

6. turvallisuuden policy

Wednesday, October 29, 2025 19:55

Nyt seuraavaksi jatkuu turvallisuuden policy asetuksia mm. salasana vaatimuksensa esim. Minimi 12 kirjainta, sisältyen erikoismerkki ja salasan päivittäminen vuosikello esim. 90 päivän välein.

Toisena harjoituksessa lisätään asetuksensa kirjautumisen yritys esim. Kirjautuu käyttäjätunnusesta josta esim. Ensimmäiset 3 yritystä jos ei pääse sisään niin käyttäjätunnus menee kuin karanteeniin/jäähylle hetkeksi n. 30min tai tunniksi. Sen ajastetun jälkeen taas 3 yritystä.

- Tähän voi vaikuttaa esim. Jos on oikea käyttäjä mutta salasanan syöttäessä menee väärin, että joko viimeisessä kirjaimessa on erikoismerki tai numero. Tämän kautta voidaan hyödyntää just Windows 11 työaseman kirjautumista ja Mac on omansa ja sama idea.
- Tämä on hyödyllinen harjoitus, koska estääkseen hakkerin tekemän "brute-force-hyökkäyksen"

Yleensä menisi miljoonaa vuotta saadakseen ja täsmennyä se oikea salasana.



Harjoitus DEMO - START HERE;

Activity 1 Password policy configuration

Configure and enforce a strong password policy for AD users

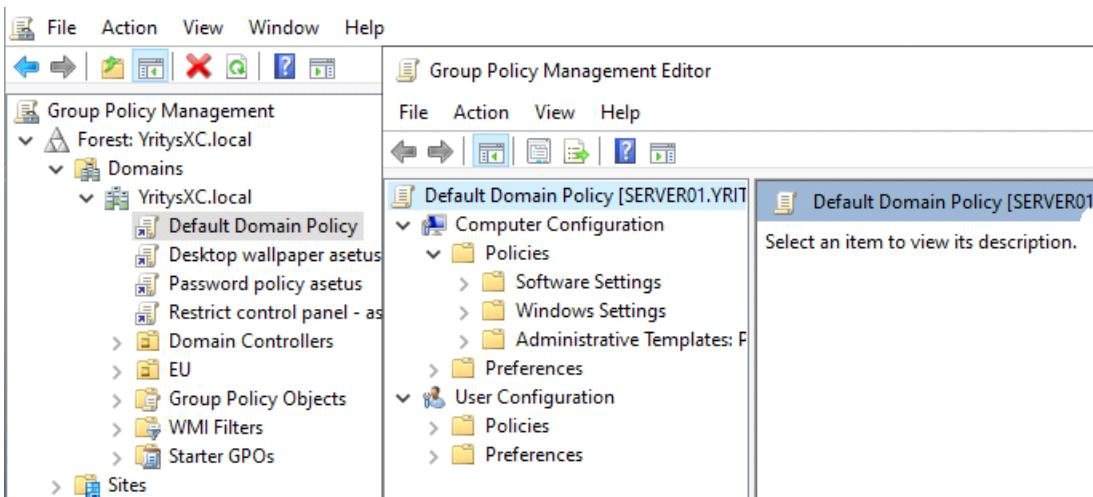
- Win minimum password length = 8 characters
 strong passwords = 12 characters or more

Avaa Windows server ja mene >> group policy management

The screenshot shows the Windows Group Policy Management console. The left pane displays a tree structure of Group Policy objects under 'Forest: YrityXC.local / Domains / YrityXC.local'. The 'Default Domain Policy' is selected and highlighted with a blue border. A context menu is open over this policy, with the 'Edit...' option highlighted. Other options in the menu include 'Enforced', 'Link Enabled', 'Save Report...', 'View', and 'New Window from Here'. The right pane shows the 'Default Domain Policy' details, with tabs for 'Scope', 'Details', 'Settings', and 'Delegations'. Below the tabs, there is a section titled 'Links' with the sub-instruction 'Display links in this location:' followed by a list of 'Domains, and OUs'.

Aikaisempi on luotu erikseen oma password policy, mutta nyt mennään tämän windows server iAD oletus asetuksensa ja siksi mennään tähän polkuun ja "EDIT"

Nyt mennään "computer configuration" koska se tulee kaikkille käyttäjille kirjautuessaan työasemaan ja siksi syöttäessä tulee olemaan vahva salasana.



Polku: policies >> windows settings >> security settings >> account policies >> password policy
HUIMOINA: tämä oletus ikkuna, että oletus asetukset ja tähän tulee pienistä muutosta

Tähän voidaan muuttaa esim. AD käyttäjälle asettamalla vahva salasana

BEFORE:

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

Näitä muutoksia riippuu yrityksen IT admin ja järjestelmävalvojast pelisäännöistä, että mikä on se pakollinen salasana pituus. Useimmin ehdotetaan:

- Minimi 8 kirjainta tai sitä enemmän, sisältyen iso kirjain, numero ja erikoismerkki.
- Ei kirjoitetta "muistilappulle" ja kirjoitettaan ylös esim. Paperille tai johonkin digitaaliseen ylös näin
- It admin asettaa elinkaaren esim. Joka 90päivän välein viahtelee sen salasansa tai jotkut saattaa päivittää esim. 2-3 kertaa vuodessa
- Sama pätee jos on useita tunnuksia ei käytetä samaa salasanaa niiden alla.

AFTER:

Tälle policy asetukset tulee sitten active directory käyttäjälle.

Policy	Policy Setting
Enforce password history	4 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Disabled

Perus keksii ja käyttää vaikeaeta salasanaa, että miellään pitkä, sisältyen erikoismerkkiä ja iso kirjainta.



Takaisin windows serverin ja luo ja lisää uusi käyttötäjä

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

YritysXC.local

Builtin Computer Domain Controller EU

Users Foreign Security Managed Services Users

New Object - User

Create in: YritysXC.local/EU/Users

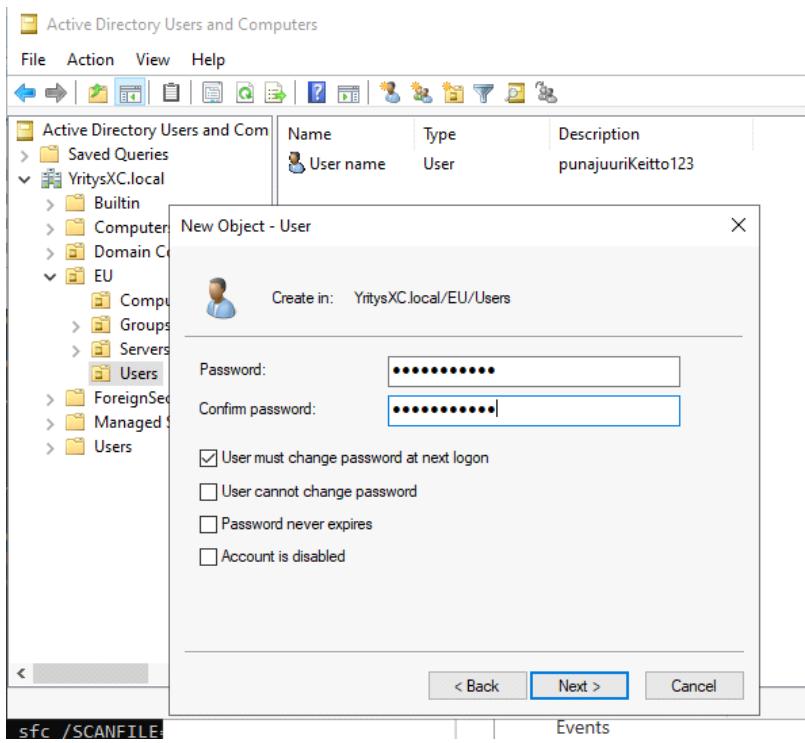
Password: Confirm password:

User must change password at next logon
 User cannot change password
 Password never expires
 Account is disabled

< Back Next > Cancel

sfc /SCANFILE

Events

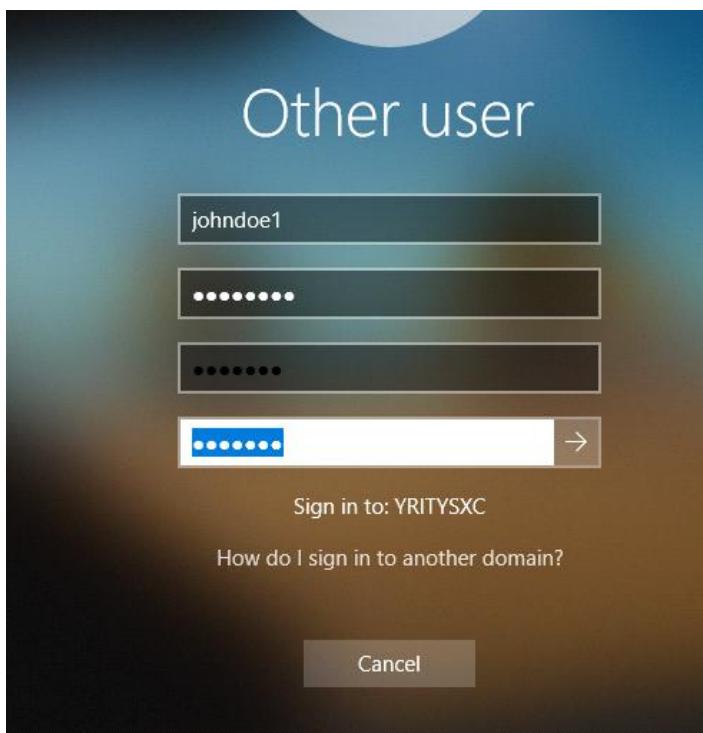
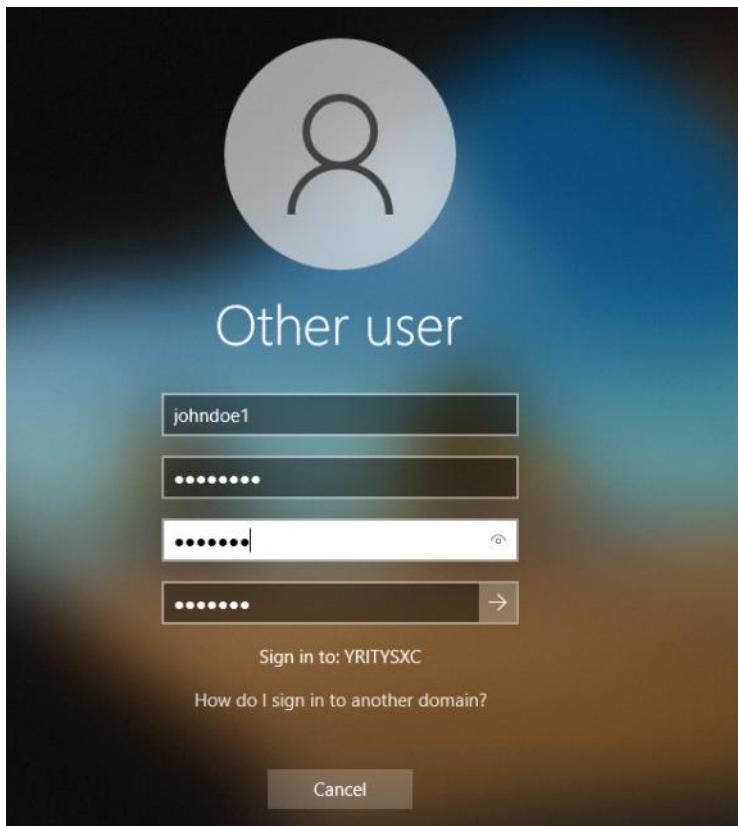


Johndoe1 ; P@ssw0rd

Onnistui eka syöttäminen

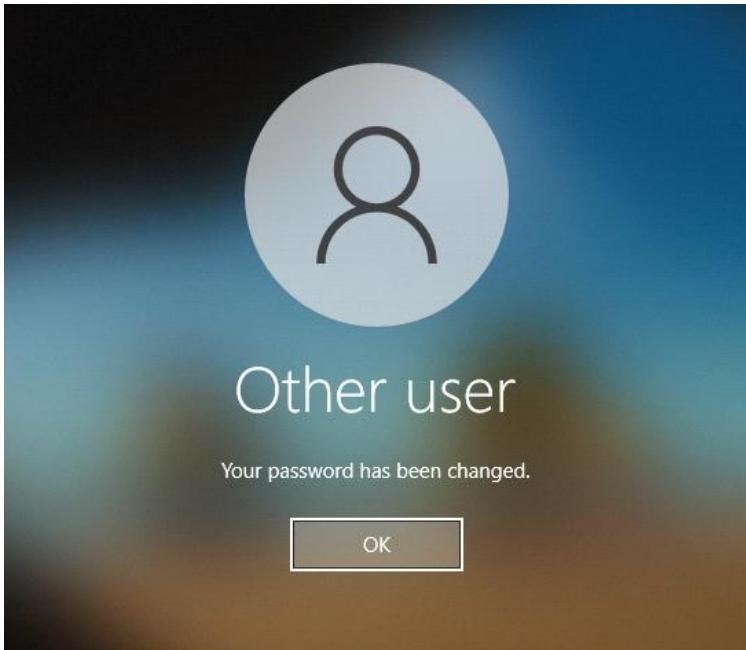


Syötin jotakin 1234567



Nyt pelitti: S€cr3ts

Pitää täyttää ne kriteerit, koska pitää sisältää mm. iso kirjain, erikoismerkki ja minimissään esim. 7 kirjainta



Activity 2: Account lockout policy configuration

- Configure an account lockout policy to protect against brute-force attacks
 - o Password threshold
 - o Password lockout duration
- The higher the threshold, the higher the probability for successful brute force attack

Eli idean, kun hakkeri/roisto yrittää kirjautua käyttäjäntunnusella sisään, että monta yritystä siinä sallitaan ennen kuin menee lukkoon eism. 3 yrityskestä menee lukkoon ja menee karanteeniin esim. 30min tai tunniksi.

Avaa "group policy management" välilehti ja luodaan uusi GPO säätö ja tämä säätö tulee editoimaan tähän oletuksensa kenttään.

A screenshot of the Group Policy Management console. The left navigation pane shows a tree structure with "Forest: YritysXC.local" and "Domains" expanded, showing "YritysXC.local" and "Default Domain Policy". The "Default Domain Policy" is selected and a context menu is open over it. The menu items are: Edit..., Enforced, Link Enabled, Save Report..., New Window from Here, Delete, and Rename. The "Enforced" option is highlighted with a green selection bar. The main pane displays status information for the domain YritysXC.local, stating it is the baseline domain controller and providing links for infrastructure status and change.

Tämä tapahtuu työaseman kirjauttutessa siksi valitaan "computer configuration" >> policies >> windows settings >> security settings >> account policies >> account lockout policy

HUOM tämä on oletuksena ensimmäisen asetuksensa siksi tässä ei ole määritelty monta yritystä saa tehdä ja lukituksena kuinka kauan.

BEFORE:

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays the 'Group Policy Management' tree, including the forest, domain, and specific GPOs like 'Default Domain Policy'. The main pane shows the 'Default Domain Policy [SERVER01.YRITYSXC.LOCA]' details. Under 'Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies', the 'Account Lockout Policy' is highlighted. A table on the right lists three policy settings: 'Account lockout duration' (Not Defined), 'Account lockout threshold' (0 invalid logon attempts), and 'Reset account lockout counter after' (Not Defined).

AFTER:

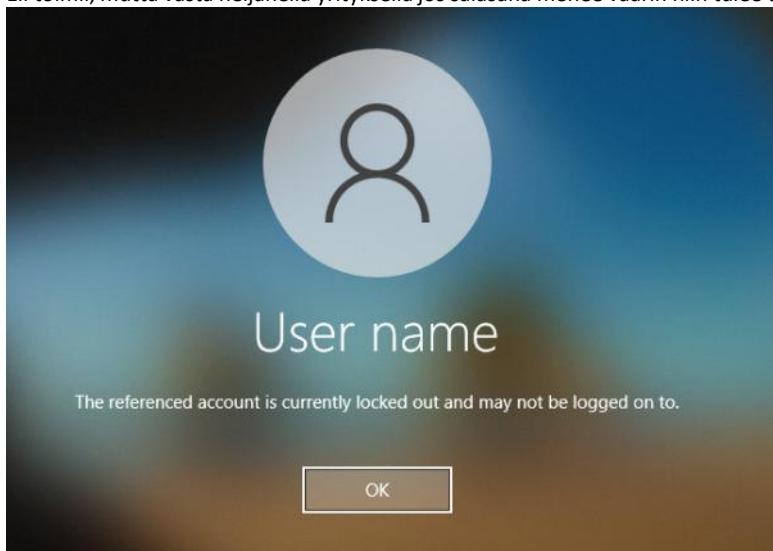
This screenshot shows the same Group Policy Management Editor interface after changes have been made. The 'Account Lockout Policy' now has a defined setting: 'Account lockout duration' is set to '30 minutes'. The other two settings remain at their original values.

Tämä on sama idea kuin esi. Mac/Apple laiteilla, josta koneelle kirjautuessa jos ensimmäiset kolme (3) yritystä jos ei toimi niin lukitsee n. ensimmäisen 1minuutin. Kokeilee seuraavaa 3 yritystä niin menee 10min, ja näin jatkuu 30min, 60min ja jne.

Seuraavaksi päivittää komennolla \$gpupdate /force
Ja suoritetaan pieni skannaus

Suoritetaan testausta ja esim. Testa satunnaisella salasanalla ja käyttäjä "user1"

Eli toimii, mutta vasta neljänellä yrityksellä jos salasana menee väärin niin tulee tällanne ilmoitus.



Activity 3: user rights assignment

- Assign and restrict user rights to enhance security
 - o Role based access
 - o Restrict remote desktop access

Tässä ikään kuin vaihtaa käyttäjää et salliko se kirjautua admin tunnuksella sisään
Toisessa win 10 RDP kirjautuu windows serveriin <nimi> , josta ponnahtaa kyselly syötä salasana (oleetus valmina käyttäjätunus) - niin jos salasana täsmentyy silti saa estonsa ettei ole oikeutta päästääkseen sisään

TÄÄ HARJOITUS SKIP

Activity 4: Implementing fine-grained password policies

- Apply different password policies to different groups of users.
- Scenario: the organization wants to apply stricter password policies to administrative accounts while allowing standard users to have less stringent requirements.
 - o Fine grained password policies

Tässä käytettää työkaluna: windows administrative tools >>> active directory administrative center (ADAC)

Tämän kautta esim. Määrittää tiettyyn ryhmille se oikeus - ja tämkin on SKIP