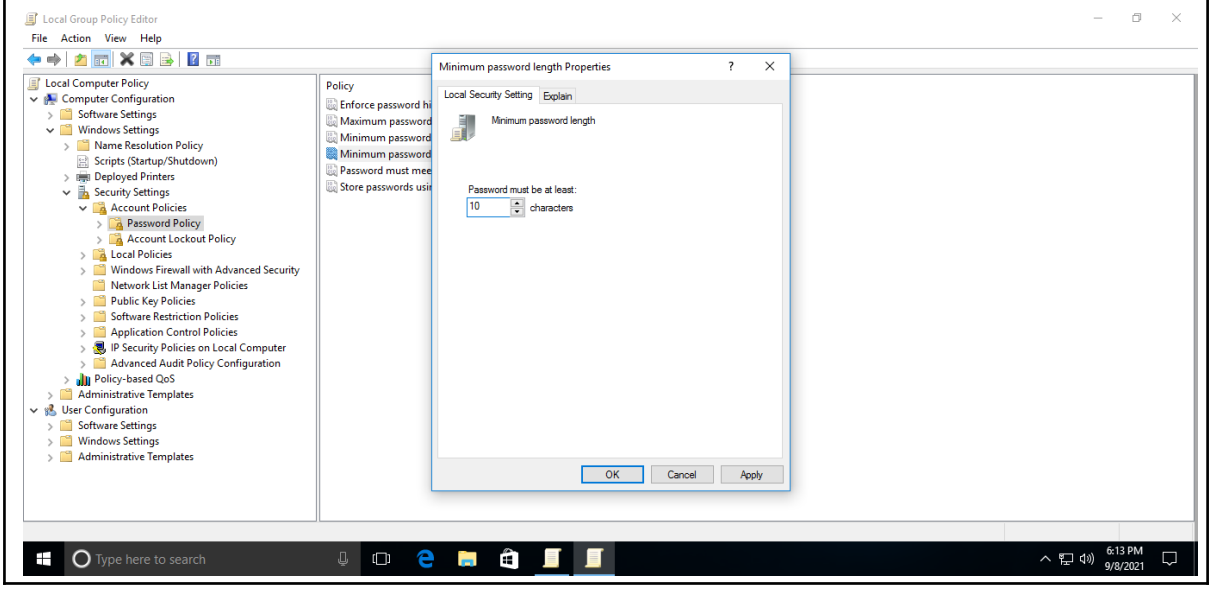
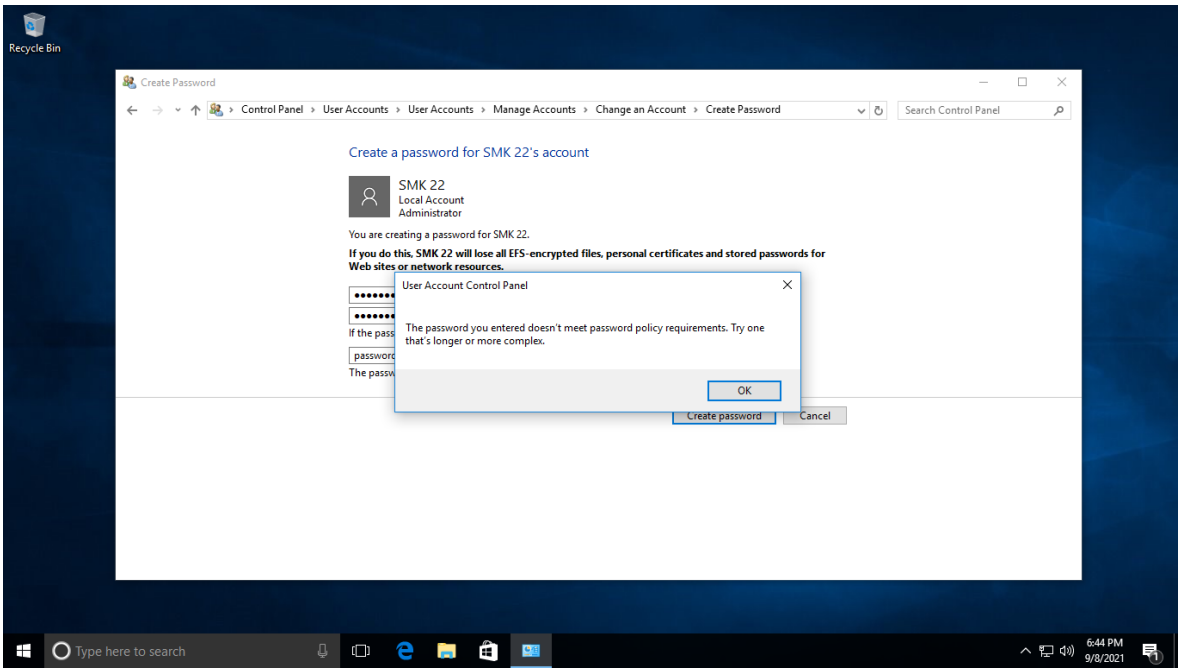
HARDENING WINDOWS 10

NAMA TIM	Kyzo
KETUA	Sahrul Anugerah
ANGGOTA	Muhammad Soleh

1. **Password Minimum Length**

Challenge : Pick random preconfigured account, change password to random one that must be no less than 10 characters (which meets complexity requirements)
Windows 10 mempunyai Security Police yang mengatur setiap user membuat password dengan minimal berapa karakter. Para peserta membuat kebijakan setiap password untuk user di Windows 10 diharuskan memasukan password dengan 10 karakter.
Answer
windows + r -> gpedit.msc -> Computer Configuration -> Windows Setting -> Security Setting -> Account Policies -> Password Policy -> Minimum Password Length diubah menjadi 10 -> Apply
ScrenShoot
Masukan screenshot penyelesaian 1. 

2.


Recycle Bin
Create Password
Control Panel › User Accounts › User Accounts › Manage Accounts › Change an Account › Create Password
Search Control Panel
Create a password for SMK 22's account
SMK 22
Local Account
Administrator
You are creating a password for SMK 22.
If you do this, SMK 22 will lose all EFS-encrypted files, personal certificates and stored passwords for Web sites or network resources.
User Account Control Panel
The password you entered doesn't meet password policy requirements. Try one that's longer or more complex.
OK
Create password
Cancel
Type here to search
6:44 PM
9/8/2021

2. **Password Complexity**

Challenge : Pick random preconfigured account, change password to random one that must be no less than 10 characters (which meets complexity requirements)

Challenge kali ini mengaktifkan fitur complexity requirements di Windows 10. Pengaturan keamanan ini menentukan apakah kata sandi harus memenuhi persyaratan kompleksitas.

Jika kebijakan ini diaktifkan, kata sandi harus memenuhi persyaratan minimum berikut:

- Tidak mengandung nama akun pengguna atau bagian dari nama lengkap pengguna yang melebihi dua karakter berturut-turut
- Panjangnya setidaknya delapan karakter
- Berisi karakter dari tiga dari empat kategori berikut:
- Huruf besar Bahasa Inggris (A sampai Z)
- Huruf kecil Bahasa Inggris (a hingga z)
- Basis 10 digit (0 hingga 9)
- Karakter non-alfabet (misalnya,!, $, #,%)

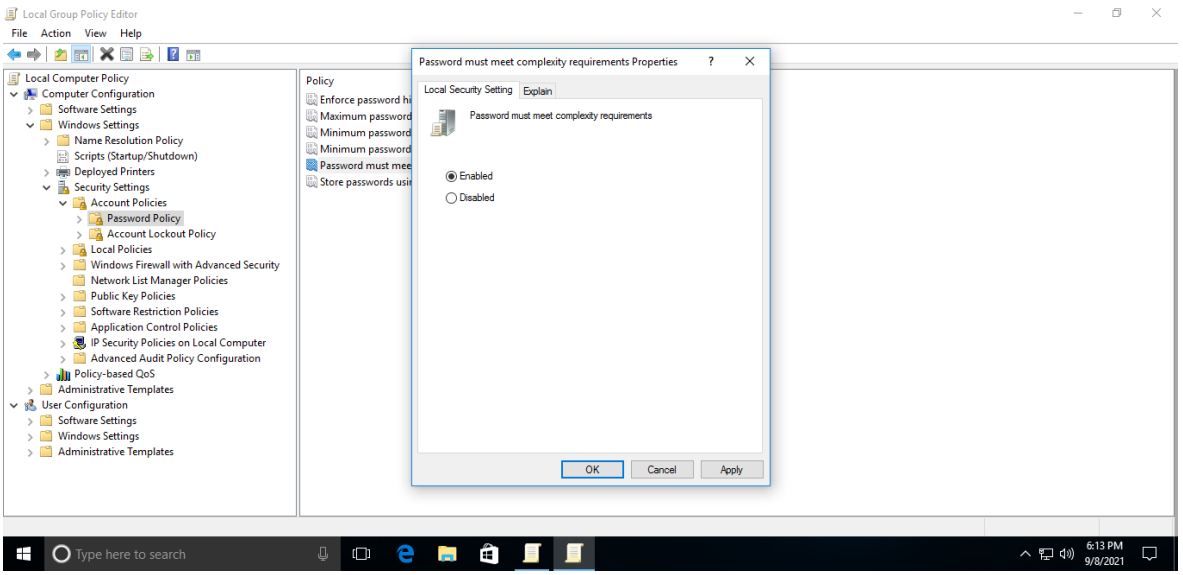
Answer

Windows + r -> gpedit.msc -> Computer Configuration -> Windows Setting -> Security Setting -> Account Policies -> Password Policy -> Password must meet complexity requirements diubah menjadi enabled -> Apply

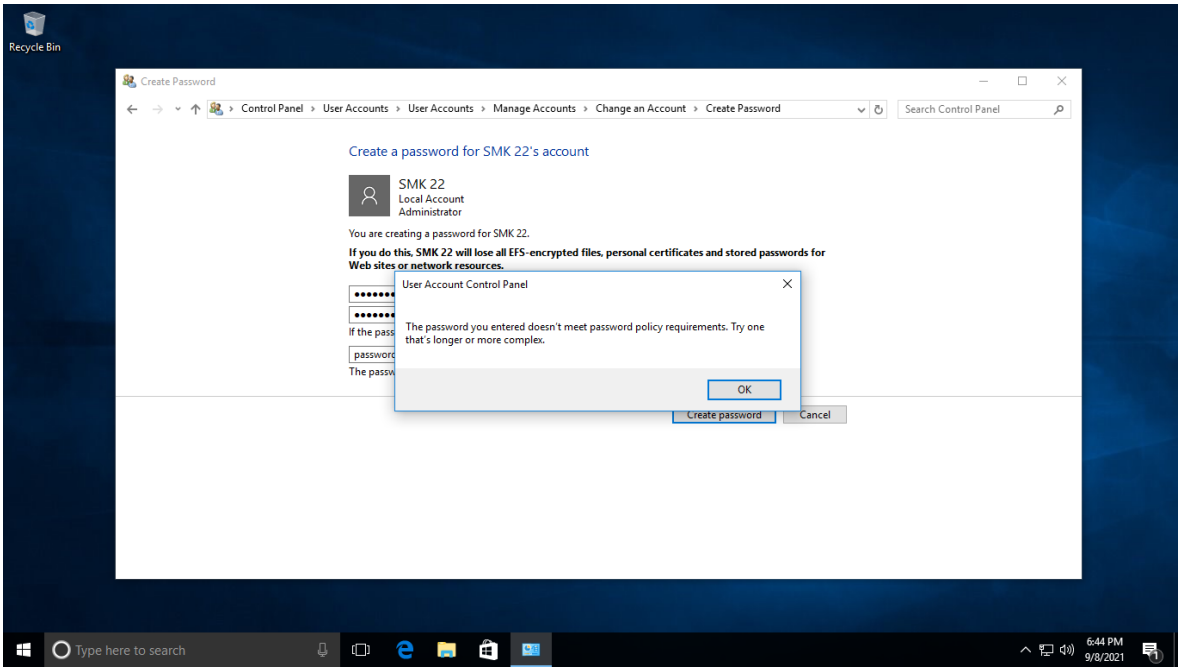
ScrenShoot

Masukan screenshot penyelesaian

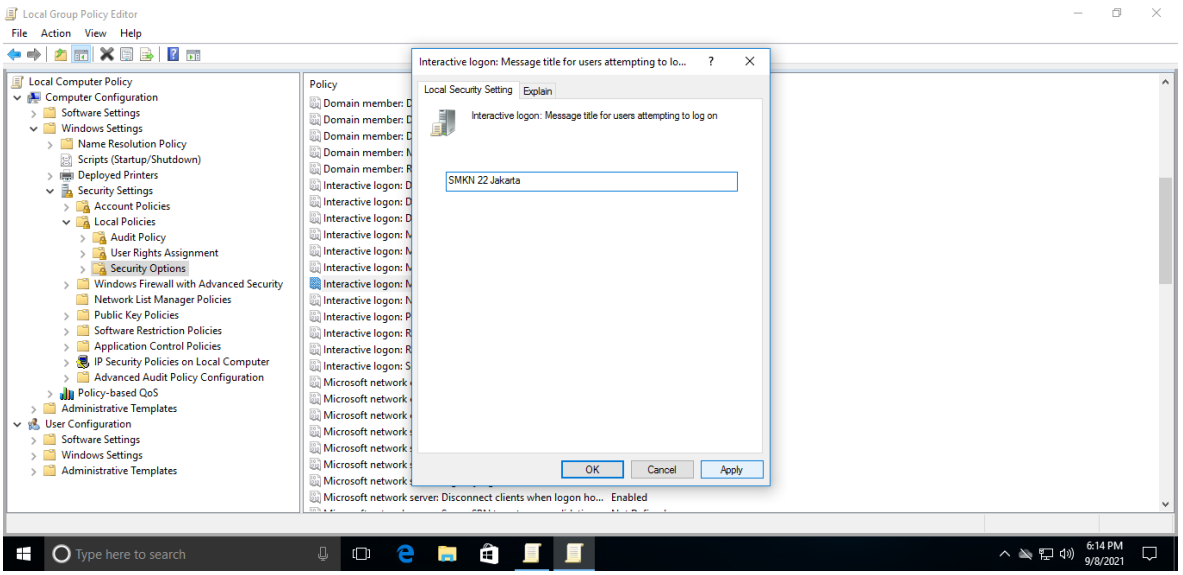
1.



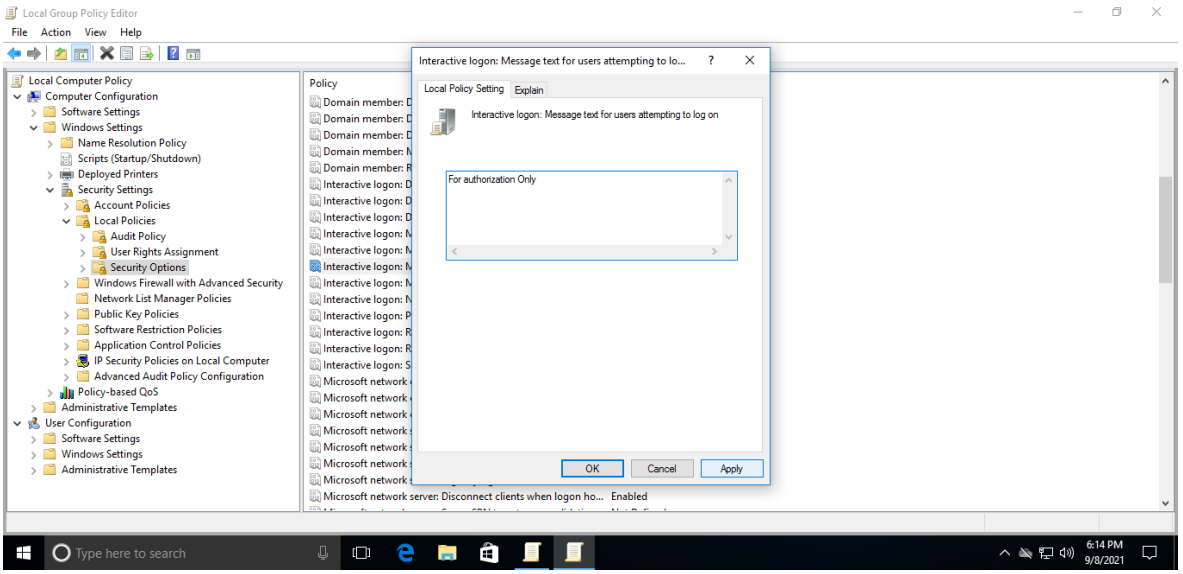
2.


Recycle Bin
Create Password
Control Panel › User Accounts › User Accounts › Manage Accounts › Change an Account › Create Password
Search Control Panel
Create a password for SMK 22's account
SMK 22
Local Account
Administrator
You are creating a password for SMK 22.
If you do this, SMK 22 will lose all EFS-encrypted files, personal certificates and stored passwords for Web sites or network resources.
User Account Control Panel
The password you entered doesn't meet password policy requirements. Try one that's longer or more complex.
OK
Create password
Cancel
Type here to search
6:44 PM
9/8/2021

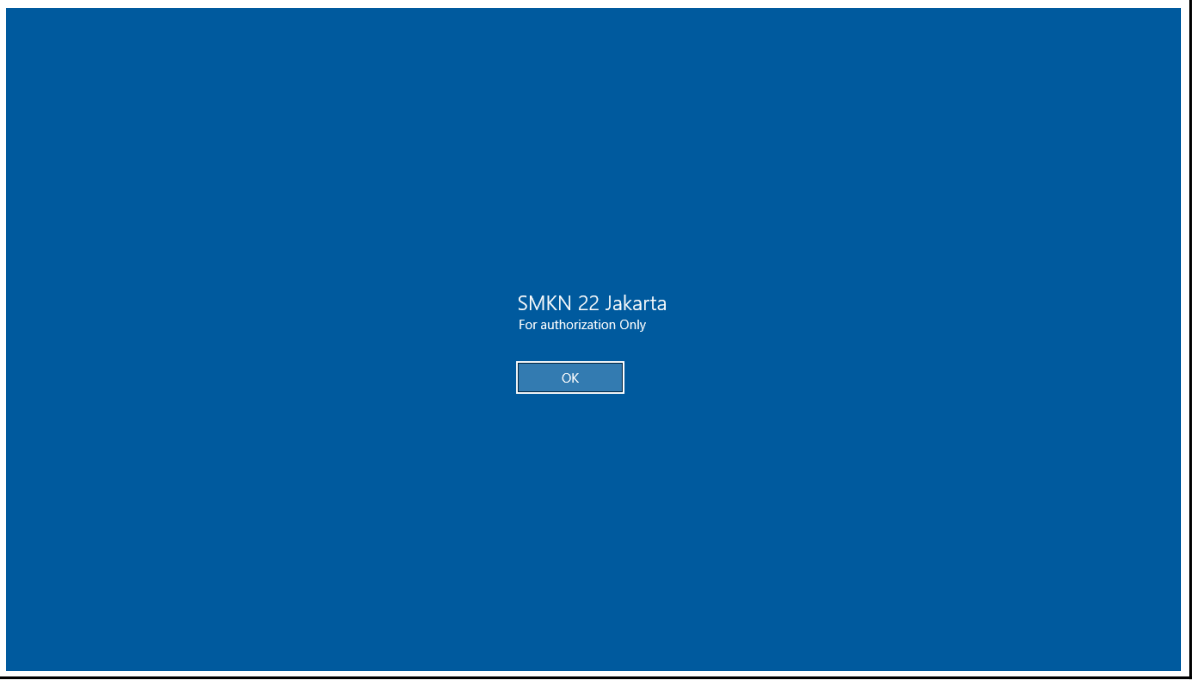
3. **Security Banner**

Challenge : On random windows machine go to login sreen
Windows 10 mempunyai fitur untuk menambahkan pesan yang ditampilkan di layar saat pengguna masuk. Untuk memberikan pesan bagi pengguna yang masuk ke komputer Windows 10 yang akan masuk/login. Pesan tersebut bersifat informatif dan tidak memberikan keamanan yang sebenarnya. Buatlah Security Banner Pesan sebelum login ke Komputer Windows 10
Answer
Windows + r -> gpedit.msc -> Computer Configuration -> Windows Setting -> Security Setting -> Local Policies -> Security Options -> lalu ubah dibagian Interactive logon: Message title for users attempting to log on dan Interactive logon: Message text for users attempting to log on Message Title : untuk dibagian title nya Message text : untuk dibagian bawah dari title nya
ScrenShoot
Masukan screenshot penyelesaian 1. 

2.


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Policy
Interactive logon: Message text for users attempting to lo...
Local Policy Setting
Explain
Interactive logon: Message text for users attempting to log on
For authorization Only
OK
Cancel
Apply
Microsoft network server: Disconnect clients when logon ho... Enabled
Type here to search
6:14 PM
9/8/2021

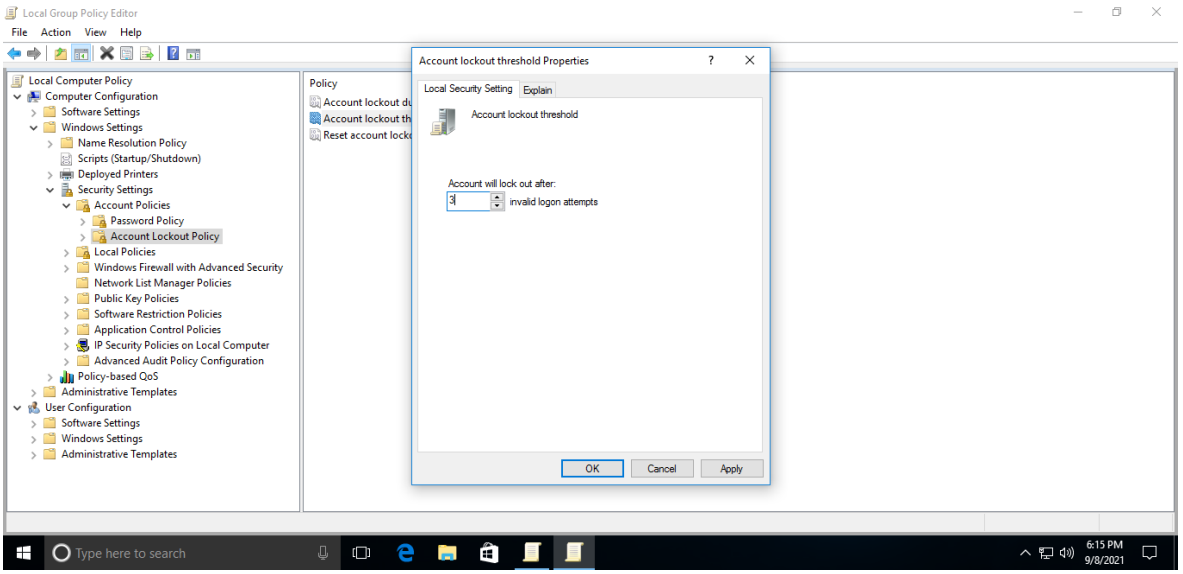
2.


SMKN 22 Jakarta
For authorization Only
OK

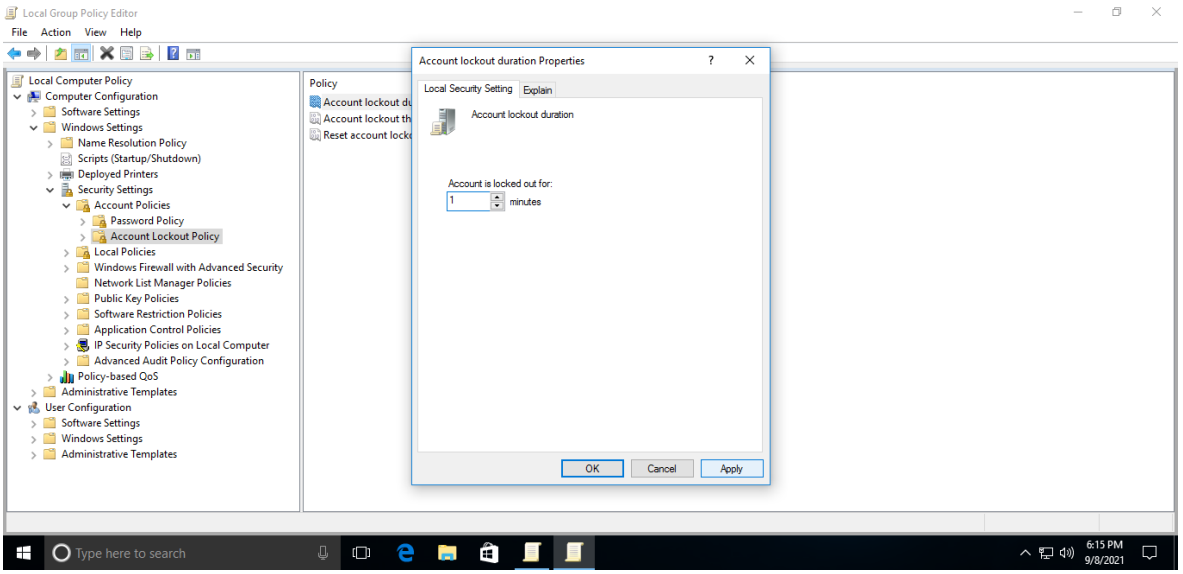
1. **Locked Failed Login**

Challenge : Try to 3 failed login and device locked 1 minute
Pengaturan kebijakan ambang penguncian akun menentukan jumlah upaya masuk yang gagal yang akan menyebabkan akun pengguna dikunci. Akun yang dikunci tidak dapat digunakan hingga Anda menyetel ulang atau hingga jumlah menit yang ditentukan oleh setelan kebijakan durasi penguncian Akun kedaluwarsa. Anda dapat menetapkan nilai dari 1 hingga 999 upaya masuk yang gagal, atau Anda dapat menentukan bahwa akun tidak akan pernah dikunci dengan menyetel nilai ke 0. Jika ambang penguncian akun diatur ke angka yang lebih besar dari nol, durasi penguncian akun harus lebih besar dari atau sama dengan nilai Reset penghitung penguncian akun setelahnya. Pengaturan kebijakan durasi penguncian akun menentukan jumlah menit agar akun yang terkunci tetap terkunci sebelum dibuka secara otomatis. Kisaran yang tersedia adalah dari 1 hingga 99.999 menit. Nilai 0 menentukan bahwa akun akan dikunci sampai administrator secara eksplisit membukanya. Jika ambang penguncian akun diatur ke angka yang lebih besar dari nol, durasi penguncian akun harus lebih besar dari atau sama dengan nilai penghitung ulang penguncian akun setelahnya. Pengaturan kebijakan ini tergantung pada pengaturan kebijakan ambang penguncian akun yang ditentukan, dan harus lebih besar dari atau sama dengan nilai yang ditentukan untuk penghitung ulang penguncian akun setelah pengaturan kebijakan. Fitur untuk mencegah brute-force login pada Windows 10
Answer
Windows + r -> gpedit.msc -> Computer configuration -> Windows Setting -> Security Setting -> Account Policies -> Account lockout policy -> Account lockout threshold diubah menjadi 3 dan Account lockout duration diubah menjadi 1 minutes -> Apply
ScrenShoot
Masukan screenshot penyelesaian

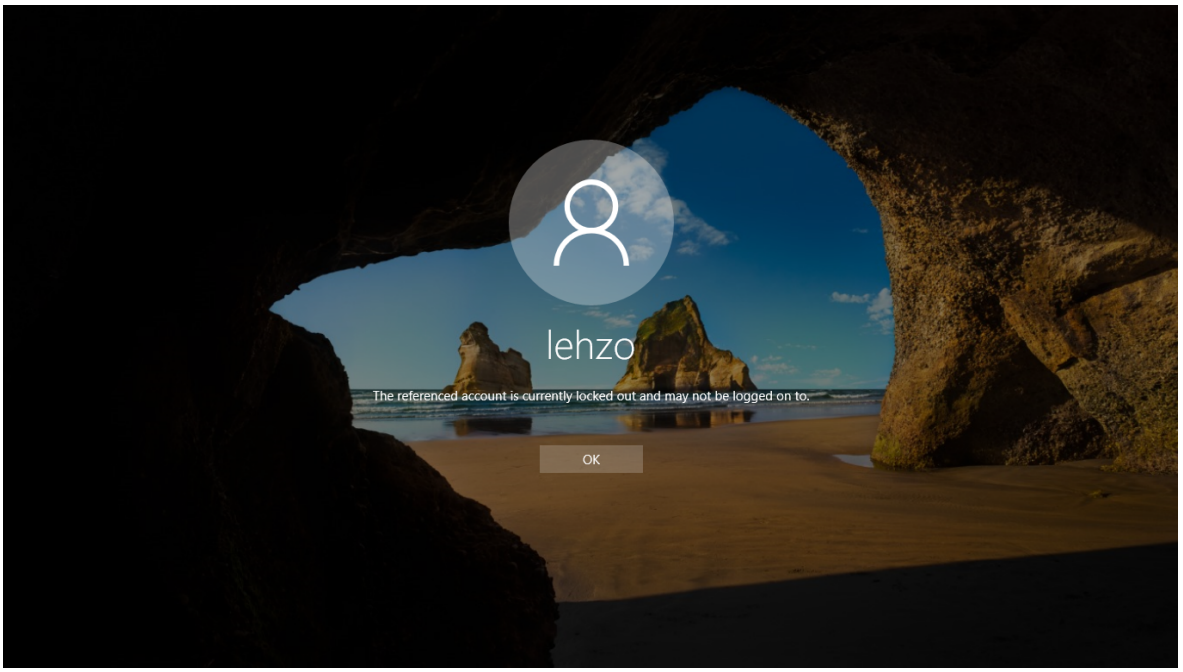
1.


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Policy
Account lockout threshold Properties
Local Security Setting
Explain
Account lockout threshold
Account will lock out after:
3
invalid logon attempts
OK
Cancel
Apply
Type here to search
6:15 PM
9/8/2021

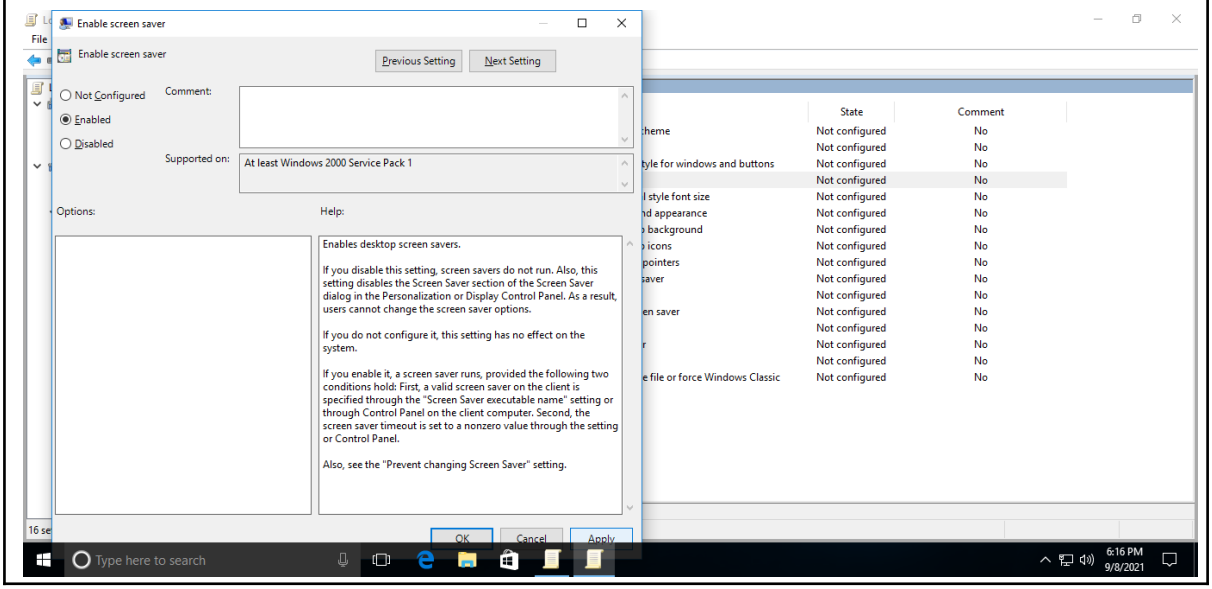
2.


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Policy
Account lockout duration Properties
Local Security Setting
Explain
Account lockout duration
Account is locked out for:
1
minutes
OK
Cancel
Apply
Type here to search
6:15 PM
9/8/2021

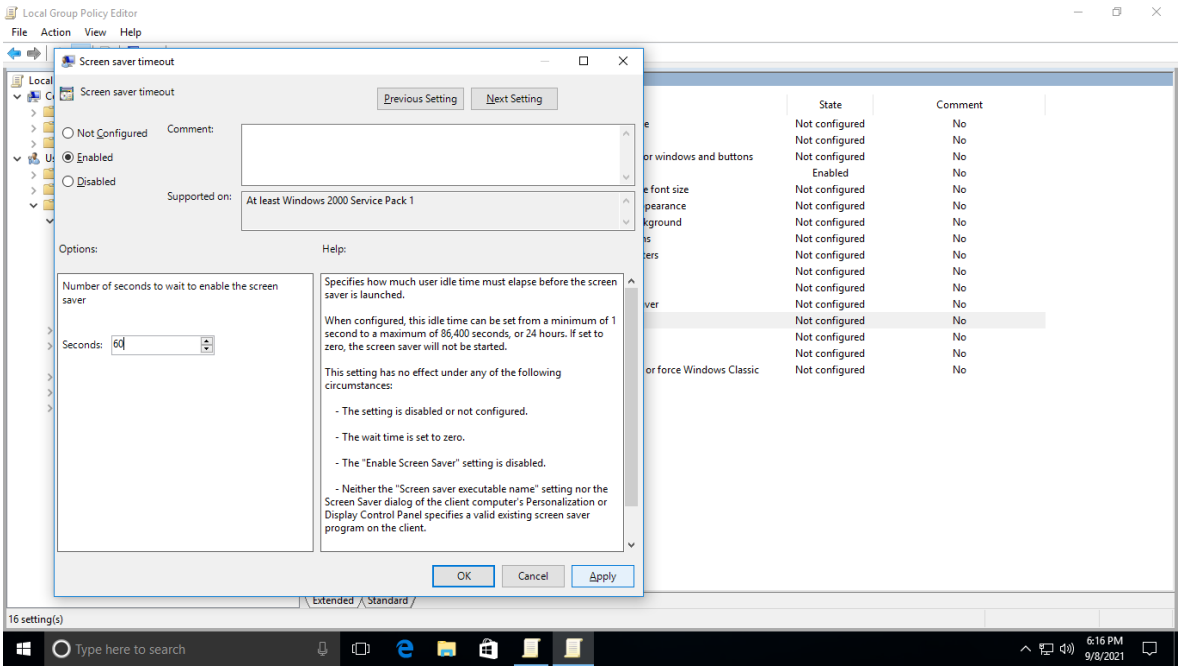
3.


lehzo
The referenced account is currently locked out and may not be logged on to.
OK

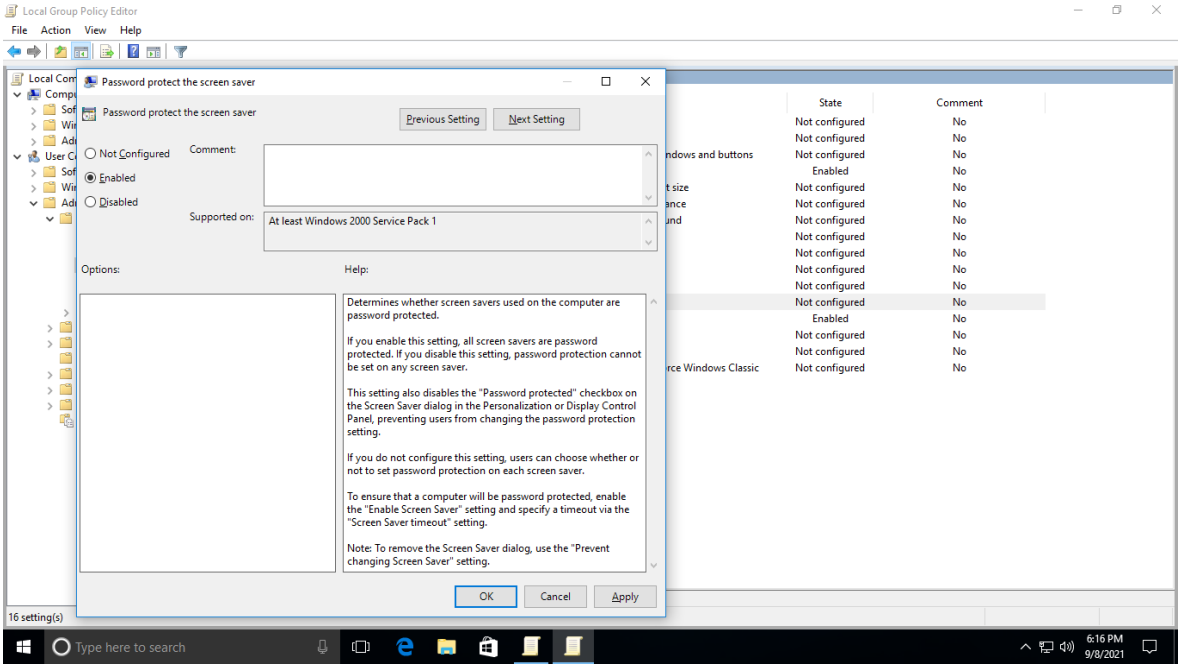
2. **Inactive timeout**

Challenge : Inactive for 1 minute then device locked
Windows memperhatikan tidak aktifnya sesi masuk, dan jika jumlah waktu tidak aktif melebihi batas tidak aktif, maka screen saver akan berjalan, mengunci sesi
Answer
Windows + r -> gpedit.msc -> User configuration -> Administrative Template -> Control Panel -> Personalization -> ada 3 yang perlu diubbah : Enable Screen Saver -> Enabled Password Protect The Server -> Enabled Screen Saver Timeout -> Enabled dan ubah number of second nya menjadi 60 second
ScrenShoot
Masukan screenshot penyelesaian 1. 

2.


Local Group Policy Editor
File Action View Help
Screen saver timeout
Screen saver timeout
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000 Service Pack 1
Options:
Help:
Number of seconds to wait to enable the screen saver
Seconds: 60
Specifies how much user idle time must elapse before the screen saver is launched.
When configured, this idle time can be set from a minimum of 1 second to a maximum of 86,400 seconds, or 24 hours. If set to zero, the screen saver will not be started.
This setting has no effect under any of the following circumstances:
- The setting is disabled or not configured.
- The wait time is set to zero.
- The "Enable Screen Saver" setting is disabled.
- Neither the "Screen saver executable name" setting nor the Screen Saver dialog of the client computer's Personalization or Display Control Panel specifies a valid existing screen saver program on the client.
OK
Cancel
Apply
State
Comment
Not configured
No
Enabled
Extended
Standard
16 setting(s)
Type here to search
6:16 PM
9/8/2021

3.


Local Group Policy Editor
File Action View Help
Password protect the screen saver
Password protect the screen saver
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows 2000 Service Pack 1
Options:
Help:
Determines whether screen savers used on the computer are password protected.
If you enable this setting, all screen savers are password protected. If you disable this setting, password protection cannot be set on any screen saver.
This setting also disables the "Password protected" checkbox on the Screen Saver dialog in the Personalization or Display Control Panel, preventing users from changing the password protection setting.
If you do not configure this setting, users can choose whether or not to set password protection on each screen saver.
To ensure that a computer will be password protected, enable the "Enable Screen Saver" setting and specify a timeout via the "Screen Saver timeout" setting.
Note: To remove the Screen Saver dialog, use the "Prevent changing Screen Saver" setting.
OK
Cancel
Apply
State
Comment
Not configured
No
Enabled
16 setting(s)
Type here to search
6:16 PM
9/8/2021

3. Cached logins (Windows machines)

Challenge : On random windows client machine - login with random account, logoff, shitdown vNIC, try to login again with the same account

Chaced Login ke computer Windows 10 kredensial akun tersimpan di cached Login system dari Windows 10.

Data cache disimpan dalam kunci registri HKLM\ SECURITY\Cache, yang hanya dapat diakses oleh akun SYSTEM. Penting juga untuk menyebutkan bahwa masa cache ini di komputer tidak terbatas.

Setting Security di cached login Windows 10 yang hanya memperbolehkan user yang terakhir yang hanya dapat login ke dalam Windows 10.

Secara teori, jika ada akses fisik ke komputer, penyerang memiliki kesempatan untuk menggunakan kredensial yang disimpan, disarankan untuk menonaktifkan cache lokal untuk keamanan yang lebih baik.
Setting Logons cached yang disimpan diatur ke nilai value 1.
Ini memungkinkan hanya pengguna terakhir untuk masuk ke sistem.

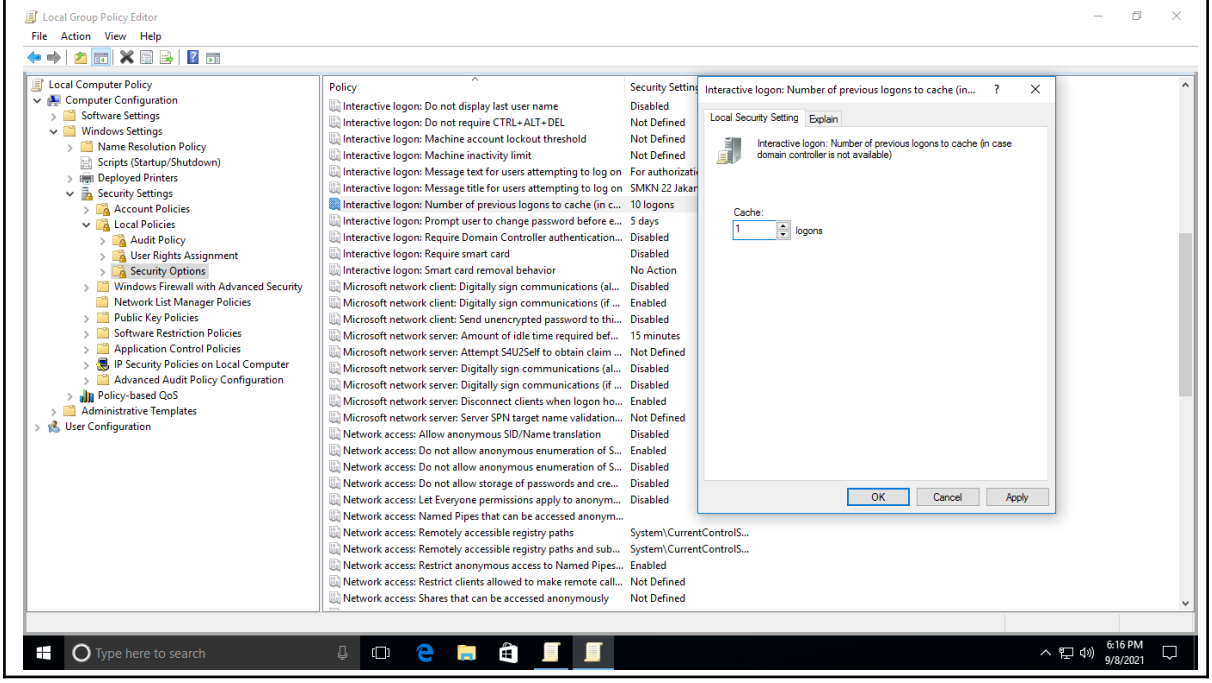
Answer

Windows + r -> gpedit.msc -> Computer configuration -> Windows Setting -> Security Setting -> Local Policies -> Security Options -> Interactive logon: Number of previous logons to cache diubah menjadi 1 -> Apply

ScrenShoot

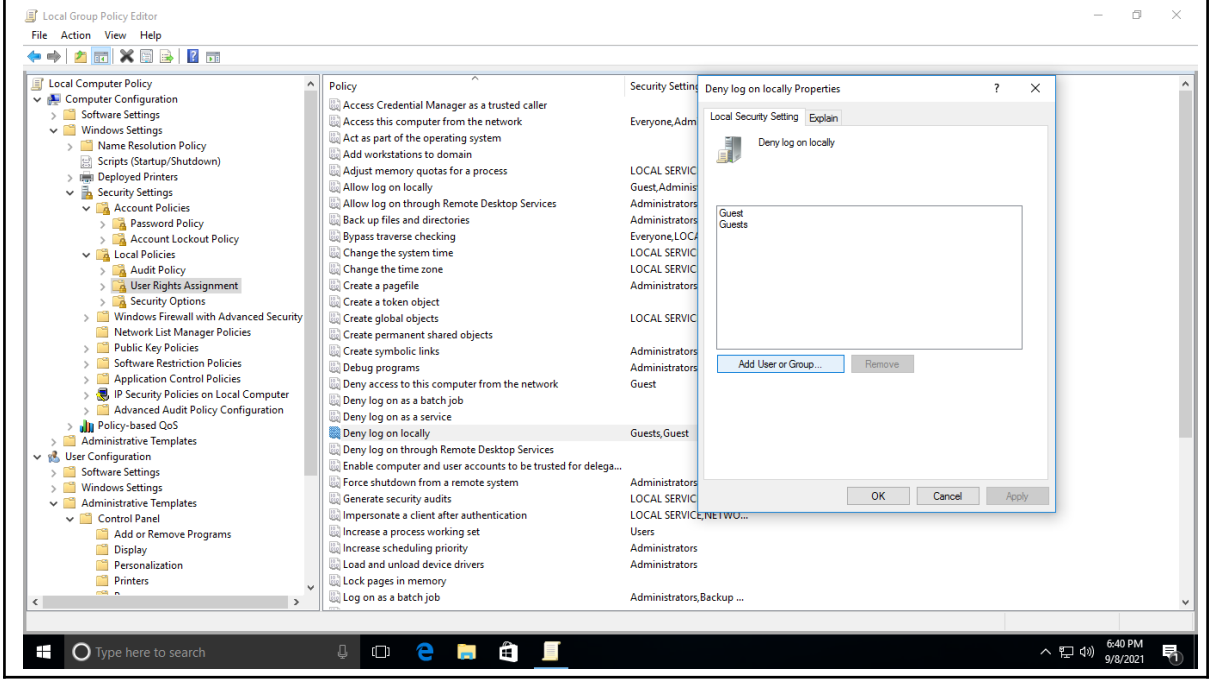
Masukan screenshot penyelesaian

1.

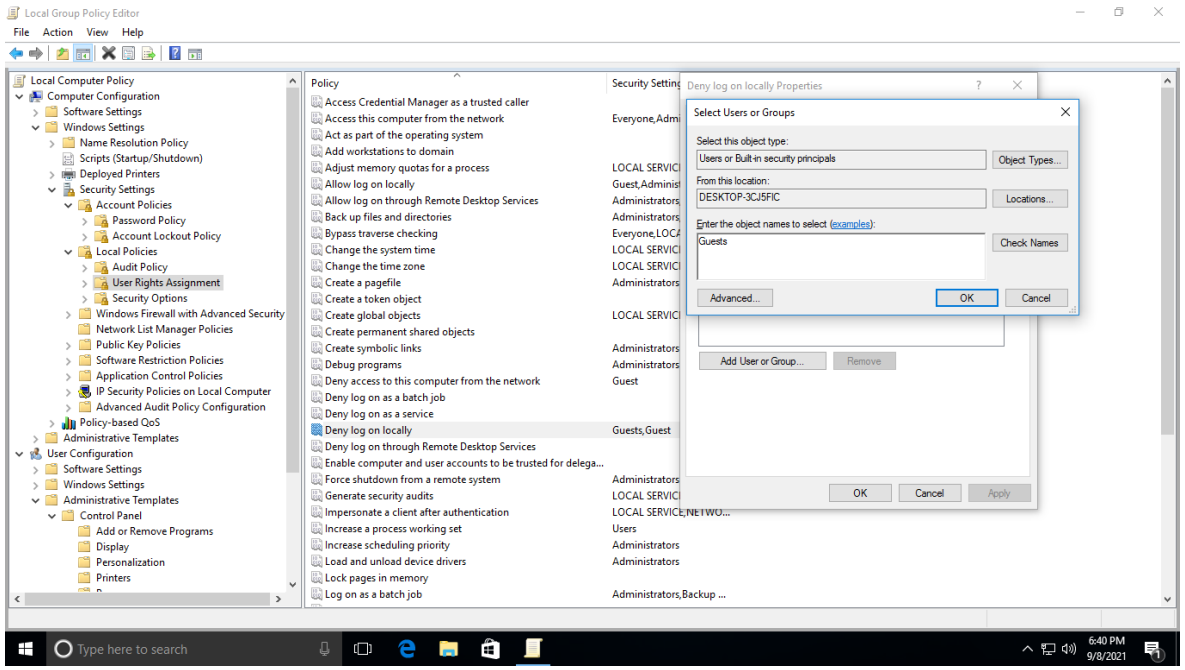


Tambahan Hardening

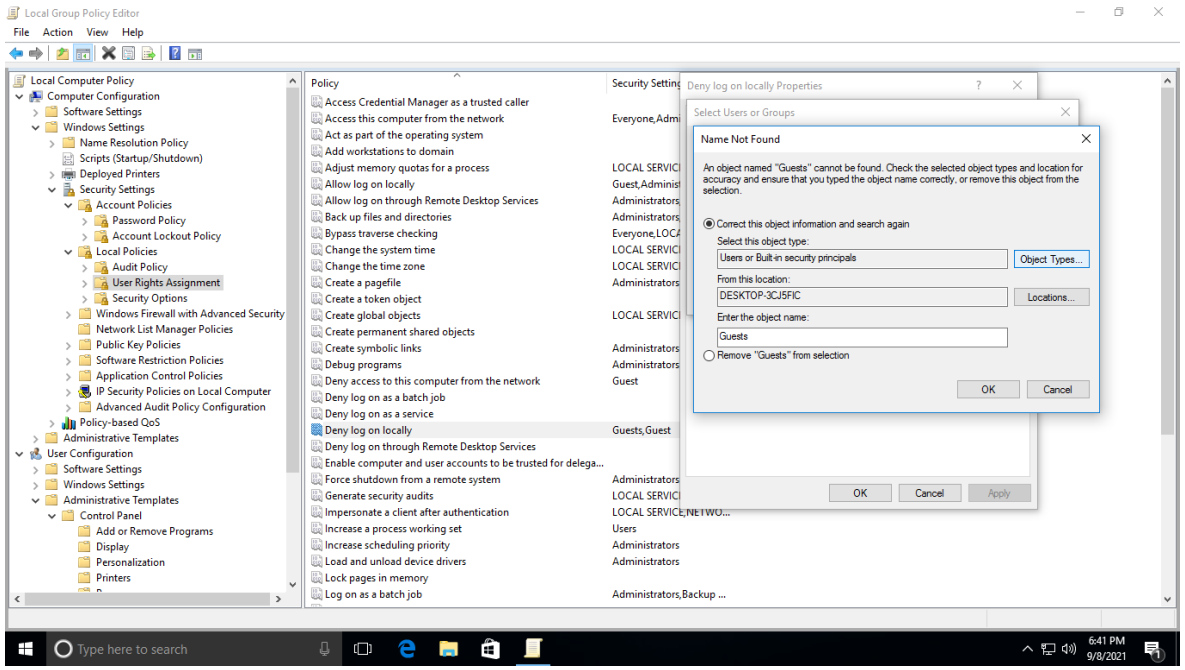
4. Disabled Account Guest log on localy

Challenge : Disabled Account Guests log on localy
Account guests adalah account yang memperbolehkan tamu untuk masuk ke dalam windows tanpa harus menggunakan akun utama jadi kita harus membuat account guests tidak dapat login secara local
Answer
Windows + r -> gpedit.msc -> Computer configuration -> Windows Setting -> Security Setting -> Local Policies -> User Rights Assigment -> Deny Log on Locally -> Add user or groups -> Masukkan nama object yang ingin dicari karena tadi yang dicari adalah guests maka kita tuliskan Guests -> Check Names -> Object types -> groups -> Ok -> Ok -> Apply
ScrenShoot
Masukan screenshot penyelesaian 1. 

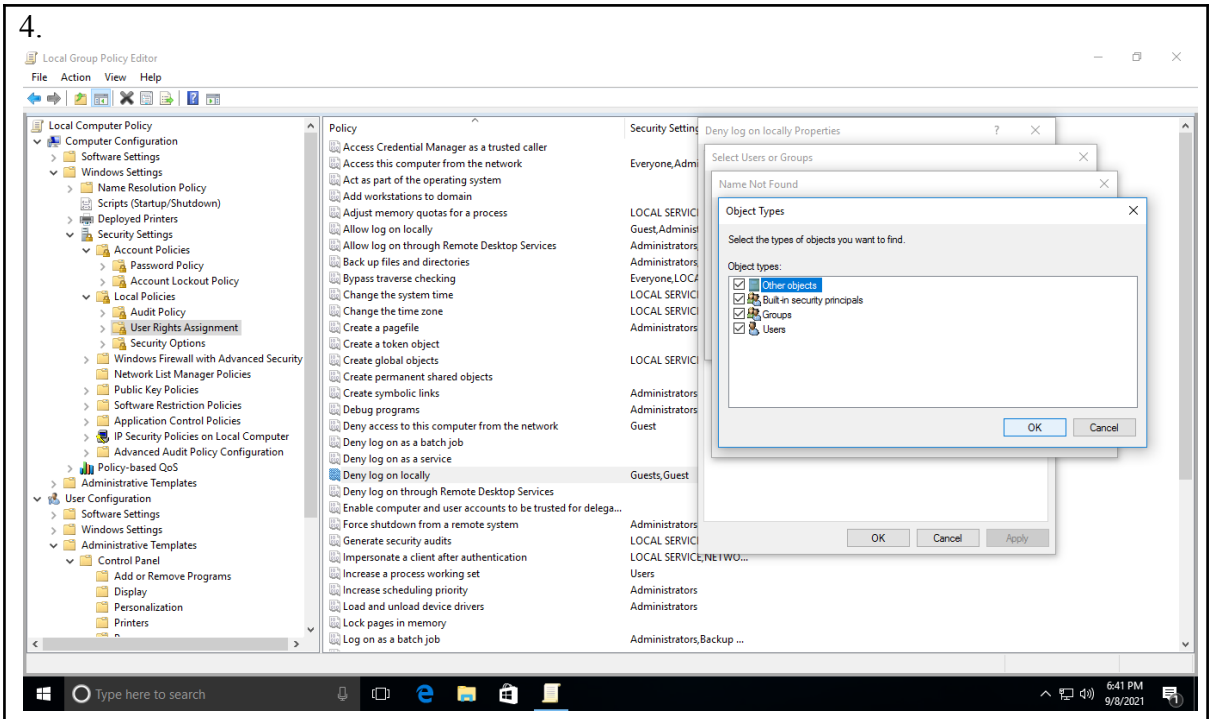
2.


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Add or Remove Programs
Display
Personalization
Printers
Policy
Security Setting
Access Credential Manager as a trusted caller
Access this computer from the network
Act as part of the operating system
Add workstations to domain
Adjust memory quotas for a process
Allow log on locally
Allow log on through Remote Desktop Services
Back up files and directories
Bypass traverse checking
Change the system time
Change the time zone
Create a pagefile
Create a token object
Create global objects
Create permanent shared objects
Create symbolic links
Debug programs
Deny access to this computer from the network
Deny log on as a batch job
Deny log on as a service
Deny log on locally
Deny log on through Remote Desktop Services
Enable computer and user accounts to be trusted for delega...
Force shutdown from a remote system
Generate security audits
Impersonate a client after authentication
Increase a process working set
Increase scheduling priority
Load and unload device drivers
Lock pages in memory
Log on as a batch job
Everyone,Admi
Guest,Administ
Everyone,LOCA
Guest
Guests,Guest
Users
Administrators,Backup ...
Deny log on locally Properties
Select Users or Groups
Select this object type:
Users or Built-in security principals
Object Types...
From this location:
DESKTOP-3CJ5FIC
Locations...
Enter the object names to select (examples):
Guests
Check Names
Advanced...
OK
Cancel
Add User or Group...
Remove
Apply
Type here to search
6:40 PM
9/8/2021

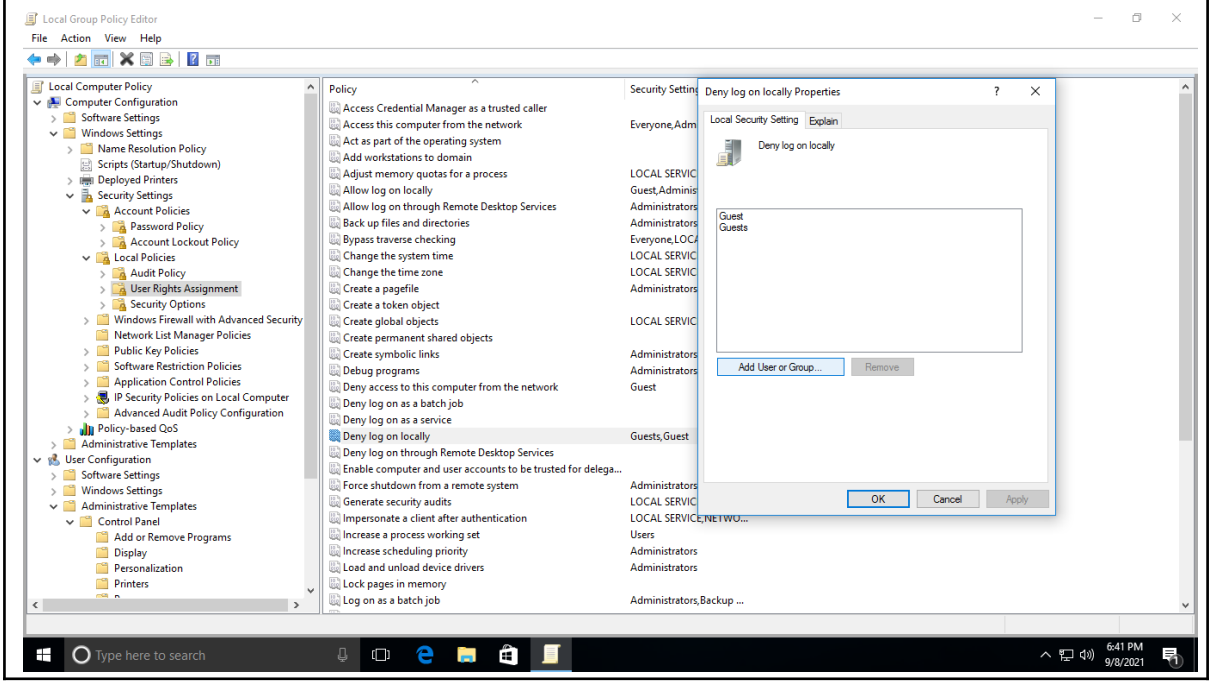
3.


Local Group Policy Editor
File Action View Help
Name Not Found
An object named "Guests" cannot be found. Check the selected object types and location for accuracy and ensure that you typed the object name correctly, or remove this object from the selection.
Correct this object information and search again
Select this object type:
Users or Built-in security principals
Object Types...
From this location:
DESKTOP-3CJ5FIC
Locations...
Enter the object name:
Guests
Remove "Guests" from selection
OK
Cancel
Type here to search
6:41 PM
9/8/2021

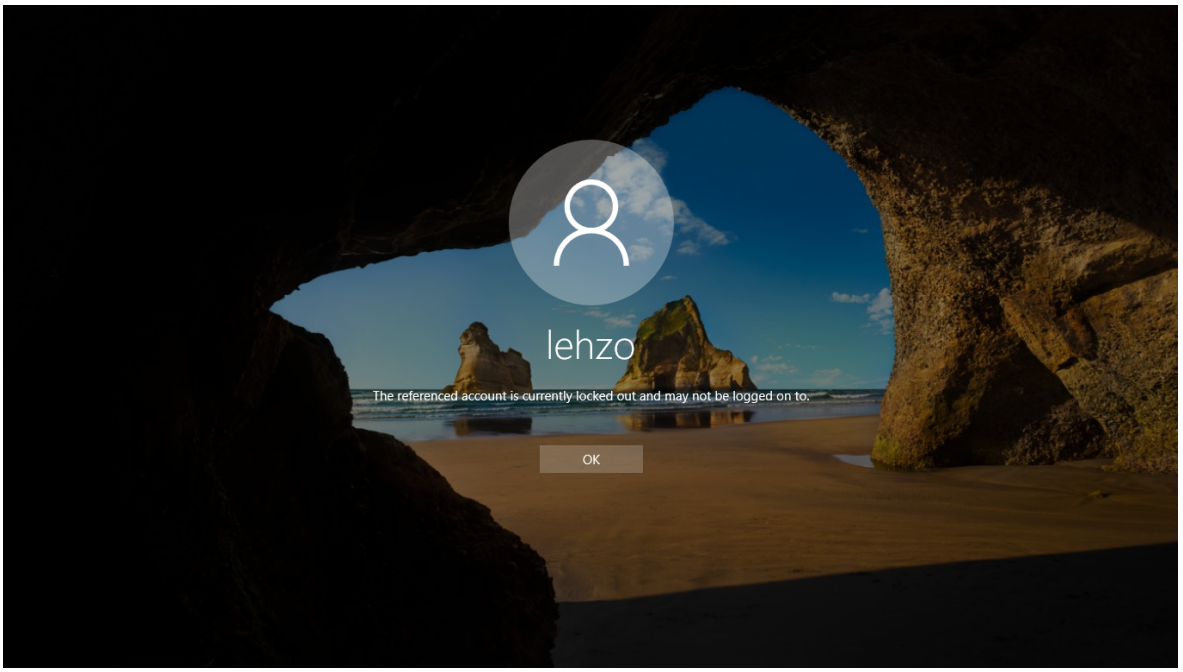
4.


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Add or Remove Programs
Display
Personalization
Printers
Policy
Security Setting
Access Credential Manager as a trusted caller
Access this computer from the network
Act as part of the operating system
Add workstations to domain
Adjust memory quotas for a process
Allow log on locally
Allow log on through Remote Desktop Services
Back up files and directories
Bypass traverse checking
Change the system time
Change the time zone
Create a pagefile
Create a token object
Create global objects
Create permanent shared objects
Create symbolic links
Debug programs
Deny access to this computer from the network
Deny log on as a batch job
Deny log on as a service
Deny log on locally
Deny log on through Remote Desktop Services
Enable computer and user accounts to be trusted for delega...
Force shutdown from a remote system
Generate security audits
Impersonate a client after authentication
Increase a process working set
Increase scheduling priority
Load and unload device drivers
Lock pages in memory
Log on as a batch job
Everyone,Adm
Guest,Administ
Everyone,LOCA
Guest
Guests,Guest
Users
Administrators,Backup ...
Deny log on locally Properties
Select Users or Groups
Name Not Found
Object Types
Select the types of objects you want to find.
Object types:
Other objects
Built-in security principals
Groups
Users
OK
Cancel
Apply
Type here to search
6:41 PM
9/8/2021

5.


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Add or Remove Programs
Display
Personalization
Printers
Policy
Security Setting
Access Credential Manager as a trusted caller
Access this computer from the network
Act as part of the operating system
Add workstations to domain
Adjust memory quotas for a process
Allow log on locally
Allow log on through Remote Desktop Services
Back up files and directories
Bypass traverse checking
Change the system time
Change the time zone
Create a pagefile
Create a token object
Create global objects
Create permanent shared objects
Create symbolic links
Debug programs
Deny access to this computer from the network
Deny log on as a batch job
Deny log on as a service
Deny log on locally
Deny log on through Remote Desktop Services
Enable computer and user accounts to be trusted for delega...
Force shutdown from a remote system
Generate security audits
Impersonate a client after authentication
Increase a process working set
Increase scheduling priority
Load and unload device drivers
Lock pages in memory
Log on as a batch job
Everyone,Adm
Guest,Administ
Everyone,LOCA
Guest
Guests,Guest
Users
Administrators,Backup ...
Deny log on locally Properties
Local Security Setting
Explain
Deny log on locally
Guest
Guests
Add User or Group...
Remove
OK
Cancel
Apply
Type here to search
6:41 PM
9/8/2021

6.


lehzo
The referenced account is currently locked out and may not be logged on to.
OK