WLabra 2

Ryhmä 13

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Koventaminen TTC6050-3006

11.10.2024

Tieto- ja viestintätekniikka

Sisältö

[1 Johdanto 4](#_Toc179551982)

[2 Teoria 4](#_Toc179551983)

[2.1 Microsoft Security Compliance Toolkit 4](#_Toc179551984)

[2.2 Group Policy Objects (GPO) 5](#_Toc179551985)

[2.3 Fine-grained password policies (FGPP) 6](#_Toc179551986)

[2.4 Muita termejä 6](#_Toc179551987)

[3 Kovennukset 7](#_Toc179551988)

[3.1 Security Compliance Toolkitin asennus 7](#_Toc179551989)

[3.2 Etäkäytön estäminen 15](#_Toc179551990)

[3.3 Työaseman asetusten muokkaamisen rajoittaminen 16](#_Toc179551991)

[3.4 Fine grained password policies 20](#_Toc179551992)

[4 Pohdinta 24](#_Toc179551993)

[Lähteet 25](#_Toc179551994)

Kuviot

[Kuvio 1. Domain admin -käyttäjän luonti 8](#_Toc179551995)

[Kuvio 2. Käyttäjän lisääminen turvaryhmään 8](#_Toc179551996)

[Kuvio 3. Asennetut paketit 9](#_Toc179551997)

[Kuvio 4. PolicyAnalyzer 9](#_Toc179551998)

[Kuvio 5. Politiikkojen vertailu 10](#_Toc179551999)

[Kuvio 6. Konfliktit 10](#_Toc179552000)

[Kuvio 7. DC scripti 11](#_Toc179552001)

[Kuvio 8. Policy objects 12](#_Toc179552002)

[Kuvio 9. workstations 12](#_Toc179552003)

[Kuvio 10. Gpupdate 13](#_Toc179552004)

[Kuvio 11. Analyysi lopputilanteessa 13](#_Toc179552005)

[Kuvio 12. Asennetut politiikat 14](#_Toc179552006)

[Kuvio 13. Estetty asennus 15](#_Toc179552007)

[Kuvio 14. Etäkäytön estäminen 15](#_Toc179552008)

[Kuvio 15. Estetty etäkäyttö 16](#_Toc179552009)

[Kuvio 16. Limit\_controlPanel GPO 17](#_Toc179552010)

[Kuvio 17. Ohjauspaneelin rajoittaminen 17](#_Toc179552011)

[Kuvio 18. Sallitut asetukset 18](#_Toc179552012)

[Kuvio 19. Työntekijän ohjauspaneeli 18](#_Toc179552013)

[Kuvio 20. Asetukset-valikon näkyvät sivut 19](#_Toc179552014)

[Kuvio 21. Työntekijälle näkyvät asetukset 19](#_Toc179552015)

[Kuvio 22. Local Log On 20](#_Toc179552016)

[Kuvio 23. Muutettu asetus 20](#_Toc179552017)

[Kuvio 24. Uusi turvallisuusryhmä salasanakäytänteitä varten 21](#_Toc179552018)

[Kuvio 25. Employees\_Password ryhmän jäsenet 21](#_Toc179552019)

[Kuvio 26. New password setting 22](#_Toc179552020)

[Kuvio 27. Salasana-asetusten luonti 22](#_Toc179552021)

[Kuvio 28. Ryhmään vaikuttavat 23](#_Toc179552022)

[Kuvio 29. Powershell testi 23](#_Toc179552023)

# Johdanto

Koventaminen-opintojakson toisessa labratyössä tarkoituksena on koventaa virtuaaliympäristömme Windows 11 virtuaaliympäristömme Microsoftin tuotteita. Tähän kuului varsinkin GPO kovennukset (DC01:llä), sekä omia valikoituja kovennuksia mitkä ryhmä näki tarpeellisiksi. Käytimme Security Compliance Toolkittiä luodaksemme pohjan kovennuksille. Sen jälkeen valitsimme netistä löydettyjä yleisiä ohjeita Windowsin koventamiseen. Merkittäviä muutoksia teimme RDP, Kontrolli-paneelin, asetusten sekä käyttäjien käyttörajoituksiin.

