Network Protocol Attacks Lab

Author: Harshal Harekar
Date: 30/10/2025

Objective

- Capture NTLMv2 hashes via SMB relay attack.
- Intercept and manipulate traffic between victim and gateway using ARP Spoofing via Ettercap
- Traffic Analysis with Wireshark

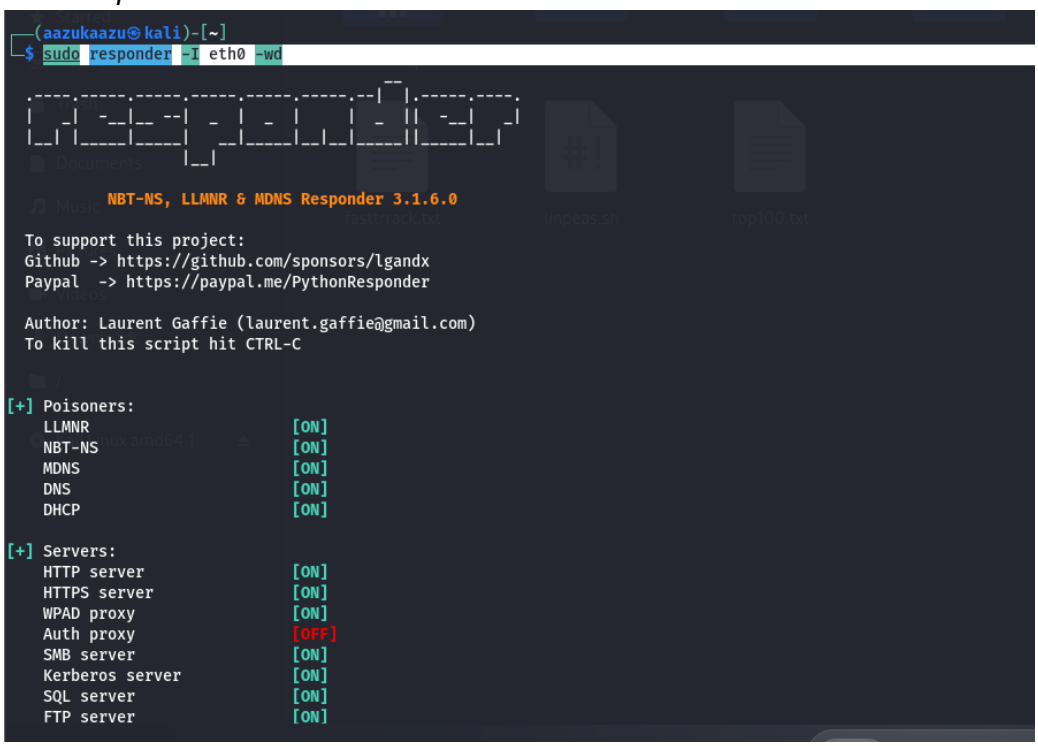
Tools

Responder, Ettercap, Wireshark

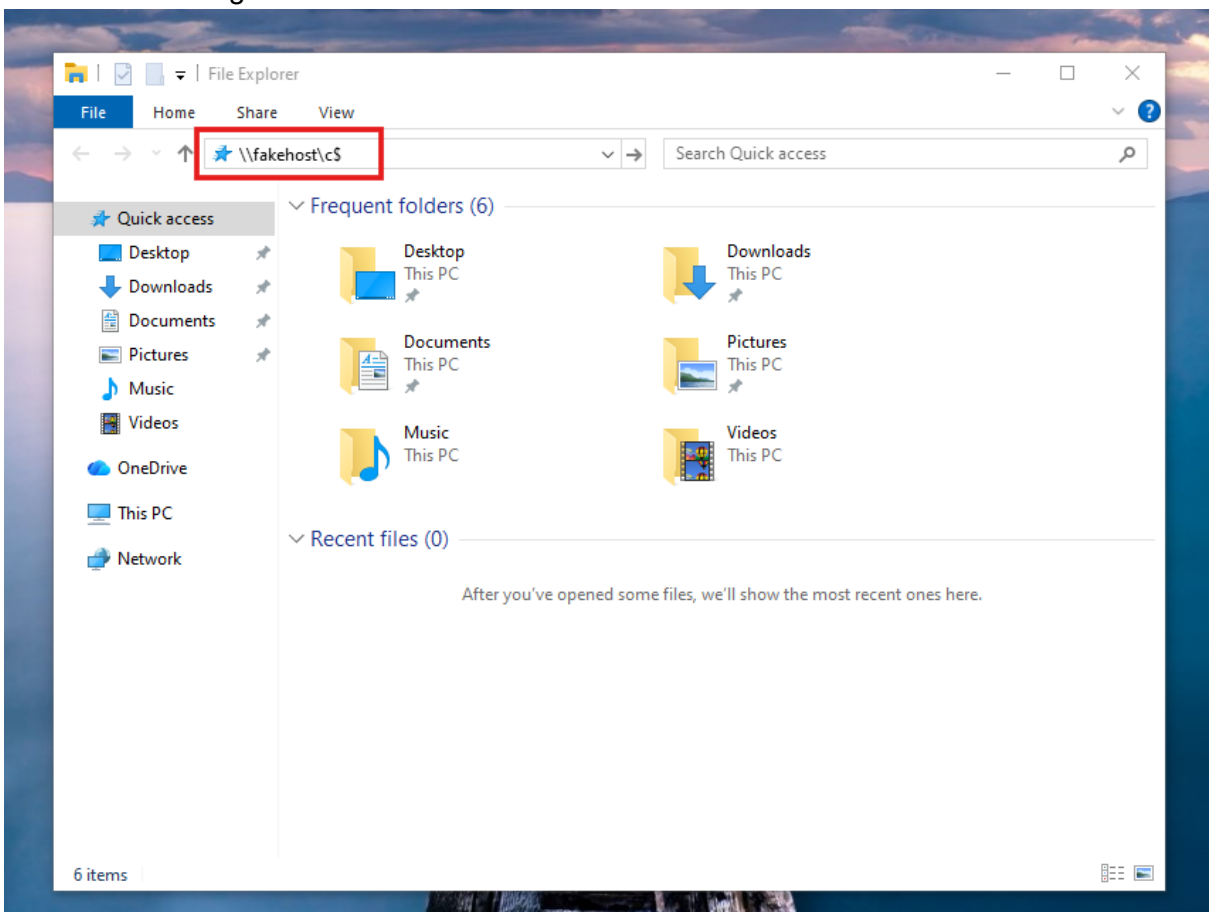
1. SMB Relay with Responder

Steps

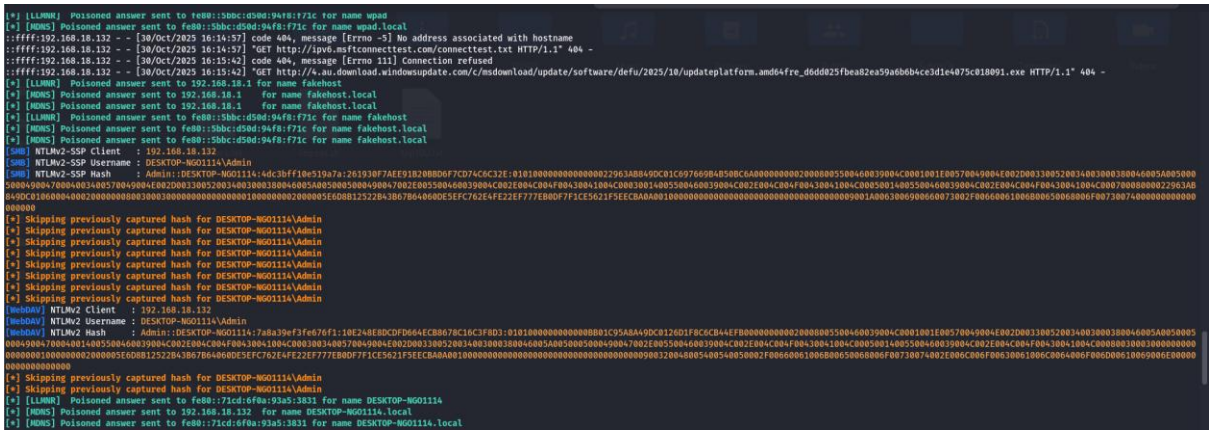
1. Start Responder on Kali:
sudo responder -I eth0 -wd



2. Wait for the target to initiate an SMB connection



3. Responder captures and logs NTLMv2 hashes.



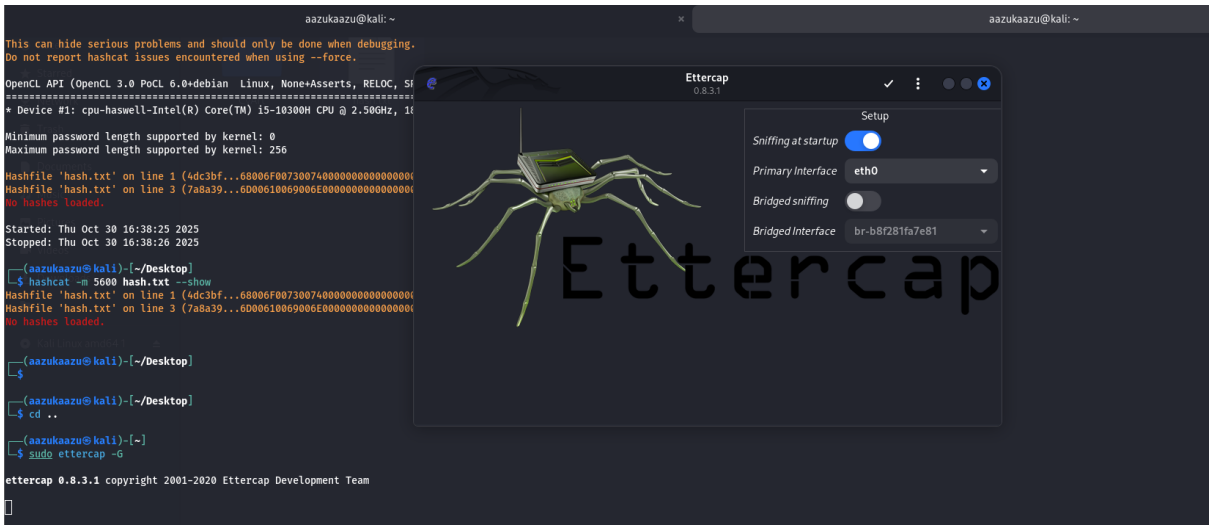
Log

Attack ID	Technique	Target IP	Status	Outcome
001	SMB Relay	192.168.18.132	Success	NTLMv2 Hash

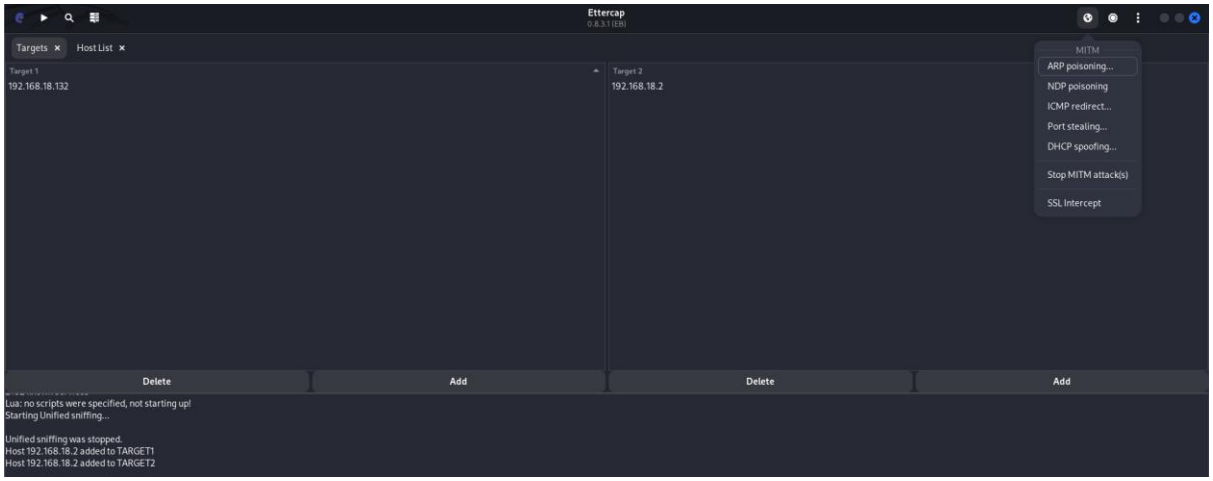
2. MitM : ARP Spoofing with Ettercap

Steps

1. Launch Ettercap in GUI or CLI:
sudo ettercap -G

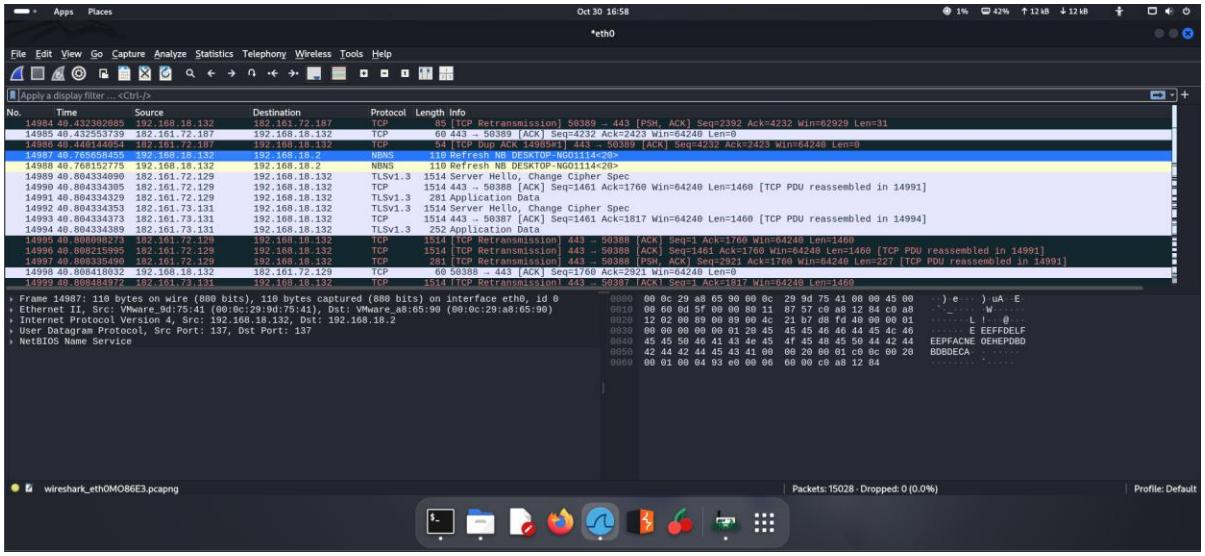


2. Select targets: victim IP and gateway IP



3. Start ARP poisoning and Start Sniffing

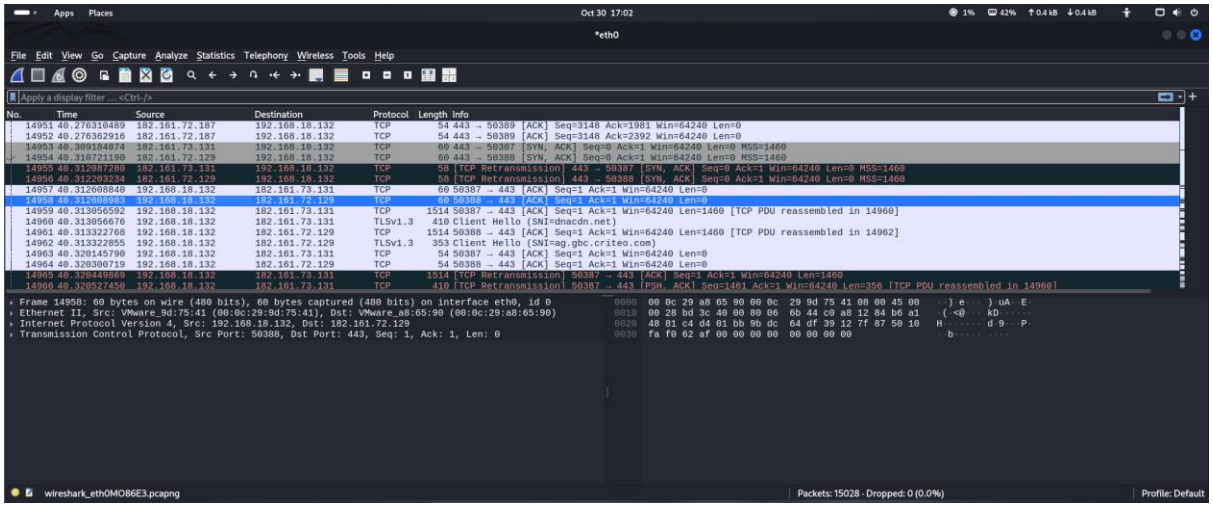
4. In wireshark, we can see the source ip of windows vm



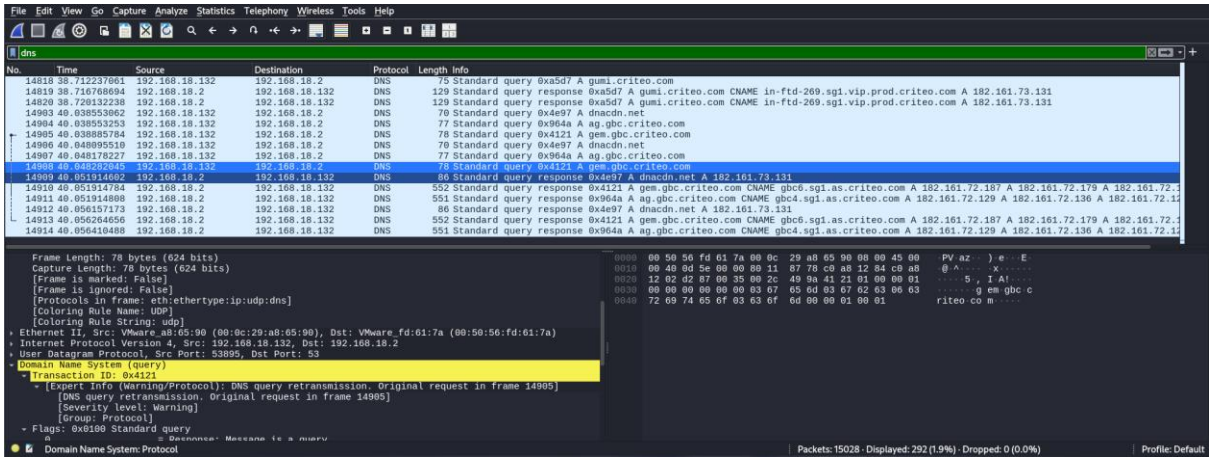
3. Traffic Analysis with Wireshark

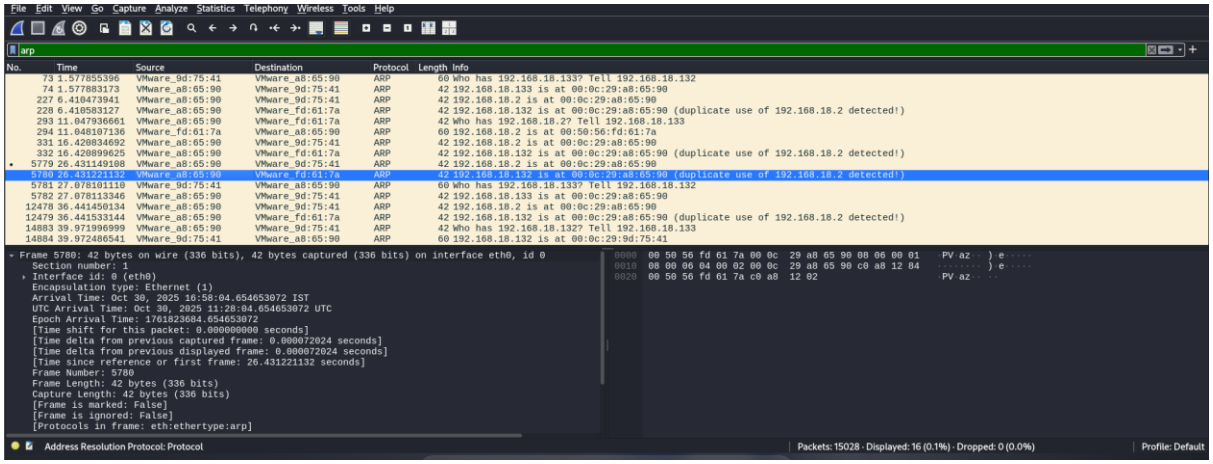
Steps

1. Open Wireshark and start capture on eth0



2. Filter for: smb / dns / http / ntlmssp / arp


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
14818 38.712237061 192.168.18.132 192.168.18.2 DNS 75 Standard query 0xa5d7 A gumi.criteo.com
14819 38.716768694 192.168.18.2 192.168.18.132 DNS 129 Standard query response 0xa5d7 A gumi.criteo.com CNAME in-ftd-269.sg1.vip.prod.criteo.com A 182.161.73.131
14820 38.720132238 192.168.18.2 192.168.18.132 DNS 129 Standard query response 0xa5d7 A gumi.criteo.com CNAME in-ftd-269.sg1.vip.prod.criteo.com A 182.161.73.131
14903 40.038553062 192.168.18.132 192.168.18.2 DNS 70 Standard query 0x4e97 A dnacdn.net
14904 40.038553253 192.168.18.132 192.168.18.2 DNS 77 Standard query 0x964a A ag.gbc.criteo.com
14905 40.038885784 192.168.18.132 192.168.18.2 DNS 78 Standard query 0x4121 A gem.gbc.criteo.com
14906 40.048095510 192.168.18.132 192.168.18.2 DNS 70 Standard query 0x4e97 A dnacdn.net
14907 40.048178227 192.168.18.132 192.168.18.2 DNS 77 Standard query 0x964a A ag.gbc.criteo.com
14908 40.048282045 192.168.18.132 192.168.18.2 DNS 78 Standard query 0x4121 A gem.gbc.criteo.com
14909 40.051914602 192.168.18.2 192.168.18.132 DNS 86 Standard query response 0x4e97 A dnacdn.net A 182.161.73.131
14910 40.051914784 192.168.18.2 192.168.18.132 DNS 552 Standard query response 0x4121 A gem.gbc.criteo.com CNAME gbc6.sg1.as.criteo.com A 182.161.72.187 A 182.161.72.179 A 182.161.72.1
14911 40.051914808 192.168.18.2 192.168.18.132 DNS 551 Standard query response 0x964a A ag.gbc.criteo.com CNAME gbc4.sg1.as.criteo.com A 182.161.72.129 A 182.161.72.136 A 182.161.72.12
14912 40.056157173 192.168.18.2 192.168.18.132 DNS 86 Standard query response 0x4e97 A dnacdn.net A 182.161.73.131
14913 40.056264656 192.168.18.2 192.168.18.132 DNS 552 Standard query response 0x4121 A gem.gbc.criteo.com CNAME gbc6.sg1.as.criteo.com A 182.161.72.187 A 182.161.72.179 A 182.161.72.1
14914 40.056410488 192.168.18.2 192.168.18.132 DNS 551 Standard query response 0x964a A ag.gbc.criteo.com CNAME gbc4.sg1.as.criteo.com A 182.161.72.129 A 182.161.72.136 A 182.161.72.12
Frame Length: 78 bytes (624 bits)
Capture Length: 78 bytes (624 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: VMware_a8:65:90 (00:0c:29:a8:65:90), Dst: VMware_fd:61:7a (00:50:56:fd:61:7a)
Internet Protocol Version 4, Src: 192.168.18.132, Dst: 192.168.18.2
User Datagram Protocol, Src Port: 53895, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x4121
[Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame 14905]
[DNS query retransmission. Original request in frame 14905]
[Severity level: Warning]
[Group: Protocol]
Flags: 0x0100 Standard query
0000 00 50 56 fd 61 7a 00 0c 29 a8 65 90 08 00 45 00
0010 00 40 0d 5e 00 00 80 11 87 78 c0 a8 12 84 c0 a8
0020 12 02 d2 87 00 35 00 2c 49 9a 41 21 01 00 00 01
0030 00 00 00 00 00 00 03 67 65 6d 03 67 62 63 06 63
0040 72 69 74 65 6f 03 63 6f 6d 00 00 01 00 01
Domain Name System: Protocol
Packets: 15028 · Displayed: 292 (1.9%) · Dropped: 0 (0.0%)
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Protocol Length Info
73 1.577855396 VMware_9d:75:41 VMware_a8:65:90 ARP 60 Who has 192.168.18.133? Tell 192.168.18.132
74 1.577883173 VMware_a8:65:90 VMware_9d:75:41 ARP 42 192.168.18.133 is at 00:0c:29:a8:65:90
227 6.410473941 VMware_a8:65:90 VMware_9d:75:41 ARP 42 192.168.18.2 is at 00:0c:29:a8:65:90
228 6.410583127 VMware_a8:65:90 VMware_fd:61:7a ARP 42 192.168.18.132 is at 00:0c:29:a8:65:90 (duplicate use of 192.168.18.2 detected!)
293 11.047936661 VMware_a8:65:90 VMware_fd:61:7a ARP 42 Who has 192.168.18.2? Tell 192.168.18.133
294 11.048107136 VMware_fd:61:7a VMware_a8:65:90 ARP 60 192.168.18.2 is at 00:50:56:fd:61:7a
331 16.420834692 VMware_a8:65:90 VMware_9d:75:41 ARP 42 192.168.18.2 is at 00:0c:29:a8:65:90
332 16.420899625 VMware_a8:65:90 VMware_fd:61:7a ARP 42 192.168.18.132 is at 00:0c:29:a8:65:90 (duplicate use of 192.168.18.2 detected!)
5779 26.431149108 VMware_a8:65:90 VMware_9d:75:41 ARP 42 192.168.18.2 is at 00:0c:29:a8:65:90
5780 26.431221132 VMware_a8:65:90 VMware_fd:61:7a ARP 42 192.168.18.132 is at 00:0c:29:a8:65:90 (duplicate use of 192.168.18.2 detected!)
5781 27.078101110 VMware_9d:75:41 VMware_a8:65:90 ARP 60 Who has 192.168.18.133? Tell 192.168.18.132
5782 27.078113346 VMware_a8:65:90 VMware_9d:75:41 ARP 42 192.168.18.133 is at 00:0c:29:a8:65:90
12478 36.441450134 VMware_a8:65:90 VMware_9d:75:41 ARP 42 192.168.18.2 is at 00:0c:29:a8:65:90
12479 36.441533144 VMware_a8:65:90 VMware_fd:61:7a ARP 42 192.168.18.132 is at 00:0c:29:a8:65:90 (duplicate use of 192.168.18.2 detected!)
14883 39.971996999 VMware_a8:65:90 VMware_9d:75:41 ARP 42 Who has 192.168.18.132? Tell 192.168.18.133
14884 39.972486541 VMware_9d:75:41 VMware_a8:65:90 ARP 60 192.168.18.132 is at 00:0c:29:9d:75:41
Frame 5780: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Section number: 1
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 30, 2025 16:58:04.654653072 IST
UTC Arrival Time: Oct 30, 2025 11:28:04.654653072 UTC
Epoch Arrival Time: 1761823684.654653072
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000072024 seconds]
[Time delta from previous displayed frame: 0.000072024 seconds]
[Time since reference or first frame: 26.431221132 seconds]
Frame Number: 5780
Frame Length: 42 bytes (336 bits)
Capture Length: 42 bytes (336 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
0000 00 50 56 fd 61 7a 00 0c 29 a8 65 90 08 06 00 01
0010 08 00 06 04 00 02 00 0c 29 a8 65 90 c0 a8 12 84
0020 00 50 56 fd 61 7a c0 a8 12 02
Address Resolution Protocol: Protocol
Packets: 15028 · Displayed: 16 (0.1%) · Dropped: 0 (0.0%)
Profile: Default