Opinnäytetyö (AMK)

Tietojenkäsittely

2021

Tapio Lehtinen

MISP

– Implementaatio ja hyödyt tietoturvayrityksessä

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2021 | 29 sivua

Tapio Lehtinen

MISP

- Implementaatio ja hyödyt tietoturvayrityksessä

MISP on avoimen lähdekoodin ohjelmisto tietoturvaan, sekä haittaohjelmiin ja tietomurtoihin liittyvän tiedon jakamiseen. Opinnäytetyön tavoitteena oli tutustua MISP-alustaan ja sen hyötyihin tietoturvaa tarjoavassa yrityksessä. Tämän lisäksi tavoitteena oli käsitellä ohjelmiston asentamista Debian 10 -virtuaalipalvelimelle niin, että lopputuloksena on toimiva MISP -instanssi, johon voidaan hakea syötteitä, aktivoida ne ja tallentaa ne välimuistiin.

Alustan asennus suoritettiin komentokehotteen komennoilla seuraten MISP -projektin omaa ohjeistusta. Asennuksen lopputuloksena tuli olla toimiva graafinen käyttöjärjestelmä, jota voi käyttää verkkoselaimella.

Alustan asennuksen jälkeen tuli alustalla suorittaa syötteiden aktivointi, jota seurasi oletussyötteen haku ja tallentaminen välimuistiin.

Opinnäytetyön tavoitteet saavutettiin ja tulokseksi saatiin toimiva demonstraatio MISP-alustasta, jonne pystyi kirjautumaan sisään ja hakemaan syötteitä sekä aktivoimaan ja tallentamaan ne välimuistiin. Tämän työn perusteella työn toimeksiantaja pystyy perehtymään MISP:n mahdollisiin hyötyihin tuotantokäytössä.

ASIASANAT:

tietoturva, haittaohjelma, MISP, syöte

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology

2021 | 29

Tapio Lehtinen

MISP

- IMPLEMENTATION AND BENEFITS FOR AN INFORMATION SECURITY COMPANY

MISP is an open source patform for collecting, storing, distributing and sharing threat intelligence and cyber security indicators. The goal of this thesis was to familiarise with the MISP platform and it's benefits for a company offering information security as a service. To install the software on a Debian 10 virtual server so that the end result is a working MISP instance that has the capability to fetch feeds, activate them and save them to cache.

The installation of the platform was carried out with command line commands following the MISP project's own guide. The purpose of the installation was to have a functional graphical user interface accessible with a web browser.

After the installation the platform was meant to be able to activate a feed, fetch the feed and to save it to cache.

The thesis project succeeded and the end result was a working demo of the MISP platform. The demo was capable of logging the user in and fetching, activating and saving the feed to the cache. As a result of this thesis the commissioner of this thesis can familiarise with the possible uses and benefits of MISP in production environment.

KEYWORDS:

Information Security, malware, MISP, feed

SISÄLTÖ

KUVAT

KÄYTETYT LYHENTEET

API	Application Programming Interface
ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
APT	Advanced Persistent Threat
CERT	Computer Emergency Response Team
CIRCL	The Computer Incident Response Center Luxembourg
CYBOX	Cyber Observable Expresision
CyDefSig	Cyber Defence Signatures
GUI	Graphical user Interface
IDS	Intrusion Detection System
IoC	Indicator of Compromise
ISAC	Information Sharing and Analysis Centre
JSON	JavaScript Object Notation
LAMP	Linux, Apache, MySQL/MariaDB, PHP/Perl/Python
MAEC	Malware Attribute Enumeration and Characterization
NATO	North Atlantic Treaty Organization
NCIRC	National Criminal Intelligence Resource Center
NIDS	Network Intrusion Detection System
MISP	Malware Information Sharing Platform
REST	representational state transfer
TAXII	Trusted Automated Exchange of Intelligence Information
TIP	Threat Intelligence Platform
TTP	Tactics, Techniques, and Procedures
URL	Uniform Resource Locator
STIX	Structured Threat Information Expression
VERIS	The Vocabulary for Event Recording and Incident Sharing

XML	Extensible Markup Language

1 JOHDANTO

MISP on avoimen lähdekoodin ohjelmisto tietoturvaan, sekä haittaohjelmiin ja tietomurtoihin liittyvän tiedon jakamiseen. Opinnäytetyöni koskee Malware Information Sharing Platformin (MISP) käyttöönottoa ja MISP alustan käytöstä mahdollisesti saatavia hyötyjä tietoturvaa tarjoavissa yrityksissä.

Opinnäytetyön toteutus aloitetaan tutustumalla MISP:n toimintaan ja hyötyihin, käyttäen kaikkea sitä tietoa mitä aiheesta on verkossa kirjoitettuna, sekä alan ammattilaisten kokemuksia ja tietoja.

Tutustumisen jälkeen siirrytään perehtymään itse ohjelmiston toimintaan asentamalla ohjelmisto virtuaaliseen Debian 10 ympäristöön ja toteuttamalla MISP -instanssissa syötteen lataus, aktivointi sekä tallennus välimuistiin

Tavoitteena on saada tietoa MISP-alustan toiminnasta ja toimintaperiaatteista, sekä oppia alustan asennus ja käyttö.

Lähdeaineistona tulee toimimaan MISP-projektin omat verkkosivut ja aineisto, GitHubista saatava lisätieto sekä muut aihetta käsittelevät verkkojulkaisut. Tämän lisäksi tulen tuottamaan omakohtaista MISP-alustan asennustyöstä saatavaa dataa muun aineiston tueksi, jotta työstä tulisi mahdollisimman kattava.

2 TIETOTURVAN KEHITTYVÄ MAISEMA

Omien havaintojeni mukaan nykypäivän nopeasti kehittyvien tietoturvauhkien täplittämässä tietoturvan maisemassa, voi uusien uhkien tunnistaminen ja tietoturvan ylläpitäminen tuntua ylitsepääsemättömältä ongelmalta. Tietoturvarikolliset kehittävät jatkuvasti uusia tapoja varastaa yritysten, järjestöjen, kunnallisten ja kansallisten toimijoiden kuin yksityishenkilöidenkin immateriaalista, sekä fyysistä omaisuutta tai pyrkivät haittaamaan jokapäiväistä toimintaa tietotekniikan parissa. Haitantekijät saattavat olla pieniä ryhmittymiä, jotka toimivat mitä erilaisimpien motiivien johdattamina aina suuriin, kansallisesti tuettuihin APT-ryhmiin (Advanced Persistent Threat), joiden motivaationa on yleensä raha tai suuryritysten tai valtiollisten- ja kunnallisten toimijoiden toiminnan vaikeuttaminen. Uusia uhkia ja haavoittuvuuksia tunnistetaan lähes päivittäin ja tämä asettaa suuria paineita tietoturvaa tarjoavien yritysten havainnointimoottoreiden, sekä henkilöstön kykyyn tunnistaa kaikki uudet uhkat ja torjua ne. Samalla tietoturvauhkat kehittyvät yhä hienostuneemmiksi ja vaikeammiksi havaita.

2.1 Tämän hetken suurimpia tietoturvahaasteita

Checkpointin(2021) mukaan tietojen kalastelu(Phishing), on yksi yleisimmistä kyberhyökkäysten tyypeistä. Pääasiallisesti siksi, koska se on tehokas tapa saada pääsy organisaation tietoverkkoon ja järjestelmiin. Tietojenkalastelukampanjoita vastaan paras puolustus on informaation saaminen mahdollisimman aikaisin, sekä jatkuva organisaation henkilöstön kouluttaminen ja informointi. Tässä apuna voi toimia tietoturvaa tarjoava yritys ja MISP:n, tai muun reitin kautta saatu tieto, jolla asiakasorganisaatiota voidaan varoittaa. (Checkpoint 2021.)

Myös etätyöskentelyn hyväksikäyttö on ollut edelleen vaikuttavan pandemian johdosta erittäin suosittu hyökkäysvektori. Varsinkin koska yritykset ovat joutuneet hyvin nopealla aikataululla siirtymään toimistossa työskentelystä etätyöskentelyyn. Tämä on aiheuttanut sen, että etätyöskentelyprotokollat ja ympäristöt ovat olleet nopeasti rakennettuja ja suunniteltuja. Tämä on helpottanut kyberrikollisten työtä. Suojautuminen etätyöskentelyn haavoittuvuuksia vastaan helpottuu, kun tiedetään vektorit ja keinot, joita kyberrikolliset ovat käyttäneet vastaavissa hyökkäyksissä. Näiden lisäksi käytettävien ohjelmistojen kuratointi ja etätyöverkkojen kovennukset ovat toimivia keinoja. (Checkpoint 2021.)

Kiristyshaittaohjelmahyökkäyksien määrät ovat viime vuosina kasvaneet huomattavasti. Osasyynä tähän ovat olleet onnistuneet korkean profiilin kiristyshaittaohjelmahyökkäykset, jotka ovat osoittaneet kyberrikollisille kyseisen vektorin hedelmällisyyden. Maailmanlaajuisesti keskimäärin joka kymmenes minuutti uusi uhri joutuu kiristyshaittaohjelman kohteeksi. Kiristyshaittahjelmat aiheuttivat yrityksille noin 20 miljardin dollarin menetykset vuonna 2020, joka on yli 75% enemmän kuin vuonna 2019. Kiristyshaittaohjelmat alana on myös kehittynyt viimevuosina valtavasti, Ransomware as a Service(RaaS) -toimijat kehittävät ja myyvät kiristyshaittaohjelmia myös pienemmille toimijoille, jotka näin saavat pääsyn korkean tason haittaohjelmiin. (Checkpoint 2021.)

2.2 Tietoturvaongelmien ratkaiseminen MISP:llä

Ongelmien ratkaisua helpottamaan on luotu sovelluksia. Näistä yksi esimerkki on MISP(Malware Information Sharing Platform). Se on haittaohjelmatiedon jakamiseen erikoistunut alusta. MISP:n avulla haitantekijät voidaan saada kiinni jo tunkeutumisvaiheen alussa, kun tunnettujen toimijoiden toimintatavat ja tunnettujen haittaohjelmien sekä tiedonkalastuskampanjoiden indikaattorit ovat helposti löydettävissä ja jaettavissa. MISP:n käytöstä saavutettavia etuja ovat muun muassa pääsy yhteisön keräämiin tietoihin haittaohjelmista ja uhkatekijöistä, jolloin mahdollisten uhkatilanteiden selvittäminen ja ratkaisu on nopeampaa sekä tehokkaampaa. (MISP2 2021.)

3 MISP - YLEISESTI

3.1 MISP taustatietoja

MISP projektin kehittäjinä toimii useista tahoista koostuva ohjelmoijaryhmä. Ryhmän jäsenet ovat CIRCListä(The Computer Incident Response Center Luxemburg), Belgian asevoimista, NATOsta(North Atlantic Treaty Organization) ja NCIRCstä(National Criminal Intelligence Resource Center). Sen rahoittajana toimii Euroopan Unioni(Connecting Europe Facilityn toimesta) ja CIRCL. (MISP2 2021.).

Projekti aloitettiin kesäkuussa 2011 Christophe Vandeplasin turhauduttua IoC:den(Indicator of Compromise) jakamiseen sähköpostitse tai pdf-tiedostoina, jolloin niiden jäsentäminen ei ollut mahdollista automaatiota hyödyntäen. Aluksi projekti tunnettiin nimellä CyDefSig: Cyber Defence Signatures. CyDefSigs oli Vandeplasin henkilökohtainen vapaa-ajan projekti. Christophe toteutti Proof of Conceptin(PoC) projektistaan hyödyntäen CakePHP:tä. (MISP2 2021.).

Projekti sai jo ensimmäisellä esityskerralla paljon positiivista palautetta hänen työpaikallaan Belgian puolustusvoimissa. Luovutettuaan pääsyn CyDefSig projektiinsa kotipalvelimellaan, Belgian puolustusvoimat alkoi hyödyntämään palvelua jo elokuussa 2011. Tämä mahdollisti Christophelle työskentelyn projektin parissa osa-aikaisesti työnsä ohella. (MISP2 2021.).

Vuoden 2012 alussa NATO kiinnostui projektista ja ensimmäinen esitys siitä pidettiin jo tammikuussa, jossa esiteltiin projektia syvällisemmin. NATOn vertailtua projektia vastaavanlaisiin tuotteisiin, päätyi NATO CyDefSig:in pariin sen avoimuuden johdosta. Ensimmäinen osa-aikainen NATO:n ohjelmoija projektissa oli Andrzej Dereszowski. NATO kuitenkin kiinnostui projektista niin paljon, että se palkkasi jo muutaman kuukauden kuluttua projektiin ensimmäisen kokopäiväisen kehittäjän parantaakseen koodin laatua ja lisätäkseen ominaisuuksia. Yhteistyö projektin saralla alkoikin siitä hetkestä. Projekti päätettiin julkaista Affero GPL lisenssin alla, jotta koodi voitaisiin jakaa mahdollisimman monen ihmisen kanssa, samalla suojaten sitä haitoilta. (MISP2 2021.).

Tässä kohtaa projektin uudeksi nimeksi valittiin MISP: Malware Information Sharing Platform. Nimen keksi NATO:n Alex Vandurme. Tammikuussa 2013 Andras Iklody nimettiin MISP-projektin pääasialliseksi kehittäjäksi. Samaan aikaan toisetkin organisaatiot

alkoivat käyttämään ohjelmistoa, mainostaen sitä CERT-yhteisöissä(CERT-EU, CIRCL ja monissa muissa). Andreas Iklody on projektin johtava kehittäjä ja työskentelee CIRCL:lle. (MISP2 2021.).

MISP -projektin laajentuessa se ei enää kata vain haittaohjelmien indikaattoreita, vaan myös huijaus- ja haavoittuvuustiedon jakaminen on osa palvelua. Palvelun nimi on nykyään MISP Threat Sharing, joka sisältää MISPin ydinohjelmiston lisäksi paljon muita työkaluja (PyMISP), sekä formaatteja MISP:in tueksi kuten core format, MISP taksonomiat ja varoituslistat. MISP on nykyään yhteisövetoinen projekti, jota johtaa ryhmä vapaaehtoisia (MISP2 2021.).

3.2 Mikä MISP on

MISP eli Malware Information Sharing Platform on avoimen lähdekoodin ilmainen uhkatiedustelualusta. Alustaa käytetään eri yhteisöjen välillä kohdennettujen hyökkäysten vaarantumisindikaattorien(IoC), uhkatiedon, talouspetosinformaation, haavoittuvuuksien ja jopa terrorisminvastaisen informaation varastoimiseen, jakamiseen, sekä vastaavuuden tarkasteluun. (Fotiadou ym. 2020.)

MISP mahdollistaa organisaatioille uhkatiedustelun informaation, indikaattoreiden, uhkatahojen tietojen, tai minkä tahansa uhkan jakamisen, joka sitten voidaan koostaa MISP:ssä. MISP:n hyöty on tunnettujen uhkien ja haittaohjelmien yhteisöllinen tiedonjako, tavoitteena kohdennettujen hyökkäysten vastatoimien kehittäminen sekä havainnoinnin ja ennaltaehkäisevien toimien pohjustaminen. (Fotiadou ym. 2020.)

Koska MISP toimii vertaisverkkoperiaatteella, useat eri toimijat voivat jakaa tietoja samanaikaisesti keskenään. Synkronointiprotokolla toimii kolmen perusperiaatteen varassa, jotka ovat: tehokkuus, tarkkuus ja skaalautuvuus. Käyttäjät voivat määrittää yksityiskohtaisesti miten heidän MISP:iin syöttämää tietoa jaetaan. Tietoa voidaan jakaa esimerkiksi organisaatiotasolla, yhteisötasolla, tai erikseen määritetyillä jakamisryhmien tasoilla. (Fotiadou ym. 2020.)

