

# LAB: PORT SCANNING

Tools used:

Ubuntu 24.04 LTS, Python 3, Nmap, PHP, NSE (Nmap Scripting Engine), Wireshark.

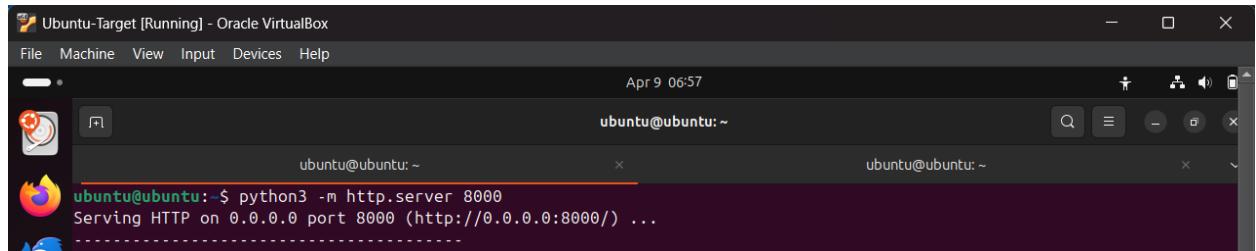
## Part 1: Active and Passive Port Scanning

For this part, I used a Bridged Adapter for both the target and attacker VMs. This setup lets both machines act like separate devices on the same physical network; just like two computers connected to the same Wi-Fi. It's a pretty common setup for internal penetration testing or when an attacker already has access to a network and wants to scan for open ports or services to gain more control.

### 1.1 Setting Up the Target Machine

On the target VM, start a service to listen on a specific TCP port. For this lab, a simple Python HTTP server is used.

- `python3 -m http.server 8000`

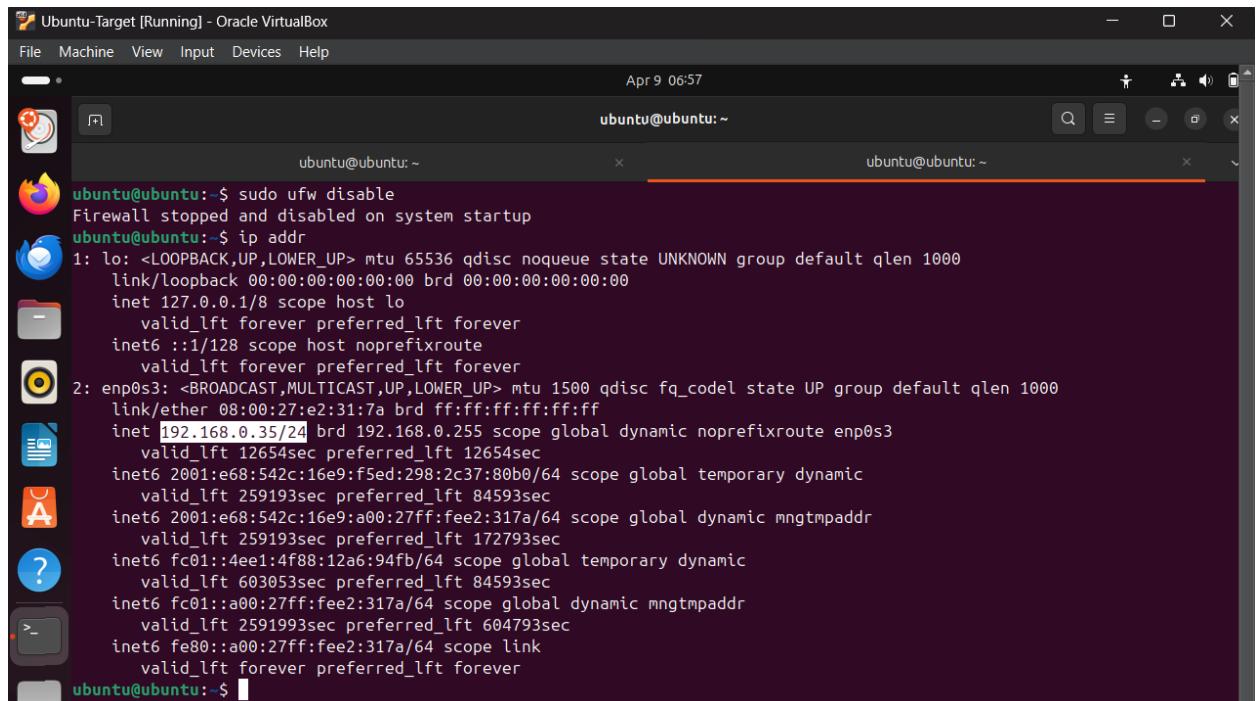


```
ubuntu@ubuntu:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

#### 1.1.1 Confirm the Port is Open

Ensure the firewall is disabled so the port is accessible.

- IP address of the target VM: 192.168.0.35/24



```
ubuntu@ubuntu:~$ sudo ufw disable
Firewall stopped and disabled on system startup
ubuntu@ubuntu:~$ ip addr
1: 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 noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e2:31:7a brd ff:ff:ff:ff:ff:ff
        inet 192.168.0.35/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s3
            valid_lft 12654sec preferred_lft 12654sec
        inet6 2001:e68:542c:16e9:f5ed:298:2c37:80b0/64 scope global temporary dynamic
            valid_lft 259193sec preferred_lft 84593sec
        inet6 2001:e68:542c:16e9:a00:27ff:fee2:317a/64 scope global dynamic mngtmpaddr
            valid_lft 259193sec preferred_lft 172793sec
        inet6 fc01::4ee1:4f88:12a6:94fb/64 scope global temporary dynamic
            valid_lft 603053sec preferred_lft 84593sec
        inet6 fe01::a00:27ff:fee2:317a/64 scope global dynamic mngtmpaddr
            valid_lft 2591993sec preferred_lft 604793sec
        inet6 fe80::a00:27ff:fee2:317a/64 scope link
            valid_lft forever preferred_lft forever
ubuntu@ubuntu:~$
```

## 1.2. Capturing Traffic on the Attacker Machine

On the attacker VM, use Wireshark to monitor network traffic. Capture data from the network interface connected to the internet. In this case, enp0s3.

### Capture



## 1.3. Performing a Port Scan with Nmap

From the attacker VM, run Nmap to scan the specified port on the target VM:

- nmap -p 8000 192.168.0.35

```
inq@ubuntu:~$ nmap -p 8000 192.168.0.35
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-09 14:53 +08
Nmap scan report for ubuntu.realtek (192.168.0.35)
Host is up (0.0030s latency).

PORT      STATE SERVICE
8000/tcp    open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
inq@ubuntu:~$
```

## 1.4. Scanning Without an Active Service

Stop the Python server on the target machine to simulate a scenario where no service is listening:

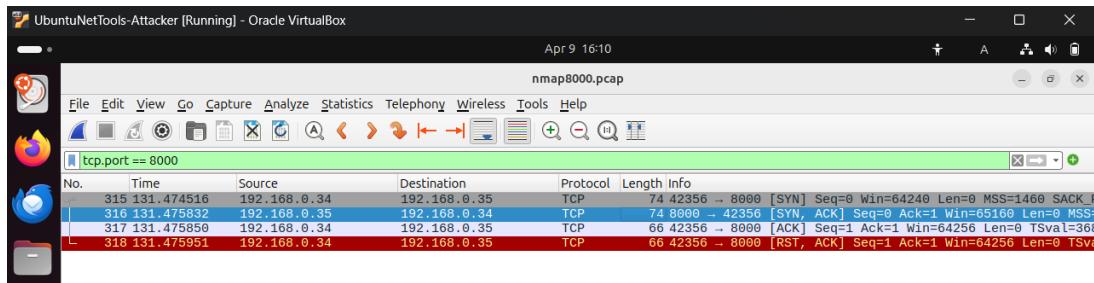
- ss -tuln

```
ubuntu@ubuntu:~$ sudo netstat -tuln | grep 8000
sudo: netstat: command not found
ubuntu@ubuntu:~$ sudo ss -tuln | grep 8000
ubuntu@ubuntu:~$ ss -tuln
Netid      State     Recv-Q      Send-Q      Local Address:Port          Peer Address:Port      Process
udp        UNCONN    0           0           0.0.0.0:5353            0.0.0.0:*              [::]:*
udp        UNCONN    0           0           0.0.0.0:39475           0.0.0.0:*              [::]:*
udp        UNCONN    0           0           127.0.0.54:53            0.0.0.0:*              [::]:*
udp        UNCONN    0           0           127.0.0.53%lo:53          0.0.0.0:*              [::]:*
tcp        LISTEN   4096        0           127.0.0.53%lo:53          0.0.0.0:*              [::]:*
tcp        LISTEN   4096        0           127.0.0.1:631             0.0.0.0:*              [::]:*
tcp        LISTEN   4096        0           127.0.0.54:53             0.0.0.0:*              [::]:*
tcp        LISTEN   4096        0           [::1]:631                0.0.0.0:*              [::]:*
```

Repeat steps 2 and 3 to observe how packet behavior changes when the port is closed.

## 1.5. Analyzing Packet Capture Results

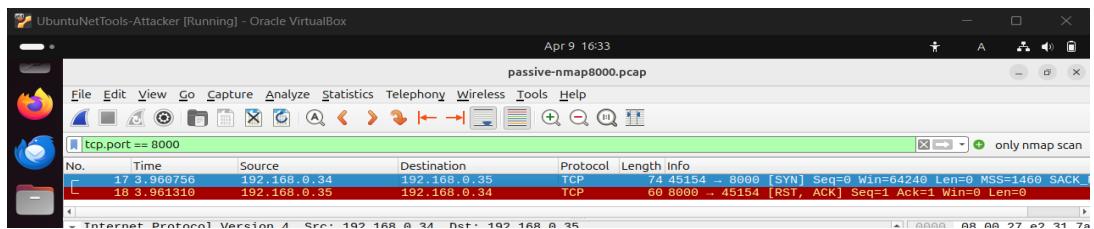
### 1.5.1. When a Service is Listening (Active Scanning)



Captured packets will show TCP flags like:

- SYN and ACK: Indicate that the port is open and responding.
- RST and ACK: Signal that the port is being closed/reset.

### 1.5.2. When No Service is Listening (Passive Scanning)



- SYN: Shows an attempt to initiate a connection (from the scanner).
- RST and ACK: Indicate that no service is available and the connection is being reset.

## Part 2: Detecting a Custom Vulnerability Header Using Nmap NSE

### 2.1 Setting Up a Custom PHP Service on the Target VM

Create a directory and file to simulate a vulnerable web application.

- mkdir www
- nano index.php
  - <?php

```
header('X-Vulnerable-Flag: BUG');

?>
```

### 2.2. Start the PHP Server

Install PHP (if not already installed):

- sudo apt install php

Run the PHP development server (should be in the same directory as index.php):

- php -S 192.168.0.35:8000 -t .

```
ubuntu@ubuntu: ~/www
^Cubuntu@ubuntu:~/www$ php -S 10.0.2.4:8080 -t ~/www
[Fri Apr 18 13:13:06 2025] PHP 8.3.6 Development Server (http://10.0.2.4:8080) started
[Fri Apr 18 13:13:10 2025] 10.0.2.6:40092 Accepted
[Fri Apr 18 13:13:10 2025] 10.0.2.6:40092 Invalid request (Connection reset by peer)
[Fri Apr 18 13:13:10 2025] 10.0.2.6:40092 Closing
[Fri Apr 18 13:13:10 2025] 10.0.2.6:40100 Accepted
[Fri Apr 18 13:13:10 2025] 10.0.2.6:40100 [200]: GET /
[Fri Apr 18 13:13:10 2025] 10.0.2.6:40100 Closing
```

### 2.3. Writing a Custom Nmap NSE Script on the Attacker VM

Create a new NSE script to detect the custom X-Vulnerable-Flag header.

- sudo nano 3inq-vuln-flag.nse

```
ubuntu@ubuntu:/usr/share/nmap/scripts
ubuntu@ubuntu:/usr/share/nmap/scripts$ sudo nano 3inq-vuln-flag.nse
ubuntu@ubuntu:/usr/share/nmap/scripts$ cat 3inq-vuln-flag.nse
local http = require "http"
local shortport = require "shortport"
local stdnse = require "stdnse"

description = [[
Lab2, Part2 - Detects HTTP servers responding with the header 'X-Vulnerable-Flag'
]]

author = "Inqsyira Zamri, 1211103098"
categories = {"discovery", "safe"}

portrule = shortport.http

action = function(host,port)
    local response = http.get(host, port, "/")
    if response and response.header then
        for name, value in pairs(response.header) do
            if string.lower(name) == "x-vulnerable-flag" then
                return "I've Found X-Vulnerable-Flag: " .. value
            end
        end
        return "X-Vulnerable-Flag not there."
    else
        return "No HTTP response received."
    end
end
```

The custom NSE script above uses standard libraries such as http, shortport, and stdnse to handle HTTP requests and scripting logic. It applies the port rule shortport.http, meaning the script only targets HTTP ports. When executed, it sends a GET request to the root (/) of the target web server and checks if a response with headers is received. It then loops through the headers to detect one named X-Vulnerable-Flag, ignoring case sensitivity. If the header is found, the script prints its value; if not, it reports that the flag is not present. In cases where no HTTP response is received at all, the script returns a corresponding message.

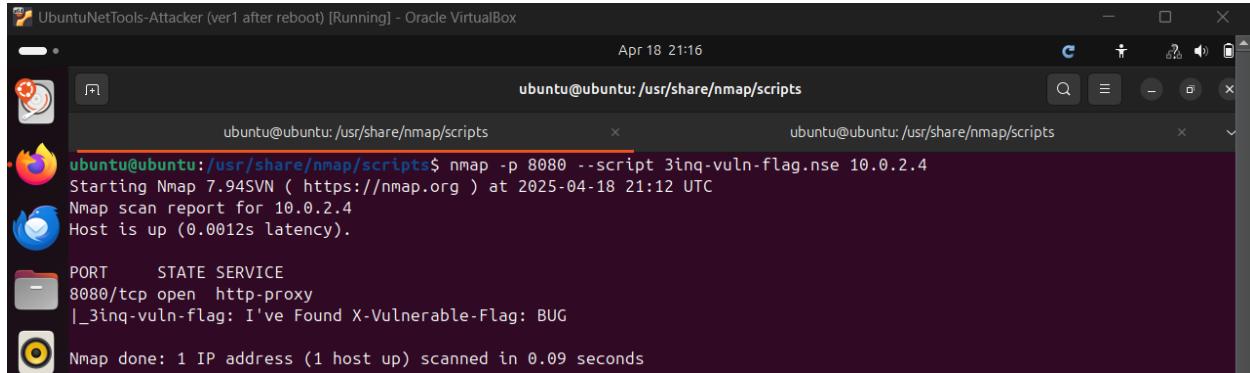
#### 2.3.1 Update the Nmap Script Database

After creating the script, it's important to update Nmap's script database so it recognizes the new .nse file:

- sudo nmap --script-updatedb

## 2.4. Running the NSE Script Against the Target VM

- nmap --script vuln-flag-detect.nse -p 8000 192.168.0.35



The screenshot shows a terminal window titled "UbuntuNetTools-Attacker [ver1 after reboot] [Running] - Oracle VirtualBox". The terminal session is running on an Ubuntu host, with the command `nmap -p 8000 --script vuln-flag-detect.nse 192.168.0.35` being executed. The output indicates that the target host at 192.168.0.35 is up and has port 8000/tcp open, serving an http-proxy service. A custom header "X-Vulnerable-Flag: BUG" was found.

```
ubuntu@ubuntu:~$ nmap -p 8000 --script vuln-flag-detect.nse 192.168.0.35
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-18 21:12 UTC
Nmap scan report for 192.168.0.35
Host is up (0.0012s latency).

PORT      STATE SERVICE
8000/tcp   open  http-proxy
|_3inq-vuln-flag: I've Found X-Vulnerable-Flag: BUG

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

In the screenshot above, the script successfully detected the custom header and printed out: "I've Found X-Vulnerable-Flag: BUG". This indicates that the target HTTP server responded with the X-Vulnerable-Flag header, and its value was set to "BUG". This confirms that the custom vulnerability flag was present, and the script worked as intended.