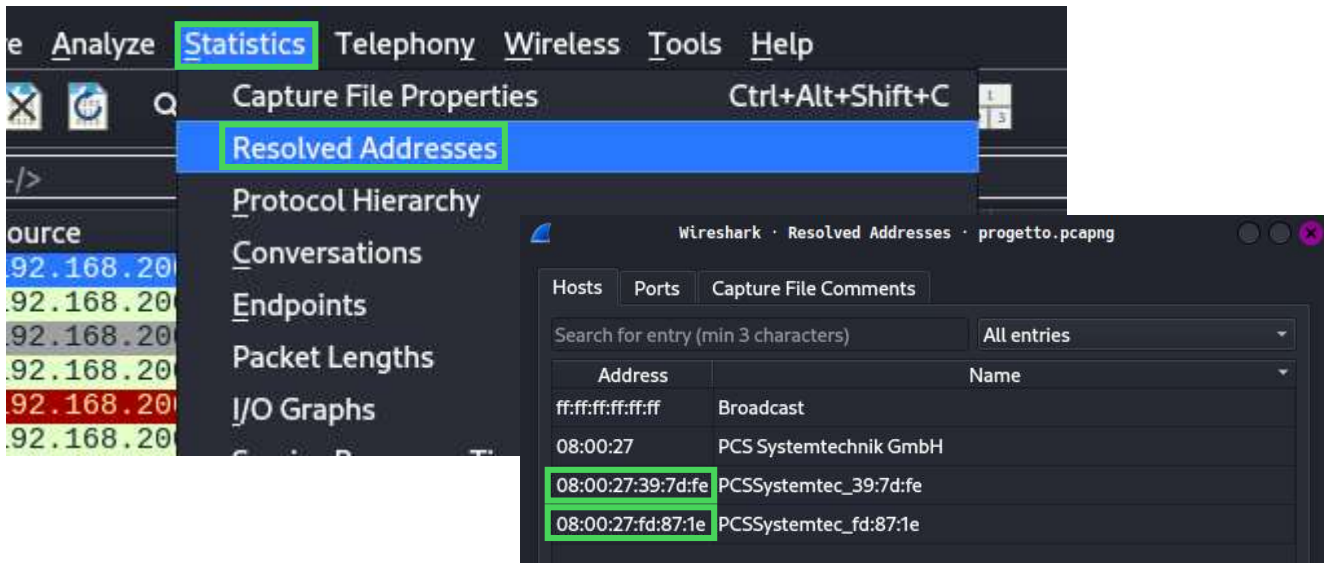


Come primo passo, sono andato a visualizzare gli indirizzi IP coinvolti in questo scambio di pacchetti andando su “Statistics” e “Resolved Addresses” possiamo visualizzare una schermata che indica i mac address risolti:



E quindi, per visualizzare gli indirizzi rispettivi ai MAC Address, vado ad inserire “arp” nei filtri e prendo in considerazione le risposte ARP per assegnare gli indirizzi IP alle macchine:

The image shows the Wireshark packet list with the filter 'arp' applied. The table below represents the data shown in the packet list:

No.	Time	Source	Destination	Protocol	Length	Info
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

192.168.200.100 con mac 08:00:27:39:7d:fe

192.168.200.150 con mac 08:00:27:fd:87:1e

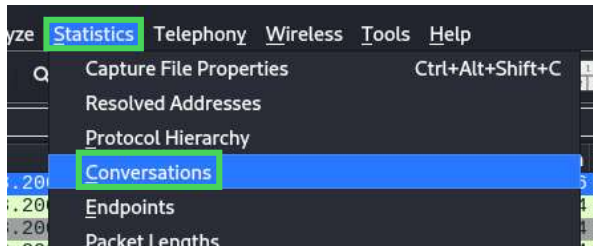
Sono poi andato a visualizzare tutti i protocolli utilizzati sempre nella scheda “Statistics” e “Protocol Hierarchy”:

The image shows the Wireshark interface. The 'Statistics' menu is open, highlighting 'Protocol Hierarchy'. The 'Protocol Hierarchy' window is also open, showing a tree view of the protocols used in the capture. The table below represents the data shown in the 'Protocol Hierarchy' window:

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU/s
Frame	100.0	2083	100.0	139872	30 k	0	0	0	2083
Ethernet	100.0	2083	25.2	35276	7,652	0	0	0	2083
Internet Protocol Version 4	99.8	2079	29.7	41580	9,019	0	0	0	2079
User Datagram Protocol	0.0	1	0.0	8	1	0	0	0	1
NetBIOS Datagram Service	0.0	1	0.1	82	17	0	0	0	1
SMB (Server Message Block Protocol)	0.0	1	0.1	162	35	0	0	0	1
SMB MailSlot Protocol	0.0	1	0.0	25	5	0	0	0	1
Microsoft Windows Browser Protocol	0.0	1	0.1	76	16	1	76	16	1
Transmission Control Protocol	99.8	2078	44.8	62652	13 k	2078	62652	13 k	2078
Address Resolution Protocol	0.2	4	0.1	112	24	4	112	24	4

Noto che il protocollo con maggior traffico è il TCP.

Deido quindi di visualizzare da chi sono stati mandati questi pacchetti andando nella scheda “Statistics” e “Conversation” per visualizzare i pacchetti inviati dalle rispettive macchine:



Andando a selezionare IPv4:

Ethernet · 2		IPv4 · 2		IPv6	TCP · 1026	UDP · 1							
Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	
192.168.200.100	192.168.200.150	2,078	139 kB	1	1,052	78 kB	1,026	62 kB	23.764215	13.1147	47 kbps	37 kbps	
192.168.200.150	192.168.200.255	1	286 bytes	0	1	286 bytes	0	0 bytes	0.000000	0.0000			

Noto che la maggior parte dei pacchetti sono stati inviati dalla macchina 192.168.200.100 alla macchina 192.168.200.150.

Essendo un comportamento molto sospetto, decido di visualizzare nel dettaglio i pacchetti inviati dall'indirizzo IP sospetto con il filtro:

ip.src == 192.168.200.100

No.	Time	Source	Destination	Protocol	Length	Info
1539	36.85884473	192.168.200.100	192.168.200.150	TCP	74	59131 → 718 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535513 TSecr=0 WS=128
1863	36.86895839	192.168.200.100	192.168.200.150	TCP	74	59144 → 85 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535532 TSecr=0 WS=128
29	36.77537889	192.168.200.100	192.168.200.150	TCP	74	59177 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
963	36.823908977	192.168.200.100	192.168.200.150	TCP	74	59239 → 941 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535487 TSecr=0 WS=128
285	36.798435780	192.168.200.100	192.168.200.150	TCP	74	59255 → 160 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535454 TSecr=0 WS=128
954	36.823535894	192.168.200.100	192.168.200.150	TCP	74	59255 → 1023 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535487 TSecr=0 WS=128
571	36.804821918	192.168.200.100	192.168.200.150	TCP	74	59311 → 195 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535468 TSecr=0 WS=128
380	36.798933139	192.168.200.100	192.168.200.150	TCP	74	59321 → 430 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535454 TSecr=0 WS=128
711	36.812043191	192.168.200.100	192.168.200.150	TCP	74	59332 → 297 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535475 TSecr=0 WS=128
1420	36.844913069	192.168.200.100	192.168.200.150	TCP	74	59332 → 281 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535508 TSecr=0 WS=128
1567	36.851786995	192.168.200.100	192.168.200.150	TCP	74	59355 → 810 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535515 TSecr=0 WS=128
187	36.782788538	192.168.200.100	192.168.200.150	TCP	74	59409 → 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
1460	36.847611651	192.168.200.100	192.168.200.150	TCP	74	59409 → 532 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535511 TSecr=0 WS=128
1343	36.841119251	192.168.200.100	192.168.200.150	TCP	74	59409 → 286 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535504 TSecr=0 WS=128
1850	36.868199128	192.168.200.100	192.168.200.150	TCP	74	59409 → 825 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535531 TSecr=0 WS=128
1634	36.854931917	192.168.200.100	192.168.200.150	TCP	74	59511 → 57 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535519 TSecr=0 WS=128
1214	36.835753319	192.168.200.100	192.168.200.150	TCP	74	59511 → 134 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535499 TSecr=0 WS=128
555	36.883927447	192.168.200.100	192.168.200.150	TCP	74	59589 → 491 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535467 TSecr=0 WS=128
974	36.824751334	192.168.200.100	192.168.200.150	TCP	74	59615 → 165 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535488 TSecr=0 WS=128
2841	36.870094687	192.168.200.100	192.168.200.150	TCP	74	59615 → 668 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535540 TSecr=0 WS=128
892	36.820496612	192.168.200.100	192.168.200.150	TCP	74	59666 → 778 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535484 TSecr=0 WS=128
2844	36.877634466	192.168.200.100	192.168.200.150	TCP	74	59666 → 452 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535540 TSecr=0 WS=128
744	36.812311487	192.168.200.100	192.168.200.150	TCP	74	59711 → 953 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535476 TSecr=0 WS=128
1892	36.874425417	192.168.200.100	192.168.200.150	TCP	74	59711 → 343 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535538 TSecr=0 WS=128
217	36.786292426	192.168.200.100	192.168.200.150	TCP	74	59733 → 129 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535450 TSecr=0 WS=128
615	36.866976283	192.168.200.100	192.168.200.150	TCP	74	59733 → 417 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535470 TSecr=0 WS=128

Notando che sono tutti pacchetti tcp con flag SYN verso la stessa macchina ma su molte porte diverse. Controllo anche i pacchetti provenienti dalla macchina presumibilmente target con lo stesso comando precedente ma cambiando l'indirizzo IP:

No.	Time	Source	Destination	Protocol	Length	Info
230	36.787864391	192.168.200.150	192.168.200.100	TCP	6	245 → 31739 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
242	36.788094799	192.168.200.150	192.168.200.100	TCP	6	234 → 39932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
250	36.788443559	192.168.200.150	192.168.200.100	TCP	6	789 → 59046 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
251	36.788443656	192.168.200.150	192.168.200.100	TCP	6	271 → 44414 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
252	36.788443666	192.168.200.150	192.168.200.100	TCP	6	476 → 50612 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
253	36.788443736	192.168.200.150	192.168.200.100	TCP	6	188 → 36266 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
254	36.788443776	192.168.200.150	192.168.200.100	TCP	6	855 → 51844 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
255	36.788443816	192.168.200.150	192.168.200.100	TCP	6	232 → 45726 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
256	36.788443867	192.168.200.150	192.168.200.100	TCP	6	894 → 27274 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
257	36.788443896	192.168.200.150	192.168.200.100	TCP	6	835 → 49488 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
258	36.788495654	192.168.200.150	192.168.200.100	TCP	6	682 → 41098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
259	36.788495663	192.168.200.150	192.168.200.100	TCP	6	291 → 44196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
265	36.788805799	192.168.200.150	192.168.200.100	TCP	6	956 → 48350 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
266	36.788805893	192.168.200.150	192.168.200.100	TCP	6	773 → 36542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
267	36.788805948	192.168.200.150	192.168.200.100	TCP	7	514 → 51390 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64
269	36.788953471	192.168.200.150	192.168.200.100	TCP	6	224 → 30765 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
271	36.789234182	192.168.200.150	192.168.200.100	TCP	6	183 → 48624 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
272	36.789378458	192.168.200.150	192.168.200.100	TCP	6	361 → 40182 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
276	36.790327864	192.168.200.150	192.168.200.100	TCP	6	617 → 46046 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
278	36.790152959	192.168.200.150	192.168.200.100	TCP	6	62 → 49069 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
279	36.790152966	192.168.200.150	192.168.200.100	TCP	6	8 → 4720 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
284	36.790407394	192.168.200.150	192.168.200.100	TCP	6	978 → 37566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
287	36.790531361	192.168.200.150	192.168.200.100	TCP	6	121 → 48384 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
288	36.790531425	192.168.200.150	192.168.200.100	TCP	6	186 → 49804 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
289	36.790531472	192.168.200.150	192.168.200.100	TCP	6	344 → 49848 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
292	36.790673451	192.168.200.150	192.168.200.100	TCP	6	168 → 59258 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

I pacchetti sono di tipo RST ovvero pacchetti “Reset” che una macchina invia quando la porta richiesta non accetta connessioni.

Sono presenti anche dei pacchetti SYN-ACK che confermano la connessione verso delle determinate porte.

Credo di poter confermare la teoria di una scansione nmap dato che anche in questo caso si tratta di una serie di pacchetti di risposta verso la stessa macchina ma provenienti da porte diverse.

Decido quindi di analizzare tutti i pacchetti con il flag SYN-ACK attivo dato che potrebbero essere state soggette a scansione e risultate aperte.

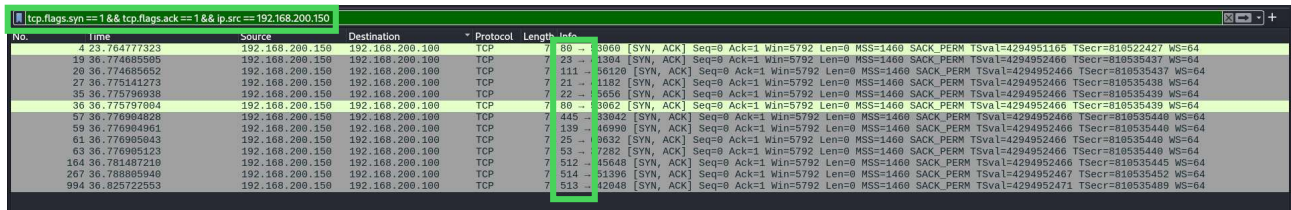
Per visualizzare solo i pacchetti di tipo SYN-ACK uso il filtro:

tcp.flags.syn == 1 && tcp.flags.ack == 1 && ip.src == 192.168.200.150

tcp.flags.syn==1 seleziona i pacchetti TCP con il flag SYN impostato ad 1

tcp.flags.ack==1 seleziona i pacchetti TCP con il flag ACK impostato ad 1

ip.src==192.168.200.150 Restringe la ricerca ai pacchetti provenienti dall'indirizzo ip specificato



No.	Time	Source	Destination	Protocol	Length	Info
4	23.764777323	192.168.200.150	192.168.200.100	TCP	78	→ 3960 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
19	36.774685595	192.168.200.150	192.168.200.100	TCP	78	→ 3960 [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	78	→ 3960 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
27	36.775141273	192.168.200.150	192.168.200.100	TCP	78	→ 3960 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
35	36.775796939	192.168.200.150	192.168.200.100	TCP	78	→ 3960 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
36	36.775797004	192.168.200.150	192.168.200.100	TCP	78	→ 3962 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
57	36.776984828	192.168.200.150	192.168.200.100	TCP	78	→ 445 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
59	36.776984961	192.168.200.150	192.168.200.100	TCP	78	→ 445 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
61	36.776985043	192.168.200.150	192.168.200.100	TCP	78	→ 445 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
63	36.776985123	192.168.200.150	192.168.200.100	TCP	78	→ 445 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
164	36.781487210	192.168.200.150	192.168.200.100	TCP	78	→ 4568 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64
267	36.788805940	192.168.200.150	192.168.200.100	TCP	78	→ 5136 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535452 WS=64
994	36.825722553	192.168.200.150	192.168.200.100	TCP	78	→ 5132 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64

Essendo di un numero ridotto, decido di analizzare il traffico di ogni singola porta usando il comando:

tcp.port==numeroDellaPorta

noto che tutte le porte hanno una serie di 4 pacchetti scambiati:



No.	Time	Source	Destination	Protocol	Length	Info
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41384 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
19	36.774685595	192.168.200.150	192.168.200.100	TCP	74	23 → 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
24	36.774708464	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
50	36.775919554	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

No.	Time	Source	Destination	Protocol	Length	Info
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
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
25	36.774711972	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
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

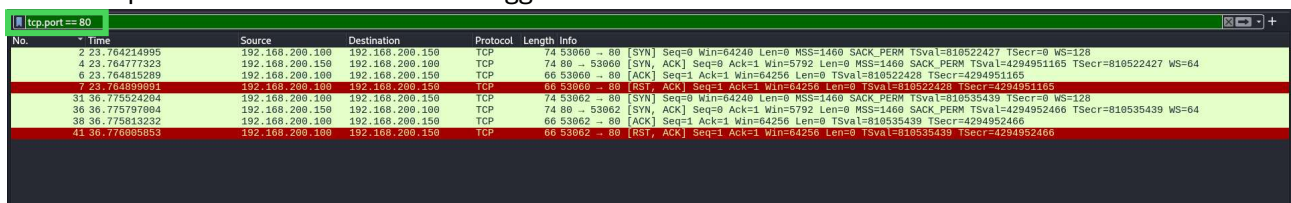
No.	Time	Source	Destination	Protocol	Length	Info
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174948	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
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

No.	Time	Source	Destination	Protocol	Length	Info
39	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
39	36.775386694	192.168.200.100	192.168.200.150	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775931766	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
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

No.	Time	Source	Destination	Protocol	Length	Info
57	36.776984828	192.168.200.150	192.168.200.100	TCP	74	445 → 33842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
45	36.776985094	192.168.200.100	192.168.200.150	TCP	74	33842 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
65	36.776984172	192.168.200.100	192.168.200.150	TCP	66	445 → 33842 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66	33842 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466

No.	Time	Source	Destination	Protocol	Length	Info
59	36.776984961	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
49	36.776478261	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
66	36.776984100	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
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=810535441 TSecr=4294952466

Tranne la porta 80 che ha un traffico maggiore:



No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53960 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53960 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53960 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764839091	192.168.200.100	192.168.200.150	TCP	66	53960 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
31	36.775524284	192.168.200.100	192.168.200.150	TCP	74	53962 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53962 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53962 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776985853	192.168.200.100	192.168.200.150	TCP	66	53962 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Analizzando il traffico, noto che viene effettuato per due volte il Three-Way Handshake il che mi fa sospettare che è stata eseguita prima una scansione nmap sulla macchina target e poi dopo che l'attaccante ha visto che la porta 80 risultava aperta, ha effettuato una seconda scansione per avere più dettagli sui servizi attualmente in esecuzione

Bouns

Azienda Mak produce dei macchinari e il cliente vuole mettere in sicurezza tutto l'ecosistema. Abbiamo da una parte l'azienda Mak, poi c'è il macchinario e dall'altra parte c'è il cliente che lo utilizza.

1. Il macchinario è bastato su Windows 10, ha porta di rete (usata solo per gli aggiornamenti e la diagnostica remota), porta USB (sono disabilitate le pendrive, ovviamente)
2. La diagnostica remota è fatta attraverso la VPN del cliente
3. Il macchinario è sostanzialmente bloccato. La partizione del sistema operativo non è scrivibile mentre c'è una seconda partizione per il software di gestione del macchinario.
4. Il software di gestione è realizzato con il linguaggio C99
5. