jamk

Arkime-pakettianalysaattorin käyttö verkkoliikenteen auditoinnissa

Otto Blomberg

Opinnäytetyö, AMK
Joulukuu 2023
Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Blomberg, Otto

Arkime-pakettianalysaattorin käyttö verkkoliikenteen auditoinnissa

Jyväskylä: Jyväskylän ammattikorkeakoulu. Joulukuu 2023, 42 sivua.

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Opinnäytetyön tarkoituksena oli syventyä tutkimaan Arkime-pakettianalysaattorin soveltuvuutta työkaluna tietoturva-auditoinneissa. Tutkimuksen päämääränä oli tarkastella Arkimen ominaisuuksia ja arvioida niiden hyödyllisyyttä verkkoliikenteen analysoinnissa. Tavoitteena oli tuottaa olennaista tietoa niille ammattilaisille ja organisaatioille, jotka harkitsevat Arkimen käyttöönottoa tietoturvatarkastuksiin tai jo hyödyntävät ohjelmistoa osana päivittäisiä työtehtäviään.

Opinnäytetyön alkuvaiheessa taustoitettiin tutkimuksen kontekstia ja laadittiin tarkentavat tutkimuskysymykset. Teoriaosuudessa esiteltiin keskeiset käsitteet ja termit liittyen verkkoliikenteen analyysiin, jonka jälkeen paneuduttiin syvällisesti Arkimen ominaisuuksiin käyttäen hyväksi ohjelmiston käyttöliittymää. Teoreettisen osan jälkeen kuvailtiin simuloitua testijärjestelmää, jonka avulla luotiin ja hallittiin testidataa. Seuraavaksi keskityttiin analysoimaan testidataa Arkimen avulla, samalla arvioiden ohjelmiston kykyä käsitellä ja visualisoida kerättyä tietoa.

Tutkimustulosten perusteella voitiin päätellä, että Arkime osoittautui erinomaiseksi työkaluksi verkkoliikenneanalyysissä. Sen vahvuuksina korostuivat tehokas verkkodatan indeksointi, mikä tehosti käsittelyprosessia ja mahdollisti monipuolisten suodattimien ja visualisointien tehokkaan hyödyntämisen. Lisäksi Arkime osoittautui skaalautuvaksi, minkä ansiosta se soveltui erilaisten järjestelmien vaatimuksiin. Kritiikkiä kohdistui lähinnä mahdollisesti monimutkaiseen asennusprosessiin ja siihen, ettei ohjelmisto tarjonnut ominaisuutta yksittäisten pakettien tarkempaan analysointiin. Näistä huomioista huolimatta Arkime todettiin kokonaisuutena erinomaiseksi työkaluksi verkkoliikenteen analysoinnissa tietoturva-auditointien kontekstissa.

Avainsanat (asiasanat)

tietoturva, tietoliikenne, pakettianalyysi, Arkime, auditointi, verkonvalvonta

jamk

Description

Blomberg, Otto

Use of Arkime packet analyzer in network traffic auditing

Jyväskylä: JAMK University of Applied Sciences, December 2023, 42 pages.

Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The purpose of the thesis was to explore the suitability of the Arkime packet analyzer as a tool for security audits. The aim of the study was to examine the features of Arkime and assess its usefulness in analysing network traffic. The aim was to provide essential information for professionals and organisations who are considering implementing Arkime for security audits or who already use the software as part of their daily work.

In the early stages of the thesis, the context of the research was established and the research questions were formulated. In the theoretical part, key concepts and terms related to network traffic analysis were introduced, followed by an in-depth look at the features of Arkime using the software's user interface. The theoretical part was followed by a description of the simulated test system used to generate and manage the test data. Next, the focus was on analysing the test data using Arkime, while assessing the software's ability to process and visualise the collected data.

Based on the results of the study, it was concluded that Arkime proved to be an excellent tool for network traffic analysis. Its strengths were highlighted in the efficient indexing of network data, which streamlined the processing process and allowed the effective use of a wide range of filters and visualisations. In addition, Arkime proved to be scalable, making it suitable for the requirements of different systems. Criticism was mainly directed at the potentially complex installation process and the lack of a feature for a more detailed analysis of individual packages. Despite these observations, Arkime was overall found to be an excellent tool for analysing network traffic in the context of security audits.

Keywords/tags (subjects)

information security, telecommunications, packet analysis, Arkime, auditing, network monitoring

Sisältö

Kuviot

1 Johdanto

Tietoturva on muuttunut oleelliseksi osaksi nykyaikaista liiketoimintaa, kun yhä suurempi osa organisaatioiden toiminnoista siirtyy digitaaliseen ympäristöön. Tämä siirtymä on kuitenkin tuonut mukanaan myös uusia riskejä ja haasteita, jotka liittyvät verkon kautta tapahtuviin tietomurtoihin, tietovuotoihin ja muihin kyberuhkiin. Tietoturva-auditoinnit ovat nousseet keskeiseksi toimintatavaksi varmistaa organisaatioiden tietojen ja järjestelmien eheys sekä paljastaa mahdolliset haavoittuvuudet ja uhat. Auditointien osana suoritetut tietoliikenneanalyysit ovat tehokas keino varmistaa järjestelmän tietoliikenteen turvallisuus sekä sujuva toiminta.

Arkime on avoimen lähdekoodin verkkoliikenteen analysointityökalu. Se tarjoaa mahdollisuuden syvälliseen verkkoliikenteen tarkasteluun ja analysointiin, joka voi avata uusia näkökulmia tietoturva-auditointien toteuttamiseen. Tämän opinnäytetyön tarkoituksena on tutkia Arkimen potentiaalia ja käyttöä tietoturva-auditoinneissa. Tässä opinnäytetyössä tutkitaan kuinka Arkimen avulla voidaan tuottaa parempaa verkkoliikennekuvaa sekä sitä, kuinka kyseisen työkalun avulla voidaan havaita mahdollisia haavoittuvuuksia sekä uhkia. Edellä mainittujen keinojen avulla esimerkiksi organisaatiot pystyvät reagoimaan erilaisiin tietoturvariskeihin nopeammin ja tehokkaammin.

Seuraavissa luvuissa käsitellään tarkemmin Arkimen kyvykkyyksiä, sen käyttöä tietoturva-auditoinneissa, käytännön toteutusta, sekä mahdollisia haasteita. Tämän tutkimuksen tavoitteena on antaa lukijalle selkeä ymmärrys siitä, kuinka Arkime voi edistää tietoturva-auditointien tehokkuutta ja auttaa organisaatioita suojaamaan arvokkaita tietojaan digitaalisessa ympäristössä.

2 Tutkimus

2.1 Tutkimuskysymykset

Tämän tutkimuksen tavoitteena on tarkastella Arkimen käyttöä tietoturva-auditoinneissa ja sen hyödyllisyyttä tietojärjestelmien verkkoliikenteen turvallisuuden tarkastelussa. Seuraavat tutkimuskysymykset ohjaavat tutkimusta:

1. **Kuinka hyvin Arkime soveltuu tietoturva-auditointien suorittamiseen?**

Tämä kysymys keskittyy arvioimaan, miten Arkimen ominaisuudet ja kyvykkyydet vastaavat tietoturva-auditointien tarpeisiin. Tämän tutkimuskysymyksen avulla pyritään myös selvittämään, kuinka tehokkaasti Arkime soveltuu käytettäväksi osana tietoturva auditointeja.

2. **Millaisia etuja ja haasteita liittyy Arkimen käyttöön tietoturva-auditoinneissa?**

Tässä kysymyksessä tarkastellaan Arkimen käyttöön liittyviä etuja ja haasteita. Tarkoituksena on selvittää, kuinka hyvin Arkime pystyy vastaamaan nykyisiin tietoturva-auditointien haasteisiin, kuten suuren datamäärän analysointiin ja uusien uhkien havaitsemiseen.

Edellä mainitut tutkimuskysymykset ohjaavat tämän opinnäytetyön etenemistä ja ne toimivat perustana tutkimuksen edistymiselle ja sen tulosten analysoinnille. Tavoitteena on saada selkeä käsitys Arkimen roolista ja vaikutuksesta tietoturva-auditointeihin sekä tarjota arvokasta tietoa toimijoille, jotka harkitsevat työkalun käyttöönottoa työtehtävissään.

2.2 Tutkimusmenetelmä

Työn tutkivasta ja kehittävästä luonteesta johtuen, tämän tutkimuksen tutkimusmenetelmäksi valikoitui tutkimuksellinen kehittämistyö. Toikon ja Rantalan (2009) mukaan tutkimuksellisessa työelämän kehittämistoiminnassa käytetään tutkimustietoa työelämän kehittämistarpeisiin tavoitteena tuottaa uutta tietoa, jota on mahdollista soveltaa käytännössä. Tutkimuksellinen kehittämistoiminta sijoittuu työelämän kehittämisen ja tutkimuksen välimaastoon, yhdistäen konkreettisen kehittämisen ja tutkimuksellisen lähestymistavan. Kehittävässä tutkimuksessa

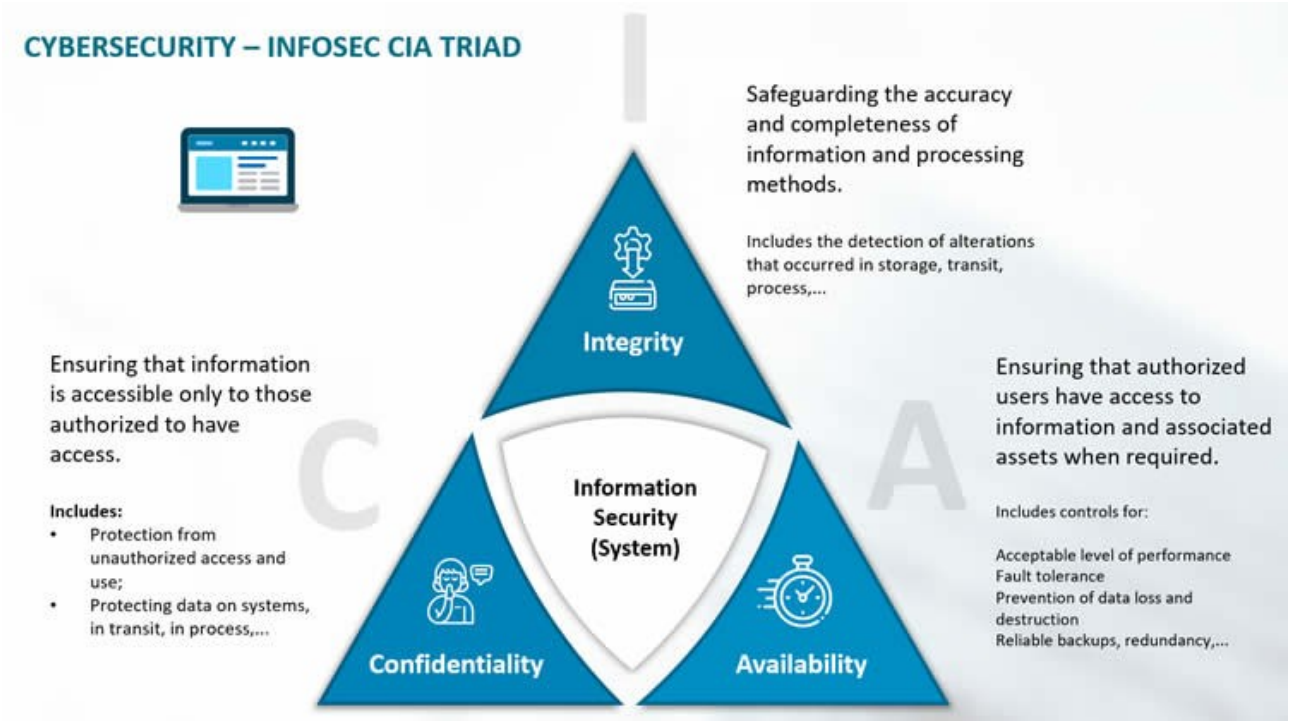
määritellään alkuun tutkimuskysymyksiä ja -menetelmiä, jonka jälkeen edetään kohti käytännön kehittämistoimintaa. Tutkimuksellisessa kehittämistoiminnassa lähtökohtana ovat käytännön ongelmat, jotka ohjaavat tiedon tuottamista käytännön toimintaympäristöissä. Tavoitteena ei ole pelkästään ratkaista yksittäistä ongelmaa, vaan myös tuottaa tietoa laajempaan keskusteluun. Esimerkkejä tutkimuksellisen kehitystoiminnan suuntauksista ovat esimerkiksi toimintatutkimus, kehittävä työntutkimus, käytäntötutkimus ja työelämän tutkimusavusteinen kehittäminen. (Toikko & Rantala, 2009.)

