

# TASK 3:

## Firewall & Network Security

### 1. Overview:

This Proof of Concept highlights the dangers of misconfigured firewalls and exposed network services. The process includes deploying a simple web server, identifying open ports through scanning, and securing the system by implementing ufw and iptables to limit access and block unwanted traffic.

### 2. Objectives:

- **Deployment:** Install and set up a basic web server (Apache2) and deactivate the firewall (ufw disable).
- **Assessment:** Utilize nmap and netcat to identify open ports and running services, illustrating how attackers can detect exposed services.
- **Protection:** Limit access using ufw (allowing only SSH and HTTP) and enforce iptables rules to block unnecessary traffic.

### 3. Setup

#### 3.1. Install and Configure Apache Web Server

##### 1. Update and Install Apache:

```
(oxydevil㉿kali)-[~]
└─$ sudo apt update && sudo apt install apache2 -y
[sudo] password for oxydevil:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
```

##### 2. Start SSH and Apache:

```
(oxydevil㉿kali)-[~]
└─$ sudo systemctl start ssh
[sudo] password for oxydevil:

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

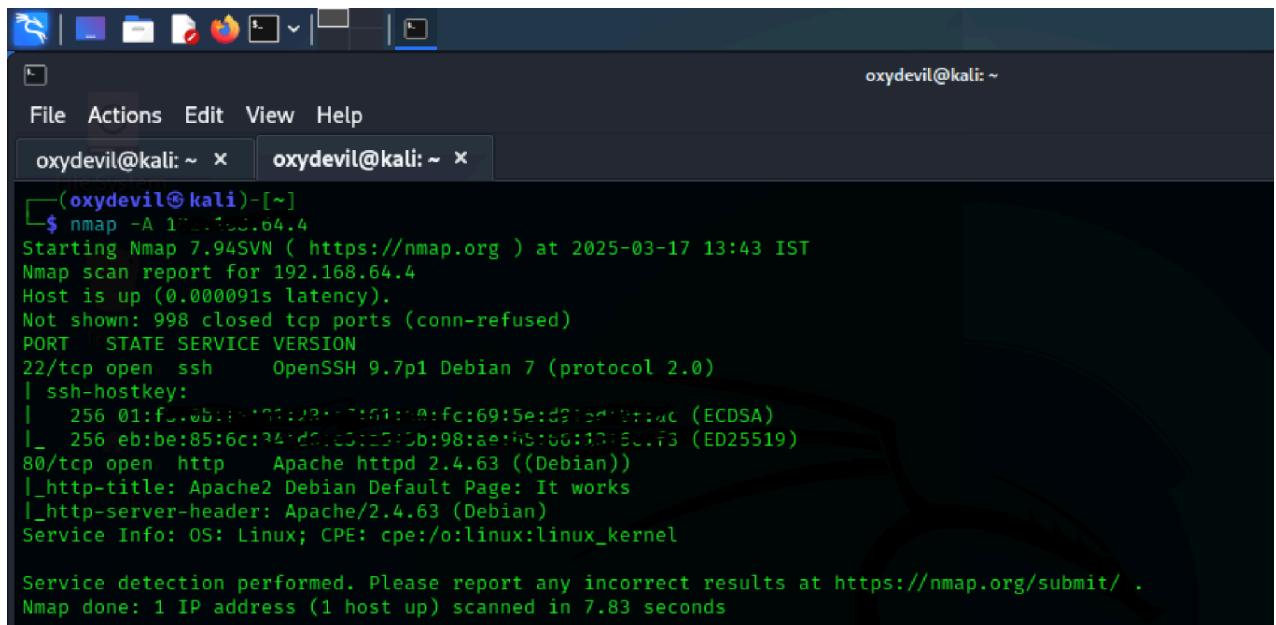
##### 3. Enable and Verify Apache Status:

```
(oxydevil㉿kali)-[~]
└─$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2

(oxydevil㉿kali)-[~]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: disabled)
     Active: active (running) since Mon 2025-03-17 13:11:56 IST; 8h ago
   Invocation: deff4a6365e34703a6d2bfaf590eb0c
     Docs: https://httpd.apache.org/docs/2.4/
```

## 4. Exploitation

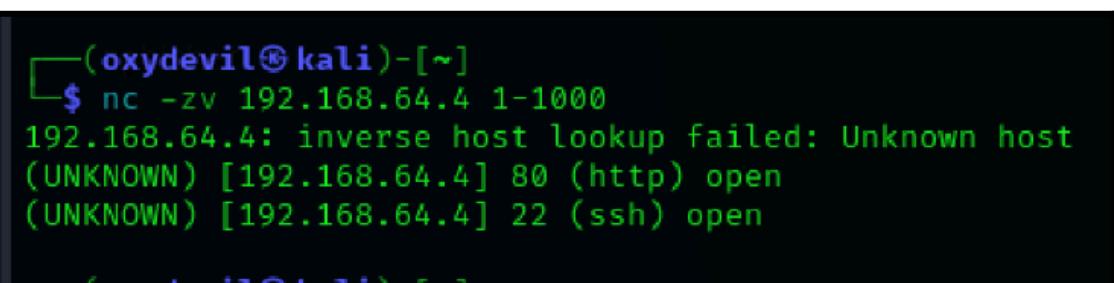
### 4.1. Scan for Open Ports Using Nmap Scan the Local Machine:



```
oxydevil@kali:~ [~]
File Actions Edit View Help
oxydevil@kali:~ x oxydevil@kali:~ x
└─(oxydevil@kali)-[~]
$ nmap -A 192.168.64.4
Starting Nmap 7.94 ( https://nmap.org ) at 2025-03-17 13:43 IST
Nmap scan report for 192.168.64.4
Host is up (0.000091s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.7p1 Debian 7 (protocol 2.0)
| ssh-hostkey:
|   256 01:f...eb:be:85:6c:94:ed:5b:98:ae:95:66:7d:5c:f3 (ED25519)
|_  256 eb:be:85:6c:94:ed:5b:98:ae:95:66:7d:5c:f3 (ED25519)
80/tcp    open  http     Apache httpd 2.4.63 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.63 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.83 seconds
```

### 4.2. Use Netcat to Test Open Ports

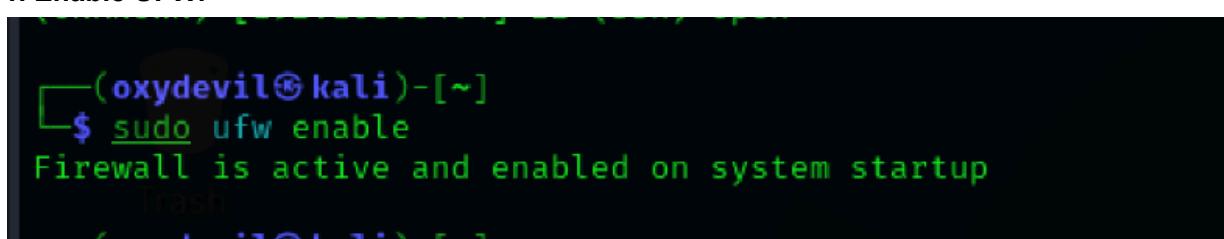


```
└─(oxydevil@kali)-[~]
$ nc -zv 192.168.64.4 1-1000
192.168.64.4: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.64.4] 80 (http) open
(UNKNOWN) [192.168.64.4] 22 (ssh) open
```

## 5. Mitigation

### 5.1. Enable and Configure UFW

#### 1. Enable UFW:



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

## 2. Set Default Policies:

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

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

## 3. Allow SSH and HTTP:

```
dash
└─(oxydevil㉿kali)-[~]
└─$ sudo ufw allow ssh
Rule added
Rule added (v6)

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

## 4. Verify UFW Status:

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

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

## 5. Save IPTables Rules:

```

oxydevil㉿kali:~$ sudo iptables-save | sudo tee /etc/iptables/rules.v4
tee: /etc/iptables/rules.v4: No such file or directory
# Generated by iptables-save v1.8.10 (nf_tables) on Mon Mar 17 14:22:09 2025
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:ufw-after-forward - [0:0]
:ufw-after-input - [0:0]
:ufw-after-logging-forward - [0:0]
:ufw-after-logging-input - [0:0]
:ufw-after-logging-output - [0:0]
:ufw-after-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-before-input - [0:0]
:ufw-before-logging-forward - [0:0]
:ufw-before-logging-input - [0:0]
:ufw-before-logging-output - [0:0]
:ufw-before-output - [0:0]
:ufw-logging-allow - [0:0]
:ufw-logging-deny - [0:0]
:ufw-not-local - [0:0]
:ufw-reject-forward - [0:0]
:ufw-reject-input - [0:0]
:ufw-select-output - [0:0]

-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN
-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN
-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny
-A ufw-not-local -j DROP
-A ufw-skip-to-policy-forward -j DROP
-A ufw-skip-to-policy-input -j DROP
-A ufw-skip-to-policy-output -j ACCEPT
-A ufw-track-output -p tcp -m conntrack --ctstate NEW -j ACCEPT
-A ufw-track-output -p udp -m conntrack --ctstate NEW -j ACCEPT
-A ufw-user-input -p tcp -m tcp --dport 22 -j ACCEPT
-A ufw-user-input -p tcp -m tcp --dport 80 -j ACCEPT
-A ufw-user-limit -m limit --limit 3/min -j LOG --log-prefix "[UFW LIMIT BLOCK]"
-A ufw-user-limit -j REJECT --reject-with icmp-port-unreachable
-A ufw-user-limit-accept -j ACCEPT
COMMIT
# Completed on Mon Mar 17 14:22:09 2025

```

## Conclusion:

This proof of concept highlights the critical role of firewall configuration and network security. By limiting access to essential services and preventing unnecessary traffic, administrators can effectively minimize potential attack vectors and enhance overall system protection.