Jaettua tietoa kutsutaan nimityksellä ”Event” eli tapahtuma, joka koostuu attribuuttilistasta. Attribuuttilista sisältää muun muassa kohde IP-osoitteet sekä tiedostojen tiivisteet. Attribuutit tunnistetaan tuple -tietotyypillä: (i) kategoria, (ii) tyyppi, (iii) arvo. Tämän lisäksi tapahtumaan linkitetään tekstimuotoista tietoa, joka sisältää mahdollisuuksien mukaan

esimerkiksi, päivämäärän, uhkatason, kuvauksen tapahtumasta, organisaation tiedot sekä MISP:n Galaxies metodin tiedot. (Fotiadou ym. 2020.)

MISP:n Galaxies metodi on tarkoitettu suurien objektien eli klustereiden käsittelyyn, ja voidaan liittää MISP tapahtumaan tai attribuuttiin. Klusteri voi rakentua yhdestä tai useammasta elementistä. Elementti esitetään avain-arvo-pareina. MISP Galaxiesissa on oletussanastoja, mutta ne voidaan ylikirjoittaa, korvata tai päivittää käyttäjän tarpeen mukaan. Sanastot koostuvat olemassaolevista standardeista, kuten MISP, Veris(The Vocabulary for Event Recording and Incident Sharing), STIX(Structured Threat Information Expression), ATT&CK(MITRE Adversarial Tactics, Techniques, and Common Knowledge), tai käyttäjän organisaation määrittelemistä sanastoista. Olemassaolevia klustereita voi käyttää sellaisenaan tai kaavana, jonka pohjalta voidaan muokata omiin tarpeisiin sopivammat klusterit. Klustereiden jakamisen yksityisyys voidaan rajoittaa klusterikohtaisesti. (CIRCL1 2021.)

MISP:n tavoitteena on

- helpottaa havaittujen haittaohjelmien ja kyberhyökkäyksien teknisen ja ei teknisen tiedon talletusta.
- automatisoida haittaohjelmien ja niiden ominaisuuksien välisten relaatioiden luominen.
- tallettaa tietoa jäsennetyssä muodossa, jotta voidaan mahdollistaa tietokannan tietojen automaattinen syöttäminen järjestelmiin tai forensiikkatyökaluihin.
- luoda verkkoon tunkeutumisen tunnistamisjärjestelmän(NIDS, Network Intrusion Detection System) sääntöjä, joita voidaan tuoda IDS järjestelmiin(esim. IP-osoitteita, domain nimiä, haittatiedostojen tiivisteitä, muistikaavat)
- jakaa haittaohjelma- ja uhkamääreitä toisten osapuolten ja luotettujen ryhmien kanssa.
- parantaa haittaohjelmien havainnointia ja vastustuskeinoja, edistääkseen tiedonvaihtoa organisaatioiden välillä.
- luoda luotettava alusta.
- tallettaa toisten instanssien tieto lokaalisti, taaten hakujen luottamuksellisuus (CIRCL3 2020).

3.3 MISP:n toiminta

MISP rakentuu tapahtumista, syötteistä, yhteisöistä ja tilaajista. Kun tapahtuma on luotu, liittää MISP sen tiettyyn syötteeseen, joka toimii keskitettynä tapahtumalistana. Tämä tapahtumalista kuuluu tietylle organisaatiolle ja sisältää määriteltyjä tapahtuma tai ryhmittelyspesifikaatioita. MISP koostuu luotettavista, riippumattomista käyttäjistä ja

organisaatioiden uhka-aineistoista, jotka molemmat ovat MISP:n käyttäjäkunnan syöttämiä. Liityttyään MISP yhteisöihin, organisaatiot voivat tilata syötteitä, jotka liittyvät heidän alansa uhkiin. Syötteen tilaamisen jälkeen organisaatiot voivat vastaanottamaan API pull -pyynnöillä havaintomoottorien sääntöjä, palomuurien estolistoja ja muuta vastaavaa dataa SIEM -alustoilta. Tämän lisäksi organisaatiot voivat osallistua näiden tietojen päivittämiseen lisäämällä omia syötteitään ja tapahtumiaan muiden vastaanotettavaksi. (CIRCL3 2020.)

MISP:a voi käyttää erilaisista käyttöliiittymistä. Vaihtoehtoina ovat selainpohjainen verkkokäyttöliittymä(Tietoturva-analyytikoille tai tietoturvatapahtuemien tutkijoille), tai REST API rajapinta(järjestelmille jotka antavat ja vastaanottavat IoC:tä). MISP:n alkuperäinen tarkoitus on olla vakaa alusta, joka mahdollistaa sujuvan toiminnan uhkatiedon paljastamiseen, jalostamiseen ja hyödyntämiseen. MISP:ssä on neljä vaihtoehtoa tapahtumien ja niiden attribuuttien jakelulle. Tapahtumia ja niiden attribuutteja voidaan jakaa joko oman organisaation sisäisesti, valituissa yhteisöissä, yhdistetyissä yhteisöissä tai niitä voidaan jakaa kaikille yhteisöille. (CIRCL3 2020; Cyware 2020)

3.4 MISP ja TIP eroja

MISP toimii keskitettynä solmukohtana uhkatiedolle, mutta siitä puuttuu monia ominaisuuksia, jotka löytyvät todellisista uhkatiedon alustoista(TIP. Threat Intelligence Platform). MISP:n puutteita TIP:hen verrattuna ovat seuraavat: (Cyware 2020)

Monilähteinen uhkatiedon syöte

Todellinen TIP voi kerätä taktista ja teknistä tietoa lukuisista ulkoisista lähteistä, kuten uhkatiedon toimittajat, regulatiiviset tahot, vertaisorganisaatiot, ISAC-tiedonvaihtoryhmät, dark web ja muut lähteet. TIP myöskin voi automaattisesti muuttaa, varastoida ja järjestellä uhkadataa useista formaateista, kuten STIX, XML(Extensible Markup Language), JSON(JavaScript Object Notation), CYBOX(Cyber Observable Expresision), MAEC(Malware Attribute Enumeration and Characterization). (Cyware 2020)

MITRE ATT&CK visualisaatiot

Kehittynyt TIP voi luoda visualisaatioita MITRE ATT&CK kehyksestä tietoturva-analyytikolle, antaen oleellista tietoa hyökkääjän TTP:stä(Tactics, Techniques and Procedures).

Tämä mahdollistaa trendien tunnistamisen kyberhyökkäysketjussa, jotta nämä tiedot voidaan suhteuttaa raportoidun tiedon kanssa. (Cyware 2020)

3.5 Vaihtoehtoja MISP:lle

Avoimen lähdekoodin ohjelmistoista ei löydy suoranaista yhden ohjelmiston vaihtoehtoa MISP:lle. Kyseessä olisi ennemminkin useamman eri ohjelmiston yhteensovittaminen, jos haluaa MISP:ä vastaavan tuotteen. Maksullisia ratkaisuja löytyykin jo enemmän ja vertaankin tässä lopuksi IBM X-Forcea ja MISP:ä toisiinsa siltä osin kuin mahdollista.(Vandeplas, C 2021; Van Impe, K 2015)

Molemmat ohjelmistot käyttävät JSON:iin perustuvaa REST -ohjelmistorajapintaa mahdollistaakseen käyttäjälle saumattoman integraation olemassaolevaan infrastruktuuriin. Yhtäläisyytenä todettakoon myös se, että molemmissa ohjelmistoissa on mahdollista tuoda tietoa STIX-formaattia hyödyntäen. Tiedon vieminen taasen onnistuu MISP:llä vain TAXII(Trusted Automated Exchange of Intelligence Information) formaatissa, kun se on IBM X-Forcessa mahdollista toteuttaa TAXII- ja STIX -formaateissa.(Van Impe, K 2015)

Tiedon jakaminen MISP:ssä tapahtuu tallettamalla haluttu tieto paikallisesti ja rajaamalla tiedon saatavuutta sivulla 5 löytyvillä ryhmittelyillä. IBM X-Force sen sijaan tallettaa tiedot pilveen. Tiedon saatavuutta pilvestä voidaan rajata niin sanotuilla kokoelmilla. Kokoelmat ovat tietopaketteja, jotka liittyvät tietoturvatutkintaan ja kokoelmien saatavuutta sekä näkyvyyttä voidaan rajata mielivaltaisesti. Kokoelmat voivat myös olla joko julkisia tai yksityisiä.(Van Impe, K 2015)

IBM X-Forcen ongelma MISP:iin nähden on tiedon tallennnus pilveen paikallisen tallentamisen sijaan. Jos esimerkiksi organisaatiossa käsitellään arkaluonteista tietoa, kuten valtiollista tietoa, voi olla laitonta jopa tallentaa tietoa pilvipalveluun.(Van Impe, K 2015)

4 MISP -ASENNUS PALVELIMELLE

Opinnäytetyössäni MISP asennettiin Debian 10 -palvelimelle. Asennus toteutettiin komentoriviltä ja hyödynnettiin MISP:n omaa dokumentaatiota GitHubissa.(GitHub 2021)

4.1 Perusasennuksen valmistelut

MISP -palvelimen perusasennuksen valmisteluina komentoriviltä suoritettiin ensin asennuksessa tarpeellisten käyttäjien luomiseen tarpeelliset komentosarjat, sekä asennuksessa välttämättömien muuttujien luominen. Muuttujia luotiin tietokannan, OpenSSL -sertifikaatin, sudo käyttäjän ja monen muun tarpeellisen luontiin ja tulevaa käyttöä varten, kuten kohdassa Kuva 1 on havainnollistettu.

```
root@debian:/home/testi# MISPvars () {
>   debug "Setting generic ${LBLUE}MISP${NC} variables shared by all flavours" 2> /dev/>   debug "Setting generic ${LBLUE}MISP${NC} variables shared by all flavours" 2> /dev/null^C
root@debian:/home/testi# <snippet-begin 0_global-vars.sh>
root@debian:/home/testi# # $ eval "$(curl -fsSL https://raw.githubusercontent.com/MISP/MISP/2.4/docs/generic/globalVariables.md | awk '/^# <snippet-begin/,0' | grep -v \`\`\`)"
root@debian:/home/testi# # $ MISPvars
root@debian:/home/testi# MISPvars () {
>   debug "Setting generic ${LBLUE}MISP${NC} variables shared by all flavours" 2> /dev/null
>   # Some distros have no openssl installed by default, catch that exception.
>   $(openssl help 2> /dev/null) || (echo "No openssl, please install to continue"; exit -1)
>   # Local non-root MISP user
>   MISP_USER="${MISP_USER:-misp}"
>   MISP_PASSWORD="${MISP_PASSWORD:-$(openssl rand -hex 32)}"
>
>   # Cheap distribution detector
>   FLAVOUR="$(. /etc/os-release && echo "$ID"| tr '[:upper:]' '[:lower:]')"
>   STREAM="$(. /etc/os-release && echo "$NAME"| grep -o -i stream |tr '[:upper:]' '[:lower:]')"
>   DIST_VER="$(. /etc/os-release && echo "$VERSION_ID")"
>   DISTRI=${FLAVOUR}${DIST_VER}${STREAM}
```

Kuva 1. Tarpeellisten komentotiivisteiden luominen muuttujia ja muita tarpeellisia osia varten

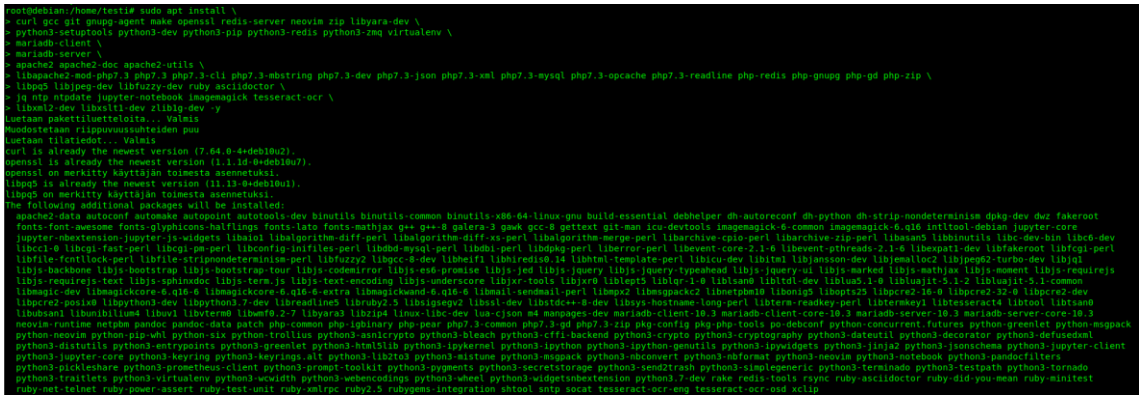
Tästä jatkettiin Kuva 2 antaman havainnollistuksen tavoin Debian ”buster” palvelinjärjestelmän ohjelmistojen asentamiseen tarvittavien komentotiivisteiden luomiseen, kuten OpenSSH palvelimen, sekä etckeeper- ja sudo-järjestelmävalvojan työkalut. Tämän lisäksi luotiin komentotiiviste käyttäjän ”MISP USER” lisäämiseksi STAFF ja WWW-DATA-ryhmiin.

```
root@debian:/home/testi#  <snippet-begin 0_sudoKeeper.sh>
bash: lauseoppivirhe lähellä odottamatonta avainsanaa ”newline”
root@debian:/home/testi# # check if sudo is installed
root@debian:/home/testi# checkSudoKeeper () {
>   echo "Checking for sudo and installing etckeeper"
>   if [[ ! -f $(which sudo) ]]; then
>     echo "Please enter your root password below to install etckeeper"
>     su -c "apt install etckeeper -y"
>     echo "Please enter your root password below to install sudo"
>     su -c "apt install sudo -y"
>     echo "Please enter your root password below to install sudo"
>     su -c "apt install curl -y"
>     echo "Please enter your root password below to add ${MISP_USER} to sudo group"
>     su -c "/usr/sbin/adduser ${MISP_USER} sudo"
>     echo "We added ${MISP_USER} to group sudo and now we need to log out and in again."
>     exit
>   else
>     sudo apt update
>     sudo apt install etckeeper -y
>   fi
> }
```

Kuva 2. Debian "buster" vähimmäisohjelmistojen sekä työkalujen asennuksessa tarvittavien komentotiivisteiden luonti

4.2 MISP-alustan asentaminen Debian 10 palvelimelle

Komentotiivisteiden ja käyttäjien luonnin jälkeen voitiin aloittaa varsinainen asennustyö. Tämä aloitettiin Kuva 3 mukaisella LAMP avoimen lähdekoodin ohjelmistojen, sekä muiden riippuvuuksien asennuksella. Esimerkiksi haveged, joka on ennustamaton satunnaislukugeneraattori. Lopuksi kaikki tehdyt muutokset aktivoitiin uudelleenkäynnistämällä apache2 palvelinohjelmisto komennolla: ”*sudo systemctl restart apache2*” .



Kuva 3. LAMP -ohjelmistojen sekä muiden riippuvuuksien asennus

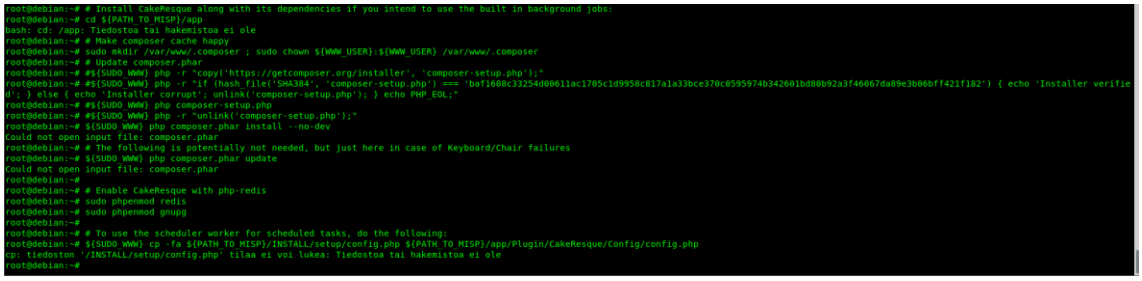
Tämän jälkeen MISP alusta voitiin asentaa. Kuten Kuva 4 esimerkistä näkee, MISP ladattiin hyödyntäen git:iä /var/www kansioon, samalla asetettiin git olemaan välittämättä

tiedostojärjestelmän oikeuksien eroista, asennettiin STIX:n kirjastot sekä tarpeelliset riippuvuudet, joita MISP asennuksessa ja käytössä tarvittiin.

```
root@debian:/home/testi# cd ${PATH_TO_MISP}
root@debian:~# ${SUDO_WWW} git clone https://github.com/MISP/MISP.git ${PATH_TO_MISP}
Cloning into 'MISP'...
remote: Enumerating objects: 139401, done.
remote: Counting objects: 100% (2247/2247), done.
remote: Compressing objects: 100% (758/758), done.
remote: Total 139401 (delta 1586), reused 2006 (delta 1418), pack-reused 137154
Receiving objects: 100% (139401/139401), 126.10 MiB | 4.21 MiB/s, done.
Resolving deltas: 100% (105421/105421), done.
root@debian:~# ${SUDO_WWW} git submodule update --init --recursive
fatal: not a git repository (or any of the parent directories): .git
root@debian:~# # Make git ignore filesystem permission differences for submodules
root@debian:~# ${SUDO_WWW} git submodule foreach --recursive git config core.filemode false
fatal: not a git repository (or any of the parent directories): .git
root@debian:~#
root@debian:~# # Make git ignore filesystem permission differences
root@debian:~# ${SUDO_WWW} git config core.filemode false
fatal: not in a git directory
root@debian:~#
root@debian:~# # Create a python3 virtualenv
root@debian:~# ${SUDO_WWW} virtualenv -p python3 ${PATH_TO_MISP}/venv
Already using interpreter /usr/bin/python3
Using base prefix '/usr'
```

Kuva 4. MISP-alustan asennus

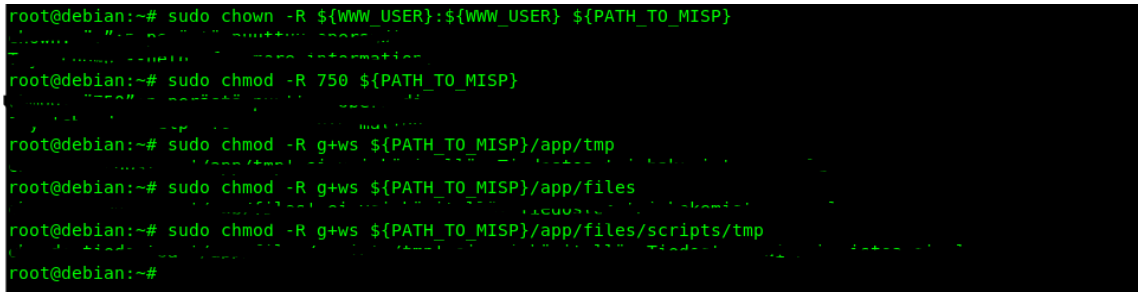
Lopuksi asennettiin CakePhP -plugin ’cakeresque’ ja päivitettiin se Kuva 5 mukaisella tavalla. Cakeresque on kirjasto jolla voidaan luoda taka-alalle prosesseja, jotka voidaan prosessoida ilman verkkoyhteyttä myöhempänä ajankohtana.



Kuva 5. Cakeresque pluginin asennus

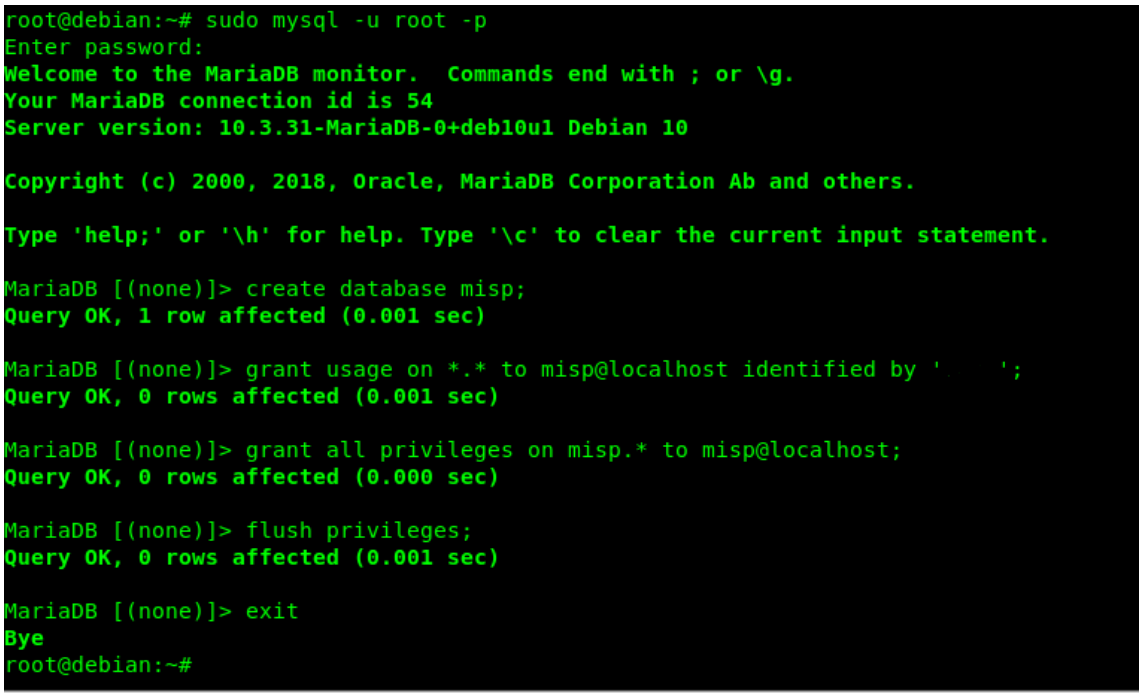
4.3 Oikeuksien varmistus sekä tietokannan ja tietokantakäyttäjän luominen

Varmistetaan, että tähänastiset oikeudet ovat asetettu oikein Kuva 6 mukaisilla komennoilla.



Kuva 6. Oikeuksien tarkastus

Oikeuksien tarkastuksen jälkeen Kuva 7 komennoilla luotiin tietokanta ’misp’ ja annettiin käyttäjälle kaikki oikeudet sekä pääsy kaikkialle aiemmin määritellyllä salasanalla.



Kuva 7. MariaDB-tietokannan luominen ja käyttäjän oikeuksien antaminen

Lopuksi tuotiin tyhjä MISP -tietokanta MariaDB:n tietokannan rakenteeksi Kuva 8 komennolla.

Kuva 8. Tyhjän MISP-tietokannan tuominen

4.4 Apachen konfigurointi

Seuraavaksi tehtiin virtuaalisen Apache web-palvelimen konfigurointi web juureen, sekä SSL-sertifikaatin asennus Kuva 9 esimerkin mukaisesti ja lopuksi vielä virtuaalisen palvelimen aktivointi, kuten Kuva 10 voidaan havaita.

```
root@debian:~# # Now configure your Apache webserver with the DocumentRoot ${PATH_TO_MISP}/app/webroot/
root@debian:~#
root@debian:~# # If the apache version is 2.4:
root@debian:~# sudo cp ${PATH_TO_MISP}/INSTALL/apache.24.misp.ssl /etc/apache2/sites-available/misp-ssl.conf
root@debian:~#
root@debian:~# # Be aware that the configuration files for apache 2.4 and up have changed.
root@debian:~# # The configuration file has to have the .conf extension in the sites-available directory
root@debian:~# # For more information, visit http://httpd.apache.org/docs/2.4/upgrading.html
root@debian:~#
root@debian:~# # If a valid SSL certificate is not already created for the server, create a self-signed certificate:
root@debian:~# sudo openssl req -newkey rsa:4096 -days 365 -nodes -x509 \
> -subj "/C=${OPENSSL_C}/ST=${OPENSSL_ST}/L=${OPENSSL_L}/O=${OPENSSL_O}/OU=${OPENSSL_OU}/CN=${OPENSSL_CN}/emailAddress=${OPENSSL_EMAILADDRESS}" \
> -keyout /etc/ssl/private/misp.local.key -out /etc/ssl/private/misp.local.crt
Generating a RSA private key
.....................................................................................................................++++
.....................................................................................++++
writing new private key to '/etc/ssl/private/misp.local.key'
-----
```

Kuva 9. Apache web-palvelimen konfigurointi sekä SSL-sertifikaatin asennus

```
root@debian:~# # activate new vhost
root@debian:~# sudo a2dissite default-ssl
Site default-ssl already disabled
root@debian:~# sudo a2ensite misp-ssl
root@debian:~# # Restart apache
root@debian:~# sudo systemctl restart apache2
```

Kuva 10. Virtuaalisen palvelimen aktivointi

Seuraavaksi suoritettiin Kuva 11 mukainen lyhyt skripti logrotaten eli lokien kierron aktivoimiseksi palvelimella, jotta vanhat ja liian suuret lokitiedostot voidaan poistaa.

```
# MISP saves the stdout and stderr of its workers in ${PATH_TO_MISP}/app/tmp/logs
# To rotate these logs install the supplied logrotate script:

sudo cp ${PATH_TO_MISP}/INSTALL/misp.logrotate /etc/logrotate.d/misp
sudo chmod 0640 /etc/logrotate.d/misp
```

Kuva 11. Logrotate skripti

4.5 MISP konfigurointi

MISP konfiguraatio aloitettiin Kuva 12 mukaisilla komentorivikomennoilla, joilla kopioitiin konfiguraatiossa tarvittavat mallitiedostot.

```
# There are 4 sample configuration files in ${PATH_TO_MISP}/app/Config that need to be copied
${SUDO_WWW} cp -a ${PATH_TO_MISP}/app/Config/bootstrap.default.php ${PATH_TO_MISP}/app/Config/bootstrap.php
${SUDO_WWW} cp -a ${PATH_TO_MISP}/app/Config/database.default.php ${PATH_TO_MISP}/app/Config/database.php
${SUDO_WWW} cp -a ${PATH_TO_MISP}/app/Config/core.default.php ${PATH_TO_MISP}/app/Config/core.php
${SUDO_WWW} cp -a ${PATH_TO_MISP}/app/Config/config.default.php ${PATH_TO_MISP}/app/Config/config.php


echo "<?php
class DATABASE_CONFIG {
        public \$default = array(
                'datasource' => 'Database/Mysql',
                //'datasource' => 'Database/Postgres',
                'persistent' => false,
                'host' => '$DBHOST',
                'login' => '$DBUSER_MISP',
                'port' => 3306, // MySQL & MariaDB
                //'port' => 5432, // PostgreSQL
                'password' => '$DBPASSWORD_MISP',
                'database' => '$DBNAME',
                'prefix' => '',
                'encoding' => 'utf8',
        );
}" | ${SUDO_WWW} tee ${PATH_TO_MISP}/app/Config/database.php
```

Kuva 12. MISP -konfiguraatiotiedostojen kopioiminen ja konfiguraatio

Sen jälkeen varmistettiin oikeuksien säilyneen ennallaan kuten Kuva 13 komentorivi esittää.

```
# and make sure the file permissions are still OK
sudo chown -R ${WWW_USER}:${WWW_USER} ${PATH_TO_MISP}/app/Config
sudo chmod -R 750 ${PATH_TO_MISP}/app/Config
```

Kuva 13. Oikeuksien säilymisen varmistus

Lopuksi vielä asetettiin taustaprosessi aktivoitumaan Kuva 14 mukaisesti kun palvelin käynnistetään.

```
# To make the background workers start on boot
sudo chmod +x ${PATH_TO_MISP}/app/Console/worker/start.sh

echo "[Unit]
Description=MISP background workers
After=mariadb.service redis-server.service

[Service]
Type=forking
User=${WWW_USER}
Group=${WWW_USER}
ExecStart=${PATH_TO_MISP}/app/Console/worker/start.sh
Restart=always
RestartSec=10

[Install]
WantedBy=multi-user.target" |sudo tee /etc/systemd/system/misp-workers.service
sudo systemctl daemon-reload
sudo systemctl enable --now misp-workers.service

if [ ! -e /etc/rc.local ]
then
    echo '#!/bin/sh -e' | sudo tee -a /etc/rc.local
    echo 'exit 0' | sudo tee -a /etc/rc.local
    sudo chmod u+x /etc/rc.local
fi
```

Kuva 14. Taustatyöläisten aktivointi palvelimen käynnistyksen yhteydessä

Lopuksi alustettiin MISP konfiguraatio, kuten Kuva 15 voidaan havaita, sekä määritettiin oletusasetuksia, jotta MISP toimisi mahdollisimman selkeästi sekä ongelmattomasti heti ensimmäisestä käynnistyksestä lähtien. Samalla myös varmistettiin tietokantojen päivityksien asennuksen onnistuminen automaattisesti ilman sisäänkirajutumista. Lisäksi tehtiin huomattava määrä muita automaatioihin, ulkonäköön ja reititykseen liittyviä hienosäätöjä.

```
# <snippet-begin 2_core-cake.sh>
# Core cake commands to tweak MISP and aleviate some of the configuration pains
# The ${RUN_PHP} is ONLY set on RHEL/CentOS installs and can thus be ignored
# This file is NOT an excuse to NOT read the settings and familiarize ourselves with them ;)

coreCAKE () {
  debug "Running core Cake commands to set sane defaults for ${LBLUE}MISP${NC}"

  # IF you have logged in prior to running this, it will fail but the fail is NON-blocking
  ${SUDO_WWW} ${RUN_PHP} -- ${CAKE} userInit -q

  # This makes sure all Database upgrades are done, without logging in.
  ${SUDO_WWW} ${RUN_PHP} -- ${CAKE} Admin runUpdates

  # The default install is Python >=3.6 in a virtualenv, setting accordingly
  ${SUDO_WWW} ${RUN_PHP} -- ${CAKE} Admin setSetting "MISP.python_bin" "${PATH_TO_MISP}/venv/bin/python"
```

Kuva 15. Konfiguraation alustus

Konfiguroinnin jälkeen MISP on valmiina alustaa käyttävän tahon valitsemien syötteiden hankintaa, käyttäjähallintaa ja muuta itse palvelussa ennen alustan käyttöönottoa tehtävää työtä varten.

5 MISP GUI:N KONFIGUROINTI

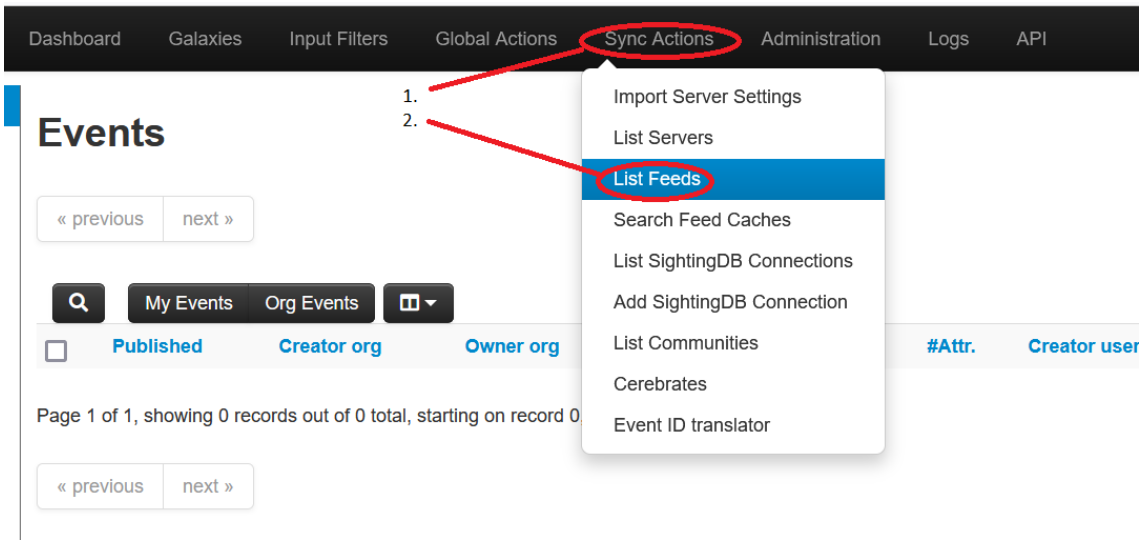
Viimeisenä vaiheena opinnäytetyössäni on suorittaa esimerkkisyötteen aktivointi ja syötteen käyttöönotto käyttäen MISP GUI:ta. Näin voidaan todeta, että asennus on onnistunut ja MISP instanssi toimii suunnitellusti. Syötteiden aktivointi ja käyttöönotto toteutettiin seuraamaalla CIRCL:n dokumentoimaa ohjeistusta MISP-instanssin perusasetusten toteuttamiseksi(CIRCL2 2021).

5.1 Syötteiden aktivointi

Syötteet ovat helppo tapa kerätä paikallista tai ulkoisesti jaettua tietoa MISP instanssiin, eikä syötteiden kerääminen vaadi ohjelmointitaitoja. Syötteitä on joko etä- tai paikallisina resursseina. Resurssit sisältävät indikaattoreita, joita voidaan tuoda MISP:iin määrätyin aikavälein. Syötteitä voidaan tuoda lähes missä tahansa formaatissa. Formaatti voi olla esimerkiksi CSV, vapaa teksti tai MISP.

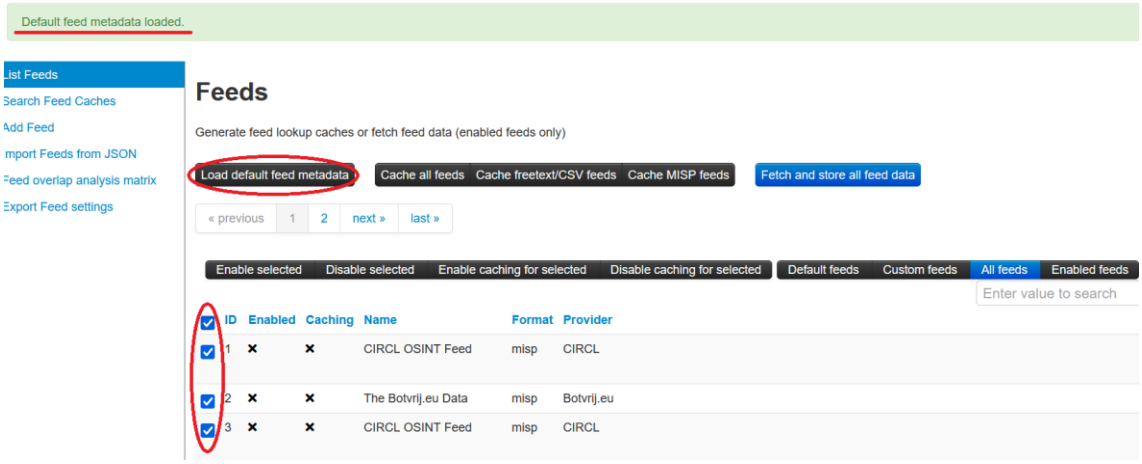
5.2 Oletussyötteiden haku ja lataus

Syötteiden aktivointi toteutetaan GUI:n ’Sync Actions’ -pudotusvalikon alta löytyvältä ’List Feeds’ -sivulta. Sivulle navigointi tapahtuu Kuva 16 osoittamalla tavalla.



Kuva 16. List Feeds -sivulle navigointi

List Feeds sivulta löytyvät MISP -projektin avoimen lähdekoodin oletussyötteet. Oletussyötteet voi ladata MISP -instanssiin valitsemalla halutut syötteet rasti ruutuun -menetelmällä ja sitten painamalla ’Load default feed metadata’ -nappia. Kuva 17 annetaan esimerkki, kuinka molemmat esimerkkisyötteet on valittu ja sivun antama palaute näkyy ’Load default metadata’ napin painalluksen jälkeen.

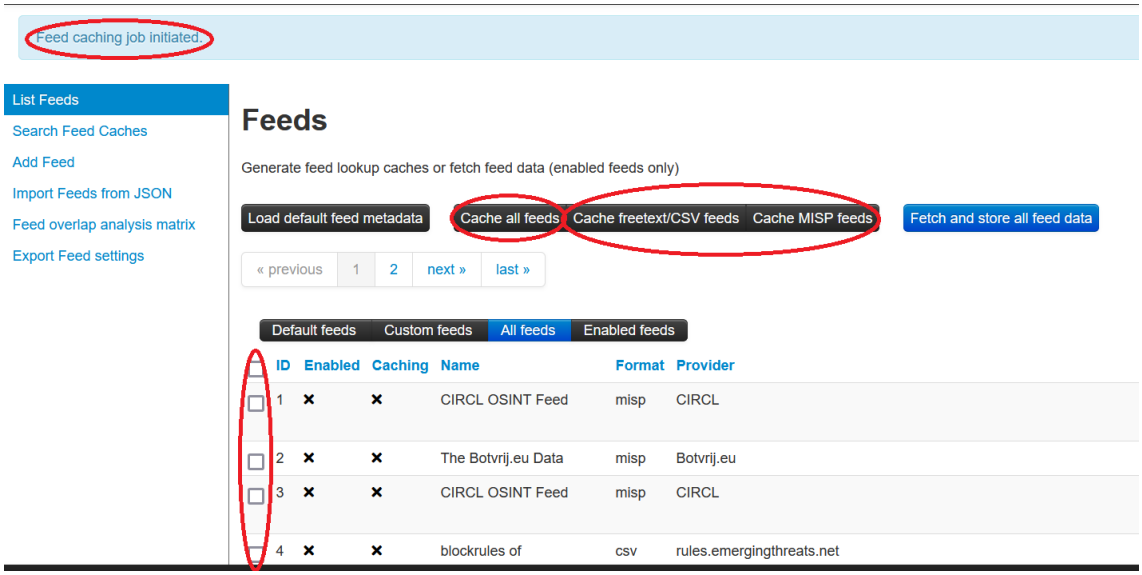


Kuva 17. Esimerkkisyötteiden valinta ja syötteiden latauksen palaute

Painalluksen jälkeen MISP -instanssi luo uudet syötteet tuomalla merkinnät tiedostosta ’app/files/feed-metadata/defaults.json’ -tietokantaan. Toiminnallisuus tarkistaa syötteiden URL:t duplikaattien varalta, joten saman URL:n omaavia kirjauksia ei tuoda. Tämän lisäksi tällä toiminnallisuudella ei päällekirjoiteta jo olemassaoleviin syötteisiin. Näin myös varmistetaan se, ettei paikallisia muokkauksia, kuten nimi, jakelu tai status tiloja koskaan päällekirjoiteta.

5.3 Syötteiden tallentaminen välimuistiin

Syötteiden tallentaminen välimuistiin lataa syötteen tiedot Redis palvelimelle MISP instanssissasi ja mahdollistaa syötteen atribuuttien sekä ”syötteen osumien” vertailun tapahtumanäkymässä(Event View). Ennen syötteen välimuistiin tallentamista tulee se ottaa käyttöön luvun 5.4 esimerkin mukaisesti. Syötteiden välimuistiin tallentaminen tapahtuu ’Feeds’ sivun yläreunassa olevia nappeja käyttämällä, kuten Kuva 18 osoittaa.

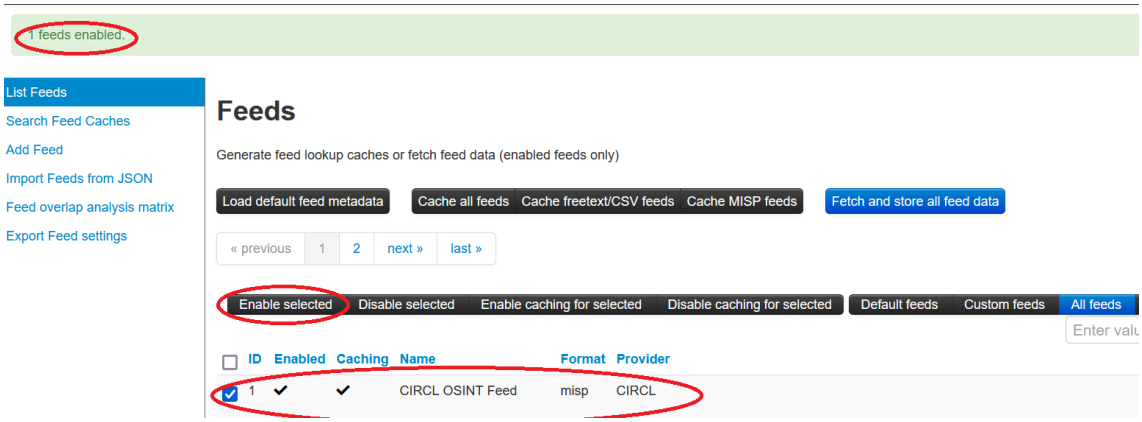


Kuva 18. Syötteiden tallentaminen välimuistiin

Valittavana on kaikkien syötteiden vapaamuotoisessa tekstimuodossa ja CSV-muodossa olevien syötteiden, tai MISP-formaatissa olevien syötteiden tallentaminen. Eri tallennusmuodot ja Redis -palvelin eivät kuulu opinnäytetyön aihealueeseen.

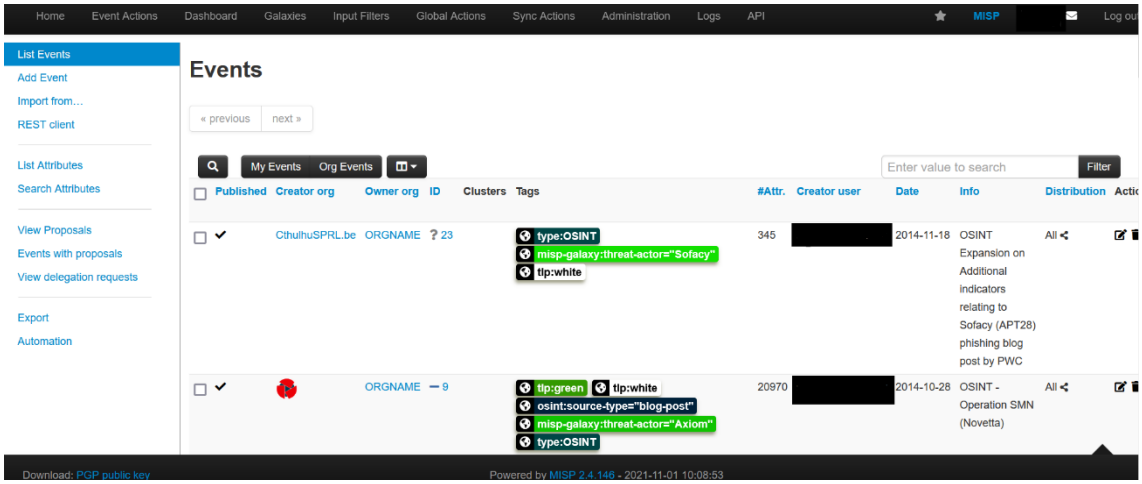
5.4 Syötteiden käyttöönotto

Syötteet voidaan ottaa käyttöön sen jälkeen kun ne ovat ladattu MISP instanssiin. Syötteen käyttöönotto tapahtuu Kuva 19 esimerkin mukaisesti valitsemalla haluttu syöte rasti ruutuun -periaatteella ja sen jälkeen ilmestyvässä näkymässä painamalla ’Enable Selected’ -nappia sekä lopuksi ’Fetch and store all feed data’ -nappia painamalla.



Kuva 19. Syötteen käyttöönotto

Kun syötteet on otettu käyttöön, ne löytyvät ’Home’ -valikosta. Kuva 20 perusteella voimme todeta, että uusia syötteitä on käytettävissä ja että MISP -instanssimme toimii.



Kuva 20. Syötenäkymä

Syötteitä voidaan käyttää IoC:den tutkinnassa tukena, jotta voidaan varmistua onko tapahtuma ollut todellinen hyökkäys(True positive), vai normaalia skannausta, jota verkossa tapahtuu jatkuvasti(False positive).

6 LOPUKSI

Opinnäytetyö oli onnistunut ja täytti projektille asetetut vaatimukset. Projektissa onnistuttiin keräämään runsaasti teoriatietoa MISP-alustasta. Lisäksi onnistuttiin tuottamaan alusta, jolla voidaan testata MISP:n toimivuutta sekä kehittää sitä tarpeen mukaan. Alusta oli toimiva ja siinä oli vaaditut ominaisuudet, kuten toimiva verkkokäyttöjärjestelmä syötteineen. Alustan koekäytöllä voidaan näinollen tutkia MISP:stä mahdollisesti koituvia hyötyjä tietoturvayritykselle.

Alustan asennuksessa ei varsinaisesti kohdattu haasteita ja asennus sekä käyttöönotto sujuivat ongelmitta. Teorian tutkimisessa suurimmaksi haasteeksi nousi lähteiden vähäinen määrä.

Jos projektia jatketaan eteenpäin, tulee seuraavaksi kokeilla useamman syötteen aktivoimista. Tätä tulisi seurata omien indikaattorien ja syötteiden luominen, sekä lopulta syötteiden datan ja todellisen NIDS-tapahtuman vertailu. Tämän lisäksi tulisi testata käyttäjien luomista, sekä käyttäjäryhmien ja käyttäjien oikeuksien määrittelyä.

LÄHTEET

Checkpoint 2021. Biggest Cyber Security Challenges in 2021. Viitattu 30.09.2021. https://www.t.com/cyber-hub/cyber-security/what-is-cybersecurity/biggest-cyber-security-challenges-in-2021/

Christophe Vandeplas 2021. MISP alternatives. Viitattu 01.11.2021. https://linuxsecurity.expert/tools/misp/alternatives/

CIRCL1 2021. Galaxies. Viitattu 02.10.2021. https://circl.lu/doc/misp/galaxy/

CIRCL2 2021. Managing Feeds. Viitattu 28.10.2021. https://www.circl.lu/doc/misp/managing-feeds/

CIRCL3 2020. MISP - Open Source Threat Intelligence Platform. Viitattu 30.09.2021. https://circl.lu/services/misp-malware-information-sharing-platform/#is-there-a-misp-user-guide

Cyware 2020. What is Malware Information Sharing Platform (MISP)?. Viitattu 30.09.2021. https://cyware.com/educational-guides/cyber-threat-intelligence/what-is-malware-information-sharing-platform-misp-b28e

Fotiadou, K.; Velivassaki, T-H.; Voulkidis, A.; Railis, K.; Trakadas, P & Zahariadis,T 2020 Incidents Information Sharing Platform for Distributed Attack Detection. Viitattu 02.10.2021. https://ieeexplore.ieee.org/abstract/document/9079479

GitHub 2021. MISP Install Documentation. Viitattu: 26.09.2021. https://misp.github.io/MISP/xINSTALL.debian10/

Koen Van Impe 2015. Comparing Different Tools for Threat Sharing. Viitattu 01.11.2021. https://securityintelligence.com/comparing-different-tools-for-threat-sharing/

MISP1 2021. MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. Viitattu 30.09.2021. https://www.misp-project.org/

MISP2 2021. Who is behind the MISP project?. Viitattu 02.10.2021. https://www.misp-project.org/who/