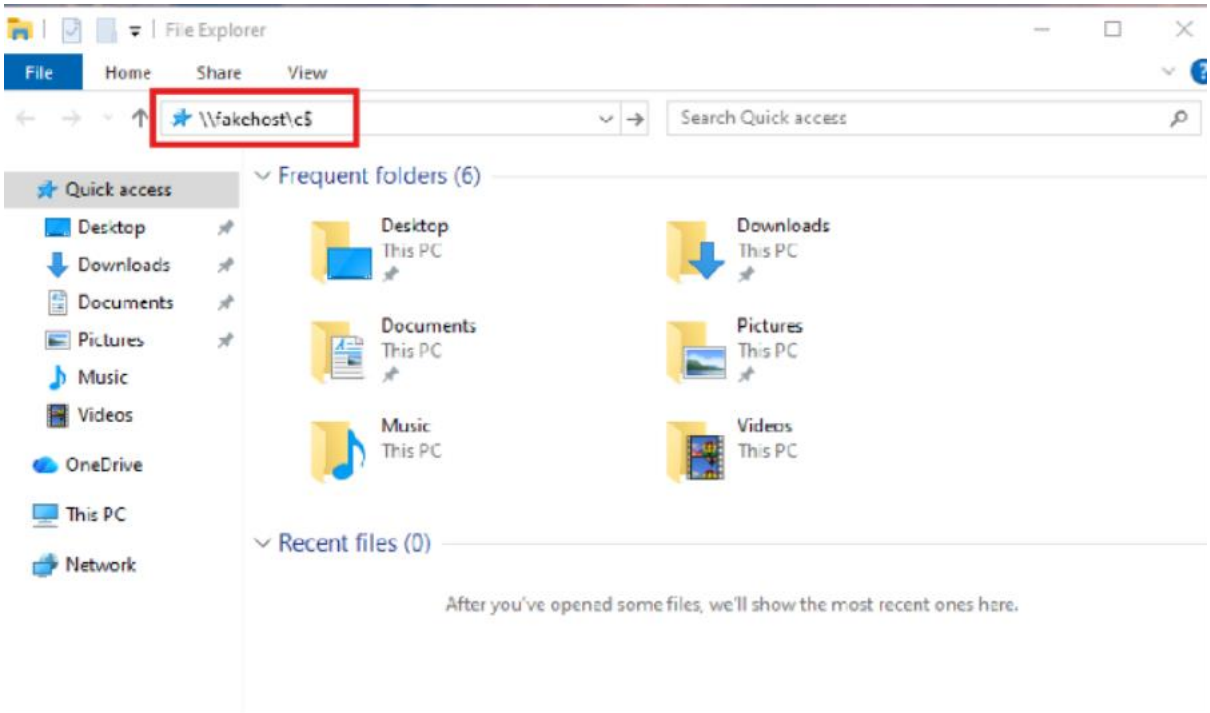
1. Network Protocol Attacks

1.1 SMB Relay

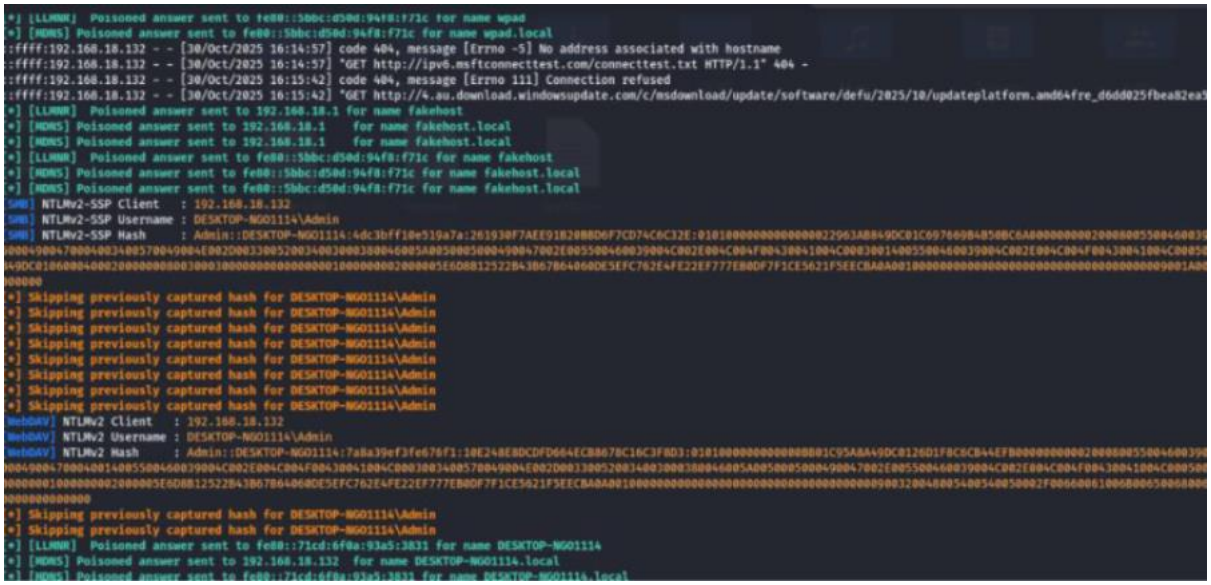
Start the responder in you kali Linux by using the following command as

sudo responder -I eth0 -wd

Waited for sometime to get the result as SMB relay and i got it

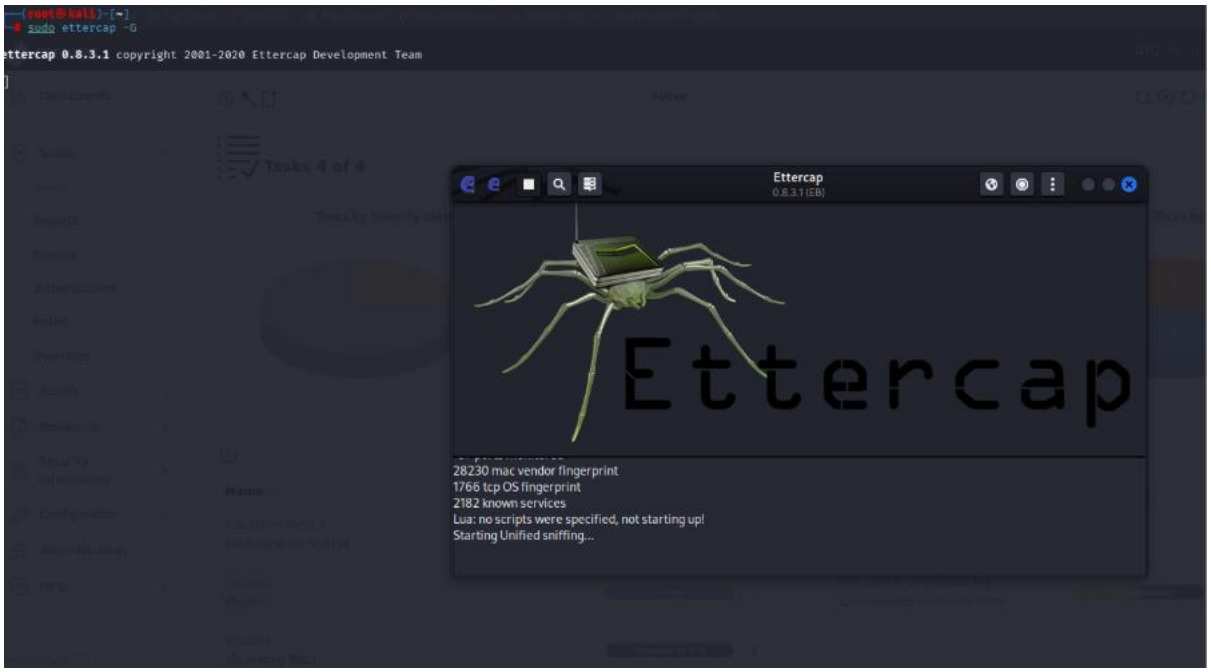


Then responsder captures and logs NTLMv2 hashes

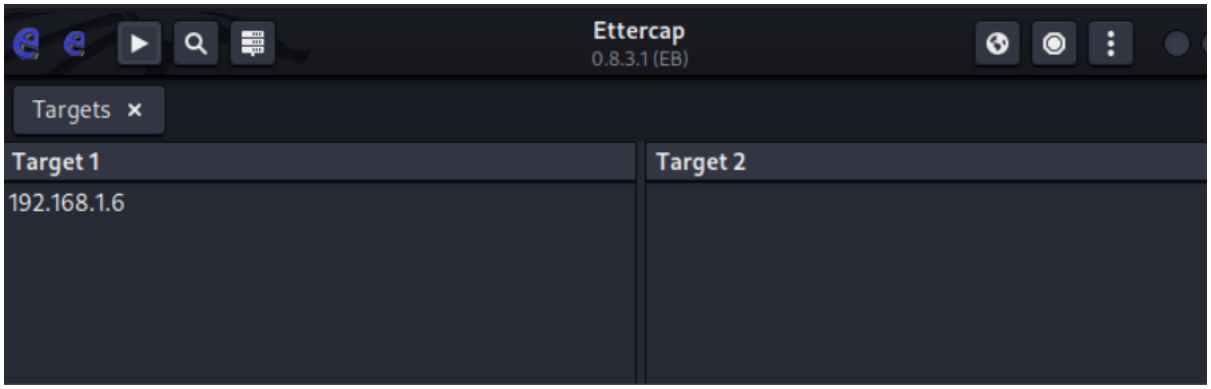


1.2 Mitm: ARP spoofing with Ettercap

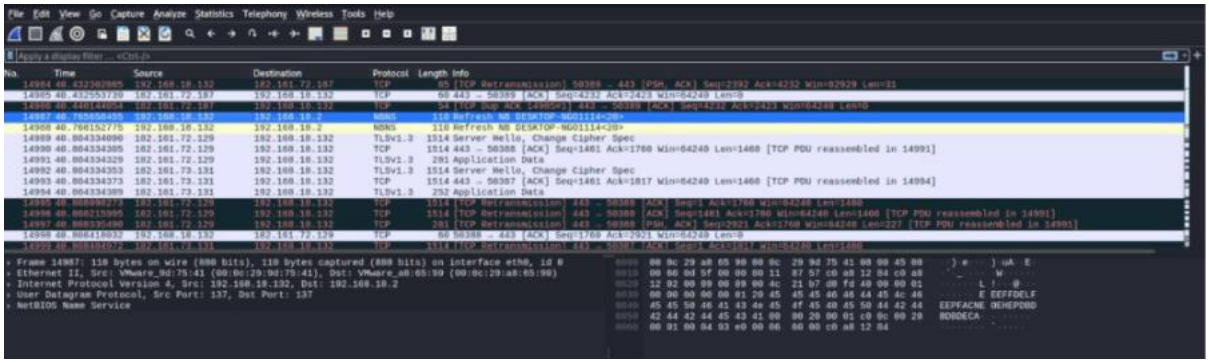
Start the Ettercap either cli/gui in your kali Linux



Then, setup a target through the Ip address and also start the ARP spoofing and start Sniffing.

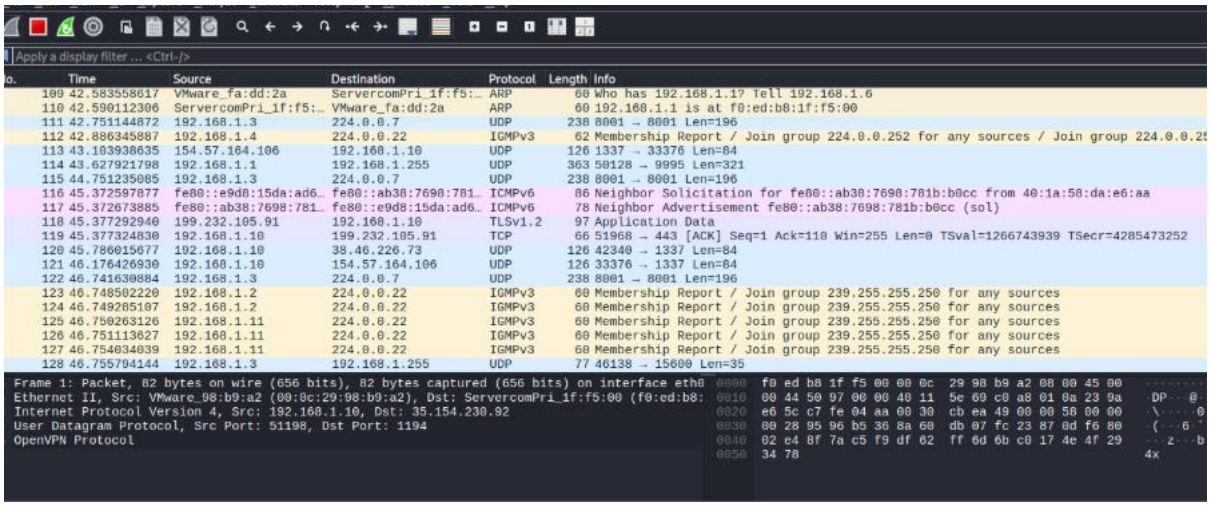


In wireshark, you can see that source ip of windows vm machine.

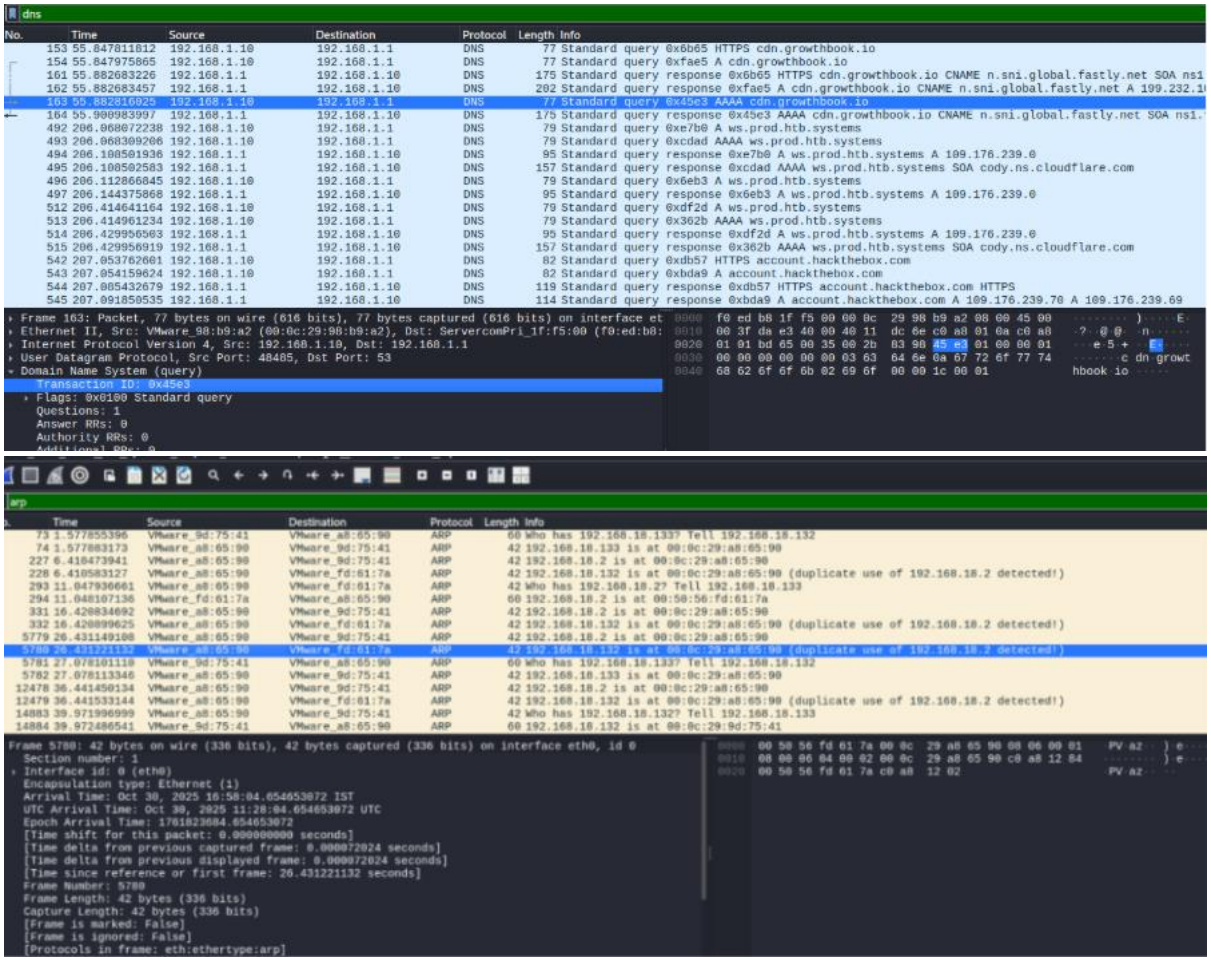


1.3 Traffic Analysis With Wireshark

Open wireshark and start the capture with eth0 and analyse the packets.



Filter for different ports as smb, arp and Dns


dns
No. Time Source Destination Protocol Length Info
153 55.847011812 192.168.1.10 192.168.1.1 DNS 77 Standard query 0x6b65 HTTPS cdn.growthbook.io
154 55.847975865 192.168.1.10 192.168.1.1 DNS 77 Standard query 0xfae5 A cdn.growthbook.io
161 55.882683226 192.168.1.1 192.168.1.10 DNS 175 Standard query response 0x6b65 HTTPS cdn.growthbook.io CNAME n.sni.global.fastly.net SOA ns1
162 55.882683457 192.168.1.1 192.168.1.10 DNS 202 Standard query response 0xfae5 A cdn.growthbook.io CNAME n.sni.global.fastly.net A 199.232.1
163 55.882816025 192.168.1.10 192.168.1.1 DNS 77 Standard query 0x45e3 AAAA cdn.growthbook.io
164 55.900983997 192.168.1.1 192.168.1.10 DNS 175 Standard query response 0x45e3 AAAA cdn.growthbook.io CNAME n.sni.global.fastly.net SOA ns1.
492 206.068072238 192.168.1.10 192.168.1.1 DNS 79 Standard query 0xe7b0 A ws.prod.htb.systems
493 206.068309206 192.168.1.10 192.168.1.1 DNS 79 Standard query 0xcdad AAAA ws.prod.htb.systems
494 206.108501936 192.168.1.1 192.168.1.10 DNS 95 Standard query response 0xe7b0 A ws.prod.htb.systems A 109.176.239.0
495 206.108502583 192.168.1.1 192.168.1.10 DNS 157 Standard query response 0xcdad AAAA ws.prod.htb.systems SOA cody.ns.cloudflare.com
496 206.112866845 192.168.1.10 192.168.1.1 DNS 79 Standard query 0x6eb3 A ws.prod.htb.systems
497 206.144375868 192.168.1.1 192.168.1.10 DNS 95 Standard query response 0x6eb3 A ws.prod.htb.systems A 109.176.239.0
512 206.414641164 192.168.1.10 192.168.1.1 DNS 79 Standard query 0xdf2d A ws.prod.htb.systems
513 206.414961234 192.168.1.10 192.168.1.1 DNS 79 Standard query 0x362b AAAA ws.prod.htb.systems
514 206.429956503 192.168.1.1 192.168.1.10 DNS 95 Standard query response 0xdf2d A ws.prod.htb.systems A 109.176.239.0
515 206.429956919 192.168.1.1 192.168.1.10 DNS 157 Standard query response 0x362b AAAA ws.prod.htb.systems SOA cody.ns.cloudflare.com
542 207.053762601 192.168.1.10 192.168.1.1 DNS 82 Standard query 0xdb57 HTTPS account.hackthebox.com
543 207.054159624 192.168.1.10 192.168.1.1 DNS 82 Standard query 0xbda9 A account.hackthebox.com
544 207.085432679 192.168.1.1 192.168.1.10 DNS 119 Standard query response 0xdb57 HTTPS account.hackthebox.com HTTPS
545 207.091850535 192.168.1.1 192.168.1.10 DNS 114 Standard query response 0xbda9 A account.hackthebox.com A 109.176.239.70 A 109.176.239.69
Frame 163: Packet, 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface et
Ethernet II, Src: VMware_98:b9:a2 (00:0c:29:98:b9:a2), Dst: ServercomPri_1f:f5:00 (f0:ed:b8:
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 48485, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x45e3
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
0000 f0 ed b8 1f f5 00 00 0c 29 98 b9 a2 08 00 45 00
0010 00 3f da e3 40 00 40 11 dc 6e c0 a8 01 0a c0 a8
0020 01 01 bd 65 00 35 00 2b 83 98 45 e3 01 00 00 01
0030 00 00 00 00 00 00 03 63 64 6e 0a 67 72 6f 77 74
0040 68 62 6f 6f 6b 02 69 6f 00 00 1c 00 01
hbook io

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 6.418473941 VMware_a8:65:90 VMware_9d:75:41 ARP 42 192.168.18.2 is at 00:0c:29:a8:65:90
228 6.418583127 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 16.420889625 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 26.431149100 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 27.078101118 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