Lab#06: UFW (Uncomplicated Firewall)

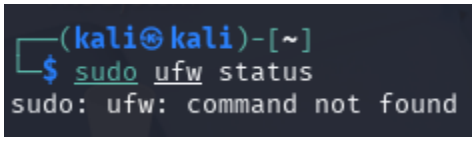
🎯 Objectives:

Setting the UFW and applying basic commands.

Step-by-Step Instructions / Summary

- Step 1: Install UFW
- Step 2: Basic Commands
- Step 3: Default Rules
- Step 4: Allowing Services/Ports
- Step 5: Denying Services/Ports
- Step 6: Allow or Deny by IP and Port
- Step 7: Deleting Rules
- Step 8: Advanced - Applications Profiles
- Step 9: Reload and Reset
- Step 10: Testing
- Step 11: Log and Monitor

1. **Installing UFW**

Check if UFW is installed sudo ufw status It appears to be not installed and the next step would be using the following command.	

sudo apt install ufw -y

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install ufw -y
Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1299
  Download size: 169 kB
  Space needed: 880 kB / 3,769 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 1s (336 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 407419 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.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' → '/usr/lib/systemd/system/ufw.service'.
Processing triggers for kali-menu (2025.1.1) ...
Processing triggers for man-db (2.13.0-1) ...
```

2. Basic Commands

a.

b. Enable UFW

sudo ufw enable	`┌──(kali㉿kali)-[~]`
	`└─$ sudo ufw enable`
	`Firewall is active and enabled on system startup`

c. Disable UFW

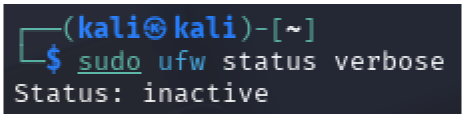
sudo ufw disable	`┌──(kali㉿kali)-[~]`
	`└─$ sudo ufw disable`
	`Firewall stopped and disabled on system startup`

d. Check Status

sudo ufw status	`┌──(kali㉿kali)-[~]`
	`└─$ sudo ufw status`
	`Status: inactive`

e. View in Verbose Mode

sudo ufw status verbose
*If the ufw is active, it'll show if IPv6 is considered for each rule

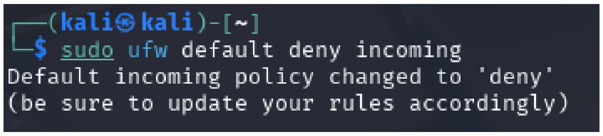


```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status verbose
Status: inactive
```

3. Default Rules

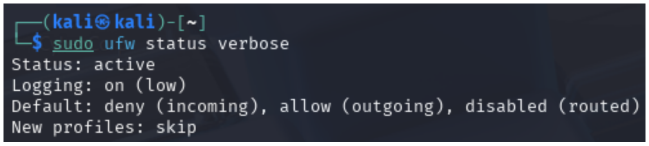
a. Set Default Policies

After changing back the ufw status active:
sudo ufw default deny incoming
*This command blocks all incoming connections by default unless specified to be allowed.



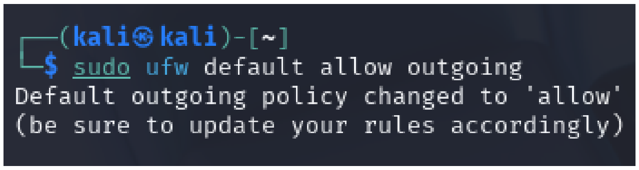
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

Checking the status after the command:



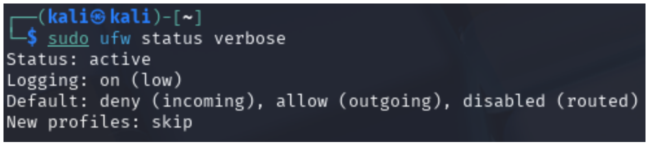
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

sudo ufw default allow outcoming
*This command allows outgoing connections by default without restriction



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```

Checking the status after the command:

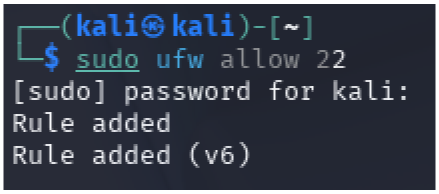


```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

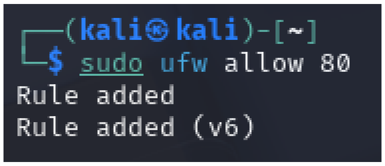
4. Allowing Services/Ports

a. Allow specific ports

sudo ufw allow 22 #SSH
sudo ufw allow 80 #HTTP
sudo ufw allow 443 #HTTPS



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22
[sudo] password for kali:
Rule added
Rule added (v6)
```



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 80
Rule added
Rule added (v6)
```

	``
┌──(kali㉿kali)-[~] └─$ sudo ufw allow 443 Rule added Rule added (v6) ```

b. **Allow by Port and Protocol**

sudo ufw allow 53/udp # DNS over UDP	``` ┌──(kali㉿kali)-[~] └─$ sudo ufw allow 53/udp Rule added Rule added (v6) ```

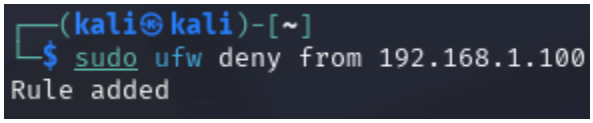
c. **Allow a Range of Ports**

sudo ufw allow 10000:20000/tcp	``` ┌──(kali㉿kali)-[~] └─$ sudo ufw allow 10000:20000/tcp Rule added Rule added (v6) ``` **Listing all rules so far:** ``` ┌──(kali㉿kali)-[~] └─$ sudo ufw status verbose Status: active Logging: on (low) Default: deny (incoming), allow (outgoing), disabled (routed) New profiles: skip To Action From -- ------ ---- 22 ALLOW IN Anywhere 80 ALLOW IN Anywhere 443 ALLOW IN Anywhere 53/udp ALLOW IN Anywhere 10000:20000/tcp ALLOW IN Anywhere 22 (v6) ALLOW IN Anywhere (v6) 80 (v6) ALLOW IN Anywhere (v6) 443 (v6) ALLOW IN Anywhere (v6) 53/udp (v6) ALLOW IN Anywhere (v6) 10000:20000/tcp (v6) ALLOW IN Anywhere (v6) ```

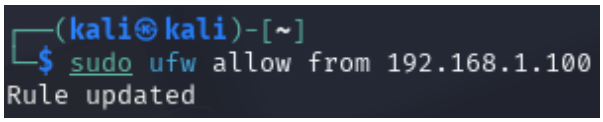
5. **Denying Services/Ports**
   a. **Deny a port**

sudo ufw deny 23 #Telnet	``` ┌──(kali㉿kali)-[~] └─$ sudo ufw deny 23 Rule added Rule added (v6) ```

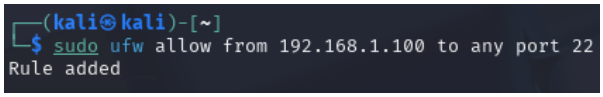
b. **Deny by IP**

sudo ufw deny from 192.168.1.100	

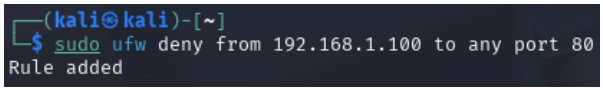
6. **Allow or Deny by IP and Port**
   a. **Allow from a specific IP**

sudo ufw allow from 192.168.1.100	

   b. **Allow from IP from a specific port**

sudo ufw allow from 192.168.1.100 to any port 22	

   c. **Deny from IP to port**

sudo ufw deny from 192.168.1.100 to any port 80	

7. **Deleting Rules**
   a. **Listing Numbered Rules**

sudo ufw status numbered

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    Anywhere
[ 2] 80                         ALLOW IN    Anywhere
[ 3] 443                        ALLOW IN    Anywhere
[ 4] 53/udp                     ALLOW IN    Anywhere
[ 5] 10000:20000/tcp            ALLOW IN    Anywhere
[ 6] 23                         DENY IN     Anywhere
[ 7] Anywhere                   ALLOW IN    192.168.1.100
[ 8] 22                         ALLOW IN    192.168.1.100
[ 9] 80                         DENY IN     192.168.1.100
[10] 22 (v6)                    ALLOW IN    Anywhere (v6)
[11] 80 (v6)                    ALLOW IN    Anywhere (v6)
[12] 443 (v6)                   ALLOW IN    Anywhere (v6)
[13] 53/udp (v6)                ALLOW IN    Anywhere (v6)
[14] 10000:20000/tcp (v6)       ALLOW IN    Anywhere (v6)
[15] 23 (v6)                    DENY IN     Anywhere (v6)
```

b. **Delete by Number**

sudo ufw delete [number]

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw delete 11
Deleting:
 allow 80
Proceed with operation (y|n)? y
Rule deleted (v6)
```

c. **Delete by Rule**

sudo ufw delete 11

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw delete 11
Deleting:
 allow 80
Proceed with operation (y|n)? y
Rule deleted (v6)
```

After deleting the rule:

sudo ufw status numbered

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    Anywhere
[ 2] 80                         ALLOW IN    Anywhere
[ 3] 443                        ALLOW IN    Anywhere
[ 4] 53/udp                     ALLOW IN    Anywhere
[ 5] 10000:20000/tcp            ALLOW IN    Anywhere
[ 6] 23                         DENY IN     Anywhere
[ 7] Anywhere                   ALLOW IN    192.168.1.100
[ 8] 22                         ALLOW IN    192.168.1.100
[ 9] 80                         DENY IN     192.168.1.100
[10] 22 (v6)                    ALLOW IN    Anywhere (v6)
[11] 443 (v6)                   ALLOW IN    Anywhere (v6)
[12] 53/udp (v6)                ALLOW IN    Anywhere (v6)
[13] 10000:20000/tcp (v6)       ALLOW IN    Anywhere (v6)
[14] 23 (v6)                    DENY IN     Anywhere (v6)
```

The removal shows that there are 14 rules now and 80 ALLOW IN rule was deleted

8. **Advanced - Applications Profiles**
   a. **List App Profiles**

sudo ufw app list
This command lists all application profiles from this directory "/etc/ufw/applications.d"

```
└─$ sudo ufw app list
Available applications:
  AIM
  Apache
  Apache Full
  Apache Secure
  Bonjour
  CIFS
  DNS
  Deluge
  IMAP
  IMAPS
  IPP
  KTorrent
  Kerberos Admin
  Kerberos Full
  Kerberos KDC
  Kerberos Password
  LDAP
  LDAPS
```

b. **Get App Info**

sudo ufw app info OpenSSH
This command displays detailed information about the predefined application profile used by the ufw firewall.

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw app info OpenSSH

Profile: OpenSSH
Title: Secure shell server, an rshd replacement
Description: OpenSSH is a free implementation of the Secure Shell protocol.

Port:
  22/tcp
```

c. **Allow by App Name**

sudo ufw allow OpenSSH

Checking the firewall rules change:
sudo ufw status

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow OpenSSH
[sudo] password for kali:
Rule added
Rule added (v6)
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
OpenSSH                    ALLOW       Anywhere
```

9. **Reload and Reset**
   a. **Reload UFW**

sudo ufw reload
Refreshes the config file without shutting down the system.

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw reload
Firewall reloaded
```

b. **Reset All Tools**

sudo ufw reset
With this command completely resets UFW to its default state

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with operation (y|n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20250626_192010'
Backing up 'before.rules' to '/etc/ufw/before.rules.20250626_192010'
Backing up 'after.rules' to '/etc/ufw/after.rules.20250626_192010'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20250626_192010'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20250626_192010'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20250626_192010'
```

10. Testing

a. Install a Web Server and setting up the server

sudo apt update

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
1295 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

sudo apt install apache2 -y

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install apache2 -y
apache2 is already the newest version (2.4.63-1).
```

sudo systemctl start apache2

b. Enable and Configure UFW (Only SSH and HTTP)

Allows SSH
sudo ufw allow OpenSSH

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow OpenSSH
Rules updated
Rules updated (v6)
```

Allows HTTP traffic (port 80)
sudo ufw allow Apache

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow Apache
Rule updated
Rule updated (v6)
```

Checking the rules after additional rules:
sudo ufw status verbose

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
80/tcp (Apache)            ALLOW IN    Anywhere
22/tcp (OpenSSH)           ALLOW IN    Anywhere
80/tcp (Apache (v6))       ALLOW IN    Anywhere (v6)
22/tcp (OpenSSH (v6))      ALLOW IN    Anywhere (v6)
```

c. Access from Another System

i. Testing allowed

Starting SSH service

Starting the ssh service:
sudo systemctl start ssh

Checking the ssh service status
sudo systemctl status ssh

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start ssh
```

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system
     Active: active (running) since Thu 2025
```

Testing SSH (allowed)
ssh kali@172.16.123.129

```
┌──(kali㉿kali)-[~]
└─$ ssh kali@172.16.123.129
kali@172.16.123.129's password:
Permission denied, please try again.
kali@172.16.123.129's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jun 28 21:16:55 2025 from 172.16.123.129
┌──(kali㉿kali)-[~]
└─$
```

Starting Apache Service

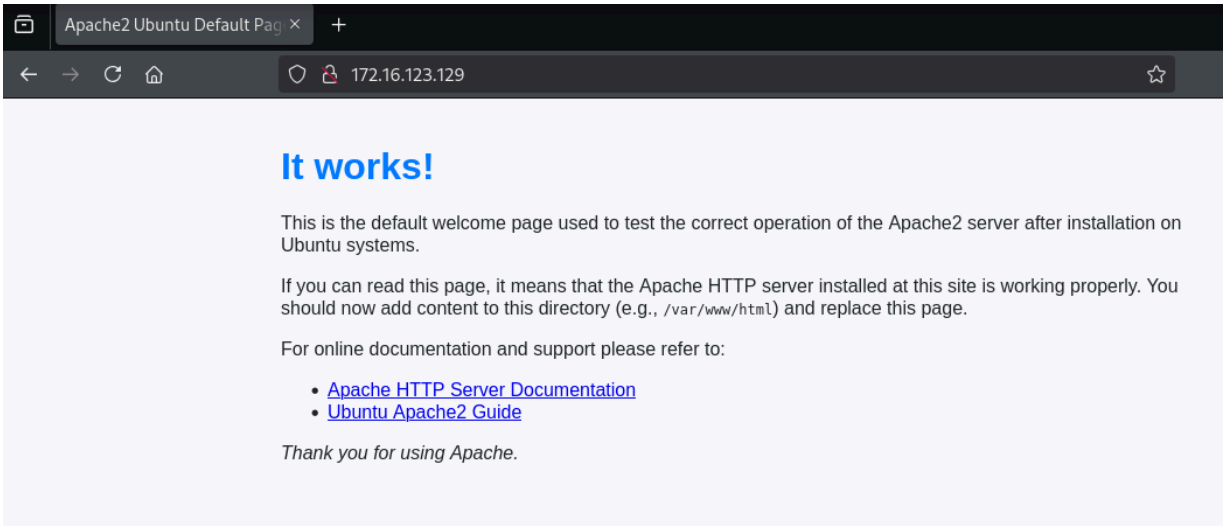
Starting the Apache service:
sudo systemctl start apache2

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start apache2
```

Checking the apache service status
sudo systemctl status apache2

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/syste
     Active: active (running) since Thu 202
```

Testing HTTP (Allowed)
Visiting: http://172.12.168



ii. Testing denied

Adding rules to deny the ports

sudo ufw deny OpenSSH
sudo ufw deny Apache

Showing the rules that were added:
sudo ufw status verbose

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw deny OpenSSH
Rule updated
Rule updated (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw deny Apache
Rule updated
Rule updated (v6)
```

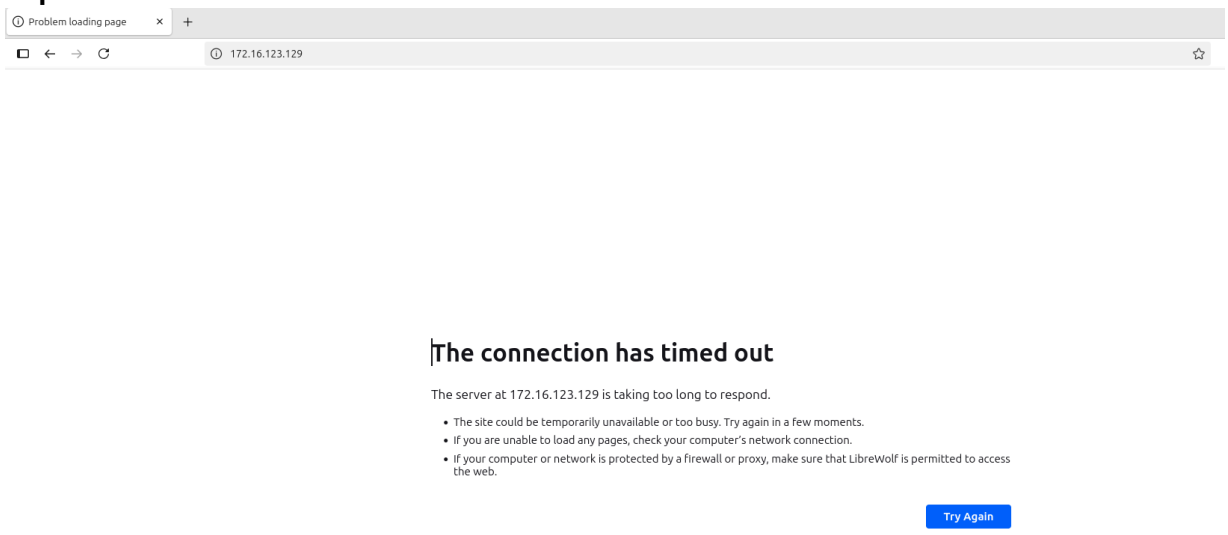
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp (OpenSSH)           DENY IN     Anywhere
80/tcp (Apache)            DENY IN     Anywhere
22/tcp (OpenSSH (v6))      DENY IN     Anywhere (v6)
80/tcp (Apache (v6))       DENY IN     Anywhere (v6)
```

The services are denied after rules were added

SSH services denied (Host OS):
ssh kali@172.16.123.129

```
tempadmin@AlexPC447:~$ ssh kali@172.16.123.129
ssh: connect to host 172.16.123.129 port 22: Connection timed out
```

Apache Services denied (Host OS):
http://172.16.123.129



sudo ufw logging on	```┌──(kali㉿kali)-[~]
	└─$ sudo ufw logging on
	Logging enabled```
	(kali㉿kali)-[~]
	$ sudo ufw logging on
	Logging enabled

11. Log and Monitor

sudo ufw logging on

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw logging on
Logging enabled
```

I used this command since the ufw logging enabled didn't create the ufw.log file.
systemctl start ufw.service

```
┌──(kali㉿kali)-[/var/log]
└─$ systemctl start ufw.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to start 'ufw.service'.
Authenticating as: kali,,, (kali)
Password:
==== AUTHENTICATION COMPLETE ====
```

```
┌──(kali㉿kali)-[/var/log]
└─$ ls
```

```
runit
samba
speech-dispatcher
stunnel4
syslog
sysstat
ufw.log
vmware-network.1.log
```

Afterwards, it's time to look through the logs

```
┌──(kali㉿kali)-[~]
└─$ sudo less /var/log/ufw.log
```

```
2025-06-30T22:34:09.742335-04:00 kali kernel: [UFW BLOCK] IN=eth0 OUT= MAC= SRC=172.16.12
3.129 DST=239.255.255.250 LEN=635 TOS=0×00 PREC=0×00 TTL=1 ID=12505 DF PROTO=UDP SPT=4806
3 DPT=3702 LEN=615
2025-06-30T22:34:09.742336-04:00 kali kernel: [UFW BLOCK] IN=eth0 OUT= MAC= SRC=fe80:0000
:0000:0000:020c:29ff:fe6e:2f58 DST=ff02:0000:0000:0000:0000:0000:0000:000c LEN=655 TC=0 H
OPLIMIT=1 FLOWLBL=271489 PROTO=UDP SPT=57121 DPT=3702 LEN=615
2025-06-30T22:34:09.742337-04:00 kali kernel: [UFW BLOCK] IN=eth0 OUT= MAC= SRC=fe80:0000
:0000:0000:020c:29ff:fe6e:2f58 DST=ff02:0000:0000:0000:0000:0000:0000:000c LEN=655 TC=0 H
OPLIMIT=1 FLOWLBL=271489 PROTO=UDP SPT=57121 DPT=3702 LEN=615
2025-06-30T22:34:09.742337-04:00 kali kernel: [UFW BLOCK] IN=eth0 OUT= MAC= SRC=172.16.12
3.129 DST=239.255.255.250 LEN=635 TOS=0×00 PREC=0×00 TTL=1 ID=12553 DF PROTO=UDP SPT=4806
3 DPT=3702 LEN=615
2025-06-30T22:34:09.742338-04:00 kali kernel: [UFW BLOCK] IN=eth0 OUT= MAC= SRC=fe80:0000
:0000:0000:020c:29ff:fe6e:2f58 DST=ff02:0000:0000:0000:0000:0000:0000:000c LEN=655 TC=0 H
OPLIMIT=1 FLOWLBL=271489 PROTO=UDP SPT=57121 DPT=3702 LEN=615
2025-06-30T22:34:09.742338-04:00 kali kernel: [UFW BLOCK] IN=eth0 OUT= MAC= SRC=172.16.12
3.129 DST=239.255.255.250 LEN=635 TOS=0×00 PREC=0×00 TTL=1 ID=12602 DF PROTO=UDP SPT=4806
3 DPT=3702 LEN=615
```

🧰 Tools & Skills Used

Tools:

- **Operating Systems:** Kali, Linux Mint (Host OS)
- **Core Services & Daemons:** Ufw (Uncomplicated Firewall), apache2, sshd
- **Command-Line Utilities:** sudo, systemctl, ssh, web browser

Skills:

- **Firewall Configuration, Log Analysis, System Troubleshooting**

🧠 Reflection & Takeaways

I learned the basics of ufw using both deny and allow connections. I had a hard time trying to show a firewall blocking my connections with another machine. I used the correct kali IP address to help me get the proper results. Another problem I had was enabling the ufw logging. I turned on the logging, but it appeared that it didn't work. So, I started the ufw.service again and I was able to capture logs.