SecurityOnion & Wazuh

Ryhmä 13

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Tietoturvakontrollit TTC6010-3007

28.11.2024

Tieto- ja viestintätekniikka

Sisältö

[1 Johdanto 3](#_Toc183428560)

[2 Teoriaa 3](#_Toc183428561)

[2.1 Wazuh 3](#_Toc183428562)

[2.2 Security Onion 4](#_Toc183428563)

[3 Toteutus 4](#_Toc183428564)

[3.1 Mikä on Zeek? 11](#_Toc183428565)

[4 Wazuh konfigurointi 12](#_Toc183428566)

[5 Testaukset 17](#_Toc183428567)

[Lähteet 21](#_Toc183428568)

[Liitteet 22](#_Toc183428569)

[Liite 1. Liitteen otsikko 22](#_Toc183428570)

[Liite 2. Liitteen otsikko 23](#_Toc183428571)

Kuviot

[Kuvio 1. VLE 3](#_Toc183428572)

[Kuvio 2. Commands1 4](#_Toc183428573)

[Kuvio 3. Onion UI 5](#_Toc183428574)

[Kuvio 4. alerts 5](#_Toc183428575)

[Kuvio 5.actions 6](#_Toc183428576)

[Kuvio 6. laajennettu 6](#_Toc183428577)

[Kuvio 7. Dashboard 7](#_Toc183428578)

[Kuvio 8. Tools 7](#_Toc183428579)

[Kuvio 9. cyberchef 8](#_Toc183428580)

[Kuvio 10. Kibana\_dashboard 8](#_Toc183428581)

[Kuvio 11. latimes.com 9](#_Toc183428582)

[Kuvio 12. eventcategories 9](#_Toc183428583)

[Kuvio 13. file 10](#_Toc183428584)

[Kuvio 14. hosts 10](#_Toc183428585)

[Kuvio 15.zeek 11](#_Toc183428586)

[Kuvio 16. Lokit 11](#_Toc183428587)

[Kuvio 17. wazuh 12](#_Toc183428588)

[Kuvio 18. agents 13](#_Toc183428589)

[Kuvio 19. agents\_view 13](#_Toc183428590)

[Kuvio 20. agentin lisäys 14](#_Toc183428591)

[Kuvio 21. agentin lisäys2 14](#_Toc183428592)

[Kuvio 22. komentojen lisäys 15](#_Toc183428593)

[Kuvio 23. agents\_active 15](#_Toc183428594)

[Kuvio 24. agents\_active2 15](#_Toc183428595)

[Kuvio 25. Linux agentit 16](#_Toc183428596)

[Kuvio 26. Linux commands 16](#_Toc183428597)

[Kuvio 27. Wazuh agents. 17](#_Toc183428598)

[Kuvio 28. Wazuh agents 2 17](#_Toc183428599)

[Kuvio 29. test\_script 18](#_Toc183428600)

[Kuvio 30. alerts 19](#_Toc183428601)

[Kuvio 31. alerts2 19](#_Toc183428602)

Taulukot

[Taulukko 1. Taulukon otsikko, ei lähdetietoja **Virhe. Kirjanmerkkiä ei ole määritetty.**](file:///C:/Users/taante/Downloads/Taulukko#_Toc432081817)

[Taulukko 2. Taulukon otsikko, ei lähdetietoja **Virhe. Kirjanmerkkiä ei ole määritetty.**](file:///C:/Users/taante/Downloads/Taulukko#_Toc432081818)

# Johdanto

Tämä harjoitustyö keskittyy SecurityOnion ja Wazuh Järjestelmien konfiguroimiseen käyttökuntoon ja ominaisuuksien testaamiseen. Tehtävä toteutetaan Kuvion 1 mukaiseen VLE ympäristöön.

Kuva, joka sisältää kohteen teksti, diagrammi, kuvakaappaus, Suunnitelma

Kuvaus luotu automaattisesti

Kuvio 1. VLE

# Teoriaa

## Wazuh

Wazuh on ilmainen, avoimen lähdekoodin tietoturva-alusta, joka tarjoaa yhdistetyt XDR (Extended Detection and Response) ja SIEM (Security Information and Event Management) -ominaisuudet. Se on suunniteltu suojaamaan erilaisia ympäristöjä, mukaan lukien julkiset ja yksityiset pilvipalvelut sekä paikallisesti hallinnoidut datakeskukset. Wazuh keskittyy erityisesti päätelaitteiden ja pilvipalveluiden työympäristöjen suojaamiseen uhkia vastaan. Wazuhin keskeisiä ominaisuuksia on esimerkiksi

* Uhkien metsäöstys ja tapahtumiin reagointi
* Tiedostojewn eheyden valvonta
* Kattavat kojelaudat tietojen analysointia varten

(Brandstaetter. 2024.)

## Security Onion

Security Onion on avoimenlähdekoodin SIEM järjestelmä, joka on erityisesti suunniteltu tietoturvatapahtumien havaitsemiseen, kirjaamiseen ja analysointiin. Se yhdistää useita tehokkaita työkaluja yhteen kokonaisuuteen, jotta organisaatiot pystyvät hallitsemaan ja analysoimaan tietoturvaa tehokkaasti. (Sadhik. 2023.)

# Toteutus

Aloitetaan konfiguroiminen käynnistämällä onion palvelin, jatkossa haluamme päästä SecurityOnioniin käsiksi omalta koneeltamme Käyttämällä GlobalProtectia joka on konfiguroitu aiemmissa töissä. Onionin verkkokäyttöliittymään pääsee käsiksi <http://10.2.0.10> osoitteesta.

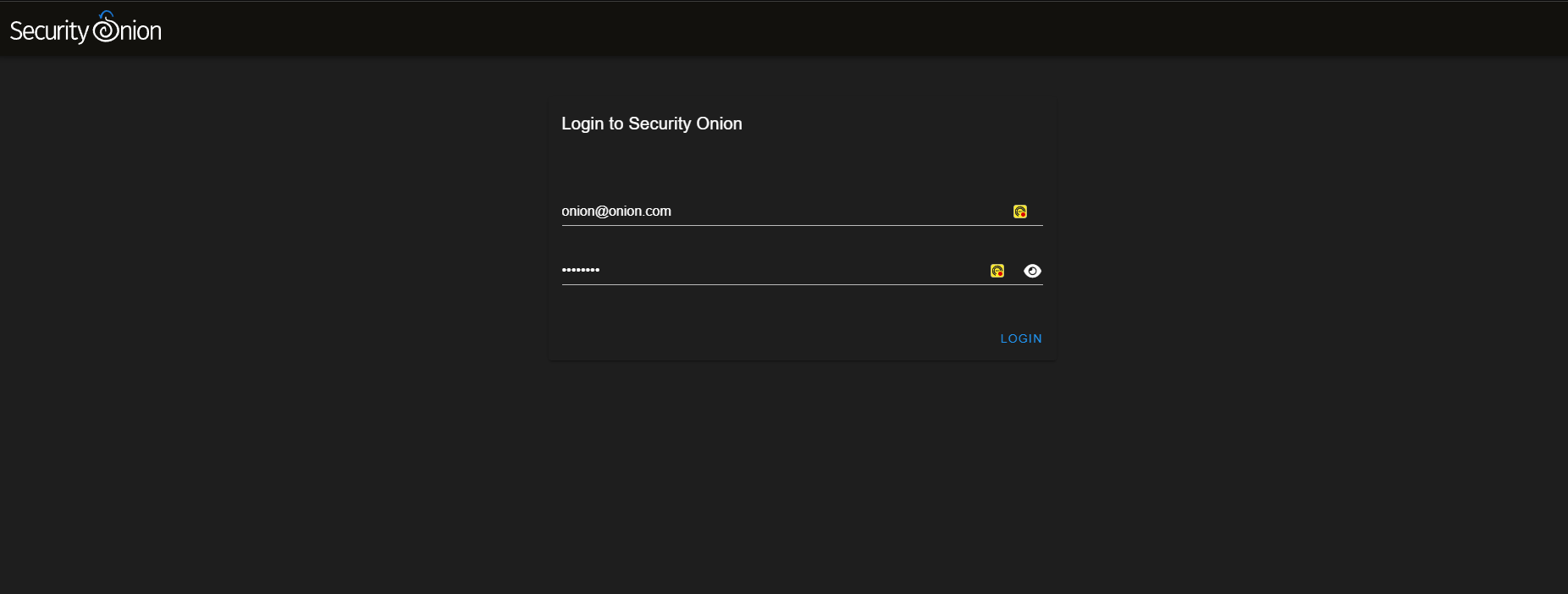
aloitetaan ajamalla komennot. (Kuvio 2)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, musta

