Jere Alanko-Luopa

Yritysverkon monitorointi avoimen lähdekoodin avulla

Security Onion

Opinnäytetyö
Kevät 2019
SeAMK Tekniikka
Insinööri (AMK), Tietotekniikka

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Tietotekniikka

Suuntautumisvaihtoehto: Tietoverkkotekniikka

Tekijä: Jere Alanko-Luopa

Työn nimi: Yritysverkon monitorointi avoimen lähdekoodin avulla

Ohjaaja: Alpo Anttonen

Vuosi: 2019 Sivumäärä: 52 Liitteiden lukumäärä: 0

Tutkimuksessani selvitettiin, miten verkonvalvonta tapahtuu yritysverkossa ja miten sitä sovelletaan avoimen lähdekoodin avulla. Tutkimuksen ideana oli opetella ja tutkia avoimen lähdekoodin ohjelmistoja sekä niiden käyttöä. Opinnäytetyössä asennettiin sekä konfiguroitiin Security Onion -niminen ohjelmisto yrityksen verkkoon sekä sitä käytettiin verkkoliikenteen tutkimiseen.

Opinnäytteen teoriaosuus sisältää yleistä teoriaa verkon valvonnasta sekä tunkeilun havainnointijärjestelmistä. Niiden erilaiset toimintamallit avataan lukijalle, ja teoriaosuudessa kerrotaan myös verkkohyökkäyksistä sekä eritellään hieman kustannuksien muodostumista verkonvalvontaympäristössä.

Tutkimuksen käytännön osuudessa asennetaan Security Onion, sekä kerrotaan ohjelmiston ominaisuuksia ja käytäntöjä. Ohjelmiston asennus kuvataan pääpiirteittäin sekä kerrotaan ongelmat ja mahdolliset ratkaisut.

Lopuksi käydään läpi tutkimuksessa ilmi tulleita ongelmia sekä asennusvaiheita. Tutkimuksen tarkoitus oli saada Security Onion-ohjelma asennettua sekä käytettyä sitä yritysympäristössä. Tämä tapahtui onnistuneesti, mutta jäi hieman vaiheeseen ongelmien vuoksi.

Avainsanat: Verkonvalvonta, Security Onion, Tietoturva, Tunkeutumisen Havainnointi, Yritysverkko

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Networking Technology

Author: Jere Alanko-Luopa

Title of thesis: Company Network Monitoring with Open Source

Supervisor: Alpo Anttonen

Year: 2019 Number of pages: 52

The idea behind this thesis was to study how network monitoring works in a company network and how it would be possible to implement it with open source software. The purpose of the thesis was to research and learn about the functionality and methods of open source software. In this thesis, Security Onion was installed and configured to work in a company network and it was in use for network monitoring.

The theory part of the thesis concentrated on the common theory of network monitoring and intrusion detection and prevention. Different approach styles of network monitoring were also presented. Attention was also paid to network attacks and it was studied what is causing the costs in network monitoring.

Installation of the Security Onion was done in the practical part. This part also provided information on the properties and methods of the Security Onion. The installation part was outlined and there was information on the problems and solutions.

The results and further actions for possible continuing of this work are at end of the thesis. The primary goal of the thesis was to install and use the Security Onion-software successfully in a company network. This goal was achieved, even though a few problems appeared during the installation of the Security Onion.

Keywords: network monitoring, Security Onion, information security, intrusion detection, company network

SISÄLTÖ

Kuvaluettelo

Käytetyt termit ja lyhenteet

Agentti	Laitteelle asennettava sovellus, joka lähettää dataa hallintakonsolille.
ANSI	American national standards institute.
API	Application programming interface, ohjelmarajapinta. Rajapintaa käytetään ohjelmoinnissa noudattaen tiettyjä kaavoja.
CIPP/E	Certified Information Privacy Professional/Europe. Sertifikaatti todistaa kattavan GDPR-tietämyksen sekä ymmärryksen tietosuojan noudattamisesta Euroopassa.
DMZ	Ylimääräinen tietoturvataso organisaation lähiverkossa. Lähiverkkoon luodaan oma aliverkko laitteille, jotka ovat yhteydessä julkiseen verkkoon, kuten DNS-palvelimet.
DNS	Domain Name System. Nimipalvelujärjestelmä, joka muuttaa verkkotunnukset IP-osoitteeksi.
FTP	File Transfer Protocol. Mahdollistaa tiedostojen siirron kahden eri laitteen välillä, kuten palvelin ja tietokone.
GDPR	General Data Protection Regulation. Henkilötietojen käsittelyä sääntelevä laki.
HIDS	Host-based intrusion detection system. Laitepohjainen tunkeilun havainnointijärjestelmä, jonka tarkoitus on ilmoittaa epäilyttävästä toiminnasta, esimerkiksi tietokoneella.
HTTP	Hypertext Transfer Protocol on protokolla, jota WWW-palvelimet ja selaimet käyttävät tiedonsiirtoon.
Intranet	Organisaation lähiverkko, jota yleisesti käytetään viestintään sekä tiedostojen jakoon.

IPS	Intrusion prevention system, tunkeilun estojärjestelmä. Järjestelmä havaitsee ja sitten estää yrityksen verkkoon tulevan tunkeilun, esimerkiksi palomuurin haavoittuvuuden takia.
ISO	International Organization for Standardization. Kansainvälinen standardisoimisjärjestö, joka luo maailmanlaajuisesti suositeltuja standardeja.
MIB	Management Information Database. Tietokanta, jota SNMP-protokolla käyttää lukiessaan laitteen tietoja.
NIDS	Network-based intrusion detection system. Verkkopohjainen tunkeilun havainnointijärjestelmä.
Netsniff-ng	Verkkoliikenteen analysointi- sekä tutkimistyökalu.
PCAP	Packet capture API. Ohjelmointirajapinta verkkoliikenteen pakettien kaappaukseen.
Ransom	Termi, jota käytetään lunnaita vaatiessa. Tässä työssä tiedostojen lukitus ja niiden avauksesta pyydettävä maksu.
SHA	Secure Hash Algorithms. Salasanojen salaukseen tarkoitettu algoritmi, jonka avulla tietokantaan tallennettavat salasanat suojataan.
SNMP	Simple Network Management Protocol. Protokolla, jota käytetään verkon monitorointiin.
SMTP	Simple Mail Transfer Protocol. Protokolla, jonka avulla sähköpostipalvelimet lähettävät viestit.
SQL	Structured Query Language. Relaatiotietokannan käsittely- / sekä hakustandardi.
SSH	Secure Shell. Salattu tietoliikenneyhteys, esimerkiksi tietokoneelta kytkimeen. Käytetään etäyhteyksissä.

SSL	Secure Sockets Layer. Salausprotokolla, jolla suojataan tietoliikenne IP-verkkojen yli.
TCP	Transmission Control Protocol. Protokolla, jonka avulla kaksi tietokonetta luo yhteyden toisiinsa.
USM	User-Based Security Model. Luotu SNMPv3-protokollalle turvallisuusjärjestelmä pääsynhallintaan sekä viestien siirtoon.

1 JOHDANTO

1.1 Tutkimuksen tausta

Tutkimus keskittyy erittäin keskeiseen aiheeseen eli verkonvalvontaan. Verkonvalvonta ja verkonturvallisuus ovat tärkeitä asioita yrityksissä, joten aihetta ei voi väheksyä tai sivuuttaa. Tiukentuneet lait tietosuojan saralla lisäävät verkonvalvonnan tärkeyttä, joten monet yritykset ovat vailla toimivia ratkaisuja verkon sekä laitteiden suojaksi. Erilaisia valmiita tuotteita on jo tarjolla, mutta osa automatisoiduista verkonvalvontapaketeista ovat kustannuksiensa puolesta mahdottomia pienille tai keskisuurille yrityksille.

Verkonvalvonta on erittäin tärkeässä osassa, jos ja kun verkkohyökkäyksiä tulee. Ilman hyviä suojauksia hyökkäyksistä ei mahdollisesti jää jälkeäkään ja on mahdotonta selvittää tapahtumia. Verkon ja laitteiden monitorointi sekä ilmoitukset lokitiedoista myös pitävät palvelut toiminnassa, eikä aikaa käytetä vikojen etsimiseen.

Pienillä tai keskisuurilla yrityksillä on usein tietoturvassa aukkoja, koska yritysten resursseja täytyy jakaa maltilla. Usein keskitytään tulokseen ja tästä johtuvaan kiireeseen, eikä muisteta tietoturvaa tai yrityksen yleisiä ohjeita laitteiden käytöstä. Kun yritys kasvaa, nousee kiinnostus yritystä kohtaan myös rikollisilla ja mahdolliset hyökkäykset aiheuttavat joko vahinkoa laitteille, tai mahdolliset tietovuodot asiakastiedoista tai sopimuksista voivat aiheuttaa yritykselle sakon tai korvauksen maksettavaksi.

Tutkimuksen aiheen ehdotus tuli yritykseltä Opsec Oy. Tutkimuksessa käytetään Security Onion -nimistä ohjelmistoa, eikä työssä tehdä erilaisten ohjelmistojen vertailua. Työ on tutkimus, eikä Security Onion käyttöohje, joten tutkimuksessa on yleistä teoriaa verkonvalvonnasta ja Security Onion-ohjelman asennus sekä testaus yritysympäristössä. Asennus- ja testausvaihe on kerrottu pääpiirteittäin, jotta lukijalle tulisi käsitys siitä, miten ohjelman asennus sekä toiminta tapahtuu.

1.2 Tutkimuksen tavoite

Tutkimuksessa tarkoituksena on kertoa lukijalle verkonvalvonnasta sekä testata konkreettisesti Security Onion-ohjelmistoa yrityskäytössä. Tavoitteena on saada lokitietoja tietokoneelta palvelimelle asennettuun Security Onioniin sekä saada lukijalle käsitys verkonvalvonnasta ja sen periaatteista sekä toimitavoista.

1.3 Työn rakenne

Työssä käsitellään ensin luvussa kaksi yleisesti verkonvalvontaa ja sen periaatteita. Tämän jälkeen kerrotaan luvussa kolme Security Onion-ohjelmistosta sekä sen komponenteista. Neljännessä luvussa käydään läpi Security Onion asennus sekä erillisen laitteen valvonnan edellyttävän ohjelman asennus. Viidennessä luvussa kerrotaan kirjoittajan mietteitä työstä sekä työn jatkokehityksestä.

1.4 Opsec Oy

Opsec Oy on eteläpohjalainen IT-alan yritys, joka perustettiin vuonna 2009 ja se työllistää tällä hetkellä 11 työntekijää. Opsec Oy on kotimainen ja yksityisessä omistuksessa oleva asiantuntijayritys. Yritys toimii koko Suomen alueella ja varsinainen toimipiste on Seinäjoella. Yrityksen toimialoihin kuuluu tietoturvan, tietosuojan sekä tietohallinnon johtamis- ja asiantuntijapalvelut. Tietosuojan saralla Opsec Oy:llä on vankkaa osaamista ja esimerkkinä siitä on tietosuojavastaavan ANSI/ISO-akkreditoitu CIPP/E-sertifikaatti. Yritys tuottaa myös IT-toimintojen ylläpito- ja tukipalveluita sekä tietoturvan puolella tietoturvatestauksia ja riskien arviointia. (Opsec Oy 2019, Yritys.)

Tietoturvatestaus on yrityksen ympäristöön tehtävä haavoittuvuuksien todennus. Mahdollisia haavoittuvuuksia ovat esimerkiksi päivitykset, vääränlaiset asetukset sekä puutteelliset suojaukset. Mahdollisia tietoturvatestauksen kohteita ovat palve-

limet, työasemat, lähiverkon aktiivilaitteet, kamerajärjestelmät sekä toiminnanohjausjärjestelmät. Lisäksi myös julkisessa verkossa olevia www-palvelimia tai palomuureja voidaan testata. Tietoturvatestaus sisältää raportin tietoturvan tasosta, havaitut haavoittuvuudet, korjausohjeet haavoittuvuuksien korjaamiseksi sekä toistuvan testauksen. Tietoturvatestaus on hyvä keino varmistua yrityksen verkon turvallisuudesta, testauksen jälkeen yhtiö täyttää tietosuoja-asetuksen tietoturvallisuuden osuuden. (Opsec Oy 2019, Tietoturvatestaus.)

Opsec Oy:llä on myös turvallisuusalan elinkeinolupa sekä FINCSC-kyberturvallisuussertifikaatti. FINCSC-sertifikaatilla Opsec Oy on hyväksytty tarjoamaan sertifiointipalveluja muille yrityksille. Opsec Oy toimii myös Fortinet Authorized -partnerina ja Fortinet-palomuurien välittäjänä sekä asiantuntijana. (Opsec Oy 2019. Yritys.)

Opsec Oy on myös julkaissut tietosuojaoppaan pienille yrityksille, jonka. (Opsec Oy 2019, Tietosuojapalvelut.)

2 VERKONVALVONTA JA SEN PERIAATTEET

2.1 Verkonvalvonta

Verkonvalvonnalla tarkoitetaan verkkoliikenteen tutkimista ja seuraamista sekä verkossa olevien laitteiden tilojen monitorointia. Mahdollisia toimenpiteitä, esimerkiksi tunkeutujan havaitsemisesta, voidaan aktivoida automaattisesti tai vastaavasti odotetaan verkonvalvontatyökalun ilmoitusta ja reagoidaan siihen. Näistä useimmin käytetään sekoitusta: Palveluiden ja laitteiden tilat otetaan ilmoituksena sähköpostiin tai puhelimeen. Verkkohyökkäys sen sijaan aktivoi suojaustoimenpiteen, esimerkiksi yhteyden katkaisun tai palvelimen sulkemisen automaattisesti. Tällöin nimitykseksi voidaan vaihtaa IDPS eli Intrusion Detection and Prevention System. (Scarfone & Mell 2007, 15.)

2.2 Käyttötarkoitus

IDPS-ohjelmistoja hyödynnetään yrityksissä silloin, kun halutaan seurata yrityksen sisäverkon liikennettä. IDPS-ohjelmistolla pystytään havaitsemaan erinäistä liikennettä ja aktiivisuutta verkossa, kuten ison tietokannan kopiointi tai kopiointiyritys, eri porttien skannaus tai tiedostojen siirto IP-osoitteeseen, joka ei kuulu yrityksen sääntöjen sallimaan listaan. (Scarfone & Mell 2007, 15.)

IDPS kerää lokitietoja mahdollisista uhista sekä hyökkäyksistä ja oppii näin tuntemaan, miten usein hyökkäyksiä tulee ja millaisia hyökkäykset ovat. Nämä lokitiedot ovat hyödyllisiä verkon turvallisuuden suunnittelussa ja lokitietoja lukemalla päätetään minkä tyyppisiä suojausmenetelmiä yritys tarvitsee. (Scarfone & Mell 2007, 15-16.)

IDPS pystyy tutkimaan verkkoliikenteen sääntöjä, jotka on asetettu palomuurilta. Jos verkossa on liikennettä, joka on estetty palomuurilta haitallisuuden vuoksi, IDPS ilmoittaa siitä ja verkonhallitsija voi korjata ongelman palomuurin asetuksiin. Vastaavat ongelmat voivat johtua palomuurin konfiguroinnissa olevasta virheestä. (Scarfone & Mell 2007, 16.)

Verkonvalvontatyökalut ovat myös passiivisia auttajia, koska työntekijät ovat varovaisempia verkossa, jos heille on informoitu verkonvalvontatyökalun olemassa olosta. Myös työntekijät, jotka liikkuvat epäilyttävillä sivuilla tai mahdollisesti rikkovat työpaikan sääntöjä verkkokäyttäytymisellä, pelkäävät kiinni jäämistä ja lopettavat työpaikan laitteiden vaarantamisen. (Scarfone & Mell 2007, 16.)

2.3 Tärkeimmät toiminnot IDPS-ohjelmassa

IDPS-ohjelman tärkein toiminto on tietenkin liikenteen tutkiminen ja sen monitorointi. Tämä koostuu eri toimenpiteistä, jotka riippuvat monitoroidun liikenteen laadusta.

Raportointi. Laitteiden ja verkon monitoroinnista syntyy lokitietoja, joista kehittyneet IDPS-ohjelmat muodostavat raportteja sekä jopa visuaalisia, reaaliaikaisia näkymiä. Näiden raporttien ja ilmoitusten luominen kuuluu IDPS-ohjelman erinomaisiin puoliin. (Scarfone & Mell 2007, 16.)

Hyökkäykset. Ohjelman tarkoitus on myös estää hyökkäyksiä sekä informoida verkonvalvojia mahdollisista tunkeutumisista, kuten lähettäen ilmoituksen estetystä tai havaitusta hyökkäyksestä sähköpostin tai puhelimen välityksellä. (Scarfone & Mell 2007, 16-17.)

Hyökkäysten esto. Hyökkäysten esto on tärkeässä roolissa, ja sen automatisointi erittäin tärkeää. IDPS-ohjelma voi estää hyökkäyksen esimerkiksi katkaisemalla yhteyden haitalliseen verkkoliikenteeseen tai estää kaiken yhteyden hyökättävään kohteeseen, kuten palvelimeen. Jos haitallinen liikenne tapahtuu tunnistetun käyttäjän kautta, ohjelma voi estää käyttäjän tai siirtää karanteeniin. IDPS-ohjelma voi myös muokata liikennettä, joka on havaittu haitalliseksi, kuten sähköpostissa oleva liitetiedosto. Ohjelma voi poistaa liitetiedoston, mutta päästää pelkkää tekstiä sisältävän sähköpostiviestin läpi. (Scarfone & Mell 2007, 17.)

2.4 Verkonvalvonnan tekniikat

Verkonvalvonta tapahtuu käyttäen erilaisia protokollia sekä tekniikoita. Yleisin protokolla, jonka kautta pystytään suorittamaan verkonvalvontaa, on SNMP. On monia muitakin työkaluja ja tekniikoita, joita käytetään tietynlaisessa valvonnassa.

2.4.1 SNMP

SNMP eli Simple Network Management Protocol on verkkoprotokolla, joka on tarkoitettu verkkolaitteiden hallintaan. SNMP-protokollalla on mahdollista tutkia erilaisten verkkolaitteiden tilaa, sekä saada hälytyksiä tilamuutoksista. Protokolla on verkonvalvonnan kulmakivi, koska ilman sitä laitteiden tilojen tutkiminen olisi erittäin haastavaa. SNMP-protokollalla pystyy monitoroimaan esimerkiksi palvelimen sisälämpötilaa, tuulettimien kuntoa sekä prosessorin käyttöä. Muita laitteita, joiden tilaa on mahdollista monitoroida, ovat esimerkiksi tulostimet, UPS-virransyöttölaitteet, kytkimet sekä tietokoneet. SNMP-protokolla mahdollistaa myös reitittimen portin liikenteen katkaisun tai tietyn portin nopeuden tarkastuksen. (Schmidt & Mauro 2005, luku 1.)

SNMP vaatii erilaisia toimia ennen kuin sitä voidaan käyttää, esimerkiksi verkonhallitsijan täytyy ottaa SNMP-tuki käyttöön, koska se on yleisesti poissa käytöstä. SNMP-protokollaa voivat hyödyntää myös rikolliset, jos verkonvalvoja ei omilla toimillaan muokkaa asetuksia sen mukaisesti. (Schmidt & Mauro 2005, luku 1.)

SNMP koostuu neljästä eri työkalusta:

- **Hallintalaite.** johon on asennettuna SNMP-hallintaohjelmisto, hallintakonsoli. Tämä laite toimii keskuksena ja sääntöjen asettajana verkon SNMP-protokollalle.

- **Agentti.** Agentti asennetaan kaikille laitteille, joita halutaan monitoroida. Agentti tutkii ja lukee laitetta ja lähettää tiedot hallintakonsolille. Agentteja on erilaisia, sekä erikseen asennettavia tai laitteessa sisäisenä valmiiksi olevia.

- **Trap.** Trap on sääntö, joka asetetaan hallintakonsolilla. Trap on hälytys, jonka laukaisee tapahtuma, joka sopii sääntöön, mikä on annettu hallintakonsolilta. Erilaisia ”trappeja” asetetaan eri laitteille sen mukaan, mitä hälytyksiä laitteelta halutaan.

- **MIB.** Management Information Base eli hallintakonsolin tietokanta. MIB pitää sisällään kaiken informaation hallittavista laitteista, joten se toimii kuten tietokanta. (Schmidt & Mauro 2005, luku 1.)

SNMP-protokollasta on kolme eri versiota: SNMPv1, SNMPv2c sekä SNMPv3.

- **SNMPv1 ja SNMPv2c.** Kaksi ensimmäistä SNMP-versiota toimivat hyvin samalla tavalla, joten niiden ominaisuudet kerrotaan yhtäaikaisesti. SNMP-protokollan täytyy luoda luottamus hallintakonsolin sekä agentin välille. Tämä tapahtuu käyttäen yhteisönimiä. Yhteisönimet ovat ikään kuin salasanoja agentin ja hallintakonsolin välillä, ja näitä on kolme: read-only, read-write sekä trap. Read-Only on nimensä mukaisesti vain lukuoikeus, eli sen avulla voidaan lukea dataa, esimerkiksi porttien läpi kulkevia paketteja, mutta dataa ei pystytä muokkaamaan. Read-Write puolestaan mahdollistaa datan muokkaamisen ja esimerkiksi reitittimen konfiguraation muutokset. Trap sallii hälytykset agentilta hallintakonsolille. (Schmidt & Mauro 2005, luku 2.)

  Yhteisönimet ovat kuin salasanoja, joten niitä valitessa tulisi vaalia samoja periaatteita kuin muissakin tärkeissä salasanoissa. Hyvä salasana ei liity yritykseen tai käyttäjään, eli ei käytetä henkilökohtaisia sanoja ja salasana koostuu isoista ja pienistä kirjaimista sekä numeroista. (Schmidt & Mauro 2005, luku 2.)

  Yhteisönimien tietoturvallinen ongelma on niiden lähetys kryptaamattomana tekstinä. Tämä lisää hyökkääjän mahdollisuuksia varastaa yhteisönimet tunkeutumalla verkkoon ja hyödyntäen SNMP-protokollaa. Tätä riskiä voidaan pienentää huomattavasti palomuurin avulla, muokkaamalla UDP-liikennettä. Palomuurilta on mahdollista konfiguroida laitteiden välinen UDP-liikennne sallituksi, eli jos laite ei ole sallittujen listalla, liikennettä ei lähetetä. Tietenkin

hyökkääjän on mahdollista ohittaa tiettyjä palomuurin sääntöjä, joten palomuuri ei ole täysin luotettava, mutta se kuitenkin pienentää hyökkäyksen riskiä. (Schmidt & Mauro 2005, luku 2.)

- **SNMPv3.** Uusimmassa versiossa, SNMPv3, on otettu huomioon tietoturvallisuuden aukot. Versiot 1 sekä 2 eivät omanneet minkäänlaista käyttäjän todennusta ja salasanat olivat selvällä, luettavalla tekstillä. Tämä on korjattu versiossa 3 ja se tekeekin uusimmasta versiosta erittäin hyvän. (Schmidt & Mauro 2005, luku 3.)

  Versio 3 ei tuo juurikaan mitään uusia ominaisuuksia tietoturvan lisäksi, mutta esimerkiksi versio 3 jättää agentit ja hallintakonsolit pois käytöstä. Näiden tilalle on luotu SNMP-kokonaisuudet, jotka hyödyntävät tietoturvallisesti parempaa käyttäjäpohjaista mallia, USM. Vaikka versio 3 ei tuo juurikaan yhtään uusia toimintoja, sen näyttää hyvinkin erilaiselta. Tämä johtuu siitä, että versioon 3 muutettiin tekstimuotoinen kokonaisuus, terminologia sekä konseptit. (Schmidt & Mauro 2005, luku 3.)

  Jokaisella SNMPv3-kokonaisuudella on SNMP-moottori sekä vähintään yksi SNMP-sovellus. Moottori on koottu neljästä eri työkalusta: pääsynhallinta-järjestelmä, turvallisuusjärjestelmä, viestinkäsittelyjärjestelmä sekä lähettäjä (Dispatcher). Lähettäjä on nimensä puolesta viestin lähettäjä sekä vastaanottaja, se tutkii viestin version (v1, v2 tai v3). Jos versio on tuettu, lähettää se viestin eteenpäin viestinkäsittelyjärjestelmälle. (Schmidt & Mauro 2005, luku 3.)

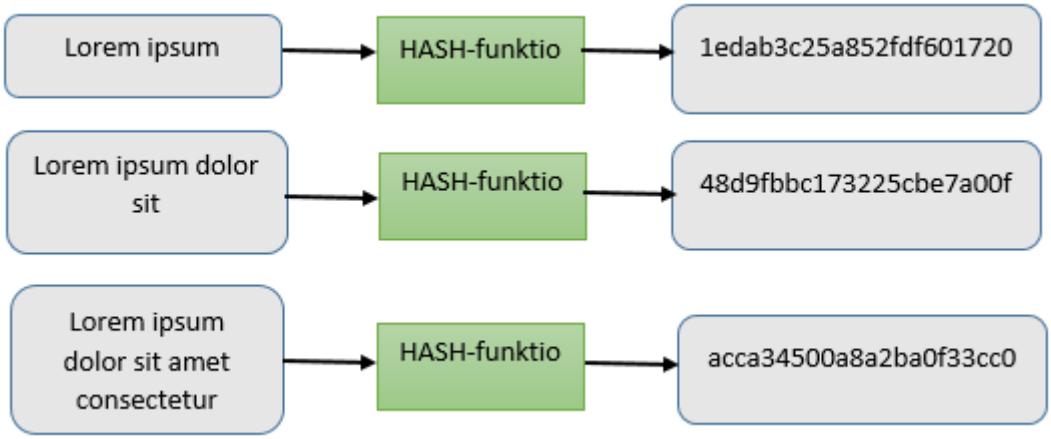
  Viestinkäsittelyjärjestelmä puolestaan käsittelee viestit, tutkien ja purkaen datan sekä valmistelee viestit lähetystä varten. Järjestelmässä on mahdollisesti useampi moduuli, riippuen halutaanko tukea eri versioita SNMP-protokollasta. (Schmidt & Mauro 2005, luku 3.)

  Pääsynhallintajärjestelmä kontrolloi pääsyä MIB-objekteihin. Järjestelmällä hallitaan Read-Only ja Read-Write oikeuksia erinäisiin osiin MIB-tietokannassa. (Schmidt & Mauro 2005, luku 3.)

Turvallisuusjärjestelmä pitää sisällään yksityisyyspalvelut sekä todennuksen. Riippuen SNMP-versiosta, käyttää todennus joko yhteisönimiä tai vastaavasti versiossa 3 käyttäjäpohjaista todennusta. Käyttäjäpohjainen todennus suojaa salasanat algoritmeja hyödyntäen, joko käyttäen MD5- tai SHA-tekniikkaa. Yksityisyyspalvelut käyttävät DES-tekniikkaa kryptaamaan SNMP-viestit. Samalla tekniikalla hoidetaan myös salauksen purkaminen. (Schmidt & Mauro 2005, luku 3.)

SHA- ja MD5-toiminnat toimivat samalla tavalla, eli algoritmi muuttaa alkuperäisen merkkijonon esimerkiksi numerosarjaksi, joka lähetetään eteenpäin. Vastaanottaja, esimerkiksi palvelin, on tallentanut salasanat salatussa muodossa, ja se tarkasteleekin vain salattua numerosarjaa, eikä alkuperäistä salasanaa. Kryptograafisen funktion käyttö salasanojen salaamiseksi on erittäin vahva keino pitää salasanat tallessa, vaikka hyökkääjä saisikin mahdollisesti pääsyn palvelimen tietokantaan, jossa salasanat sijaitsevat. Hyökkääjä löytäisi vain ja ainoastaan salattuja salasanoja, joiden purkaminen on erittäin vaikeaa tai mahdotonta, riippuen SHA versiosta. (SHA 2017.)

MD5-tekniikka on jo murrettu 2000-luvun alussa, ja sen käyttämistä täytyisikin vältellä. Vieläkin on ohjelmia, joissa on MD5 käytössä, mutta SHA-256 on yleinen, jopa standardi tällä hetkellä.



Kuva 1. Esimerkki, miten HASH-salaus toimii.

SNMPv3-sovellukset ovat moottorissa olevia ohjelmia, joilla hoidetaan erinäisiä toimintoja:

- **Komentogeneraattori.** Luo get, getnext ja getbulk pyynnöt sekä asettaa pyynnöt ja prosessoi vastaukset esimerkiksi kytkimiltä, reitittimiltä tai tietokoneilta.
- **Komentovastaanottaja.** Hoitaa muiden asettamia pyyntöjä, kuten get, getnext ja getbulk.
- **Ilmoitustenhallitsija.** Luo SNMP-trapit sekä -ilmoitukset. Esimerkiksi kytkimeltä tuleva trap-ilmoitus rikkoutuneesta tuulettimesta luodaan tällä ohjelmalla.
- **Ilmoitusten vastaanottaja (Dispatcher).** Toimii vain vastaanottajana, ja ilmoittaa tulevan viestin. (Schmidt & Mauro 2005, luku 3.)

2.4.2 Ping

Ping-komento on eniten käytetty verkon ongelmien selvitystyökalu. Ping selvittää, onko laitteelta yhteys toiselle, lähettäen paketin valittuun IP-osoitteeseen. Ping-komennolla on myös mahdollista lähettää paketti DNS-nimeä käyttäen. (Lowe 2003, 786.)

Ping käyttää Internet Control Message Protocol (ICMP)-protokollan kaiku(echo)-viestejä saadakseen tiedon, onko osoitteessa oleva laite aktiivinen, yhteyden laadun eli katoaako paketteja matkalla sekä matka-ajan. Nämä tiedot auttavat selvittämään, onko vika laitteilla, yhteyksissä vai kenties kaapelissa. (Cisco 2006.)

Ping-komento lähettää echo request -paketin valittuun osoitteeseen ja odottaa vastausta. Ping-komento on onnistunut, jos echo request -paketti pääsee osoitteeseen, ja osoitteesta palautetaan paketti tarpeeksi nopeasti. (Cisco 2006.)

2.4.3 Syslog

Syslog on järjestelmä, jonka avulla verkossa olevat laitteet voivat lähettää erilaisia ilmoituksia liittyen laitteen toimintaan. Syslog-järjestelmän avulla tulleista viesteistä voidaan lukea mm. järjestelmän eri tapahtumia tai turvallisuuteen liittyviä ilmoituksia. Esimerkiksi palomuurit, kytkimet, tulostimet sekä tietokoneet pystyvät lähettämään näitä ilmoituksia. (Solarwind. [Viitattu 2.4.2019].)

2.5 Verkonvalvonnan hyödyt

Verkonvalvonta yritysmaailmassa on nykyisin lähes pakollista. Yhä useammin yrityksiin kohdistuu verkkohyökkäyksiä ja mahdollisia tiedostojen lukituksia sekä tästä syntyvää kiristystä. Hyvillä työkaluilla pystytään estämään mahdolliset hyökkäykset sekä tallentamaan todisteita tapahtunutta hyökkäystä vastaan. (Helpsystems. [Viitattu 1.3.2019].)

Verkonvalvontaa hyödynnetään myös laitteiden kanssa, jolloin mahdolliset tulevat laitteistoviat sekä äkilliset ongelmat saadaan hoidettua nopeasti. Tämä lisää yrityksen työntekijöiden työajan hyötykäyttöä, jos palvelut ja palvelimet ovat toiminnassa työajalla. Ajastetut huoltotyöt sekä käyttökatkot voidaan ilmoittaa etukäteen ja näin välttyä yllätyksiltä yrityksessä. (Helpsystems. [Viitattu 1.3.2019].)

2.6 Verkonvalvonnan eri muodot ja metodit

Verkonvalvontaa suoritetaan usealla eri tasolla, esimerkiksi laite-, verkko- tai protokollakohtaisesti. Nämä kaikki jakavat saman periaatteen eli tunkeutujan havaitsemisen, IDS. Verkonvalvonnan lisäksi on mahdollista estää tietynlainen liikenne ennen-

kuin se pääsee syvemmälle verkkoon. Tälläistä metodia kutsutaan IDPS-järjestelmäksi eli Intrusion detection and prevention system-järjestelmäksi. (Scarfone & Mell 2007, 21.)

IDPS on joko sovellus tai ohjelmisto, jolla tutkitaan ja valvotaan verkkoa. Riippuen tarpeesta ja yrityksen koosta käytetään yhtä sovellusta tai vastaavasti useamman sovelluksen yhdistelmää. Sovelluksia on useita erilaisia, niistä osa on ollut markkinoilla jo kymmeniä vuosia. Vaihtelua on jokaisessa sovelluksessa, vaikka tarkoitusperät hyvin samanlaisia. Hinta mukautuu yleisesti sen mukaan, kuinka paljon käyttäjän täytyy tehdä itse työtä IDPS-sovelluksen käyttöönotossa. (Scarfone & Mell 2007, 21.)

IDPS tarvitsee sääntöjä ja asetuksia toimiakseen, eikä siihen riitä pelkkä asennus. IDPS on erinomainen työkalu, mutta se vaatii huoltoa ja sääntöjen säännöllistä päivitystä sekä tietyillä IDPS-tyypeillä tietokantojen päivitystä. Sääntöihin luetellaan esimerkiksi mistä verkosta tuleva liikenne on sallittua. (Scarfone & Mell 2007, 22.)

2.6.1 Yleiset komponentit verkonvalvontatyökaluissa

Yleisimmin käytetyt komponentit verkonvalvontatyökaluissa ovat:

- **Agentti tai sensori.** Agentit ja sensorit tutkivat verkon tai laitteen aktiivisuutta sekä tekevät ilmoitukset mahdollisista poikkeamista. Agentti on yleisimmin käytössä laitekohtaisessa monitoroinnissa, kun taas sensori verkkopohjaisessa. (Scarfone & Mell 2007, 23.)

- **Hallintapalvelin.** Laite, joka hallitsee kaikkia sensoreita sekä agentteja. Laitteen kautta voidaan lukea lokitietoja sekä hallintalaite voi tehdä eri hälytyksistä yhteenvedon, koska laite pystyy yhdistämään eri sensoreille tulleet ilmoitukset. (Scarfone & Mell 2007, 23.)

- **Tietokantapalvelin.** Tietokanta, johon agentit ja sensorit tallentavat kaiken datan. (Scarfone & Mell 2007, 23.)

- **Konsoli.** Ohjelma, joka asennetaan verkonvalvontaohjelman käyttäjille. Ohjelman kautta käyttäjät voivat seurata sensoreiden tilaa sekä hälytyksiä. (Scarfone & Mell 2007, 23.)

2.6.2 HIDPS - Host-based intrusion detection and prevention system

HIDS tarkoittaa laitteen, esimerkiksi työntekijän tietokoneen tai yrityksen palvelimen valvomista. Laitteelle asennetaan agentti, joka mahdollistaa laitteen verkkoliikenteen sekä laitteen lokitietojen seuraamisen. Agentti myös lähettää tiedot hallintapalvelimelle sekä tietokantaan. Näistä tiedoista tehdään lokitiedosto. Tätä käytetään esimerkiksi palvelimilla, jotta tieto mahdollisesta viasta tai tietyn sovelluksen päivityksestä saadaan mahdollisimman nopeasti tietoon. Tällä myös valvotaan ja mahdollisesti estetään työntekijän tietokoneen joutumista rikollisten hallitsemaksi. Tämä ominaisuus on tärkeä, sillä yrityksen verkossa olevan koneen hallinta antaa pääsyn yrityksen sisäverkkoon ja aiheuttaa ison riskin yritykselle. (Scarfone & Mell 2007, 73.)

Laitekohtaisessa valvonnassa on isona etuna tarkkuus. Kyseisellä agentilla voidaan lukea salaamattomana verkkoliikenne laitteelle, kun taas verkkopohjaisessa valvonnassa se ei ole mahdollista. Agentti pystyy lukea liikenteen salaamattona, koska se on asennettuna laitteelle jossa liikenne tapahtuu. Laitteen lokitiedot eivät ole salattuna laitteen sisällä. Kuitenkin laitekohtaisessa valvonnassa on myös enemmän työtä verkonhallitsijalle, joten aina se ei ole paras vaihtoehto. Esimerkiksi jokaisen agentin asennus, huolto ja päivitys sekä monitorointi vaativat aikaa, mikä voi olla esteenä, kun valitaan verkonvalvontatyökalua. (Scarfone & Mell 2007, 75.)

Laitekohtaisessa valvonnassa on mahdollista kerätä tiettyä informaatiota laitteelta, kuten laitteen lokitietoja, verkontilaa ja sen muutoksia, eri ohjelmien toimintoja, koodin analysointia ennen kuin ohjelma suorittaa sen sekä tiedostojen monitorointia. Esimerkiksi työkalu voi analysoida koodia, etsien siitä mahdollisia poikkeamia, kuten järjestelmänvalvojan käyttöoikeuksien jakamista tai muuta vakavaa, normaalisti käyttäytymisestä poikkeavaa aktiivisuutta. Kaikista hälytyksistä tehdään loki, johon kirjataan aikaleima, hälytyksen tyyppi, arvio vakavuudesta, tapahtuman tarkemmat tiedot kuten IP-osoite, portti, jota hyödynnettiin tai ohjelman nimi, joka hälytyksen

aiheutti sekä toiminto, joka suoritettiin hälytyksen tullessa. Näillä tiedoilla verkonvalvoja kykenee korjaamaan vian tai haavoittuvuuden laitteella. (Scarfone & Mell 2007, 76 – 77.)

Laitekohtaisessa valvonnassa on muutamia rajoitteita, jotka voivat olla mahdollisia esteitä valitessa verkonvalvontatyökalua.

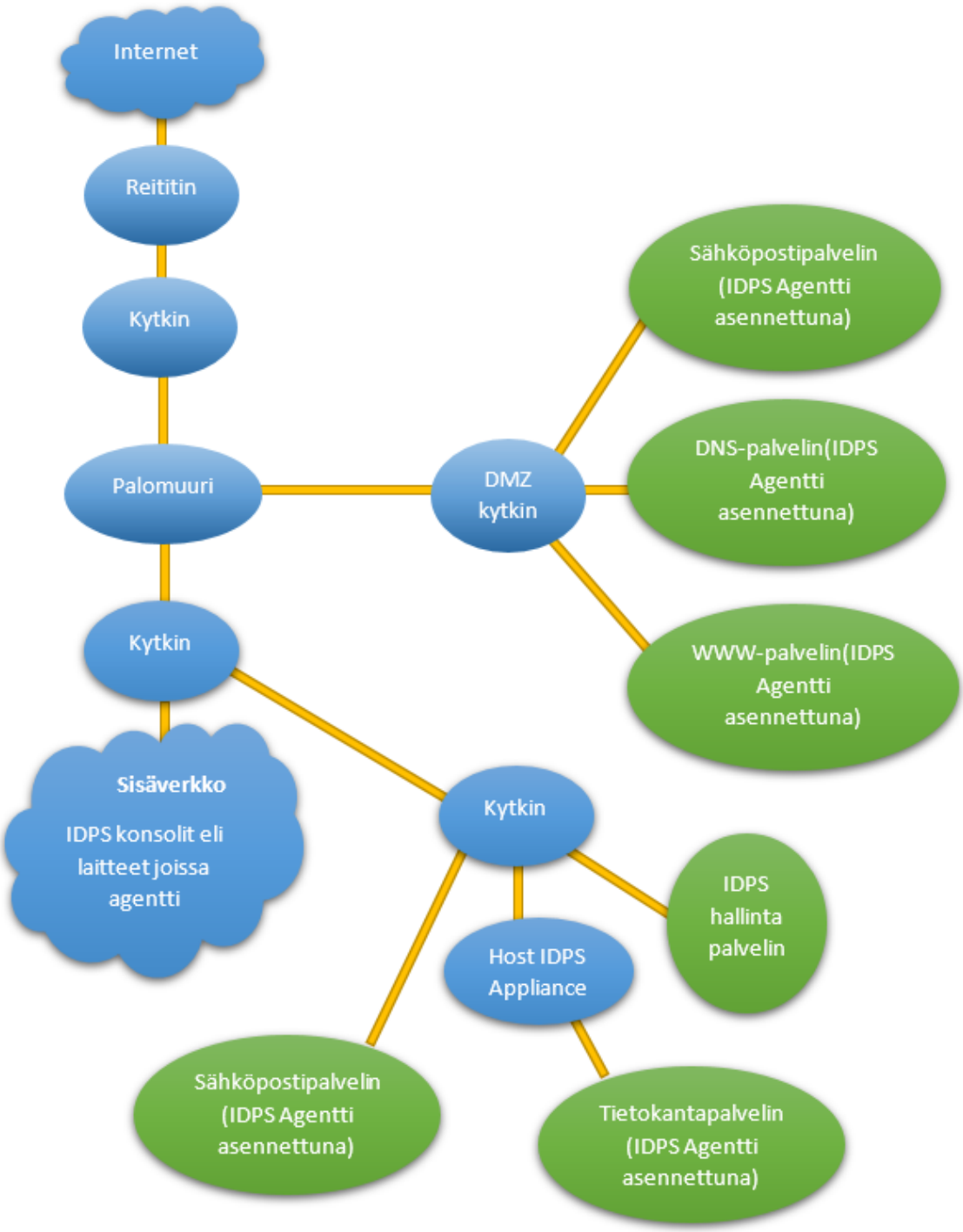
- **Laitteen resurssien käyttö.** Laitteelle täytyy asentaa agentti, joka suorittaa monitorointia sekä estää haavoittuvuuksien hyödyntämisen. Agentti tarvitsee laitteen resursseja toimiakseen, mikä voi hidastaa heikompaa laitetta ja jopa vaikuttaa käyttöön. (Scarfone & Mell 2007, 79.)

