, miten torjuntaominaisuus on toteutettu.

Täytyy muistaa, että paras ratkaisu tiettynä ajankohtana tarjoaa parhaan suojan vain sillä hetkellä. Jos ratkaisu ei ole itse kehitetty, vaan kaupallinen tuote, voi olla ettei kyseistä tuotetta ole enää edes olemassa parin vuoden päästä. Tai voi olla, että entinen kärkituote ei ole enää ollut aktiivisen kehittämisen kohteena.

Jos päädytään kaupalliseen ratkaisuun, tuotteiden ominaisuuksia kannattaa ehdottomasti kokeilla ennen ostopäätöstä joko omassa ympäristössä tai suurempien valmistajien testilaboratorioissa. Osalla valmistajista on myös valmiita eri hyökkäystyyppejä simuloivia

testisarjoja, joita voi hyödyntää testauksessa.

Palvelunestohyökkäyksen uhka luultavasti vain kasvaa jatkossa. Internetiin liitettyjen koneiden määrä lisääntyy jatkuvasti, toisin sanoen verkossa on enemmän potentiaalisia agentteja ja myös hyökkäyksen kohteita. Internet-yhteydet muuttuvat koko ajan nopeammiksi, jolloin yksi agentti pystyy generoimaan enemmän hyökkäysliikennettä. Lisäksi ohjelmistot muuttuvat yhä vain monimutkaisemmiksi. Monimutkaisten ohjelmistojen haavoittuvuuksia voidaan hyödyntää paitsi agenttien hankkimisessa myös itse palvelunestohyökkäyksissä.

Tässä opinnäytetyössä olevan materiaalin perusteella yritys A päätti tutustua lähemmin F5 Networksin Viprion-tuotteeseen. PoC-testi (Proof of Consept), jossa todennettiin kyseisen tuotteen ominaisuustaulukon toiminnallisuudet, suoritettiin marraskuussa 2010 F5:n TechCenterissä Seattlessa. Hyvin menneen PoC-testin seurauksena yritys A hankki F5 Networksin Viprion-tuotteen tammikuussa 2011.

Yritys A:lla on myös luvussa 7.1. kuvattu BGP:hen perustuva suojaus käytössä siten, että ulkomaan liikenne saadaan torjuttua omin toimin tarpeen niin vaatiessa. Myös Viestintäviraston CERT-FI-yksikön ja tietoliikenneoperaattorin kanssa on etukäteen sovittu erityisistä toimenpiteistä, jos yritys A joutuu laajamittaisen ja voimakkaan palvelunestohyökkäyksen kohteeksi. Kevään 2011 aikana on torjuttu ainakin yksi sellainen hyökkäys, minkä kanssa oltaisiin oltu suurissa vaikeuksissa ennen nyt käytössä olevia torjuntaelementtejä.

Työ eteni hyvin ja yritys A sai hankittua hyvän tuotteen. Tuotteiden ominaisuustaulukoiden täyttäminen ts. tiedon hankinta tuotteista oli suhteellisen työlästä. Toisaalta se oli aivan oleellinen työvaihe, koska sen perusteella valittiin tuote PoC-testiin. Yritys A hankki Viprion-tuotteen, koska torjuntatuotteelle palvelunestohyökkäyksiä vastaan oli todellinen tarve. Tämä tarve saneli myös sen, että aikaa ei ollut hukattavaksi. Jos aikaa olisi ollut enemmän, PoC-testiin olisi voitu valita useampia tuotteita, ainakin Arbor Networksin ja ehkä myös Juniper Networksin tuotteet.

Lähteet

[AuN97]
Tuomas Aura; Pekka Nikander, *Stateless Connections*, HUT, Digital Systems Laboratory, 1997

[Cer01]
Palvelunestohyökkäykset eestiläisiä kohteita vastaan jatkuvat
http://www.cert.fi/tietoturvanyt/2007/05/P.html (16.10.2010)

[Cer02]
Palvelunestohyökkäys suomalaista verkkosivustoa kohtaan
http://www.cert.fi/katsaukset/2009/tietoturvakatsaus32009.html(16.10.2010)

[Cer03]
Tietoturvayhteisöjen kansainvälinen yhteistyö on osoittautunut toimivaksi
http://www.cert.fi/attachments/tietoturvakatsaukset/5mv2ocAMp/CERT-FI_vuosikatsaus_2009.pdf (16.10.2010)

[Cer04]
Massapostitettuja palvelunestohyökkäysuhkauksia liikkeellä
http://www.cert.fi/tietoturvanyt/2010/08/ttn201008131648.html (16.10.2010)

[Cer05]
HTTP-palvelimiin kohdistettu palvelunestohyökkäystyökalu ja rajoituskeinot
http://www.cert.fi/tietoturvanyt/2009/06/5hkJYDHtL.html (2.1.2011)

[Cha09]
Eric Chan-Tin, *Distributed Denial of Service Attacks: Analysis of Defenses*, VDM, 2009

[DPV06]
Dainotti, A.; Pescape, A.; Ventre, G.; , "NIS04-1: Wavelet-based Detection of DoS Attacks," *Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE* , vol., no., pp.1-6, Nov. 27 2006-Dec. 1 2006
doi: 10.1109/GLOCOM.2006.279
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4150909&isnumber=4150630

[EAT08]
El-Hajj, W.; Aloul, F.; Trabelsi, Z.; Zaki, N.; , "On Detecting Port Scanning using Fuzzy Based Intrusion Detection System," Wireless Communications and Mobile Computing Conference, 2008. IWCMC '08. International , vol., no., pp.105-110, 6-8 Aug. 2008
doi: 10.1109/IWCMC.2008.19
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4599918&isnumber=4599899

[Eni01]
Estonia cyber attacks
http://www.enisa.europa.eu/act/cert/contact/press-releases/enisa-commenting-on-massive-cyber-attacks-in-estonia?searchterm=denial (16.10.2010)

[FBI01]
InfraGard - Public Private Partnership -Federal Bureau of Investigation (FBI)
http://www.infragard.net/index.php?mn=0 (16.10.2010)

[FBI02]
Estonia vs. Russia, The DDOS War
http://www.cis.uab.edu/forensics/blog/Estonian.DDOS.pdf (16.10.2010)

[FJT06]
Fanglu Guo; Jiawu Chen; Tzi-cker Chiueh; , "Spoof Detection for Preventing DoS Attacks against DNS Servers," *Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on* , vol., no., pp. 37, 2006
doi: 10.1109/ICDCS.2006.78
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1648824&isnumber=34569

[FSR09]
Feily, M.; Shahrestani, A.; Ramadass, S.; , "A Survey of Botnet and Botnet Detection," Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on , vol., no., pp.268-273, 18-23 June 2009
doi: 10.1109/SECURWARE.2009.48
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5210988&isnumber=5210974

[GoS98]
Li Gong and Paul Syverson. Fail-stop protocols: An approach to designing secure protocols. In R. K. Iyer, M. Morganti, Fuchs W. K, and V. Gligor, editors, Dependable Computing for Critical Applications 5, pages 79–100. IEEE Computer Society, 1998.

[JPP10]
Jun Bi; Ping Hu; Peiguo Li; , "Study on Classification and Characteristics of Source Address Spoofing Attacks in the Internet," Networks (ICN), 2010 Ninth International Conference on , vol., no., pp.226-230, 11-16 April 2010
doi: 10.1109/ICN.2010.43
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5473981&isnumber=5473952

[JuB99]
A. Juels; J. Brainard, *Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks*, NDSS '99, RSA Laboratories, 1999

[KiR08]
Kim, S. S. and Reddy, A. L. 2008. Statistical techniques for detecting traffic anomalies through packet header data. IEEE/ACM Trans. Netw. 16, 3 (Jun. 2008), 562-575. DOI= http://dx.doi.org/10.1109/TNET.2007.902685

[Kum07]
Kumar, S.; , "Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet," Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on , vol., no., pp.25, 1-5 July 2007
doi: 10.1109/ICIMP.2007.42

URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4271771&isnumber=4271740

[Lex01]
Finlex
http://www.finlex.fi/fi/oikeus/kko/kko/2003/20030036 (22.2.2011)

[MDD05]
Jelena Mirkovic; Sven Dietrich; David Dittrich; Peter Reiher, *Internet Denial of Service: Attack and Defense Mechanisms*, PRENTICE HALL, 2005

[Mea99]
Catherine Meadows, *A Formal Framework and Evaluation Method for Network Denial of Service*, csfw, IEEE Computer Security Foundations Workshop, 1999

[MIT09]
MIT OpenCourseWare, 6.033 Computer System Engineering
http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-033-computer-system-engineering-spring-2009/recitations/MIT6_033s09_rec11_routing.pdf (16.10.2010)

[MOR09]
Moilanen, Teemu; Ojasalo, Katri; Ritalahti, Jarmo: "Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan.", WSOY 2009

[Möl06]
Jarmo Mölsä, *Mitigating denial of service attacks in computer networks*, Doctoral Dissertation, TKK Dissertations 32, Espoo 2006

[Nes01]
Nessus
http://www.nessus.org/ (22.2.2011)

[OAM05]
Ohsita, Y.; Ata, S.; Murata, M.; , "Deployable overlay network for defense against distributed SYN flood attacks," Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on , vol., no., pp. 407- 412, 17-19 Oct. 2005
doi: 10.1109/ICCCN.2005.1523897
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1523897&isnumber=32582

