

-Windows Hardening Essentials-

Checklist:

User Authorization:

- Remove Unauthorized Users ☐
- Examine User Permissions ☐
- Change Default user Passwords ☐
- Disable Guest Account ☐

Malware Scanning:

- Download Malware Bytes (scan regularly) ☐
- Check Windows Defender (Turn on/update) ☐
- Schedule Re-Occurring Scans ☐

Examine System:

- Check Task Manager for background tasks ☐
- Check scheduled tasks ☐
- Check/remove unwanted services ☐
- Browse file system for malware ☐
- Check for Windows updates ☐

Group Policy Objects:

- Create Group Password Policy ☐

Firewall Security:

- Turn on firewall
- Check in-bound/out-bound ports ☐
- Update firewall settings ☐

Helpful Ps Commands

(Read from file)

```
PS C:\> Get-Content -TotalCount 5 /PS/Names.txt
```

(Write to a file)

```
PS C:\> Set-Content - Value "Rachel Rose" -Path /PS/Names.txt
```

(create new folder)

```
New-Item -Path 'C:\temp\Test Folder' -ItemType Directory
```

(create new file)

```
New-Item -Path 'C:\temp\Test Folder\file.txt' -ItemType File
```

(execution policy)

```
Get-ExecutionPolicy
```

```
Set-ExecutionPolicy <unrestricted/restricted>
```

(list all services on system)

```
Get-Service
```

(view/alter processes)

```
Get-Process
```

```
Stop-Process
```

(view event logs)

```
Get-EventLog
```

(test network connection)

```
Test-NetConnection
```

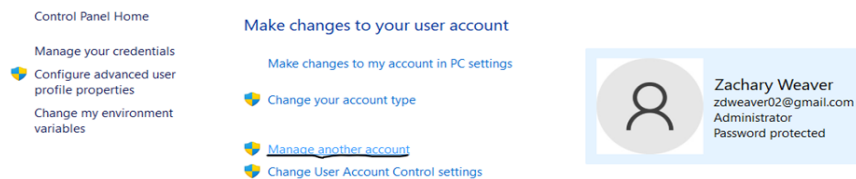
(verify port open/closed)

```
Test-NetConnection -ComputerName 127.0.0.1 -Port 4000
```

-User Authentication-

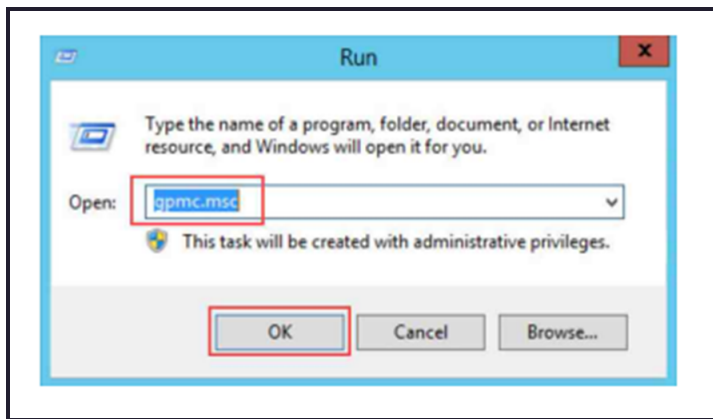
Control Panel > User Accounts > Manage another account (admin)

(from here remove/disable any unauthorized users, change passwords, etc.)



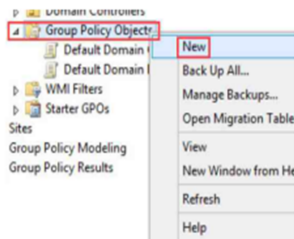
-Group Policy (windows Server)-

Windows start > run terminal > gpmmc.msc

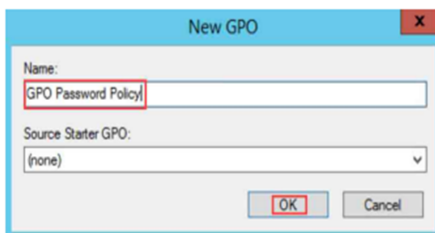


Create new group policy object:

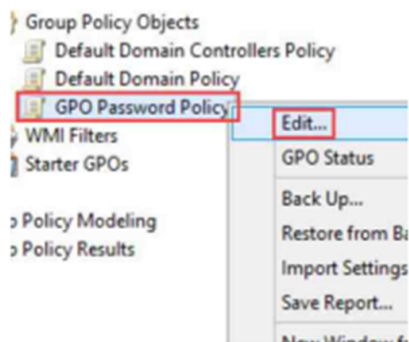
1. In the *Group Policy Management Center*, right-click **Group Policy Object** **New**.



2. Type **GPO Password Policy** into the *Name* field and click **OK**.



Set a new password policy: Group Policy Objects > Select policy > right click > edit



(computer config > policies > Windows Settings > security settings > Password policy)

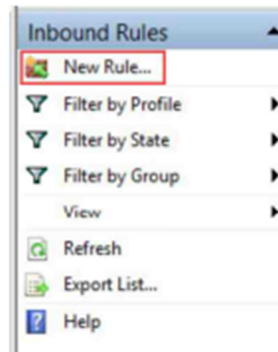
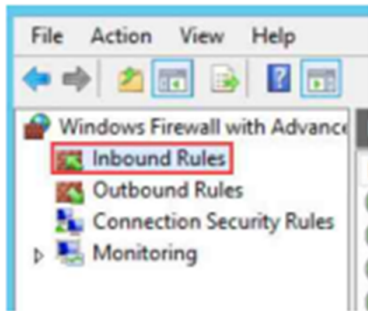
Enforcing Password Requirements:

Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	Not Defined
Password must meet complexity requirements	Not Defined
Store passwords using reversible encryption	Not Defined

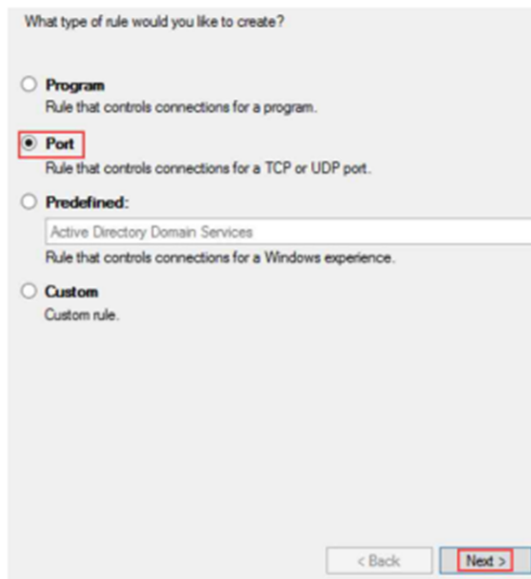
-Port Security-

Creating firewall rule

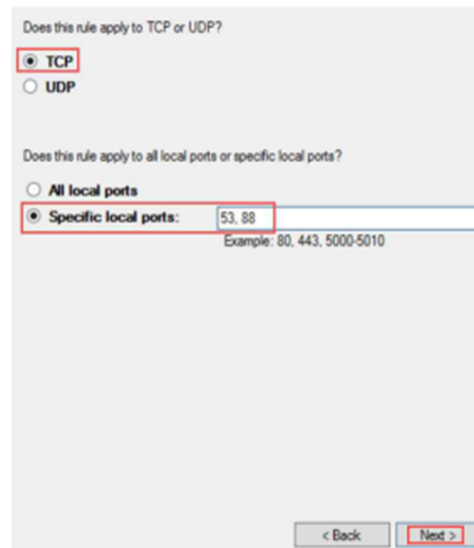
Open Windows Firewall > advanced settings > Inbound Rules > New Rule



Select Rule Type:



Specify What ports:



Select What action to be taken, add a rule name > Finish

What action should be taken when a connection matches the specified conditions?

☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection S Rule node.
[Customize...](#)

☒ **Block the connection**

< Back Next >

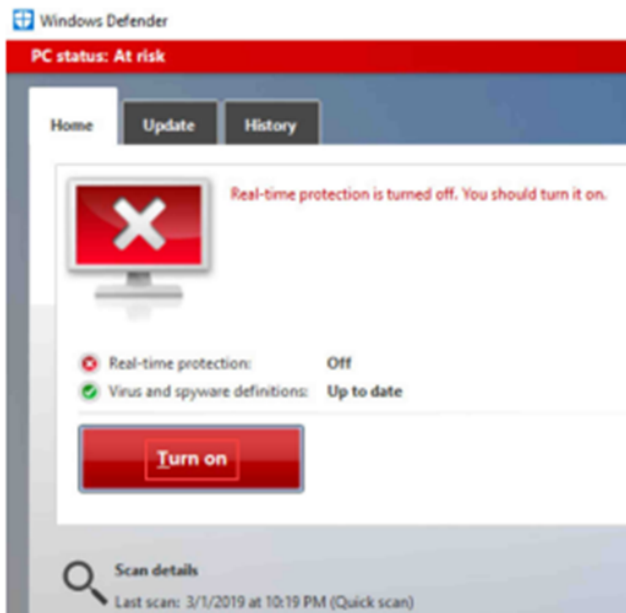
Name:

Description (optional):

< Back Finish

-Windows Defender Policies-

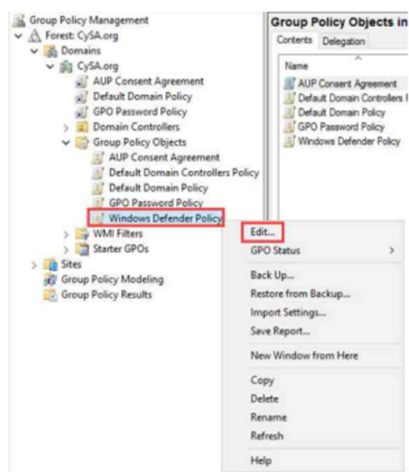
1. Open windows defender/turn on/update



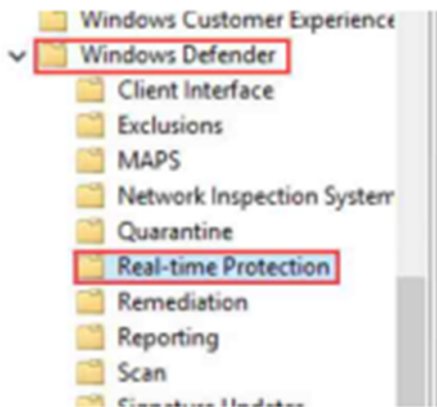
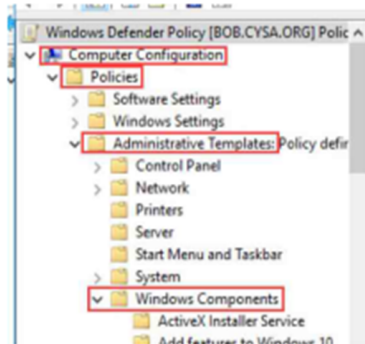
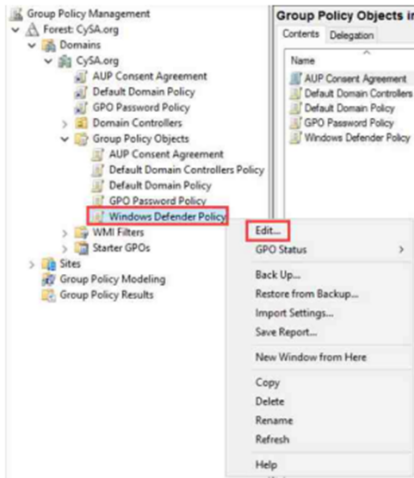
2. Real time protection - scanning downloads/documents

-group policy

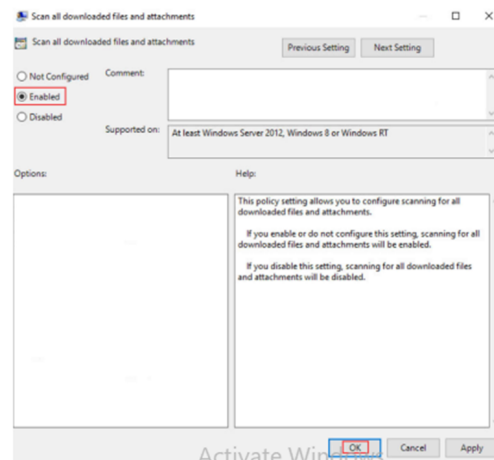
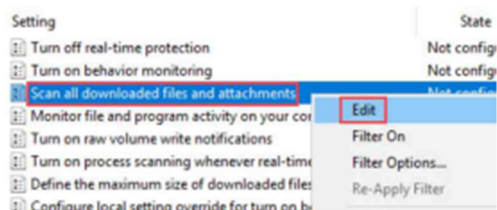
-create new policy “windows defender”



- Computer config > Policies > Admin Templates > windows components
- Windows defender > Real-time protection



- Right click on scan all downloaded files/attachments > edit
- Click enable to allow defender to scan downloads



Password Sheet

Machine:

IP Adress:

User	Password

Notes:

Password Sheet

Machine:

IP Adress:

User	Password

Notes:

Password Sheet

Machine:

IP Adress:

User	<i>Password</i>

Notes:

Password Sheet

Machine:

IP Adress:

User	Password

Notes: