

Recon & Enumeration Lab Report

Objective:

To perform basic reconnaissance and enumeration between two virtual machines (Ubuntu as the target and Kali Linux as the attacker).

Environment Setup:

- Host OS: Windows (with VirtualBox)
- Target VM: Ubuntu (Apache Web Server)
- Attacker VM: Kali Linux
- Network Mode: Bridged Adapter

Step 1: Configure Ubuntu (Target)

1. Open terminal and check the IP address:

\$ ip a

```
VirtualBox:~$ ip a
: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:22:ba:2d brd ff:ff:ff:ff:ff:ff
  inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
    valid_lft 5649sec preferred_lft 5649sec
  inet6 fe80::931:5f2d:b09a:8861/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
```

2. Install Apache Web Server:

\$ sudo apt install apache2

```

root@kali-VirtualBox:~# sudo apt install apache2 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libqt5designer5 libqt5help5 libqt5sql5 libqt5sql5-sqlite libqt5test5 libqt5xml5 python3-gpg python3-packaging
  python3-pyqt5 python3-pyqt5.sip
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
0 upgraded, 8 newly installed, 0 to remove and 229 not upgraded.
Need to get 1,922 kB of archives.
After this operation, 7,728 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapr1 amd64 1.7.0-8ubuntu0.22.04.2 [108 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1 amd64 1.6.1-5ubuntu4.22.04.2 [92.8 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-5ubuntu4.22.04.2 [1
1.3 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-ldap amd64 1.6.1-5ubuntu4.22.04.2 [9,170 B]
Get:5 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-bin amd64 2.4.52-1ubuntu4.14 [1,349 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-data all 2.4.52-1ubuntu4.14 [165 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-utils amd64 2.4.52-1ubuntu4.14 [89.0 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2 amd64 2.4.52-1ubuntu4.14 [97.9 kB]
Fetched 1,922 kB in 3s (619 kB/s)
Selecting previously unselected package libapr1:amd64.
(Reading database ... 203105 files and directories currently installed.)
Preparing to unpack .../0-libapr1_1.7.0-8ubuntu0.22.04.2_amd64.deb ...
Unpacking libapr1:amd64 (1.7.0-8ubuntu0.22.04.2) ...
Selecting previously unselected package libaprutil1:amd64.
Preparing to unpack .../4-libaprutil1_1.6.1-5ubuntu4.22.04.2_amd64.deb ...
Unpacking libaprutil1:amd64 (1.6.1-5ubuntu4.22.04.2) ...
Selecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
Preparing to unpack .../5-libaprutil1-dbd-sqlite3_1.6.1-5ubuntu4.22.04.2_amd64.deb ...
Unpacking libaprutil1-dbd-sqlite3:amd64 (1.6.1-5ubuntu4.22.04.2) ...
Selecting previously unselected package libaprutil1-ldap:amd64.
Preparing to unpack .../6-libaprutil1-ldap_1.6.1-5ubuntu4.22.04.2_amd64.deb ...
Unpacking libaprutil1-ldap:amd64 (1.6.1-5ubuntu4.22.04.2) ...
Selecting previously unselected package apache2-bin.
Preparing to unpack .../7-apache2-bin_2.4.52-1ubuntu4.14_amd64.deb ...
Unpacking apache2-bin (2.4.52-1ubuntu4.14) ...
Selecting previously unselected package apache2-data.
Preparing to unpack .../apache2-data_2.4.52-1ubuntu4.14_all.deb ...
Unpacking apache2-data (2.4.52-1ubuntu4.14) ...
Selecting previously unselected package apache2-utils.
Preparing to unpack .../apache2-utils_2.4.52-1ubuntu4.14_amd64.deb ...
Unpacking apache2-utils (2.4.52-1ubuntu4.14) ...
Selecting previously unselected package apache2.
Preparing to unpack .../apache2_2.4.52-1ubuntu4.14_amd64.deb ...
Unpacking apache2 (2.4.52-1ubuntu4.14) ...
Setting up libapr1:amd64 (1.7.0-8ubuntu0.22.04.2) ...
Setting up libaprutil1:amd64 (1.6.1-5ubuntu4.22.04.2) ...
Setting up libaprutil1-dbd-sqlite3:amd64 (1.6.1-5ubuntu4.22.04.2) ...
Setting up libaprutil1-ldap:amd64 (1.6.1-5ubuntu4.22.04.2) ...
Setting up apache2-bin (2.4.52-1ubuntu4.14) ...
Setting up apache2-data (2.4.52-1ubuntu4.14) ...
Setting up apache2-utils (2.4.52-1ubuntu4.14) ...
Setting up apache2 (2.4.52-1ubuntu4.14) ...

```

3. Start Apache Service:

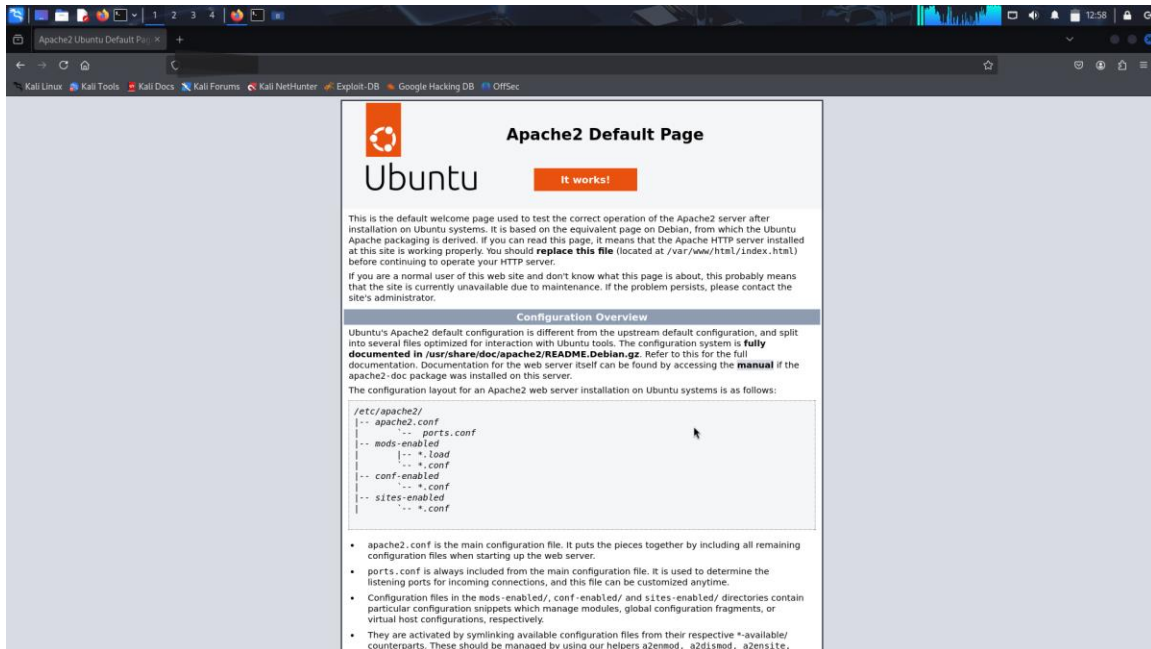
\$ sudo systemctl start apache2

```

root@kali-VirtualBox:~# sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2025-04-18 12:55:05 IST; 1min 18s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Main PID: 3222 (apache2)
    Tasks: 55 (limit: 7019)
   Memory: 5.6M
      CPU: 155ms
  CGroup: /system.slice/apache2.service
          └─3222 /usr/sbin/apache2 -k start
            └─3223 /usr/sbin/apache2 -k start
              └─3224 /usr/sbin/apache2 -k start

```

4. Verify Apache is working by visiting `http://<ubuntu-ip>` in a browser.



Step 2: Configure Kali Linux (Attacker)

1. Ping Ubuntu to verify connectivity:

```
$ ping <ubuntu-ip>
```

2. Install Nmap (if not already installed):

```
$ sudo apt install nmap
```

3. Run Nmap scan on Ubuntu:

```
$ sudo nmap -sV <ubuntu-ip>
```

```
File Actions Edit View Help
)~[~/Desktop]
$ nmap -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 12:48 IST
Nmap scan report for
Host is up (0.0030s latency).
All 1000 scanned ports on are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds

)~[~/Desktop]
```

```
~[~/Desktop]
$ nikto -h http://
- Nikto v2.5.0

+ Target IP:
+ Target Hostname:
+ Target Port: 80
+ Start Time: 2025-04-18 12:59:29 (GMT+5.5)

+ Server: Apache/2.4.52 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-headers/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak indices via iftop, header found with file /, inode: 29af, size: 63386a8b055f0, etime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.52 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ 1180 requests: 0 error(s) and 0 item(s) reported on remote host
+ End Time: 2025-04-18 13:00:48 (GMT+5.5) (79 seconds)
```

Summary:

Successfully set up a basic reconnaissance lab using Kali and Ubuntu. Scanned open ports and services running on Ubuntu using nmap and verified Apache web server via browser.