- **Raporttien siirto hallintapalvelimelle.** Yleinen käytäntö hälytyksien ja lokitietojen datan lähetyksessä on keskitetty lähetys eli raporttiin kerätään esimerkiksi 15 minuuttia dataa, ja sitten kaikki agentit lähettävät tiedot hallintapalvelimelle. Tämä aiheuttaa pienen viiveen ja käytännössä heikentää tietoturvan laatua. (Scarfone & Mell 2007, 79.)

- **Hälytyksien generointi.** Agentit generoivat hälytyksiä jatkuvasti, mutta tietynlaiset tapahtumat tarkistetaan vain tietyllä aikavälillä päivässä tai vain kerran viikossa. Nämä hälytykset tulevat viiveellä ja vaikeuttavat verkonvalvojan reagointia ongelmiin. (Scarfone & Mell 2007, 79.)

- **Laitteiden uudelleenkäynnistys.** Kuten kaikkia ohjelmistoja, myös IDPS-agentteja täytyy päivittää. Usein päivitykset vaativat uudelleenkäynnistyksen, joten verkonvalvojan täytyykin olla tarkkana, miten ja milloin käynnistykset tapahtuvat. (Scarfone & Mell 2007, 80.)

- **Valmiina olevien tietoturvakäytäntöjen reagointi.** IDPS-agentilla on jo valmiiksi konfiguroidut asetukset, joten jo valmiina olevat suojaukset, kuten palomuuri, voidaan kytkeä pois päältä automaattisesti. Tietenkään tätä ei haluta, joten verkonvalvojan tehtävänä on konfiguroida agentti ja muut sovellukset toimimaan yhdessä. (Scarfone & Mell 2007, 79.)



Kuva 2. HIDPS-tekniikka mallinnettuna

2.6.3 NIDPS eli Network-based intrusion detection and prevention system

NIDS on verkonvalvonnan muoto, joka monitoroi ja analysoi verkkoliikennettä tietyillä verkon alueilla tai laitteilla sekä tutkii protokollien liikennettä etsien mahdollista tunkeutujaa. Se toimii sensoreiden avulla, jotka voidaan asettaa tutkimaan sisään

tulevaa liikennettä. Sensorit lukevat silloin samaa liikennettä kuin palomuuri, ja pystyvät estämään mahdollisen hyökkäyksen. On myös mahdollista, että sensorit vain lukevat liikenteen, mutta eivät estä sitä. Tällöin liikenne kirjataan lokitiedostoon. (Scarfone & Mell 2007, 35.)

NIDS voi toimia myös erilaisena työkaluna verkossa:

- Laitteiden tunnistus: Laitteista voidaan luoda lista, joko käyttäen IP-osoitetta tai laitteen MAC-osoitetta. Kun verkkoon liitetään uusi laite, ilmoittaa sensori sen verkonvalvojalle. (Scarfone & Mell 2007, 42.)

- Käyttöjärjestelmän tunnistus: Sensori voi kertoa verkonvalvojalle eri laitteiden käyttöjärjestelmät ja listata laitteet niiden mukaan. Tätä hyödynnetään tietoturvassa, koska eri käyttöjärjestelmillä on erilaiset haavoittuvuudet. (Scarfone & Mell 2007, 42.)

- Sovellusten tunnistus: Laitteiden käyttämät sovellukset voidaan myös tunnistaa, esimerkiksi tutkimalla mitä portteja sovellus käyttää. Sovellusten tunnistusta myös hyödynnetään tietoturvassa, jotta mahdolliset haavoittuvuuden sisältävät sovellukset saadaan päivitettyä tai poistettua. (Scarfone & Mell 2007, 42.)

- Verkon konfiguraation tunnistus: Sensorit keräävät tietoa verkosta ja sen toiminnasta. Jos verkkoon tehdään muutoksia, sensorit huomaavat poikkeaman ja ilmoittavat siitä. Tällä voidaan jäljittää mahdollinen tunkeutuja verkossa. (Scarfone & Mell 2007, 42.)

NIDPS on useimmiten käytössä lokitietojen keräykseen. Lokitietoja hyödynnetään monissa erilaisissa tilanteissa, kuten vian ilmentyessä tai tunkeilijan aiheuttamien hälytysten selvitykseen. Lokitiedoista voidaan selvittää esimerkiksi seuraavat asiat:

- Aikaleima, eli kellonaika ja päivämäärä

- Tapahtuman tai hälytyksen tyyppi

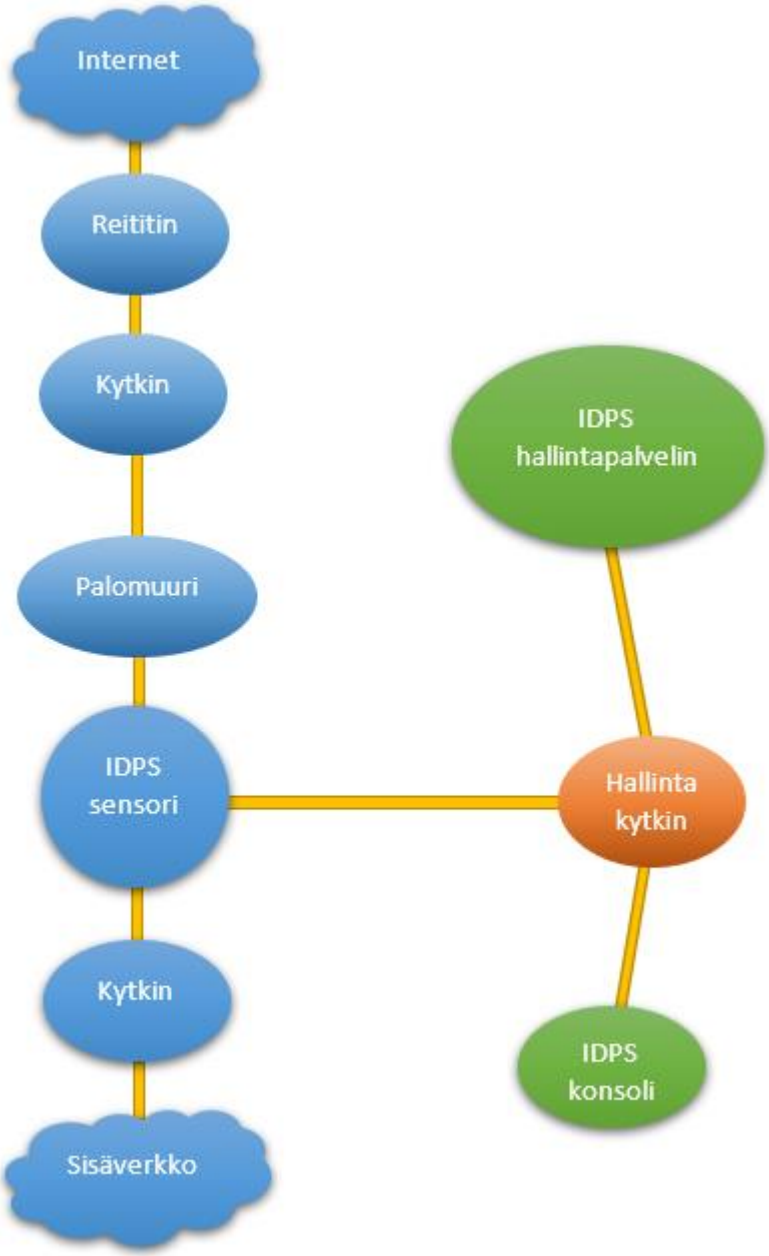
- Tapahtuman kriittisyys

- Käytetyt protokollat

- IP-osoitteet, joiden välillä tapahtuma oli
- TCP- tai UDP-portit, joita käytettiin
- Käyttäjät, esimerkiksi toimialueessa
- Kuinka paljon dataa liikkui avatussa yhteydessä
- Yhteyden tai istunnon tunnus
- Sovellusten pyynnöt ja vastaukset. (Scarfone & Mell 2007, 42-43.)

Yleisimpiä tapahtumia, joita verkkopohjainen valvonta huomaa:

- Sovellustason tiedustelu ja hyökkäykset: salasanan arvailu, haavoittuvuuksien hyödyntäminen esimerkiksi sovelluksissa tai haittaohjelmien siirto. NIDPS tutkii monia eri protokollia, joiden kautta mahdollinen hyökkäys tehdään. Protokollia ovat esimerkiksi DHCP (protokolla, joka jakaa lähiverkossa IP-osoitteet laitteille), DNS (muuttaa verkkotunnukset IP-osoitteiksi), FTP (file transfer protocol eli tiedostojen siirto), HTTP (selainten ja www-palvelinten protokolla) sekä monia muita. (Scarfone & Mell 2007, 43.)
- Tiedonsiirtoon liittyvät hyökkäykset: TCP- ja UDP-protokollia vastaan tehdyt hyökkäykset, kuten porttien skannaus tai pakettien rikkominen (Scarfone & Mell 2007, 43).
- Verkkotason hyökkäykset: IPv4-, ICMP- tai IGMP-protokollia vastaan tehdyt hyökkäykset, kuten IP-osoitteen väärennys (Scarfone & Mell 2007, 43).
- Tiettyjen verkkosivujen tai porttien esto: Käyttäjät mahdollisesti vierailevat sivuilla, jotka ovat yrityksen sääntöjä vastaan. NIDPS kerää kaikki verkkovierailut ja lokitietoja lukemalla voidaan estää tietyille sivuille pääsy (Scarfone & Mell 2007, 44).



Kuva 3. NIDPS-tekniikka mallinnettuna

2.6.4 Signature-based intrusion detection system

Signature-based intrusion detection system on IDS-tyyppi, joka tutkii ja monitoroi verkkoliikennettä ja vertailee sitä tietokannassa olevaan dataan. Tietokantaan tallennetaan tietynlaiset haitalliset datatyypit sekä osoitteet ja niistä luodaan tunniste, johon järjestelmä reagoi vertailun jälkeen. Tämän tyyppisellä järjestelmällä pysty-

tään vähentämään vääriä hälytyksiä, mutta sen tietoturvataso ei ole parhain mahdollinen uuden tyyppisiä hyökkäyksiä vastaan, koska se ei reagoi liikenteeseen, joka ei täsmää tunnisteiden kanssa. (Scarfone & Mell 2007, 18.)

2.6.5 Anomaly-based intrusion detection system

Anomaly-based intrusion detection system on IDS-tyyppi, joka monitoroi verkkotunkeilua sekä laitetunkeilua. Tämä eroaa edellisestä, Signature-based järjestelmästä siten, että tämä tutkii kaiken liikenteen ja täten myös lähettää enemmän vääriä hälytyksiä. Järjestelmä käyttää tekoälyä apunaan tunnistaakseen mahdolliset tunkeilut, verraten liikennettä normaaliin jo opittuun liikenteeseen. Järjestelmän etu tulee sen mahdollisuudesta tunnistaa tunkeilu, joka käyttää täysin uutta tyyliä, jota ei vielä ole tallennettuna ja tunnistettuna tietokantoihin, mutta haittapuolena on useat väärät hälytykset (False alarm). (Scarfone & Mell 2007, 18-19.)

2.6.6 Stateful protocol analysis

Stateful protocol analysis on verkonvalvonta metodi, jossa käytetään universaaleja profiileja ja niitä hyödyntäen tutkitaan verkossa ja protokollissa tapahtuvia pyyntöjä. Komennoilla on useimmiten tietty kaava, miten niitä käytetään, ja näitä poikkeamia analysoidaan tällä metodilla. Esimerkiksi komento, johon täytyy kirjoittaa käyttäjänimi ja salasana, vaatii yleensä n. 20 merkkiä enimmillään. Jos merkkejä tulee tuhansia kenttään, jossa yleensä on kymmenen, ilmoitetaan siitä verkonvalvojalle. Myös saman komennon jatkuva toisto aiheuttaa hälytyksen. (Scarfone & Mell 2007, 19-20.)

Metodin heikkoutena on mahdollinen resurssipula, koska vaikeat analysoinnit vaativat suuria määriä resursseja laitteelta (Scarfone & Mell 2007, 20).

2.6.7 Verkonvalvontatyökalujen ylläpito

Työkalut vaativat huoltoa, joten on erittäin tärkeää huoltaa verkonvalvontatyökalut. IDPS -ohjelman huoltoon kuuluu esimerkiksi komponenttien toimivuuden varmistus, ohjelman toimivuus, päivitysten testaus sekä suoritus, ohjelman kehittäjän huomiot sekä päivitykset liittyen bugeihin tai virheisiin ohjelmassa ja yleisien haavoittuvuuksien testaus. (Scarfone & Mell 2007, 29-30.)

Verkonvalvontatyökaluihin tulee päivityksiä joko liittyen ohjelmistoon, tai uusien tietoturvauhkien ja haavoittuvuuksien ilmenemiseen. Päivitykset voi joko ladata kehittäjän verkkosivuilta tai verkonvalvontatyökalun käyttöliittymän avulla. Osa kehittäjistä myös lähettävät päivityksiä CD/DVD-muodossa. (Scarfone & Mell 2007, 30.)

2.7 Verkonvalvonta yrityksessä

Verkonvalvonta yrityksessä on tärkeä asia, mutta samalla erittäin suurta harkintaa ja tarkkuuta vaativa operaatio. Liian tarkalla verkonvalvonnalla voi työnantaja joutua nopeasti vaikeuksiin ja jopa oikeuteen. Yksityisyyden suojaa rikkovat teot ovat Suomessa vakavia ja rangaistavia tekoja.

Tilastollista datan keruuta ja analyysia saa tehdä, esimerkiksi listaus sivustoista, joilla työntekijät eniten vierailevat. Työnantaja voi estää tietyille sivuille pääsyn, jos sivustoilla ei ole mitään yhteistä työnkuvan kanssa. Myös koko internetselailun voi kieltää, jos sitä ei tarvitse työssä. Lähtökohtana Suomessa verkonvalvontaa ei saa yhdistää yksittäiseen henkilöön, eikä esimerkiksi sivustohakuja tai sivustovierailuja saa tallentaa tai tutkia ilman erittäin painavia perusteita. Jos työntekijä rikkoo lakia, voi työnantaja kuitenkin luovuttaa tietoja viranomaisille. (Tietosuojauutiset 2017.)

Työnantajalla on oikeus tutkia ja seurata työntekijöiden intranetissä olevien viestien selailua, koska viestintä tapahtuu työntekijän ja työnantajan välillä eikä näin riko työntekijän viestintäsalaisuutta. Myös kirjautuminen työnantajan tietojärjestelmään oikeuttaa työnantajan tallentamaan ja tutkimaan lokitietoja tapahtuneesta. (Tietosuojauutiset 2017.)

Suomessa lähtökohtaisesti yhteyden ja laitteiden omistaja ei voi valvoa laitteidensa käyttöä, mutta voi kuitenkin antaa ohjeistusta ja neuvontaa, miten ja mihin laitteita käytetään. Kuitenkin, jos työnantaja näkee fyysisesti rikkeen laitteen käytössä, voi hän rangaista työntekijää, esimerkiksi varoituksella. (Tietosuojauutiset 2017.)

Sähköpostin tai muiden sähköisten viestien valvonta sekä tutkiminen ovat yksityisyyden laissa kiellettyä, mutta yksittäisien sähköpostiviestien lukeminen on sallittua seuraavien ehtojen täyttyessä:

- Työntekijä toimii itsenäisesti, kuitenkin työnantajalle. Jos erillistä kirjausmenetelmää ei ole, tehdyistä töistä ei välttämättä ole muuta tietoa kuin sähköiset viestit.

- Työntekijän tämän hetkisistä töistä selviää ilmeisesti, että viestejä on lähetetty tai vastaanotettu.

- Työntekijällä on tilapäinen mahdottomuus suorittaa työtehtäviä ja työnantaja ei pääse käsiksi viesteihin, vaikkakin työnantaja olisi huolehtinut pykälässä 18 (Työnantajan huolehtimisvelvollisuudet) mainituista velvollisuuksista.

- Työntekijältä ei saada suostumusta kohtuullisessa ajassa ja asian tärkeys pakottaa kiireelliseen toimenpiteeseen. (L 13.8.2004/759.)

Kuitenkin, työntekijän sähköpostin sekä muiden sähköisten viestien lukeminen on erittäin arka aihe, joten sitä täytyykin vältellä mahdollisimman paljon.

2.8 Verkkohyökkäykset

Yrityksiin ja sen laitteisiin kohdistuvia hyökkäyksiä ja uhkia on monia erilaisia. Haittaohjelmia voidaan levittää sähköpostin liitteenä, hyperlinkkeinä tai esimerkiksi tiliä koskevina vahvistuspyyntöinä. Näitä hyökkäyksiä kutsutaan tietojenkalasteluksi (phishing). Tietojenkalasteluyritykset ovat erittäin suosittuja, koska niitä vastaan ei voida täysin suojautua verkkoliikennettä ja laitteita suojaamalla. Tietojenkalaste-

lussa pääideana on ihmisen tietämättömyyden hyödyntäminen, eikä niinkään laitteiden tietoturva-aukkojen käyttäminen, joten yrityksessä onkin erittäin tärkeää opettaa ja kertoa mahdollisista tietojenkalasteluyrityksistä ja miten niitä kohdatessa täytyy toimia. (Timm & Perez 2010, luku 3.)

Yrityksillä on jo kauan ollut ja tulee aina olemaan suuria ongelmia haittaohjelmien kanssa. Erilaisia haittaohjelmia on jo vuosien ajan kehitelty, kuten madot (Worms), troijalaiset (Trojans) sekä muut virukset. Niiden levitys tapahtuu hyperlinkkien, sähköpostin, verkkosivujen mainosten sekä ilmaisien sovelluksien kautta. Jos esimerkiksi yrityksessä yksi tietokone saastuu haittaohjelmasta, on mahdollista, että se saastuttaa muitakin laitteita samassa verkossa. Yrityksen sähköpostin kautta lähtevät sähköpostit, joiden viesteissä on linkkejä haitallisille sivuille, tahraa yrityksen mainetta sekä altistaa asiakkaita ja yrityskumppaneita samoille haittaohjelmille. (Timm & Perez 2010, luku 2.)

Haittaohjelmilla on erilaisia toimintoja ja niiden tarkoitusperät ovat aina hyökkääjän käsissä. Kuitenkin, jokainen haittaohjelma antaa mahdollisuuden hyödyntää laitteen resursseja haitalliseen ja jopa rikolliseen toimintaan. Hyökkääjä voi esimerkiksi jakaa haittaohjelmaa verkkosivujen kautta. Kun tarpeeksi moni laite on saastunut, hyökkääjä luo näistä laitteista bottiverkon (Botnet). Bottiverkkoa voidaan hyödyntää mm. DDoS-hyökkäyksissä, jotka ovat vaarallisia ja isoa vahinkoakin aiheuttavia palvelunestohyökkäyksiä. Bottiverkko koostuu verkossa olevista eri laitteista, joiden resursseja hyökkääjä hyödyntää rikollisiin toimenpiteisiin, kuten identiteettivarkauksiin, roskapostin levitykseen sekä lunnashyökkäyksiin (Ransom attack). Bottiverkon käyttäjän on erittäin vaikea jäädä kiinni, koska bottiverkko koostuu eri laitteista ympäri maailmaa, eikä sijoitu yhteen paikkaan. (Timm & Perez 2010, luku 1.)

DDoS eli Distributed Denial of Service -hyökkäysten tarkoituksena on estää yritysten palveluiden toiminta, esimerkiksi kuormittamalla yrityksen palvelinta TCP-pyynnöillä. Kun palvelin ei pysty vastaamaan pyyntöihin, se sammuttaa palvelut ja tällöin kukaan ei pysty käyttämään yrityksen palvelua, kuten verkkokauppaa. Tämä johtaa tietenkin rahallisiin tappioihin ja jopa asiakkaiden menetyksiin. DDoS-hyökkäyksen

järjestäminen on suhteellisen helppoa, tämä tekeekin siitä vaarallisen sekä pelottavan metodin. (Timm & Perez 2010, luku 1.)

2.9 Kustannukset

Verkonvalvontaohjelmistot tuovat kustannuksia, ja niitä hankkiessa täytyykin tehdä selvä kartoitus tarpeista, budjetista sekä mahdollisista lisämaksuista ohjelmistojen päivityksissä tai lisäosissa (Scarfone & Mell 2007, 104).

Kustannukset muodostuvat monesta eri asiasta ja hankinnasta, mutta hankinta- sekä asennusvaiheessa täytyy ottaa huomioon seuraavia seikkoja:

- Uudet laitteet, kuten kytkimet, palomuurit ja palvelimet.
- Ohjelmistot sekä niiden lisenssit.
- Asennuksen tuomat kulut, kuten asennuksessa apuna oleva henkilö ohjelmiston myyvältä yritykseltä.
- Ohjelmiston muokkaus omaan ympäristöön voi vaatia ohjelmoijan työtä esimerkiksi skriptien kirjoittamiseen.
- Koulutuksesta tulevat kustannukset, jos koulutus ei kuulu ohjelmiston hintaan. Myös menetetty työaika omien työntekijöiden koulutuksessa uuteen ohjelmistoon maksaa yritykselle. (Scarfone & Mell 2007, 105.)

Lisäksi kustannuksia tulee käytön aikana, esimerkiksi tukipalveluista, jos ilmenee ongelmia, joita yritys ei itse pysty korjaamaan tai lisämuutoksien tekeminen, kuten uudet skriptit tai lisäosat. Myös uusien lisäpalveluiden hankinta voi olla tarpeellista, jos yrityksessä kasvaa verkko sekä työntekijämäärä lisääntyy. IDPS-sovellus tuo mukanaan myös lisätyötä verkonhallitsijoille, koska siitä tulevia lokitietoja täytyy analysoida sekä reagoida mahdollisiin vikoihin. (Scarfone & Mell 2007, 105.)

3 SECURITY ONION

3.1 Security Onion

Security Onion on avoimen lähdekoodin Linux-jakelupaketti, joka toimii verkon turvallisuuden monitorina. Käyttötarkoituksia on monia, kuten haavoittuvuuksien ja vanhentuvien SSL-sertifikaattien tunnistaminen tai vaihtoehtoisesti tietoturvaa loukkaavien tapausten ilmoitus ja todisteiden kerääminen. Vaikka Security Onion-ohjelman asentaminen on nopeaa ja varsin yksinkertaista, vaatii se toimiakseen kuitenkin säätöä ja sääntöjen asettamista. Kun kyseessä on monitorointiohjelmisto, vaatii se ihmisen apua ja tästä syystä Security Onion kannattaakin ajatella apuvälineenä, eikä niinkään valmiina avaimet käteen -pakettina. (Security Onion Solutions, 2018a.)

Security Onion-ohjelmassa on kolme ydin komponenttia: isäntälaitteiden tunkeilun valvonta ja verkon tunkeilun valvonta (HIDS ja NIDS) käyttäen Wazuh HIDS-, Bro IDS- tai Snort-ohjelmistoa, täysi pakettien kaappaus käyttäen Netsniff-ng-ohjelmistoa sekä datan analysointiin Kibana ja Squil (Security Onion Solutions, 2018a).

Käytännössä Security Onion-ohjelma on iso kokoelma erilaisia työkaluja, jotka ovat yhdistettynä yhteen pakettiin. Kuitenkaan näitä kaikkia työkaluja ei tarvitse asentaa, ja vaikka olisikin asentanut, on käytöstä poisto helppoa ja mutkatonta.

3.2 Laitteistovaatimukset

Laitteistovaatimuksina yrityskäytössä on vähintään kahdeksan CPU-ydintä, 16–128GB keskusmuistia sekä tarpeeksi levytilaa tallentamaan kaikki lokitiedot. Pakettien kaappaus vie paljon levytilaa, mutta se on tärkeässä osassa, koska paketit ovat todisteina tietoturvaloukkausta vastaan, ja järjestelmän lokitiedoista voidaan jälkeenpäin etsiä syytä laiterikolle tai muulle ongelmalle. Esimerkiksi yhteys, jossa sensoreilla on täysi paketin kaappaus ja jonka keskiarvo liikenne on 20 Mb/s, vaatii päivän levytilaksi n. 220 Gigabittiä kiintolevytilaa. (Security Onion Solutions 2018C.)

3.3 Virtuaalipalvelin

Security Onion asennetaan virtuaaliseen ympäristöön. Virtuaalinen ympäristö tarkoittaa sitä, että yhdessä fyysisessä palvelimessa on monia eri palvelimia sisällä, virtuaalisena. Tämä lisää fyysisen laitteen käyttömahdollisuuksia, eikä rajoita sitä vain yhteen tarkoitukseen. Esimerkiksi useat eri ohjelmistot tai sovellukset vaativat oman palvelimen, koska ne toimivat eri käyttöjärjestelmillä, joten usean fyysisen palvelimen osto tulisi erittäin kalliiksi ja palvelinten käyttöaste jäisi vajaaksi. Virtualisoinnilla saadaan yhdestä fyysisestä laitteesta mahdollisimman suuri hyöty. (Netstandard 2014.)

Virtuaalipalvelimia hyödynnetään usein uusien tuotteiden testauksessa. Yrityksen on helpompi tehdä kopio käytössä olevasta palvelimesta sekä sen konfiguraatiosta ja testata uusia ohjelmistoja kopioidulla palvelimella. Jos ohjelmisto ei ole stabiili ja jotain menee vikaan, ongelmat eivät ole tuotantokäytössä olevalla palvelimella. (Netstandard 2014.)

3.3.1 Virtuaalialustat

Virtuaalisille palvelimille ja -tietokoneille on useita erilaisia ohjelmia eri tyyppiseen käyttöön. Tässä listataan muutama erilainen:

- **Oracle VM Virtualbox.** Virtualbox on ilmainen avoimen lähdekoodin sovellus, jolla on mahdollista luoda Windows-, Mac OS-, Linux- tai Oracle Solaris-käyttöjärjestelmän sisältävän palvelimen tai tietokoneen (Oracle VM Virtuabox 2019.).

- **VMware.** VMware on myös erittäin suosittu ohjelmisto, joka mahdollistaa erilaisten käyttöjärjestelmien luonnin virtuaalisesti. VMware ja Virtualbox ovat molemmat hyviä, niin yksityiseen kuin yrityskäyttöön, mutta VMwaren yrityskäyttöön tarkoitetut virtuaalisovellukset tarjoavat laajemman skaalan ominaisuuksia ja suuressa palvelinympäristössä VMware on toimivampi ratkaisu. (Nakivo 2018.)

Yleinen näkemys onkin, että suuremmat yritykset käyttävät VMwarea saadakseen parhaan mahdollisen laadun. VMware on maksullinen, joten yksityisen henkilön tai pienemmän yrityksen täytyy puntaroida, onko rahalle vastinetta tarpeeksi. Jos VMwaren käyttö kohdentuu omiin tarpeisiin ja testailuihin, on VMware ilmainen yksityiselle henkilölle. Kuitenkin, jos VMwarea aikoo käyttää mahdollisiin rahaa tuottaviin tehtäviin, on ostettava lisenssi.

- **QEMU.** QEMU on Linux-, Windows- sekä macOS-käyttöjärjestelmillä toimiva virtuaalilaitteiden luomis- sekä ylläpitotyökalu (QEMU. 2019a). QEMU on myös emulaattori, jolla voi emuloida esimerkiksi PowerPC-, MIPS64-, ARM-järjestelmiä sekä muita sulautettujen järjestelmien laitteita. (QEMU. 2019b.)

3.4 Bro

Bro, nykyisin Zeek, on avoimen lähdekoodin ohjelmisto, jonka tarkoituksena on kerätä informaatiota ja lokitietoja verkossa liikkuvasta liikenteestä. Bron käyttö ei rajoitu pelkästään verkon turvallisuuteen, vaan sitä käytetään myös verkon suorituskyvyn mittaamiseen, vikojen ehkäisyyn sekä vianetsintään. (Bro. 2019a.)

Ohjelmistolla on mahdollista tarkkailla esimerkiksi http-, ftp-, smtp-, irc-, ssh-, ssl- ja dns-protokollien liikennettä. Bron toiminta perustuu pakettien kaappaamiseen PCAP-ohjelmointirajapintaa käyttäen. Rajapinta lähettää paketit Event Enginelle, joka analysoi paketit luodakseen neutraaleja tapahtumia ja hyödyntää näitä, kun se huomaa uusia ip-osoitteita tai tiedostoja. (Bro. 2019a. Intro.)

Bro koostuu kahdesta pääkomponentista, jotka ovat Event Engine eli tapahtumien käsittely sekä Policy Script Interpreter eli skriptien hallinta. Event Engine seuloo tulevia paketteja ja muodostaa näistä tapahtumat. Tapahtumissa esimerkiksi kerrotaan mitä tallennetuissa paketeissa oli, minne sivustolle on tehty GET-pyyntö sekä IP-osoite ja portti. Nämä tiedot Event Engine lähettää toiselle pääkomponentille, Policy Script Interpreterille, joka reagoi sisältöön verraten paketteja jo luotuihin Event

Handler -sääntöihin. Event Handler eli tapahtumien käsittelijä on skripti, joka on kirjoitettu Bron kustomoidulla ohjelmointikielellä. Skripteillä on mahdollista lähettää reaaliaikaisia hälytyksiä tai suorittaa komentoja sekä uusia skriptejä. (Bro 2019a.)

3.5 Snort

Snort on avoimen lähdekoodin tunkeilun havaitsemisjärjestelmä eli englanniksi Intrusion Detection System, IDS. IDS tutkii verkkoliikennettä samalla analysoiden mahdollisia loukkauksia. Jos Snortin haluaa toimimaan yhteydellä 1000 Mbps, täytyy konfiguroida lokitietojen lukijaksi Barnyard. Barnyard lukee Snortin tallentamat lokitiedot binäärilukuina ja muokkaa sekä lähettää tiedot eteenpäin, esimerkiksi tietokantaan. (Snort 2018a.)

Snortia on mahdollista käyttää kolmena eri työkaluna:

- Nuuskijana eli Snort lukee verkossa liikkuvat paketit ja näyttää ne konsolissa.
- Pakettilokina eli sovellus tallentaa verkossa liikkuvat paketit lokitiedostoon, josta voidaan tutkia liikennettä joko reaaliajassa tai myöhemmin, jos huomataan epäilyttävää toimintaa.
- Tunkeilun havaitsemisjärjestelmänä, jolla monitoroidaan verkkoliikennettä ja sitä analysoidaan käyttäjän asettamien sääntöjen mukaan. Snort suorittaa tietyn toiminnon, jos jokin liikenteessä on vastoin käyttäjän asettamia sääntöjä. (Snort 2018a.)

3.6 Squil

Squil on avoimen lähdekoodin ohjelma, joka toimii verkonvalvontamonitorina ja pitää sisällään graafisen käyttöliittymän. Squil-ohjelmassa on useita sensoreita ja sensorit keräävät monen tyyppistä informaatiota:

- Snort monitoroi verkon turvallisuutta ja kerää tiedot lokitiedostoon.

- Barnyard kerää tapahtumat lokitiedostosta ja lähettää ne eteenpäin tietokantaan.
- Snort kerää myös kaikki verkossa liikkuvat paketit erilliseen lokitiedostoon, mutta tämä vaatii ison dataosion tiedostokoon vuoksi.
- SANCP on verkkotyökalu, joka kerää TCP/IP-yhteydet ja lähettää niistä informaation tietokantaan. (Squil 2019a.)

Esimerkiksi kun SANCP on lisännyt tietokantaan eri IP-osoitteita, voidaan Squil-ohjelman avulla hakea tietokannasta kaikki saman IP-osoitteen toiminnot ja jäljittää yhteys. Tämä on tärkeä ominaisuus turvallisuuden näkökulmasta. (Squil 2019.)

3.7 Squert

Squert on selainpohjainen käyttöliittymä, jolla tutkitaan IDS-sovelluksen hälytyksiä. Squert lukee datan Squil-tietokannasta ja muuttaa sen visuaaliseksi näkymäksi. Squert on ohjelmoitu PHP-ohjelmointikielellä ja sitä käytetään verkkoselaimella, mieluiten Chromiumilla tai Google Chromella. (Squert 2019.)

Squertin avulla voidaan lukea hälytyksistä esimerkiksi, milloin hälytys on tapahtunut, kuinka monta samanlaista hälytystä on tullut, hälytyksen IP-osoite tai hälytyksessä käytetty protokolla (Security Onion 2019).

Security Onion käyttää omaa muunnelmaa Squertista, koska Squertin kehittäjä Paul Halliday on lopettanut sen kehittämisen (Security Onion 2016).

3.8 Wireshark

Wireshark on yksi maailman tunnetuimmista ja käytetyimmistä verkkoprotokollien monitorointi- ja analysointisovelluksista. Sen käyttötarkoituksia on mm. verkkovian selvitys, tietoliikenneverkon turvallisuuden analysointi ja verkkosovellusten analysointi. Lisäksi sitä käytetään opetusmielessä oppilaitoksissa opettaen verkkoliiken-

teen protokollia. (Wireshark 2019b.) Sitä käytetään yleisesti verkkoliikenteen tutkimiseen ja sillä voi esimerkiksi lukea yli sataa erilaista protokollaa, analysoida liikennettä reaaliajassa, purkaa pakattuja paketteja ja analysoida sisältö ja sen analysoinnin tuloksen voi tallentaa XML- , PostScript- sekä CSV-muodossa tai vaihtoehtoisesti normaalilla tekstillä. Wiresharkia on kehitetty vapaaehtoisten ammattilaisten avulla ja esimerkiksi Suomesta kehittämässä on ollut Nokian työntekijöitä. Wiresharkin perusti Gerald Combs vuonna 1998. (Wireshark 2019a.)

Wiresharkilla voidaan esimerkiksi tutkia verkon TCP-liikennettä. TCP-liikenne on esimerkiksi HTTP-protokollan kautta kulkevia paketteja, jotka toisin sanoen liikkuvat silloin, kun käyttäjä yhdistää verkkosivulle selaimellaan. Tällöin TCP-paketteja liikkuu verkkopalvelimelta selaimelle. TCP-liikennettä kulkee myös esimerkiksi SMTP-, FTP- ja SNMP-protokollien kautta. (CCNA 2019.)

Täytyy kuitenkin muistaa, että Wireshark ei ole tunkeutumisen esto- tai havainnointijärjestelmä, vaan sillä pelkästään mitataan verkkoliikenteen dataa. Tietenkin datasta verkonvalvoja pystyy tutkimaan ja määrittelemään, onko data sallittua vai vahingollista. (Wireshark 2019c.)

3.9 Wazuh

Wazuh on laitekohtaiseen monitorointiin tarkoitettu työkalu, joka tarvitsee hallintakonsolin palvelimelle ja vaatii agentin jokaiselle laitteelle, jota halutaan monitoroida. Agentti liitetään hallintakonsolille, jonka jälkeen laite lähettää itsestään informaatiota. Wazuh on kehitetty muunnelma OSSEC HIDS -ohjelmistosta ja sen konfiguraatiotiedostoista löytyykin vielä ossec-komentoja. (Wazuh 2019.)

Agentti lukee tiedostoja ja sen avulla voidaan tutkia laitteen tiedostojen lupia, omistajuutta, attribuutteja sekä sisältöä.

Erittäin hyvä ominaisuus Wazuh-työkalussa on lokitiedostojen lähetys hallintakonsolille: Agentti lukee ja lähettää lokitietoja erinäisistä tietokoneen tapahtumista, kuten järjestelmän virheistä, päivitysten asennuksessa tapahtuvista virheistä tai haitallisesta aktiviteetistä. (Wazuh 2019.)

Wazuh-agentti monitoroi ja analysoi laitetta etsien mahdollisia haitta- sekä piilohallintaohjelmia (rootkit). Piilohallintaohjelmat ovat erittäin vaarallisia, sillä ne pystyvät peittämään jälkensä käyttäen tietoturvahaavoittuvuuksia. Vaikka piilohallintaohjelma ei itsessään ole haitallinen, on näiden ohjelmien yleinen motiivi antaa etäkäyttö mahdollisuus hyökkääjälle. Hyökkääjä levittää tämän jälkeen haitallisia sovelluksia tietokoneelle tai kaappaa laitteen bottiverkkoon (botnet). (F-Secure 2019.)

3.10 Elastic Stack

Elastic Stack on ohjelmistopaketti, johon on yhdistetty useampi eri avoimen lähdekoodin ohjelma. Siihen kuuluu Elasticsearch, Kibana, LogStash sekä Beats. Elastic Stackia voidaan käyttää moneen eri tarkoitukseen, kuten yksittäisten lokitiedostojen lukemiseen tai koko yritysverkon verkkoliikenteen monitoroimiseen. (Elastic Stack 2019e.)

3.10.1 Kibana

Kibana on avoimen lähdekoodin sovellus ja Elasticsearchin lisäosa. Kibanaa käytetään saadun datan etsimiseen ja tutkimiseen. Kibanalla myös luodaan datasta visuaalisia kuvioita, taulukoita sekä karttoja. (Elastic Stack 2019a.)

Kibanalla voi visualisoida verkosta otettua liikennettä esimerkiksi maantieteellisen sijainnin mukaan tai tapahtuma-ajan perusteella ja ne voidaan jakaa erilaisilla säännöillä omiin väreihin tai kuvoihin. Kibanalla on myös mahdollista nähdä datasta tietoja, joita ei välttämättä juuri sillä hetkellä etsi. (Elastic Stack 2019a.)

3.10.2 Elasticsearch

Elasticsearch on avoimen lähdekoodin työkalu, jolla etsitään ja analysoidaan dataa. Elasticsearch:lla haetaan, tallennetaan ja analysoidaan dataa, esimerkiksi verk-

koliikenteestä tai sivustoilta, kuten verkkokaupoista. Elasticsearch käyttää tietokantana SQL-tietokantaa, mutta sillä on mahdollista käyttää muitakin tietokantoja, vaatien pieniä muutoksia konfiguraatiossa. (Elastic Stack 2019c.)

3.10.3 Logstash

Logstash on avoimen lähdekoodin sovellus, joka kerää tapahtumat ja lokitiedot. Nämä tiedot se lähettää Elasticsearchille, joka puolestaan tallentaa datan tietokantaan. Logstash voi esimerkiksi kerätä palvelimen lähettämät järjestelmäviestit tai tietoturvailmoitukset, muuntaa ne JSON-dokumenteiksi ja lähettää eteenpäin. Tämän jälkeen Elasticsearch tallentaa dokumentit ja Kibanalla luodaan viesteistä kaavio. Kaaviossa on mahdollisesti useita eri viestejä, joista voidaan lukea vian tai tietoturvauhan laatu. (Elastic Stack 2019b.)

3.10.4 Beats

Beats on kokoelma useasta datan kerääjästä: Auditbeat, Filebeat, Functionbeat, Hearbeat, Journalbeat, Metricbeat, Packetbeat sekä Winlogbeat. Näillä työkaluilla voidaan kerätä informaatiota ja dataa niin laitteilta, kuin verkosta tai pilvestä. Esimerkiksi Filebeat mahdollistaa laitteen lokitietojen lähetyksen Logstashille. Metricbeat kerää tietoa laitteiden järjestelmän tasosta, kuten keskusmuistin käytöstä, prosessorin kuormituksesta sekä eri prosesseista, joita laitteella on käynnissä. (Elastick Stack 2019d.)

4 SECURITY ONION-OHJELMAN ASENNUS

Security Onion testattiin yrityksen ympäristössä, käyttäen yrityksen fyysistä palvelinta. Palvelimelle asennettiin VMwarella oma virtuaalinen palvelin, johon asennettiin Security Onionin. Testit tehtiin yrityksen verkossa, johon tehtiin oma aliverkko työtä varten. Tutkittavina laitteina käytettiin yhtä yrityksen tietokonetta sekä tämän työn tekijän kannettavaa tietokonetta. Kahdella eri laitteella tehdyt testit antoivat hyvän esimerkin, miten laitekohtaisia ongelmia ilmenee asennusvaiheissa. Asennustyön pääpainona oli laitekohtainen valvonta ja Wazuh-ohjelmiston käyttö. Työssä yritettiin saada selville, miten laitekohtainen valvonta onnistuisi yrityskäytössä, käyttäen Security Onion -ohjelmistoa.

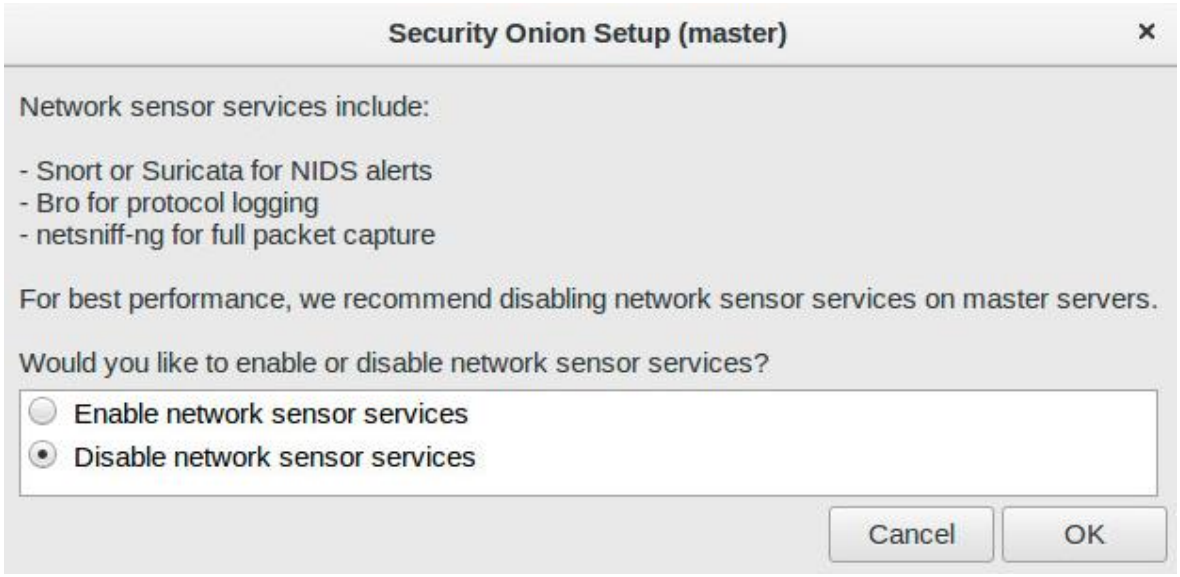
4.1 Alkutilanne

Security Onion asennetaan käyttäen iso-tiedostoa, joka ladataan Security Onionin verkkosivuilta. Tiedostoa ei suositella ladattavaksi mistään muualta kuin Security Onionin verkkosivuilta, sillä on erittäin tärkeää, ettei iso-tiedoston mukana tule mitään ylimääräistä, kuin Security Onionin käyttöjärjestelmä. Tiedoston lataus on ilmaista ja Security Onionin käyttö ei maksa mitään, mutta tietyissä ohjelmissa, kuten Snortissa on maksullisia lisäpalveluita.

Kun virtuaalikone käynnistetään iso-tiedostoa käyttäen, aukeaa Ubuntu 16.04 -versio, jossa on Security Onion -asennustyökalu. Työkalua käytetään koko Security Onionin asennuksen ajan, ja sen ohjeita seuraamalla asennus on erittäin yksinkertainen. Kun verkkoasetukset ja muut alkukonfiguraatiot, kuten päivitykset on tehty, päätetään, kumpi versio asennetaan, Master vai Standalone. Virtuaalikoneista on kuitenkin hyvä luoda varmuuskopio (snapshot), ennen kuin jatkaa asentamista. Varmuuskopiot ovat hyvä keino palata vanhaan tilaan, jos asennuksessa ilmenee ongelmia.

Standalone-versio otetaan käyttöön silloin, kun verkonvalvontaa ei ole tarkoitus tehdä kuin yhdellä laitteella. Standalone-versiossa ei käytetä agentteja muilla laitteilla, se sopiikin erittäin hyvin silloin, kun palvelimen resurssit ovat vähäiset ja halutaan tutkia verkkoliikennettä.

Master/Slave-versio asennetaan, kun halutaan tutkia niin verkkoliikennettä kuin laitteiden lokitietoja. Master/Slave-nimike tuleekin siitä, että palvelimesta tehdään hallintakonsoli ja muista laitteista verkossa, kuten tietokoneista, tehdään datankerääjiä. Tietokoneet lähettävät itsestään ja verkkoliikenteestään erilaisia tietoja hallintakonsolille agentin ja SNMP-protokollan kautta. Master-versiossa ei tutkita itse hallintakonsolin liikennettä, joten sen sensori täytyy poistaa käytöstä asennuksen yhteydessä.



Kuva 4. Dokumentaation mukaan Master-laitteen sensori kannattaa kytkeä pois päältä

Seuraavaksi asennetaan Security Onioniin kuuluvia ohjelmia, kuten Bro, Snort, Elastic Stack (Kibana, Logstash, Elasticsearch), Squert, Squil sekä netsniff-ng. Snortia asentaessa asennustyökalu kysyy, minkälaisia IDS-sääntöjä halutaan käyttää. Tähän on erilaisia variaatioita, mutta *oinkcode*-koodin vaativat ovat maksullisia. Maksullisissa versioissa on mm. nopeammat päivitykset sääntöihin, mutta tämä ei ole pakollinen hankinta.

Kuva 5. Security Onion-ohjelman asennuksen aloitus

Kun edellä mainitut ohjelmat on asennettu, voidaan testata IDS-toimivuutta sekä katsoa visuaalista näkymää Kibanalla. Ensin testataan palveluiden tila avaamalla komentokehote ja käyttäen komentoa: *sudo so-status.*

```
Status: securityonion
  * sguil server                                                [  OK  ]
Status: HIDS
  * ossec_agent (sguil)                                         [  OK  ]
Status: Elastic stack
  * so-elasticsearch                                            [  OK  ]
  * so-logstash                                                 [ FAIL ]
  * so-kibana                                                   [  OK  ]
  * so-curator                                                  [  OK  ]
  * so-elastalert                                               [  OK  ]
```

Kuva 6. so-status-komennolla saatu näkymä, josta voidaan huomata, että Logstash ei ole käynnissä

Komento näyttää palveluiden tilat ja niitä voidaan käynnistää uudelleen, jos ne eivät ole käynnistyneet asennuksen jälkeen mm. käyttäen komentoa: *sudo so-start*

4.2 Wazuh-hallintakonsoli

Wazuh-hallintakonsoli tulee asennuksessa valmiina, mutta se vaatii konfigurointia toimiakseen.

Agentit asennetaan erikseen jokaiselle laitteelle ja ne täytyy lisätä myös hallintakonsoliin, jotta ne saavat yhteyden ja niistä voidaan ottaa datatiedot vastaan. Hallintakonsolilla ohjataan eri laitteiden agentteja keräämään haluttua dataa, kuten tunkeilusta aiheutuvia hälytyksiä, järjestelmän lokitietoja, ilmoituksia puuttuvista päivityksistä tai laitteen toimintakyvystä eli prosessorin käyttöasteesta, muistin käytöstä sekä komponenttien lämpötilasta. Näitä sääntöjä muutetaan omaan tarpeeseen, mutta tässä työssä testaamista tehtiin vakioasetuksilla.

Hallintakonsolilta voidaan tarkastella agenttien tilaa käyttäen komentoa: *sudo /var/ossec/bin/agent_control -l*

Komento näyttää kaikki agentit, jotka on liitetty hallintakonsoliin. Agentista näytetään id, IP-osoite, ja onko agentti yhdistettynä tällä hetkellä.

4.3 Wazuh-agentti

Wazuh-agentti on tärkeä palanen laitekohtaisessa valvonnassa. Ilman agenttia ei monitorointia voitaisi suorittaa. Agentti asennettiin lataamalla asennustiedosto Wazuhin omilta verkkosivuilta, käyttäen Wazuhin dokumentointia oppaana. Asennuksen voi suorittaa käyttämällä graafista käyttöliittymää tai komentokehotteen komentoja hyödyntäen. Tässä työssä käytettiin graafista käyttöliittymää, mutta suurempaan ympäristöön agenttien asennus on järkevämpää tehdä komentokehotteen kautta, käyttäen komentoa:

wazuh-agent-3.8.2-1.msi /q ADDRESS=" hallintakonsolin IP-osoite" AUTHD_SERVER="hallintakonsolin IP-osoite" PASSWORD="salasana" AGENT_NAME="Annetaan agentille mieleinen nimi"

Agentti vaatii todennusavaimen ja hallintakonsolin IP-osoitteen, jotta se saa yhteyden palvelimella olevaan hallintakonsoliin. Todennusavain löytyy palvelimelta käyttäen */var/ossec/bin/manage_agents* -komentoa, ja todennusavain siirretään laitteelle joko manuaalisesti, tai käyttäen *AUTHD* -komentoja. Työssä siirrettiin avaimen manuaalisesti, mutta suuremmassa ympäristössä on tämäkin järkevämpää tehdä komentokehotteelta, joko lisäämällä avain jo asennusvaiheessa komentoon tai jälkeenpäin AUTHD-komennoilla.

Tämän jälkeen agentille avataan palvelimen palomuurille portit, jotta TCP- ja UDP-liikenne pääsee läpi. Ilman palomuurin muutoksia, dataa ei voida toimittaa palvelimelle ja agentti ei näy aktiivisena. Security Onionissa palomuuriin tehdään muutos antamalla komento: *sudo so-allow*

```
[a] - Analyst - ports 22/tcp, 443/tcp, and 7734/tcp
[b] - Logstash Beat - port 5044/tcp
[c] - apt-cacher-ng client - port 3142/tcp
[e] - Elasticsearch REST endpoint - port 9200
[f] - Logstash forwarder - standard - port 6050/tcp
[j] - Logstash forwarder - JSON - port 6051/tcp
[l] - Syslog device - port 514
[n] - Elasticsearch node-to-node communication - port 9300
[o] - OSSEC agent - port 1514
[s] - Security Onion sensor - 22/tcp, 4505/tcp, 4506/tcp, and 7736/tcp
```

Kuva 7. Valikosta valitaan tarpeellinen palomuurin portti, joka täytyy avata liikenteelle

Listasta valitaan portti, joka halutaan avata. Wazuh-agentti tarvitsee pääsyn portista 514, joka on UDP-liikenteelle eli syslogien liikuttamiseen, sekä portin 1514, josta liikkuu muu UDP-liikenne. Portit voi avata koko verkolle tai vastaavasti jokaiselle IP-osoitteelle erikseen. Kuitenkin, jos kyseessä on suurempi ympäristö, ei agenteilla ole staattisia IP-osoitteita, joten portit avataan tietylle verkon alueelle.

Kun agentti on asennettu ja sille on tehty tarvittavat konfiguraatiot, käynnistetään agentti uudelleen, joko käyttäen graafista käyttöliittymää tai antamalla palvelimelta uudelleenkäynnistyksen komento: */var/ossec/bin/agent_control -R "agentin id, jonka haluat käynnistää"*

Kun agentti on käynnistynyt uudelleen, katsotaan hallintakonsolilta, onko konsoli saanut yhteyden agenttiin. Tämä tapahtuu antamalla komentokehotteelta komennon: */var/ossec/bin/agent_control -l*

```
Wazuh agent_control. List of available agents:
   ID: 000, Name: Master (server), IP: 127.0.0.1, Active/Local
   ID: 002, Name: PC1_agentti, IP: 10.100.51.4/24, Never connected
   ID: 003, Name: PC2_agentti, IP: 10.100.51.5, Active

List of agentless devices:
```

Kuva 8. Kuvassa PC2_agentin liitos on onnistunut ja PC1_agentin liitos epäonnistunut

4.4 Virtuaalinen analysointitietokone

Kun agentit on yhdistetty hallintakonsoliin, niiden lokitietoja voidaan tutkia sekä niistä voidaan itse luoda näkymiä Kibana-sovelluksella. Tähän tarkoitukseen asennettiin virtuaalinen tietokone, jota Security Onionin -dokumentaatiossa nimitetään nimellä *Analyst-VM.* Analysointikoneeseen asennettiin Ubuntu 16.04- käyttöliittymä Security Onionin iso -tiedostoa käyttäen.

Tämän virtuaalitietokoneen tarkoituksena on toimia analysoinnin ja lokitietojen tutkinnan työkaluna, eli esimerkiksi verkonvalvoja käyttää tätä tietokonetta tutkiessaan Kibanan sekä Squertin näkymiä. Nämä molemmat ohjelmat toimivat verkkoselaimessa, joten ei ole tarpeellista eikä hyödyllistä käyttää palvelinta siihen. Analysointitietokoneen käyttö ei myöskään rasita samalla tavalla palvelinta, kuin jos käyttäjä olisi suoraan kirjautunut palvelimelle.

4.5 Raportointi / Squert

Laitteille asennetut agentit toimittavat tällä hetkellä dataa hallintakonsolille. Datasta muodostetaan erilaisia näkymiä ja sitä hyödynnetään monessakin eri yritysverkon

ylläpito- ja huoltotoimenpiteessä. Security Onion tekee raportoinnin Squert-ohjelman avulla. Squert hakee datan Squil-tietokannasta, ja luo verkkoselaimessa toimivaan ohjelmaan näkymiä hälytyksistä. Nämä hälytykset sisältävät erilaisia ilmoituksia tietokoneelta, kuten päivitysten puuttuminen, tunkeiluyritykset tai käyttäjätilin vaihtuminen. Käyttäjätilin vaihtuminen ei itsessään kuulosta vaaralliselta, eikä se sitä yleensä olekaan, mutta joissain tapauksissa se voi olla merkki laitteen väärinkäytöstä. Security Onion kerää lokitietoja paljon, eikä niitä kaikkia tarvitse raportoida. Näitä voi muokata omien tarpeiden mukaisesti, mutta tässä työssä niitä ei ole konfiguroitu.

COUNT	%TOTAL	#SRC	#DST	SIGNATURE	ID
9	39.13%	1	1	[OSSEC] Integrity checksum changed.	550
4	17.39%	1	1	[OSSEC] Host-based anomaly detection event (rootcheck).	510
4	17.39%	1	1	[OSSEC] Windows error event.	18103
4	17.39%	1	1	[OSSEC] Windows: User account changed	20011
1	4.35%	1	1	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).	533
1	4.35%	1	1	[OSSEC] Web server 400 error code.	31101

Kuva 9. Squert-näkymä yhden laitteen monitoroinnista

Pelkästään tätä näkymää katsomalla verkonvalvojalle selviää laitteiden tila sekä vaadittavat toimenpiteet.

4.6 Ongelmat

Työn asennusvaiheessa tuli muutamia ongelmia vastaan, joiden selvittämiseen kului suhteellisen paljon aikaa. Ensimmäinen ongelma oli Wazuh -agentissa, joka asennuksen ja konfiguroinnin jälkeen ei ilmestynytkään hallintakonsolin näkymään. Tämän selvittely kuitenkin tuotti tulosta ja agentti saatiin toimimaan normaalisti. Asennuksen alussa annettu IP-osoite oli oikein, mutta jossain kohtaa konfigurointia se oli mennyt väärin. Tämä esti hallintakonsolin yhteyden agentille.

Toinen ongelma oli Kibana-sovelluksen näkymissä. Niiden tekeminen sekä konfigurointi osoittautui tutkimushetkellä vaikeaksi, joten se jätettiin työstä pois. Kuitenkin jatkotoimenpiteenä Kibana-näkymä konfiguroidaan toimintaan. Näkymällä olisi

mahdollista luokitella jokainen laite erikseen, sekä tietyn hälytyksen perusteella jaotella laitteet. Nämä helpottavat verkonvalvojan työtä sekä nopeuttaa mahdollisiin vikatilanteisiin reagoimista.

5 TULOKSET JA JOHTOPÄÄTÖKSET

Tutkimuksen lähtökohtana oli selvittää, miten avoimen lähdekoodin ohjelmistoa voidaan hyödyntää yrityksen verkonvalvonnassa. Tutkimuksen edetessä ja Security Onionia tutkiessa selvisi, että se on oikea työkalu pienen tai keskisuuren yrityksen verkonvalvontaan. Kuitenkin, avoimen lähdekoodin ohjelmistoissa on asennusvaiheessa paljon työtä sekä täytyy tietää, mitä konfiguroi. Verkon ylläpidon täytyy olla tuttua, eikä sitä voi aloittaa ilman hyvää suunnittelua.

Security Onion on ilmainen, mutta siihen on maksullisia harjoituskursseja, joita suositellaan käytäväksi, jos aikeissa on Security Onionin käyttöönotto. Myös Security Onionin dokumentaation tarkka läpikäynti auttoi asennuksessa ja konfigurointiin löytyikin tarvittavia komentoja suoraan dokumentaatiosta.

Tutkimuksessani sain vastauksen tutkimusongelmaan sekä hyvän kuvan siitä, miten tärkeää verkonvalvonta yrityksessä on. Tutkimuksessa selvisi myös, miten paljon resursseja Security Onion vaatii palvelimelta. Tämä on esitetty luvussa 3.2 sekä havainnoitu itse asennusvaiheessa, jolloin ongelmaksi muodostui Security Onion -hallintakonsolin hidastelu. Luvussa 3.2 esitettyjä laitteistovaatimuksia ei pystytty täyttämään kyseisessä asennuksessa, tämä aiheutti palveluiden hidastelua sekä lisäsi uudelleenkäynnistyksen tarpeita. Jatkotoimenpiteinä työtä pyritään jatkamaan ja saamaan laitteiden valvonta keskitetysti toimimaan sekä korjaamaan luvussa 4.6 esitetty ongelma.

LÄHTEET

Bro. 2019. Intro. [Verkkosivu]. [Viitattu 18.1.2019]. Saatavissa: https://www.zeek.org/manual/release/intro/index.html

CCNA. 2019. TCP explained. [Verkkosivu]. [Viitattu 1.4.2019]. Saatavissa: https://study-ccna.com/tcp-explained/

Cisco. 2006a. Understanding the Ping and Traceroute Commands. [Verkkosivu]. [Viitattu 18.3.2019]. Saatavissa: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html#ping_com

Elastic Stack. 2019a. Kibana. [Verkkosivu]. [Viitattu 10.2.2019]. Saatavissa: https://www.elastic.co/guide/en/kibana/current/introduction.html

Elastic Stack. 2019b. LogStash. [Verkkosivu]. [Viitattu 15.1.2019]. Saatavissa: https://wikitech.wikimedia.org/wiki/Logstash

Elastic Stack. 2019c. Elasticsearch. [Verkkosivu]. [Viitattu 15.1.2019]. Saatavissa: https://www.elastic.co/guide/en/elasticsearch/reference/current/getting-started.html

Elastick Stack. 2019d. Beats. [Verkkosivu]. [Viitattu 9.3.2019]. Saatavissa: https://www.elastic.co/guide/en/beats/libbeat/current/beats-reference.html

Elastick Stack. 2019e. Elastic Stack. [Verkkosivu]. [Viitattu 2.4.2019]. Saatavissa: https://www.elastic.co/guide/en/elastic-stack-get-started/current/get-started-elastic-stack.html

Elastic. 2019a. Kibana. [Verkkosivu]. [Viitattu 25.3.2019]. Saatavissa: https://www.elastic.co/products/kibana

F-Secure. 2019a. Rootkit. [Verkkosivu]. [Viitattu 26.3.2019]. Saatavissa: https://www.f-secure.com/v-descs/rootkit.shtml

Helpsystems. Ei päiväystä. Why Monitor Your Network. [Verkkosivu]. [Viitattu 1.3.2019]. Saatavissa: https://www.helpsystems.com/resources/guides/top-8-reasons-smbs-need-monitor-their-networks

L 13.8.2004/759. Laki yksityisyyden suojasta työelämässä

Lowe, D. 2003. Networking All-in-one Desk Reference for Dummies. [Viitattu 27.2.2019].

Nakivo. 2018. VMware vs. Virtualbox. [Verkkosivu]. [Viitattu 31.3.2019]. Saatavissa: https://www.nakivo.com/blog/vmware-vs-virtual-box-comprehensive-comparison/

Netstandard. 2014. How Virtual Servers Work. [Verkkosivu]. [Viitattu 13.3.2019]. Saatavissa: https://www.netstandard.com/virtual-servers-work/

Opsec Oy. 2019. Tietosuojapalvelut. [Verkkosivu]. [Viitattu 2.4.2019]. Saatavissa: https://www.opsec.fi/fi/palvelut/tietosuoja/

Opsec Oy. 2019. Tietoturvatestaus. [Verkkosivu]. [Viitattu 2.4.2019]. Saatavissa: https://www.opsec.fi/fi/palvelut/tietoturva/tietoturvatestaus/

Opsec Oy. 2019. Yritys. [Verkkosivu]. [Viitattu 2.4.2019]. Saatavissa: https://www.opsec.fi/fi/yritys/

Oracle VM Virtuabox. 2019. Chapter 1.4 Supported Host Operating Systems. [Verkkosivu]. [Viitattu 13.3.2019]. Saatavissa: https://www.virtualbox.org/manual/ch01.html#virt-why-useful

QEMU. 2019a. Download QEMU. [Verkkosivu]. [Viitattu 15.3.2019]. Saatavissa: https://www.qemu.org/download/

QEMU. 2019b. About QEMU. [Verkkosivu]. [Viitattu 15.3.2019]. Saatavissa: https://wiki.qemu.org/Main_Page

Scarfone, K. & Mell, P. 2007. Guide to Intrusion Detection and Prevention Systems (IDPS).

Schmidt, K. & Mauro, D. 2005. Essential SNMP, 2nd Edition. [Verkkokirja]. O'Reilly Media. [Viitattu 3.3.2019]. Saatavana O'Reilly -palvelusta. Vaatii käyttöoikeuden.

Security Onion Solutions. 2018a. Introduction. [Verkkosivu]. GitHub: Security Onion Solutions. [Viitattu 1.1.2019]. Saatavissa: https://github.com/Security-Onion-Solutions/security-onion/wiki/IntroductionToSecurityOnion

Security Onion Solutions. 2018b. Kibana. [Verkkosivu]. GitHub: Security Onion Solutions. [Viitattu 2.1.2019]. Saatavissa: https://github.com/Security-Onion-Solutions/security-onion/wiki/Kibana

Security Onion Solutions. 2018c. Hardware. [Verkkosivu]. Githug: Security Onion Solutions. [Viitattu 15.1.2019]. Saatavissa: https://github.com/security-onion-solutions/security-onion/wiki/Hardware

SHA.2017. Secure Hash Algorithms. [Verkkosivu]. [Viitattu: 17.3.2019]. Saatavissa: https://brilliant.org/wiki/secure-hashing-algorithms/

Snort. 2018. User manual. [Verkkosivu]. [Viitattu 2.1.2019]. Saatavissa: https://www.snort.org/#documents

Solarwind. Ei päiväystä. Basics of Network Monitoring. [Verkkosivu]. [Viitattu 2.4.2019]. Saatavissa: https://thwack.solarwinds.com/community/resources/guides/basics-of-network-monitoring

Security Onion. 2016. Squert Development. [Verkkosivu]. [Viitattu 25.3.2019]. Saatavissa: https://blog.securityonion.net/2016/09/squert-development.html

Security Onion. 2019. Squert. [Verkkosivu]. [Viitattu 25.3.2019]. Saatavissa: https://securityonion.readthedocs.io/en/latest/squert.html

Squil. 2019. About Squil. [Verkkosivu]. [Viitattu 10.1.2019]. Saatavissa: http://nsmwiki.org/Sguil

Tietosuojauutiset. 2017. Tekninen valvonta työpaikalla. [Verkkosivu]. Tietosuojauutiset.fi. [Viitattu 18.1.2019]. Saatavissa: https://tietosuojauutiset.fi/2017/09/15/tyontekijoiden-teknisin-menetelmin-toteutetusta-valvonnasta/

Timm, C. & Perez, R. 2010. Seven Deadliest Social Network Attacks. [Verkkokirja]. [Viitattu 30.3.2019]. Saatavana O'Reilly -palvelusta. Vaatii käyttöoikeuden.

Wazuh. 2019a. [Verkkosivu]. [Viitattu 26.3.2019]. Saatavissa: https://documentation.wazuh.com/current/getting-started/index.html

Wireshark. 2019a. About Wireshark. [Verkkosivu]. [Viitattu 25.3.2019]. Saatavissa: https://www.wireshark.org/

Wireshark. 2019b.Some intended purposes. [Verkkosivu]. [Viitattu 31.3.2019]. Saatavissa: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs

Wireshark. 2019c. What Wireshark is not. [Verkkosivu]. [Viitattu 31.3.2019]. Saatavissa: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs