

# Elevate Labs (Cyber-Security Internship)

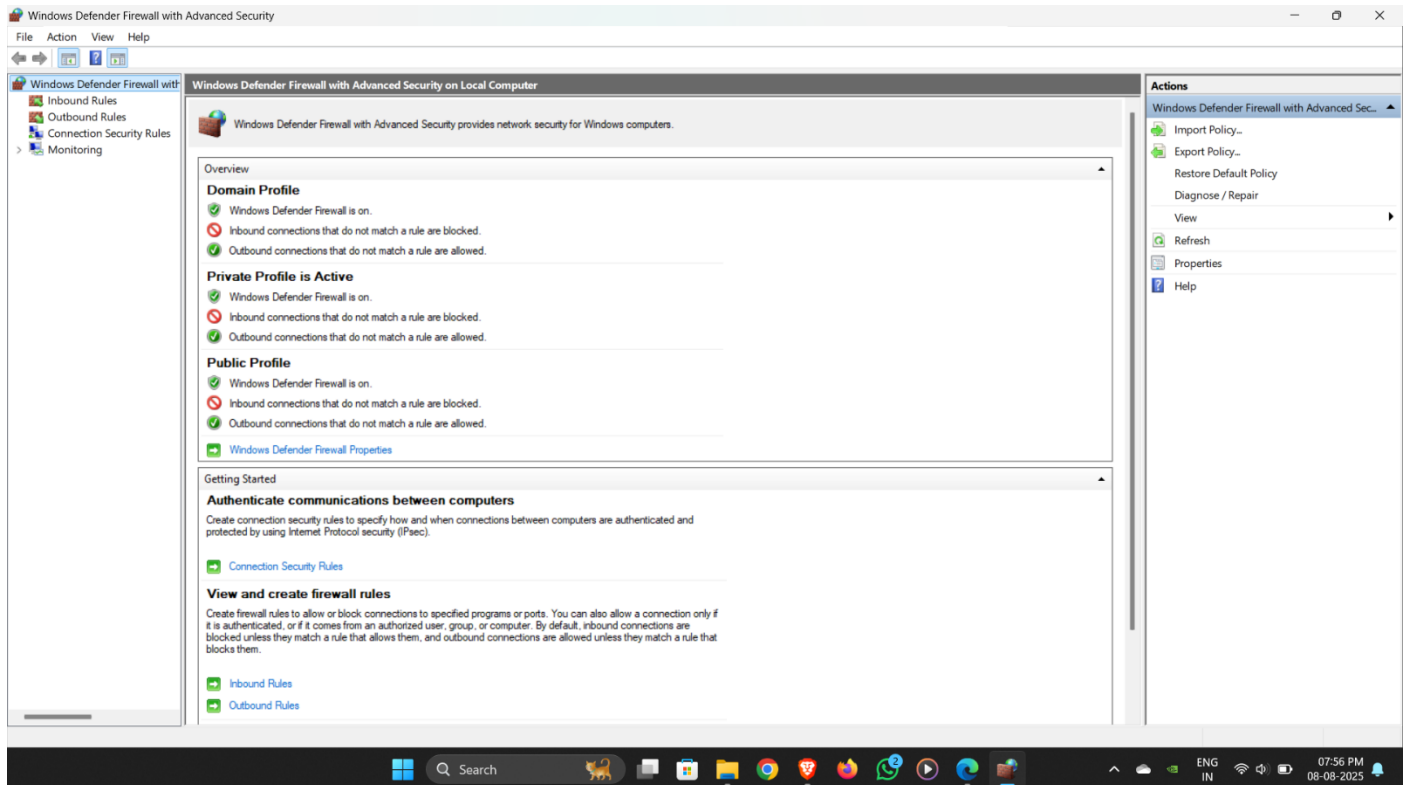
## Task 4 : Setup and Use a Firewall on Windows/Linux

**Objective:** Configure and test basic firewall rules to allow or block traffic.

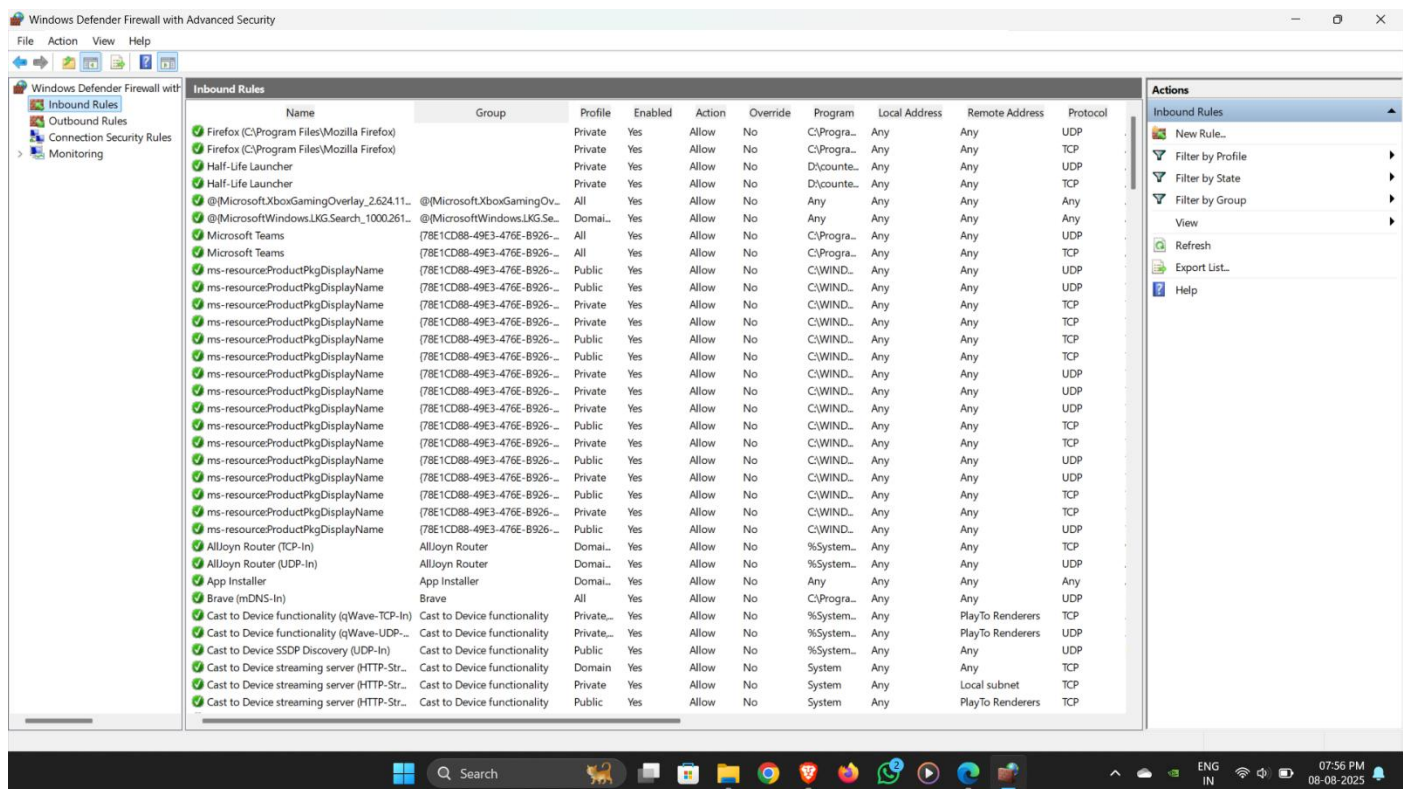
**Tools:** Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

**Deliverables:** Screenshot/Configuration file showing Firewall rules applied.

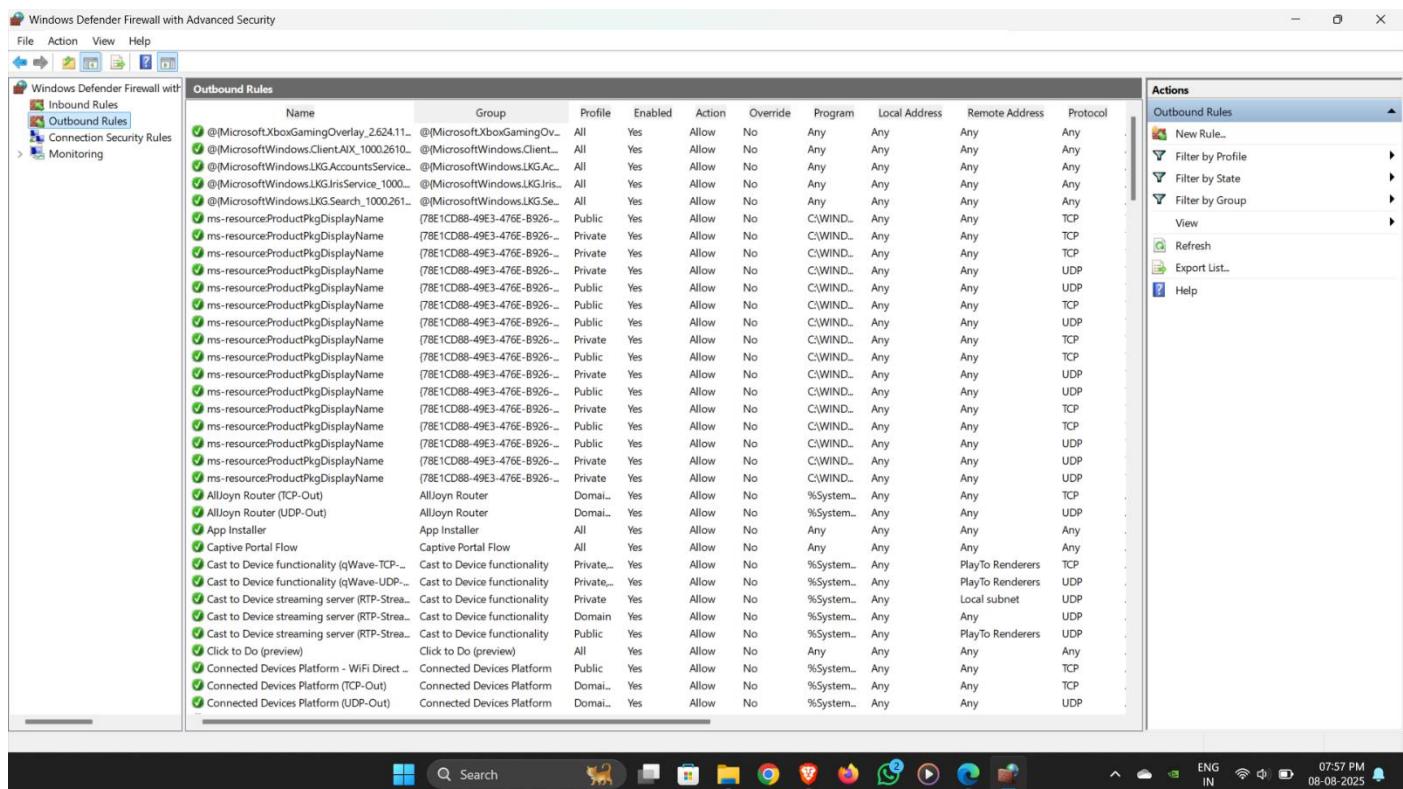
## Windows Defender Firewall with Advance Security – (Windows OS):



### In-Bound Rule's:



## Out-Bound Rule's:



# Steps to Block In-Bound Traffic on PORT (23):

Windows Defender Firewall with Advanced Security

File Action View Help

Windows D

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

Rule Type

Protocol and Ports

Action

Profile

Name

What type of rule would you like to create?

☐ Program

Rule that controls connections for a program.

☒ Port

Rule that controls connections for a TCP or UDP port.

☐ Predefined:

AllowIn Router

Rule that controls connections for a Windows experience.

☐ Custom

Custom rule.

< Back

Next >

Cancel

Cast to Device functionality (qWave-TCP-In)

Cast to Device functionality

Private...

Yes

Allow

Cast to Device functionality (qWave-UDP-In)

Cast to Device functionality

Private...

Yes

Allow

Cast to Device SSDP Discovery (UDP-In)

Cast to Device functionality

Public

Yes

Allow

Cast to Device streaming server (HTTP-Str...

Cast to Device functionality

Domain

Yes

Allow

Cast to Device streaming server (HTTP-Str...

Cast to Device functionality

Private

Yes

Allow

Cast to Device streaming server (HTTP-Str...

Cast to Device functionality

Public

Yes

Allow

Override	Program	Local Address	Remote Address	Protocol
No	C:\Progra...	Any	Any	UDP
No	C:\Progra...	Any	Any	TCP
No	D:\counte...	Any	Any	UDP
No	D:\counte...	Any	Any	TCP
No	Any	Any	Any	Any
No	Any	Any	Any	Any
No	C:\Progra...	Any	Any	UDP
No	C:\Progra...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	%System...	Any	Any	TCP
No	%System...	Any	Any	UDP
No	Any	Any	Any	Any
No	C:\Progra...	Any	Any	UDP
No	%System...	Any	PlayTo Renderers	TCP
No	%System...	Any	PlayTo Renderers	UDP
No	%System...	Any	Any	UDP
No	System	Any	Any	TCP
No	System	Any	Local subnet	TCP
No	System	Any	PlayTo Renderers	TCP

Actions

Inbound Rules

New Rule...

Filter by Profile

Filter by State

Filter by Group

View

Refresh

Export List...

Help

Windows Defender Firewall with Advanced Security

File Action View Help

Windows D

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

Rule Type

Protocol and Ports

Action

Profile

Name

Does this rule apply to TCP or UDP?

☒ TCP

☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports

☒ Specific local ports:

23

Example: 80, 443, 5000-5010

< Back

Next >

Cancel

Cast to Device functionality (qWave-TCP-In)

Cast to Device functionality

Private...

Yes

Allow

Cast to Device functionality (qWave-UDP-In)

Cast to Device functionality

Private...

Yes

Allow

Cast to Device SSDP Discovery (UDP-In)

Cast to Device functionality

Public

Yes

Allow

Cast to Device streaming server (HTTP-Str...

Cast to Device functionality

Domain

Yes

Allow

Cast to Device streaming server (HTTP-Str...

Cast to Device functionality

Private

Yes

Allow

Cast to Device streaming server (HTTP-Str...

Cast to Device functionality

Public

Yes

Allow

Override	Program	Local Address	Remote Address	Protocol
No	C:\Progra...	Any	Any	UDP
No	C:\Progra...	Any	Any	TCP
No	D:\counte...	Any	Any	UDP
No	D:\counte...	Any	Any	TCP
No	Any	Any	Any	Any
No	Any	Any	Any	Any
No	C:\Progra...	Any	Any	UDP
No	C:\Progra...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	%System...	Any	Any	TCP
No	%System...	Any	Any	UDP
No	Any	Any	Any	Any
No	C:\Progra...	Any	Any	UDP
No	%System...	Any	PlayTo Renderers	TCP
No	%System...	Any	PlayTo Renderers	UDP
No	%System...	Any	Any	UDP
No	System	Any	Any	TCP
No	System	Any	Local subnet	TCP
No	System	Any	PlayTo Renderers	TCP

Actions

Inbound Rules

New Rule...

Filter by Profile

Filter by State

Filter by Group

View

Refresh

Export List...

Help

Windows Defender Firewall with Advanced Security

File Action View Help

New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

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 Security Rule node.

☒ Block the connection

< Back Next > Cancel

Override	Program	Local Address	Remote Address	Protocol
No	C:\Progra...	Any	Any	UDP
No	C:\Progra...	Any	Any	TCP
No	D:\counte...	Any	Any	UDP
No	D:\counte...	Any	Any	TCP
No	Any	Any	Any	Any
No	Any	Any	Any	Any
No	C:\Progra...	Any	Any	UDP
No	C:\Progra...	Any	Any	TCP
No	C:\WINDL...	Any	Any	UDP
No	C:\WINDL...	Any	Any	UDP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	UDP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	UDP
No	C:\WINDL...	Any	Any	UDP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	UDP
No	%System...	Any	Any	TCP
No	%System...	Any	Any	UDP
No	Any	Any	Any	Any
No	C:\Progra...	Any	Any	UDP
No	%System...	Any	PlayTo Renderers	TCP
No	%System...	Any	PlayTo Renderers	UDP
No	%System...	Any	Any	UDP
No	System	Any	Any	TCP
No	System	Any	Local subnet	TCP
No	System	Any	PlayTo Renderers	TCP

Actions

Inbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Cast to Device functionality (qWave-TCP-In) Cast to Device functionality Private... Yes Allow

Cast to Device functionality (qWave-UDP-In) Cast to Device functionality Private... Yes Allow

Cast to Device SSDP Discovery (UDP-In) Cast to Device functionality Public Yes Allow

Cast to Device streaming server (HTTP-Str...) Cast to Device functionality Domain Yes Allow

Cast to Device streaming server (HTTP-Str...) Cast to Device functionality Private Yes Allow

Cast to Device streaming server (HTTP-Str...) Cast to Device functionality Public Yes Allow

Windows Defender Firewall with Advanced Security

File Action View Help

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☒ Domain  
Applies when a computer is connected to its corporate domain.

☒ Private  
Applies when a computer is connected to a private network location, such as a home or work place.

☒ Public  
Applies when a computer is connected to a public network location.

< Back Next > Cancel

Override	Program	Local Address	Remote Address	Protocol
No	C:\Progra...	Any	Any	UDP
No	C:\Progra...	Any	Any	TCP
No	D:\counte...	Any	Any	TCP
No	D:\counte...	Any	Any	TCP
No	Any	Any	Any	Any
No	Any	Any	Any	Any
No	C:\Progra...	Any	Any	UDP
No	C:\Progra...	Any	Any	TCP
No	C:\WINDL...	Any	Any	UDP
No	C:\WINDL...	Any	Any	UDP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	UDP
No	C:\WINDL...	Any	Any	UDP
No	C:\WINDL...	Any	Any	UDP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	UDP
No	C:\WINDL...	Any	Any	TCP
No	C:\WINDL...	Any	Any	TCP
No	%System...	Any	Any	TCP
No	%System...	Any	Any	UDP
No	Any	Any	Any	Any
No	C:\Progra...	Any	Any	UDP
No	%System...	Any	PlayTo Renderers	TCP
No	%System...	Any	PlayTo Renderers	UDP
No	%System...	Any	Any	UDP
No	System	Any	Any	TCP
No	System	Any	Local subnet	TCP
No	System	Any	PlayTo Renderers	TCP

Actions

Inbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Cast to Device functionality (qWave-TCP-In) Cast to Device functionality Private... Yes Allow

Cast to Device functionality (qWave-UDP-In) Cast to Device functionality Private... Yes Allow

Cast to Device SSDP Discovery (UDP-In) Cast to Device functionality Public Yes Allow

Cast to Device streaming server (HTTP-Str...) Cast to Device functionality Domain Yes Allow

Cast to Device streaming server (HTTP-Str...) Cast to Device functionality Private Yes Allow

Cast to Device streaming server (HTTP-Str...) Cast to Device functionality Public Yes Allow



Windows Defender Firewall with Advanced Security

FileActionViewHelp

Windows D

Inbound

Outbound

Connected

Monitor

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

Rule Type

Protocol and Ports

Action

Profile

Name

Name:

Block PORT (23) - Telnet (Windows)

Description (optional):

Here, we will CHECK how, to BLOCK the In-Coming Telnet Request on Port 23

< Back

Finish

Cancel

Override	Program	Local Address	Remote Address	Protocol
No	C:\Progra...	Any	Any	UDP
No	C:\Progra...	Any	Any	TCP
No	D:\counte...	Any	Any	UDP
No	D:\counte...	Any	Any	TCP
No	Any	Any	Any	Any
No	Any	Any	Any	Any
No	C:\Progra...	Any	Any	UDP
No	C:\Progra...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	UDP
No	C:\WIND...	Any	Any	TCP
No	C:\WIND...	Any	Any	TCP
No	%System...	Any	Any	TCP
No	%System...	Any	Any	UDP
No	Any	Any	Any	Any
No	C:\Progra...	Any	Any	UDP
No	%System...	Any	PlayTo Renderers	TCP
No	%System...	Any	PlayTo Renderers	UDP
No	%System...	Any	Any	UDP
No	System	Any	Any	TCP
No	System	Any	Local subnet	TCP
No	System	Any	PlayTo Renderers	TCP

Cast to Device functionality (qWave-TCP-In)

Cast to Device functionality

Private...

Yes

Allow

Cast to Device functionality (qWave-UDP-In)

Cast to Device functionality

Private...

Yes

Allow

Cast to Device SSDP Discovery (UDP-In)

Cast to Device functionality

Public

Yes

Allow

Cast to Device streaming server (HTTP-Str...

Cast to Device functionality

Domain

Yes

Allow

Cast to Device streaming server (HTTP-Str...

Cast to Device functionality

Private

Yes

Allow

Cast to Device streaming server (HTTP-Str...

Cast to Device functionality

Public

Yes

Allow

Actions

Inbound Rules

New Rule...

Filter by Profile

Filter by State

Filter by Group

View

Refresh

Export List...

Help

Search

ENG

IN

07:59 PM

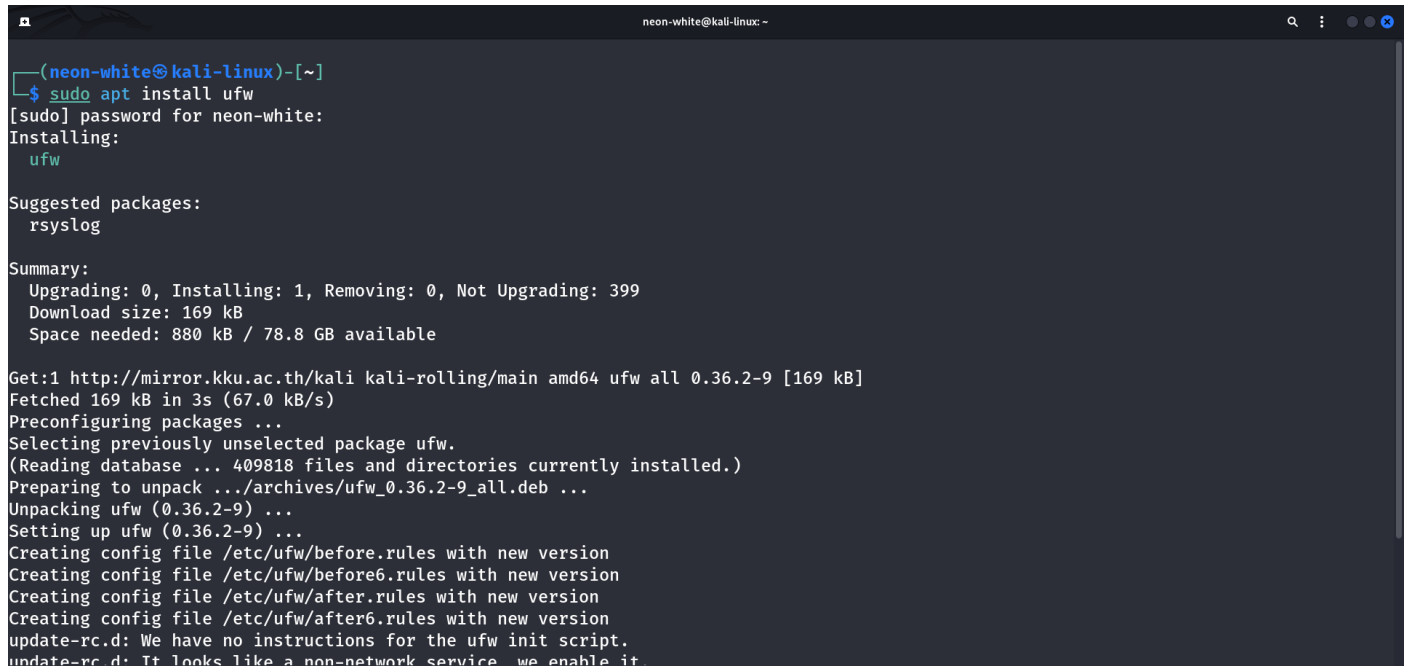
08-08-2025



## UFW (Un-complicated Firewall) – (Kali-Linux OS):

### Step 1: First, we will INSTALL: UFW (Un-complicated Firewall)

**Command:** `sudo apt install ufw`

A terminal window titled 'neon-white@kali-linux -' showing the command 'sudo apt install ufw' being executed. The output includes the password prompt, package suggestions (rsyslog), a summary of the installation (1 package, 169 kB), and the progress of downloading and unpacking the package. The terminal text is as follows:

```
(neon-white@kali-linux)-[~]
$ sudo apt install ufw
[sudo] password for neon-white:
Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 399
  Download size: 169 kB
  Space needed: 880 kB / 78.8 GB available

Get:1 http://mirror.kku.ac.th/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 3s (67.0 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 409818 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
```

### Step 2: Second, we will ENABLE (UFW):

**Command:** `sudo ufw enable`

### Step 3: Third, we will ADD-RULE: (DENY PORT-23/TCP):

**Command:** `sudo ufw deny 23/tcp`

A terminal window titled 'neon-white@kali-linux -' showing the command 'sudo ufw deny 23/tcp' being executed. The output shows 'Rules updated' and 'Rules updated (v6)'. The terminal text is as follows:

```
(neon-white@kali-linux)-[~]
$ sudo ufw deny 23/tcp
Rules updated
Rules updated (v6)

(neon-white@kali-linux)-[~]
$
```

**Step 4: Fourth, we will ALLOW-RULE: (SSH PORT-22/TCP):**

**Command:** `sudo ufw allow 22/tcp`

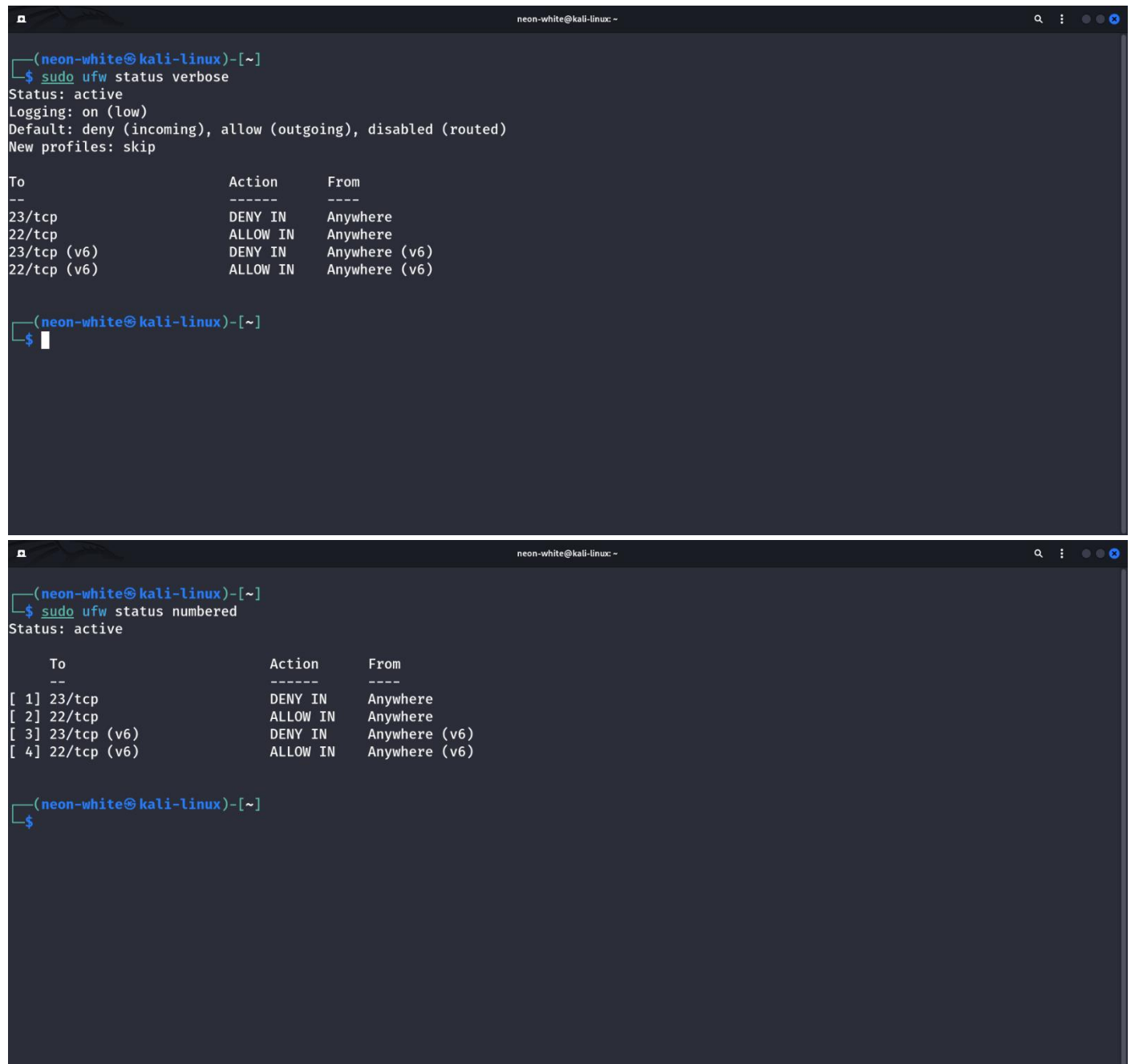
A terminal window with a dark background and light blue text. The window title is 'neon-white@kali-linux:'. The prompt is '(neon-white@kali-linux)-[~]'. The user enters the command '\$ sudo ufw allow 22/tcp'. The output is 'Rules updated' followed by 'Rules updated (v6)'. The prompt returns to '(neon-white@kali-linux)-[~]'.

```
(neon-white@kali-linux)-[~]  
$ sudo ufw allow 22/tcp  
Rules updated  
Rules updated (v6)  
(neon-white@kali-linux)-[~]  
$
```



**Step 5: Fifth, we will CHECK, newly Added-Rule's:**

**Command:** `sudo apt ufw status verbose/numbered`



The image shows two terminal windows from a Kali Linux system, demonstrating the output of the `sudo ufw status` command with different flags.

**Terminal 1 (Top):** The command `sudo ufw status verbose` is executed. The output shows the firewall is active, logging is on (low), the default policy is deny for incoming and outgoing traffic, and new profiles are skipped. A table of rules is displayed:

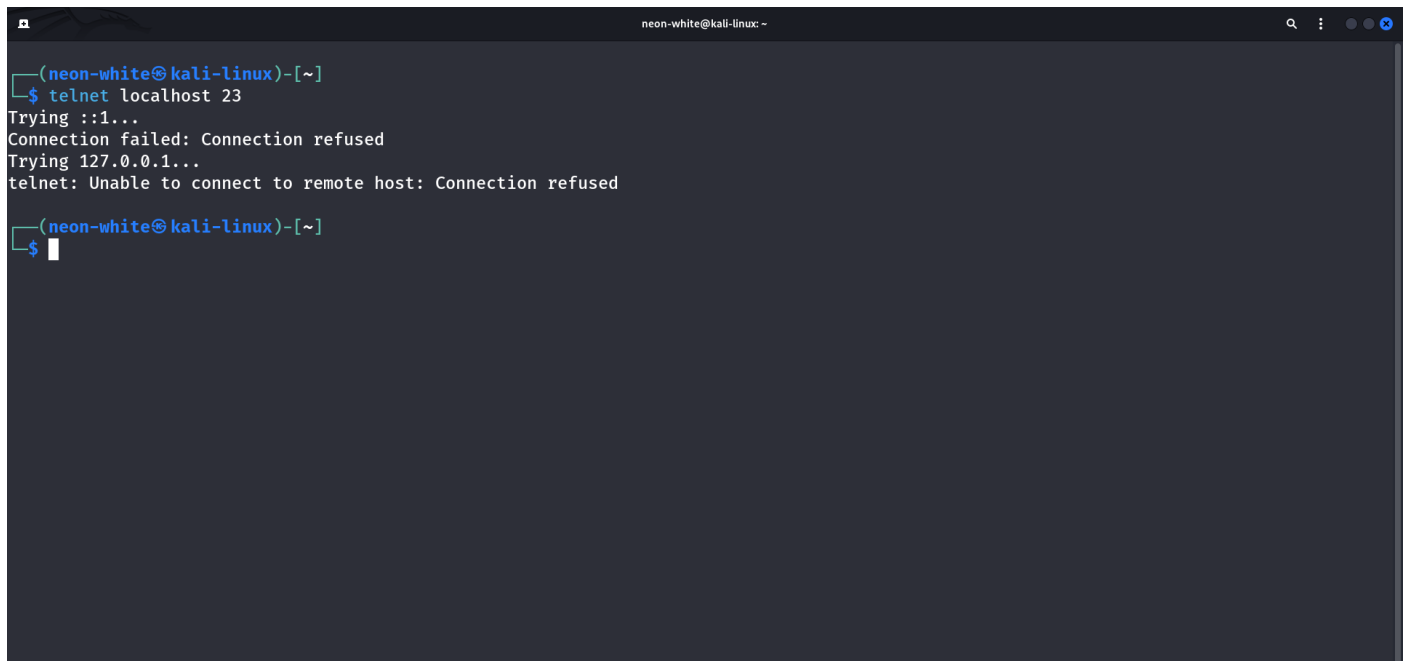
To	Action	From
23/tcp	DENY IN	Anywhere
22/tcp	ALLOW IN	Anywhere
23/tcp (v6)	DENY IN	Anywhere (v6)
22/tcp (v6)	ALLOW IN	Anywhere (v6)

**Terminal 2 (Bottom):** The command `sudo ufw status numbered` is executed. The output shows the firewall is active. A table of rules is displayed, with each rule numbered:

To	Action	From
[ 1 ] 23/tcp	DENY IN	Anywhere
[ 2 ] 22/tcp	ALLOW IN	Anywhere
[ 3 ] 23/tcp (v6)	DENY IN	Anywhere (v6)
[ 4 ] 22/tcp (v6)	ALLOW IN	Anywhere (v6)

**Step: 6: At-Last, we will RUN (TELNET-Command):**

**Command:** telnet localhost 23

A terminal window titled 'neon-white@kali-linux: -' with search and window control icons in the top right. The terminal shows a user prompt '(neon-white@kali-linux)-[~]' followed by the command '\$ telnet localhost 23'. The output is: 'Trying ::1...', 'Connection failed: Connection refused', 'Trying 127.0.0.1...', and 'telnet: Unable to connect to remote host: Connection refused'. The prompt returns to '(neon-white@kali-linux)-[~]' followed by '\$' and a cursor.

```
(neon-white@kali-linux)-[~]  
$ telnet localhost 23  
Trying ::1...  
Connection failed: Connection refused  
Trying 127.0.0.1...  
telnet: Unable to connect to remote host: Connection refused  
  
(neon-white@kali-linux)-[~]  
$
```