Kuvaus luotu automaattisesti

Kuvio 2. Commands1

Nyt pääsemme omalla laitteellamme onioniin. (Kuvio 3)



Kuvio 3. Onion UI

Seuraavaksi alamme tutkimaan SecurityOnionista löytyviä ominaisuuksia. siirrytään ensin tutkimaan alert näkymää. (Kuvio 4)

Kuva, joka sisältää kohteen kuvakaappaus, teksti, ohjelmisto, Multimediaohjelmisto

Kuvaus luotu automaattisesti

Kuvio 4. alerts

Kun jotain hälytystä painaa, aukeaa valikko, josta voimme viedä hälytyksen esimerkiksi tarkasteltavaksi. Esimerkiksi actions välilehden alta virustotaliin. (Kuvio 5)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Multimediaohjelmisto

Kuvaus luotu automaattisesti

Kuvio 5.actions

Alertin saa laajennettua, kun painaa alaspäin nuolta hälytyksen vasemmasta laidasta. (Kuvio 6)

Kuva, joka sisältää kohteen kuvakaappaus, teksti, ohjelmisto, Multimediaohjelmisto

Kuvaus luotu automaattisesti

Kuvio 6. laajennettu

Dashboards välilehdellä saamme näkymään visuaalisia kuvauksia havaitusta liikenteestä ja pystymme analysoimaan esimerkiksi lähteitä, joista dataa on tullut. (Kuvio 7)

Kuva, joka sisältää kohteen kuvakaappaus, Multimediaohjelmisto, ohjelmisto, Grafiikkaohjelmisto

Kuvaus luotu automaattisesti

Kuvio 7. Dashboard

Tools osiosta löytyy security onioniin liitettyjä ja yleisesti käytettyjä työkaluja (Kuvio 8)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

Kuvio 8. Tools

Otetaan esimerkiksi CyberChef jonka avulla voidaan käsitellä vaikka salauksia. Kuviossa 9 on käännetty base64 salauksesta merkkijono.

Kuva, joka sisältää kohteen teksti, Fontti, ohjelmisto, viiva

Kuvaus luotu automaattisesti

Kuvio 9. cyberchef

avataan seuraavaksi kibana vasemmasta palkista tools osion alta

Kibana aukeaa dashboard näkymään. (Kuvio 10)

Kuva, joka sisältää kohteen kuvakaappaus, teksti, Multimediaohjelmisto, diagrammi

Kuvaus luotu automaattisesti

Kuvio 10. Kibana\_dashboard

Kokeillaan mitä saamme näkyviin, kun menemme WS01:llä osoitteeseen [www.latimes.com](http://www.latimes.com) ja avataan kibanasta discover välilehti. Täällä näemme ws01 menneen sivustolle latimes.com. (Kuvio 11)

Kuva, joka sisältää kohteen teksti, ohjelmisto, Multimediaohjelmisto, Grafiikkaohjelmisto

Kuvaus luotu automaattisesti

Kuvio 11. latimes.com

Kun palaamme dashboard välilehdelle, saa sieltä auki erilaisia näkymiä tapahtumiin liittyen. (Kuvio 12)

Kuva, joka sisältää kohteen kuvakaappaus, teksti, Multimediaohjelmisto, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 12. eventcategories

mennään file näkymään, jossa pystymme tarkastelemaan liikutettuja tiedostoja. (Kuvio 13)

Kuva, joka sisältää kohteen kuvakaappaus, teksti, ohjelmisto, Multimediaohjelmisto

Kuvaus luotu automaattisesti

Kuvio 13. file

hosts osiossa näkyy aiemmin tekemämme muutokset onion palvelimella, kun sallimme GlobalProtectin avulla yhteyden luomisen. (Kuvio 14)

Kuva, joka sisältää kohteen kuvakaappaus, Multimediaohjelmisto, ohjelmisto, Grafiikkaohjelmisto

Kuvaus luotu automaattisesti

Kuvio 14. hosts

lisätään seuraavaksi suodatin dashboard näkymässä, jotta voimme suodattaa haluamamme datan suuresta data määrästä. Otetaan vaikka vain Zeek avainsanan sisältävät tapahtumat näkyviin. (Kuvio 15)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Fontti

Kuvaus luotu automaattisesti

Kuvio 15.zeek

Zeek antaa valtavan määrän dataa. (Kuvio 16)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, muotoilu

Kuvaus luotu automaattisesti

Kuvio 16. Lokit

Tämä johtuu siitä, että Zeek kerää loki tietoa niin laajasti, tutkien verkkoliikennettä pakettien sovelluskerroksen tasolla asti.

## Mikä on Zeek?

Zeek on passiivinen, avoimen lähdekoodin verkkoliikenteen analysointityökalu. Sen ensisijainen tarkoitus on toimia verkon turvallisuusmonitorina, mutta se tukee myös hyvin muita liikenteen analyysitehtäviä. Zeek koostuu kahdesta pääkomponentista.

* **Tapahtumamoottori:** Tämä muuttaa saapuvan pakettiliikenteen korkeamman tason tapahtumiksi. Se kuvaa neutraalisti, mitä verkossa on havaittu, mutta ei tulkitse havaintojen merkitystä
* **Skriptitulkki:** Suorittaa Zeekin omalla skriptikielellä kirjoitettuja tapahtumankäsittelijöitä. Skriptit voivat ilmaista organisaation tietoturvakäytäntöjä ja määritellä tapahtumiin reagointia

Zeek reagoi verkkotapahtumien perusteella, kuten verkkoyhteydenotot ja DNS-kyselyt. Työkalu ymmärtää tunnetuimmat verkkoliikenneprotokollat ja tekee verkkotapahtumista selkeämpiä lokitietoja. Zeek lokeissa on tärkeät tiedot tapahtumista, kuten lähde- ja kohde IP-osoitteet, hostit ja SSL-sertifikaatit. Sillä voidaan myös tutkia tallennettuja pcap tiedostoja, joiden datan, kuten HTTP kyselyt se esittää lokimuodossa. (Zeek Hello World. 2024)

# Wazuh konfigurointi

Wazuh käyttöliittymään pääsee kirjautumaan osoitteella <HTTPS://10.2.0.12>

myös Wazuh käyttää Elastic:iä. (Kuvio 17)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Tietokonekuvake

Kuvaus luotu automaattisesti

Kuvio 17. wazuh

seuraavaksi lisätään agentit päätelaitteille DC01, WS01, WSUS, NS12 ja WWW. Siirrytään agents välilehdelle. (Kuvio 18)

Kuva, joka sisältää kohteen teksti, ohjelmisto, Tietokonekuvake, Verkkosivusto

Kuvaus luotu automaattisesti

Kuvio 18. agents

Agents välilehdellä näkyy meidän haluamat laitteet mutta agentin tila on disconnected. (Kuvio 19)

Kuva, joka sisältää kohteen teksti, numero, Fontti, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 19. agents\_view

poistetaan disconnected agentit myöhemmin, lisätään aluksi uusi WS01. (Kuvio 20)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Verkkosivusto

Kuvaus luotu automaattisesti

Kuvio 20. agentin lisäys

ajetaan seuraavat komennot. (Kuvio 21)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Verkkosivusto

Kuvaus luotu automaattisesti

Kuvio 21. agentin lisäys2

suoritetaan komennot WS01:llä. (Kuvio 22)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Fontti

Kuvaus luotu automaattisesti

Kuvio 22. komentojen lisäys

aiemmin disconnected WS01 on nyt paikattu uudella, joka on aktiivinen. (Kuvio 23)

Kuva, joka sisältää kohteen teksti, Fontti, viiva, numero

Kuvaus luotu automaattisesti

Kuvio 23. agents\_active

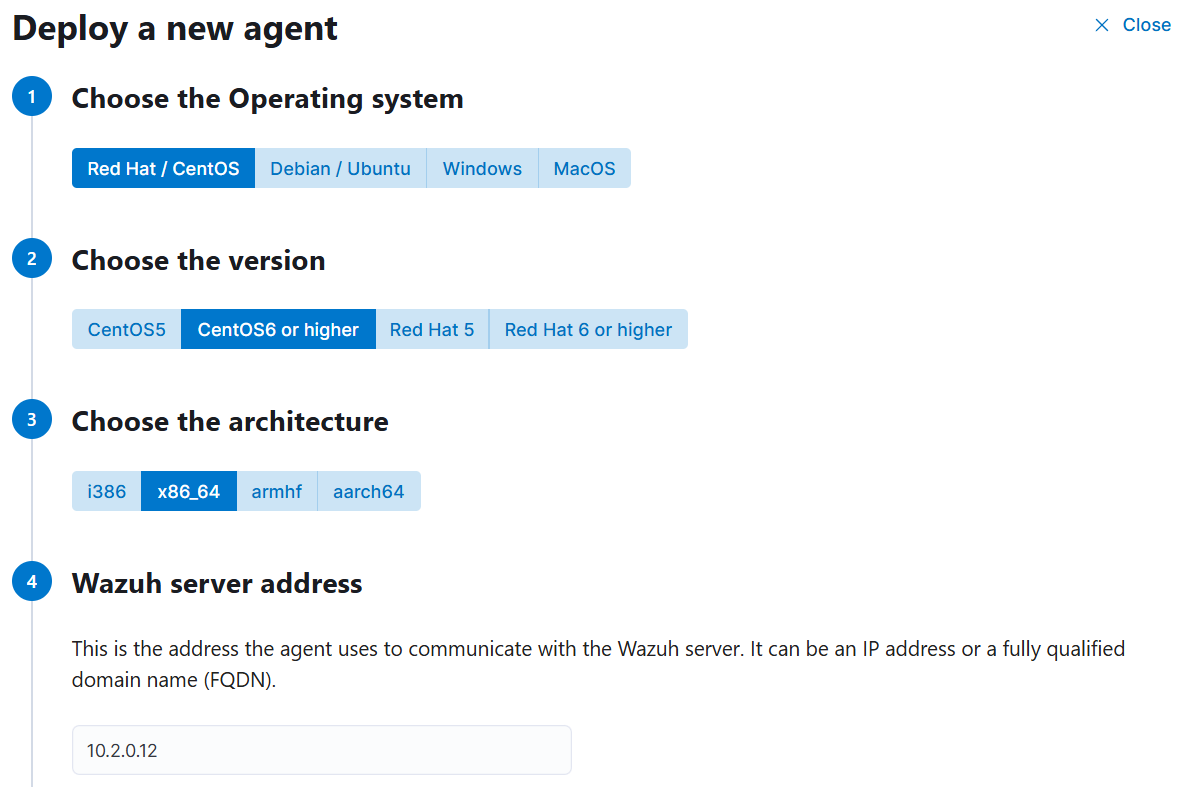
toistetaan sama SRV01, DC01 ja WSUS palvelimille, tämän jälkeen agents näyttää tältä. (Kuvio 24)

Kuva, joka sisältää kohteen teksti, Fontti, numero, viiva

Kuvaus luotu automaattisesti

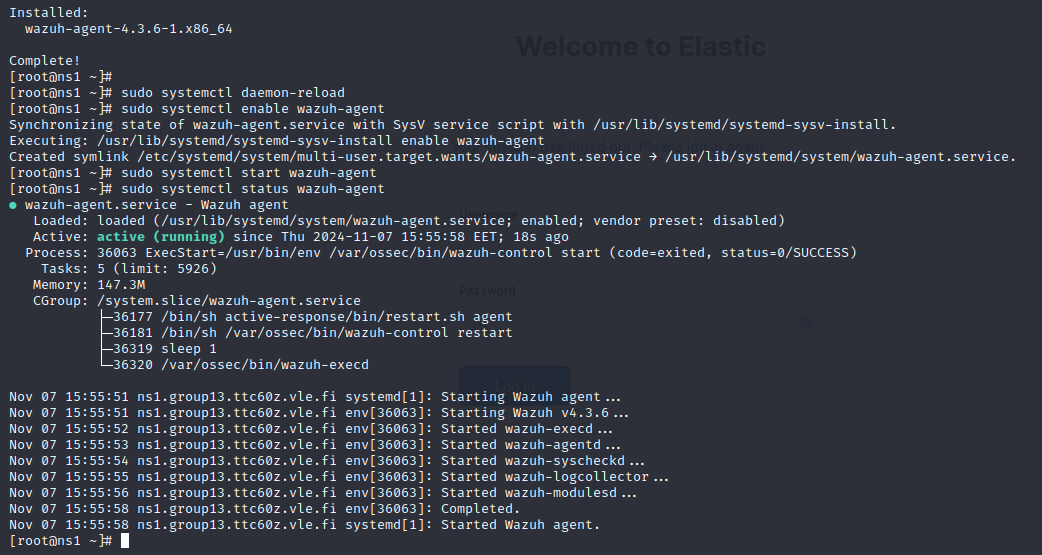
Kuvio 24. agents\_active2

Seuraavaksi linux agentit WWW ja NS1 toimimaan. Agentit luotiin kuvan (Kuvio 25) mukaisilla asetuksilla.



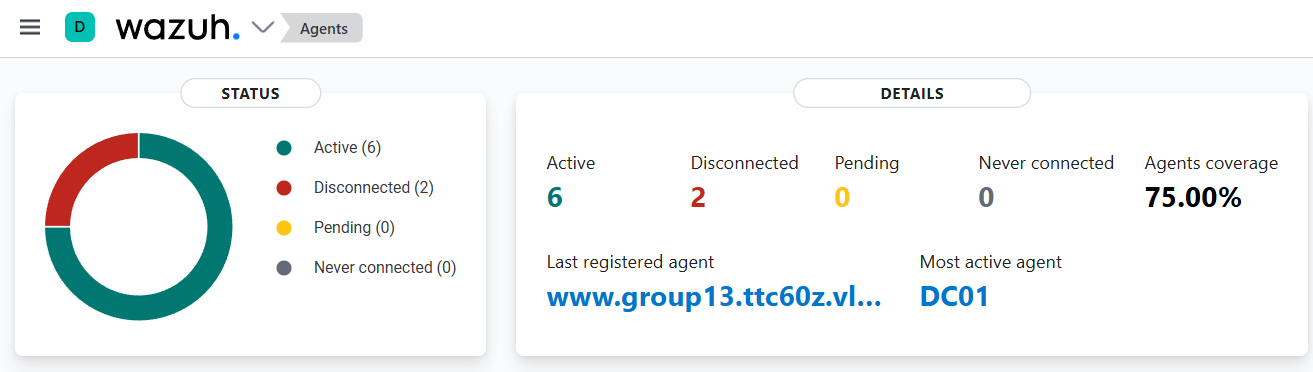
Kuvio 25. Linux agentit

Agentti asennettu Linux-käyttöjärjestelmälle (NS1) ja tehty samalla tavalla WWW:lle. Alla kuva, jossa ilmenee tila Running. (Kuvio 26)

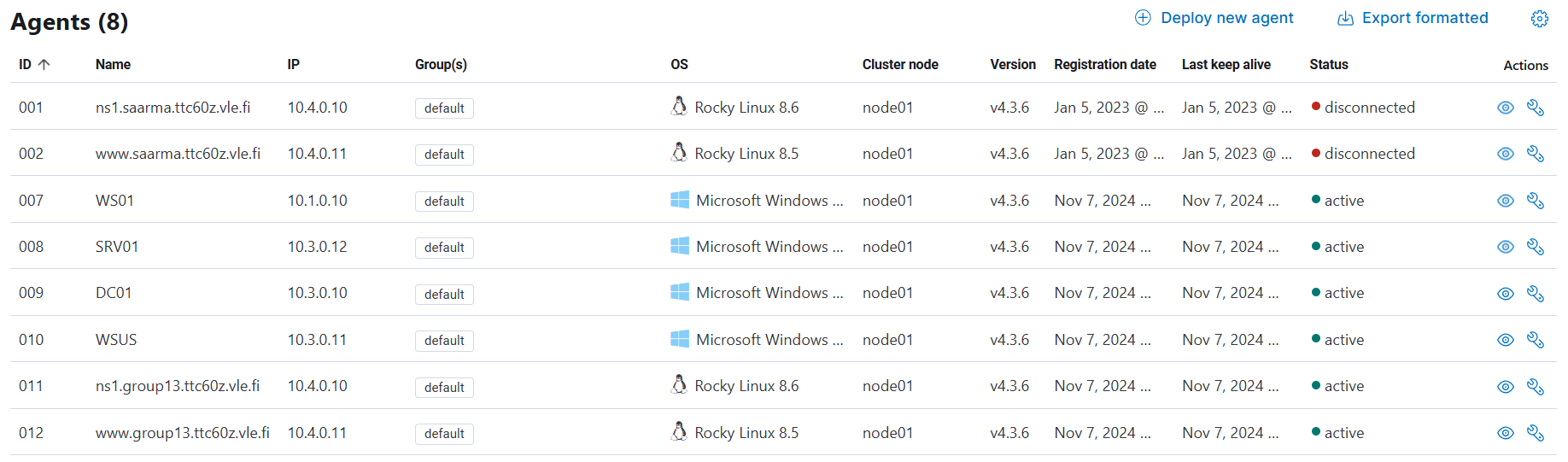


Kuvio 26. Linux commands

Saatiin myös Linux agentit (NS1, WWW) aktiivisiksi (Kuvio 27 & 28). Aiemmin varmaan opettajan toimesta luodut agentit näkyvät vieläkin listassa (ns1.saarma ja [www.saarma](https://www.saarma)), luotu vuonna 2023.



Kuvio 27. Wazuh agents.



Kuvio 28. Wazuh agents 2

# Testaukset

Seuraavaksi aiheutamme hälytyksiä asentamiimme järjestelmiin testataksemme niiden reaktiota.

Aloitetaan ajamalla kali-ws laitteella seuraava skripti tiedosto. (Kuvio 29)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 29. test\_script

Skripti suorittaa useita eri verkkojen ja haavoittuvuuksien skannauksia, kuten porttiskannaus, verkkoskannaus sekä metasloit viitekehyksen RPC ja SMB haavoittuvuus skannaukset. Skripti suorittaa myös RDP salasanan murto yrityksen. näistä aiheutuu useita erilaisia hälytyksiä security onion järjestelmään. (Kuvio 30)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Multimediaohjelmisto

Kuvaus luotu automaattisesti

Kuvio 30. alerts

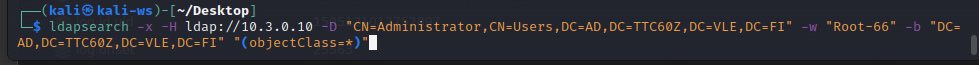
Wazuh järjestelmässä ilmaantuu myös useita hälytyksiä. Kuviossa 31 näkyvissä esimerkiksi yksi epäonnistunut kirjautumisyritys brute-forcen jäljiltä.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, Tontti

Kuvaus luotu automaattisesti

Kuvio 31. alerts2

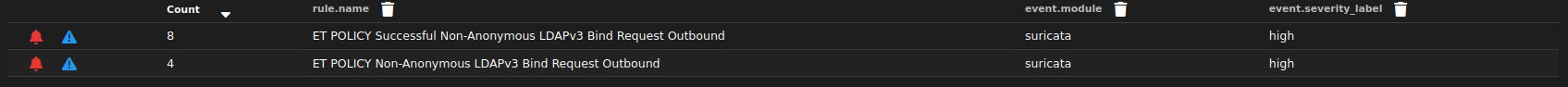
Kokeillaan ajaa LDAP-tiedustelu komento kali-ws:llä kuvion 32 mukaan.



Kuvio 32.ldap

Komento käyttää ldap protokollaa tiedustellakseen Active Directory -ympäristöstä.

tästä aiheutuu Security Onioniin hälytyksiä.



Kuvio 33. alert\_SecOnion

avataan alempi hälytys ryhmittely tarkempaan tarkasteluun Hunt ominaisuudella. Kuviossa 34 ilmenee lähde ja kohde ip osoitteet ja portit.

Kuva, joka sisältää kohteen kuvakaappaus, viiva

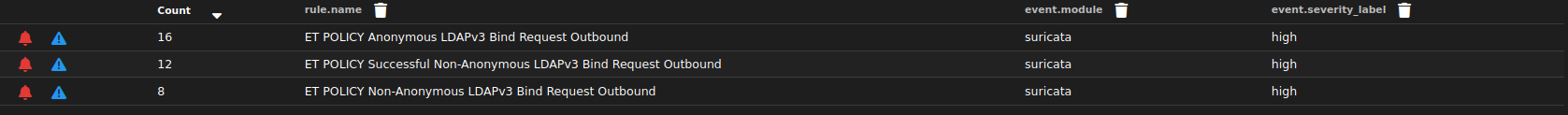
Kuvaus luotu automaattisesti

Kuvio 34. hunt

ajetaan vielä Nmap skanni hyödyntäen NSE-skriptejä kuvion 35 komennolla.



Security Onion hälytykset kuviossa 35. Samoja hälytyksiä syntyi aiemmasta testistä, mutta niiden määrä on lisääntynyt ja ylin rivi on uusi.



Kuvio 35.Alerts\_SecOnion2

Lähteet

Sigmund Brandstatetter. Understanding Wazuh: The Free, Open Source Security Platform For XDR & SIEM. Medium-verkkosivun artikkeli. 25.2.2024. Viitattu 7.11.2024. <https://osintph.medium.com/understanding-wazuh-the-free-open-source-security-platform-for-xdr-siem-48b3c3dfba9d>

Zeek Hello World. Zeek opetus sivusto. 2024. Viitattu 7.11.2024. <https://try.zeek.org/#/tryzeek/saved/8603a937b2454fa4bfdc58b579f7f704>

Jadhusan Sadhik. Basic Overview of a Powerful Security Monitoring Platform. Medium artikkeli. 2023. Viitattu 28.11.2024. https://medium.com/@jadhusan24/basic-overview-of-a-powerful-security-monitoring-platform-fd8ce3db445b

Liitteet

Liite 1. Liitteen otsikko

Liite 2. Liitteen otsikko