

This tutorial aims to guide you to misconfigure various systems and services within the provided network topology to simulate a vulnerable environment for cybersecurity analysis.

Disable Security Features (Windows & Linux)

1. Disable Windows Security Features (Firewall, Antivirus, and Automatic Updates) in Windows Server 2022 & Windows 10 Client

a. Disable Windows Firewall

Open the Control Panel > System and Security > Windows Defender Firewall.

Click Turn Windows Defender Firewall on or off on the left.

Select Turn off Windows Defender Firewall for all network profiles (Domain, Private, Public).

Click OK.

b. Disable Windows Defender Antivirus

Go to Settings > Update & Security > Windows Security > Virus & Threat Protection.

Under Virus & Threat Protection Settings, click Manage settings.

Turn off Real-time protection and Cloud-delivered protection.

c. Disable Automatic Updates:

Go to Settings > Update & Security > Windows Update > Advanced options.

Turn off all options under the Update Settings section (Pause updates, Download updates automatically, etc.).

You may also use Search options to search for the above to disable.

2. Disable Linux Security Features

a. Disable Firewall

Check if ufw (Uncomplicated Firewall) is active by running:

```
sudo ufw status
```

- If it's active, disable it with:

```
sudo ufw disable
```

b. Disable Automatic Updates

```
sudo nano /etc/apt/apt.conf.d/20auto-upgrades
```

Set both options to 0:

```
APT::Periodic::Update-Package-Lists "0";
```

```
APT::Periodic::Unattended-Upgrade "0";
```

```
sudo systemctl status unattended-upgrades
```

```
sudo systemctl stop unattended-upgrades.service
```

c. Configure SSH with Weak Settings

i. Install OpenSSH Server if not already installed:

```
sudo apt install openssh-server
```

ii. `sudo nano /etc/ssh/sshd_config`

Modify the following:

```
PermitRootLogin yes
```

```
PubkeyAuthentication no
```

```
PasswordAuthentication yes
```

```
ChallengeResponseAuthentication yes
```

iii. `sudo systemctl restart ssh`

d. Enable Telnet and FTP

i. Install Telnet

```
sudo apt install telnetd
```

ii. Install FTP (vsftpd)

```
sudo apt install vsftpd
```

iii. Edit the FTP configuration file:

```
sudo nano /etc/vsftpd.conf
```

Set `anonymous_enable=YES` to allow anonymous login.

```
sudo systemctl restart vsftpd
```

e. Vulnerable Web Applications (Bee Box Machine)

i. Configure Bee Box for Low Security Mode

Login to Bee Box using the default credentials.

Access the DVWA (Damn Vulnerable Web Application) via a web browser.

In DVWA, click on the DVWA Security tab.

Set the security level to Low.

Ensure that vulnerabilities such as SQL Injection, XSS, and File Inclusion are enabled by testing these in the various tools within DVWA.

3. For: Windows Server 2022 and Client

a. Open Group Policy Management Editor:

i. Run gpedit.msc from the Run dialog

ii. Navigate to Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy.

- Minimum password length: Set to 0 characters.

- Password must meet complexity requirements: Disabled.

- Enforce password history: 0 passwords remembered.

- Maximum password age: Set to 365 or never expires.

Hint: In a Domain Controller, find this in GPM in Tools. (Computer Configuration, Policies, Windows Settings, Security Settings, Account Policies, Password Policy)

b. Enable Insecure RDP Settings

i. Open System Properties by right-clicking on This PC and selecting Properties.

ii. Click Remote Settings on the left panel.

iii. Under Remote Desktop, select Allow remote connections to this computer.

iv. Uncheck the option that says, "Allow connections only from computers running Remote Desktop with Network Level Authentication (NLA)".

- v. Click Apply and OK.
- c. Misconfigure IIS and DNS Services for Exploitation
 - i. Open IIS Manager (inetmgr in the Run dialog).
 - ii. Select the server or website under Connections.
 - iii. In the middle pane, under IIS, double-click Directory Browsing.
 - iv. Click Enable on the right to allow directory browsing.
 - v. Go back to the main site properties, and under Authentication, ensure Anonymous Authentication is enabled.
 - vi. Open DNS Manager (dnsmgmt.msc).
 - vii. Right-click the DNS server and select Properties.
 - viii. Go to the Advanced tab.
 - ix. Check that Enable recursion is enabled, which can allow DNS amplification attacks.
 - x. Click Apply and OK.
- d. In Windows 10: Join the Domain, Disable Local Security Features, and Enable SMBv1
 - i. Right-click This PC and select Properties.
 - ii. Click Change settings next to Computer name.
 - iii. Click Change to rename the machine and join the domain.
 - iv. Enter the domain accb6000.local.
 - v. Provide weak credentials (e.g., username: student, password: password123).
 - vi. Restart the machine after joining the domain.
 - vii. Open Control Panel > Programs > Turn Windows features on or off.
 - viii. Scroll down to SMB 1.0/CIFS File Sharing Support.
 - ix. Check the box next to SMB 1.0/CIFS Server and click OK.
 - x. Restart the machine when prompted.

4. Validate Vulnerability Exposure

After completing the misconfigurations, validate that the vulnerabilities are exposed by:

- a. Accessing services like IIS and FTP anonymously.
- b. Setting up weak Passwords

