Footprinting & Scanning

Footprinting & Scanning

Module 1 - Mapping a Network

Mapping a Network

The **Purpose** is Scope and Discovery. Find out what device(s) on the network are we allowed to target, or find what is in scope.

Physical Access

- Physical Security
  - Testing Access Control, Guards, Cameras, anything we can find or get into physically.
- OSINT
  - DNS Records, Websites, IPs, Emails, Domains, etc.
- Social Engineering
  - 'Trick' someone into giving us any information we are after.

Sniffing

- Passive Recon
  - Find hosts, IPs, MAC Addresses are on the network with sniffing.
- Watch Network Traffic
  - Using TCPDump, Wireshark, etc. to see emails, websites visited, what files are being stored or accessed from a file server.

ARP

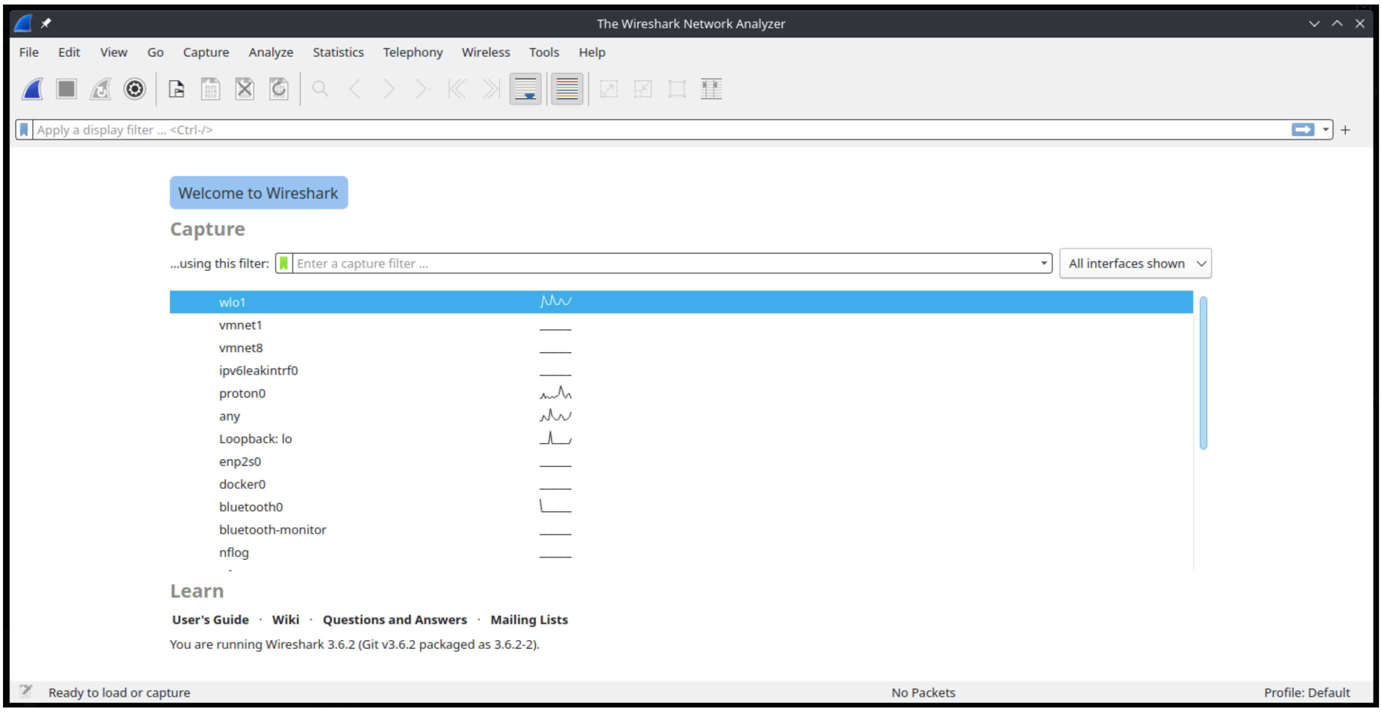
Taking advantage of ARP to resolve IP addresses to MAC addresses to add machines to our ARP table.

ICMP

ICMP can be used for network connectivity issues using Ping or Traceroute.

Tools:

Wireshark



Capture

...using this filter: Enter a capture filter ... All interfaces shown

```
wlo1
vmnet1
vmnet8
ipv6leakintrf0
proton0
any
Loopback: lo
enp2s0
docker0
bluetooth0
bluetooth-monitor
nflog
```

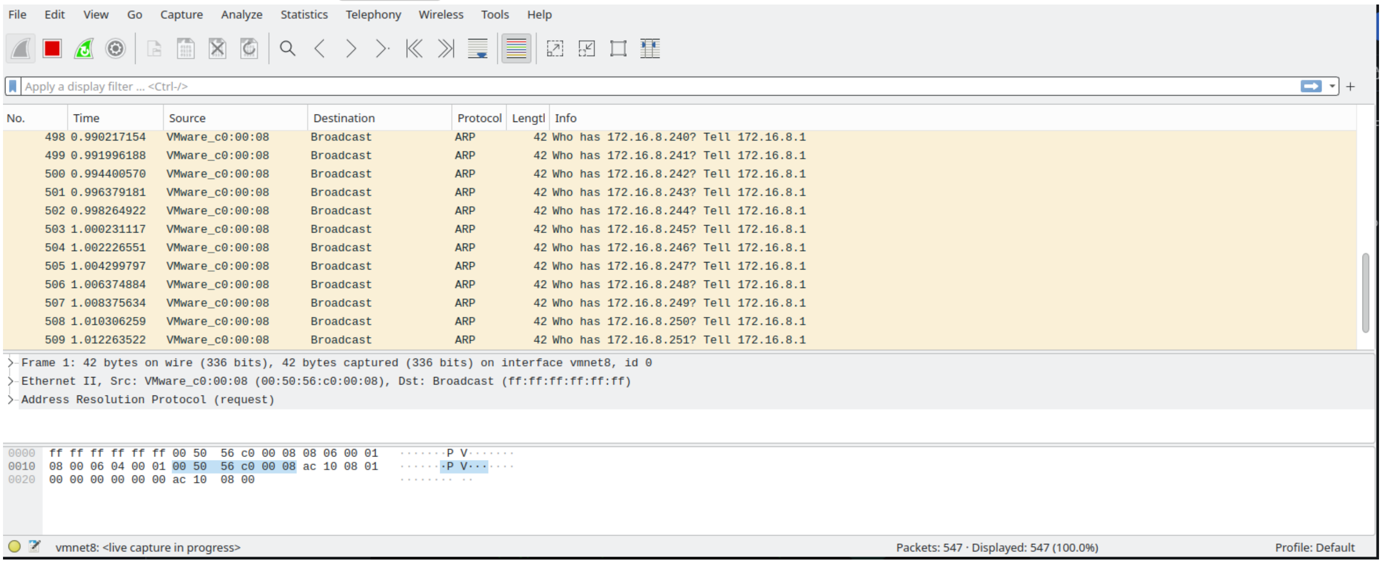
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.2 (Git v3.6.2 packaged as 3.6.2-2).

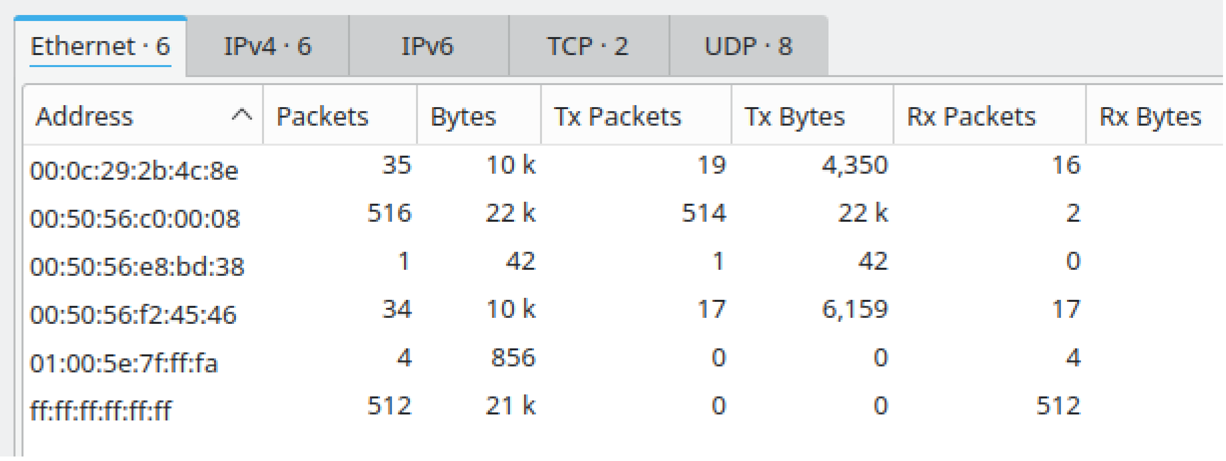
Ready to load or capture   No Packets   Profile: Default

We will be looking at the `vmnet8` adapter to start a packet capture.



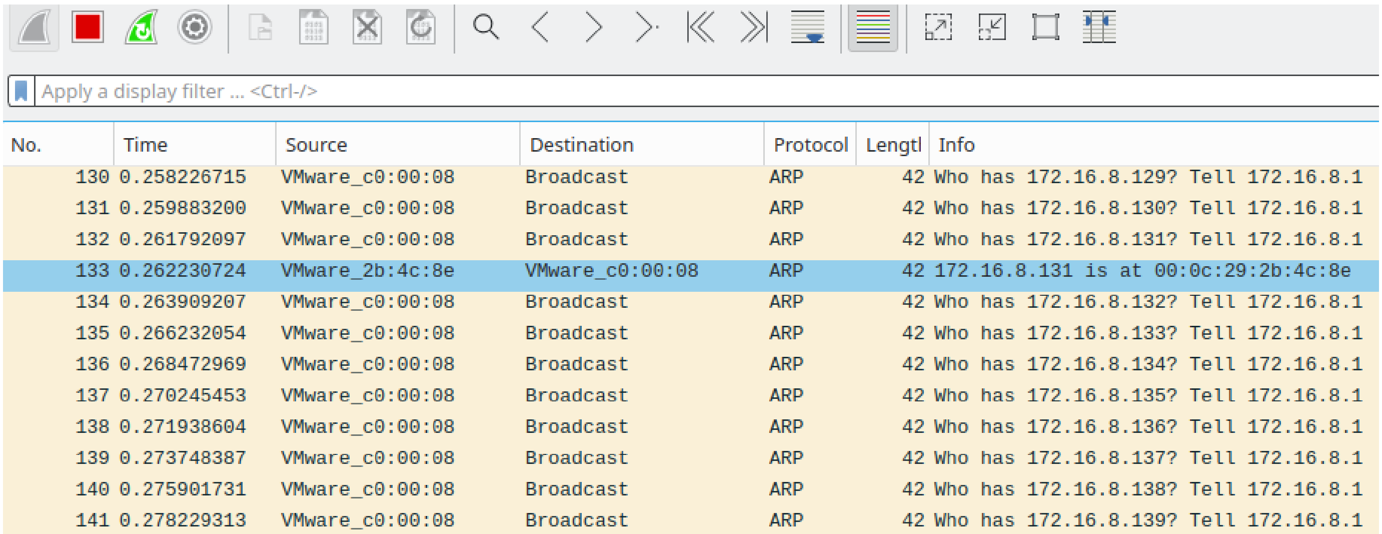
```
No.   Time         Source          Destination  Protocol Lengtl Info
  498 0.990217154  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.240? Tell 172.16.8.1
  499 0.991996188  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.241? Tell 172.16.8.1
  500 0.994400570  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.242? Tell 172.16.8.1
  501 0.996379181  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.243? Tell 172.16.8.1
  502 0.998264922  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.244? Tell 172.16.8.1
  503 1.000231117  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.245? Tell 172.16.8.1
  504 1.002226551  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.246? Tell 172.16.8.1
  505 1.004299797  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.247? Tell 172.16.8.1
  506 1.006374884  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.248? Tell 172.16.8.1
  507 1.008375634  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.249? Tell 172.16.8.1
  508 1.010306259  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.250? Tell 172.16.8.1
  509 1.012263522  VMware_c0:00:08 Broadcast    ARP        42 Who has 172.16.8.251? Tell 172.16.8.1

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface vmnet8, id 0
> Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 50  56 c0 00 08 08 06 00 01   ·······P V·······
0010  08 00 06 04 00 01 00 50  56 c0 00 08 ac 10 08 01   ·······P V·······
0020  00 00 00 00 00 00 ac 10  08 00                     ········ ··

vmnet8: <live capture in progress>    Packets: 547 · Displayed: 547 (100.0%)    Profile: Default
```

We can go to Statistics > Endpoints to see a list of MAC addresses.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:0c:29:2b:4c:8e	35	10 k	19	4,350	16	
00:50:56:c0:00:08	516	22 k	514	22 k	2	
00:50:56:e8:bd:38	1	42	1	42	0	
00:50:56:f2:45:46	34	10 k	17	6,159	17	
01:00:5e:7f:ff:fa	4	856	0	0	4	
ff:ff:ff:ff:ff:ff	512	21 k	0	0	512	

Looking in the logs, we can also see a reply telling us the MAC address of the IP



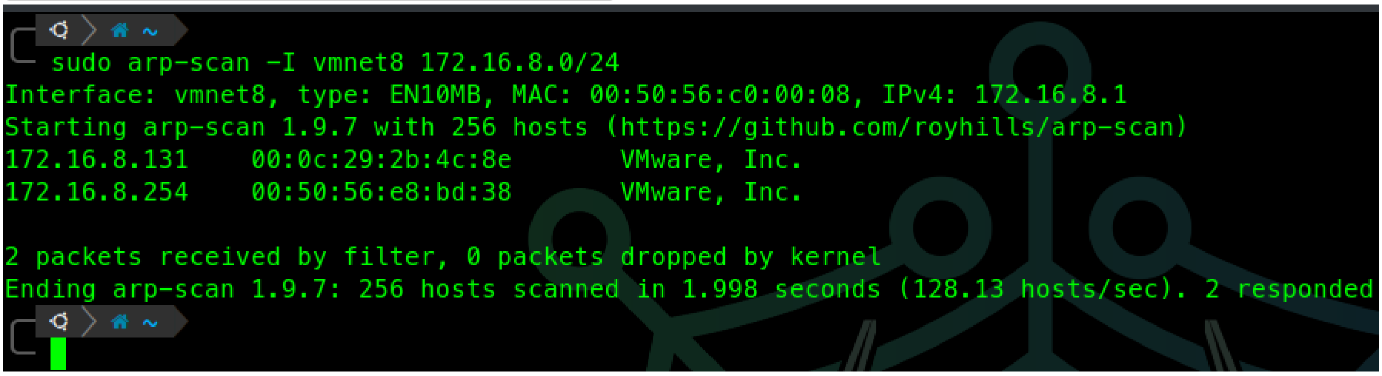
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Lengtl	Info
130	0.258226715	VMware_c0:00:08	Broadcast	ARP	42	Who has 172.16.8.129? Tell 172.16.8.1
131	0.259883200	VMware_c0:00:08	Broadcast	ARP	42	Who has 172.16.8.130? Tell 172.16.8.1
132	0.261792097	VMware_c0:00:08	Broadcast	ARP	42	Who has 172.16.8.131? Tell 172.16.8.1
133	0.262230724	VMware_2b:4c:8e	VMware_c0:00:08	ARP	42	172.16.8.131 is at 00:0c:29:2b:4c:8e
134	0.263909207	VMware_c0:00:08	Broadcast	ARP	42	Who has 172.16.8.132? Tell 172.16.8.1
135	0.266232054	VMware_c0:00:08	Broadcast	ARP	42	Who has 172.16.8.133? Tell 172.16.8.1
136	0.268472969	VMware_c0:00:08	Broadcast	ARP	42	Who has 172.16.8.134? Tell 172.16.8.1
137	0.270245453	VMware_c0:00:08	Broadcast	ARP	42	Who has 172.16.8.135? Tell 172.16.8.1
138	0.271938604	VMware_c0:00:08	Broadcast	ARP	42	Who has 172.16.8.136? Tell 172.16.8.1
139	0.273748387	VMware_c0:00:08	Broadcast	ARP	42	Who has 172.16.8.137? Tell 172.16.8.1
140	0.275901731	VMware_c0:00:08	Broadcast	ARP	42	Who has 172.16.8.138? Tell 172.16.8.1
141	0.278229313	VMware_c0:00:08	Broadcast	ARP	42	Who has 172.16.8.139? Tell 172.16.8.1

ARP-Scan

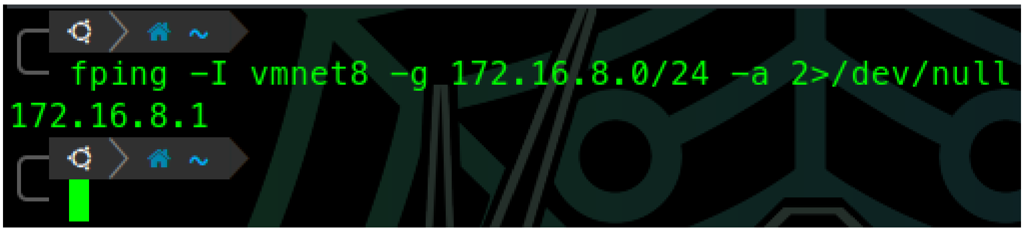
Wecan initiate the arp-scan with `sudo arp-scan -I (interface) (IP and Subnet)`

```
sudo arp-scan -I vmnet8 172.16.8.0/24
```



```
 sudo arp-scan -I vmnet8 172.16.8.0/24
Interface: vmnet8, type: EN10MB, MAC: 00:50:56:c0:00:08, IPv4: 172.16.8.1
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
172.16.8.131    00:0c:29:2b:4c:8e       VMware, Inc.
172.16.8.254    00:50:56:e8:bd:38       VMware, Inc.

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.998 seconds (128.13 hosts/sec). 2 responded
```

Ping



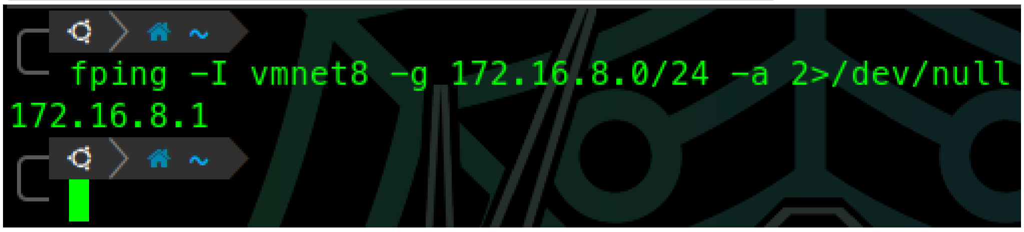
```
 fping -I vmnet8 -g 172.16.8.0/24 -a 2>/dev/null
172.16.8.1
```

We can ping an IP we have found from our scanning to verify communication with the host.

FPing

Will send out pings to multiple hosts at one time. Using `fping -i (internaface) -g (IP Range) -a 2>/dev/null` to show us only the alive hosts removing the all the errors of the unreachable hosts.

```
fping -I vmnet8 -g 172.16.8.0/24 -a 2>/dev/null
```



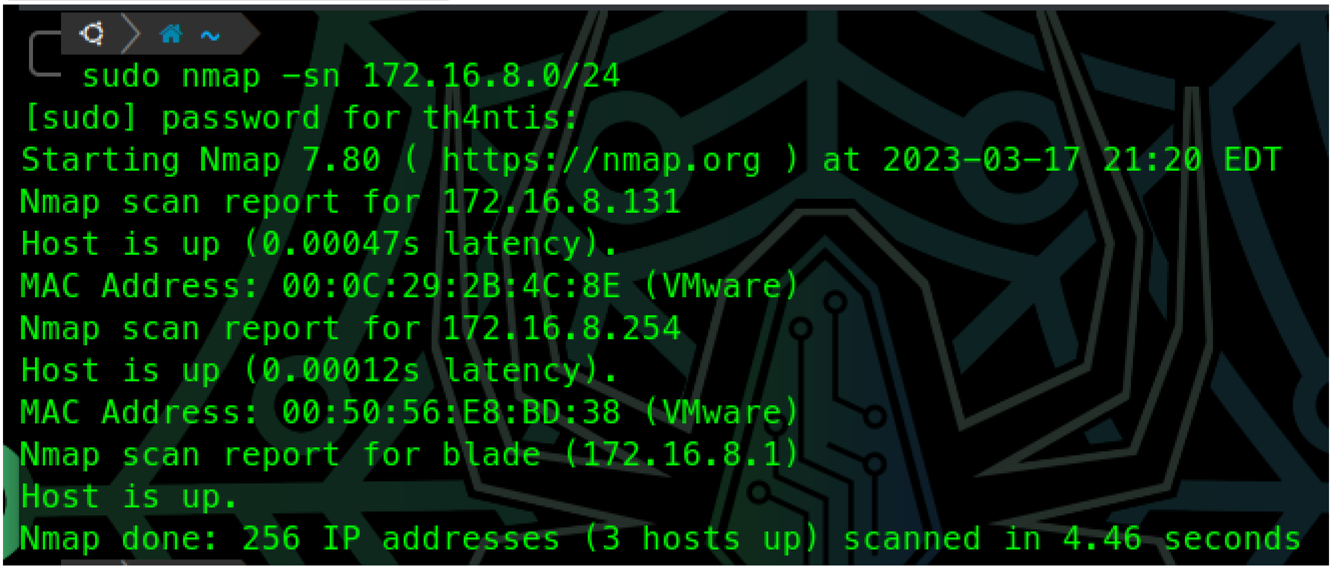
```
 fping -I vmnet8 -g 172.16.8.0/24 -a 2>/dev/null
172.16.8.1
```

Notice the .131 address is missing, this is due to the machine not responding to ping requests.

Nmap

We have seen in the previous section

`sudo nmap -sn 172.16.8.0/24`



```
sudo nmap -sn 172.16.8.0/24
[sudo] password for th4ntis:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-17 21:20 EDT
Nmap scan report for 172.16.8.131
Host is up (0.00047s latency).
MAC Address: 00:0C:29:2B:4C:8E (VMware)
Nmap scan report for 172.16.8.254
Host is up (0.00012s latency).
MAC Address: 00:50:56:E8:BD:38 (VMware)
Nmap scan report for blade (172.16.8.1)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.46 seconds
```

Zenmap

Simple, a GUI version of NMap