──(root㉿kali)-[~]

└─# ping 192.168.116.131

PING 192.168.116.131 (192.168.116.131) 56(84) bytes of data.

64 bytes from 192.168.116.131: icmp\_seq=1 ttl=64 time=0.407 ms

64 bytes from 192.168.116.131: icmp\_seq=2 ttl=64 time=0.275 ms

64 bytes from 192.168.116.131: icmp\_seq=3 ttl=64 time=0.266 ms

64 bytes from 192.168.116.131: icmp\_seq=4 ttl=64 time=0.245 ms

64 bytes from 192.168.116.131: icmp\_seq=5 ttl=64 time=0.335 ms

64 bytes from 192.168.116.131: icmp\_seq=6 ttl=64 time=0.259 ms

64 bytes from 192.168.116.131: icmp\_seq=7 ttl=64 time=0.302 ms

64 bytes from 192.168.116.131: icmp\_seq=8 ttl=64 time=0.317 ms

64 bytes from 192.168.116.131: icmp\_seq=9 ttl=64 time=0.260 ms

^C

--- 192.168.116.131 ping statistics ---

9 packets transmitted, 9 received, 0% packet loss, time 8200ms

rtt min/avg/max/mdev = 0.245/0.296/0.407/0.048 ms

┌──(root㉿kali)-[~]

└─# nmap -A 192.168.116.131

Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-19 04:12 EST

Nmap scan report for 192.168.116.131

Host is up (0.00025s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|\_http-title: Apache2 Ubuntu Default Page: It works

|\_http-server-header: Apache/2.4.29 (Ubuntu)

MAC Address: 00:0C:29:D5:33:93 (VMware)

Device type: general purpose

Running: Linux 4.X|5.X

OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5

OS details: Linux 4.15 - 5.8

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.25 ms 192.168.116.131

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 8.06 seconds

┌──(root㉿kali)-[~]

└─# nmap -sS 192.168.116.131

Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-19 04:18 EST

Nmap scan report for 192.168.116.131

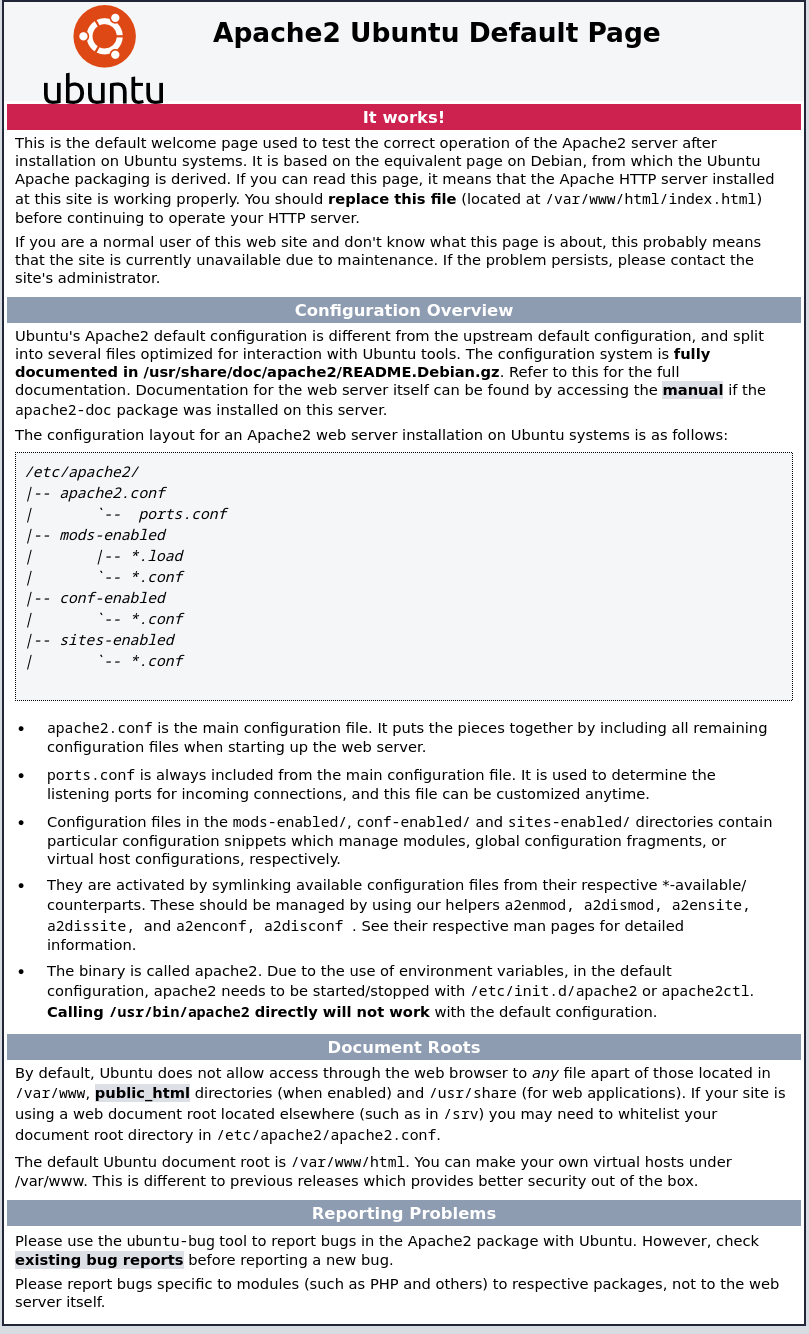
Host is up (0.00032s latency).

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE

80/tcp open http

MAC Address: 00:0C:29:D5:33

:93 (VMware)

Currently scanning: 10.4.153.0/8 | Screen View: Unique Hosts

78 Captured ARP Req/Rep packets, from 4 hosts. Total size: 4680

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IP At MAC Address Count Len MAC Vendor / Hostname

-----------------------------------------------------------------------------

192.168.116.1 00:50:56:c0:00:08 1 60 VMware, Inc.

192.168.116.2 00:50:56:e1:0c:93 20 1200 VMware, Inc.

192.168.116.131 00:0c:29:d5:33:93 55 3300 VMware, Inc.

192.168.116.254 00:50:56:e8:2c:ff 2 120 VMware, Inc.

┌──(root㉿kali)-[~]

└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.116.131/ -x "txt"

===============================================================

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

===============================================================

[+] Url: http://192.168.116.131/ -x txt

[+] Method: GET

[+] Threads: 10

[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.6

[+] Timeout: 10s

===============================================================

Starting gobuster in directory enumeration mode

===============================================================

Progress: 220560 / 220561 (100.00%)

===============================================================

Finished

===============================================================