Labra 4

Ryhmä 13

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Tietoturvakontrollit TTC6010-3007

Palautuspvm

Tieto- ja viestintätekniikka

Sisältö

[1 Johdanto 4](#_Toc179828544)

[2 Teoria 4](#_Toc179828545)

[3 Toteutus 6](#_Toc179828546)

[3.1 Active Directory Integrointi 13](#_Toc179828547)

[3.2 Testaaminen 27](#_Toc179828548)

[4 Pohdinta 33](#_Toc179828549)

[Lähteet 35](#_Toc179828550)

Kuviot

[Kuvio 1. Snapshot alkutilanteesta 6](#_Toc179828551)

[Kuvio 2. Users 7](#_Toc179828552)

[Kuvio 3. Authentication profile 7](#_Toc179828553)

[Kuvio 4. Authentication profile advanced 8](#_Toc179828554)

[Kuvio 5. Authentication portal 8](#_Toc179828555)

[Kuvio 6. Authentication Enforcement 9](#_Toc179828556)

[Kuvio 7. Authentication policy 10](#_Toc179828557)

[Kuvio 8. Turvallisuussääntö WS-NET + ADMIN-NET -> DMZ 10](#_Toc179828558)

[Kuvio 9. Kalin hosts-tiedosto 10](#_Toc179828559)

[Kuvio 10. Captive Portal kirjautuminen 11](#_Toc179828560)

[Kuvio 11. Hello world 11](#_Toc179828561)

[Kuvio 12. Monitor 12](#_Toc179828562)

[Kuvio 13. Rajapinnan asettaminen 13](#_Toc179828563)

[Kuvio 14. Rajapinnan asettaminen 2 14](#_Toc179828564)

[Kuvio 15. Uuden käyttäjän luonti 14](#_Toc179828565)

[Kuvio 16. Uuden käyttäjän luonti 2 15](#_Toc179828566)

[Kuvio 17. Ryhmien lisäys3 16](#_Toc179828567)

[Kuvio 18. UDP-porttien salliminen 17](#_Toc179828568)

[Kuvio 19. Portien salliminen tcp 17](#_Toc179828569)

[Kuvio 20. Allekirjoitettu sertifikaatti 18](#_Toc179828570)

[Kuvio 21. WinRM 1 18](#_Toc179828571)

[Kuvio 22. WinRM 2 19](#_Toc179828572)

[Kuvio 23. Sertifikaatin vienti 19](#_Toc179828573)

[Kuvio 24. Sertifikaatin vienti onnistui 20](#_Toc179828574)

[Kuvio 25. Sertifikaatin tuonti 21](#_Toc179828575)

[Kuvio 26. LDAP-profiili 22](#_Toc179828576)

[Kuvio 27. User-ID agentin asetukset 22](#_Toc179828577)

[Kuvio 28. Monitored server 23](#_Toc179828578)

[Kuvio 29. CIMV2-asetukset 24](#_Toc179828579)

[Kuvio 30. Advanced-välilehti 24](#_Toc179828580)

[Kuvio 31. Yhteys avattu 25](#_Toc179828581)

[Kuvio 32. User Mapping 25](#_Toc179828582)

[Kuvio 33. Virheviesti 26](#_Toc179828583)

[Kuvio 34. Käytön estänyt GPO 26](#_Toc179828584)

[Kuvio 35. group mapping 27](#_Toc179828585)

[Kuvio 36. Boross YouTubessa 27](#_Toc179828586)

[Kuvio 37. Autentikointiprofiili ad\_auth 28](#_Toc179828587)

[Kuvio 38. Autentikointiprofiilin vaihto 28](#_Toc179828588)

[Kuvio 39. Captive Portalin profiilin vaihto 29](#_Toc179828589)

[Kuvio 40. Monitor MaMyyjä 29](#_Toc179828590)

[Kuvio 41. Hyväksyttyjen käyttäjien lisääminen turvallisuuspolitiikkaan 29](#_Toc179828591)

[Kuvio 42. Matti Myyjä verkossa 30](#_Toc179828592)

[Kuvio 43. Käyttäjäryhmän lisääminen turvallisuuspolitiikkaan 31](#_Toc179828593)

[Kuvio 44. Hanna HR verkossa. 31](#_Toc179828594)

[Kuvio 45. Captive portal Kalilla lopussa 32](#_Toc179828595)

[Kuvio 46. Bob Ross verkossa 32](#_Toc179828596)

[Kuvio 47. Boross-käyttäjä monitorissa 33](#_Toc179828597)

# Johdanto

Tietoturvakontrollit labrassa 4 (Paloalto User-ID) parannetaan palomuurin läpi kulkevan liikenteen tunnistamista ja seurantaa. User-ID sääntöjen avulla voidaan tehdä tarkempia, käyttäjäkohtaisia turvallisuussääntöjä, joiden avulla esimerkiksi lokitiedoista nähdään IP osoitteen lisäksi kirjautunut käyttäjätunnus. Seurannan tarkentaminen auttaa ymmärtämään paremmin hallintaympäristöä ja tapahtuneiden ongelmien jäljittämistä. Labra 4:n tavoitteena on siis varmistaa vain tiettyjen käyttäjien pääsyn meidän www-sivuillemme.

Tavoitteena on myös saada PaloAlton ja Windows Active Directoryn välille yhteys, jotta Windows käyttäjä- ja ryhmätiedot saadaan suoraan palomuurin asetuksiin. AD:n ja PaloAlton integrointi on suhteellisen haastava homma, mutta sen seurauksena nykyiset käyttäjätiedot, ja tietojen muutokset saadaan jatkossa päivittymään palomuuriin. Tätä ennen tehdään sääntö PaloAltoon Captive Portalin avulla tunnistautuville käyttäjille, jotta heidän toimintaansa saadaan seurattua, näin voidaan testata käyttäjäkohtaisten politiikoiden toimintaa käytännössä.

# Teoria

Palomuurin liikenteen seurannassa on olennaista saada mahdollisimman paljon tietoa siitä, mitä on tehty, miltä laitteelta ja kuka on tehnyt. Varsinkin, kun tiedetään tekijä, on paljon helpompaa lähteä selvittämään asetuksia tai toimintoja, jotka ovat johtaneet vaikkapa haittaohjelmien tai viruksien pääsyn omaan sisäverkkoon. Näin on helpompaa selvittää, onko hakkerit päässeet käyttäjätietoihin käsiksi. Tarvittaessa voidaan kysyä käyttäjätunnuksen haltijalta, oliko hän kirjautuneena lokitietojen näyttämään aikaan ja esimerkiksi onko hänen omat konfigurointinsa menneet metsään. Edellisessä labrassa tehdyillä estosäännöillä ja varoituksilla, esimerkiksi tarpeettomat nettisivut voitaisiin estää/sallia käyttäjäkohtaisesti tai ryhmäkohtaisesti, jotka muille käyttäjille olisivat vapaasti käytettävissä.

Ennen Active Directoryn integrointia tulee testata käyttäjäkohtaisten sääntöjen toimintaa Palo Alto Local Database Authentication toiminnon avulla. Palomuurin omaan tietokantaan voidaan siis lisätä käyttäjiä tai ryhmiä, joilta vaaditaan tunnistautuminen nettisivuille. Näin käyttäjien toimintaa sivuilla voidaan monitoroida tarkemmin palomuurilla. Paikallisten käyttäjien tunnistamisen saadaan aikaiseksi autentikointi profiilin avulla, joka liitetään Captive Portal kirjautumiseen. Käyttäjä “TestUser” sallitaan myös turvallisuus säännöissä, jotta pääsee sivuille (Admin-net,WS-net -> DMZ) ja kirjautumaan.

Active Directoryn liittäminen Palo Altoon tapahtuu DC:n avulla. Palo Alto tarvitsee yhteyden Active Directoryyn, jotta se voi käyttää käyttäjätietoja ja päivittää niitä. **LDAP** (**Lightweight Directory Access Protocol**) avulla saadaan verkon yli pääsy AD:n tietoihin palomuurilta. Sen avulla PaloAlto pääsee hakemaan käyttäjä- ja ryhmätietoja Active Directorysta, näin käyttäjä- tai ryhmäkohtaisia sääntöjä voidaan asettaa palomuuriin, esimerkiksi rajaten muiden käyttäjien kuin haluttujen pääsyn johonkin sovellukseen tai nettisivuun. Labrassa palomuuri liitetään LDAP palvelimeen (dc01), josta AD tiedot saadaan palomuurille. Windows päässä tulee myös sallia Windows Firewall asetuksista portit, joita esim. LDAP ja WinRM vaativat yhteyden muodostamiseen.

**WinRM** (**Windows Remote Management**) on Microsoft protokolla, jolla voidaan hallita ja valvoa Windows- järjestelmää. Sen avulla saadaan etäyhteys AD:n ja muiden palveluiden etähallintaan, se ei kuitenkaan liity suoraan hakemistopalveluun (AD), vaan nimenomaan turvallisen yhteyden muodostamiseen. **WinRM** tarvitsee sertifikaatit, Windows – Palo Alto välisen yhteyden salaamiseksi. Tässä labrassa **WinRM** käyttää HTTPS:ää, jonka avulla palomuuri ja palvelin saadaan yhdistettyä salatun tunnelin sisällä (SSL). Palomuuri siirtää AD:n tunnistetiedot (käyttäjänimi ja salasana) SSL-tunnelissa. (Configure Server Monitoring Using WinRM. 2024)

**User-ID** on Palo Alto palomuurin ominaisuus, jonka avulla voidaan tunnistaa käyttäjät verkkoympäristössä eri menetelmien avulla. Tämän avulla käyttäjien toimia voidaan seurata verkon eri sijainneissa ja monilla eri käyttöjärjestelmillä. Active Directoryn integroinnissa User-ID kerää ja käyttää AD:n käyttäjätietoja, kuten käyttäjänimiä ja ryhmiä. (User-ID Overview. 2024)

User-ID mahdollistaa käyttäjäkohtaiset politiikat palomuurissa, joilla voidaan rajata tiettyjen käyttäjien pääsyä sovelluksiin tai palveluihin. Se auttaa myös lokituksessa ja forensiikassa, jos on tapahtunut kyberhyökkäys organisaatiota kohtaan tai haittaohjelmia on päätynyt verkon laitteille, saadaan helpommin selville mitä on tapahtunut etsimällä epäilyttäviä toimintoja lokitiedoista. (User-ID Overview. 2024). User-ID vaatii myös erikseen luodun Service-profiilin, jonka avulla voidaan kerätä ja käsitellä käyttäjätietoja, jotka perustuvat tietoturvalokeihin. (Create a dedicated Service Account for the User-ID Agent. 2024)

# Toteutus

Otimme aluksi snapshotin alkutilanteesta, jotta voimme palata toimivaan asetelmaan, mikäli jokin menee vikaan. (Kuvio 1)

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

Kuvaus luotu automaattisesti

Kuvio 1. Snapshot alkutilanteesta

Emme luoneet aluksi uusia käyttäjiä vaan käytimme testaukseen aiemmassa harjoituksessa luotua TestUser tiliä. (Kuvio 2)

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

Kuvaus luotu automaattisesti**

Kuvio 2. Users

Loimme uuden autentikointiprofiilin palomuurin oman käyttäjätietokannan (Local Database) käyttäjien todentamista varten, kuten aiemmin luotu TestUser.

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

Kuvaus luotu automaattisesti

Kuvio 3. Authentication profile

Advanced välilehdellä lisäsimme hyväksyttyihin käyttäjiin all, eli kaikki paikallisen tietokannan käyttäjät sallitaan. (Kuvio 4)

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

Kuvaus luotu automaattisesti

Kuvio 4. Authentication profile advanced

Muokkasimme User Indetification -välilehdeltä autentikointi portaalin asetuksia, jotta paikalliset käyttäjät voivat tunnistautua. (Kuvio 5)

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

Kuvaus luotu automaattisesti

Kuvio 5. Authentication portal

Objects-välilehden authentication osiossa loimme uuden tunnistautumistavan. Tähän valitsimme Authentication profile -kohtaan aiemmin tehdyn Local\_auth -profiilin. Authentication method kohta määrittelee itse tunnistautumistavan, tähän valitsimme web-form eli kirjautumislomake. (Kuvio 6).

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

Kuvaus luotu automaattisesti

Kuvio 6. Authentication Enforcement

Siirryimme Policies-välilehdelle Authentication-osioon. Loimme sinne uuden politiikan nimeltä DMZ suojaus. Kuvion 7 mukaisesti määrittelimme, että tunnistautumista pyydetään tuntemattomilta käyttäjiltä ja heidät ohjataan tunnistautumaan erillisellä lomakkeella (Captive Portal).

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

Kuvaus luotu automaattisesti

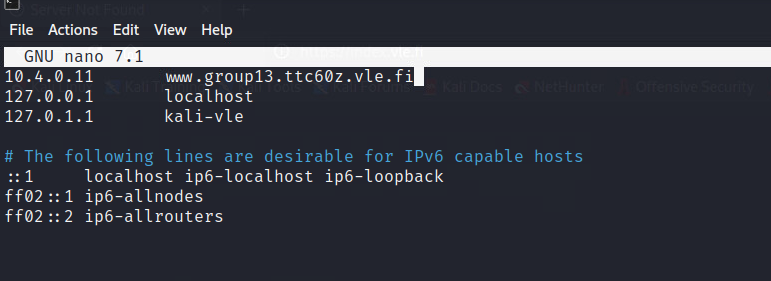
Kuvio 7. Authentication policy

Loimme Policies-välilehdellä Security-osiossa uuden turvallisuussäännön. WS-NETistä ja ADMIN-NETistä DMZ:lle tuleva liikenne sallitaan TestUser käyttäjältä. (Kuvio 8).



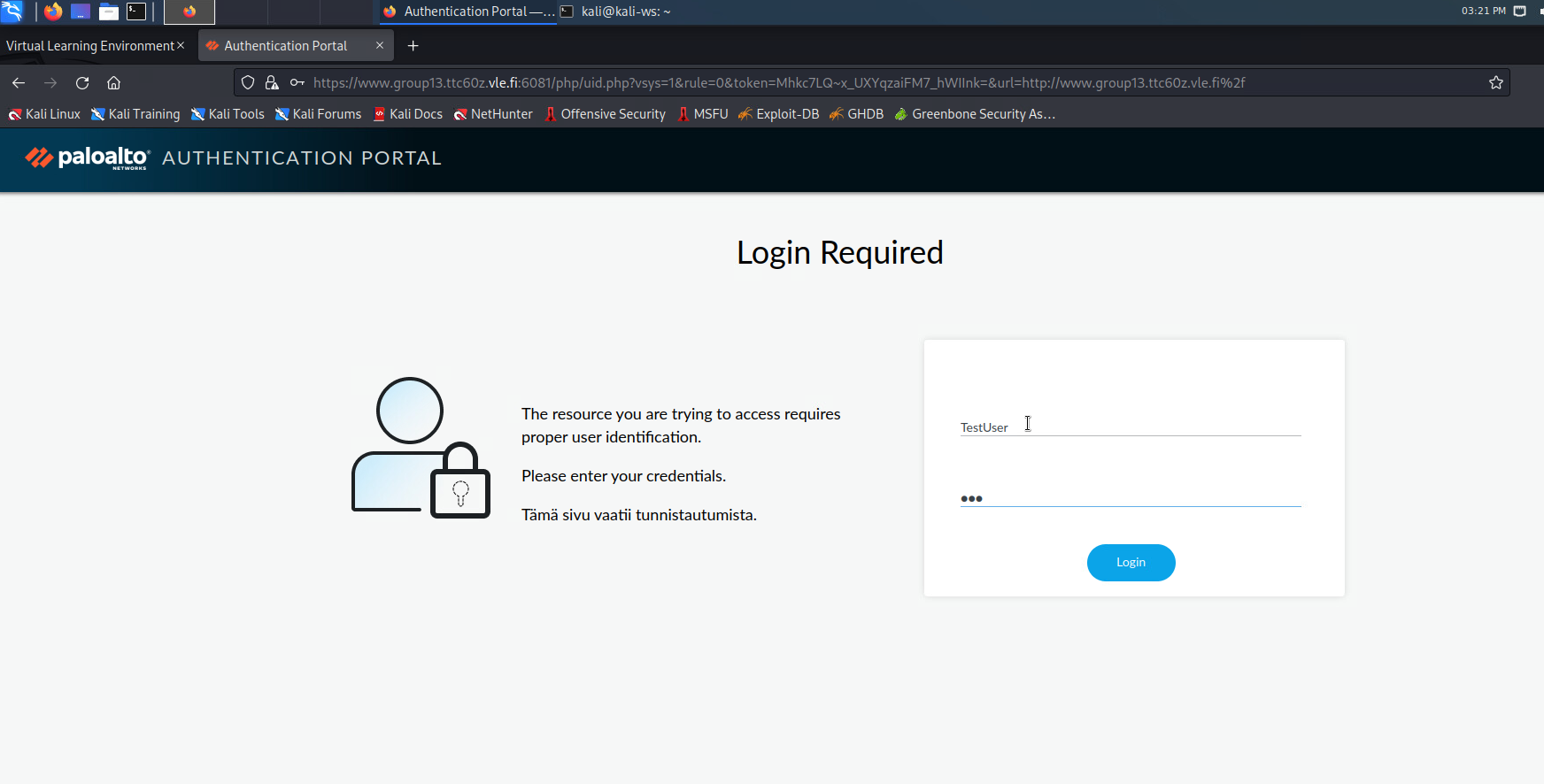
Kuvio 8. Turvallisuussääntö WS-NET + ADMIN-NET -> DMZ

Siirryimme Kali-WS virtuaalikoneelle, joka sijaitsee ADMIN-NET turvallisuusalueella. Ajoimme komennon sudo nano /etc/hosts ja lisäsimme sinne rivin, jossa on www-palvelimen sisäverkon IP:n ja sivun osoitteen (Kuvio 9).



Kuvio 9. Kalin hosts-tiedosto

Kun navigoimme selaimella osoitteeseen [www.group13.ttc60z.vle.fi](http://www.group13.ttc60z.vle.fi), niin sivusto pyytää tunnistautumista (Kuvio 10). Tähän syötimme aiemmin määritellyn käyttäjän ja salasanan, jolla sivulle pitäisi päästä, eli TestUser:n.



Kuvio 10. Captive Portal kirjautuminen

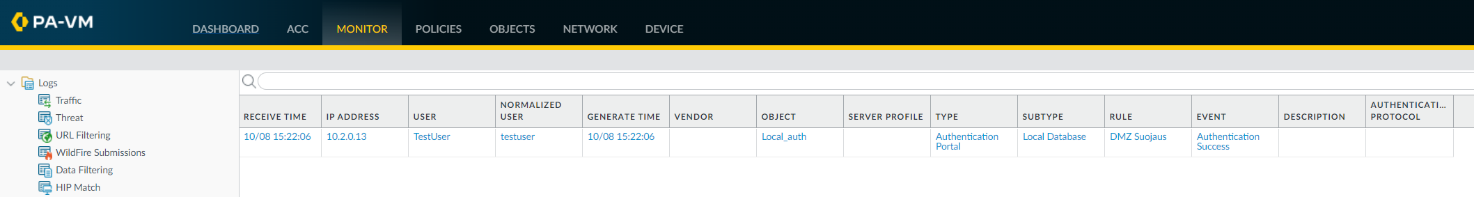
Tunnistautumisen jälkeen pääsimme sivustolle. (Kuvio 11).

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

Kuvaus luotu automaattisesti

Kuvio 11. Hello world

Palo Alton monitorissa näkyi kirjautuminen (Kuvio 12). Monitori näyttää käyttäjän, miten on tunnestauduttu ja mikä autentikointiprofiili on kyseessä (Local\_auth).



Kuvio 12. Monitor

## Active Directory Integrointi

AD:n integroimisiseksi täytyy Palo Alto -palomuurin päässä asettaa rajapinta, josta se saa haettua käyttäjä- ja ryhmätiedot. (Kuvio 13).

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

Kuvaus luotu automaattisesti

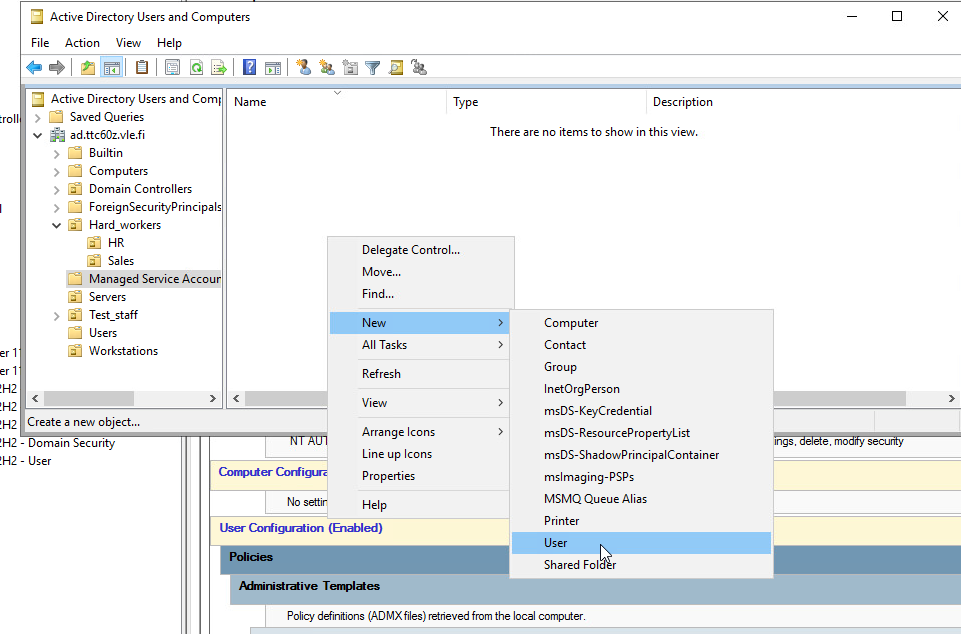
Kuvio 13. Rajapinnan asettaminen

User-ID (UID) agentille asetimme lähdeosoitteeksi dc01, jotta Palo Alto osaa kysellä tietoja sieltä. Tämä tehtiin myös LDAP agentille samoilla arvoilla. (Kuvio 14).



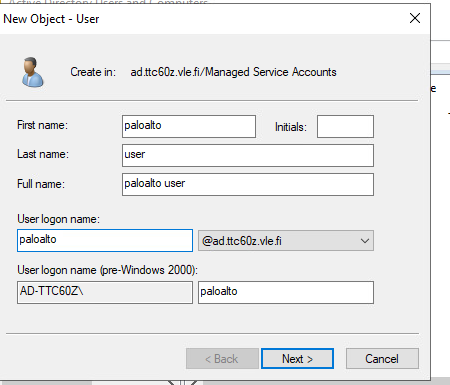
Kuvio 14. Rajapinnan asettaminen 2

Seuraavaksi avasimme DC01 -virtuaalikoneen ja loimme uuden palveluprofiili-käyttäjän, jonka avulla saamme kerättyä lokitietoja DC:ltä ja välitettyä ne sitten Palo Altolle. (Kuvio 15).



Kuvio 15. Uuden käyttäjän luonti

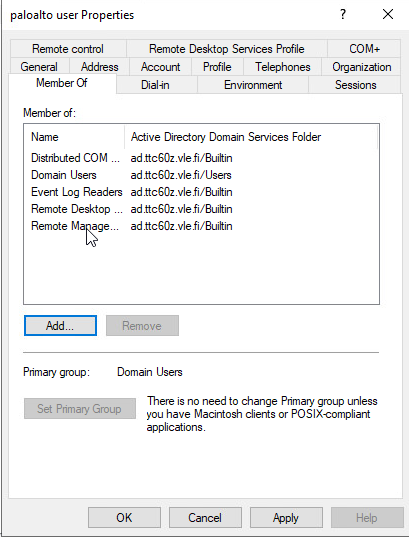
Annoimme käyttäjälle nimeksi paloalto, jotta tiedämme käyttäjän tarkoituksen. (Kuvio 16)



Kuvio 16. Uuden käyttäjän luonti 2

Tällä “paloalto” käyttäjällä tulee olla tarvittavat valtuudet lukea lokitietoja ja saada etäyhteys palvelimeen. Valtuudet tarvitaan, koska tämä käyttäjä tulee olemaan Palo Alto palomuurin “server monitoring” tili, tai User-ID tili, eli käyttäjätili, jonka avulla palomuuri voi hakea tietoa AD:sta. Event Log Readers ja Remote Management Users ovat ryhmät, joihin käyttäjä tulee ainakin liittää, näillä valtuuksilla saadaan näkymään lokitiedot ja ne saadaan haettua etäyhteydellä AD:sta Palo Altoon. Agentin avulla AD:n toimintaa pystytään seuraamaan myös käyttäjän tunnuksen perusteella, ei pelkästään IP-osoitteen avulla.

Lisäsimme käyttäjän kuvion 17 mukaisiin ryhmiin.



Kuvio 17. Ryhmien lisäys3

WinRM (Remote Management) yhteyden saamiseksi tuli meidän täytyi avata useita portteja palomuurin kautta. Tarpeellisten porttien lista löytyi Palo Alton dokumentaatioista. Teimme säännön UDP-porteille. (Kuvio 18).

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

Kuvaus luotu automaattisesti

Kuvio 18. UDP-porttien salliminen

Teimme toisen samanlaisen säännön erikseen TCP-porteille. (Kuvio 19)

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

Kuvaus luotu automaattisesti

Kuvio 19. Portien salliminen tcp

Seuraavaksi loimme sertifikaatin, jotta yhteys saadaan salattua AD:n ja palomuurin välillä. Ajoimme kuvion 20 mukaisen komennon PowerShellillä ja kopioimme saadun Thumbprintin.

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

Kuvaus luotu automaattisesti

Kuvio 20. Allekirjoitettu sertifikaatti

Loimme uuden Windows Remote Management (WinRM) kuuntelija, joka käyttää HTTPS-protokollaa tiedonsiirtoon. Käytimme aiemmin luotua sertifikaattia asettamalla CertificateThumbprint kohtaan tallentamamme Thumbprintin. (Kuvio 21).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 21. WinRM 1

Muokkasimme vielä WinRM konfiguraatioita niin että hyödynnämme Basic Authenticationia kuvion 22 mukaisesti.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 22. WinRM 2

Otimme luodun sertifikaatin ulos MMC:n kautta ja viemme sen Palo Altoon. (Kuvio 23).

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

Kuvaus luotu automaattisesti

Kuvio 23. Sertifikaatin vienti

File Format kohtaan vaihdoimme kuvion 26 mukaisesti Base64 Encoded X.509 (\*.cer), eli tiedostomuodoksi tulee .cer. (Kuvio 24).

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

Kuvaus luotu automaattisesti

Kuvio 24. Sertifikaatin vienti onnistui

Seuraavaksi lisäsimme sertifikaatin Palo Altoon Device-välilehden Certificate Management -osiosta. (Kuvio 25).

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

Kuvaus luotu automaattisesti

Kuvio 25. Sertifikaatin tuonti

Loimme LDAP palvelinprofiili ja asetimme sen käyttämään AD:lla luotuoa palveluprofiilia paloalto. LDAP- protokolla hakee tämän käyttäjän avulla tiedot Active Directorysta. Profiili vaati myös LDAP palvelimen IP- osoitteen ja portin, jonka kautta kommunikoida sen kanssa. (Kuvio 26)

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

Kuvaus luotu automaattisesti

Kuvio 26. LDAP-profiili

Seuraavaksi siirryimme Device-välilehde User Identification osioon, jossa painoimme mutteria Palo Alto Networks User-ID Agent Setup laatikon yläkulmasta. Asetimme tähän aiemmin luomamme paloalto-palveluprofiilin tunnisteet. (Kuvio 27).

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

Kuvaus luotu automaattisesti

Kuvio 27. User-ID agentin asetukset

User Identification Monitored Server asetuksilla saadaan Palo Alto yhdistettyä AD palvelimeen WinRM-HTTPS kuljetusprotokollan avulla. Palvelimen tyyppi saadaan valittua Palo Alto palomuurin hyväksytyistä tiedostopalveluista. Valitsimme valikosta Microsoft Active Directoryn, koska käytämme sitä. (Kuvio 28).

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

Kuvaus luotu automaattisesti

Kuvio 28. Monitored server

Törmäsimme ongelmaan, jossa user agent ei suostunut yhdistämään, jos DC01:n palomuuri oli päällä tai paloalto käyttäjällä. Vaihdoimme käyttäjän administraattoriin ja palomuurin pois päältä ja tällöin Palo Alto sai yhteyden DC01:n. Ongelma johtui WMI kontrollien oikeuksista, käyttäjä paloaltolle piti lisätä ROOT\CIMV2 oikeuksia. (Kuvio 29).

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

Kuvaus luotu automaattisesti

Kuvio 29. CIMV2-asetukset

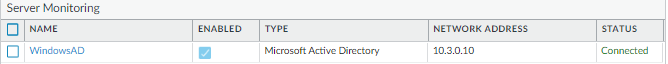
Varmistimme vielä Advanced-välilehdeltä, että Applies to- kohdassa on valittuna this namespace and subnamespaces. (Kuvio 30).

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

Kuvaus luotu automaattisesti

Kuvio 30. Advanced-välilehti

Nyt saimme yhteyden käyttäen paloalto käyttäjää ja ilman palomuuria. (Kuvio 33).



Kuvio 31. Yhteys avattu

Kun asetimme palomuurin päälle niin yhteys katkesi. Lisäsimme HTTPS-portin 5986 sallittaviin TCP-yhteyksiin. Tämä ratkaisi ongelman ja yhteys pysyi päällä, vaikka laitoimme DC01:n palomuurin takaisin päälle.

Seuraavaksi loimme säännön User-Id:lle Device-välilehdellä User Identification -osiossa Group Mapping Settings kohdassa. (Kuvio 32).

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

Kuvaus luotu automaattisesti

Kuvio 32. User Mapping

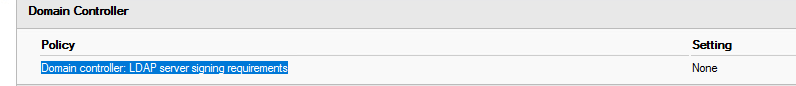
Kun yritimme lisätä käyttäjäryhmiä huomioitaviin käyttäjäryhmiin, saimme virheviestin tarvittavasta vahvemmasta tunnistautumisesta. (Kuvio 33).

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

Kuvaus luotu automaattisesti

Kuvio 33. Virheviesti

Käyttäjäryhmiä ei jostain syystä pystynyt lisäämään. Huomasimme, että ongelma johtui GPO-säännöstä ”LDAP server signing requirements”. Vaihdoimme tähän none. (Kuvio 34).



Kuvio 34. Käytön estänyt GPO

Nyt pystyimme lisäämään käyttäjäryhmiä ja lisäsimme aluksi users, administrators ja sales -ryhmät. (Kuvio 35).

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

Kuvaus luotu automaattisesti

Kuvio 35. group mapping

## Testaaminen

Kirjauduimme WS01-virtuaalikoneelle boross-käyttäjällä, joka kuuluu sales-ryhmään, ja avasimme selaimella YouTuben. Palo Alton monitorissa näkyi boross-käyttäjän käynti YouTubessa. (Kuvio 36)

Kuva, joka sisältää kohteen teksti, kuvakaappaus

Kuvaus luotu automaattisesti

Kuvio 36. Boross YouTubessa

Jotta saamme autentikointiportaaliin tunnistautumisen onnistumaan ad tunnuksilla, loimme uuden authentication profiiliin. (Kuvio 37)

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

Kuvaus luotu automaattisesti

Kuvio 37. Autentikointiprofiili ad\_auth

Seuraavaksi vaihdoimme Devices-välilehdeltä User Identification -osiosta Authentication Portal settings -kohdasta käytettäväksi profiiliksi luomamme ad\_auth. (Kuvio 38)

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 38. Autentikointiprofiilin vaihto

Vaihdoimme myös aiemmin tekemäämme R13\_Captive\_portal:iin autentikointiprofiiliksi ad\_auth:n. (Kuvio 39)

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

Kuvaus luotu automaattisesti

Kuvio 39. Captive Portalin profiilin vaihto

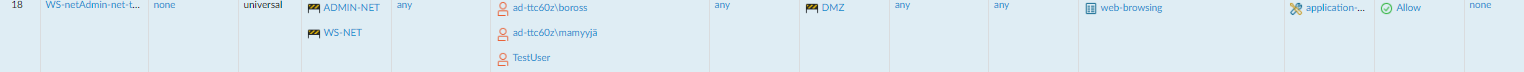
Seuraavkais kokeilimme mennä sales-ryhmään kuuluvalla MaMyyjä-käyttäjällä [www.group13.ttc60z.vle.fi](http://www.group13.ttc60z.vle.fi) -sivullemme. Monitorissa näkyi action kohdassa deny, eli pääsy estettiin. (Kuvio 40).

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

Kuvaus luotu automaattisesti

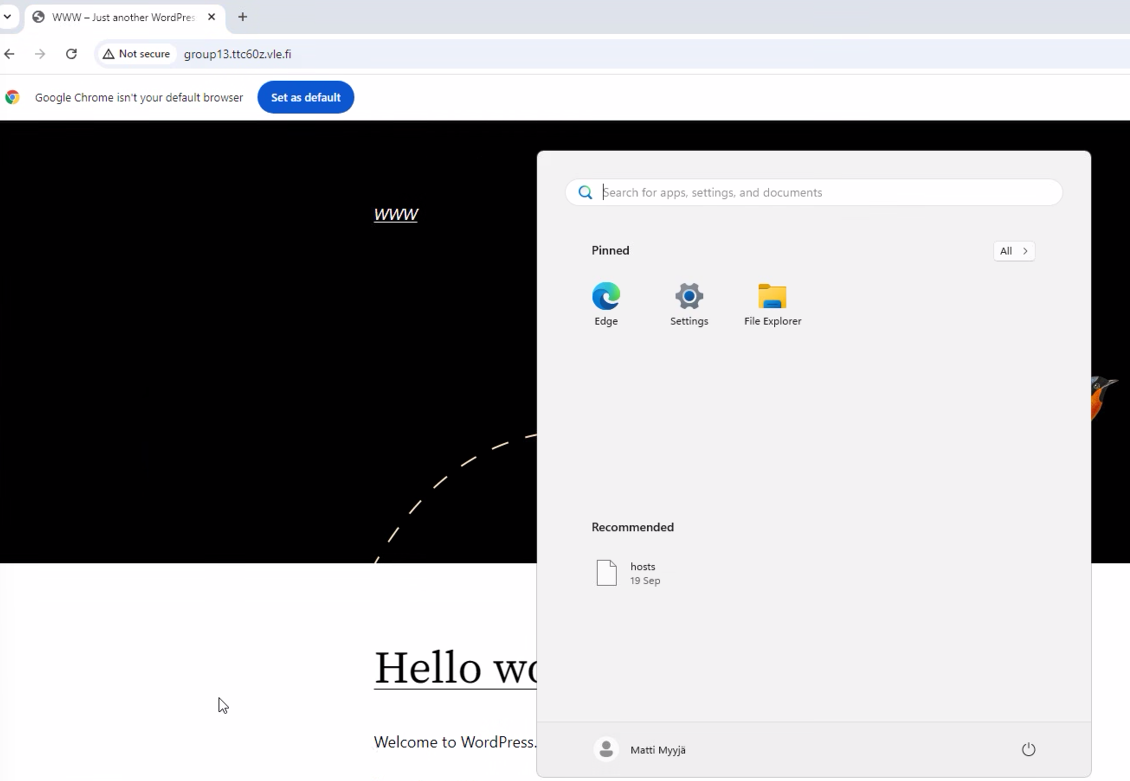
Kuvio 40. Monitor MaMyyjä

Lisäsimme käyttäjän MaMyyjä turvallisuuspolitiikkaan, jonka loimme harjoituksen alussa. (Kuvio 41).



Kuvio 41. Hyväksyttyjen käyttäjien lisääminen turvallisuuspolitiikkaan

Tämän jälkeen MaMyyjäkin pääsi sivullemme. (Kuvio 42).



Kuvio 42. Matti Myyjä verkossa

Testasimme vielä AD-ryhmän perusteella. Kokeilimme Hanna Hr -käyttäjää, joka kuuluu HR-ryhmään. Lisäsimme tämän ryhmän turvallisuuspolitiikkaan. (Kuvio 43).

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

Kuvaus luotu automaattisesti

Kuvio 43. Käyttäjäryhmän lisääminen turvallisuuspolitiikkaan

Nyt pääsi myös Hanna Hr sivuille. (Kuvio 44)

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

Kuvaus luotu automaattisesti

Kuvio 44. Hanna HR verkossa.

Testasimme vielä Captive Portalin toiminnan boross -käyttäjällä Kalilla. (Kuvio 45).

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

Kuvaus luotu automaattisesti

Kuvio 45. Captive portal Kalilla lopussa

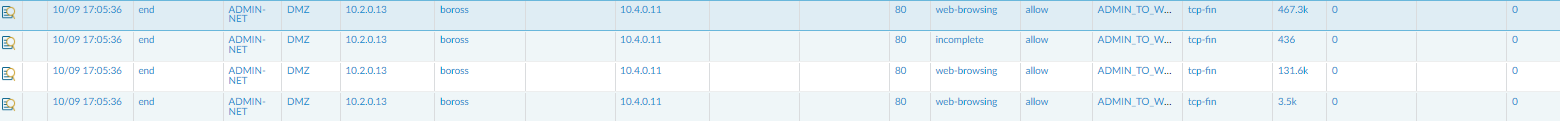
Ja tunnistus onnistui hyvin. (Kuvio 46)

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

Kuvaus luotu automaattisesti

Kuvio 46. Bob Ross verkossa

Varmistimme asian vielä monitorista. Lähteenä näkyy 10.2.0.13 eli Kali ja käyttäjänä boross. (Kuvio 47)



Kuvio 47. Boross-käyttäjä monitorissa

# Pohdinta

Harjoitustyössä pääsimme tutustumaan vielä syvällisemmin paloalton asetuksiin ja mahdollisuuksiin. Loimme tunnistautumisportaalin ja konfiguroimme Active Directory -integraation, jonka avulla pystymme rajoittamaan käyttäjien ja käyttäjäryhmien pääsyä ja tunnistautumista haluamiimme kohteisiin.

Ongelmilta ei vältytty tässäkään ja jouduimme syventymään ad:n ja paloalton toimintaan vielä enemmän ongelmien ratkomiseksi. Ensimmäinen ongelma tuli vastaan, kun koitimme yhdistää domain controllerille käyttäen paloalto käyttäjää, yhteys onnistui kuitenkin administraattorina, ja kun palomuurit olivat pois päältä eli ongelmaa löytyi sekä käyttäjästä, että palomuuri asetuksista. Ongelma johtui käyttäjän WMI (Windows Management Instrumentation) oikeuksien puutteesta. Lisäsimme siis oikeuksia nimialueeseen Root\CIMV2, joiden avulla käyttäjä voi suorittaa tarvittavia WMI-kyselyjä. Palomuurin kanssa olevan ongelman saimme ratkaistua lisäämällä palomuurin asetuksista TCP-portteihin HTTPS-portin 5986.

Harjoitusta tehdessä myös muut ryhmät olivat törmänneet samankaltaisiin ongelmiin. Ryhmämme oli kerennyt jo ratkaista ongelmat, joten pääsimme auttamaan muita ryhmiä. Tämä oli ryhmällemme hyvää kertausta labran aiheista. Pääsimme myös tutustumaan ongelmiin, mitä meillä itsellämme ei ollut.

Kaiken kaikkiaan harjoitus oli opettavainen ja mielenkiintoinen. Harjoituksen sai suurimmaksi osaksi tehtyä ohjeiden avulla, mutta käytimme työssä myös laajasti paloalton omia ohjeistuksia ja dokumentaatioita, varsinkin ongelman ratkaisussa.

Lähteet

Configure Server Monitoring Using WinRM. Palo Alto ohje. 2024. Viitattu 10.10.2024. <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/configure-server-monitoring-using-winrm>

User-ID Overview. Palo Alto dokumentti. 2024. Viitattu 8.10.2024. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-overview>

Create a dedicated Service Account for the User-ID Agent. Palo Alto dokumentti. 2024. Viitattu 10.10.2024. <https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/user-id/map-ip-addresses-to-users/create-a-dedicated-service-account-for-the-user-id-agent>