Koventaminen – Labra 2

Ryhmä 3

Juha-Matti Hietala

Markus Pollari

Topi Liljeqvist

Maija Virta

Oppimistehtävä

Helmikuu 2023

Tekniikan ala

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

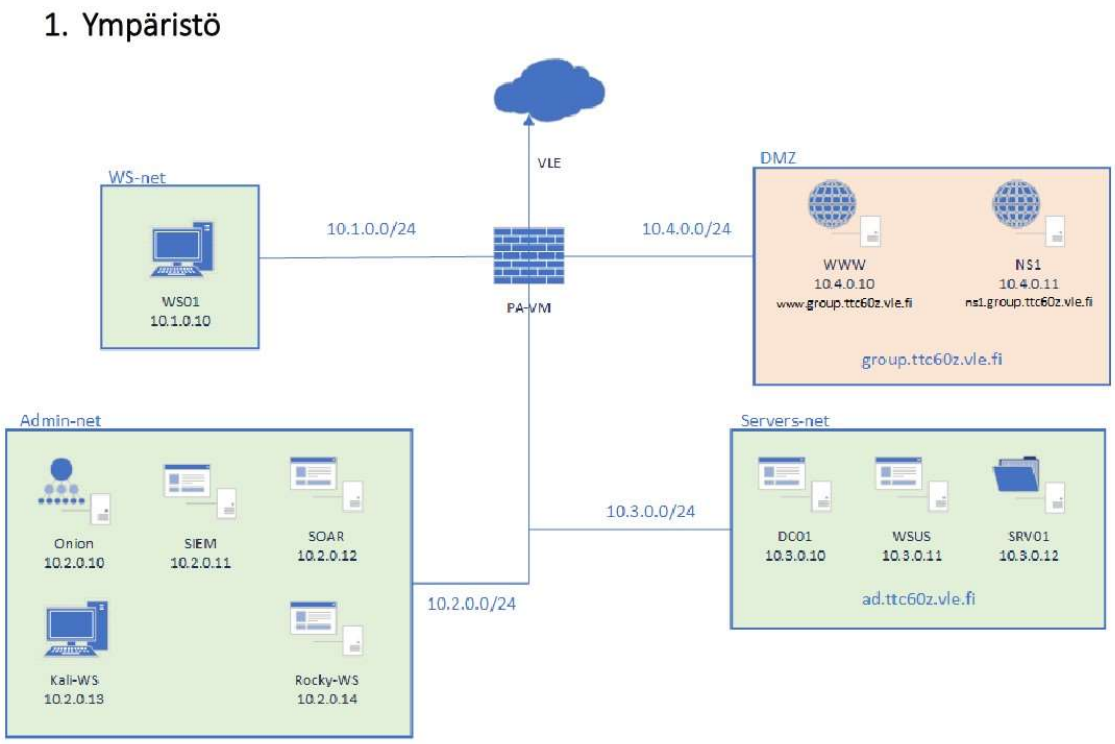
Kuvat

1 Johdanto

Dokumentaatio on osana koventamisen kurssin (TTC6050-3002) laboratorioharjoituksia. Toisen LAB2 harjoituksen tavoitteena on Windows 11 koventaminen. Ryhmä tekee GPO (Group Policy Object) kovennukset käyttäen Microsoftin Security Compliance Toolkit:iä joka sisältää baselinen Windows 11 sekä lisäksi muutaman esimerkin kovennuksen tekemisestä manuaalisesti.

Windows 11 kovennuksien analysointiin käytetään Microsoft Policy Analyzeria. Kovennukset dokumentoidaan kuvankaappauksilla sekä havainnollistetaan, miten kovennus tehdään. Analyzer ajetaan harjoitusta aloittaessa sekä lopuksi tehtyjen kovennuksien jälkeen, jotta voidaan vertailla lähtö- ja lopputilannetta.

Teorialla ja koventamisen harjoituksilla ryhmän jäsenet saavat taidot ja ymmärryksen Windows 11 koventamisesta. Lisäksi dokumentoinnissa käydään läpi teoriaa X sekä Microsoft Policy Analyzerista. Harjoitus toteutetaan kurssin VLE ympäristössä oleville DC01 (IP 10.3.0.10) ja WS01 (IP 10.1.0.10). Ympäristö esitettynä alla.



Kuva 1 Laboratorio ympäristö

2 Teoria

2.1 Microsoft Security Compliance Toolkit (SCT)

Microsoft Security Compliance Toolkit (SCT) on kokoelma työkaluja ja resursseja, jotka on suunniteltu auttamaan organisaatioita määrittämään ja arvioimaan Microsoft Windows -pohjaisten järjestelmiensä turvallisuutta. SCT sisältää joukon suojauksen perusasetuksia, jotka ovat ennalta määritettyjä ryhmäkäytäntöasetuksia, joita organisaatiot voivat soveltaa järjestelmiinsä parantaakseen turvallisuuttansa. (Nemnom 2022)

Työkalupakkaus sisältää myös työkaluja tietoturvan perusperiaatteiden noudattamisen arvioimiseen sekä työkaluja Windows-pohjaisten järjestelmien suojauskokoonpanon hallintaan ja ylläpitoon. (Nemnom 2022)

Microsoft Security Compliance Toolkit on ensisijaisesti tarkoitettu IT-ammattilaisille ja tietoturvajärjestelmänvalvojille, jotka ovat vastuussa Windows-pohjaisten järjestelmien hallinnasta ja suojaamisesta organisaatioissaan. Se on suunniteltu auttamaan näitä ammattilaisia pysymään ajan tasalla uusimpien turvallisuuden parhaiden käytäntöjen kanssa ja varmistamaan, että heidän järjestelmänsä on määritetty turvallisesti ja alan ja säädösten standardien mukaisesti. (Nemnom 2022)

2.2 Microsoft Policy Analizer

Microsoft Policy Analyzer on yksi Microsoft Sercurity Compliance Toolkitiin sisältyvistä työkaluista. Se on apuväline ryhmäkäytäntöobjekteista (GPO) koostuvien joukkojen vertailuun ja analysointiin, eli se mahdollistaa GPO:iden tuomisen eri lähteistä ja niiden vertailun. Microsoft Policy Analyzerilla voi esimerkiksi verrata nykyisiä GPO-asetuksia Microsoftin suosittelemiin asetuksiin tai vanhempaan varmuuskopioon nähdäkseen, mikä on muuttunut. (Loos 2018)

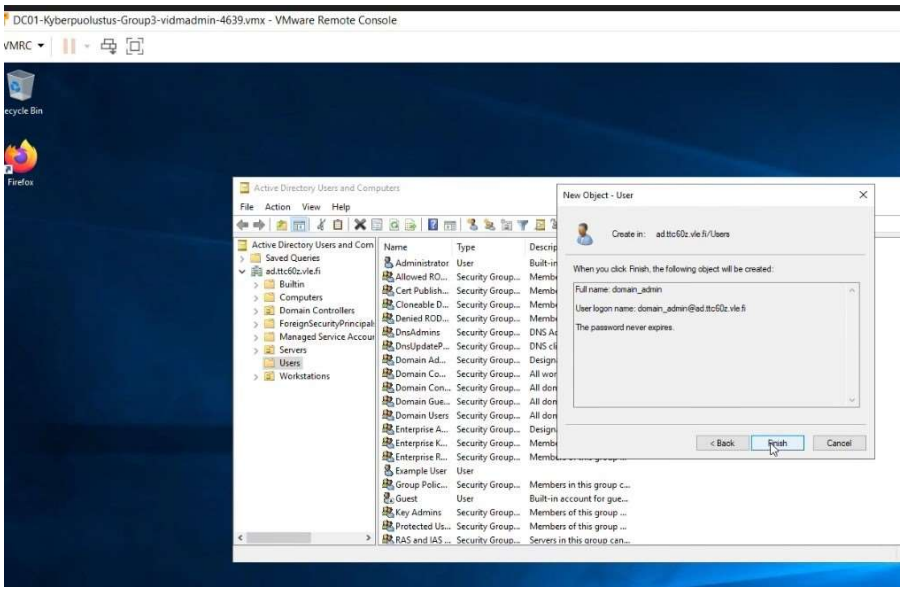
Microsoft Policy Analyzer käsittelee GPO-joukkoa yhtenä yksikkönä, jolloin se pystyy helposti määrittelemään, löytyykö GPO-joukosta ristiriitaisia tai toistuvia asetuksia. Löydökset on mahdollista myös tuoda Microsoft Exceliin. (Margosis 2019)

3 WINDOWS 11 TYÖASEMAN KOVENTAMINEN

3.1 Microsoft Security Compliance Toolkit

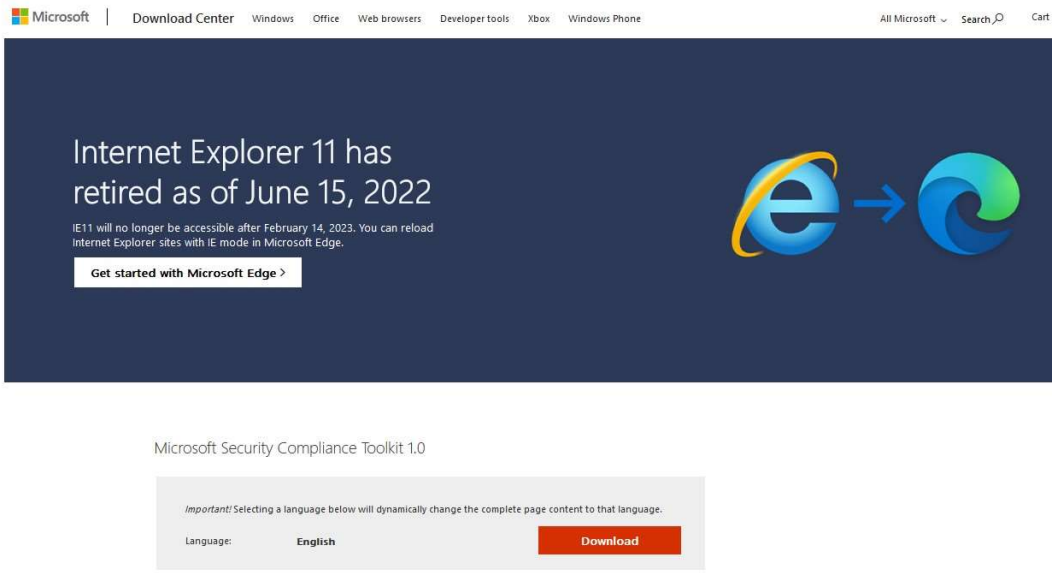
3.1.1 DC01

Harjoitustehtävä lab2 aloitettiin kirjautumalla DC01 (IP 10.3.0.10) ja luomalla uuden domain admin käyttäjän. Käyttäjän avulla pystytään tarkistamaan myöhemmin, että säädetyt säännöt DC01:llä ovat tulleet voimaan. Esitetty kuvassa alla.



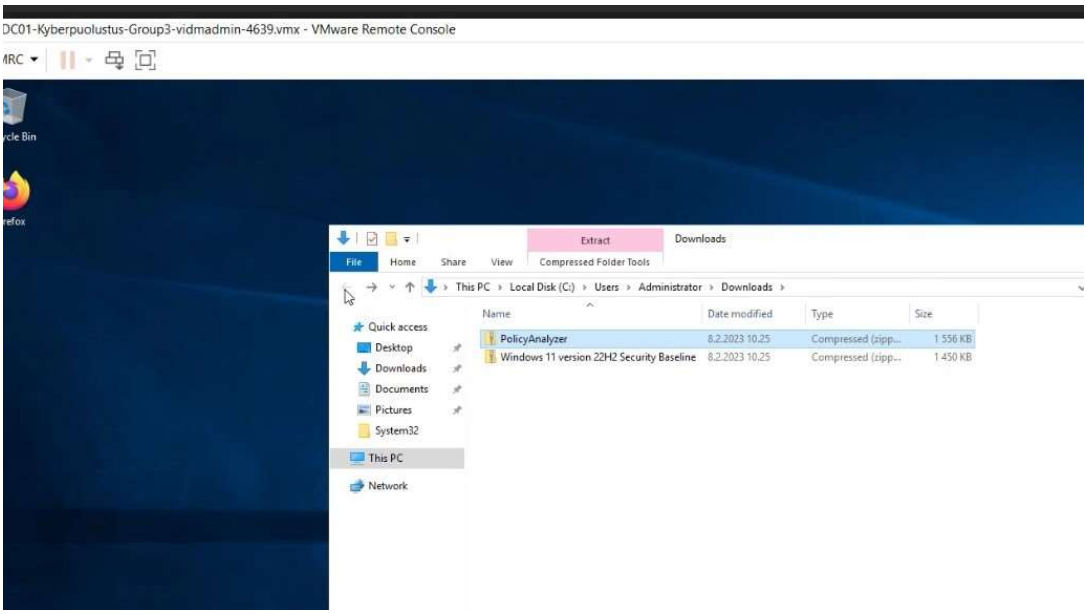
Kuva 2 domain_admin (Root-66) käyttäjän luonti

Seuraavaksi ladattiin Microsoftin verkkosivuilta Microsoft Security Compliance Toolkit 1.0, esitetty kuvassa 3.



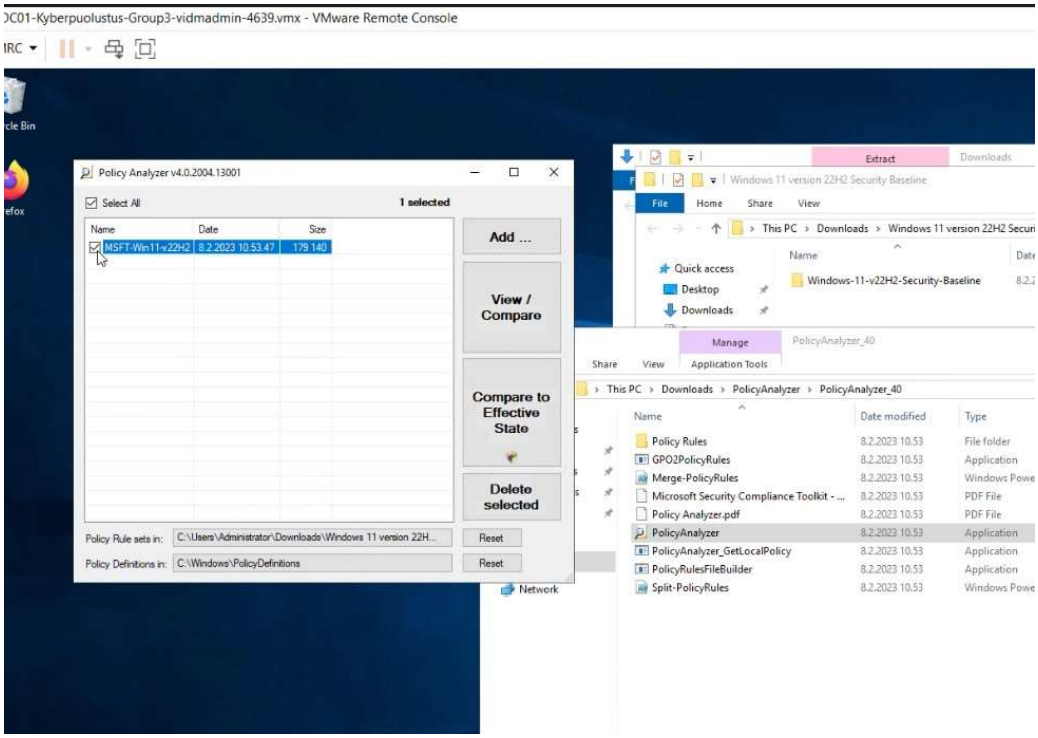
Kuva 3 Microsoft download Center

Ladattujen .zip tiedostojen purkaminen ja sen jälkeen Policy Analyerin avaaminen, esitetty alla.



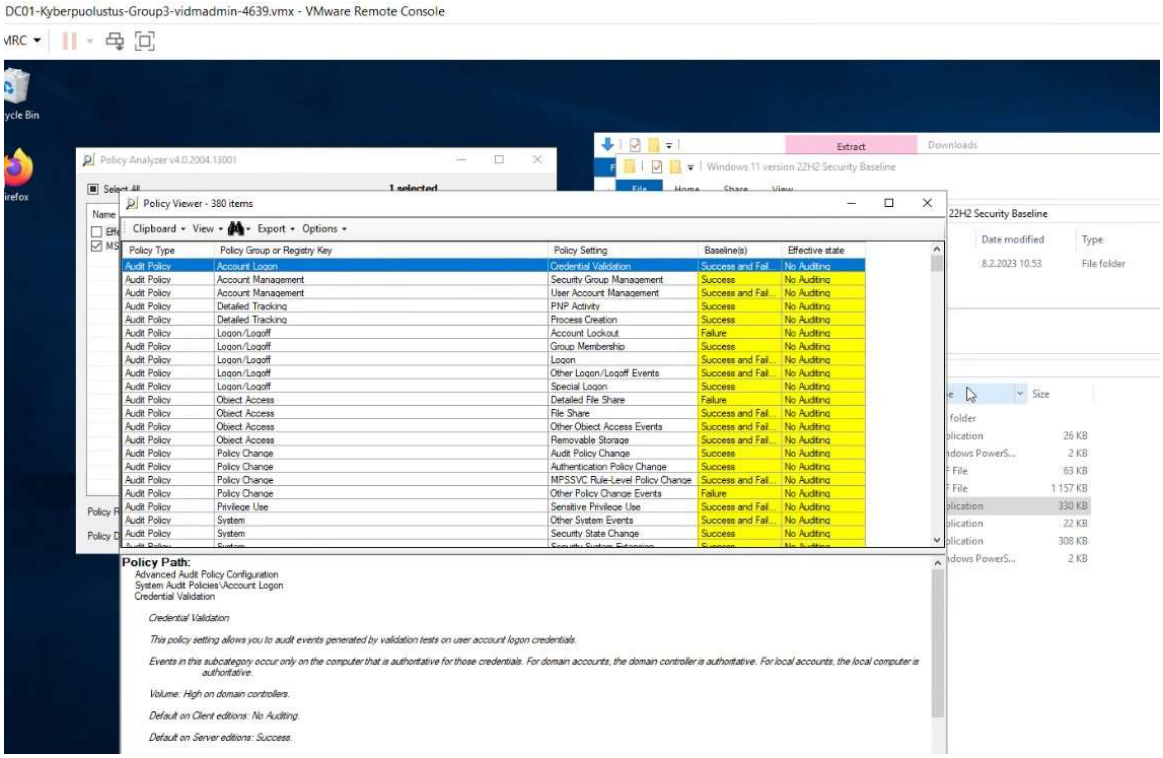
Kuva 4 Ladattujen tiedostojen purku

Seuraavaksi ladattiin Policy Analyzer ja Windows 11 22H2 Security Baseline listaus, testattiin ennen kovennuksia. Esitetty kuvassa alla.



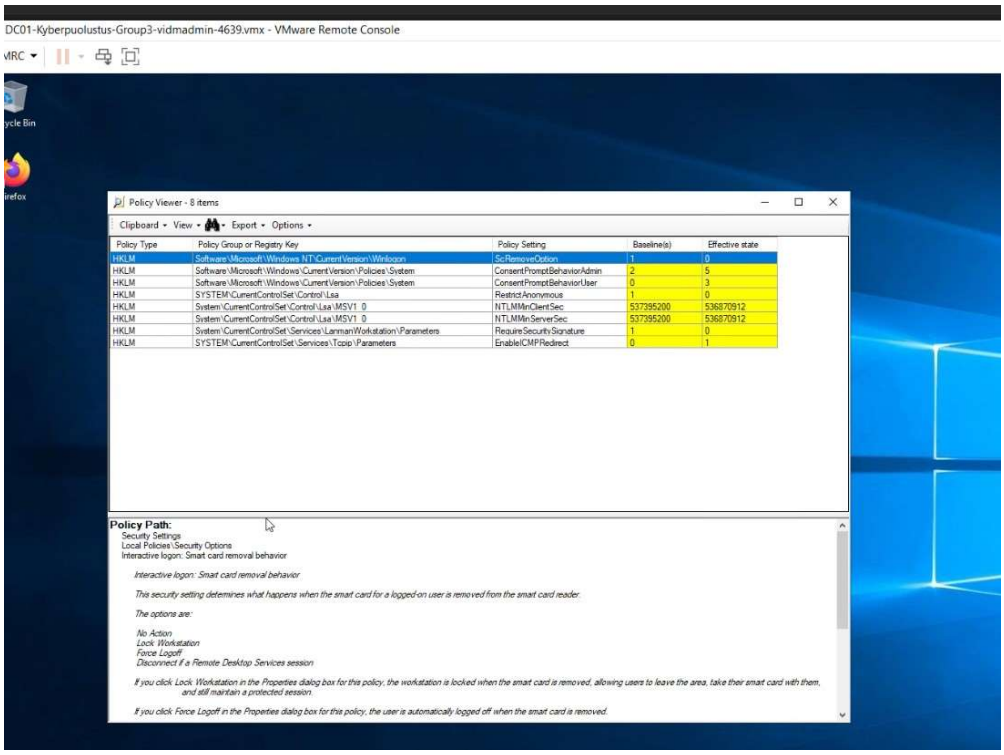
Kuva 5 Windows 11 baseline

Valittiin ladattu Windows 11 baseline ja ”Compare to Effective State”. Esitetty kuvassa 6.



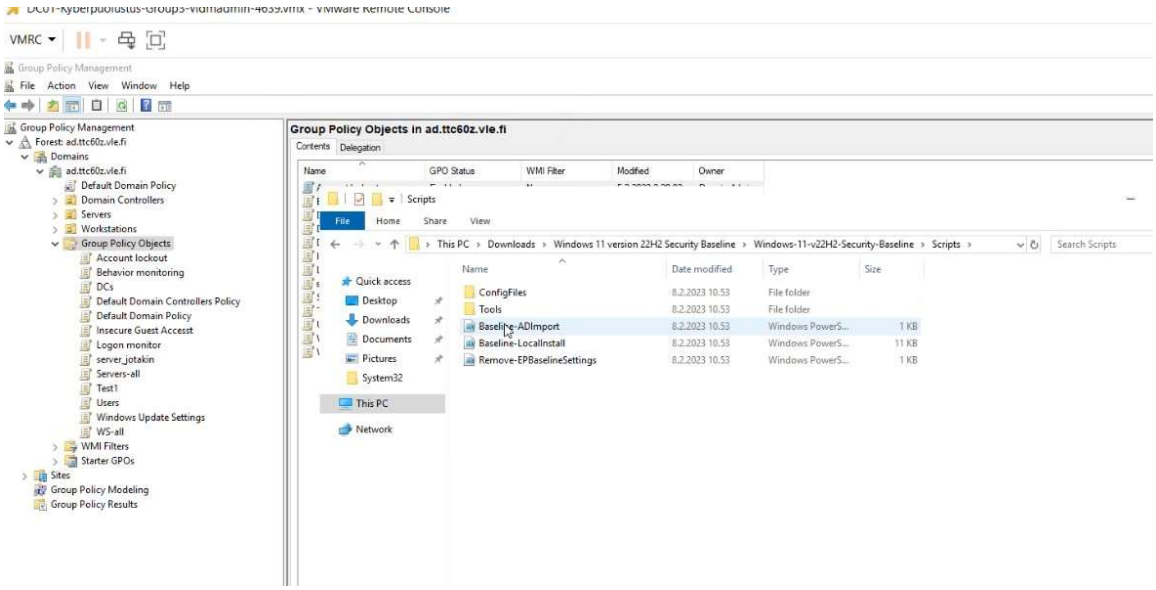
Kuva 6 Policy viewer lähtötilanteessa

Kopioitiin alkutilanne talteen valitsemmalla Show only conflicts – Clipboard – Select all – Copy.

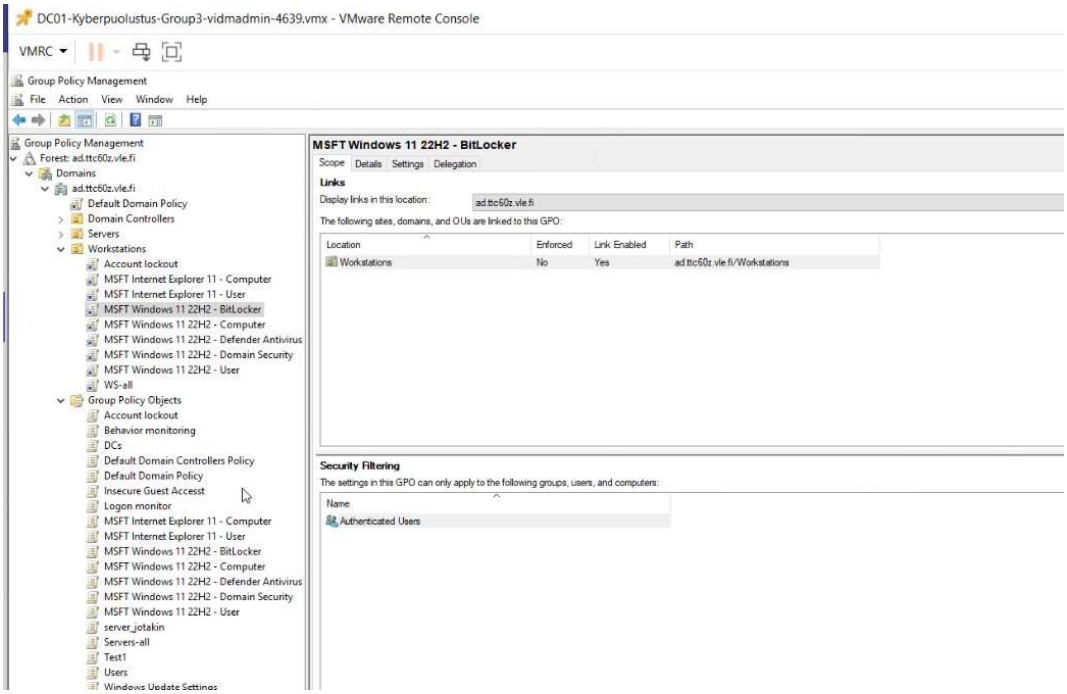


Kuva 7 Show only conflicts DC01

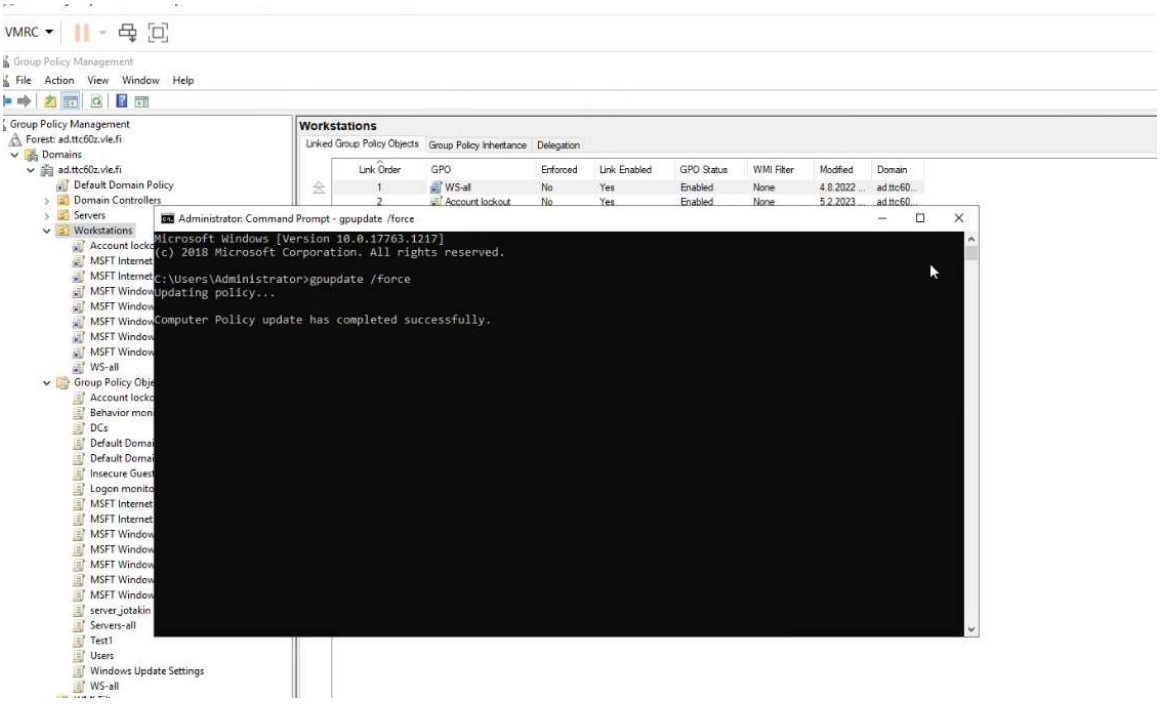
Ladattiin Windows 11 22H2 Security Baseline kovennukset ”Baseline ADI-import – GPO:lle sekä Workstationille. Esitetty seuraavissa kuvissa 8-9.



Kuva 8 Windows 11 version 22H2 Security Baseline – Skripts



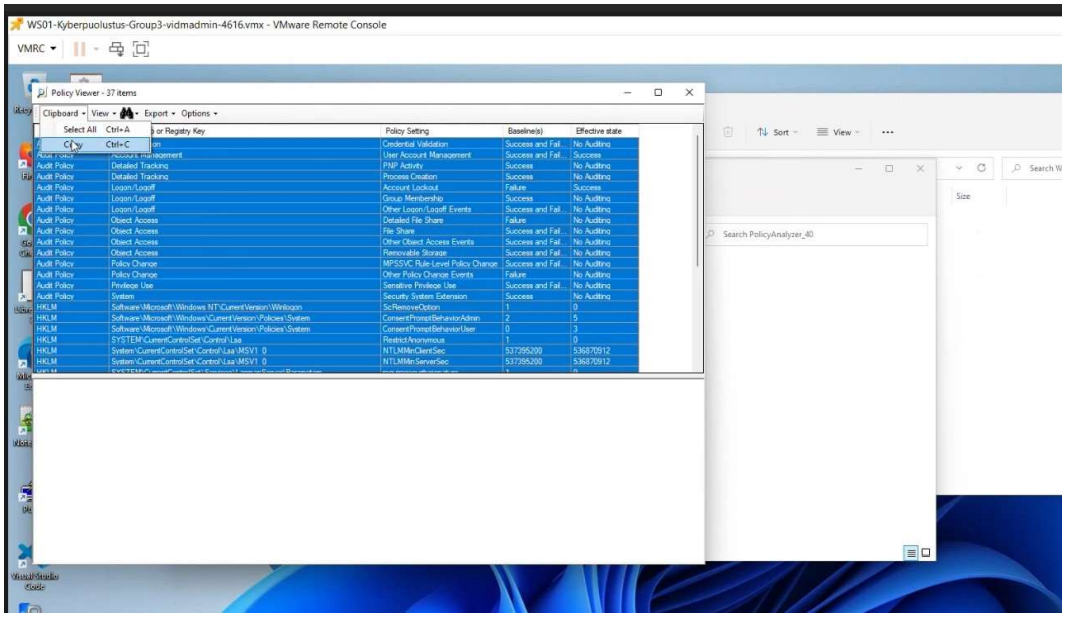
Kuva 9 Workstations kovennukset



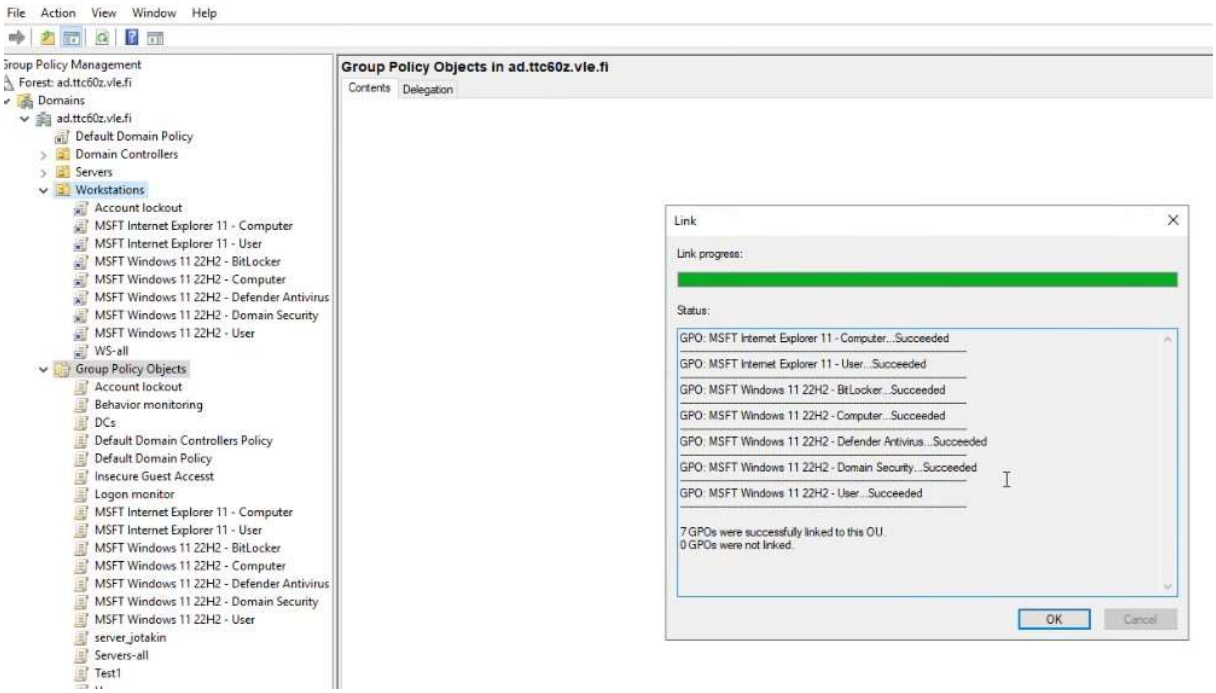
Kuva 10 Powershellin avulla kovennukset pakotetaan Windows 11:lle

3.1.2 WS01

WS-NET:tiin WS01 Koneeseen sama Microsoft Security Compliance Toolkit 1.0 lataaminen ja Policy Analyzer Windows 11 22H2 Security Baseline.

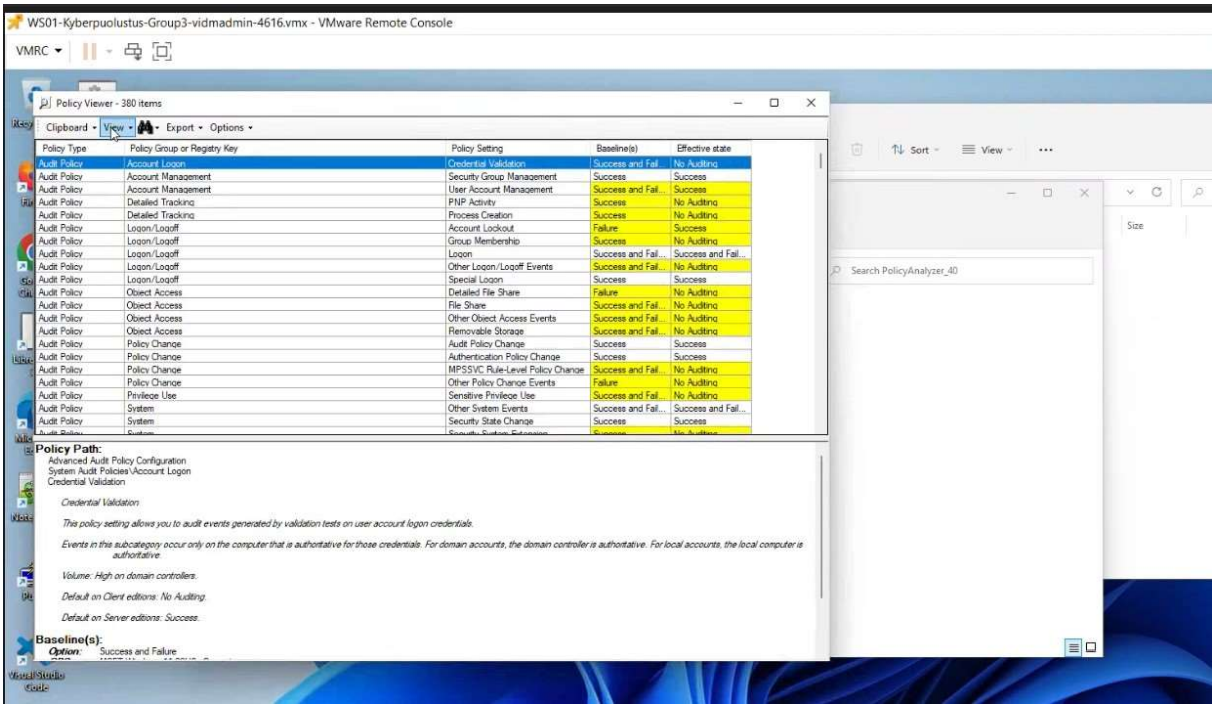


Kuva 11 WS01 Alkutilanteen tallentaminen

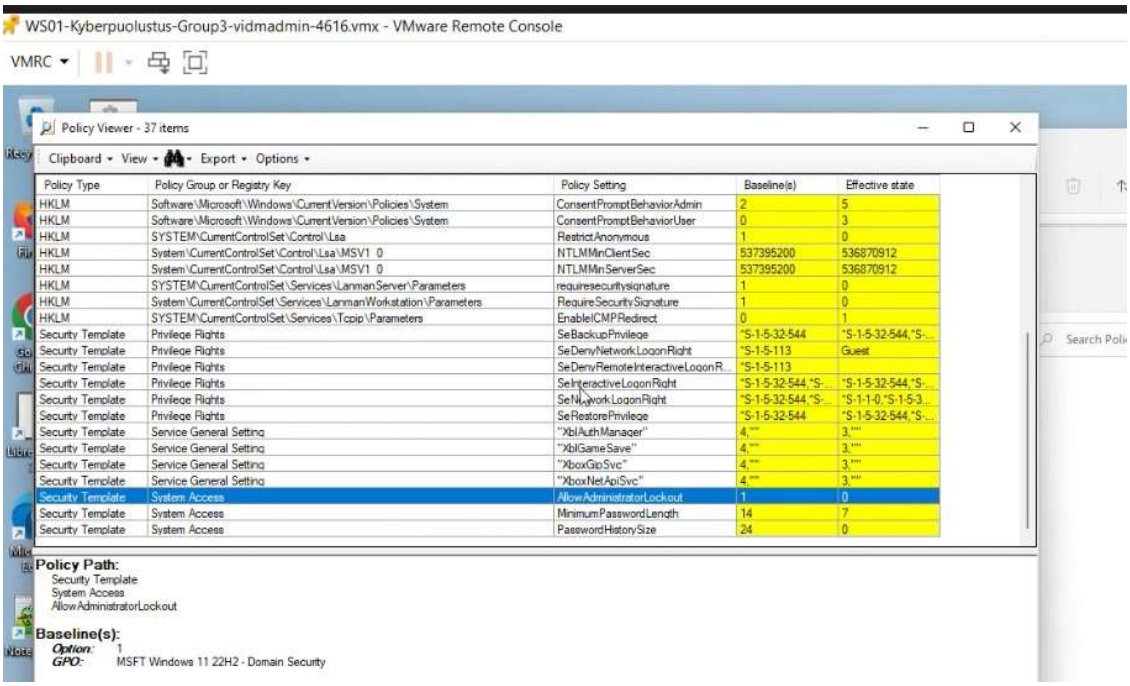


Kuva 12 WS01 Kovennukset

Tarkastettiin vielä, että ajetut kovennukset näkyvät effective statessa. Esitetty kuvissa alla.

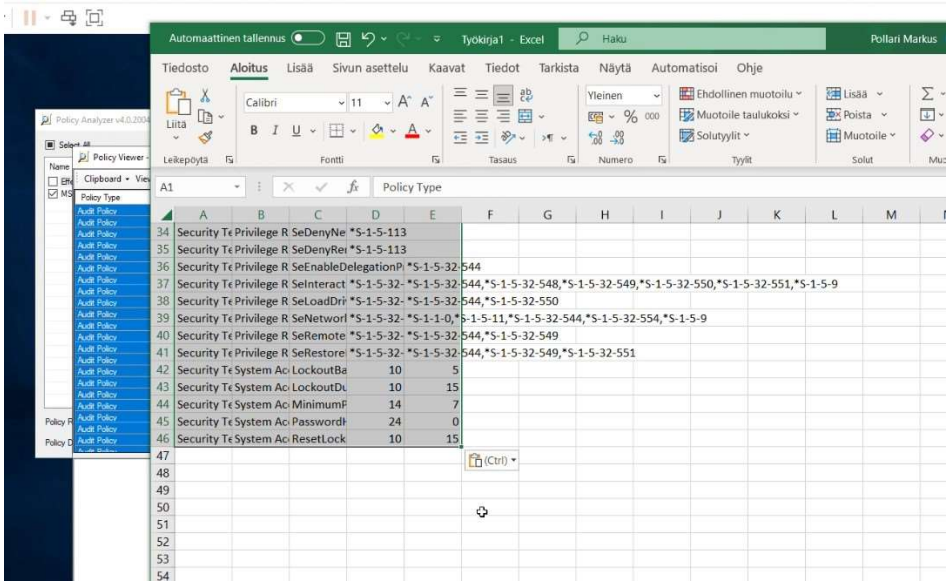


Kuva 13 Policy Viewer - WS01



Kuva 14 Policy Viewer loppuosa - WS01

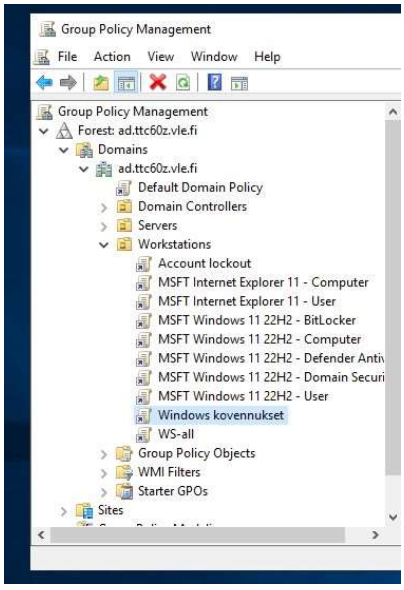
Kopio talteen: Show only conflicts- Clipboard -> Select all -> copy ja kopioitiin omalle koneelle. Esitetty tallennustapa alla.



Kuva 15 Excel kopio talteen

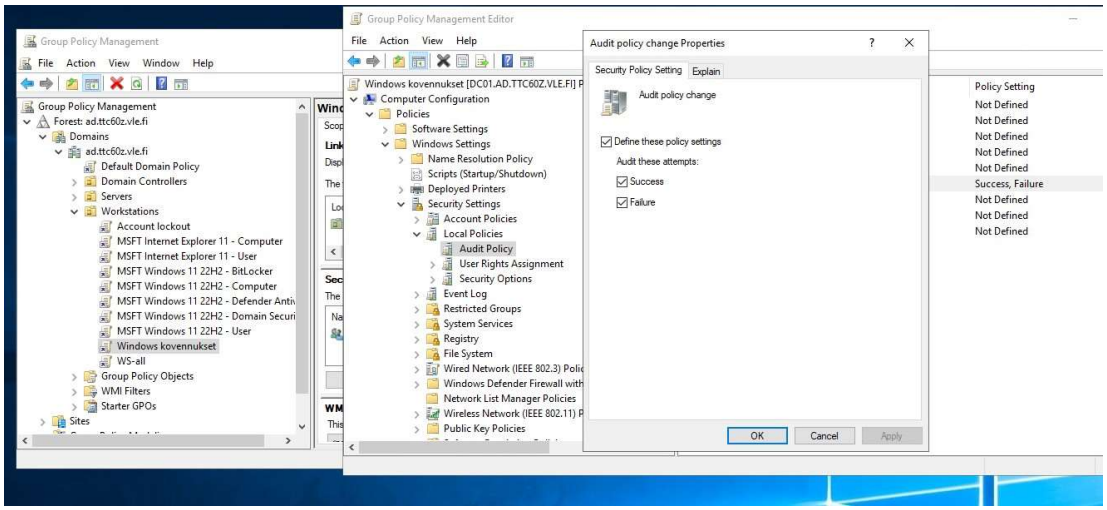
3.2 Lisäkovennukset

Microsoftin Security Compliance Toolkitin lisäksi esimerkinomaisesti kaksi kovennusta, kuinka ne tehdään manuaalisesti. Ensin luotiin ”Windows kovennukset” jonka alle kovennukset tehtiin. Esitetty alla.



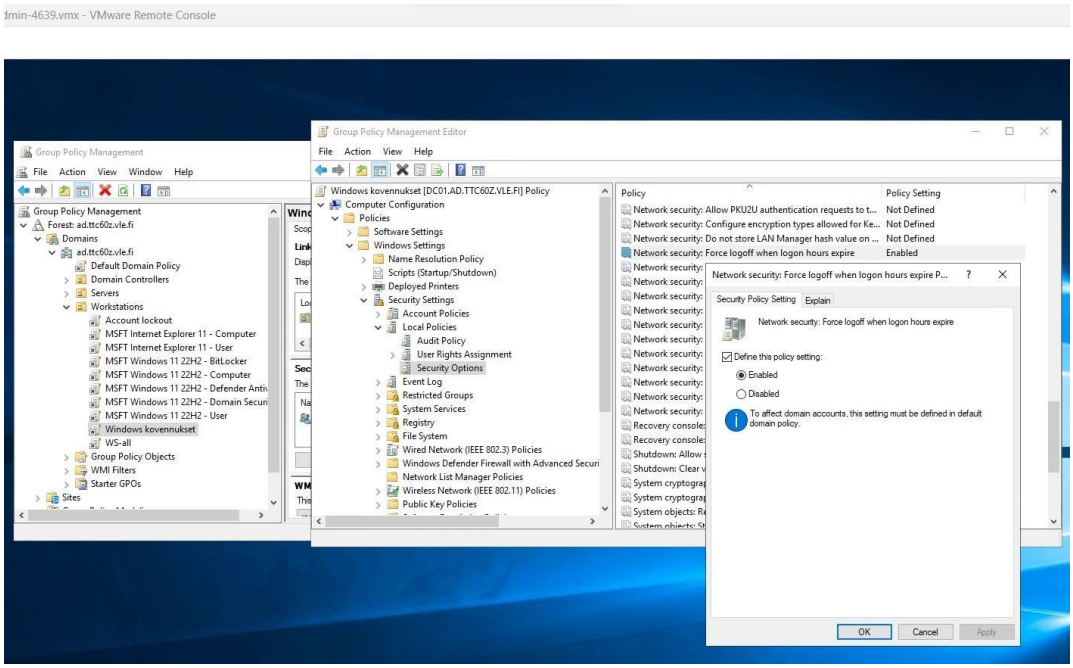
Kuva 16 Manuaaliset Windows 11 kovennukset

Tehtiin kovennus Audit Policyyn – Audit policy change properties, eli jos tekee onnistuneita tai epäonnistuneita muutoksia auditointi sääntöihin, siitä muodostuu auditointi tapahtuma, jonka avulla voidaan seurata muutettuja sääntöjä. Kovennus esitetty alla.



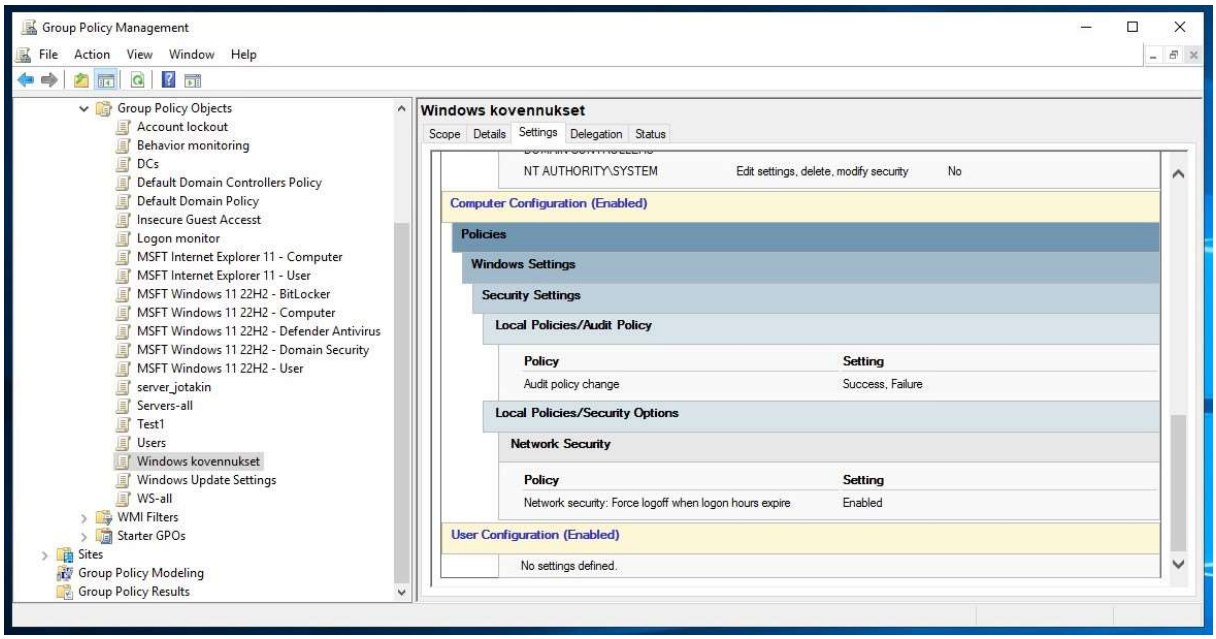
Kuva 17 GPO Kovennus 1 - Audit Policy

Toiseksi kovennukseksi valitsimme Security options – Network security – Force logoff when logon hours expire – Enabled. Pakottaa uloskirjautumisen, kun kirjautumisaika vanhenee. Esitetty kuvassa 18 alla.



Kuva 18 GPO Kovennus 2 - Force logoff

Yhteenvetona tehdyt manuaaliset kovennukset esitettynä alla.



Kuva 19 Yhteenveto manuaalisista GPO kovennuksista Win11

4 POHDINTA

LAB2 harjoituksen tavoitteena oli Windows 11 koventaminen. Ryhmä teki GPO (Group Policy Object) kovennukset käyttäen Microsoftin Security Compliance Toolkit:iä. Lisäksi ryhmä teki kaksi kovennusta manuaalisesti. Teorialla ja koventamisen harjoituksilla ryhmän jäsenet saivat taidot ja ymmärryksen Windows 11 koventamisesta. Lisäksi dokumentoinnissa käytiin läpi teoriaa Microsoft Security Compliance Toolkitistä sekä Microsoft Policy Analyzerista. Harjoitus toteutettiin kurssin VLE ympäristössä oleville DC01 (IP 10.3.0.10) ja WS01 (IP 10.1.0.10).

Windows 11 kovennuksien analysointiin käytettiin Microsoft Policy Analyzeria. Analyzer ajettiin harjoituksen alussa sekä lopussa, tehtyjen kovennuksien jälkeen, jotta voitiin vertailla lähtö- ja lopputilannetta.

Koventamiseen tehdyt valmiit paketit kuten harjoituksessa käyttämämme Microsoft Security Compliance Toolkit (SCT) ovat nopea ja suhteellisen helppo tapa ajaa monia eri sääntöjä järjestelmään. Tällaisia paketteja asennettaessa kannattaa kuitenkin käydä läpi sääntöjä hieman myös manuaalisesti, sillä kaikki paketin ajamat asetukset eivät välttämättä ole hyödyllisiä siihen ympäristöön mihin ne on ajettu.

Käydessämme läpi SCT asettamia kovennuksia huomasimme esimerkiksi, että salasanan minimi pituus oli asetettu 14 merkkiin, ympäristössä missä tällä hetkellä työskentelemme tällaisesta kovennuksesta, on enemmän haittaa kuin hyötyä.

Lähteet

Loos, A. 29.8.2018. Introduction to Microsoft Policy Analyzer. Viitattu 20.2.2023. https://arnaud-loos.com/2018/intro-to-policy-analyzer/

Margosis, A. 18.6.2019. New Tool: Policy Analzyer. Viitattu 20.2.2023. https://techcommunity.microsoft.com/t5/microsoft-security-baselines/new-tool-policy-analyzer/ba-p/701049

Nemnom, C. 29.8.2022. Learn All About The Microsoft Security Compliance Toolkit! Viitattu 19.2.2023 https://charbelnemnom.com/microsoft-security-compliance-toolkit/?utm_content=cmp-true