hyväksymispäivä arvosana

arvostelija

Tunkeutumisen havaitseminen

Antti Rantasaari

Helsinki 16. huhtikuuta 2003

Seminaari

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Sisältö

1 Johdanto

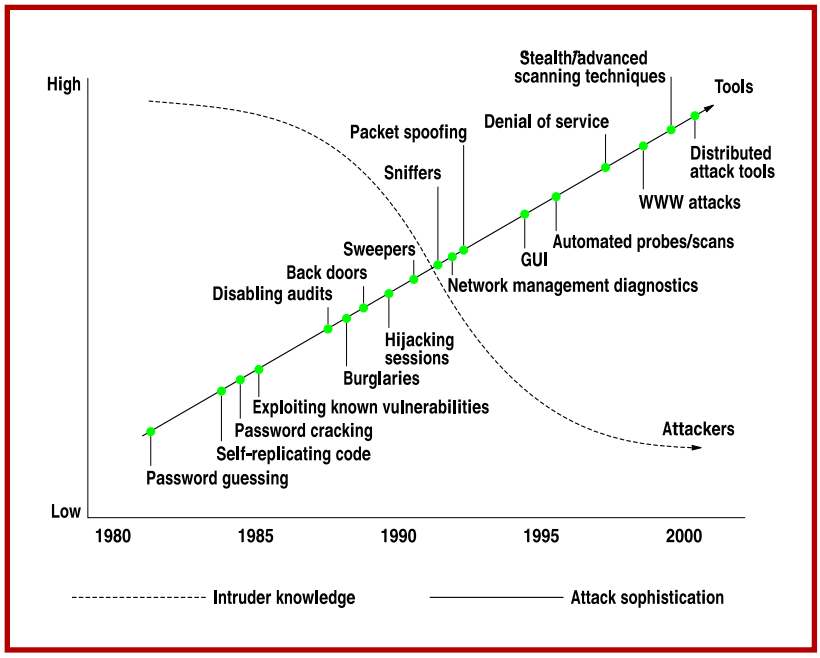
Tietotekniikan, niin laitteiden, ohjelmistojen kuin verkkojenkin, nopea kehitys tarjoaa lukemattomia uusia mahdollisuuksia uuden tekniikan hyödyntämiseen ja väärinkäyttöön. Tietojärjestelmien tulisi tarjota käyttäjille luottamuksellista, eheää ja varmaa palvelua. Tämän saavuttamiseksi järjestelmistä on pyritty kehittämään mahdollisimman turvallisia. Tyypillisiä turvatoimia ovat mm. salasanat, palomuuri ja VPN (Virtual Private Network). Vaikka näillä toimilla palvelun luvatonta käyttöä pystytään vaikeuttamaan, täysin turvallisen järjestelmän kehittäminen on käytännössä mahdotonta. Lisäksi edellämainitut turvatoimet eivät suojaa tietojärjestelmiä järjestelmän sisältä tulevia hyökkäyksiä, joiden on todettu olevan paljon ulkoisia hyökkäyksiä yleisempiä ja vaarallisempia, vastaan.

2 Tunkeutumisen havaitseminen

Turvajärjestelmät, jotka torjuvat luvatonta pääsyä järjestelmään, ovat tärkeitä, mutta tarvitaan myös keinoja havaita tunkeutumisyrityksiä ja korjata mahdollisen hyökkäyksen aiheuttamia vahinkoja. Anderson [A80] ehdotti vuonna 1980 kirjausketjujen käyttöä uhkien tarkkailemiseen ja hyökkäysten paljastamiseen. Ennen Andersonin artikkelia tälläisen datan tärkeyttä ei ymmärretty ja kaikki tietoturvan parantamiseen liittyvät menetelmät keskittyivät pääsyn estämiseen arkaluonteiseen dataan. Andersonin artikkelin katsotaan olleen synty *tunkeutumisen havaitseminen*-käsitteelle ja artikkelin jälkeen on tutkittu ja kehitetty useita tekniikoita sen toteuttamiseen.

2.1 Tarve tunkeutumisen havaitsemiseen

Viime vuosikymmenen aikana tietomurrot ovat kasvaneet nopeaa vauhtia. Täysin luotettavaa tietoa tietomurtojen määrästä ei ole saatavilla, mutta Computer Security Instituten ja FBI:n vuonna 2002 tekemän tutkimuksen mukaan noin 90% yrityksistä oli murron kohteena – vastaava luku vuonna 1996 oli 42% [P02]. Monien asiantuntijoiden mielestä todellisuudessa tapahtuu murtoja kuitenkin vielä enemmän, koska yritykset haluavat vaieta niitä vastaan kohdistuneista tietomurroista. Samalla kun tietomurrot ovat yleistyneet, on hyökkäysyritysten tekemistä helpotettu. 80-luvulla ammattitaitoiset murtautujat käyttivät yksinkertaisia ja yksilöllisiä keinoja murtautumiseen, nykyään lähes kuka tahansa voi yrittää tunkeutua luvatta tietojärjestelmään käyttämällä avukseen kehittyneitä, valmiiksi tehtyjä työkaluja [AMC00]. Kuvassa 1 näkyy kehitys tunkeutujien ammattitaidon ja hyökkäysten hienouden muutoksesta.



Kuva 1: Tunkeutujien ammattitaidon ja hyökkäyksien hienouden muutos [AMC00]

Tunkeutumisyritysten käsittelyyn on olemassa kaksi lähestymistapaa [S96]. Yksi tapa on rakentaa järjestelmä, johon tunkeutuminen on estetty. Voidaan ottaa käyttöön esimerkiksi hyvin tiukka pääsynvalvonta, salata luottamuksellinen tieto ja vaatia käyttäjiä yksilöimään ja varmantamaan itsensä. Lähtökohta ei kuitenkaan yksistään riitä eikä ole toteuttamiskelpoinen, koska

- ei ole käytännössä mahdollista kehittää täysin turvallista järjestelmää mm. ohjelmistoissa ja käyttöjärjestelmissä olevien ohjelmavirheiden takia.
- erilaisten tietojärjestelmien valtava määrä hidastaa siirtymistä turvallisempiin järjestelmiin.
- salaamisessa on omat ongelmansa. Salasanoja voidaan murtaa ja kadottaa sekä kokonaisia salausjärjestelmiä voidaan rikkoa.
- kaikki erittäin hyvinkin suojatut järjestelmät ovat haavoittuvaisia järjestelmän sisältä tulevia hyökkäyksiä vastaan.

Tämän takia perinteisen suojautumisen tueksi tarvitaan muita järjestelmiä. Jos on oletettavaa, että tietomurtoja tapahtuu, on tarpeellista saada niistä mahdollisimman nopeasti tieto, jotta murto pystyttäisiin keskeyttämään tai ainakin murron aiheuttamat vahingot voitaisiin selvittää ja korjata nopeasti. Tunkeutumisen havaitsemisjärjestelmät (Intrusion Detection System, IDS) on kehitetty tätä varten.

2.2 Tunkeutumisen havaitsemisjärjestelmät

IDS-järjestelmät toimivat tutkimalla järjestelmän kirjausketjuja. Koska lähes kaikki järjestelmässä tehtävät toiminnot tallettuvat lokitiedostoihin, voidaan niitä lukemalla selvittää järjestelmään tehdyt tunkeutumisyritykset. Lokitietojen valtavan määrän, mahdollisesti satojen megatavujen, takia manuaalinen tutkiminen

ei ole järkevää, mutta ennalta määriteltyjen ohjeiden perusteella IDS-järjestelmät voidaan automatisoida analysoimaan dataa ja tunkeutumisyrityksen havaitessaan toimimaan halutulla tavalla. Reaaliaikainen lokien seuraaminen on tärkeää, koska ammattitaitoinen tunkeutuja pyrkii peittämään tunkeutumisesta aiheutuneet jäljet, jolloin tunkeutujan havaitseminen on mahdollista vain tunkeutumisen aikana.

Tunkeutujan havaitseminen perustuu oletukseen, että tunkeutujan käytös poikkeaa järjestelmän normaalista käytöstä. Ero normaalin käyttäjän, ylläpitäjän ja tunkeutujan käytöksessä ei välttämättä ole kovinkaan suuri. Mitä tiukemmin kirjausketjuja tulkitaan, sitä suurempi mahdollisuus IDS-järjestelmällä on huomata tunkeutuminen. Toisaalta tiukka tulkinta johtaa suureen määrään vääriä hälytyksiä, jolloin IDS-järjestelmä tulkitsee luvallisen käyttäjän toimet tunkeutumisena.

IDS-järjestelmät toimivat varoittajana tunkeutumisesta, eivätkä välttämättä toimi aktiivisesti tunketumisen torjumiseksi. Ne voidaan asentaa mm. estämään yhteyksiä, tappamaan prosesseja ja muuttamaan palomuurien konfiguraatioita, mutta tämän toteuttamisessa on myös ongelmia. IDS-järjestelmä saattaa tulkita järjestelmän normaalin käytön tunkeutumiseksi, jolloin aktiiviset toimenpiteet saattavat aiheuttaa häiriötä käyttäjille. Esimerkkinä voidaan mainita, että IDS-järjestelmä muuttaa palomuurin estämään verkkoliikenteen tietystä osoitteesta. Jos tunkeutuja on kuitenkin väärentää osoitteensa näyttämään läheisen reitittimen osoitteelta, estää uudelleenkonfiguroitu palomuuri liikenteen reitittimelle, mikä estää verkkoyhteydet reitittimen kautta ja aiheuttaa suurta vahinkoa.

2.3 IDS-järjestelmän toteutustavat

IDS-järjestelmät voidaan toteuttaa joko verkkoasemakohtaisesti tai verkkokohtaisesti [SD02]. Luvussa 3 selvitetään tarkemmin, miten IDS-järjestelmät havaitsevat

tunkeutumisen.

Verkkoasemakohtaisessa ratkaisussa IDS-järjestelmä asennetaan koneille, joiden toimintaa halutaan tarkastella. Koneen lokitiedostoja ja järjestelmän tarkistusagentteja hyväksikäyttäen IDS tarkkailee koneen verkkoliikennettä ja toimintaa epäilyttävien prosessien havaitsemiseksi. Verkkoasemakohtainen ratkaisu on erityisen tehokas sisältä tulevien hyökkäyksien havaitsemiseksi, mutta huonona puolena IDS-järjestelmä täytyy asentaa jokaiseen koneeseen, jonka halutaan kuuluvan tarkkailun piiriin. Lisäksi IDS-järjestelmä käyttää koneella samoja resursseja kuin muutkin ohjelmat, joten kuormitetulla koneella IDS voi aiheuttaa suorituskyvyn voimakasta laskua.

Verkkokohtainen IDS-järjestelmä (Network Intrusion Detection System, NIDS) on asemakohtaista ratkaisua uudempi. Sen ideana on, että verkossa on haluttu määrä koneita, joiden tehtävänä on tarkkailla verkkoliikennettä. NIDS-järjestelmän toteutus vaatii, että verkkomonitorina toimiva kone pystyy nappaamaan kaiken verkossa liikkuvan datan ja tutkimaan sen sisällön etsien datan seasta mahdollisia tunkeutumisyrityksiä. NIDS-järjestelmä on suosittu, koska se on verkkoasemakohtaiseen ratkaisuun verrattuna helppo ottaa käyttöön sekä ylläpitää eikä valvottavien koneiden teho kulu IDS-järjestelmän ajamiseen. Verkkokohtaisen ratkaisun suurin ongelma on, että verkkojen nopeutuessa valvontakoneelle käsiteltäväksi tulevan datan määrä kasvaa huomattavasti. Valvontakoneen resurssit ei välttämättä riitä verkkoliikenteen tehokkaaseen valvontaan ja verkkoa joudutaan osittamaan pienempiin segmentteihin, joilla jokaisella on oma valvontakone.

2.4 IDS-järjestelmän käyttöönotto

Gross [G97] esittää erilaisia tapoja IDS-järjestelmän käyttöönottoon. IDS-järjestelmien sijoituspaikkojen hyvällä valinnalla on tärkeä merkitys niiden optimaalisen tehokkuuden saavuttamiseksi. Gross ehdottaa

- suojaamattomiin koneisiin, jotka eivät kirjoita itse lokia toiminnastaan (esim. Windows 98), konekohtainen järjestelmä
- arkoihin kohtiin verkkoa, kuten sisäänsoittopalvelimen ja palomuurin lähelle, verkkokohtaista IDS-järjestelmää
- palvelinten eristämistä muusta verkosta omaan verkkosegmenttiin, jota valvoo verkkokohtainen IDS-järjestelmä

Koska IDS-järjestelmät eivät itsessään suojaa tietoverkkoa tunkeutumiselta, täytyy ennen niiden käyttöönottoa turvallisuuden perusratkaisut olla kunnossa. Grossin mukaan tietoverkko tulee paloitella moneen osaan tietyille koneille tarvittavien turvavaatimusten perusteella ja sijoittaa palomuurit erottamaan verkkosegmentit. Tämän jälkeen toiminta tulisi testata esimerkiksi haavoittuvuusskannerilla ja mahdolliset tietoturva-aukot pitäisi tukkia. Verkkokohtaisilla IDS-järjestelmillä tutkitaan sen jälkeen verkossa, johon tunkeutujien ei pitäisi päästä, kulkevaa liikennettä ja etsitään tunkeutumisyrityksiä. Konekohtaiset IDS-järjestelmiä tulisi käyttää onnistuneiden tunkeutumisten estämiseksi tärkeillä koneilla.

3 IDS-järjestelmien toiminta

IDS-järjestelmän täytyy kyetä havaitsemaan tunkeutumisyritykset tietojärjestelmän normaalin käytön seasta. Kaksi käytetyintä tunkeutujan havaitsemistapaa

ovat sääntöpohjainen (kappale 3.1) ja tilastollinen (kappale 3.2) havaitseminen. Molemmilla niistä on vahvat ja heikot puolensa. Kappaleessa 3.4 tarkastellaan täysin erilaista ratkaisua, tiedostojen eheyden arviointia (File Integrity Assessment, FIA). Lisäksi IDS-järjestelmiin liittyviä houkuttimia, "hunajapurkkeja", tarkastellaan kappaleessa 3.5.

3.1 Sääntöpohjainen havaitseminen (misuse detection)

Sääntöpohjaisessa havaitsemisessa oletetaan, että hyökkäykset täyttävät tunkeutumiselle tyypilliset tunnusmerkit. Järjestelmään määritellään ennalta tiettyjä sääntöjä, joilla yritetään tunnistaa, onko kyseessä tunkeutujan käytös. Järjestelmä voi myös yhdistellä sääntöjä ja muunnella niitä hieman, jolloin pystytään havaitsemaan myös variaatioita tunnetuista tunkeutumismenetelmistä.

Sääntöpohjainen järjestelmä on tehokas tunnettujen hyökkäysten havaitsemisessa, eikä se aiheuta paljoa vääriä hälytyksiä, koska ilmoitus tunkeutumisesta tehdään vain sääntöihin määriteltyjen toimintojen tapahtuessa. Suurena ongelmana on kuitenkin se, että säännöt täytyy määritellä itse, eikä järjestelmä kykene siten havaitsemaan kokonaan uudenlaisia hyökkäyksiä, koska tunkeutuminen ei täytä mitään järjestelmään määritellyistä tunnusmerkeistä.

3.2 Tilastollinen havaitseminen (anomaly detection)

Tilastollisessa havaitsemisessa lähtökohtaisena oletuksena on, että tunkeutumisyritys poikkeaa järjestelmän normaalista käytöstä. Normaali käyttö määritellään tarkkailemalla järjestelmän toimintaa silloin, kun järjestelmään ei kohdistu hyökkäyksiä. Toisin sanoen, normaaliksi käytöksi tulkitaan ainoastaan tarkkailun aikana tapahtunut tietojärjestelmän käyttö. IDS-järjestelmä tulkitsee normaalin käytön meluksi, ja yrittää havaita verkkoliikenteestä datan, joka ei ole pel-

kästään melua. Tunkeutumisen erottaminen melusta ei ole yksinkertaista. IDS-järjestelmän pohjaksi täytyy rakentaa tilasto tietojärjestelmien normaalista käytöstä, ja tilastoa tulee päivittää jatkuvasti käyttötapojen muuttuessa. Kaikki, mikä ei ole normaalia tilastossa määriteltyä käytöstä, tulkitaan tunkeutumiseksi.

Tilastollisen havaitsemisen suurin etu sääntöpohjaiseen järjestelmään verrattuna on sen kyky havaita kaikki hyökkäykset, ei vain niitä, jotka on osattu järjestelmään määritellä. Toisaalta kaikkea järjestelmien normaalia, sallittua käyttöä ei ole mitenkään voitu tilastoida IDS-järjestelmään. Toimintatavastaan johtuen tilastollisella järjestelmällä on kaksi suurta heikkoutta - normaali, poikkeava käyttö tulkitaan tunkeutumiseksi, mikä aiheuttaa suuren määrän vääriä hälytyksiä sekä tunkeutuminen, joka ei poikkea normaalista käytöstä, jää huomaamatta. Erityisesti jälkimmäinen näistä on vaarallista.

Määritelmä-perusteinen havaitseminen on samantapainen kuin tilastollinen havaitseminen. Erona on se, että tietojärjestelmän sallittua käyttöä ei määritellä tarkkailemalla järjestelmän toimintaa, vaan määrittelemällä normaaliksi käytöksi kaikki sallittu tietojärjestelmän käyttö, ei pelkästään aiemmin nähty käyttö. Hyötynä on se, että väärien hälytysten määrää saadaan vähennettyä huomattavasti, koska ennennäkemätöntä käyttöä ei aina tulkita tunkeutumiseksi. Toisaalta suuri ongelma on sallitun käytön määrittely, mikä saattaa olla paljon aikaa vaativaa työtä.

3.3 IDS-järjestelmien kehitys

Uusia, tehokkaampia IDS-järjestelmiä on kehitetty yhdistämällä sääntöpohjaisen ja tilastollisen havaitsemisen vahvoja puolia yrittäen samalla eliminoida heikkouksia. Nykyisten järjestelmien ongelmana on se, että ne ovat kykeneviä havaitsemaan ammattitaidottomien tunkeutujien yritykset, mutta ammattitaitoiset

tunkeutumiset jäävät huomaamatta [AMC00]. Usein juuri nämä aiheuttavat suurimman uhkan yrityksille.

IDS-järjestelmät pystyvät havaitsemaan tunkeutumisia, mutta toisaalta tuottavat myös paljon vääriä hälytyksiä, mikä saattaa lannistaa tietoturvasta vastuussa olevia työntekijöitä. Jos vääriä hälytyksiä on liikaa, ei niihin kiinnitetä enää tarpeeksi huomiota ja todelliset hyökkäykset saattavat hukkua väärien hälytysten sekaan.

Väärien hälytysten määrän vähentämiseen ja havaitsemiskyvyn parantamiseen on pystytty esimerkiksi ratkaisulla [Setal02], jossa on yhdistetty tilastollinen havaitseminen ja määritelmä-perusteinen havaitseminen. Määrittelyprotokollan avulla tehtävä tilastointi ja määrittely paitsi tekee tehtävänsä tehokkaasti, myös helpottaa normaalisti tilastollisen havaitsemisen käyttöönottoa edeltävää manuaalista normaalin käytön määrittelyä.

3.4 Tiedostojen eheyden arviointi

Tiedostojen eheyden arvioinnilla tarkoitetaan järjestelmä- ja sovellustiedostojen ja mahdollisesti rekistereiden tarkastelua. FIA-ohjelmistot tekevät tämän tallettamalla tietokantaan puhtaan järjestelmän alkutilanteen – sen miltä järjestelmän pitäisi näyttää. Tämä tehdään tavallisesti tallettamalla tarkkailtavien objektien nimet ja niiden kryptografiset tiivisteet ("hash-arvo). Tämän jälkeen objektien muuttaminen on mahdotonta tekemättä tiivistettä vialliseksi. Tasaisin väliajoin FIA-ohjelmistot tekevät tarkkailtavista objekteista uudet tiivisteet ja vertaavat niitä alkuperäisiin arvoihin.

Mikäli tunkeutuja onnistuu pääsemään järjestelmään ja tekemään muutoksia tarkkailtaviin objekteihin, huomaa FIA-ohjelmisto sen seuraavalla kerralla tiivisteitä vertaillessaan ja aiheuttaa hälytyksen. Tämä tekee tiedostojen eheyden arvioinnista erittäin hyvän apuvälineen tapahtuneen hyökkäyksen vahinkojen

selvittämiseen, koska kaikki tärkeät, muutetut, objektit voidaan löytää helposti. Huonona puolena FIA-järjestelmässä on se, että tarkkailu tehdään tietyin väliajoin eikä tosiaikaisesti. Sen takia siitä ei ole apua, mikäli tarvitaan tosiaikaista tunkeutumisen havaitsemiskykyä ja hyökkäys halutaan torjua ennen kuin vahinkoa pääsee syntymään.

3.5 Houkuttimet (honeypots)

Houkuttimella tarkoitetaan järjestelmää, jonka tehtävänä on harhauttaa tunkeutujaa murtautumaan siihen eikä varsinaiseen tietojärjestelmään. Ulospäin houkutin näyttää murtautujalle kiinnostavalta kohteelta, mutta se ei sisällä mitään tärkeää dataa. Houkutin voidaan asentaa varsinaisen tietoverkon ulkopuolelle, jolloin sen kautta jatkomurtautuminen ei helpotu, ja siihen voidaan tarkoituksella asentaa vanhentuneita ohjelmistoja, jotta houkuttimeen murtauminen helpottuisi. Tarkoituksena on, että houkutin kirjaa lokiin kaiken koneella tapahtuvan toiminnan.

Houkuttimen avulla on mahdollista saada aikaisia varoituksia murtautumisyrityksistä. Koska tunkeutuja saattaa erehtyä luulemaan haluamakseen kohteeksi, varoitus tunkeutumisaikeista saadaan ennen kuin tunkeutuminen kohdistuu varsinaiseen, suojattuun tietojärjestelmään. Tämä antaa tietoturvasta vastuussa oleville henkilöille viitteitä käytössä olevista murtautumismenetelmistä ja mahdollisuuden varautua niihin.

4 Tunkeutumisen havaitsemisohjelmistoja

Markkinoilla on useita tarjolla useita erilaisia IDS-ohjelmistoja, sekä kaupallisia että vapaasti levitettäviä. Tarjolla olevista ohjelmistoista osassa on toteutettu to-

siaikainen tunkeutumisen havaitseminen ja osassa havaitseminen suoritetaan jälkikäteen. Koska tunkeutumisen havaitseminen on suhteellisen uusi tekniikka, ovat myös markkinat kehittymättömät eikä varsinaisia laatustandardeja tai ohjelmistojen tehokkuutta painoteta läheskään yhtä paljon kuin itse markkinointia. Tuotteet muuttuu jatkuvasti, uusia ohjelmistoja saapuu markkinoille ja vanhoja poistuu.

Tässä luvussa esitellään esimerkinomaisesti kolme erilaista saatavilla olevaa ohjelmistoa. Internet Security Systems RealSecure ja Snort ovat tosiaikaiseen tunkeutumisen havaitsemiseen kykeneviä ohjelmistoja. Niiden tehokkuutta tarkastellaan lopuksi NSS Groupin [NSS] suorittaman IDS-ohjelmistotutkimuksen avulla. Tripwire on havaitsemisen jälkikäteen tekevä ohjelmisto. Muita saatavilla olevia IDS-ohjelmistoja, joita ei tässä esitellä, ovat mm. Cisco Secure IDS, Entercept, NFR HID, ja Okena Stormwatch.

4.1 Internet Security Systems RealSecure

RealSecure oli ensimmäisiä kaupallisia IDS-ohjelmistoja, jota pidetään vieläkin jonkinlaisena standardina IDS-ohjelmistoille. Se on tosiaikainen IDS-järjestelmä, joka käyttää kolmiosaista arkkitehtuuria. Se koostuu verkkotason tunnistuskoneesta, konekohtaisesta tunnistuskoneesta sekä hallintamoduulista. Hallintamoduulin avulla IDS-järjestelmän kaikkia osia pystytään tarkkailemaan ja asetuksia pystytään muuttamaan, mikä helpottaa järjestelmän konfiguroimista tunkeutumisten tehokkaaseen havaitsemiseen.

Verkkotason tunnistuskone toimii sille tarkoitetulla koneella kyeten siten verkkokohtaiseen tunkeutumisen havaitsemiseen. Järjestelmä mahdollistaa verkon jakamisen erillisiin segmentteihin, joilla jokaisella on oma verkkokohtainen IDS-koneensa. Reagointi havaittuun tunkeutumiseen on ylläpitäjän määriteltävissä,

mahdollisia toimintoja ovat mm. tunkeutuvat yhteyden katkaiseminen, hälytyksen lähettäminen hallintamoduulille, istunnon taltioiminen ja palomuurin asetusten muuttaminen.

Konekohtainen tunnistuskone analysoi kirjausketjuja etsien merkkejä tunkeutumisesta ja turva-aukoista hyökkäysten havaitsemiseksi. Konekohtainen tunnistuskone voi keskeyttää tunkeutumisen tappamalla prosesseja tai lakkauttamalla käyttäjätunnuksia. Myös samat toimenpiteet kuin verkkotason tunnistuskoneella ovat mahdollisia.

4.2 Snort

Snort on vapaasti levitettävä, vapaan lähdekoodin ohjelmisto, joka on kehitetty kevyeksi ja tehokkaaksi IDS-järjestelmäksi ennen kaikkea Unix/Linux-järjestelmiin, mutta nykyään ohjelmistosta on saatavana versio myös Windows-alustalle. Snort on tosiaikainen verkkokohtainen IDS-järjestelmä, joka muodostuu kolmesta osasta – pakettien dekoodaajasta, havaitsemiskoneesta sekä kirjaus- ja hälytysosasta.

Pakettien dekoodaaja ja havaitsemiskoneesta, jotka kykenevät yhteistyössä verkkoliikenteen analysointiin, pakettien kirjaamiseen IP-verkossa, protokolla-analyysiin, sisällön tutkimiseen ja sitä voidaan käyttää erilaisten hyökkäysten, kuten puskurin ylivuodon, piilotettujen porttiskannausten ja käyttöjärjestelmän tutkimisen havaitsemiseen. Havaitsemiskoneella on konfiguroitu tunkeutumisen havaitsemisessa käytettävät säännöt ja jokainen verkossa kulkeva paketti tarkistetaan sääntöjen perusteella. Mikäli paketti ei vastaa mitään määritellyistä säännöistä, se hylätään. Kirjaus- ja hälytysjärjestelmä toimii dekoodaajalta tai havaitsemiskoneelta tulleiden käskyjen perusteella.

Snort kehitys on hyvin nopeaa, koska sen lähdekoodi on vapaa ja lukuisat sen ke-

hittämisestä kiinnostuneet käyttäjät pystyvät osallistumaan kehitystyöhön. Siitä syystä Snort on usein ensimmäinen ohjelmisto, johon uusimpien hyökkäysten tunnismerkit pystytään lisäämään. Tämä tekee Snortista tehokkaan IDS-järjestelmän, joka on usein askeleen kilpailijoita edellä.

4.3 Tripwire

Tripwire on tiedostojen eheystarkistukseen tarkoittettu ohjelma, josta on olemassa sekä kaupallinen että vapaasti levitettävä versio. Tripwire luo kriittisistä järjestelmätiedostoista tietokannan, joka sisältää tiedostojen pituudet sekä niiden sisällön perusteella tehdyt tarkistussummat. Tietokannan perusteella Tripwire tarkistaa, onko tiedostoihin tehty muutoksia ja ilmoittaa mahdollisista muutoksista käyttäjälle. On käyttäjän vastuulla päättää, johtuuko tiedoston muuttuminen tunkeutumisesta vai esimerkiksi uuden ohjelmiston asentamisesta. Järjestelmätiedostojen ei muuten pitäisi muuttuua, joten muutos on usein selvä merkki tunkeutumisesta tai luvattomasta käytöstä. Tripwire ei tee muuta kuin ilmoittaa muutoksista.

4.4 IDS-järjestelmien testaus

NSS Group suoritti vuonna 2002 IDS-järjestelmien toimivuustestin. Testissä selvitettiin useita IDS-järjestelmän toimintaan liittyviä asioita, mutta seuraavassa tarkastellaan ainoastaan Snortin ja RealSecuren kykyä havaita tunkeutumisyrityksiä. Testiympäristönä toimineeseen verkkoon asennettiin usealle koneelle IDS-sensorit ja lisäksi yhdelle koneelle hallintakonsoli toiminnan seuraamiseen. Tarkemmat tiedot testiympäristöstä ja testin tuloksista NSS Groupin www-sivuilla [NSS].

Hyökkäyksen tunnistamistestissä ajettiin useita tunnettuja hyökkäyksiä käyttäen

erilaisia työkaluja sekä testiä varten kehitettyjä C-ohjelmia ja skriptejä. Hyökkäystekniikoita oli useita. Kaikki hyökkäykset kohdistettiin testiverkossa oleville erilaisia käyttöjärjestelmiä käyttäville koneille.

RealSecure selviytyi testistä hyvin. Sen tunkeutumisen havaitsemiskyky oli erinomainen ja se toimi hyvin myös raskaasti kuormitetussa verkossa. RealSecure, jonka helppokäyttöisellä hallintamoduulilla ylläpitäjä pystyy valvomaan ja konfiguroimaan useilla eri koneilla olevia IDS-sensoreita, todetiin testissä erittäin hyväksi ohjelmistoksi. Ohjelmistoa on myös automatisoitu melko paljon, mikä vähentää huomattavasti ylläpitäjän työtä. Kuva 2 esittelee tarkemmin RealSecuren kyvyn havaita tunkeutumisia.

NIDS Test 1 – Attack Recognition	Attacks	Detected
Application bugs	5	4
Back Doors/Trojans/DDOS	11	9
DOS	16	13
Finger	7	7
FTP	11	11
HTTP	18	15
ICMP	2	0
Mail	7	6
Malicious Data Input	3	2
Reconnaissance	10	8
SNMP	2	2
SANS Top 20 (network-based attacks only)	17	17
Total	**109**	**94**

Kuva 2: RealSecure – hyökkäysten tunnistaminen [NSS]

Snortia mainostetaan sopivana työkaluna pienten verkkojen IDS-järjestelmäksi, mutta NSS:n testissä ohjelmiston havaittiin kykenevän tehokkaaseen tunkeutumisen havaitsemiseen myös isossa verkkoympäristössä. Ohjelmiston tunkeutumisen havaitsemiskyky todettiin hyväksi ja pienellä lisävaivalla oletusasetuksia muuttamalla havaitsemiskykyä pystyisi parantaa. Ohjelmiston hallinta on kuitenkin melko vaivalloista ja vaatii ylläpitäjältä suhteellisen paljon ammattitaitoa ja aikaa tehokkaan järjestelmän saamiseksi optimaaliseksi. Myös hälytysten kä-

sittely jää täysin ylläpidon vastuulle. Snortin kykyä havaita tunkeutumisia esitellään tarkemmin kuvassa 3.

NIDS Test 1 – Attack Recognition	Attacks	Detected
Application bugs	5	4
Back Doors/Trojans/DDOS	11	11
DOS	16	10
Finger	7	6
FTP	11	6
HTTP	18	12
ICMP	2	2
Mail	7	4
Malicious Data Input	3	1
Reconnaissance	10	5
SNMP	2	0
SANS Top 20 (network-based attacks only)	17	13
Total	**109**	**74**[3]

Kuva 3: Snort – hyökkäysten tunnistaminen [NSS]

5 Yhteenveto

IDS-järjestelmät ovat tarkoitettuja tunkeutumisen havaitsemiseen eivätkä ne itsessään tarjoa usein minkäänlaista suojaa tunkeutumisia vastaan. Ne antavat ainoastaan ilmoituksen mahdollisesta tunkeutumisesta sellaisen havaitessaan. IDS-järjestelmien käyttöönotto yrityksissä on täysin turhaa, mikäli niiden toimintaa ei ymmärretä eikä niiden käyttöön osata resursoida tarpeeksi voimavaroja. Annetusta tunkeutumishälytyksestä ei ole mitään hyötyä, ellei joku osaa ja ehdi toimia hälytyksen tullessa sopivalla tavalla.

Lähteet

AMC00 Allen, J., McHugh, J., Christie, A., Defending Yourself: The Role of Intrusion Detection Systems. *IEEE Software* September/October (2000)

A80 Anderson, J. P., Computer Security Threat Monitoring and Surveillance. Technical Report, James P Anderson Co., Fort Washington, Pennsylvania, (1980)

G97 Gross, A., Analyzing Computer Intrusions. Ph.D. thesis, University of California, Department of Computer Science, San Diego, CA, (1997)

KS94 Kumar, S., Spafford, E., A Pattern matching Model for Misuse Intrusion Detection. *Proceedings of the Seventeenth National Computer Security Conference* Baltimore, MD (1994)

MHL94 Mukherjee, B., Heberlein, L., Levitt, K., Network intrusion detection. *IEEE Network* May/June (1994)

NSS The NSS Group, http://www.nss.co.uk/ *IDS Group Test (Edition 1)* (2002)

P02 Power, R., 2002 CSI/FBI Computer Crime and Security survey. *Computer Security Issues and Trends* (2002)

Setal02 Sekar, R., Gupta, A., Frullo J., Shanbhag, T., Tiwari, A., Yang, H., Zhou, S., Specification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. *Proceedings of the 9th ACM conference on Computer and communication security* 265-274 (2002)

SD02 Sherif, J., Dearmond, T., Intrusion Detection: Systems and Models. *Proceedings of the eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises* June (2002)

S96 Sundaram, A., An Introduction to Intrusion Detection. *Crossroads: The ACM Student Magazine*, 2, 2 (1996)