[OWA10]
OWASP Top Ten Project
(http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (16.10.2010)

[PCI08]
PCI Data Security Standard (DSS), Requirement 6.6, 2008
(https://www.pcisecuritystandards.org/pdfs/infosupp_6_6_applicationfirewalls_codereviews.pdf
(16.10.2010)

[PDB07]
Paruchuri, V.; Durresi, A.; Barolli, L.; , "FAST: Fast Autonomous System Traceback," Advanced Information Networking and Applications, 2007. AINA '07. 21st International Conference on , vol., no., pp.498-505, 21-23 May 2007
doi: 10.1109/AINA.2007.69
URL:

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4220933&isnumber=4220857

[PLR07]
Peng, T., Leckie, C., and Ramamohanarao, K. 2007. Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Comput. Surv. 39, 1 (Apr. 2007), 3. DOI= http://doi.acm.org/10.1145/1216370.1216373

[PML07]
Pappas, V.; Massey, D.; Lixia Zhang; , "Enhancing DNS Resilience against Denial of Service Attacks," Dependable Systems and Networks, 2007. DSN '07. 37th Annual IEEE/IFIP International Conference on , vol., no., pp.450-459, 25-28 June 2007
doi: 10.1109/DSN.2007.42
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4272996&isnumber=4272935

[ScV08]
Schuhmann, S.; Volker, L.; , "Combining Passive Autoconfiguration and Anomaly-Based Intrusion Detection in Ad Hoc Networks," Applications and Services in Wireless Networks, 2008. ASWN '08. Eighth International Workshop on , vol., no., pp.87-95, 9-10 Oct. 2008
doi: 10.1109/ASWN.2008.14
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4690845&isnumber=4690826

[SiD07]
Silveira, F. and Diot, C. 2007. Identifying statistically anomalous regions in time series of network traffic. In Proceedings of the 2007 ACM CoNEXT Conference (New York, New York, December 10 - 13, 2007). CoNEXT '07. ACM, New York, NY, 1-2. DOI= http://doi.acm.org/10.1145/1364654.1364730

[Sno01]
Snort
http://www.snort.org/ (22.2.2011)

[THT08]
Toth, E.; Hornak, Z.; Toth, G.; , "Protection System against Overload and Distributed Denial of Service Attacks," Dependability of Computer Systems, 2008. DepCos-RELCOMEX '08. Third International Conference on , vol., no., pp.195-202, 26-28 June 2008
doi: 10.1109/DepCoS-RELCOMEX.2008.53
URL:

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4573057&isnumber=4573023

[Tk_01]
Isku Veikkauksen verkkoon harvinaisen raju

http://www.tietokone.fi/uutiset/2009/isku_veikkauksen_verkkoon_harvinaisen_raju (16.10.2010)

[Tk_02]
Veikkauksen nettipalveluun hyökätään
http://www.tietokone.fi/uutiset/2009/veikkauksen_nettipalveluun_hyokataan (16.10.2010)

[TKK06]
TKK, S-38.3192 Verkkopalvelujen tuotanto, Luento 6: BGP
(http://www.netlab.tkk.fi/opetus/s383192/2006/kalvot/L6.pdf (16.10.2010)

[Tut01]
DoS-seminaariraportti
http://www.cs.tut.fi/kurssit/TLT-3700/dos-seminaari.pdf (8.1.2011)

[Tie01]
Verkkohyökkäys jumitti Veikkauksen palveluja
http://www.tietoviikko.fi/kaikki_uutiset/article318136.ece (16.10.2010)

[UdA09]
Udhayan, J.; Anitha, R.; , "Demystifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis," Advance Computing Conference, 2009. IACC 2009. IEEE International , vol., no., pp.558-564, 6-7 March 2009
doi: 10.1109/IADCC.2009.4809072
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4809072&isnumber=4808969

[YIS07]
Yatagai, T.; Isohara, T.; Sasase, I.; , "Detection of HTTP-GET flood Attack Based on Analysis of Page Access Behavior," Communications, Computers and Signal Processing, 2007. PacRim 2007. IEEE Pacific Rim Conference on , vol., no., pp.232-235, 22-24 Aug. 2007
doi: 10.1109/PACRIM.2007.4313218
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4313218&isnumber=4313156

[ZhC08]
Zhaoyang Qu; Chunfeng Huang; , "A Fractional-Step DDoS Attack Source Traceback Algorithm Based on Autonomous System," Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on , vol., no., pp.1383-1387, 15-17 Aug. 2008
doi: 10.1109/IIH-MSP.2008.61
URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4604300&isnumber=4603987

