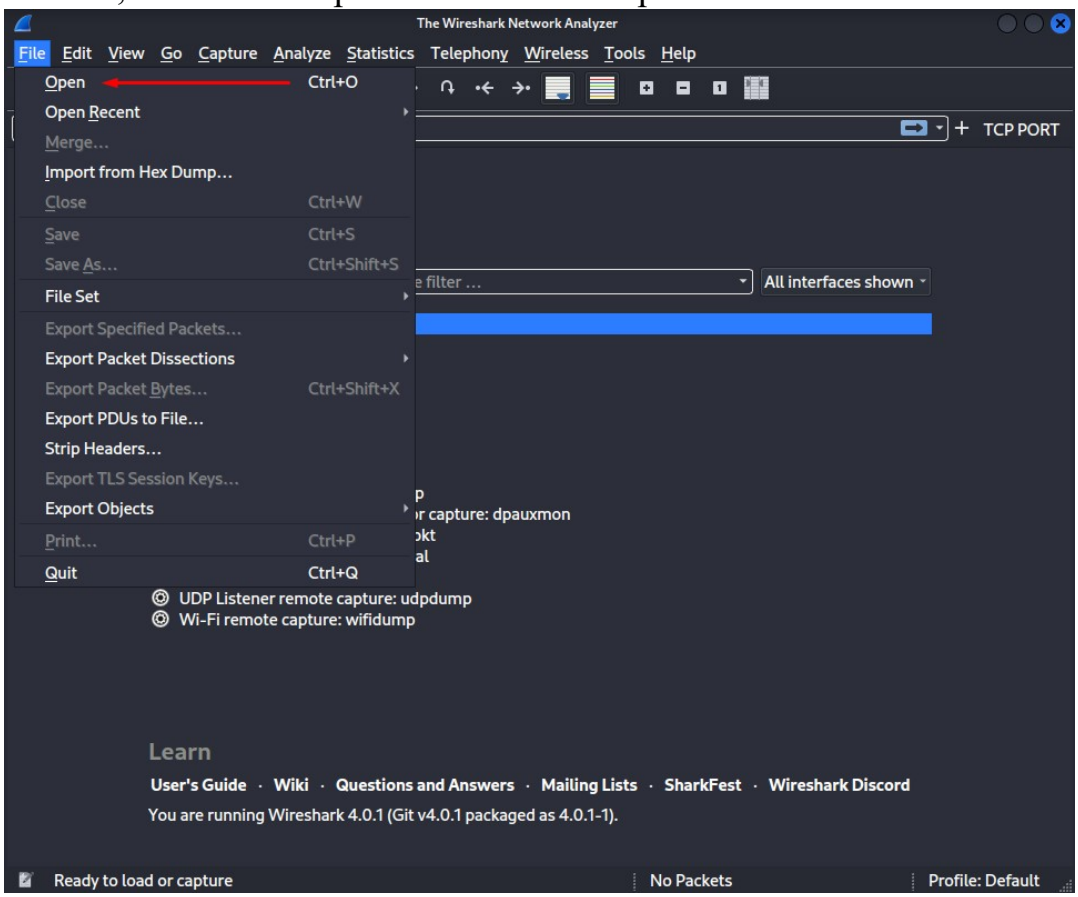
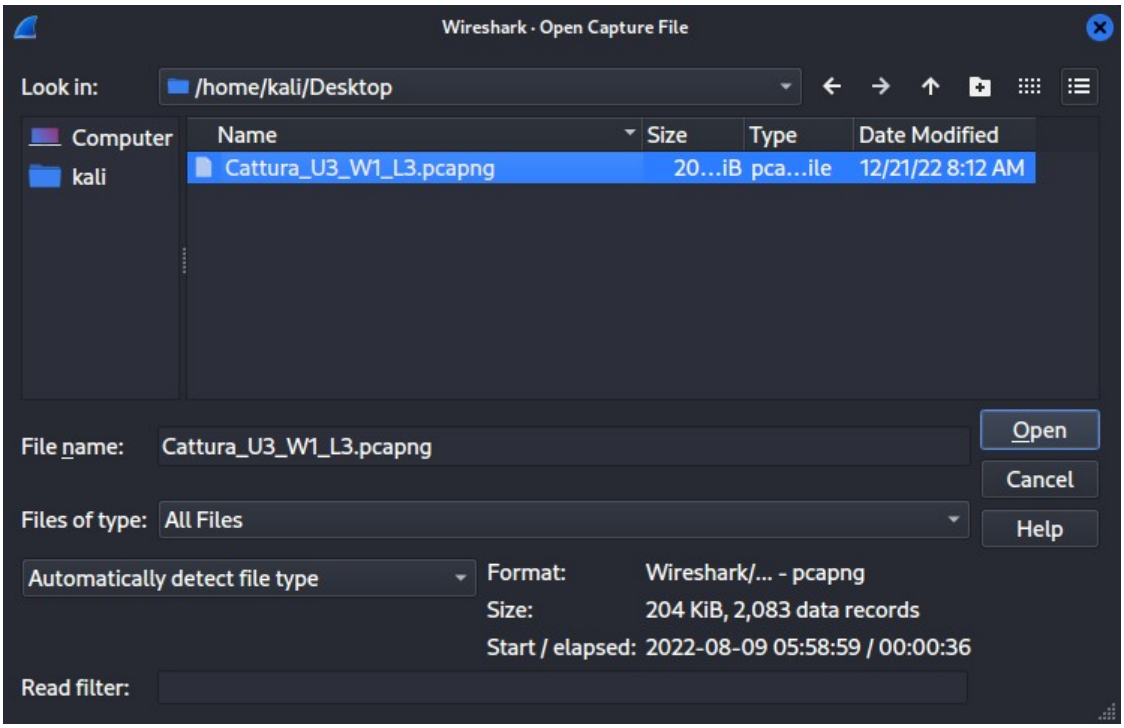
Alaimo Alessandro
21/12/2022

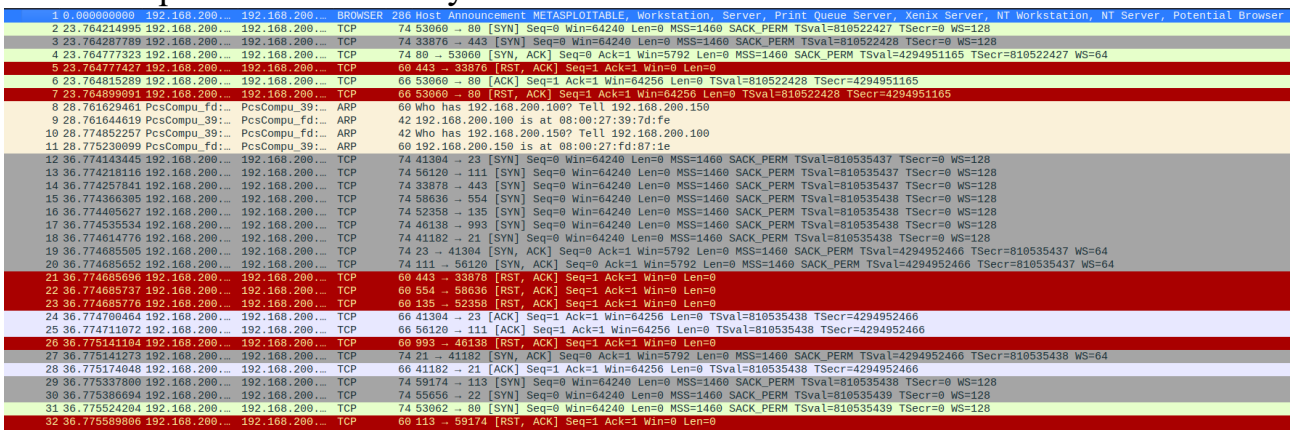
Report Thread Intelligence & IOC

Dopo aver scaricato il file in allegato all'esercizio ed averlo estratto sulla cartella condivisa di Kali, andiamo ad aprire Wireshark ed aprire il file estratto al suo interno:



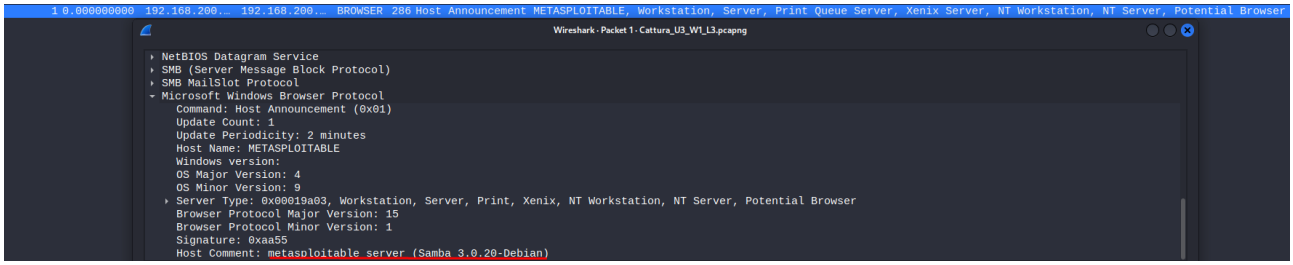


Quello che ci ritroveremo sarà la seguente scansione, nella quale possiamo capire che viene effettuato uno scan con il tool nmap usando lo switch -sT poiché notiamo che viene completato il Three-Way Handshake:



1	0.000000000	192.168.200.…	192.168.200.…	BROWSER	286 Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
2	23.764214995	192.168.200.…	192.168.200.…	TCP	74 53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.…	192.168.200.…	TCP	74 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.…	192.168.200.…	TCP	74 80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.…	192.168.200.…	TCP	60 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.…	192.168.200.…	TCP	66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.…	192.168.200.…	TCP	66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PcsCompu_fd:…	PcsCompu_39:…	ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:…	PcsCompu_fd:…	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:…	PcsCompu_fd:…	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:…	PcsCompu_39:…	ARP	60 192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143445	192.168.200.…	192.168.200.…	TCP	74 41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.…	192.168.200.…	TCP	74 56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.…	192.168.200.…	TCP	74 33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366305	192.168.200.…	192.168.200.…	TCP	74 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.…	192.168.200.…	TCP	74 52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.…	192.168.200.…	TCP	74 46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.…	192.168.200.…	TCP	74 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685505	192.168.200.…	192.168.200.…	TCP	74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.…	192.168.200.…	TCP	74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.…	192.168.200.…	TCP	60 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.…	192.168.200.…	TCP	60 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.…	192.168.200.…	TCP	60 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.…	192.168.200.…	TCP	66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.…	192.168.200.…	TCP	66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.…	192.168.200.…	TCP	60 993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.…	192.168.200.…	TCP	74 21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.…	192.168.200.…	TCP	66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337890	192.168.200.…	192.168.200.…	TCP	74 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.…	192.168.200.…	TCP	74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.…	192.168.200.…	TCP	74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775589806	192.168.200.…	192.168.200.…	TCP	60 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Possiamo notare che se viene effettuato un doppio clic sulla prima riga, scorrendo tutto in basso, possiamo notare che server è, come di seguito:



Detto ciò, ipotizzando fosse una scansione nmap -sT, cosa possiamo fare per evitare ciò? Un consiglio, che sarebbe quello più immediato, sarebbe di dover attivare un Firewall in modo tale che da una possibile scansione non si può capire se la porta sia aperta o meno dato che risulterà filtered. Altro consiglio è quello di bloccare il traffico di dati verso quel determinato indirizzo IP, 192.168.200.100, che abbiamo trovato tramite Wireshark.