2.3 Kirjallisuuskatsaus

2.3.1 Tietoturva

Tietoturva on käytäntö, joka suojaa verkkoja, laitteita ja tietoja luvattomalta käytöltä tai haitalliselta toiminnalta. Tietoturvan päätavoitteena on varmistaa tiedon luottamuksellisuus, eheys ja saatavuus. Nykypäivän digitaalisessa maailmassa ollaan voimakkaasti riippuvaisia tietokoneista ja internetistä osana arkipäivän monia toimintoja. Tietotekniikkaa käytetään muun muassa kommunikointiin, viihteeseen, liikkumiseen, ostotapahtumiin, terveydenhuoltoon ja moniin muihin asioihin. Tästä johtuen tietokoneet ja Internet ovat merkittävä osa arkipäivää. Monilla ihmisillä on henkilökohtaisia tietoja tallennettuna omiin laitteisiinsa, kuten tietokoneisiin, älypuhelimiin ja tabletteihin, sekä ulkoisille palvelimille, jotka ovat kolmansien osapuolten hallinnoimia. Tämä verkottuneisuus korostaa tietoturvan äärimmäisen tärkeää roolia digitaalisten varojemme ja yksityisyytemme suojelemisessa. (What is cybersecurity, 2021.)

Yksi tietoturvan keskeisimmistä periaatteista on CIA-kolmio (ks. kuvio 1), joka muodostuu kolmesta eri ulottuvuudesta: luottamuksellisuus (eng. confidentiality), eheys (eng. integrity) ja saatavuus (eng. availability).



Kuvio 1. CIA-kolmio. (The CIA triad of confidentiality, integrity and availability, N.d)

Luottamuksellisuus on kriittinen osa tietoturvaa, sillä se keskittyy yksityisyyden ylläpitämiseen tietojen ja informaation suhteen. Siihen sisältyy tarkka kontrolli siitä, kuka voi käyttää tiettyjä tietoja, tiedostoja ja kohteita, kuten käyttäjänimiä, salasanayhdistelmiä ja lääketieteellisiä tietoja. Luottamuksellisuuden ensisijainen huolenaihe on varmistaa, että vain valtuutetut henkilöt, laitteet tai prosessit voivat nähdä nämä tiedot tai informaation. Luottamuksellisuus on tärkeää siksi, että siitä voi aiheutua erilaisia ongelmia, jos valtuuttamattomat osapuolet saavat pääsyn arkaluontoisiin tietoihin tai informaatioon. (Nweke, 2017.)

Tietoturvan näkökulmasta datan eheyden ylläpitäminen on tärkeää, sillä se varmistaa, että data säilyy alkuperäisessä muodossaan sitä siirrettäessä, käsiteltäessä ja tallennettaessa. Tämä on tärkeää, jotta estetään tahattomat tai haitalliset muutokset. Esimerkiksi pienikin muutos viestissä, saattaa aiheuttaa merkittävän muutoksen koko viestiin ja tehdä siitä mahdollisesti korruptoituneen tai lukukelvottoman. (Nweke, 2017.)

Saatavuus varmistaa sen, että käyttäjillä, joilla on oikeudet käsitellä määrättyä tietoa, on mahdollisuus suorittaa tehtävänsä, vaikka kaikki kyberturvallisuuden suojatoimet ovat käytössä laitteistojen, ohjelmistojen, ihmisten, prosessien ja muiden käsittelyssä. Tämä edellyttää, että

hyväksytyillä käyttäjillä on oltava vaivaton pääsy resursseihin, joita he tarvitsevat tehtäviensä suorittamiseen, samalla kun taataan järjestelmän turvallisuus sekä sujuva toiminta. (Nweke, 2017.)

2.3.2 Tietoturva-auditointi

Auditointi on perusteellinen arviointi organisaation tietojärjestelmistä. Tämä arviointi yleensä tarkastelee tietojärjestelmän turvallisuutta vertaamalla sitä alan parhaisiin käytäntöihin, ulkoisiin standardeihin tai valtion määräyksiin perustuvaan kriteeristöön. Tunnetuimpia globaaleja tietoturva kriteeristöjä ovat muun muassa NIST (National Institute of Standards and Technology), ISO 27000 (International Organization for Standardization) ja Suomessa ulkoministeriön julkaisema KATAKRI (kansallinen turvallisuusauditointikriteeristö). Kattava turvallisuustarkastus arvioi organisaation tietoturvakäytäntöjä seuraavilla alueilla:

1. Tietojärjestelmien fyysiset aspektit ja ympäristö, jossa tietojärjestelmä sijaitsee.
2. Organisaation käyttämät sovellukset ja ohjelmistot, mukaan lukien päivitysten hallinta.
3. Tietoverkkojen turvallisuus, sisältäen verkkojen konfiguraatiot ja pääsynhallinnan sekä valvonnan.
4. Ihmisten toimintamallit, mukaan lukien työntekijöiden tapa käsitellä, jakaa ja säilyttää tietoa.
5. Organisaation yleinen turvallisuusstrategia, mukaan lukien turvallisuuspolitiikat, organisaatiokaaviot ja riskiarvioinnit.

(Vicente, 2023.)

Tämä opinnäytetyö keskittyy organisaation tietoverkkojen arviointiin, joka on osa auditoinnin teknistä osaa. Seuraavana on eritelty Traficomin arviointilaitoksille suunnatussa tietoturvallisuuden ohjeessa (Ohje tietoturvallisuuden arviointilaitoksille, 2022) laatimat vähimmäisvaatimukset teknisen tietoturvan tarkastelun osalta.

- Passiivinen rajapinta-analyysi
- Järjestelmä-konfiguraatioiden turvallisuuden tarkastelu
- Aktiivinen rajapinta-analyysi
- Sovellusturvallisuuden tarkastelut järjestelmätyypeittäin
- Salausratkaisujen turvallisuuden todentaminen

- Käytettävyystestaukset (ml. kuormitustestaukset)
- Fyysisen turvallisuuden suojausten todentamismenetelmät
- Yhdyskäytävä ratkaisujen turvallisuuden testaukset
- Poikkeamahavainnointikyvyn testaukset
- Hajasäteilysuojausten todentaminen
- Luvattomien teknisten laitteiden olemassaolon todentaminen

2.3.3 Verkkoliikenteen analysointi

Verkkoanalyysi on prosessi, jossa kerätään verkkotietoja ja tutkitaan niitä huolellisesti, jotta pystytään muodostamaan mahdollisimman selkeä kuva siitä, mitä verkossa tapahtuu. Verkkoanalysaattori purkaa eli analysoi protokollien datapaketit ja esittää verkkoliikenteen ihmisen luettavassa muodossa. Muita verkkoanalyysin nimityksiä ovat muun muassa salakuuntelu, nuuskiminen, liikenneanalyysi, protokolla-analyysi ja pakettianalyysi. (Syngress, 2004.)

Pakettianalyysin avulla järjestelmien ylläpitäjät voivat suorittaa seuraavia asioita:

- Binäärimuotoisten tietopakettien muuntaminen ihmisen luettavaan muotoon.
    - Pakettianalysaattori ohjelman avulla voidaan muuttaa binäärimuotoiset tiedot, kuten verkkoliikenne, paketit selkokielelle. Tämä helpottaa niiden tarkastelua ja analysointia.
- Verkon ongelmien ratkaiseminen
    - Kerätyn datan avulla voidaan suorittaa vianmääritystä verkkoliikenteelle ja täten ylläpitää verkon toimintaa
- Verkon suorituskyvyn tutkiminen pullonkaulojen tunnistamiseksi
    - Voidaan tunnistaa heikkoja kohtia tietoverkossa ja tarkastella, miksi ne eivät toimi halutulla tavalla
- Verkkoon tunkeutumisen havaitseminen
    - Verkkoliikenteestä on mahdollista tunnistaa, jos ympäristössä on ei-haluttuja toimijoita. Kerättyä tietoa voidaan myös analysoida tunkeutumisyritysten tunnistamiseksi.
- Verkkoliikenteen kaappaaminen rikosteknistä analyysia ja todisteiden esittämistä varten.
    - Nauhoitettua tietoliikennettä voidaan käyttää todisteena rikosoikeudellisissa asioissa, sillä tallennettua tietoliikennettä voidaan käyttää osoittamaan, mitä rikolliset ovat tehneet verkossa.
- Ohjelmien toiminnan tutkiminen

    - Verkkoliikenteestä voidaan tunnistaa ohjelmien toimintaan liittyviä konfiguraatiovirheitä sekä mahdollisia ohjelmien toimintaa haittaavia epäkohtia
- Palvelunestohyökkäyksen (DoS) alkuperän jäljittäminen.
    - Kerättyä pakettidataa voidaan käyttää hyödyksi tunnistettaessa palvelunestohyökkäyksen lähdettä sekä torjuttaessa hyökkäystä.
- Vakoiluohjelmien löytäminen
    - Verkkoliikenteen nauhoituksen avulla voidaan etsiä verkossa liikennöiviä haitallisia ohjelmia.

(Syngress, 2004.)

Verkkoanalyysia toteutettaessa on olemassa kaksi eri tyyliä: reitittimettömiin ja reitittimiin perustuvat analyysit. Reitittimiin perustuvat lähestymistavat ovat sellaisia, joissa seurataan suoraan reitittimiin integroituja ominaisuuksia ilman, että on tarpeen asentaa ylimääräisiä laitteistoja tai ohjelmistoja. Muut kuin reitittimeen perustuvat menetelmät tarjoavat enemmän konfiguraatio-ominaisuuksia, mutta edellyttävät lisälaitteistojen ja -ohjelmistojen asentamista. (Efficient Packet Monitoring for Network Management, 2002.)

Pakettianalyysin suorittamiseen on tarjolla erilaisia pakettikaappaamisohjelmia, jotka voivat olla sekä ilmaisia että kaupallisia. Eri ohjelmilla on eri ominaisuuksia ja kaikki ohjelmat eivät esimerkiksi ole yhteensopivia kaikkien käyttöjärjestelmien kanssa. Analyysiohjelmaa valittaessa tulee tutustua saatavilla oleviin vaihtoehtoihin ja verrata niitä omiin tarpeisiin. Muutamia suosittuja pakettianalyysiohjelmia Arkimen lisäksi ovat esimerkiksi tcpdump ja Wireshark. Mainituista ohjelmista tcpdump on komentoriviohjelma ja Wireshark on varustettu graafisella käyttöliittymällä. (Sanders, 2011.)

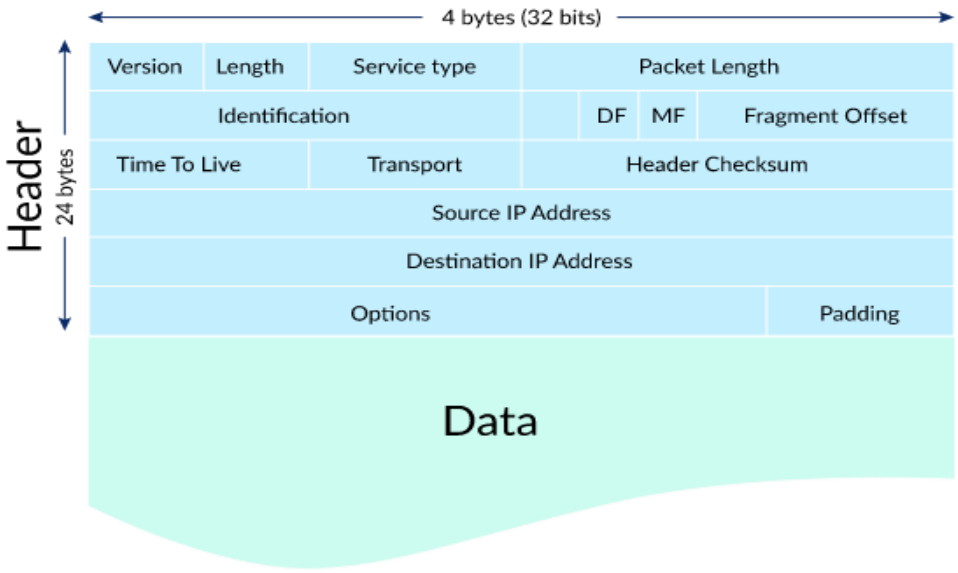
2.3.4 Aktiivinen ja passiivinen verkkoanalyysi

Aktiivinen verkkoanalyysi käyttää siihen erikoistuneita seurantatyökaluja tai -ohjelmistoja, joilla luodaan aktiivisesti testiliikennettä kohdeverkkoon. Laitteen pingaaminen tai ohjelmoitujen testien suorittaminen ovat esimerkkejä generoiduista tapahtumista, joita käytetään usein aktiivisessa seurannassa verkon suorituskyvyn arvioimiseksi ja mahdollisten ongelmien löytämiseksi. Tämä tarjoaa tietoa verkon reagointikyvystä, sovellusten suorituskyvystä ja käytettävyydestä. (Charest, 2023.)

Passiivinen verkkoanalyysi ei edellytä liikenteen lisäämistä verkkoon. Sen sijaan siinä käytetään verkon kuuntelua tai porttien peilausta tarkasteltavan järjestelmän autenttisen verkkoliikenteen keräämiseen ja analysointiin. Passiivinen valvonta tarjoaa kattavan näkymän verkon todelliseen käyttäytymiseen, mikä mahdollistaa liikennemallien, tietoturvariskien ja sovellusten suorituskyvyn syvällisen tutkimisen ajan mittaan. (Charest, 2023.)

2.3.5 Verkkopaketti

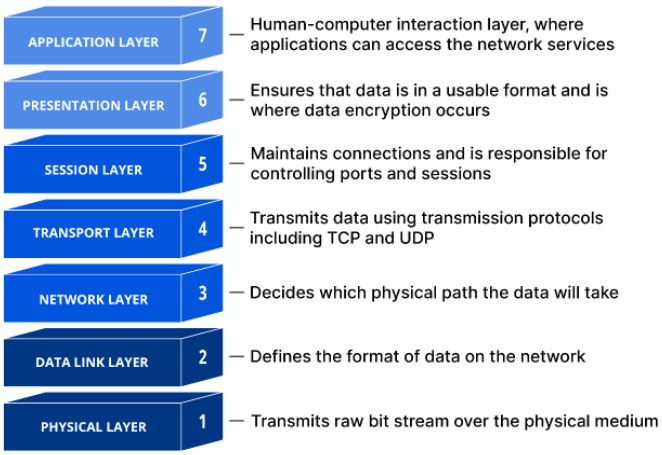
Verkkopaketti on datapaketti, jonka laite lähettää verkon kautta. Tämä paketti sisältää sekä hyötykuorman (eng. payload), että hyötykuorman toimittamiseen tarvittavia tietoja. Paketit ovat pieniä palasia suuremmasta viestistä. Kun tietoja siirretään tietoliikenneverkoissa, ne jaetaan paketeiksi, jotka vastaanottava laite kokoaa uudelleen. Suurten viestien pilkkominen pienempiin paketteihin auttaa pitämään viestintäkaistan vapaina muille laitteille, mikä edesauttaa verkon sujuvaa toimintaa. Ilman paketointia laitteet joutuisivat odottamaan muiden verkossa olevien laitteiden tiedonsiirtoa ennen kuin ne voisivat itse lähettää viestinsä vastaanottajalle. Tämä voisi osaltaan hidastaa verkon toimintaa. (What is a Network Packet? N.d). Kuviossa 2 on esitelty yksityiskohtaisemmin verkkopaketin sisältöä. IPV4 paketti koostuu otsikkotiedoista (eng. header) sekä data-osiosta.



Kuvio 2. IPv4 –paketin sisältö. (IP packets, N.d)

2.3.6 OSI-malli

OSI-malli (Open Systems Interconnection) on standardoitu malli, jota käytetään kuvaamaan tietovirran liikkumista yhdestä tietokoneesta toiseen verkkoympäristössä. OSI-malli määrittelee joukon sääntöjä ja vaatimuksia tietoliikenteelle sekä eri laitteiden, tuotteiden ja ohjelmistojen yhteensopivuudelle verkkoinfrastruktuurissa. (OSI Reference Model and Its Importance, 2022.)



Kuvio 3. OSI-mallin eri tasot. (What is the OSI Model, N.d)

Kuviossa 3 on esitelty OSI-malli, joka on jaettu seitsemään eri kerrokseen:

1. Sovelluskerros

    - Sovelluskerros on käytössä loppukäyttäjän ohjelmistoissa, kuten selaimissa ja sähköpostiohjelmissa. Se tarjoaa protokollia, jotka mahdollistavat tiedon

lähettämisen ja vastaanottamisen sekä merkityksellisen datan esittämisen käyttäjille. Tähän kerrokseen kuuluvat muun muassa HTTP, FTP, POP, SMTP ja DNS.

2. Esitystapakerros

    - Esitystapakerros valmistelee datan sovelluskerrokselle. Se huolehtii siitä, miten data koodataan, salataan ja pakataan, jotta se vastaanotetaan oikein. Esityskerros käsittelee sovelluskerrokselta tulevan datan ja valmistelee sen siirrettäväksi istuntokerrokselle.

3. Istuntokerros

    - Istuntokerros luo viestintäkanavia, eli istuntoja, laitteiden välille. Se vastaa istuntojen avaamisesta, ylläpidosta datan siirron aikana ja niiden sulkemisesta viestinnän loputtua. Lisäksi istuntokerros voi luoda tarkistuspisteitä datan siirron keskeytyessä, jotta vikatilanteissa siirto voidaan jatkaa viimeisestä tarkistuspisteestä, eikä koko tiedonsiirtoa tarvitse aloittaa alusta.

4. Kuljetuskerros

    - Kuljetuskerros ottaa datan istuntokerrokselta ja pilkkoo sen segmentteihin lähettävässä päässä. Se kokoaa segmentit uudestaan vastaanottavassa päässä, jotta istuntokerros osaa tulkita niitä. Kuljetuskerros vastaa tiedonsiirron virtauksen hallinnasta, varmistaen datan lähettämisen vastaanottavan laitteen nopeuden mukaisesti. Se myös vastaa virheiden hallinnasta tarkistamalla väärin vastaanotetut datat ja pyytämällä niitä uudelleen tarvittaessa.

5. Verkkokerros

    - Verkkokerros pilkkoo kuljetuskerroksen luomat segmentit verkkopaketeiksi ja kokoaa ne uudelleen vastaanottavalla päässä. Lisäksi se reitittää paketteja parhaan

reitin löytämiseksi fyysisessä verkossa. Verkkokerros käyttää verkko-osoitteita, kuten IP-osoitteita, ohjatakseen paketit kohteeseensa.

6. Siirtokerros

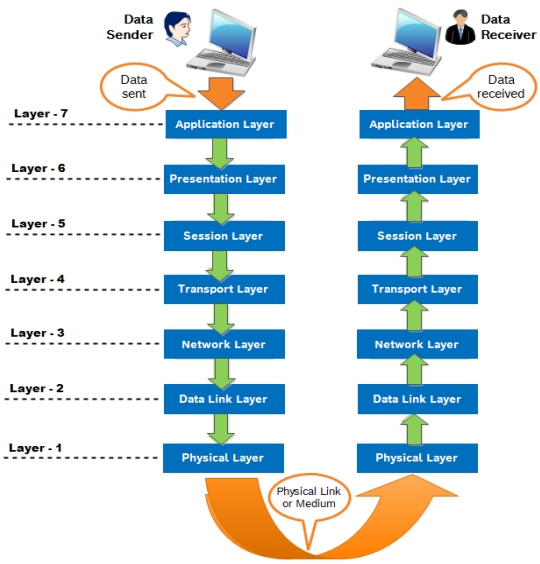
   - Siirtokerros vastaa yhteyden luomisesta ja katkaisemisesta fyysisesti yhdistettyjen verkkolaitteiden välillä. Siirtokerros tarkastaa siirretyn datan eheyden ja lähettää sen vastaanottavalle laitteelle käyttäen apunaan laitteiden MAC-osoitteita.

7. Fyysinen kerros

   - Fyysinen kerros hallinnoi fyysistä kaapelia tai langatonta yhteyttä verkkosolmujen välillä. Se määrittelee liittimet, sähkökaapelin tai langattoman tekniikan laitteiden välillä, ja huolehtii raakadatan eli bittien siirrosta verkossa.

(What is OSI Model, N.d.)

Kuvio 4 kuvastaa kuinka lähetetty data kulkee OSI-mallin mukaisesti lähettäjän ja vastaanottajan välillä.



Kuvio 4. Havainnollistava kuva OSI-mallin toiminnasta. (OSI Layers – Microsoft has oftenly referred this term in Azure security topics. What is it all about?, 2021)

3 Johdatus Arkimeen

Arkime on avoimen lähdekoodin verkkoliikenteen analyysiohjelma, joka tunnettiin alun perin nimellä Moloch. Sitä käytetään verkkopakettien tallentamiseen, indeksointiin ja hakuun. Se on suunniteltu auttamaan tietojärjestelmien verkkoliikenteen tarkastelussa ja sitä voidaan käyttää apuna verkkoturvallisuuden valvonnassa, vianmäärityksessä sekä suorituskyvyn analysoinnissa. Arkime on saatavilla Linux -pohjaisille järjestelmille ja se tukee suosituimpia Linux-jakeluita kuten esimerkiksi, Ubuntu, Debian, CentOS, Red Hat Enterprise Linux (RHEL), Fedora, openSUSE sekä Arch Linux. Windows käyttöjärjestelmille ei ole vielä julkaistu toimivaa versiota. Arkimen on alun perin kehittänyt yhdysvaltalainen AOL omiin tarpeisiinsa, mutta se on sittemmin julkaistu avoimena lähdekoodina kaikkien saataville. (Arkime, Github.)

Pakettien kaappaus, tallennus ja tarkastelu

Arkime on suunniteltu keräämään ja tallentamaan verkkopaketteja tehokkaasti. Se pystyy keräämään paketteja monista verkkoliitännöistä samanaikaisesti ja tallentamaan ne tietokantaan, jotta niitä voidaan analysoida myöhemmin. Arkime soveltuu erinomaisesti tietojärjestelmiin, joissa liikennöi suuria määriä dataa, koska se on mahdollista hajauttaa käytettäväksi useissa tietojärjestelmän laitteessa, sekä sen voi skaalata käsittelemään kymmeniä gigabittejä sekunnissa tapahtuvaa liikennettä.

Arkime tarjoaa verkkopohjaisen käyttöliittymän, joka tarjoaa selkeän näkymän kerättyyn dataan. Käyttöliittymä sisältää vaihtoehtoja verkkotietojen etsimiseen, suodattamiseen ja visualisointiin, mikä helpottaa tietoturvaongelmien tunnistamista ja tutkimista. (Arkime, Github.)

Indeksointi ja haku

Yksi Arkimen merkittävimmistä ominaisuuksista on sen kyky indeksoida ja etsiä tehokkaasti kerättyjä tietoja käyttäen Elastisearchia. Elasticsearch indeksoi lukuisia verkkopakettien ominaisuuksia, kuten IP-osoitteita, portteja ja protokollia, minkä ansiosta kerätystä tiedosta on

helppo etsiä haluttuja verkkotapahtumia. Tämä on hyödyllistä, kun on kyse tietoturvaloukkausten nopeasta tunnistamisesta ja niihin reagoimisesta. (Arkime, Github.)

Protokollatuki, verkkopakettien tarkastelu ja istuntojen uudelleen rakentaminen

Arkime tukee käytetyimpien protokollien (HTTP, HTTPS, DNS ja SMTP) lisäksi myös harvinaisempia protokollia. Tämän ominaisuuden ansiosta se voi kaapata ja analysoida monenlaista verkkoliikennettä.

Arkimen avulla voidaan purkaa pakettidataa, mikä tarkoittaa, että sen avulla voidaan kerätä tietoa kaapatuista paketeista, kuten sähköpostien, verkkosivujen tai verkon kautta siirrettyjen tiedostojen sisällöstä. Tämä pakettien purkaminen on hyödyllinen tapa, kun halutaan ymmärtää paremmin verkkoviestinnän dataa. Tämä edellyttää kuitenkin sitä, ettei kyseinen liikenne ole salattua.

Verkkoviestintä edellyttää usein lukuisten pakettien lähettämistä kahden päätepisteen välillä. Arkime pystyy kokoamaan nämä paketit uudelleen kokonaisiksi istunnoiksi, jolloin kahden laitteen välistä liikennöintiä on helpompi seurata. (Arkime, Github.)

Integrointi muihin tietoturvaohjelmistoihin

Koska Arkime käyttää Elasticsearchia, se voidaan integroida erilaisiin ELK Stackin tietoturva - ja analyysiohjelmistoihin, esimerkiksi viusalisointityökalu Kibanaan tai Suricata IDS -ohjelmistoon. Yhdistämällä Arkimen ominaisuuksia muihin työkaluihin ja teknologioihin käyttäjät voivat luoda kattavia verkkovalvontaratkaisuja. (Topasna, 2020). Arkimen keräämät PCAP-istunnot ovat avattavissa muissakin kyseistä tiedostoformaattia tukevissa ohjelmissa kuten esimerkiksi Wiresharkissa. Tästä on hyötyä, jos halutaan tarkastella yhden paketin sisältöä tarkemmin. (Arkime, Github.)

Avoin lähdekoodi

Koska Arkime on avoimen lähdekoodin järjestelmä, se on kustannustehokas ratkaisu toimijoille, jotka haluavat laajamittaisia pakettikaappausominaisuuksia ilman kaupallisiin vaihtoehtoihin liittyviä kalliita lisenssikustannuksia. Avoimen lähdekoodin myötä, Arkimella on aktiivinen

kehittäjä- ja käyttäjäyhteisö, jonka takia sille julkaistaan päivityksiä ja parannuksia usein (Arkime, Github.)

Edellä mainitut ominaisuudet tekevät siitä erinomaisen työkalun verkonvalvontaan, uhkien havaitsemiseen ja tietoturvaloukkausten tutkimiseen kaikenkokoisissa tietojärjestelmissä. Auditoinneissa se on tehokas työkalu selkeän käyttöliittymän ja tarkan indeksoinnin johdosta. Suuresta datamäärästä on nopea etsiä auditoijaa kiinnostavat asiat ja suodattaa muu ei-relevantti liikenne pois. (Arkime, Github.)

3.1 Ohjelmistokomponentit

Arkime koostuu kolmesta eri komponentista:

Akime Viewer

- Akime Viewer -komponentin avulla hallitaan Arkime web-käyttöliittymää ja siirretään PCAP-tiedostoja. Sen avulla käyttäjän on mahdollista tarkastella ja käsitellä kerättyä pakettidataa. Arkime Viewer on node.js -pohjainen ohjelmisto.

Arkime Capture

- Arkime Capture on komponentti, joka vastaa verkkoliikenteen keräämisestä ja tallentamisesta. Se kerää paketteja verkkoliitänteistä tai jo olemassa olevista PCAP -tiedostoista ja tallentaa ne tietokantaan myöhempää analysointia varten.

Elasticsearch

- Elasticsearch on avoimen lähdekoodin haku- ja analytiikkaohjelmisto, jota käytetään Arkimessa taustatietokantana. Se on olennainen komponentti verkkoliikennedatan tallentamisessa ja noutamisessa. Elasticsearchia käytetään indeksoimaan ja tallentamaan metadataa ja muuta tietoa kerätystä verkkoliikenteestä sekä se tarjoaa tehokkaan haku- ja kyselytoiminnon, jonka avulla käyttäjät voivat nopeasti noutaa haluttua tietoa tallennetusta verkkoliikennedatasta. (Andhavarapu, 2017.)

3.2 Järjestelmävaatimukset ja asennus

Arkimen minimivaatimukset ovat suoraan verrannollisia tarkasteltavan järjestelmän suuruuteen ja siellä liikkuvan verkkoliikenteen määrään. Arkime tarjoaa käyttäjille https://arkime.com/estimators -sivulla laskurin, jonka mukaan käyttäjä voi suunnitella omat resurssinsa Arkimen ajamista varten. Jos Arkimea käytetään vain pienten ympäristöjen verkkoliikenteen tarkasteluun lyhyen ajanjakson välillä, sitä voidaan ajaa vain yhdellä Linux -pohjaisella laitteella. Seuraava asennusohje on tarkoitettu edellä mainittuun tarkoitukseen.

Arkimen perusasennuksen vaiheet:

1. Ladataan omaa käyttöjärjestelmää vastaava versio Arkimesta osoitteesta http://arkime.com/index.html#downloads ja asennetaan ladattu paketti käyttämällä esimerkiksi apt- paketinhallinta työkalua
2. Määritellään Arkimen perusasetukset ajamalla Configure-skripti hakemistosta /opt/arkime/bin/Configure. Seurataan Configure -skriptin ohjeita ja asennetaan käyttäjän preferenssin mukaan joko Elasticsearch tai OpenSearch. Tässä työssä tietokannaksi valitaan Elasticsearch. Valitaan myös mitä verkkorajapintoja Arkimen halutaan nauhoittavan.
3. Alustetaan Elasticsearchin konfiguraatio ajamalla komento “/opt/arkime/db/db.pl http://localhost:9200 init.
4. Lisätään uusi ylläpito käyttäjä komennolla /opt/arkime/bin/arkime_add_user.sh admin "Admin User" [SALASANA]--admin”
5. Käynnistetään Arkimen käyttämät prosessit ajamalla komento “systemctl start arkimecapture.service arkimeviewer.service”
6. Jos prosessit eivät käynnisty oikein, vikaa voidaan tutkia tarkastelemalla arkime.viewer tai arkime.capture -lokeja hakemistosta /opt/arkime/logs/
7. Kun kaikki Arkimen vaatimat prosessit on saatu onnistuneesti toimimaan, voidaan asennuksen toimivuus tarkastaa vierailemalla jollakin verkkoselaimella Arkime Viewer -osoitteessa http://localhost:8005, johon syötetään kohdassa 4 annetut käyttäjätunnukset. Tämän jälkeen Arkime Viewer -näkymä pitäisi avautua käyttäjälle.

(Instructions for using the prebuilt Arkime packages. N.d.)

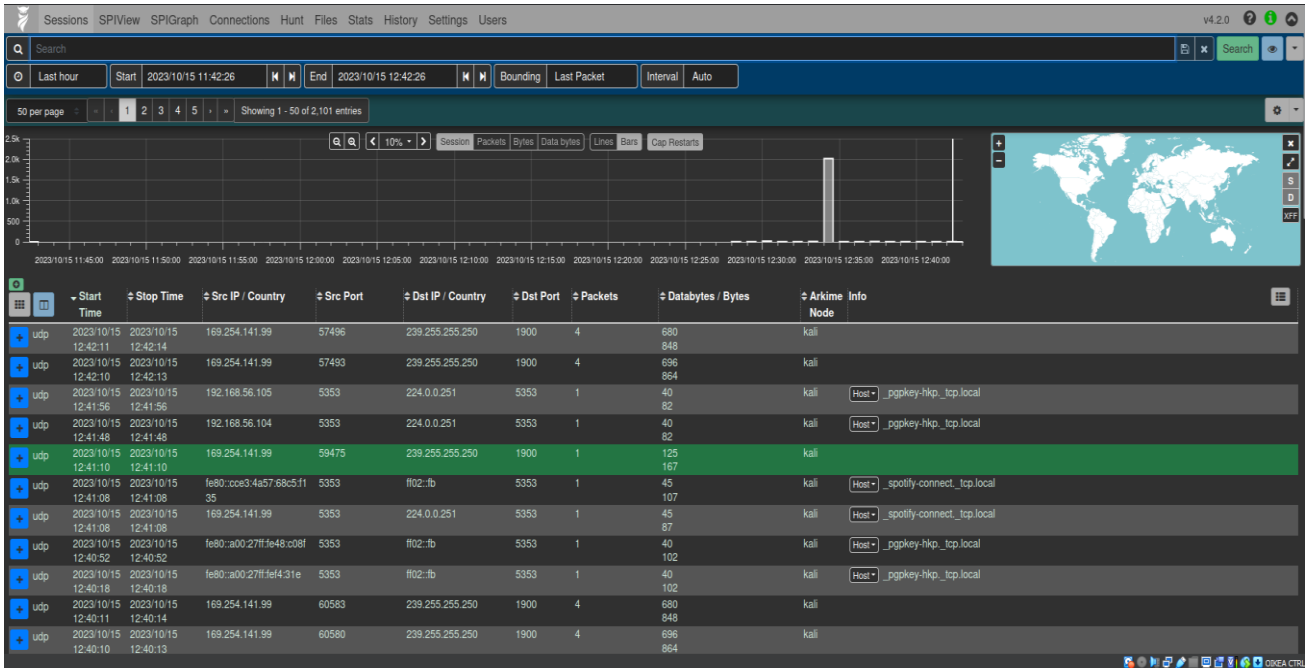
3.3 Arkimen ominaisuudet ja kyvykkyydet

Sessions

Istunnot-sivu on keskeinen välilehti verkkoistuntojen seurannassa ja tarkastelussa (ks. kuvio 5). Se antaa yhteenvedon tallennetuista verkkoliikenneistunnoista halutulla aikavälillä ja sen avulla voidaan tutkia istuntojen yksityiskohtia, lähde- ja kohdetietoja, käytettyjä protokollia ja tiedonsiirtotilastoja. Käyttäjä voi itse valita mitä tietoja kerätystä datasta halutaan esille konfiguroimalla näkyvissä olevia sarakkeita sivun vasemmasta laidasta löytyvästä ruudukko -painikkeesta. (Arkime, N.d.)

Sivun ylälaidassa sijaitsevan hakukentän avulla voidaan kohdistaa kerättyyn dataan käyttäjän haluamia kyselyitä. Sen avulla voidaan hakea tiedoista esimerkiksi vain halutun ip -osoitteen liikennöintiä tai vain tiettyyn porttiin kohdistuvaa liikennettä. Tietyn tiedon etsimiseen nauhoitetusta verkkoliikenteestä voidaan käyttää apuna myös sivulta löytyviä “Timeline search” ja “Country search” -valikkoja. “Timeline search” on hakukentän alla oleva pylväsdiagrammi, josta voidaan määrittää haluttu tarkasteluajankohta raahaamalla diagrammista hiirellä tietyn aikavälin kokoinen alue. “Country search” on sivulla näkyvä maailman kartta, josta voidaan klikata haluamaa maata, jolloin se asetetaan automaattisesti yhdeksi hakukriteeriksi. (Arkime Help. N.d.)

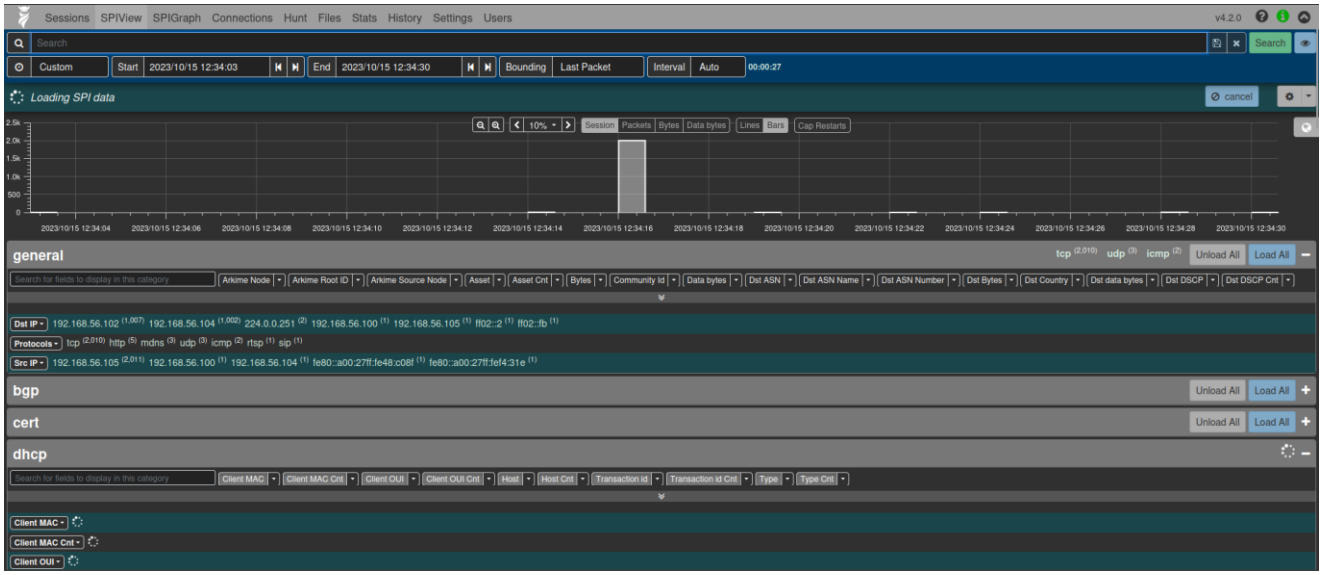
Muita hyödyllisiä ominaisuuksia Sessions -sivulla ovat “Export PCAP” sekä “Session detail” -painikkeet, joka on merkitty plus -merkillä jokaisen data rivin vasemmassa reunassa. Se antaa lisätietoa kyseisestä istunnosta sekä mahdollistaa kerätyn pakettidatan tarkastelun. “Export PCAP” valinnan avulla voidaan esillä oleva data ladata PCAP-formaatissa käyttäjän paikalliselle laitteelle. “Export PCAP” löytyy sivun oikeassa yläkulmassa olevan alasvetovalikon takaa. PCAP-dataa voidaan tämän jälkeen tarkastella myös jollain muulla pakettianalysaattorilla, kuten esimerkiksi Wiresharkilla. (Arkime Help. N.d.)



Kuvio 5. Näkymä Arkimeviewerin Sessions -välilehdeltä.

SPIView

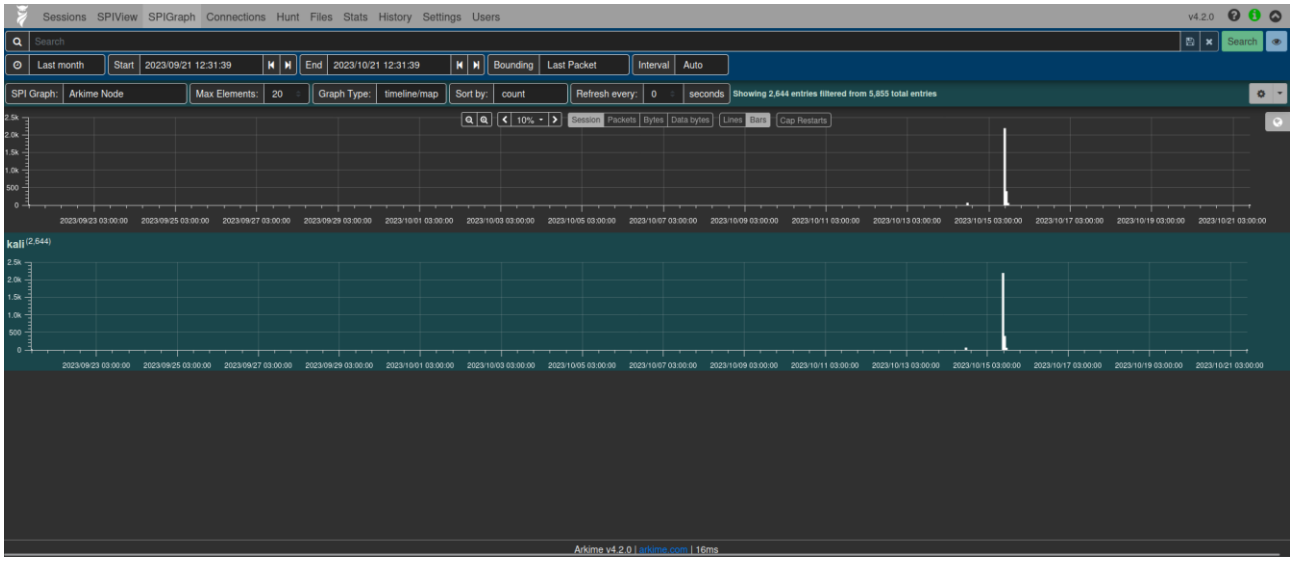
Arkimen "SPIView"-välilehti on lyhenne sanoista "Stream Progression Index View". Sitä voidaan käyttää verkon datapakettien seuraamiseen kaapattujen verkkoistuntojen sisällä sekä niiden tarkasteluun ja analysointiin. Se tarjoaa graafisen kuvauksen datapakettien lähetyksen ja vastaanoton ajoituksesta verkkoyhteyden aikana (ks. kuvio 6). SPIView on hyödyllinen, kun halutaan tarkastella syvemmin tiettyjä istuntoja. Tällöin tarkastelija voi nopeasti valita halutut arvot hakuehdoiksi yksinkertaisesti klikkaamalla niitä. Näkymästä on helppo ottaa tarkastelun kohteeksi esimerkiksi vain tiettyä protokollaa käyttävät istunnot tai vain tiettyjen IP-osoitteiden välillä kulkeva liikenne. (Arkime Help. N.d.)



Kuvio 6. SPIView-sivun näkymä Arkimen verkkosivulla.

SPIGraph

Käyttäjä voi visualisoida minkä tahansa SPIView -sivulla olevan kohteen kuvion 7 mukaan pylväsdiagrammien avulla SPI Graph -sivulla. Sen avulla voidaan esittää esimerkiksi kaikki HTTP-porttiin 80 otetut yhteydet järjestelmässä ja sijoittaa ne aikajanalle. Tällöin analyytikon on nopeaa tarkastaa mihin aikoihin tiettyjä kaapattujen pakettien ominaisuuksia on ilmentynyt tarkasteltavassa verkkoympäristössä. Muita hyödyllisiä tarkastelun kohteita ovat esimerkiksi havaittujen pakettien käyttämät protokollat tai tiettyyn IP-osoitteeseen suunnatut liikennöinnit. (Arkime Help. N.d.)



Kuvio 7. SPIGraph –sivulla näkyvät nauhoitetut yhteydet.

Connections

Connections -sivulla kaapattua liikennettä voidaan tarkastella puukaavion muodossa (ks. kuvio 8). Puukaaviota voidaan käyttää eri laitteiden yhteyksien visuaaliseen määrittämiseen. Connections -sivu luo yksityiskohtaisen näkymän lähde- ja kohde-IP-osoitteiden välille muodostuneista yhteyksistä sekä niihin liittyvistä metatiedoista. Sivulla näkyviä solmukohtia voidaan liikutella kaaviossa vapaasti sekä solmujen välillä näkyvien linkkien relaatiota kaapatun istunnon tietoihin voidaan muokata. Tämä mahdollistaa liikenteen tarkastelijan oman mielen mukaisen kuvaajan luomisen. Klikkaamalla näkyvissä olevaa solmukohtaa saadaan lisätietoa näkyville. Se mitä lisätietoja valitusta solmusta näytetään, on myös käyttäjän muokattavissa kaavion ylälaidassa sijaitsevan O-valinnan takaa. (Arkime Help. N.d.)

Kun kuvaaja on muokattu käyttäjän mieleiseksi, se voidaan tallentaa “Download Graph” -valinnalla, jolloin se voidaan tallentaa lokaalisti PNG-tiedostomuodossa. Kyseiset kuvaajat ovat erittäin käytännöllisiä, kun halutaan tutkia kaapattua liikennettä visuaalisesti. (Arkime Help. N.d.)

Kuvio 8. Nauhoitetusta verkkoliikenteestä laadittu puukaavio.

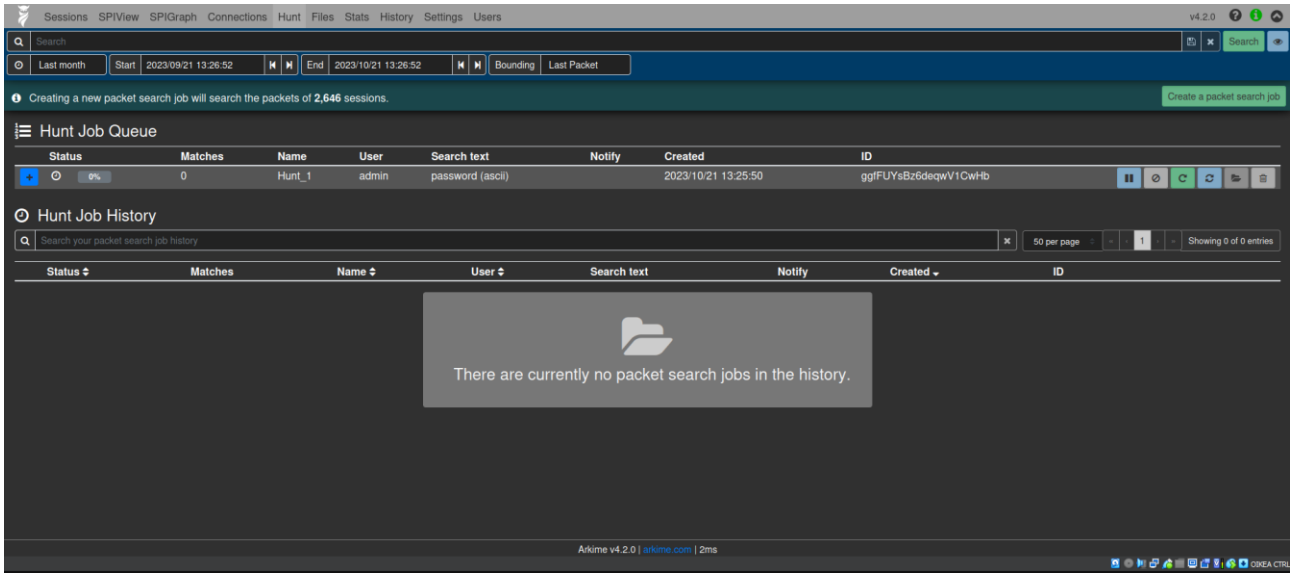
Hunt

Hunt -välilehdellä voidaan etsiä tekstiä kaapatuista istuinnoista. Ennen haun aloittamista käyttäjän tulee tarkentaa tarkasteltavaa aikaväliä Sessions -välilehdellä, sillä etsintä suoritetaan vain valittuihin istuntoihin.

Hunt -välilehdellä voidaan luoda uusi istunto, johon käyttäjä voi määritellä seuraavat asiat oman tarpeensa mukaan:

- Huntin nimi
- istuntoa kohti tutkittavien pakettien enimmäismäärä
- hakumerkkijono ja sen muoto (ascii, hex, regex tai hex regex).
- haetaanko lähdepaketteja, kohdepaketteja vai molempia.
- haetaanko raakapaketteja vai uudelleen koottuja paketteja.

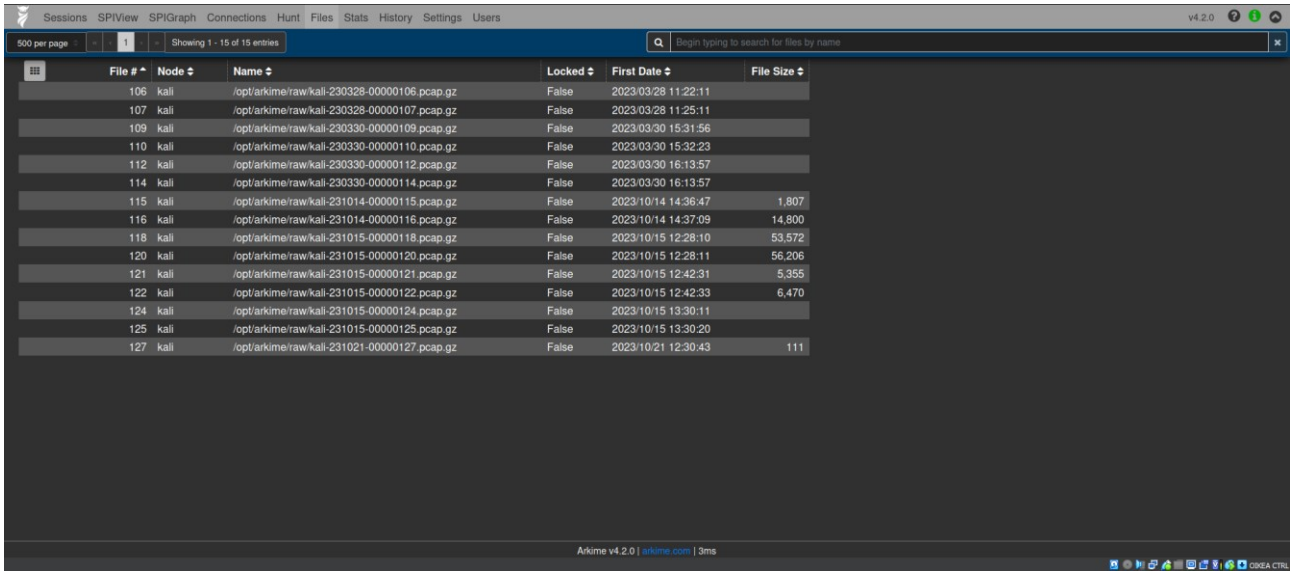
Hunt -työkalu on hyödyllinen ominaisuus esimerkiksi selkokielisten salasanojen tai käyttäjätunnuksien löytämiseen verkkoliikenteestä. Alla oleva kuvio havainnollistaa kuinka luodut “Huntit” näkyvät käyttäjälle Hunt -välilehdellä. (Arkime Help. N.d.)



Kuvio 9. Hunt-välilehden aloitusnäkymä.

Files

Files -välilehdeltä löytyvät Arkime Capturen tallentamat PCAP-tiedostot. Näkymä kertoo jokaisesta tiedostosta perustietoja muun muassa tiedoston koon sekä milloin se on tallennettu ensimmäisen kerran (ks. kuvio 10). (Arkime Help. N.d.)



Kuvio 10. Tallennetut raakapakettitiedostot Arkimen Files -välilehdellä

Stats

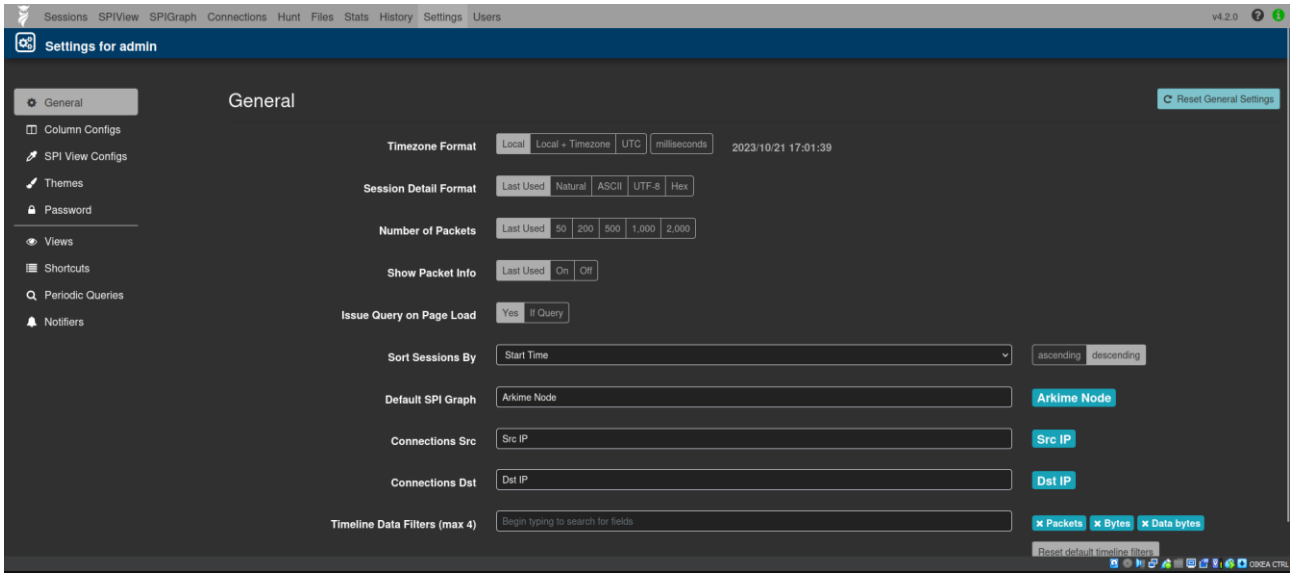
Stats -välilehdellä on tietoa Elasticsearchin sekä Arkime Capturen kaappauskomponenttien toiminnasta. Tämä näkymä on hyödyllinen, kun toimitaan laajassa ympäristössä ja halutaan tarkastella Arkimen eri komponenttien toimintaa tai mahdollisesti jäljittää vikoja Arkimen toiminnassa. Stats -välilehti antaa kattavan näkymän Arkime järjestelmän suorituskykyyn. (Arkime Help. N.d.)

History

Arkimen History-välilehti toimii lokina eri käyttäjien toimista järjestelmässä. Se kirjaa käyttäjien istuntohistoriat, hakukyselyt ja muut Arkime -järjestelmän käytöt. Normaalikäyttäjät näkevät siellä vain omat toimintansa, mutta ylläpitäjät voivat käyttää History -välilehteä toiminnan seurannassa ja valvonnassa. Se edesauttaa järjestelmän oikeudenmukaista käyttöä sekä jäljitettävyyttä vikatilanteissa. (Arkime Help. N.d.)

Settings

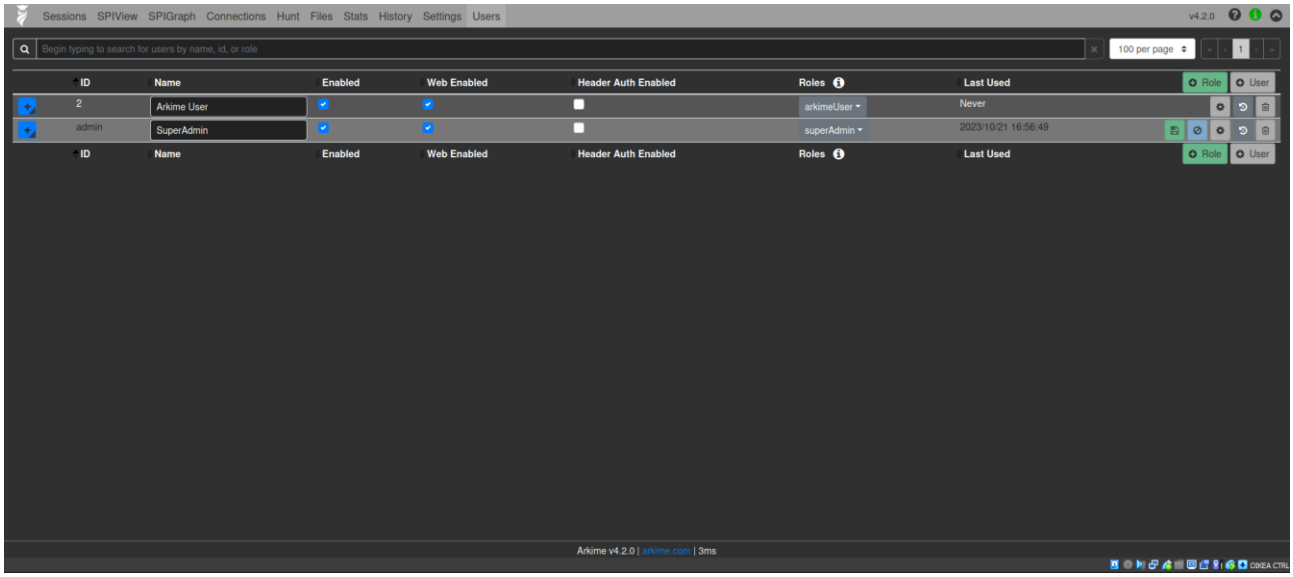
Arkimen Settings -välilehti tarjoaa keskitetyn paikan järjestelmän eri osa-alueiden konfigurointiin ja mukauttamiseen. Sen avulla ylläpitäjät voivat määritellä Arkimen asetuksia vastaamaan heidän omia tarpeitaan ja mieltymyksiään. Välilehden kautta käyttäjät voivat hallinnoida esimerkiksi oman web-käyttöliittymän asetuksia tai vaihtaa palveluun salasanansa. Settings -välilehti mahdollistaa myös ylläpitäjille tavan konfiguroida ilmoituksia, joita Arkime lähettää haluttaessa esimerkiksi mielenkiintoisista löydöksistä kaapatussa datassa. Arkimen Settings -välilehden näkymä käyttäjälle on esitelty kuviossa 11. (Arkime Help. N.d.)



Kuvio 11. Arkimen asetukset Settings -välilehdellä

Users

Arkimen Users -välilehdelle on keskitetty käyttäjähallinta sekä käyttöoikeuksien valvonta. Sen avulla ylläpitäjät voivat luoda uusia ja hallita jo olemassa olevia käyttäjätilejä sekä määrittää niiden oikeudet ja roolit järjestelmässä. Arkimeen on luotu valmiita käyttäjäryhmiä (ks. kuvio 12), joilla on tiettyjä oikeuksia järjestelmän käyttöön. Tämä helpottaa käyttäjien pääsynhallinnassa ja varmistaa, että järjestelmän eri käyttäjillä on vain ne oikeudet, joita he tehtävissään tarvitsevat. (Arkime Help. N.d.)



Kuvio 12. Users -välilehden näkymä.

4 Kerätyn pakettidatan analysointi

Ilman ymmärrystä siitä, mikä on tarkasteltavan verkon normaalia liikennettä, epänormaalien tapahtumien havaitseminen siinä on mahdotonta. Ennen liikenteen analysoinnin aloittamista on luotava hahmotelma siitä, mikä on verkon toivottua ja normaalia toimintaa. Tarkastelijan on tiedettävä protokollat ja portit, joiden käyttö verkossa on tarpeellista sen toivotun toiminnan kannalta. Lisäksi on oltava tieto siitä, mitkä verkon laitteet saavat keskustella toistensa kanssa, jotta ylimääräiset laitteet ja yhteydenotot voidaan havaita analyysiä tehdessä. (Lucas, 2010.)

Mainittujen asioiden toteutumiseksi on perusteltua suorittaa seuraavat asia analyysia tehdessä

- Valitaan datan keräämiseksi sopiva aikaväli, esimerkiksi viikko, jotta saadaan tarpeeksi kattava tietoperusta analyysille.
- Tarkastellaan kerättyä dataa ja verrataan sitä järjestelmän dokumentaatioon.
- Etsitään mahdollisia laitteita, portteja ja yhteyksiä, joita ei ole mainittu dokumentaatiossa.

(Lucas, 2010.)

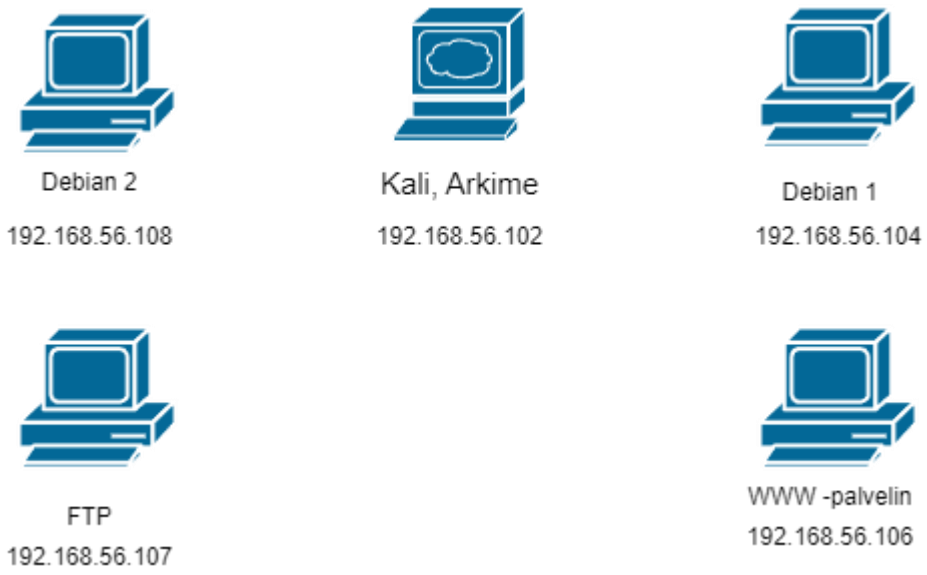
Tämä voi muodostua ongelmaksi laajoissa ja monimutkaisissa verkoissa, joissa liikennöivän datan määrä voi kasvaa erittäin suureksi. Tämän takia on usein järkevää analysoida tarkasteltavaa verkkoa pienemmissä osissa, kuitenkin niin että datan keräämisen aikaväli on tarpeeksi laaja. Tämä voi vaihdella järjestelmän mukaan, mutta liian suppean datan tarkastelu ei tuota luotettavaa tulosta verkkoliikenteen turvallisuudesta.

Jokaisesta tietojärjestelmästä ja sen toiminnasta tulisi olla kattava dokumentaatio valmiina järjestelmän kehittäjän toimesta, jonka käyttö tässä analyysin vaiheessa on oleellista. Jokainen havaittu toiminta verkossa, joka ei ole dokumentaation mukaista, on tutkittava. Kaikki ylimääräinen liikenne ei ole välttämättä haitallista tai hyökkääjän toimintaa, koska kyse voi olla esimerkiksi vain konfiguraatiovirheestä järjestelmän toiminnassa. Konfiguraatiovirheiden

löytyminen järjestelmästä on silti oleellinen havainto, joka tulee korjata verkon luotettavuuden lisäämiseksi.

4.1 Testiympäristön esittely

Arkimen ominaisuuksien esittelemisen avuksi luotiin alla esitelty yksinkertainen testiympäristön VirtualBoxin avulla. Testiympäristön laitteet luovat ajastetusti yksinkertaista ennalta määrättyä liikennettä verkkoon, jonka ympäristön Kali -tietokone nauhoittaa käyttäen Arkimea. Kaikki työssä käytetyt verkkoliikennenauhoitukset ovat luotu käyttäen kyseistä testiympäristöä. Testiympäristön topologia on esitelty kuviossa 13.



Kuvio 13. Havainnollistava kuva testiympäristöstä

Testijärjestelmässä liikennöi ajastetusti seuraavaa dataa:

- Debian 2 sekä Debian 1 -laitteet liikennöivät FTP-protokollaa käyttäen FTP-palvelimelle. Ne lataavat palvelimelta tiedoston, jonka jälkeen ne lataavat sinne uuden tiedoston omista tiedostoistaan. Tämän on tarkoitus luoda FTP-liikennettä testijärjestelmään, joka voidaan havainnoida verkkoliikenteestä Arkimen avulla

- Debian 1 sekä Debian 2 -laitteet vierailevat WWW- palvelin laitteen ajamalla http -palvelussa, tehden siellä erinäisiä toimenpiteitä. Tämän liikenteen on tarkoitus generoida http -liikennettä Arkimen nähtäväksi.

- Järjestelmään on myös manuaalisesti luotu SSH-liikennettä, joka toimii esimerkkinä salatusta liikenteestä.

4.2 Arkimen konfigurointitiedoston optimointi

Arkimen pakettikaappausominaisuuksia on mahdollista määrittää sen hetkistä käyttötarkoitusta varten uudelleen. Konfigurointitiedosto löytyy hakemistosta /opt/arkime/etc/config.ini ja sitä voidaan muokata tekstieditorilla esimerkiksi Nanolla tai Vimillä. Hyödyllisiä asetuksia auditoinnin näkökulmasta ovat:

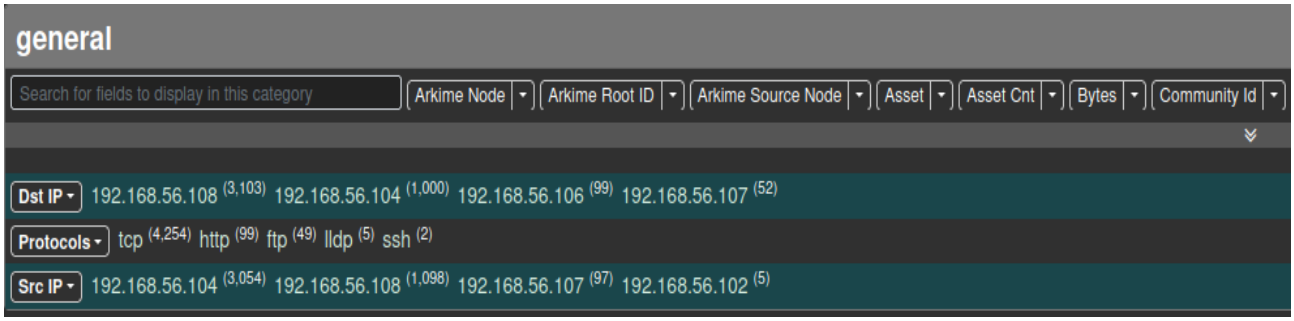
- interfaces
    - Interfaces -valinnan avulla voidaan määrittää, mitä verkkoliitäntöjä Arkimen halutaan nauhoittavan. Valinta ottaa syötteenä listan verkkoliitäntöjen nimistä puolipisteen avulla eroteltuna. Esimerkiksi “eth-host;eth-lan".

- maxPackets
    - Tällä valinnalla määritetään kuinka monta pakettia Arkime kerää nauhoitettavasta liikenteestä ennen kuin se muodostaa siitä session ja välittää sen arkimeviewerille näkyväksi. Jos tarkasteltava järjestelmä on pieni ja siellä liikkuu vain vähän dataa, tätä arvoa kannattaa laskea, jotta paketit saadaan nopeasti näkymään käyttöliittymässä. Vakioarvo maxPacketille on 10 000 pakettia.

- interfaceOps
    - Tämä valinta on hyödyllinen, kun sama Arkime capture -ohjelmisto nauhoittaa montaa eri verkkoliitäntää samanaikaisesti. Kyseinen valinta leimaa jokaisen nauhoitetun verkkoistunnon kyseisen verkkoliitännän nimellä. Tämä auttaa tarkastelijaa havaitsemaan mistä verkosta kyseinen nauhoitettu istunto on tullut.

4.3 Pakettien hakeminen ja tiedon suodatus

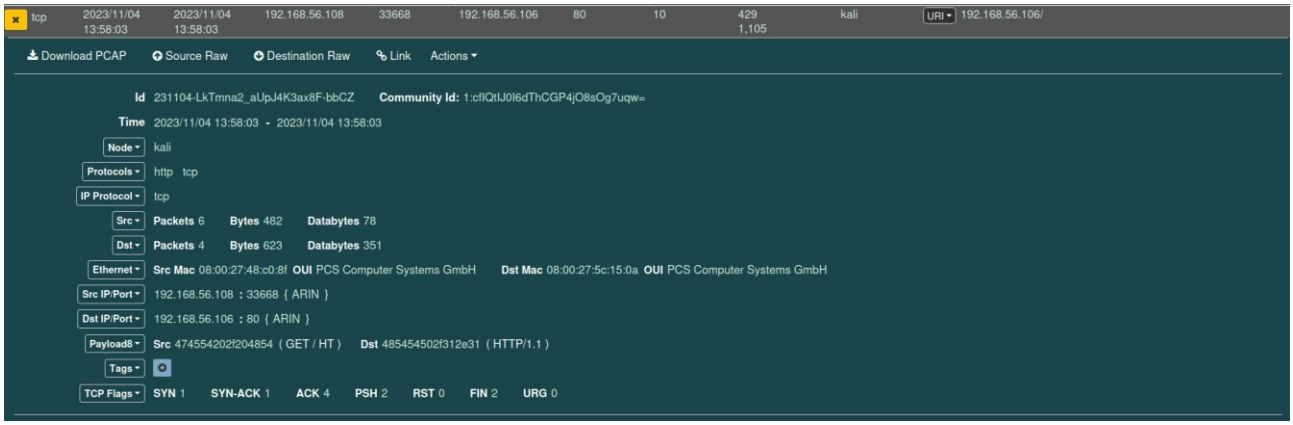
Arkimen avulla voidaan auditoinnin aikana tehokkaasti etsiä epänormaaleja tapahtumia verkosta. SPIViewin avulla saa selkeän ja kattavan näkymän siitä, mitkä laitteet ja protokollat ovat liikennöineet verkkoliikenteen nauhoituksen aikana. SPIView kerää kaikki nauhoitetussa datassa esiintyvät IP-osoitteet general -otsikon alle, jossa ne on lajiteltu tarkemmin vielä kohde sekä lähde IP-osoitteisiin (ks. kuvio 14). Vertailemalla kyseisiä osoitteita järjestelmän dokumentaatioon, voidaan havaita ylimääräiset osoitteet tehokkaasti ympäristöstä. IP-osoitteiden lisäksi valikossa on myös eritelty mitä protokollia kyseisten laitteiden yhteydenotoissa on käytetty.



Kuvio 14. General -taulukon sisältö SPIView -sivulla.

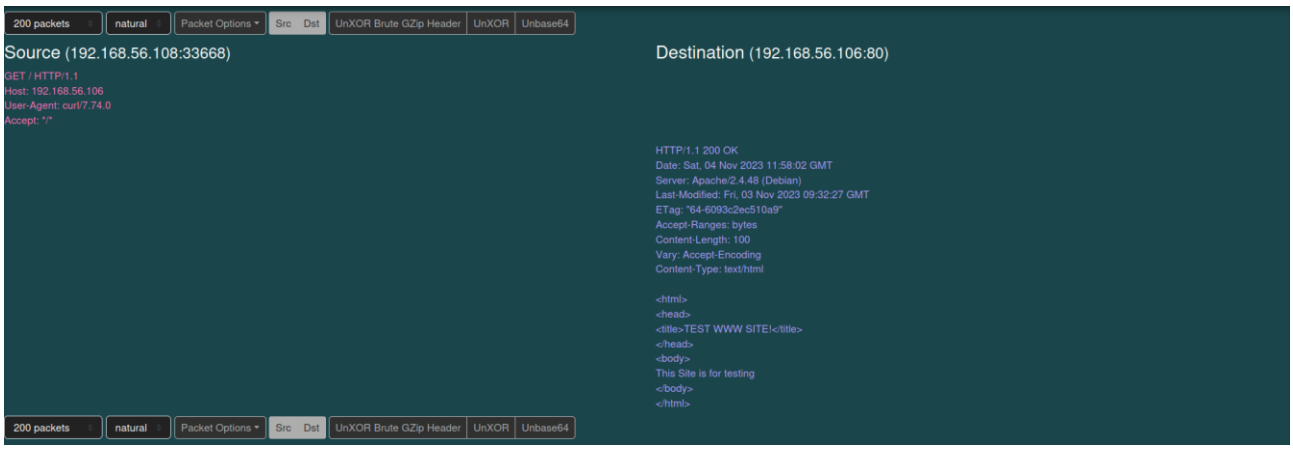
Jokainen ominaisuus (IP-osoite tai protokolla) voidaan valita suodatusperusteeksi klikkaamalla sitä, jolloin se siirtyy sivun yläreunassa olevaan hakukenttään. Kun tämän jälkeen suorittaa uuden haun, voidaan yksittäistä protokollaa tai IP-osoitetta tarkastella syvällisemmin. Tämä on erityisen hyödyllistä silloin, kun datasta löytyy tunnistamaton osoite. Tällöin on mahdollista nopeasti aloittaa selvitys siitä, mitä kyseinen laite on järjestelmässä tehnyt.

Arkimella on mahdollista avata nauhoitettuja istuntoja tarkempaa analysointia varten Sessions -välilehdeltä. Avaamalla istunnon, kuten kuviossa 15, siitä voidaan tarkastella muun muassa pakettien määriä sekä viestittelevien laitteiden MAC-osoitteita.



Kuvio 15. Näkymä kaapatun verkkoistunnon tiedoista.

Jos tietoliikenne ei ole salattua, sen sisältöä voidaan tutkia myös avaamalla istunto tarkempaa käsittelyä varten (ks. kuvio 16). Selkokielisestä datasta on helppo päätellä mitä verkossa on tapahtunut ja mitä tietoa liikennöivät laitteet ovat vaihtaneet.



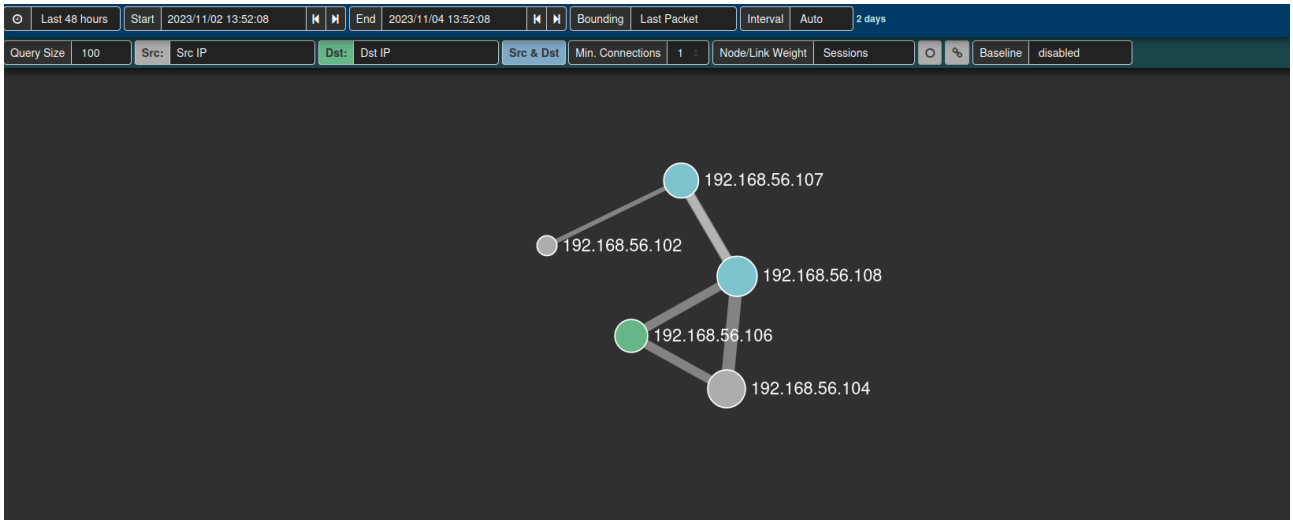
Kuvio 16. Selkotekstinä nauhoitetun verkkoistunnon sisältö.

Kun liikenne kulkee salattuna tietojärjestelmässä, kuten on toivottua tietoturvan kannalta, pakettien sisältöä ei pysty tulkitsemaan (ks. kuvio 17). Tämä estää tietojen urkinnan mahdollisten uhkatoimijoiden näkökulmasta.

Kuvio 17. Salatun SSH-istunnon sisältö.

4.4 Visuaalinen tarkastelu Connections -työkalulla

Connections -sivu on erittäin hyödyllinen auditointia suorittaessa, kun halutaan visualisoida nauhoitetussa liikenteessä esiintyvien laitteiden välisiä yhteyksiä. Kuvaajan avulla on helppo saada käsitys siitä, kuinka liikennöinti laitteiden välillä toimii tarkasteltavassa järjestelmässä. Kuvaaja koostuu kuvion 18 mukaan solmuista sekä niiden välillä esiintyvistä linkeistä. Jokainen linkki ja solmu on avattavissa syvempää tarkastelua varten, joten esimerkiksi kahden solmun välistä linkkiä klikkaamalla voidaan analysoida tarkemmin liikennettä, joka on kulkenut kyseisten laitteiden välillä. Tästä voi olla tarkastelijalle suuri apu silloin, kun verkosta on löytynyt jokin tunnistamaton osoite ja halutaan nopeasti selvittää mihin muihin järjestelmän laitteisiin se on ollut yhteydessä, sekä mitä kyseiset laitteet ovat keskenään liikennöineet.



Kuvio 18. Testiympäristön liikenteen perusteella luotu puukaavio.

Kuvaajassa näkyvillä olevat osoitteet ovat täysin käyttäjän valittavissa. Näkyvissä olevia laitteita voidaan määrittää sivun yläreunassa olevan hakupalkin avulla. Hakupalkki toimii samalla tavalla kuin muillakin web käyttöliittymän sivuilla. Arkime käyttää yksinkertaista kyselykieltä suodatuksen muodostamiseen. Se tukee ryhmittelyä sulkujen avulla sekä AND- ja OR-lausekkeita käyttämällä &&- ja ||-merkintöjä. Esimerkiksi haulla “ip.src == 192.168.56.105 && ip.dst == 192.168.56.107” nähtäisiin kaikki liikenne kahden edellä mainitun osoitteen välillä. Kuten kuviossa 19 on esitetty, käyttäjä voi myös määrittää suodatusehtoja automaattisesti valitsemalla halutun osoitteen hiirellä ja määrittämällä aukeavasta alasvetovalikosta halutun ehdon kyseiselle osoitteelle.

Kuvio 19. Näkymä yksittäisen IP-osoitteen lisävalinnoista

5 Johtopäätökset

Tutkimuksen tavoitteena oli selvittää, kuinka hyvin pakettianalysaattori Arkime soveltuu tietoturva-auditointien osana suoritettavaan tietoliikenneanalyysiin. Työn aikana Arkimen ominaisuuksia tarkasteltiin eri osa-alueilta ja havainnollistettiin, kuinka niitä on mahdollista käyttää verkkoliikenteen tarkastelussa apuna. Tutkimuksen alussa laadittiin kaksi tutkimuskysymystä, joiden avulla työtä alettiin viemään eteenpäin.

Työn aikana huomattiin, että Arkime soveltuu tietoliikenteen analysointiin hyvin. Arkimen vahvuuksina on käyttäjäystävällinen käyttöliittymä, joka tekee ohjelman käytöstä selkeää ja sen myötä myös tehokasta. Navigointi eri sivujen välillä Arkimen web-käyttöliitymässä on helppoa, joka mahdollistaa datan tulkitsemisen nopeasti eri työkalujen avulla. Arkime pystyy kuvamaan kerättyä dataa monipuolisesti käyttäen erilaisia graafeja sekä kuvaajia, joka osaltansa helpottaa tarkastelijaa hahmottamaan järjestelmässä liikkuvaa tietoliikennettä. Arkimen tapa koota yksittäiset paketit kokonaisiksi istunnoiksi laitteiden välillä antaa tutkijalle selkeän näkymän mitä eri laitteet ovat järjestelmässä keskenään viestineet.

Mahdollisten uhkien tai anomalioiden löytymisen yhteydessä, Arkimen eri työkalujen avulla on helppo alkaa selvittämään kyseisen havainnon vaikutusta ja toimintaa tarkasteltavassa verkossa. SPIView-sivun avulla on tehokasta alkaa suodattamaan nauhoitettua dataa niin, että sieltä saadaan esille kyseistä havaintoa koskeva hyödyllinen tieto. Tarkastelija voi myös luoda kaapatusta liikenteestä puukaavion mukaisen kuvaajan käyttäen Connections -sivua, jonka avulla tarkastelija voi havainnoida dataa halutessaan visuaalisesti.

Arkime soveltuu ominaisuuksiltaan myös verkonvalvonta työkaluksi. Ominaisuuksien puitteissa voidaankin huomata, että se onkin ollut Arkimen alkuperäinen kehittämistarkoitus. Se pystyy nauhoittamaan suuria määriä liikennettä monista eri verkkoliitänteistä samanaikaisesti ja se on mahdollista myös integroida Elastic Stack:iin, joka tehostaa sen toimintaa entisestään. Tämä tekee siitä loistavan vaihtoehdon SOC (Security Operations Center) -toimijoille. Kuten aikaisemmin on todettu, sitä voidaan kuitenkin käyttää tehokkaana työkaluna tietoturva-auditointien yhteydessä. Yksi merkittävä positiivinen puoli on Arkimen avoimen lähdekoodin periaate, joka mahdollistaa yhteisön osallistumisen sen kehitykseen ja pitää ohjelmiston ilmaisena kaikille halukkaille käyttäjille.

Arkimen haasteita on hieman monimutkainen asennus, koska sitä ei voida asentaa käyttämällä Linux-käyttöjärjestelmän pakettienhallintatyökaluja. Vaikka Arkimen asennukseen löytyy ohjeet verkosta, sen käyttöönotto vaatii hieman enemmän Linux -käyttöjärjestelmän tuntemista sekä erinäisten asetusten muuttamista. Tämä ei todennäköisesti ole ongelma asiantuntevalle henkilölle, mutta kokemattomampi henkilö voi tuntea asennusprosessin monimutkaiseksi.

Arkimen avulla ei myöskään voida tutkia kaapattuja paketteja yhtä syvällisellä tasolla kuin muutamilla muilla tarjolla olevilla pakettianalysaattoreilla. Arkime kuitenkin tallentaa kaappaamansa paketit standardoidussa PCAP-tiedostomuodossa, joten tallennetut pakettidatat on mahdollista avata jollain toisella ohjelmalla, jos niitä on tarve analysoida tarkemmin. Kyseisissä tilanteissa voidaan käyttää apuna esimerkiksi ilmaista Wireshark -ohjelmaa, joka tarjoaa erinomaisen näkyvyyden protokolla tasolle saakka.

6 Pohdinta

Tutkimuksen tavoitteena oli tutkia Arkimen potentiaalia ja käyttöä tietoturva-auditoinneissa sekä kuinka Arkimen avulla voidaan tarkastella verkkoliikennettä, havaita haavoittuvuuksia ja uhkia, sekä tehostaa järjestelmävastaavia reagoimaan mahdollisiin havaittuihin tietoturvariskeihin. Työ pyrki myös tuottamaan hyödyllistä tietoa Arkimesta toimijoille, jotka harkitsevat tai jo käyttävät ohjelmistoa osana toimintaansa. Tutkimuksen tulosten valossa on turvallista todeta, että Arkime on varsin hyvä työkalu kyseisten toimintojen suorittamiseen.

Nykyaikaisissa tietojärjestelmissä verkkoliikenteen määrä voi olla todella suurta, joka hankaloittaa verkkoliikenteenanalysointia huomattavasti. Tässä työssä ei pystytty simuloimaan modernin tietojärjestelmän mukaista liikennettä johtuen rajoitetuista resursseista. Siitä huolimatta testidataa saatiin generoitua tarpeeksi, jotta sen avulla oli mahdollista demonstroida Arkimen eri työkalujen toimintaa. Arkimen työkalujen hyödyllisyys ja sen tapa indeksoida kerättyä dataa alkaakin vasta suurien datavirtojen käsittelyssä osoittamaan tehokkuuttaan.

Arkimen tietoperustan luominen työhön oli hieman ongelmallista, koska ainoat lähteet liittyen itse ohjelmistoon ja sen käyttöön oli peräisin Arkimen omasta dokumentaatiosta. Tästä syystä ristikkäin vertailu eri lähteiden välillä osoittautui vaikeaksi. Muun aiheeseen liittyvän tietoperustan laatiminen oli selkeämpää, koska lähteitä oli tarjolla runsaasti.

Jatkokehittämisen kannalta olisi hyödyllistä testata Arkimen kyvykkyyksiä suuremmalla ja monipuolisemmalla verkkoliikennedatalla. Tällöin saataisiin arvokasta tietoa siitä, kuinka se suoriutuu suurien tietomassojen käsittelemisestä ja kuinka relevantin datan parsiminen nauhoitetusta liikenteestä onnistuu vielä monipuolisemmasta tietoliikenteestä. Jatkokehittämisen aiheena voisi olla myös Arkimen integrointiin Elasticsearch Stack –ohjelmistoon ja tutkia saavutetaanko sen avulla vielä lisähyötyjä liittyen tietoturva-auditointeihin.

Lähteet

Andhavarapu, A. (2017). Learning Elasticsearch. Packt Publishing Ltd.

Arkime. N.d. Verkkosivu. Viitattu 20.10.2023 https://github.com/arkime/arkime#background

Charest F. 2023. Active vs. Passive Network Monitoring: Which Method is Right for You. Viitattu 24.10.2023. https://obkio.com/blog/active-vs-passive-network-monitoring/

Instructions for using the prebuilt Arkime packages. N.d. Verkkosivu. Viitattu 16.10.2023. https://raw.githubusercontent.com/arkime/arkime/main/release/README.txt

K.G.Anagnostakis, S.Ioannidis, S. Miltchev, J. Ioannidis, M.Greenwald, J.M.Smith, 2002, Efficient Packet Monitoring for Network Management, Artikkeli, Viitattu 12.10.2023, https://dsl.cis.upenn.edu/FLAME/efficient_packet_mon.pdf

Lucas, M. (2010). Network flow analysis (1st edition.). No Starch Press. Viitattu 14.11.2023

Nweke L, 2017, Using the CIA and AAA Models to Explain Cybersecurity Activities. Artikkeli. Viitattu 9.10.2023. https://pmworldlibrary.net/wp-content/uploads/2017/05/171126-Nweke-Using-CIA-and-AAA-Models-to-explain-Cybersecurity.pdf

Ohje tietoturvallisuuden arviointilaitoksille, 2022, Traficom, Viitattu 24.10.2023, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Arviointilaitosohje%20210-2022%20O%20%2822.6.2022%29_1.pdf

OSI Layers – Microsoft has oftenly referred this term in Azure security topics. What is it all about? Verkkosivu. 2021. Viitattu 14.11.2023. https://industry40.co.in/networking-osi-layers/

Sanders, C. 2011. Practical Packet Analysis. 2 painos. San Francisco: No Starch

Syngress. Ethereal Packet Sniffing, Elsevier Science & Technology Books, 2004. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=294122.

Syngress. Ethereal Packet Sniffing, Elsevier Science & Technology Books, 2004. ProQuest Ebook Central. Viitattu 5.10.2023. http://ebookcentral.proquest.com/lib/jypoly-ebooks/detail.action?docID=294122.

The CIA triad of confidentiality, integrity and availability, N.d. Verkkosivu. Viitattu 4.11.2023 https://www.i-scoop.eu/cybersecurity/cia-confidentiality-integrity-availability-security/

Toikko, T. & Rantanen, T. 2009. Tutkimuksellinen kehittämistoiminta. Tampere: Tampereen yliopistopaino oy. Viitattu 14.11.2023. https://urn.fi/URN:ISBN:978-951-44-7732-4

Topsana, Kyle. 2020. Indexing Network Traffic with Moloch and Elastic. Viitattu 14.11.2023. https://medium.com/swlh/indexing-network-traffic-with-moloch-and-elastic-931dda8a1685

Vice Vicente, 2023, Security Audits: A Comprehensive Overview, Blogi, Viitattu 30.09.2023, https://www.auditboard.com/blog/what-is-security-audit/

What is a Network Packet?. N.d. Verkkosivu. Viitattu 14.11.2023. https://www.netscout.com/what-is/packet

What is Cybersecurity?. 2021. Blogi. Viitattu 15.10.2023. https://www.cisa.gov/news-events/news/what-cybersecurity

What is OSI Model. N.d. Verkkosivu. Viitattu 9.11.2023 https://www.imperva.com/learn/application-security/osi-model/

What Is The OSI Model? Definition, Layers, and Importance. 2022. Verkkosivu. Viitattu 9.11.2023. https://www.spiceworks.com/tech/networking/articles/what-is-osi-model/

What is the OSI Model?. Verkkosivu. N.d. Viitattu 8.11.2023.
https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/