[ZhZ06]
Zhijun Wu; Zhifeng Chen; , "A Three-Layer Defense Mechanism Based on WEB Servers Against Distributed Denial of Service Attacks," Communications and Networking in China, 2006. ChinaCom '06. First International Conference on , vol., no., pp.1-5, 25-27 Oct. 2006
doi: 10.1109/CHINACOM.2006.344851 URL:
http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4149816&isnumber=4117415

Liite: Palvelunestohyökkäysten torjuntatuotteiden ominaisuustaulukot

Arbor Networks

Ratkaisu: Arbor TMS

Löytyy	Ei löydy	Ominaisuus
X		Syn proxy – tekee tcp-kättelyn, estää syn flood-hyökkäykset
X		Connection limiting – yhteysmäärien rajoitus, estää yhdestä lähteestä tulevat hyökkäykset
X		Connection reset/aging (mahdollisuus resetoida idle-yhteydet, session TTL)
X		Käytösanalyysi ja näkymä liikenteeseen (reaaliaikainen ja historia, baseline)
X*		Adaptiivinen kaistanhallinta (liikenteen mukaan muuntuvat thresholdit) - Ingress, Egress
X*		Kiinteä kaistanhallinta (fixed thresholds) (L3 Frag,src/dst IP, L4 tcp/udp port, icmp, syn)
X*		Porttiskannauksen esto (madot yms.)
X		Botnet/DDoS-esto (heuristiikka, algoritmit, riittävä suorituskyky)
X		Source tracking – hyökkäyslähteen identifiointi/esto
X		Protokolla-anomaliat (http, https header)
X		Tila-anomaliat (syn-ack tilat, sekvenssinumeromuutokset jne.)
X		Dark addresses-esto (julkiset ip-alueet, joita ei rekisteröity kenellekään tai eivät aktiivisessa käytössä)
X**		Mahdollisuus ohjata liikennettä eri vipeille (source-osoitteen perusteella -> vlan ja/tai dst ip)
X		White/black-listaukset (päästetään läpi ilman muita tarkistuksia/estetään/ohjataan eri vipille)
HTTP		Autentikointi voimassa / ei voimassa ja ohjaus sen mukaan (jos mahdollista https-paketissa)
X		DNS-palvelujen suojaaminen flooding-hyökkäyksiltä
X		ICMP-liikenteen rajoittamismahdollisuus
X		Kaksi 1 Gbit kupariporttia, joiden läpi liikenne kulkee (in-line)
X		Liikenteen käsittelykyky 1 Gbps
X		Yhtäaikaisten yhteyksien maksimimäärä vähintään 300k
X		Uusia yhteyksiä 50k/sek minimi
X		SynFlood käsittelykyky min. 1Msyns/sek
X		HTTP GET Flood (L7) –esto
HA	Stateful failover	HA/Stateful failover
X***		Poispudotetun liikenteen ohjaamismahdollisuus liikenneanalysaattorille (span/mirror tms.)
X		Joko sisäänrakennettu tai erikseen saatavilla oleva bypass-switch, jolla voidaan suojauslaitteisto ohittaa vikatilanteessa automaattisesti ja manuaalisesti esim. etäyhteydellä
X		Reitittimillä Black holeen/nulliin ohjattavan liikenteen ohjaaminen ja monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
X****		HTTP Idle timeout 300 sek (DDos) – 360 sek palomuuri (säädetään tarpeen mukaan)
X****		HTTPS idle timeout 1800 sek (DDos) – 1860 sek palomuuri (säädetään tarpeen mukaan)
X****		HTTP connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
X****		HTTPS connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
X		DDos-laitteistolla ”roskiin” ohjatun liikenteen monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
X		Lokien ja hälytysten ohjaaminen lokivalvontajärjestelmään

* Mitigointi aktivoitava manuaalisesti

** Vain kohde-IP:n perusteella

*** Blackhole sinkhole luotava

**** SW-versiossa 5.1

Cisco

Ratkaisu: Cisco Guard

Löytyy	Ei löydy	Ominaisuus
X		Syn proxy – tekee tcp-kättelyn, estää syn flood-hyökkäykset
X		Connection limiting – yhteysmäärien rajoitus, estää yhdestä lähteestä tulevat hyökkäykset
X		Connection reset/aging (mahdollisuus resetoida idle-yhteydet, session TTL)
X		Käytösanalyysi ja näkymä liikenteeseen (reaaliaikainen ja historia, baseline)
X		Adaptiivinen kaistanhallinta (liikenteen mukaan muuntuvat thresholdit) - Ingress, Egress
X		Kiinteä kaistanhallinta (fixed thresholds) (L3 Frag,src/dst IP, L4 tcp/udp port, icmp, syn)
	X	Porttiskannauksen esto (madot yms.)
X		Botnet/DDoS-esto (heuristiikka, algoritmit, riittävä suorituskyky)
X		Source tracking – hyökkäyslähteen identifiointi/esto
X		Protokolla-anomaliat (http, https header)
X		Tila-anomaliat (syn-ack tilat, sekvenssinumeromuutokset jne.)
X		Dark addresses-esto (julkiset ip-alueet, joita ei rekisteröity kenellekään tai eivät aktiivisessa käytössä)
	X	Mahdollisuus ohjata liikennettä eri vipeille (source-osoitteen perusteella -> vlan ja/tai dst ip)
	X	White/black-listaukset (päästetään läpi ilman muita tarkistuksia/estetään/ohjataan eri vipille)
	X	Autentikointi voimassa / ei voimassa ja ohjaus sen mukaan (jos mahdollista https-paketissa)
X		DNS-palvelujen suojaaminen flooding-hyökkäyksiltä
X		ICMP-liikenteen rajoittamismahdollisuus
X		Kaksi 1 Gbit kupariporttia, joiden läpi liikenne kulkee (in-line)
X		Liikenteen käsittelykyky 1 Gbps
X		Yhtäaikaisten yhteyksien maksimimäärä vähintään 300k
X		Uusia yhteyksiä 50k/sek minimi
X		SynFlood käsittelykyky min. 1Msyns/sek
X		HTTP GET Flood (L7) –esto
	X	HA/Stateful failover
X		Poispudotetun liikenteen ohjaamismahdollisuus liikenneanalysaattorille (span/mirror tms.)
X		Joko sisäänrakennettu tai erikseen saatavilla oleva bypass-switch, jolla voidaan suojauslaitteisto ohittaa vikatilanteessa automaattisesti ja manuaalisesti esim. etäyhteydellä
X	X	Reitittimillä Black holeen/nulliin ohjattavan liikenteen ohjaaminen ja monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
	X	HTTP Idle timeout 300 sek (DDos) – 360 sek palomuuri (säädetään tarpeen mukaan)
	X	HTTPS idle timeout 1800 sek (DDos) – 1860 sek palomuuri (säädetään tarpeen mukaan)
X		HTTP connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
X		HTTPS connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
	X	DDos-laitteistolla ”roskiin” ohjatun liikenteen monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
X		Lokien ja hälytysten ohjaaminen lokivalvontajärjestelmään

Juniper Networks

Ratkaisu: IDP, Juniper SRX 3400

Löytyy	Ei löydy	Ominaisuus
X		Syn proxy – tekee tcp-kättelyn, estää syn flood-hyökkäykset
X		Connection limiting – yhteysmäärien rajoitus, estää yhdestä lähteestä tulevat hyökkäykset
X		Connection reset/aging (mahdollisuus resetoida idle-yhteydet, session TTL)
STRM*		Käytösanalyysi ja näkymä liikenteeseen (reaaliaikainen ja historia, baseline)
X		Adaptiivinen kaistanhallinta (liikenteen mukaan muuntuvat thresholdit) - Ingress, Egress
X		Kiinteä kaistanhallinta (fixed thresholds) (L3 Frag,src/dst IP, L4 tcp/udp port, icmp, syn)
X		Porttiskannauksen esto (madot yms.)
X		Botnet/DDoS-esto (heuristiikka, algoritmit, riittävä suorituskyky)
X		Source tracking – hyökkäyslähteen identifiointi/esto
X		Protokolla-anomaliat (http, https header)
X		Tila-anomaliat (syn-ack tilat, sekvenssinumeromuutokset jne.)
X		Dark addresses-esto (julkiset ip-alueet, joita ei rekisteröity kenellekään tai eivät aktiivisessa käytössä)
X		Mahdollisuus ohjata liikennettä eri vipeille (source-osoitteen perusteella -> vlan ja/tai dst ip)
X		White/black-listaukset (päästetään läpi ilman muita tarkistuksia/estetään/ohjataan eri vipille)
	X	Autentikointi voimassa / ei voimassa ja ohjaus sen mukaan (jos mahdollista https-paketissa)
X		DNS-palvelujen suojaaminen flooding-hyökkäyksiltä
X		ICMP-liikenteen rajoittamismahdollisuus
X		Kaksi 1 Gbit kupariporttia, joiden läpi liikenne kulkee (in-line)
X		Liikenteen käsittelykyky 1 Gbps
X		Yhtäaikaisten yhteyksien maksimimäärä vähintään 300k
X		Uusia yhteyksiä 50k/sek minimi
X		SynFlood käsittelykyky min. 1Msyns/sek
X		HTTP GET Flood (L7) –esto
X		HA/Stateful failover
X		Poispudotetun liikenteen ohjaamismahdollisuus liikenneanalysaattorille (span/mirror tms.)
verkko-tasolla	X	Joko sisäänrakennettu tai erikseen saatavilla oleva bypass-switch, jolla voidaan suojauslaitteisto ohittaa vikatilanteessa automaattisesti ja manuaalisesti esim. etäyhteydellä
X		Reitittimillä Black holeen/nulliin ohjattavan liikenteen ohjaaminen ja monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
		HTTP Idle timeout 300 sek (DDos) – 360 sek palomuuri (säädetään tarpeen mukaan)
		HTTPS idle timeout 1800 sek (DDos) – 1860 sek palomuuri (säädetään tarpeen mukaan)
		HTTP connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
		HTTPS connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
		DDos-laitteistolla ”roskiin” ohjatun liikenteen monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
X		Lokien ja hälytysten ohjaaminen lokivalvontajärjestelmään

* Erillinen tuote

Radware

Ratkaisu: Radware Defense Pro

Löytyy	Ei löydy	Ominaisuus
X		Syn proxy – tekee tcp-kättelyn, estää syn flood-hyökkäykset
X		Connection limiting – yhteysmäärien rajoitus, estää yhdestä lähteestä tulevat hyökkäykset
X		Connection reset/aging (mahdollisuus resetoida idle-yhteydet, session TTL)
X		Käytösanalyysi ja näkymä liikenteeseen (reaaliaikainen ja historia, baseline)
X		Adaptiivinen kaistanhallinta (liikenteen mukaan muuntuvat thresholdit) - Ingress, Egress
X		Kiinteä kaistanhallinta (fixed thresholds) (L3 Frag,src/dst IP, L4 tcp/udp port, icmp, syn)
X		Porttiskannauksen esto (madot yms.)
X		Botnet/DDoS-esto (heuristiikka, algoritmit, riittävä suorituskyky)
X		Source tracking – hyökkäyslähteen identifiointi/esto
X		Protokolla-anomaliat (http, https header)
X		Tila-anomaliat (syn-ack tilat, sekvenssinumeromuutokset jne.)
API:lla		Dark addresses-esto (julkiset ip-alueet, joita ei rekisteröity kenellekään tai eivät aktiivisessa käytössä)
	X	Mahdollisuus ohjata liikennettä eri vipeille (source-osoitteen perusteella -> vlan ja/tai dst ip)
X		White/black-listaukset (päästetään läpi ilman muita tarkistuksia/estetään/ohjataan eri vipille)
HTTP		Autentikointi voimassa / ei voimassa ja ohjaus sen mukaan (jos mahdollista https-paketissa)
X		DNS-palvelujen suojaaminen flooding-hyökkäyksiltä
X		ICMP-liikenteen rajoittamismahdollisuus
X		Kaksi 1 Gbit kupariporttia, joiden läpi liikenne kulkee (in-line)
X		Liikenteen käsittelykyky 1 Gbps
X		Yhtäaikaisten yhteyksien maksimimäärä vähintään 300k
X		Uusia yhteyksiä 50k/sek minimi
X		SynFlood käsittelykyky min. 1Msyns/sek
X		HTTP GET Flood (L7) –esto
HA	Stateful failover	HA/Stateful failover
	X	Poispudotetun liikenteen ohjaamismahdollisuus liikenneanalysaattorille (span/mirror tms.)
X		Joko sisäänrakennettu tai erikseen saatavilla oleva bypass-switch, jolla voidaan suojauslaitteisto ohittaa vikatilanteessa automaattisesti ja manuaalisesti esim. etäyhteydellä
	X	Reitittimillä Black holeen/nulliin ohjattavan liikenteen ohjaaminen ja monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
X		HTTP Idle timeout 300 sek (DDos) – 360 sek palomuuri (säädetään tarpeen mukaan)
X		HTTPS idle timeout 1800 sek (DDos) – 1860 sek palomuuri (säädetään tarpeen mukaan)
X		HTTP connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
X		HTTPS connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
	X	DDos-laitteistolla ”roskiin” ohjatun liikenteen monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
X		Lokien ja hälytysten ohjaaminen lokivalvontajärjestelmään

TippingPoint

Ratkaisu: TippingPoint IPS

Löytyy	Ei löydy	Ominaisuus
X		Syn proxy – tekee tcp-kättelyn, estää syn flood-hyökkäykset
X		Connection limiting – yhteysmäärien rajoitus, estää yhdestä lähteestä tulevat hyökkäykset
X		Connection reset/aging (mahdollisuus resetoida idle-yhteydet, session TTL)
X		Käytösanalyysi ja näkymä liikenteeseen (reaaliaikainen ja historia, baseline)
X		Adaptiivinen kaistanhallinta (liikenteen mukaan muuntuvat thresholdit) - Ingress, Egress
X		Kiinteä kaistanhallinta (fixed thresholds) (L3 Frag,src/dst IP, L4 tcp/udp port, icmp, syn)
X		Porttiskannauksen esto (madot yms.)
X		Botnet/DDoS-esto (heuristiikka, algoritmit, riittävä suorituskyky)
X		Source tracking – hyökkäyslähteen identifiointi/esto
X		Protokolla-anomaliat (http, https header)
X		Tila-anomaliat (syn-ack tilat, sekvenssinumeromuutokset jne.)
X		Dark addresses-esto (julkiset ip-alueet, joita ei rekisteröity kenellekään tai eivät aktiivisessa käytössä)
	X*	Mahdollisuus ohjata liikennettä eri vipeille (source-osoitteen perusteella -> vlan ja/tai dst ip)
X		White/black-listaukset (päästetään läpi ilman muita tarkistuksia/estetään/ohjataan eri vipille)
	X	Autentikointi voimassa / ei voimassa ja ohjaus sen mukaan (jos mahdollista https-paketissa)
	X	DNS-palvelujen suojaaminen flooding-hyökkäyksiltä
	X	ICMP-liikenteen rajoittamismahdollisuus
X		Kaksi 1 Gbit kupariporttia, joiden läpi liikenne kulkee (in-line)
X		Liikenteen käsittelykyky 1 Gbps
X		Yhtäaikaisten yhteyksien maksimimäärä vähintään 300k
X		Uusia yhteyksiä 50k/sek minimi
X		SynFlood käsittelykyky min. 1Msyns/sek
	X	HTTP GET Flood (L7) –esto
X		HA/Stateful failover
X		Poispudotetun liikenteen ohjaamismahdollisuus liikenneanalysaattorille (span/mirror tms.)
X		Joko sisäänrakennettu tai erikseen saatavilla oleva bypass-switch, jolla voidaan suojauslaitteisto ohittaa vikatilanteessa automaattisesti ja manuaalisesti esim. etäyhteydellä
	X*	Reitittimillä Black holeen/nulliin ohjattavan liikenteen ohjaaminen ja monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
	X	HTTP Idle timeout 300 sek (DDos) – 360 sek palomuuri (säädetään tarpeen mukaan)
	X	HTTPS idle timeout 1800 sek (DDos) – 1860 sek palomuuri (säädetään tarpeen mukaan)
	X	HTTP connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
	X	HTTPS connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
	X*	DDos-laitteistolla ”roskiin” ohjatun liikenteen monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
	X*	Lokien ja hälytysten ohjaaminen lokivalvontajärjestelmään

* Koska laite on transparentti, niin se ei tee liikenteen uudelleenohjausta/reititystä.

Top Layer Security

Ratkaisu: Top Layer IPS 5500

Löytyy	Ei löydy	Ominaisuus
X		Syn proxy – tekee tcp-kättelyn, estää syn flood-hyökkäykset
X		Connection limiting – yhteysmäärien rajoitus, estää yhdestä lähteestä tulevat hyökkäykset
X		Connection reset/aging (mahdollisuus resetoida idle-yhteydet, session TTL)
X		Käytösanalyysi ja näkymä liikenteeseen (reaaliaikainen ja historia, baseline)
X		Adaptiivinen kaistanhallinta (liikenteen mukaan muuntuvat thresholdit) - Ingress, Egress
X		Kiinteä kaistanhallinta (fixed thresholds) (L3 Frag,src/dst IP, L4 tcp/udp port, icmp, syn)
X		Porttiskannauksen esto (madot yms.)
X		Botnet/DDoS-esto (heuristiikka, algoritmit, riittävä suorituskyky)
X		Source tracking – hyökkäyslähteen identifiointi/esto
X		Protokolla-anomaliat (http, https header)
X		Tila-anomaliat (syn-ack tilat, sekvenssinumeromuutokset jne.)
X		Dark addresses-esto (julkiset ip-alueet, joita ei rekisteröity kenellekään tai eivät aktiivisessa käytössä)
	X	Mahdollisuus ohjata liikennettä eri vipeille (source-osoitteen perusteella -> vlan ja/tai dst ip)
X		White/black-listaukset (päästetään läpi ilman muita tarkistuksia/estetään/ohjataan eri vipille)
	X	Autentikointi voimassa / ei voimassa ja ohjaus sen mukaan (jos mahdollista https-paketissa)
X		DNS-palvelujen suojaaminen flooding-hyökkäyksiltä
X		ICMP-liikenteen rajoittamismahdollisuus
X		Kaksi 1 Gbit kupariporttia, joiden läpi liikenne kulkee (in-line)
X		Liikenteen käsittelykyky 1 Gbps
X		Yhtäaikaisten yhteyksien maksimimäärä vähintään 300k
X		Uusia yhteyksiä 50k/sek minimi
X		SynFlood käsittelykyky min. 1Msyns/sek
X		HTTP GET Flood (L7) –esto
X		HA/Stateful failover
X		Poispudotetun liikenteen ohjaamismahdollisuus liikenneanalysaattorille (span/mirror tms.)
X		Joko sisäänrakennettu tai erikseen saatavilla oleva bypass-switch, jolla voidaan suojauslaitteisto ohittaa vikatilanteessa automaattisesti ja manuaalisesti esim. etäyhteydellä
	X	Reitittimillä Black holeen/nulliin ohjattavan liikenteen ohjaaminen ja monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
X		HTTP Idle timeout 300 sek (DDos) – 360 sek palomuuri (säädetään tarpeen mukaan)
X		HTTPS idle timeout 1800 sek (DDos) – 1860 sek palomuuri (säädetään tarpeen mukaan)
X		HTTP connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
X		HTTPS connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
	X	DDos-laitteistolla ”roskiin” ohjatun liikenteen monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
Syslog		Lokien ja hälytysten ohjaaminen lokivalvontajärjestelmään

F5 Networks

Ratkaisu: F5 BIG-IP Viprion

Löytyy	Ei löydy	Ominaisuus
X		Syn proxy – tekee tcp-kättelyn, estää syn flood-hyökkäykset
X		Connection limiting – yhteysmäärien rajoitus, estää yhdestä lähteestä tulevat hyökkäykset
X		Connection reset/aging (mahdollisuus resetoida idle-yhteydet, session TTL)
X		Käytösanalyysi ja näkymä liikenteeseen (reaaliaikainen ja historia, baseline)
X*		Adaptiivinen kaistanhallinta (liikenteen mukaan muuntuvat thresholdit) - Ingress, Egress
X		Kiinteä kaistanhallinta (fixed thresholds) (L3 Frag,src/dst IP, L4 tcp/udp port, icmp, syn)
X		Porttiskannauksen esto (madot yms.)
X**		Botnet/DDoS-esto (heuristiikka, algoritmit, riittävä suorituskyky)
X		Source tracking – hyökkäyslähteen identifiointi/esto
X***		Protokolla-anomaliat (http, https header)
X		Tila-anomaliat (syn-ack tilat, sekvenssinumeromuutokset jne.)
X		Dark addresses-esto (julkiset ip-alueet, joita ei rekisteröity kenellekään tai eivät aktiivisessa käytössä)
X		Mahdollisuus ohjata liikennettä eri vipeille (source-osoitteen perusteella -> vlan ja/tai dst ip)
X		White/black-listaukset (päästetään läpi ilman muita tarkistuksia/estetään/ohjataan eri vipille)
X		Autentikointi voimassa / ei voimassa ja ohjaus sen mukaan (jos mahdollista https-paketissa)
X****		DNS-palvelujen suojaaminen flooding-hyökkäyksiltä
X		ICMP-liikenteen rajoittamismahdollisuus
X		Kaksi 1 Gbit kupariporttia, joiden läpi liikenne kulkee (in-line)
X		Liikenteen käsittelykyky 1 Gbps
X		Yhtäaikaisten yhteyksien maksimimäärä vähintään 300k
X		Uusia yhteyksiä 50k/sek minimi
X		SynFlood käsittelykyky min. 1Msyns/sek
X		HTTP GET Flood (L7) –esto
X		HA/Stateful failover
X*****		Poispudotetun liikenteen ohjaamismahdollisuus liikenneanalysaattorille (span/mirror tms.)
X		Joko sisäänrakennettu tai erikseen saatavilla oleva bypass-switch, jolla voidaan suojauslaitteisto ohittaa vikatilanteessa automaattisesti ja manuaalisesti esim. etäyhteydellä
X		Reitittimillä Black holeen/nulliin ohjattavan liikenteen ohjaaminen ja monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia
X		HTTP Idle timeout 300 sek (DDos) – 360 sek palomuuri (säädetään tarpeen mukaan)
X		HTTPS idle timeout 1800 sek (DDos) – 1860 sek palomuuri (säädetään tarpeen mukaan)
X*****		HTTP connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
X*****		HTTPS connection limit per IP/User/sek – 50 (säädetään tarpeen mukaan)
X*****		DDos-laitteistolla ”roskiin” ohjatun liikenteen monitorointi esim. liikenneanalysaattorin avulla (ohjaus analysaattorille, jossa voidaan liikennettä tarkemmin tutkia)
X		Lokien ja hälytysten ohjaaminen lokivalvontajärjestelmään

* F5 BIG-IP LTM RateShaping + iRule yhdistelmällä
** F5 BIG-IP LTM ASM/PSM yhdistelmällä
*** F5 BIG-IP LTM ASM/PSM + iRule yhdistelmällä
**** F5 BIG-IP + iRule yhdistelmällä
***** F5 BIG-IP LTM + iRule yhdistelmällä