

Task 3: Firewall & Network Security (PoC)

Setup: Install & Configure Web Server

Install Apache Web Server

sudo apt update && sudo apt install -y apache2

sudo systemctl enable apache2

sudo systemctl start apache2

sudo apt install ufw

```
root@kali:~# sudo apt update && sudo apt install -y apache2 && sudo systemctl enable apache2 && sudo systemctl start apache2 && sudo apt install ufw
[sudo] password for root:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
1564 packages can be upgraded. Run 'apt list --upgradable' to see them.
Upgrading:
  apache2 apache2-bin apache2-data apache2-utils ldap-utils libldap-common
Installing dependencies:
  libldap2
Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1558
  Download size: 2,378 kB
  Space needed: 622 kB / 8,388 MB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 libldap2 amd64 2.6.9+dfsg-2 [194 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 apache2 amd64 2.4.63-1 [219 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 apache2-data all 2.4.63-1 [168 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 ldap-utils amd64 2.6.9+dfsg-2 [152 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 libldap-common all 2.6.9+dfsg-2 [34.8 kB]
Get:6 http://mirror.uktel.net/kali kali-rolling/main amd64 apache2-bin amd64 2.4.63-1 [1,399 kB]
Get:7 http://mirror.uktel.net/kali kali-rolling/main amd64 apache2-utils amd64 2.4.63-1 [212 kB]
Fetched 2,378 kB in 2s (1,146 kB/s)
Selecting previously unselected package libldap2:amd64.
(Reading database ... 486107 files and directories currently installed.)
Preparing to unpack .../0-libldap2_2.6.9+dfsg-2_amd64.deb ...
Unpacking libldap2:amd64 (2.6.9+dfsg-2) ...
Preparing to unpack .../1-apache2_2.4.63-1_amd64.deb ...
Unpacking apache2 (2.4.63-1) over (2.4.62-3) ...
Preparing to unpack .../2-apache2-bin_2.4.63-1_amd64.deb ...
Unpacking apache2-bin (2.4.63-1) over (2.4.62-3) ...
Preparing to unpack .../3-apache2-data_2.4.63-1_all.deb ...
Unpacking apache2-data (2.4.63-1) over (2.4.62-3) ...
Preparing to unpack .../4-apache2-utils_2.4.63-1_amd64.deb ...
Unpacking apache2-utils (2.4.63-1) over (2.4.62-3) ...
Preparing to unpack .../5-ldap-utils_2.6.9+dfsg-2_amd64.deb ...
Unpacking ldap-utils (2.6.9+dfsg-2) over (2.5.18+dfsg-3+b1) ...
Preparing to unpack .../6-libldap-common_2.6.9+dfsg-2_all.deb ...
Unpacking libldap-common (2.6.9+dfsg-2) over (2.5.18+dfsg-3) ...
Setting up libldap-common (2.6.9+dfsg-2) ...
Installing new version of config file /etc/ldap/ldap.conf ...
Setting up apache2-data (2.4.63-1) ...
Setting up libldap2:amd64 (2.6.9+dfsg-2) ...
Setting up apache2-utils (2.4.63-1) ...
Setting up apache2-bin (2.4.63-1) ...
Setting up ldap-utils (2.6.9+dfsg-2) ...
Setting up apache2 (2.4.63-1) ...
apache2.service is a disabled or a static unit not running, not starting it.
apache-htcacheclean.service is a disabled or a static unit not running, not starting it.
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for libc-bin (2.40-3) ...
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
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /usr/lib/systemd/system/apache2.service.
Installing:
  ufw
Suggested packages:
  rsyslog
Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1558
  Download size: 169 kB
  Space needed: 880 kB / 8,399 MB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 1s (182 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 486287 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 (2024.4.0) ...
Processing triggers for man-db (2.13.0-1) ...

root@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 Wed 2025-03-26 10:34:25 EDT; 3min 58s ago
  Invocation: c90ad3b1f75ddff9447c31cfb7f4c1f
     Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 73469 (apache2)
      Tasks: 6 (limit: 65536)
     Memory: 18.3M (peak: 18.6M)
        CPU: 390ms
     CGroup: /system.slice/apache2.service
            └─73469 /usr/sbin/apache2 -k start
              └─73416 /usr/sbin/apache2 -k start
                └─73417 /usr/sbin/apache2 -k start
                  └─73418 /usr/sbin/apache2 -k start
                    └─73419 /usr/sbin/apache2 -k start
                      └─73420 /usr/sbin/apache2 -k start

Mar 26 10:34:25 vbox systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Mar 26 10:34:25 vbox systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Disable UFW (Uncomplicated Firewall)

```
sudo ufw disable
```

```
(zerotodo@vbox)-[~]  
$ sudo ufw disable  
Firewall stopped and disabled on system startup
```

Verify Apache is Running

```
systemctl status apache2
```

Check Open Ports

```
sudo netstat -tulnp | grep LISTEN
```

Expected output:

```
(zerotodo@vbox)-[~]  
$ sudo netstat -tulnp | grep LISTEN  
tcp        0      0 0.0.0.0:22          0.0.0.0:*          LISTEN      40567/sshd: /usr/sb  
tcp6       0      0 :::80              :::*                LISTEN      73409/apache2  
tcp6       0      0 :::22              :::*                LISTEN      40567/sshd: /usr/sb
```

Exploit: Scanning for Open Ports & Services

1. Use Nmap to Find Open Ports

```
nmap -sV -p- <Your-IP>
```

```
(zerotodo@vbox)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fd00::c675:87e5:aac2:b315 prefixlen 64 scopeid 0<global>  
    inet6 fd00::a00:27ff:fedd:f797 prefixlen 64 scopeid 0<global>  
    inet6 fe80::a00:27ff:fedd:f797 prefixlen 64 scopeid 0<link>  
    ether 08:00:27:dd:f7:97 txqueuelen 1000 (Ethernet)  
    RX packets 75144 bytes 98801948 (94.2 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 14564 bytes 2790230 (2.6 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
$ nmap -p- 10.0.2.15  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-26 10:42 EDT  
Nmap scan report for 10.0.2.15  
Host is up (0.0000070s latency).  
Not shown: 65533 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

-sV: Service detection
-p-: Scan all 65,535 ports

2. Use Netcat to Interact with Open Ports
nc -vz <YOUR-IP>

Expected output:
Connection to <YOUR_IP> 80 port [tcp/http] succeeded!

3. Impact Analysis

Without a firewall, attackers can discover all open services and attempt brute-force attacks or exploits.

Mitigation: Firewall Hardening

Enable UFW & Allow Only Necessary Services

```
sudo ufw enable
sudo ufw allow 22/tcp
sudo ufw allow 80/tcp
sudo ufw deny 23/tcp # Block Telnet
sudo ufw deny 3306/tcp # Block MySQL
```

```
(zerotodo@vbox)-[~]
$ sudo ufw enable
Firewall is active and enabled on system startup
Rule added
Rule added (v6)
Rule added
Rule added (v6)
Rule added
Rule added (v6)
Rule added
Rule added (v6)
```

Verify UFW Rules

```
sudo ufw status verbose
```

```
(zerotodo@vbox)-[~]
$ 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
80/tcp ALLOW IN Anywhere
23/tcp DENY IN Anywhere
3306/tcp DENY IN Anywhere
22/tcp (v6) ALLOW IN Anywhere (v6)
80/tcp (v6) ALLOW IN Anywhere (v6)
23/tcp (v6) DENY IN Anywhere (v6)
3306/tcp (v6) DENY IN Anywhere (v6)
```

Implement IPTables for Extra Protection

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 3306 -j DROP
sudo iptables -A INPUT -p tcp --dport 23 -j DROP
```

Re-scan Using Nmap to Verify

`nmap -sV -p- <YOUR-IP>`

```
(zerotodo@vbox)-[~]
$ nmap -sV -p- 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-26 10:48 EDT
Nmap scan report for 10.0.2.15
Host is up (0.0000070s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.9p2 Debian 1 (protocol 2.0)
80/tcp    open  http     Apache httpd 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 8.70 seconds
```

Conclusion

Before Hardening: Open services exposed to attacks.

After Hardening: Only SSH (22) & HTTP (80) remain accessible.

Firewall rules significantly reduce the attack surface.