S9L5

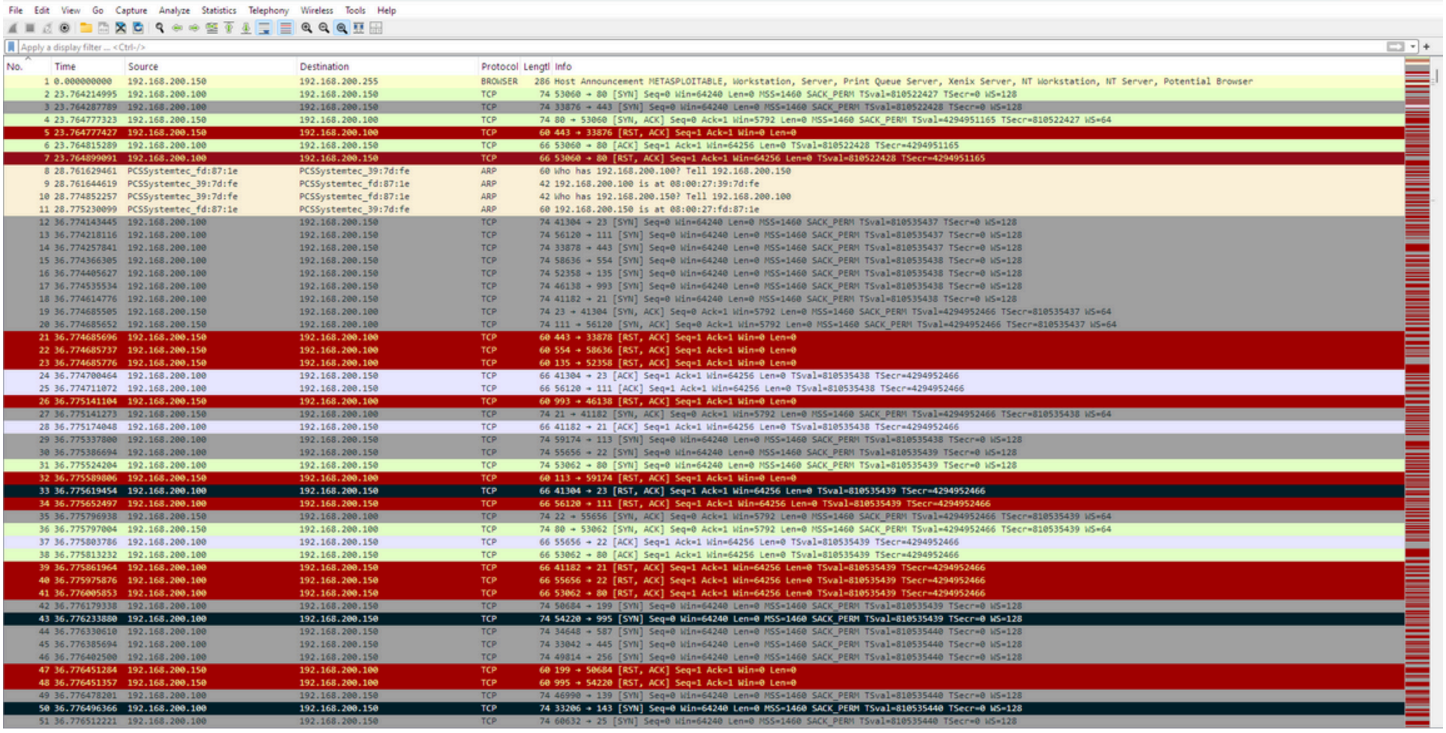
Conti Mirco

Data: 29/11/24

INFORMAZIONI PRINCIPALI

Traccia: Esercizio Threat Intelligence & IOC Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto. Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti: ● Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso ● In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati ● Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro

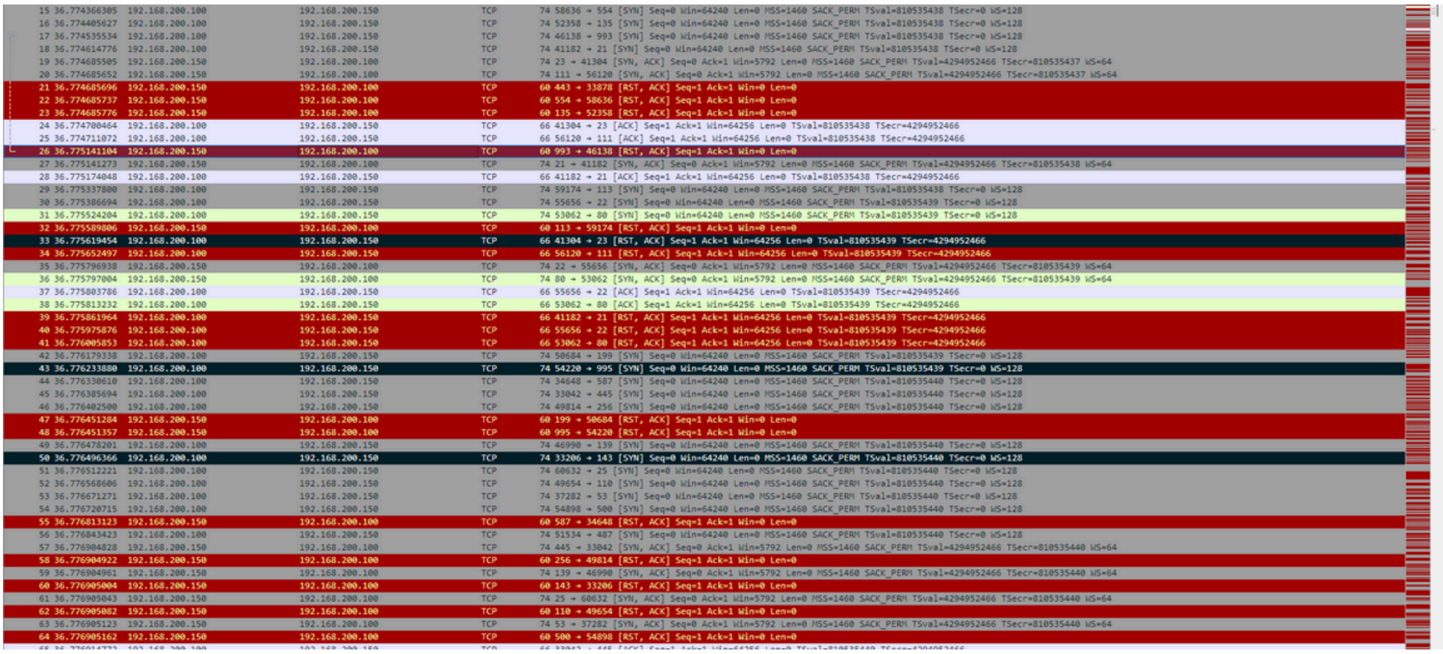
INIZIO ESERCIZIO



No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	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	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:fe	PCSSystemtec_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:1e	PCSSystemtec_39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685505	192.168.200.150	192.168.200.100	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	192.168.200.150	192.168.200.100	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	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	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	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	36.776402500	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128

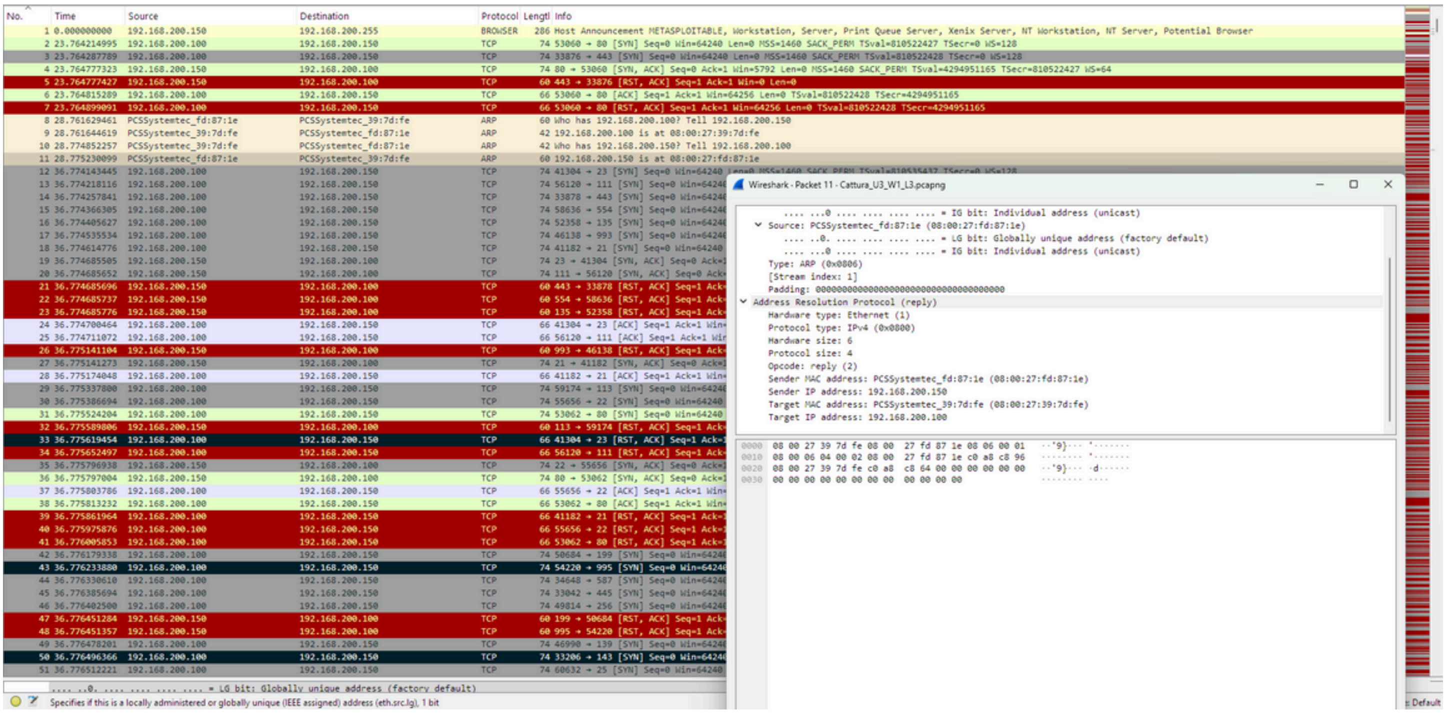
Dall'analisi svolta, un utente interno (192.168.200.100) Nella nostra stessa rete e stesi nomi delle macchine (hostnames). Ha eseguito una scansione delle porte sulla macchina con IP 192.168.200.150 utilizzando uno strumento come nmap. Questo comportamento è tipico di un'attività di ricognizione volta a individuare porte aperte e servizi attivi sul server, ma non risulta essere un attacco diretto come un DoS o DDoS.

I pacchetti catturati mostrano il classico schema del three-way handshake del protocollo TCP, con sequenze di pacchetti SYN, SYN-ACK e ACK, seguiti da risposte RST che chiudono le connessioni. Questo dimostra che non siamo di fronte a un attacco SYN Flood, poiché le connessioni non rimangono "half-open" (aperte a metà) e si chiudono regolarmente. Inoltre, la scansione non mostra cicli infiniti di connessioni aperte e chiuse, escludendo anche un TCP Flood, che si manifesterebbe con un flusso continuo di connessioni ripetute verso una o più porte, Inoltre non ci sono pacchetti UDP o ICMP evidenti, quindi non si tratta di un UDP Flood o ICMP Flood.



```
15 36.774366305 192.168.200.100   192.168.200.150   TCP   74 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16 36.774405627 192.168.200.100   192.168.200.150   TCP   74 52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17 36.774535534 192.168.200.100   192.168.200.150   TCP   74 46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18 36.774614776 192.168.200.100   192.168.200.150   TCP   74 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19 36.774685505 192.168.200.150   192.168.200.100   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 192.168.200.150   192.168.200.100   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 192.168.200.150   192.168.200.100   TCP   60 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 36.774685737 192.168.200.150   192.168.200.100   TCP   60 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 36.774685776 192.168.200.150   192.168.200.100   TCP   60 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 36.774700464 192.168.200.100   192.168.200.150   TCP   66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25 36.774711072 192.168.200.100   192.168.200.150   TCP   66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26 36.775141104 192.168.200.150   192.168.200.100   TCP   60 993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27 36.775141273 192.168.200.150   192.168.200.100   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 192.168.200.100   192.168.200.150   TCP   66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29 36.775337800 192.168.200.100   192.168.200.150   TCP   74 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30 36.775386694 192.168.200.100   192.168.200.150   TCP   74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31 36.775524204 192.168.200.100   192.168.200.150   TCP   74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32 36.775589806 192.168.200.150   192.168.200.100   TCP   60 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33 36.775619454 192.168.200.100   192.168.200.150   TCP   66 41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34 36.775652497 192.168.200.100   192.168.200.150   TCP   66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35 36.775796938 192.168.200.150   192.168.200.100   TCP   74 22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36 36.775797004 192.168.200.150   192.168.200.100   TCP   74 80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37 36.775803786 192.168.200.100   192.168.200.150   TCP   66 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38 36.775813232 192.168.200.100   192.168.200.150   TCP   66 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39 36.775861964 192.168.200.100   192.168.200.150   TCP   66 41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40 36.775975876 192.168.200.100   192.168.200.150   TCP   66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41 36.776005853 192.168.200.100   192.168.200.150   TCP   66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42 36.776179338 192.168.200.100   192.168.200.150   TCP   74 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43 36.776233880 192.168.200.100   192.168.200.150   TCP   74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44 36.776330610 192.168.200.100   192.168.200.150   TCP   74 34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45 36.776385694 192.168.200.100   192.168.200.150   TCP   74 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46 36.776402500 192.168.200.100   192.168.200.150   TCP   74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47 36.776451284 192.168.200.150   192.168.200.100   TCP   60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48 36.776451357 192.168.200.150   192.168.200.100   TCP   60 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49 36.776478201 192.168.200.100   192.168.200.150   TCP   74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50 36.776496366 192.168.200.100   192.168.200.150   TCP   74 33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51 36.776512221 192.168.200.100   192.168.200.150   TCP   74 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52 36.776568606 192.168.200.100   192.168.200.150   TCP   74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
53 36.776671271 192.168.200.100   192.168.200.150   TCP   74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
54 36.776720715 192.168.200.100   192.168.200.150   TCP   74 54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
55 36.776813123 192.168.200.150   192.168.200.100   TCP   60 587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56 36.776843423 192.168.200.100   192.168.200.150   TCP   74 51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
57 36.776904828 192.168.200.150   192.168.200.100   TCP   74 445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
58 36.776904922 192.168.200.150   192.168.200.100   TCP   60 256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59 36.776904961 192.168.200.150   192.168.200.100   TCP   74 139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
60 36.776905004 192.168.200.150   192.168.200.100   TCP   60 143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61 36.776905043 192.168.200.150   192.168.200.100   TCP   74 25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
62 36.776905082 192.168.200.150   192.168.200.100   TCP   60 110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63 36.776905123 192.168.200.150   192.168.200.100   TCP   74 53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
64 36.776905162 192.168.200.150   192.168.200.100   TCP   60 500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65 36.776914773 192.168.200.100   192.168.200.150   TCP   66 33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
```