# Teoria

Koventamisen toteuttaminen voi olla monimutkaista ja aikaa vievää varsinkin, jos kyseessä on isompi organisaatio ja laajempi, monimutkaisempi ympäristö. Jotkut turvallisuusominaisuudet voivat aiheuttaa ylimääräistä kuormitusta järjestelmälle ja vaikuttaa sen suorituskykyyn. Lisäksi muutokset järjestelmän konfiguraatioissa voivat häiritä normaalia toimintaa. Koventamisen toteuttamisessa on myös tärkeää noudattaa alan standardeja kuten Computer Information Security (CIS) Benchmarks -ohjeita. Ympäristön koventamista varten on myös laaja valikoima työkaluja, skriptoja sekä automaatioita, jotka helpottavat tarvittavien muutosten toteuttamista ja analysointia. (Shruti456rawal. 2024).

## Microsoft Security Compliance Toolkit

Security Compliance Toolkit (SCT) on Microsoftin kehittämä työkalu, jonka tarkoitus on administraattorin ryhmäpolitiikkaobjektien (GPO) ja tietoturva-asetusten hallitsemisen helpottaminen. Työkalulla pystytään vertaamaan käytössä olevien ryhmäpolitiikkaobjektien ja Microsoftin GPO-suositusten eroavaisuuksia, ja konfiguroimaan käytänteen noudattamaan Microsoftin suosituksia. (Microsoft Security Compliance Toolkit - How to use. 2024)

**Policy analyzer** on Microsoft SCT:n apuohjelma, jolla voidaan analysoida ja verrata GPO sääntöjä. Sen tehtävänä on esittää päällekkäiset asetukset ja ristiriidat ryhmäpolitiikoiden välillä. Työkalu voi verrata esimerkiksi GPO:n asetuksia siihen, mitä on käytössä paikallisella tasolla. Näin työkalun avulla voidaan havaita poikkeamat ja muutokset vaikkapa paikallisella koneella verrattuna koko domainin asetuksiin. Policy Analyzer siis helpottaa erojen tunnistamista ja mahdollisten poikkeamien havaitsemista. (Microsoft Security Compliance Toolkit - How to use. 2024)

## Group Policy Objects (GPO)

Group Policy Objects (GPO) ovat keskeinen osa Microsoftin Active Directory -infrastruktuuria. GPO:t mahdollistavat hallittujen asetusten määrittämisen käyttäjille ja tietokoneille. Oikein suunniteltuna ja toteutettuina niillä voidaan parantaa järjestelmän tietoturvallisuutta sekä parantaa IT-infrastruktuurin toimintaa merkittävästi. (Group Policy Objects. 2018)

Muutamia esimerkkejä parhaista käytännöistä (**Best Practices**) Group Policy Objects.

**Organisointiyksiköiden (OU) jakaminen käyttäjiin ja tietokoneisiin**. Jakamalla käyttäjät ja tietokoneet erillisiin OU:hin helpottaa erilaisten käytäntöjen soveltamista. Esimerkiksi tietokonepolitiikat voidaan kohdistaa ympäristön joka tietokoneeseen ja käyttäjäpolitiikat jokaiseen käyttäjään, tai vaikka vain tiettyyn ryhmään, esimerkiksi HR tai SALES.

**Selkeä nimeämiskäytäntö GPO**. Käytä GPO:n nimeämisessä selkeitä, kohdetta kuvaavia nimiä, jotta asetetun GPO:n merkitys helppo ymmärtää nimestä. Esimerkiksi käyttäjäpolitiikoille voi käyttää "U\_" ja tietokonepolitiikoille "C\_" alkuja, kuten “U\_user\_policy” ja “C\_computer\_policy”. Näin nimi itsessään kertoo, mihin kohteeseen kyseinen GPO vaikuttaa.

**GPO priorisointi**. GPO:ta sovelletaan järjestyksessä **LSDOU** (Local, Site, Domain, OU). Asetukset paikallisella (Local) omaavat matalimman, kun taas OU-tason asetukset korkeimman prioriteetin. Priorisointi määrää, mitkä asetukset lopulta ovat voimassa.

**Rajoita pääsyä ohjauspaneeliin**. Rajoittamalla pääsyä ohjauspaneeliin voidaan estää vaikka normaali käyttäjiä tekemästä muutoksia järjestelmäasetuksiin, muutosten tekemisen kuuluessa ylläpitäjille. Tämä estää virheiden syntyä perus käyttäjien toimesta ja näin parantaa turvallisuutta.

**Estä siirrettävien medioiden käyttö**. USB-tikut ja muut siirrettävät mediat voivat olla mahdollinen tietoturvariski, sillä ne voivat levittää haittaohjelmia. GPO:n soveltamisen avulla on mahdollisuus estää nämäkin. Tulee miettiä, käytetäänkö siirrettävää mediaa paljon ja miten niiden estäminen vaikuttaa käytettävyyteen. (Group Policy Best Practices. 2024)

## Fine-grained password policies (FGPP)

Fine-grained password policies ovat active directory (AD) ominaisuus, jonka avulla voidaan määrittää erilaisia salasanojen ja tilin lukkiutumis- sääntöjä käyttäjille, sekä käyttäjäryhmille organisaatiossa. Tämä mahdollistaa salasanojen turvallisuuden hallinnan joustavammalla ja tarkemmalla tavalla. (Configure fine grained password policies for Active Directory Domain Services. 2024)

## Muita termejä

**Windows toimialue** (**Domain**) kattaa koko ympäristön laitteet ja niiden keskitetyn hallinnan. **Domain** mahdollistaa käyttäjien kirjautumisen mille tahansa laitteelle toimialueella, eli kirjautuminen on toimialuekohtaista, eikä laitekohtaista. Toimialuetta voidaan hallita ryhmien ja sääntöjen avulla, jotka saadaan asetettua koko alueeseen kerralla, helpottaen ylläpitoa. (Hyytiäinen. 2024)

**Paikallinen pääkäyttäjä** (**Local Admin**) on tietyn päätelaitteen admin, joka on valtuutettu tekemään muutoksia vain tiettyyn laitteeseen toimialueella. **Toimialueen pääkäyttäjä** (**Domain Admin**) on koko toimialueen **Admin**, joka voi tehdä asetuksiin muutoksia koko toimialueessa. (Hyytiäinen. 2024)

**Korkeiden käyttöoikeuksien hallinta** tai **Privileged Access Management** (**PAM**) on tietoturvaratkaisu, jolla voidaan suojata ympäristön tietoturvaa hallitsemalla korkeampien käyttöoikeuksien omaavia käyttäjiä ja auditoimalla niiden toimintaa. Hallitsemalla tavallisten käyttäjien pääsyä järjestelmien kriittisiin asetuksiin, saadaan suojattua järjestelmää esim. hakkereiden sivuttaisliikkeen (Lateral Movement) varalta, tai vaikka henkilökunnan tiettyjen ryhmien tarpeettoman pääsyn palomuuriasetuksiin tai ohjauspaneelin hallintaan. Korkean tason käyttöoikeudet käyttäjätileillä ovat tietoturvariski, mikäli kyberhyökkääjät pääsevät tilien tunnuksiin käsiksi. Tilien laajoilla käyttöoikeuksilla voidaan varastaa salaista tietoa organisaatiosta ja muunnella kriittisiä asetuksia toimialueen laitteilla. Tämän vuoksi näiden tilien suojauksen tulee olla huomattavasti vahvempi esimerkiksi monivaiheisen tunnistautumisen avulla (MFA), kuin toimialueen tavallisilla käyttäjillä. (Hyytiäinen. 2024)

**RDP** (Remote Desktop Protocol) on protokolla, joka mahdollistaa etäyhteyden luomisen toiseen tietokoneeseen verkon yli. RDP on salattu TCP (transmission control protocol) protokollaa käyttäen. (Understanding the Remote Desktop Protocol (RDP).2023)

**Gpupdate /force** on komento, jonka avulla pakotetaan ryhmäkäytäntöjen päivittäminen välittömästi tietokoneeseen. (gpupdate.2023)

**Gpresult /r** on komento, joka näyttää tietokoneessa sovellettavat GPO:t. (gpresult.2023)

# Kovennukset

Tässä harjoituksessa tarkoituksenamme oli koventaa Windows 11 -työasemaa. Ohjeistuksessa sanottiin, että tässä vaiheessa olisi hyvä käyttää Security Compliance Toolkitiä ja sen lisäksi tehdä muutamia muita kovennuksia. Aloitimme harjoituksen Security Compliance Toolkitin asennuksella.

## Security Compliance Toolkitin asennus

Aloitimme Security Compliance Toolkitin asennuksen luomalla uuden domain admin -käyttäjän, jolla voimme asentaa ja ajaa tiedostoja. (Kuvio 1.)

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

Kuvaus luotu automaattisesti

Kuvio 1. Domain admin -käyttäjän luonti

Lisäsimme käyttäjän turvaryhmään domain admins. (Kuvio 2).

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

Kuvaus luotu automaattisesti

Kuvio 2. Käyttäjän lisääminen turvaryhmään

Latasimme Security Compliance Toolkitin WS01 -työasemalle ja asensimme kuvion 3 mukaiset paketit.

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

Kuvaus luotu automaattisesti

Kuvio 3. Asennetut paketit

Seuraavaksi ajoimme PolicyAnalyzerin, joka suoritti analyysin käytössä olevista turvallisuus politiikoista. (Kuvio 4.)

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

Kuvaus luotu automaattisesti

Kuvio 4. PolicyAnalyzer

Ohjelma listasi vertailun käytössä olevista ja työkalun mukaan hyvistä politiikoista. (Kuvio 5.)

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

Kuvaus luotu automaattisesti

Kuvio 5. Politiikkojen vertailu

Otimme kuvion 7 mukaisen kuvan konflikteista. (Kuvio 7).

Kuva, joka sisältää kohteen teksti, kuvakaappaus

Kuvaus luotu automaattisesti

Kuvio 6. Konfliktit

Siirsimme WS01:llä toolkitin jaetulle verkkoasemalle, johon pääsimme käsiksi DC01:llä. Siirryimme DC01:lle ja ajoimme tiedoston Baseline-ADImport.ps1 powershellillä. (Kuvio 7).

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

Kuvaus luotu automaattisesti

Kuvio 7. DC scripti

Nyt kun policy objectit oli tuotu Active Directoryyn (kuvio 8), siirsimme ne workstations Organizational Unitin alle (kuvio 9). Credential Guard poistettiin, koska ohjeistuksen mukaan se aiheuttaa WS01:llä blue screenin VLE-ympäristössämme.

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

Kuvaus luotu automaattisesti

Kuvio 8. Policy objects

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

Kuvaus luotu automaattisesti

Kuvio 9. workstations

Ajoimme WS01-työasemalla komentokehotteella komennon gpupdate /force, jotta politiikat päivittyvät käyttöön. (Kuvio 10).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 10. Gpupdate

Ajoimme uuden analyysin konflikteista ja niitä ei enää ollut. Politiikat olivat siis onnistuneesti asennettu. (Kuvio 11).

Kuva, joka sisältää kohteen teksti, kuvakaappaus, viiva

Kuvaus luotu automaattisesti

Kuvio 11. Analyysi lopputilanteessa

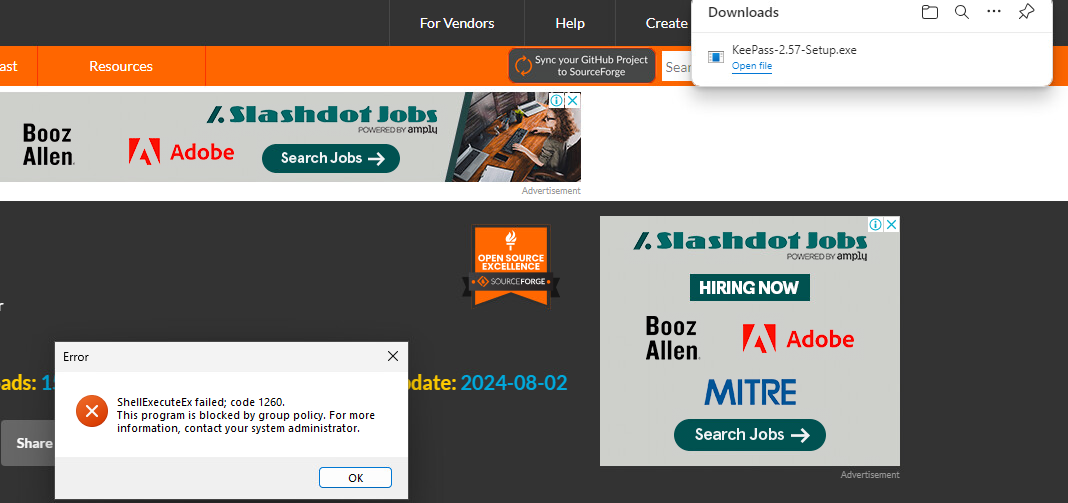
Ajoimme vielä analyysin asennetuista politiikoista. Lista on erittäin pitkä, joten vain pieni osa mahtui kuvaan, mutta kuten kuviosta 12 ilmenee, listassa on 311 kohtaa.

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

Kuvaus luotu automaattisesti

Kuvio 12. Asennetut politiikat

DC01:llä ajamamme skripti toi mukanaan useita koventamisen näkökulmasta hyödyllisiä asetuksia käyttöön, esimerkiksi yksi näistä on ohjelmistojen asentamisen estäminen käyttäjillä. (Kuvio 13).



Kuvio 13. Estetty asennus

## Etäkäytön estäminen

Halusimme estää etäkäytön niiltä käyttäjiltä, joilla ei ole siihen tarvetta. Etäkäyttö on yleinen turvallisuusriski, jota hyökkääjät käyttävät tunkeutuessaan järjestelmiin. Loimme siis uuden säännön, joka estää tämän työntekijöiltä. (Kuvio 14).

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

Kuvaus luotu automaattisesti

Kuvio 14. Etäkäytön estäminen

Yritimme käynnistää etäkäytön, kun olimme kirjautuneet WS01:lle työntekijän tunnuksilla. Tämä antoi virheilmoituksen, että etäkäytön käyttäminen on estetty. Tarkistimme myös komentokehotteella komennolla gpresult /r mitkä politiikat kohdetuvat käyttäjään ja sieltä löytyi luomamme etäkäytön estävä politiikka. (Kuvio 15).

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

Kuvaus luotu automaattisesti

Kuvio 15. Estetty etäkäyttö

## Työaseman asetusten muokkaamisen rajoittaminen

Kaikilla käyttäjillä ei ole tarvetta päästä käsiksi työaseman kaikkiin asetuksiin, joten päätimme rajoittaa näiden asetusten näkyvyyttä.

Loimme uuden GPO:n nimeltä Limit\_controlPanel ja avasimme group policy editorin. (Kuvio 16).

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

Kuvaus luotu automaattisesti

Kuvio 16. Limit\_controlPanel GPO

Muokkasimme asetusta Show only specified Control Panel items, jonka avulla saimme määritettyä käyttäjälle näkyvät paneelin asetukset. (Kuvio 17.)

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

Kuvaus luotu automaattisesti

Kuvio 17. Ohjauspaneelin rajoittaminen

Vaihdoimme asetuksen enabled tilaan. Lisäsimme käyttäjille näkyviin ohjauspaneelin asetuksiin kohteita avaamalla options-ikkunan show-painikkeesta. Valitsimme kohteita tarpeen mukaan kuvion 18 mukaisesti.

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

Kuvaus luotu automaattisesti

Kuvio 18. Sallitut asetukset

Siirryimme WS01:lle työntekijän tunnuksilla ja asetukset olivat astuneet voimaan. Käyttäjä pystyy siis muokkaamaan vain muutamia asetuksia ohjauspaneelin kautta. (Kuvio 19)

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

Kuvaus luotu automaattisesti

Kuvio 19. Työntekijän ohjauspaneeli

Rajasimme myös työntekijöiden mahdollisuutta muokata työaseman asetuksia Asetukset-valikon kautta. Laitoimme Settings page visibility asetuksen käyttöön ja listasimme sinne sivut, jotka halusimme näkyvän käyttäjien Asetukset-valikossa. (Kuvio 20)

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

Kuvaus luotu automaattisesti

Kuvio 20. Asetukset-valikon näkyvät sivut

Asetusten voimaantulon jälkeen työntekijöiden Asetukset-valikko näytti kuvion 21 mukaiselta.

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

Kuvaus luotu automaattisesti

Kuvio 21. Työntekijälle näkyvät asetukset

Huomasimme että file serverille SRV01 pystyi kirjautumaan millä vain tunnuksilla, ja päätimme rajata toistaiseksi kirjautumisen vain administraattoreille Allow log on locally asetuksella. (Kuvio 22).

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

Kuvaus luotu automaattisesti

Kuvio 22. Local Log On

Käytännössä muutimme siis kuvion 23 mukaisen asetuksen.

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

Kuvaus luotu automaattisesti

Kuvio 23. Muutettu asetus

## Fine grained password policies

Luodaksemme salasanakäytänteitä, jotka koskevat rajattua käyttäjäryhmää, käytimme fine grained password policy menetelmää. Teimme ensin turvallisuusryhmän, jonka lisäsimme kaikille työntekijöille, jotta salasana käytänteet koskevat vain heitä. Tämä asetus tulisi voimaan normaalisti kaikille, mutta emme halua muuttaa adminien salasanoja, koska se on ohjeistuksessa kielletty. (Kuvio 24). Turvallisuus ryhmä kannattaisi nimetä U\_ alkuiseksi, selkeytettäväksi politiikan kohdistumista käyttäjiin.

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

Kuvaus luotu automaattisesti

Kuvio 24. Uusi turvallisuusryhmä salasanakäytänteitä varten

Lisäsimme luodun ryhmän työntekijöidemme käyttäjille. Siirsimme aiemmin tekemämme AD ryhmän myös Hard\_workers OU:n alle. (Kuvio 25).

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

Kuvaus luotu automaattisesti

Kuvio 25. Employees\_Password ryhmän jäsenet

Avasimme DC01:lla Admin Directory Administrative centerin ja sijaintiin system\Password settings container ja loimme uuden salasana-asetuksen. (Kuvio 26).

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

Kuvaus luotu automaattisesti

Kuvio 26. New password setting

Syötimme salasanapolitiikan rajoitukset sekä ryhmän, jota se koskee. Halusimme, että työntekijöiden salasanat ovat vähintään 10 merkkiä pitkiä, salasana tulee vaihtaa 29 vuorokauden välein ja vanhoja salasanoja ei voi käyttää. (Kuvio 27).

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

Kuvaus luotu automaattisesti

Kuvio 27. Salasana-asetusten luonti

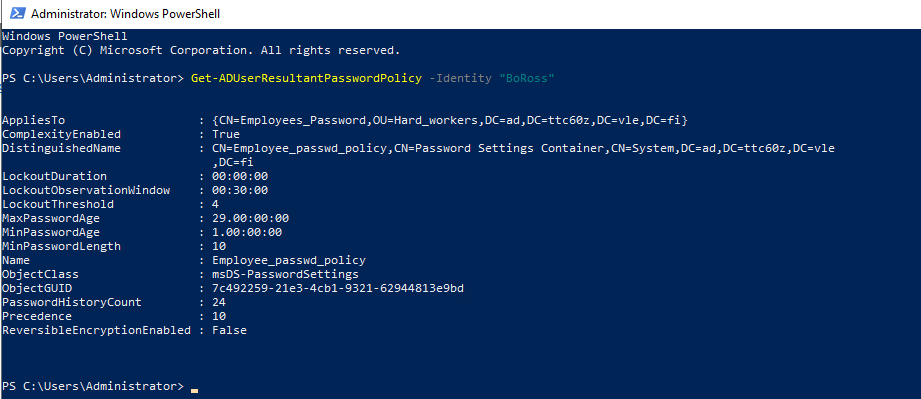
Kun siirryimme katsomaan employees\_password ryhmään vaikuttavia salasana-asetuksia password settings osiossa, näimme siellä tekemämme salasanapolitiikan. (Kuvio 28).

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

Kuvaus luotu automaattisesti

Kuvio 28. Ryhmään vaikuttavat

Ajoimme vielä powershell-komennon ja totesimme, että salasana politiikka tuli käyttöön työntekijöille. (Kuvio 29).



Kuvio 29. Powershell testi

# Pohdinta

Koventamisen toisessa labratyössä pääsimme syventymään koventamiseen ja käyttämään Micosoftin security compliance toolkittiä GPO kovennusten toteuttamiseksi. Saimme myös paremman kuvan GPO:iden käyttäytymisestä ja asetusten muokkaamisesta.

Yksi keskeisistä huomioista labratyössä oli ryhmäkäytäntöjen (GPO) monipuolisuus ja tehokkuus organisaation tietoturvan hallinnassa. GPOn avulla voimme keskitetysti hallita ja määrittää turvallisuusasetuksia useille työasemille ja käyttäjäryhmille, mikä vähentää inhimillisten virheiden mahdollisuutta ja parantaa tietoturvan hallittavuutta. Tämä korostui esimerkiksi siinä, kuinka saimme estettyä RDP käytön tietyiltä käyttäjäryhmiltä ja rajoitettua Control Panel- ja settings valikkoja, mikä vähentää väärinkäytön riskiä ja yksinkertaistaa käyttäjäkokemusta.

Lisäksi salasanakäytännöt (Fine-Grained Password Policies) olivat uusi oppimisen osa-alue. Niiden avulla pystyimme räätälöimään eri käyttäjäryhmille soveltuvat salasanavaatimukset, mikä tuo joustavuutta organisaation tietoturvakäytäntöihin. Tämä mahdollistaa sen, että korkeamman riskin ryhmillä, kuten ylläpitäjillä, voi olla tiukemmat salasanavaatimukset verrattuna tavallisiin käyttäjiin.

Labran toteuttaminen sujui suurimmaksi osaksi ilman isompia ongelmia, ja nekin ongelmat mitä tuli vastaan saatiin ratkottua yhteistuumin ja niistäkin opittiin paljon. Esimerkiksi SCT:n käyttäminen ja FGPP tulivat uusina asioina. Syvennyimme myös hieman ryhmäkäytäntöjen hallitsemiseen OU tasolla.

Lähteet

Configure fine grained password policies for Active Directory Domain Services. Microsoft Learn artikkeli. 2024. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/fine-grained-password-policies?tabs=adac>

gpresult. Microsoft Learn artikkeli. 2023. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult>

Group Policy Best Practices. Netwrix ohje. 2024. Viitattu 3.10.2024. <https://www.netwrix.com/group_policy_best_practices.html>

Group Policy Objects. Microsoft Learn artikkeli. 2018. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects>

gpupdate. Microsoft Learn artikkeli. 2023. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate>

Microsoft Security Compliance Toolkit - How to use. Microsoft Learn artikkeli. 2024. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/security-compliance-toolkit-10>

Pasi Hyytiäinen. TTC6050-Koventaminen AD, PIM&PAM, JIT & JEA. JAMK opetus PDF. 2024. Viitattu 3.10.2024. <https://moodle.jamk.fi/pluginfile.php/1461084/mod_label/intro/AD%20pimpam%20JIT.pdf>

Shruti456rawal. What is System Hardening? Geeksforgeeks-verkkosivuston artikkeli. 1.3.2024. Viitattu 3.10.2024. <https://www.geeksforgeeks.org/what-is-system-hardening/?ref=header_outind>

Understanding the Remote Desktop Protocol (RDP). Microsoft Learn artikkeli. 2023. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol>