

# Cyber Security Internship Task 4: Firewall Setup and Testing

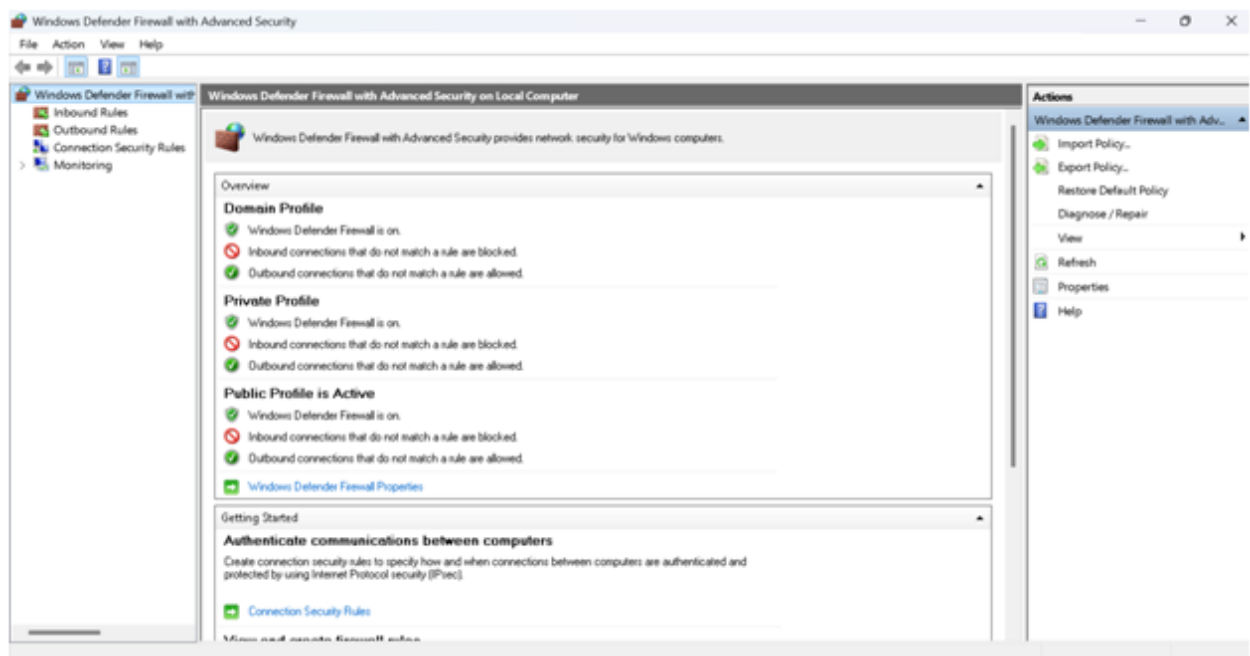
## Objective

Configure firewall rules to block Telnet (port 23) and allow SSH (port 22), test these rules, and restore the firewall to its original state. This task is performed on both Windows (using GUI) and Linux (using UFW).

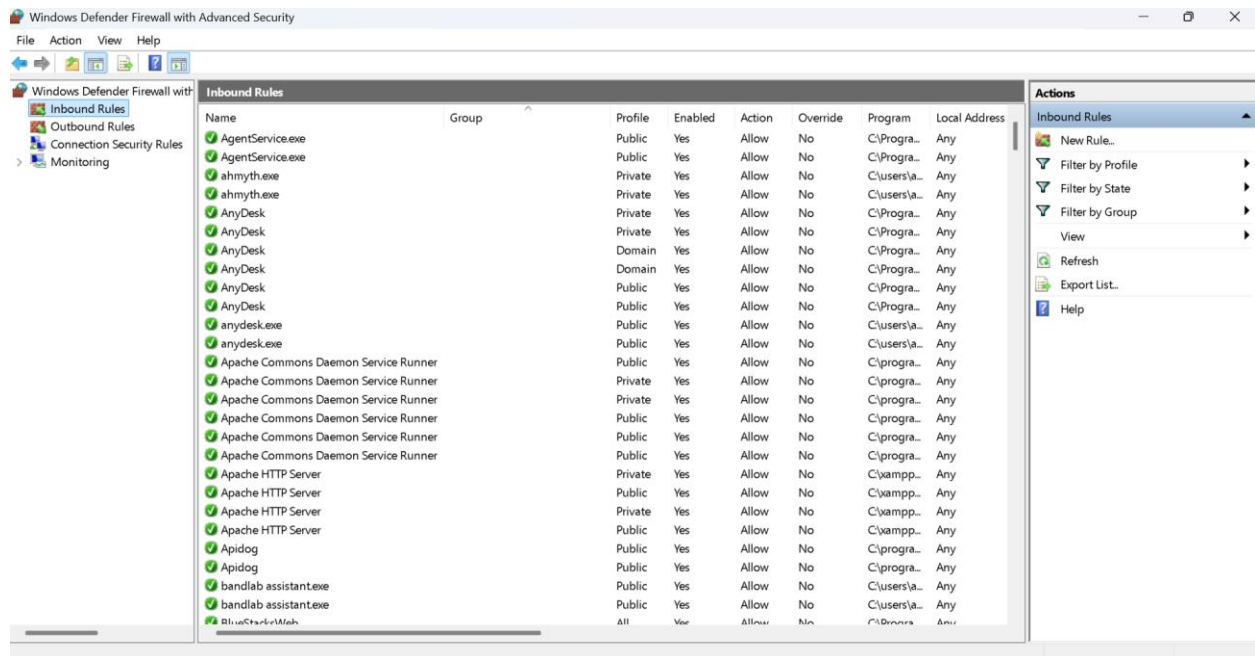
## Windows Firewall Configuration (Using GUI)

### Steps Performed:

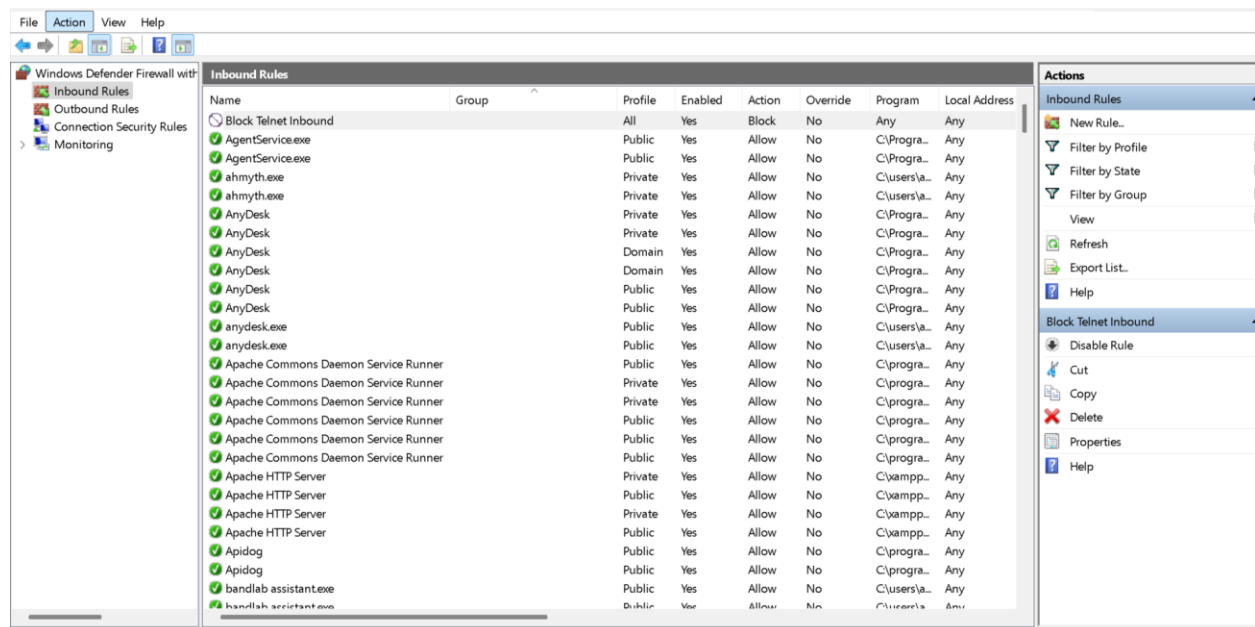
1. Opened **Windows Defender Firewall with Advanced Security** (`wf.msc`).



## 2. Viewed current inbound rules.



## 3. Created a new inbound rule to \*\*block TCP port 23 (Telnet)\*\*.

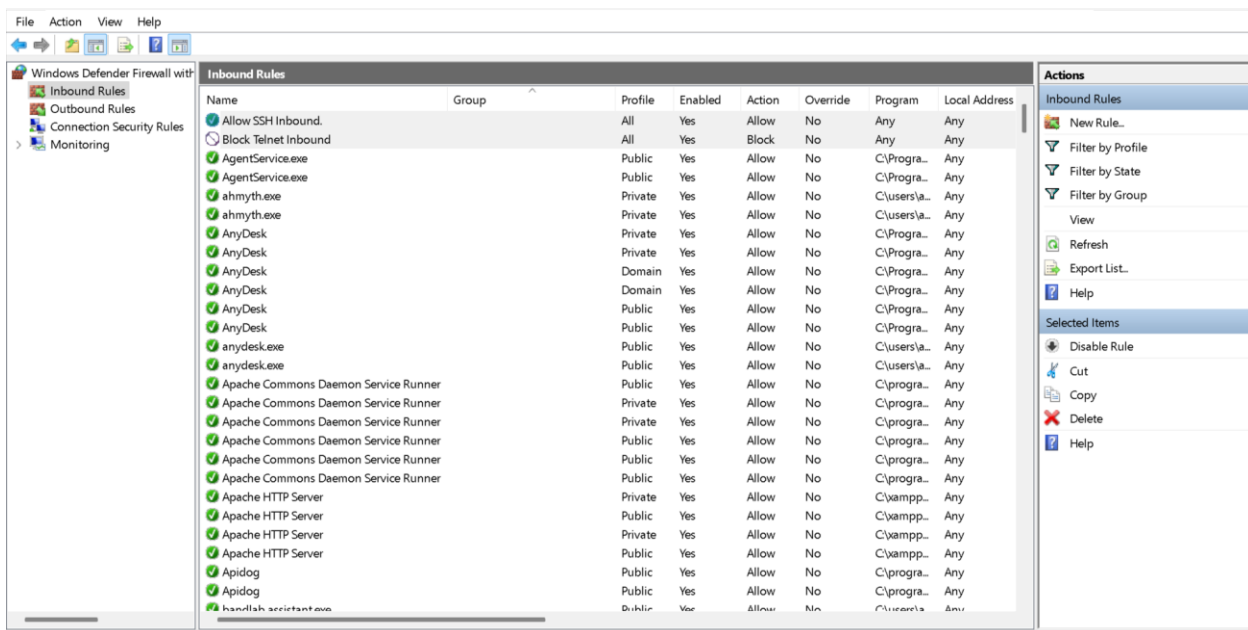


4. Tested Telnet connection to 192.168.56.101 on port 23 using Command Prompt. The connection failed, confirming the block.

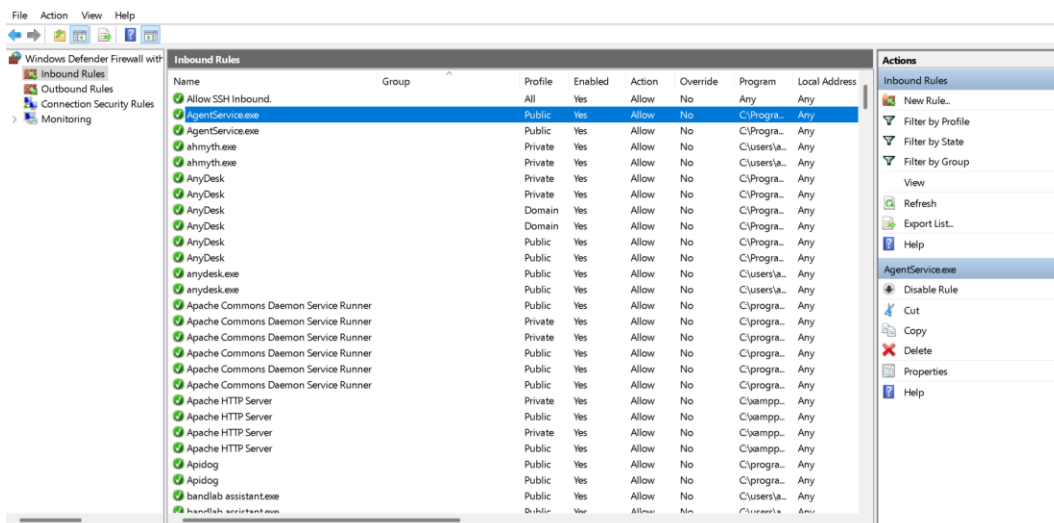
```
Administrator: Windows PowerShell

PS C:\WINDOWS\system32> telnet localhost 23
Connecting To localhost...Could not open connection to the host, on port 23: Connect failed
PS C:\WINDOWS\system32>
```

5. Created a new inbound rule to \*\*allow TCP port 22 (SSH)\*\* (optional if SSH server is present).



6. Removed the block rule on port 23 to restore the original state.



## Linux Firewall Configuration (Using UFW)

### Commands and Output:

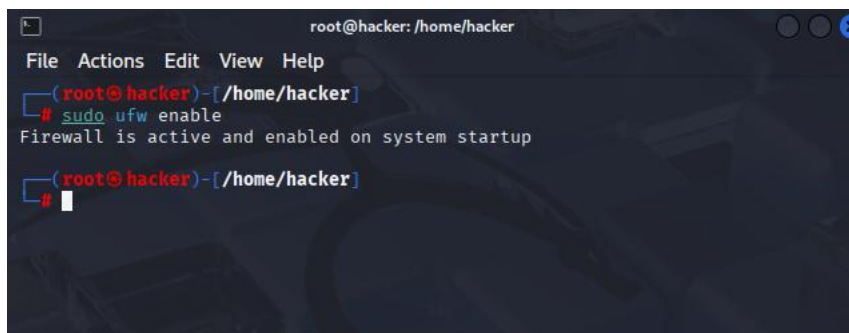
#### 1. Checked initial UFW status and rules:

```
bash
```

```
sudo ufw status verbose
```

#### 2. Enabled UFW firewall (if it was not enabled):

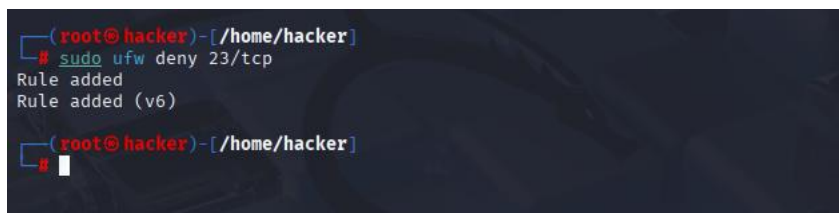
```
sudo ufw enable
```

A terminal window with a dark background and light blue text. The title bar shows 'root@hacker: /home/hacker'. The prompt is '(root@hacker)-[/home/hacker]'. The user enters 'sudo ufw enable'. The output is 'Firewall is active and enabled on system startup'. The prompt returns to '(root@hacker)-[/home/hacker]'.

```
(root@hacker)-[/home/hacker]  
# sudo ufw enable  
Firewall is active and enabled on system startup  
(root@hacker)-[/home/hacker]  
#
```

#### 3. Blocked inbound traffic on port 23 (Telnet):

```
sudo ufw deny 23/tcp
```

A terminal window with a dark background and light blue text. The title bar shows 'root@hacker: /home/hacker'. The prompt is '(root@hacker)-[/home/hacker]'. The user enters 'sudo ufw deny 23/tcp'. The output is 'Rule added' and 'Rule added (v6)'. The prompt returns to '(root@hacker)-[/home/hacker]'.

```
(root@hacker)-[/home/hacker]  
# sudo ufw deny 23/tcp  
Rule added  
Rule added (v6)  
(root@hacker)-[/home/hacker]  
#
```

#### 4. Tested Telnet connection to port 23 (expected to fail):

```
telnet 192.168.56.101 23
```

```
root@hacker: /home/hacker
File Actions Edit View Help
(root@hacker)-[/home/hacker]
# telnet 192.168.56.101 23
Trying 192.168.56.101 ...
telnet: Unable to connect to remote host: Connection refused

(root@hacker)-[/home/hacker]
#
```

## 5. Allowed inbound SSH port 22:

sudo ufw allow 22/tcp

```
(root@hacker)-[/home/hacker]
# sudo ufw allow 22/tcp
Rule added
Rule added (v6)

(root@hacker)-[/home/hacker]
#
```

## 6. Verified final UFW status showing all rules:

sudo ufw status verbose

```
(root@hacker)-[/home/hacker]
# sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22/tcp ALLOW IN Anywhere
22/tcp (v6) ALLOW IN Anywhere (v6)

Security Tip: If this is a fresh Kali or Debian system, the default is to deny all incoming connections, so all ports may be open unless a rule is added to allow them.
```