Ethical Hacking Project Report

Completed by: Luswepo Daniel Sinyinza

PHASE 1: Network and Port Scanning

For my initial ethical hacking practice, I used Kali Linux installed on a virtual machine via the VirtualBox hypervisor. My goal was to scan my host device (a Mac) to identify open ports and running services using Nmap.

1. Basic Network Scan

To begin, I verified connectivity between my Kali Linux VM and the host device.

- Step 1: Ping the Host

I ran the following command to ensure my host (IP: `172.20.10.4`) was reachable:

ping 172.20.10.4

- Step 2: Install Nmap (if not pre-installed)

sudo apt update

sudo apt install nmap

- Step 3: Ping Sweep to Discover Live Devices

I scanned my network to identify active devices:

nmap -sn 172.20.10.1/24

My host device (`172.20.10.4`) appeared in the list of live devices.

2. Port Scan on the Host (Mac)

Next, I conducted a port scan to identify open ports on my host.

- Step 1: Basic Port Scan

To scan common ports (1-1024):

nmap 172.20.10.4

- Step 2: Full Port Scan

To scan all 65,535 ports:

nmap -p- 172.20.10.4

- Step 3: Service Enumeration

To identify services running on the open ports:

nmap -sV 172.20.10.4

PHASE 2: Results of Port Scans

The scans revealed the following open ports on my host:

1. Port 80 (HTTP)
2. Port 5000 (UPnP)
3. Port 7000 (AFS3 Fileserver)

1. Exploring Port 80 (HTTP)

- Goal: Enumerate the HTTP service and identify potential vulnerabilities.

- Step 1: Access the Web Service

curl http://172.20.10.4

Alternatively, I visited `http://172.20.10.4` in a browser.

- Step 2: HTTP Service Enumeration with Nmap

nmap -p 80 --script http-enum 172.20.10.4

- Step 3: Directory Bruteforcing (Optional)

Using Gobuster to find hidden directories:

gobuster dir -u http://172.20.10.4 -w /usr/share/wordlists/dirb/common.txt

2. Exploring Port 5000 (UPnP)

- Goal: Investigate potential misconfigurations in the UPnP service.

- Step 1: UPnP Enumeration with Nmap

nmap -p 5000 --script upnp-info 172.20.10.4

3. Exploring Port 7000 (AFS3 Fileserver)

- Goal: Probe the AFS3 file server for vulnerabilities.

- Step 1: AFS3 Service Scan with Nmap

nmap -p 7000 --script afs3-info 172.20.10.4

PHASE 3: Analysis and Next Steps

Port 80 (HTTP)

The scans indicated:

- A directory listing under `/icons/` suggesting misconfigured access.

- Files like `.htaccess` and `index.html` with accessible (200) and restricted (403) statuses.

Next Steps:

1. Explore the `/icons/` directory:

   curl http://172.20.10.4/icons/

2. Check the contents of `index.html`:

   curl http://172.20.10.4/index.html

3. Research vulnerabilities related to the web server software.

Port 5000 (UPnP)

- The UPnP service may expose network configurations if misconfigured.

Next Steps:

1. Perform deeper UPnP enumeration:

   sudo upnpc -l

2. Investigate known UPnP vulnerabilities.

Port 7000 (AFS3 Fileserver)

- The AFS3 scan revealed limited information.

Next Steps:

1. Further probe using Nmap scripts:

   nmap -p 7000 --script banner 172.20.10.4

2. Research AFS3 vulnerabilities and potential exploits.

PHASE 4: Summary of Findings

1. Port 80 (HTTP)
   - Directory listing under `/icons/` may expose sensitive files.
   - Potential misconfigurations or outdated web server software.

2. Port 5000 (UPnP)
   - UPnP service may present security risks if misconfigured.

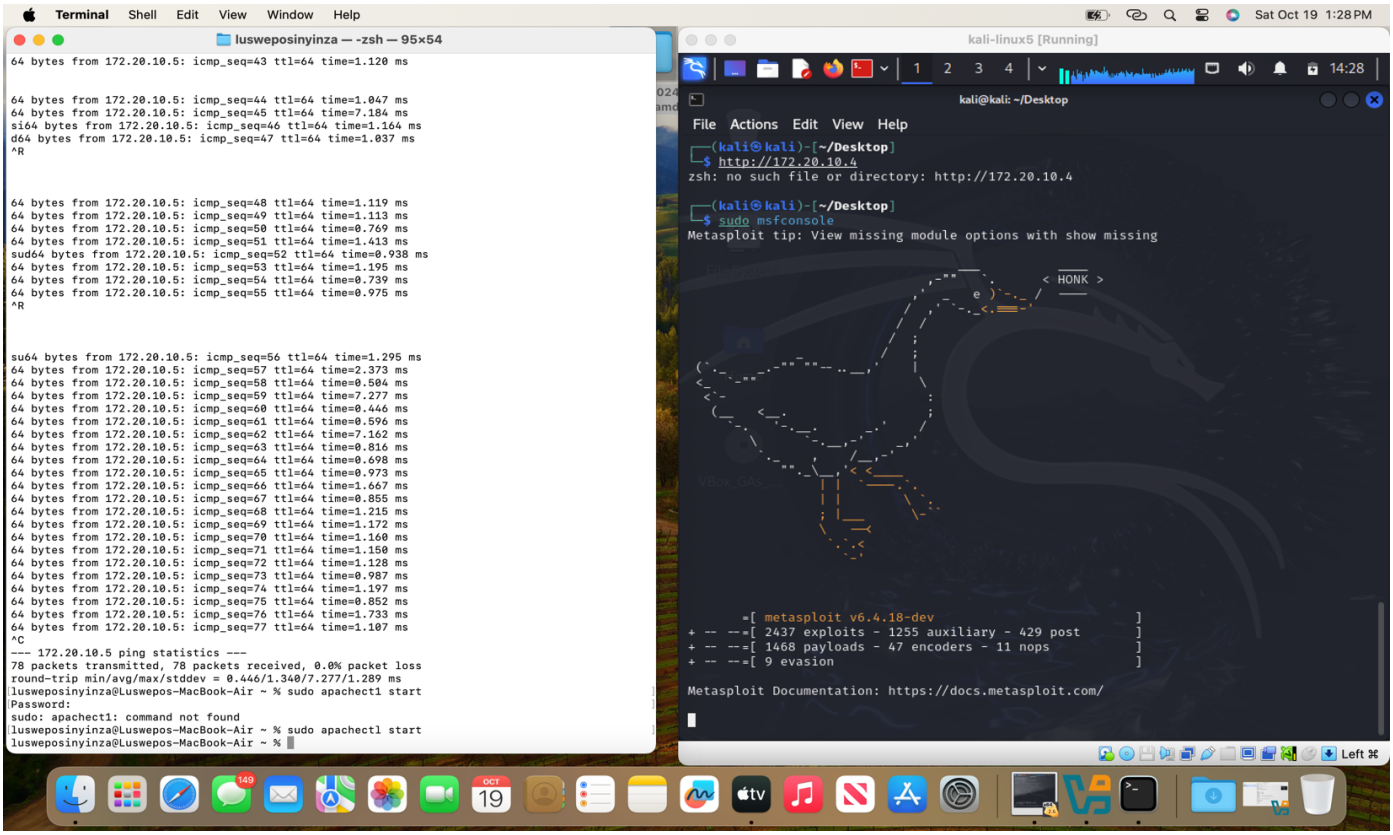
3. Port 7000 (AFS3 Fileserver)
   - Limited information; further investigation needed.

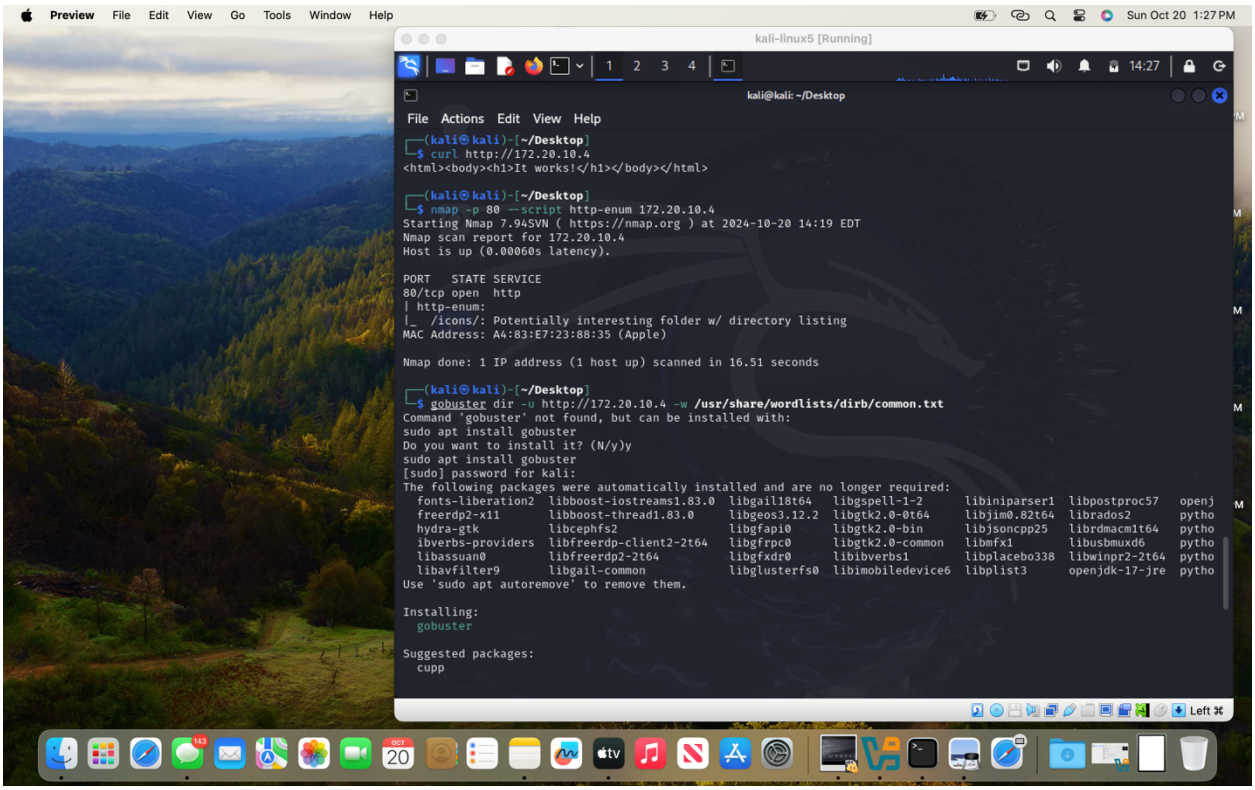
Next Steps:

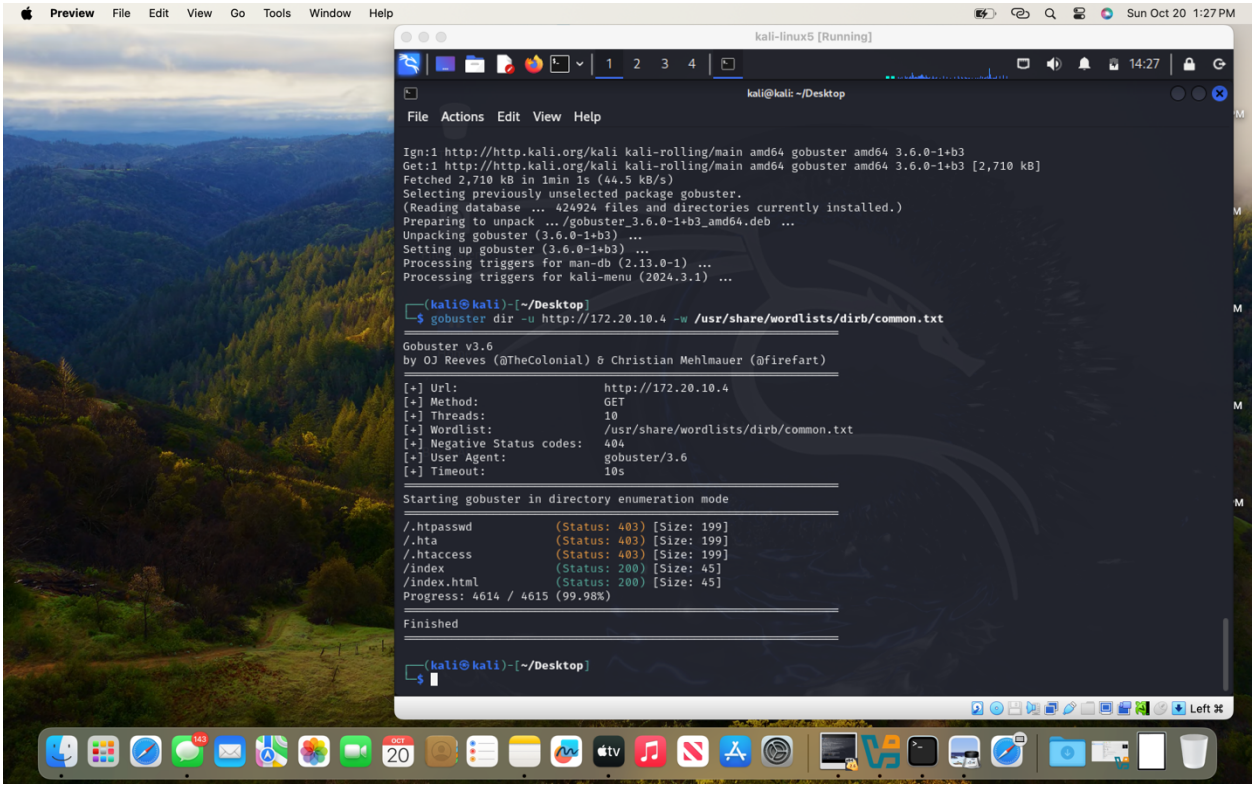
Based on these findings, I will focus on exploiting potential vulnerabilities related to the HTTP service, investigate UPnP misconfigurations, and explore AFS3 weaknesses.

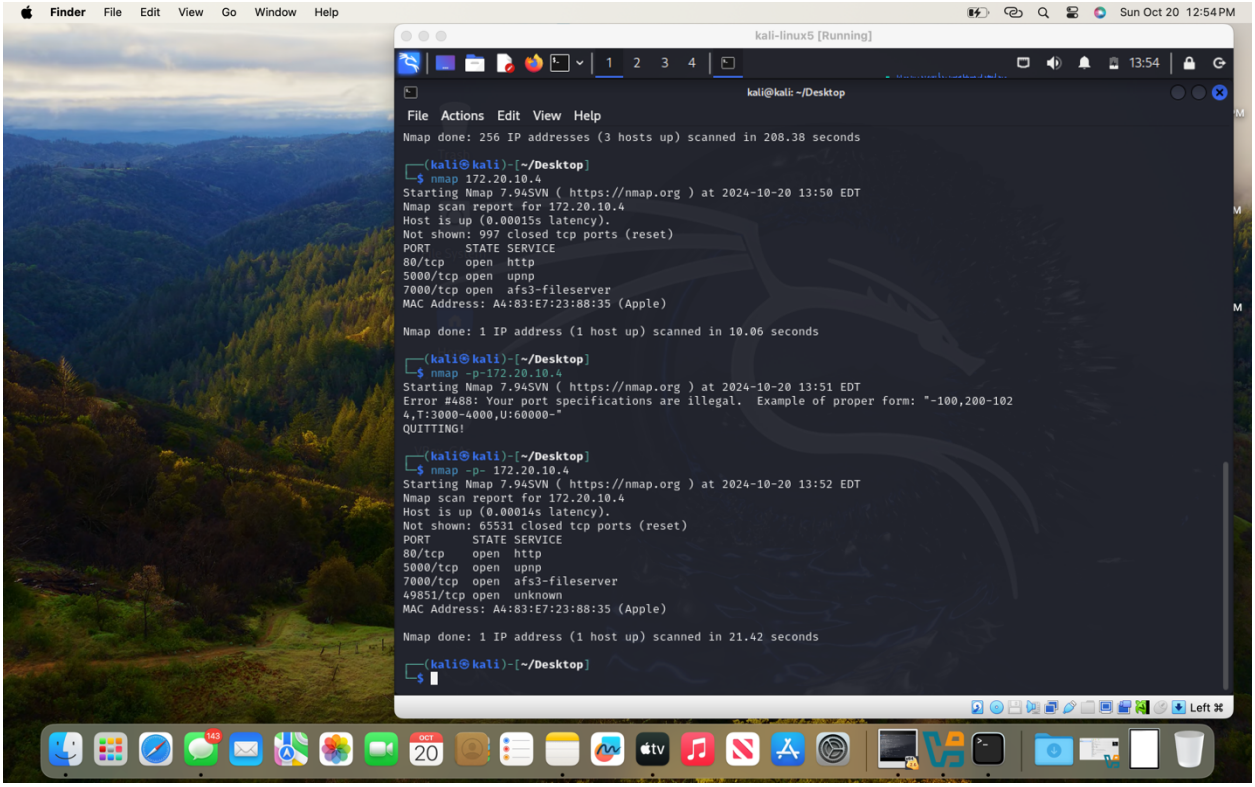
This structured approach provided a clear roadmap for ethical hacking and vulnerability assessment on my host device.

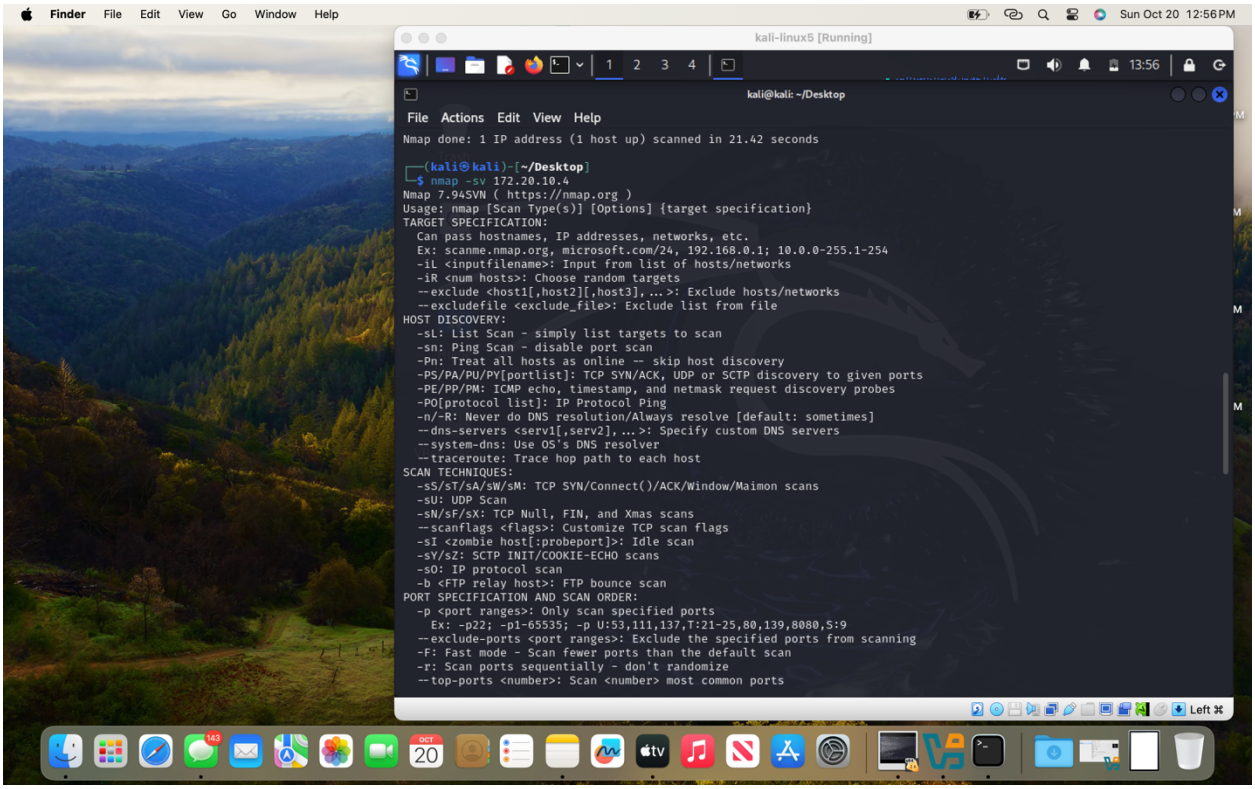
Below are some of the screenshots from the project:




Preview File Edit View Go Tools Window Help
Sun Oct 20 1:27 PM
kali-linux5 [Running]
14:27
kali@kali: ~/Desktop
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop]
└─$ curl http://172.20.10.4
<html><body><h1>It works!</h1></body></html>
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 80 --script http-enum 172.20.10.4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-20 14:19 EDT
Nmap scan report for 172.20.10.4
Host is up (0.00060s latency).
PORT STATE SERVICE
80/tcp open http
| http-enum:
|_ /icons/: Potentially interesting folder w/ directory listing
MAC Address: A4:83:E7:23:88:35 (Apple)
Nmap done: 1 IP address (1 host up) scanned in 16.51 seconds
┌──(kali㉿kali)-[~/Desktop]
└─$ gobuster dir -u http://172.20.10.4 -w /usr/share/wordlists/dirb/common.txt
Command 'gobuster' not found, but can be installed with:
sudo apt install gobuster
Do you want to install it? (N/y)y
sudo apt install gobuster
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
fonts-liberation2 libboost-iostreams1.83.0 libgail18t64 libgspell-1-2 libiniparser1 libpostproc57 openj
freerdp2-x11 libboost-thread1.83.0 libgeos3.12.2 libgtk2.0-0t64 libjim0.82t64 librados2 pytho
hydra-gtk libcephfs2 libgfapi0 libgtk2.0-bin libjsoncpp25 librdmacm1t64 pytho
ibverbs-providers libfreerdp-client2-2t64 libgfrpc0 libgtk2.0-common libmfx1 libusbmuxd6 pytho
libassuan0 libfreerdp2-2t64 libgfxdr0 libibverbs1 libplacebo338 libwinpr2-2t64 pytho
libavfilter9 libgail-common libglusterfs0 libimobiledevice6 libplist3 openjdk-17-jre pytho
Use 'sudo apt autoremove' to remove them.
Installing:
gobuster
Suggested packages:
cupp
Left ⌘


Preview File Edit View Go Tools Window Help
Sun Oct 20 1:27 PM
kali-linux5 [Running]
14:27
kali@kali: ~/Desktop
File Actions Edit View Help
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 gobuster amd64 3.6.0-1+b3
Get:1 http://http.kali.org/kali kali-rolling/main amd64 gobuster amd64 3.6.0-1+b3 [2,710 kB]
Fetched 2,710 kB in 1min 1s (44.5 kB/s)
Selecting previously unselected package gobuster.
(Reading database ... 424924 files and directories currently installed.)
Preparing to unpack .../gobuster_3.6.0-1+b3_amd64.deb ...
Unpacking gobuster (3.6.0-1+b3) ...
Setting up gobuster (3.6.0-1+b3) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.3.1) ...
┌──(kali㉿kali)-[~/Desktop]
└─$ gobuster dir -u http://172.20.10.4 -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://172.20.10.4
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/.htpasswd (Status: 403) [Size: 199]
/.hta (Status: 403) [Size: 199]
/.htaccess (Status: 403) [Size: 199]
/index (Status: 200) [Size: 45]
/index.html (Status: 200) [Size: 45]
Progress: 4614 / 4615 (99.98%)
Finished
┌──(kali㉿kali)-[~/Desktop]
└─$
Left ⌘


Finder File Edit View Go Window Help
Sun Oct 20 12:54 PM
kali-linux5 [Running]
13:54
kali@kali: ~/Desktop
File Actions Edit View Help
Nmap done: 256 IP addresses (3 hosts up) scanned in 208.38 seconds
(kali㉿kali)-[~/Desktop]
$ nmap 172.20.10.4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-20 13:50 EDT
Nmap scan report for 172.20.10.4
Host is up (0.00015s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE
80/tcp open http
5000/tcp open upnp
7000/tcp open afs3-fileserver
MAC Address: A4:83:E7:23:88:35 (Apple)
Nmap done: 1 IP address (1 host up) scanned in 10.06 seconds
(kali㉿kali)-[~/Desktop]
$ nmap -p-172.20.10.4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-20 13:51 EDT
Error #488: Your port specifications are illegal. Example of proper form: "-100,200-102
4,T:3000-4000,U:60000-"
QUITTING!
(kali㉿kali)-[~/Desktop]
$ nmap -p- 172.20.10.4
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-20 13:52 EDT
Nmap scan report for 172.20.10.4
Host is up (0.00014s latency).
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE
80/tcp open http
5000/tcp open upnp
7000/tcp open afs3-fileserver
49851/tcp open unknown
MAC Address: A4:83:E7:23:88:35 (Apple)
Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds
(kali㉿kali)-[~/Desktop]
$
Left ⌘


Finder File Edit View Go Window Help
Sun Oct 20 12:56 PM
kali-linux5 [Running]
13:56
kali@kali: ~/Desktop
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds
(kali㉿kali)-[~/Desktop]
$ nmap -sv 172.20.10.4
Nmap 7.94SVN (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports sequentially - don't randomize
--top-ports <number>: Scan <number> most common ports
Left ⌘