Nei pacchetti non è presente nessuna richiesta HTTP, come GET o POST, quindi è chiaro che l’attività non è stata effettuata tramite un browser. È Confermata che la scansione è stata avviata con un comando nmap, nmap -sT -Pn -p 80,443, per sondare le porte 80 e 443. Il traffico ARP presente indica che la macchina attaccante ha effettuato una risoluzione automatica degli indirizzi MAC, comportamento standard durante una scansione di rete. E poco dopo nmap -sT -Pn -p 0,1023 per uno scan esclusivo su queste porte (note). Deve essere per forza -sT perchè altrimenti non completerebbe la "handshake". -Pn perchè tratta tutte le connessioni come attive e non ci sono pacchetti icmp. Nmap invia pacchetti ICMP (ping), TCP SYN o ARP per determinare se un host è attivo prima di iniziare una scansione delle porte (hence why it can't be without -Pn)



```
No.  Time          Source                Destination           Protocol Lengtl Info
 1 0.000000000   192.168.200.150       192.168.200.255       BROWSER  286 Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
 2 23.764214995  192.168.200.100       192.168.200.150       TCP       74 53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
 3 23.764287789  192.168.200.100       192.168.200.150       TCP       74 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
 4 23.764777323  192.168.200.150       192.168.200.100       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  192.168.200.150       192.168.200.100       TCP       60 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 6 23.764815289  192.168.200.100       192.168.200.150       TCP       66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
 7 23.764899091  192.168.200.100       192.168.200.150       TCP       66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
 8 28.761629461  PCSSystemtec_fd:87:1e PCSSystemtec_39:7d:fe ARP       60 Who has 192.168.200.100? Tell 192.168.200.150
 9 28.761644619  PCSSystemtec_39:7d:fe PCSSystemtec_fd:87:1e ARP       42 192.168.200.100 is at 08:00:27:39:7d:fe
10 28.774852257  PCSSystemtec_39:7d:fe PCSSystemtec_fd:87:1e ARP       42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230099  PCSSystemtec_fd:87:1e PCSSystemtec_39:7d:fe ARP       60 192.168.200.150 is at 08:00:27:fd:87:1e
12 36.774143445  192.168.200.100       192.168.200.150       TCP       74 41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13 36.774218116  192.168.200.100       192.168.200.150       TCP       74 56120 → 111 [SYN] Seq=0 Win=6424
14 36.774257841  192.168.200.100       192.168.200.150       TCP       74 33878 → 443 [SYN] Seq=0 Win=6424
15 36.774366305  192.168.200.100       192.168.200.150       TCP       74 58636 → 554 [SYN] Seq=0 Win=6424
16 36.774405627  192.168.200.100       192.168.200.150       TCP       74 52358 → 135 [SYN] Seq=0 Win=6424
17 36.774535534  192.168.200.100       192.168.200.150       TCP       74 46138 → 993 [SYN] Seq=0 Win=6424
18 36.774614776  192.168.200.100       192.168.200.150       TCP       74 41182 → 21 [SYN] Seq=0 Win=64240
19 36.774685505  192.168.200.150       192.168.200.100       TCP       74 23 → 41304 [SYN, ACK] Seq=0 Ack=1
20 36.774685652  192.168.200.150       192.168.200.100       TCP       74 111 → 56120 [SYN, ACK] Seq=0 Ack
21 36.774685696  192.168.200.150       192.168.200.100       TCP       60 443 → 33878 [RST, ACK] Seq=1 Ack
22 36.774685737  192.168.200.150       192.168.200.100       TCP       60 554 → 58636 [RST, ACK] Seq=1 Ack
23 36.774685776  192.168.200.150       192.168.200.100       TCP       60 135 → 52358 [RST, ACK] Seq=1 Ack
24 36.774700464  192.168.200.100       192.168.200.150       TCP       66 41304 → 23 [ACK] Seq=1 Ack=1 Win
25 36.774711072  192.168.200.100       192.168.200.150       TCP       66 56120 → 111 [ACK] Seq=1 Ack=1 Wir
26 36.775141104  192.168.200.150       192.168.200.100       TCP       60 993 → 46138 [RST, ACK] Seq=1 Ack
27 36.775141273  192.168.200.150       192.168.200.100       TCP       74 21 → 41182 [SYN, ACK] Seq=0 Ack=1
28 36.775174048  192.168.200.100       192.168.200.150       TCP       66 41182 → 21 [ACK] Seq=1 Ack=1 Win
29 36.775337800  192.168.200.100       192.168.200.150       TCP       74 59174 → 113 [SYN] Seq=0 Win=6424
30 36.775386694  192.168.200.100       192.168.200.150       TCP       74 55656 → 22 [SYN] Seq=0 Win=64240
31 36.775524204  192.168.200.100       192.168.200.150       TCP       74 53062 → 80 [SYN] Seq=0 Win=64240
32 36.775589806  192.168.200.150       192.168.200.100       TCP       60 113 → 59174 [RST, ACK] Seq=1 Ack
33 36.775619454  192.168.200.100       192.168.200.150       TCP       66 41304 → 23 [RST, ACK] Seq=1 Ack=1
34 36.775652497  192.168.200.100       192.168.200.150       TCP       66 56120 → 111 [RST, ACK] Seq=1 Ack
35 36.775796938  192.168.200.150       192.168.200.100       TCP       74 22 → 55656 [SYN, ACK] Seq=0 Ack=1
36 36.775797004  192.168.200.150       192.168.200.100       TCP       74 80 → 53062 [SYN, ACK] Seq=0 Ack=1
37 36.775803786  192.168.200.100       192.168.200.150       TCP       66 55656 → 22 [ACK] Seq=1 Ack=1 Win
38 36.775813232  192.168.200.100       192.168.200.150       TCP       66 53062 → 80 [ACK] Seq=1 Ack=1 Win
39 36.775861964  192.168.200.100       192.168.200.150       TCP       66 41182 → 21 [RST, ACK] Seq=1 Ack=1
40 36.775975876  192.168.200.100       192.168.200.150       TCP       66 55656 → 22 [RST, ACK] Seq=1 Ack=1
41 36.776005853  192.168.200.100       192.168.200.150       TCP       66 53062 → 80 [RST, ACK] Seq=1 Ack=1
42 36.776179338  192.168.200.100       192.168.200.150       TCP       74 50684 → 199 [SYN] Seq=0 Win=6424
43 36.776233880  192.168.200.100       192.168.200.150       TCP       74 54220 → 995 [SYN] Seq=0 Win=6424
44 36.776330610  192.168.200.100       192.168.200.150       TCP       74 34648 → 587 [SYN] Seq=0 Win=6424
45 36.776385694  192.168.200.100       192.168.200.150       TCP       74 33042 → 445 [SYN] Seq=0 Win=6424
46 36.776402500  192.168.200.100       192.168.200.150       TCP       74 49814 → 256 [SYN] Seq=0 Win=6424
47 36.776451284  192.168.200.150       192.168.200.100       TCP       60 199 → 50684 [RST, ACK] Seq=1 Ack
48 36.776451357  192.168.200.150       192.168.200.100       TCP       60 995 → 54220 [RST, ACK] Seq=1 Ack
49 36.776478201  192.168.200.100       192.168.200.150       TCP       74 46990 → 139 [SYN] Seq=0 Win=6424
50 36.776496366  192.168.200.100       192.168.200.150       TCP       74 33206 → 143 [SYN] Seq=0 Win=6424
51 36.776512221  192.168.200.100       192.168.200.150       TCP       74 60632 → 25 [SYN] Seq=0 Win=64240
```

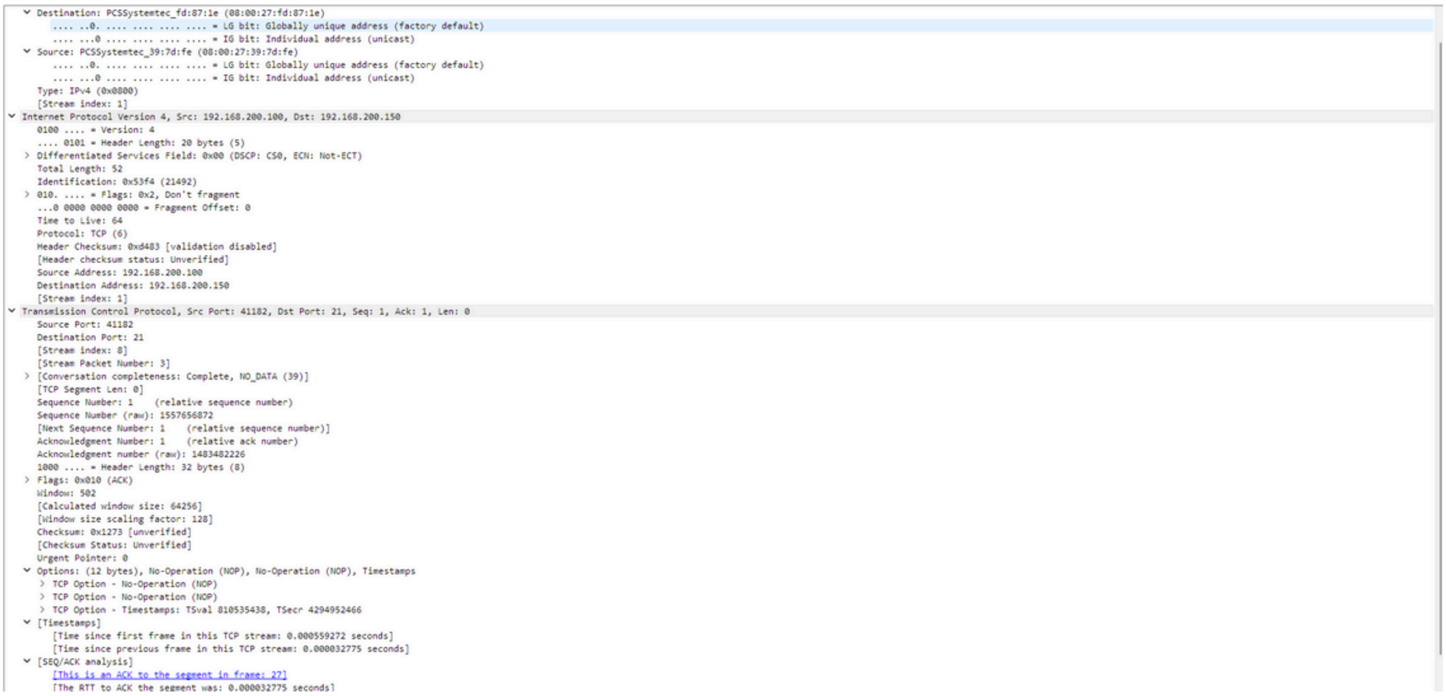
```
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
```

Specifies if this is a locally administered or globally unique (IEEE assigned) address (eth.src.lg), 1 bit

Wireshark · Packet 11 · Cattura_U3_W1_L3.pcapng

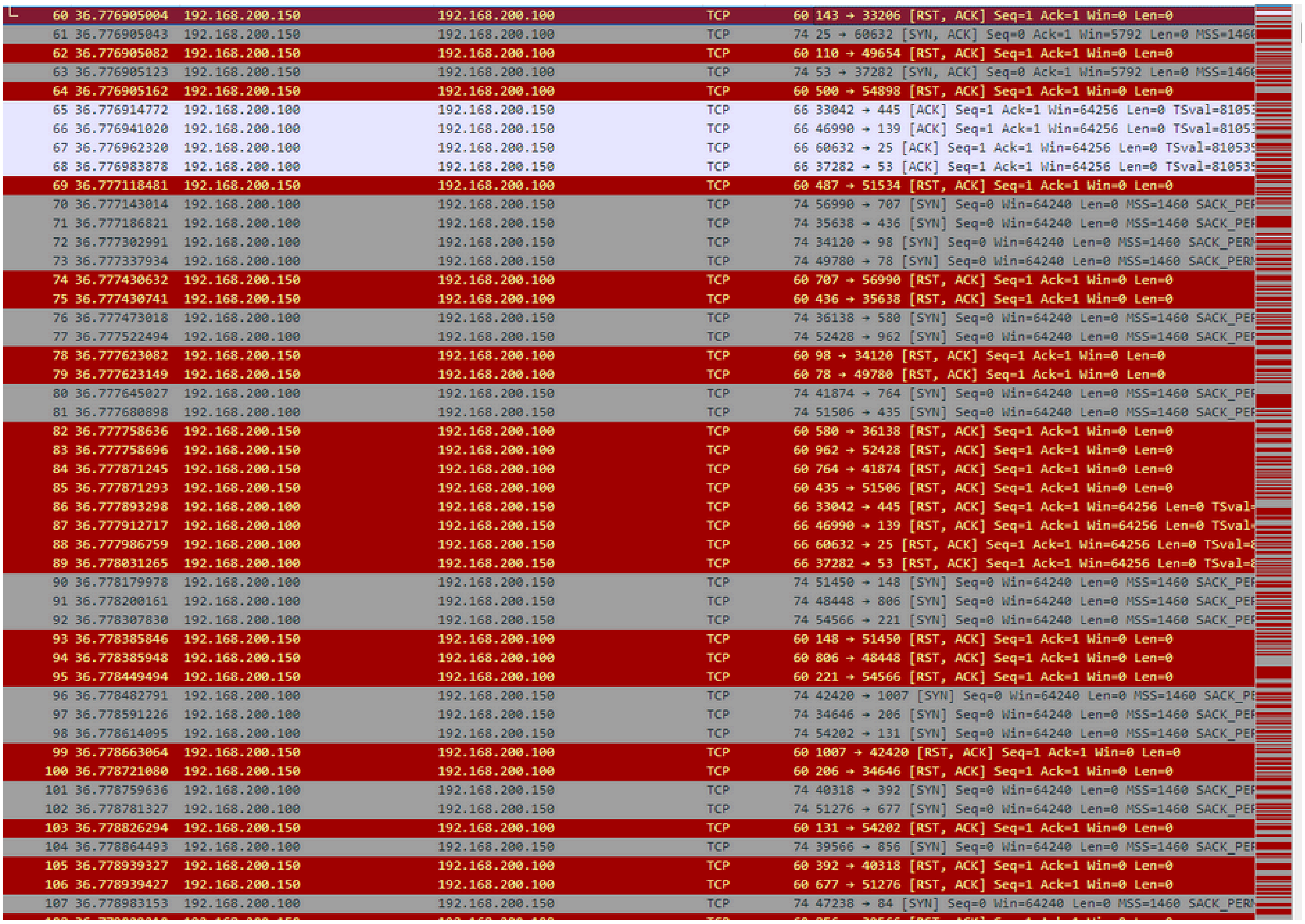
```
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  [Stream index: 1]
  Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e)
  Sender IP address: 192.168.200.150
  Target MAC address: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe)
  Target IP address: 192.168.200.100
```

```
0000  08 00 27 39 7d fe 08 00  27 fd 87 1e 08 06 00 01   ··'9}···  '·······
0010  08 00 06 04 00 02 08 00  27 fd 87 1e c0 a8 c8 96   ········  '·······
0020  08 00 27 39 7d fe c0 a8  c8 64 00 00 00 00 00 00   ··'9}···  ·d······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········  ····
```



```
  ˅ Destination: PCSSystemtec_fd:87:1e (08:00:27:fd:87:1e)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ˅ Source: PCSSystemtec_39:7d:fe (08:00:27:39:7d:fe)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
˅ Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x53f4 (21492)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xd483 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.200.100
    Destination Address: 192.168.200.150
    [Stream index: 1]
˅ Transmission Control Protocol, Src Port: 41182, Dst Port: 21, Seq: 1, Ack: 1, Len: 0
    Source Port: 41182
    Destination Port: 21
    [Stream index: 8]
    [Stream Packet Number: 3]
  > [Conversation completeness: Complete, NO_DATA (39)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1557656872
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1483482226
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0x1273 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ˅ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
      > TCP Option - No-Operation (NOP)
      > TCP Option - No-Operation (NOP)
      > TCP Option - Timestamps: TSval 810535438, TSecr 4294952466
  ˅ [Timestamps]
        [Time since first frame in this TCP stream: 0.000559272 seconds]
        [Time since previous frame in this TCP stream: 0.000032775 seconds]
  ˅ [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 27]
        [The RTT to ACK the segment was: 0.000032775 seconds]
```

Il traffico catturato evidenzia una velocità elevata delle connessioni, suggerendo l'uso di una scansione in modalità T4 (alta velocità. a me risulta identico uno scan con nmap -T4 Ma non siamo nel pc dell'attacante). Questo comportamento è tipico di nmap, che cerca di bilanciare velocità ed evasione dai sistemi di difesa. Inoltre, l'assenza di richieste (Get) per ottenere informazioni sui protocolli (come accadrebbe con il comando -sV) conferma che si tratta di una semplice scansione delle porte note (0-1023) senza ulteriori dettagli sui servizi



```
 60 36.776905004  192.168.200.150   192.168.200.100   TCP   60 143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 61 36.776905043  192.168.200.150   192.168.200.100   TCP   74 25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=146
 62 36.776905082  192.168.200.150   192.168.200.100   TCP   60 110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 63 36.776905123  192.168.200.150   192.168.200.100   TCP   74 53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=146
 64 36.776905162  192.168.200.150   192.168.200.100   TCP   60 500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 65 36.776914772  192.168.200.100   192.168.200.150   TCP   66 33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81053
 66 36.776941020  192.168.200.100   192.168.200.150   TCP   66 46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81053
 67 36.776962320  192.168.200.100   192.168.200.150   TCP   66 60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535
 68 36.776983878  192.168.200.100   192.168.200.150   TCP   66 37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535
 69 36.777118481  192.168.200.150   192.168.200.100   TCP   60 487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 70 36.777143014  192.168.200.100   192.168.200.150   TCP   74 56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 71 36.777186821  192.168.200.100   192.168.200.150   TCP   74 35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 72 36.777302991  192.168.200.100   192.168.200.150   TCP   74 34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
 73 36.777337934  192.168.200.100   192.168.200.150   TCP   74 49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
 74 36.777430632  192.168.200.150   192.168.200.100   TCP   60 707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 75 36.777430741  192.168.200.150   192.168.200.100   TCP   60 436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 76 36.777473018  192.168.200.100   192.168.200.150   TCP   74 36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 77 36.777522494  192.168.200.100   192.168.200.150   TCP   74 52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 78 36.777623082  192.168.200.150   192.168.200.100   TCP   60 98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 79 36.777623149  192.168.200.150   192.168.200.100   TCP   60 78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 80 36.777645027  192.168.200.100   192.168.200.150   TCP   74 41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 81 36.777680898  192.168.200.100   192.168.200.150   TCP   74 51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 82 36.777758636  192.168.200.150   192.168.200.100   TCP   60 580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 83 36.777758696  192.168.200.150   192.168.200.100   TCP   60 962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 84 36.777871245  192.168.200.150   192.168.200.100   TCP   60 764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 85 36.777871293  192.168.200.150   192.168.200.100   TCP   60 435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 86 36.777893298  192.168.200.100   192.168.200.150   TCP   66 33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=
 87 36.777912717  192.168.200.100   192.168.200.150   TCP   66 46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=
 88 36.777986759  192.168.200.100   192.168.200.150   TCP   66 60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8
 89 36.778031265  192.168.200.100   192.168.200.150   TCP   66 37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=8
 90 36.778179978  192.168.200.100   192.168.200.150   TCP   74 51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 91 36.778200161  192.168.200.100   192.168.200.150   TCP   74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 92 36.778307830  192.168.200.100   192.168.200.150   TCP   74 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 93 36.778385846  192.168.200.150   192.168.200.100   TCP   60 148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 94 36.778385948  192.168.200.150   192.168.200.100   TCP   60 806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 95 36.778449494  192.168.200.150   192.168.200.100   TCP   60 221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 96 36.778482791  192.168.200.100   192.168.200.150   TCP   74 42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
 97 36.778591226  192.168.200.100   192.168.200.150   TCP   74 34646 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 98 36.778614095  192.168.200.100   192.168.200.150   TCP   74 54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
 99 36.778663064  192.168.200.150   192.168.200.100   TCP   60 1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100 36.778721080  192.168.200.150   192.168.200.100   TCP   60 206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101 36.778759636  192.168.200.100   192.168.200.150   TCP   74 40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
102 36.778781327  192.168.200.100   192.168.200.150   TCP   74 51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
103 36.778826294  192.168.200.150   192.168.200.100   TCP   60 131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104 36.778864493  192.168.200.100   192.168.200.150   TCP   74 39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
105 36.778939327  192.168.200.150   192.168.200.100   TCP   60 392 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106 36.778939427  192.168.200.150   192.168.200.100   TCP   60 677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107 36.778983153  192.168.200.100   192.168.200.150   TCP   74 47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
```

Le risposte RST (reset) frequenti e ravvicinate sono messe in evidenza in rosso da Wireshark, segnalando potenzialmente un comportamento sospetto. Tuttavia, il fatto che le connessioni vengano chiuse in modo regolare e in successione veloce si capisce che non è un attacco "diretto" (specifico ad una porta, altrimenti vedrei sempre tentativi sulla stessa).

Come rimedio, è consigliabile bloccare il traffico verso le porte che non sono strettamente necessarie per il funzionamento del server e applicare filtri firewall per limitare l'accesso alle sole macchine autorizzate. È inoltre utile configurare un sistema di monitoraggio che rilevi tentativi di scansione o attività anomale, oltre a implementare meccanismi di rate-limiting per prevenire eventuali abusi. Infine, è sempre buona pratica monitorare e pulire periodicamente la cache ARP per evitare problemi legati alle informazioni residue lasciate da scansioni simili.

Inoltre Se abbiamo preso i MAC "Address" di ogni pc aziendale, sappiamo a chi appartiene e possiamo andare direttamente da lui e capire se è stato infettato (o e lui) ed isolarlo* (Prevention, sapremo già se l'attacante sta usando un computer aziendale e anche di chi è) altrimenti possiamo anche staccare il wi-fi (per comprendere se l'attacco è sulla rete fissa aziendale o dall'esterno tramite rete wireless aziendale, ovviamente in congruenza con il Business Continuity.) Quando possibile.

CONCLUSIONE

Il traffico analizzato non evidenzia un attacco DoS o DDoS, Mitm(arp poisoning), Backdoor(Reverse tcp o altre minaccie). Possiamo appurare che l'attacante ha effettuato uno scan da un computer sulla nostra rete locale con un tool come nmap o l'equivalente di questo comando <nmap -sT -Pn -p 0,1023> facendo uno scan sulle porte note in modo veloce. è un'attività di ricognizione tramite scansione delle porte note e sebbene non rappresenti una minaccia diretta, questo tipo di comportamento deve essere monitorato e bloccato per prevenire escalation o attacchi futuri.

Recap

Scan di nmap con:

-sT 100% perchè negli altri modi tipo sS non completerebbe l'handshake

(-sT syn,syn/ack,ack-rst/ack o syn) Completa (-sS syn,syn/ack-rst/ack non completando l'handshake "half open")

-sV non è possibile perchè non sono presenti richieste di GET per le versioni dei protocolli (Non potrà sfruttare vulnerabilità dovute a versioni non aggiornate, che comunque non dovrebbe accadere in primis e bisogna sempre tenere tutto aggiornato)

-Pn 100% perchè non ci sono richieste icmp per verificare l'host se è attivo <host discovery> (icmp echo request also known as "Ping")

e -p 0,1023 100% (più specifico) perchè l'attacante fa uno scan solamente delle porte note mirato.

--top-ports 1023 o anche -p- non possono essere: --top-ports 1023 scansionerebbe le 1023 porte più comuni in base al database interno di Nmap (nmap-services), che ordina le porte in base alla loro frequenza di utilizzo. Questo potrebbe includere porte sparse su tutto il range (0-65535), non limitandosi solo alle prime 1023.

-p- non avrebbe riguardo, farebbe una ricerca completa (0-65535)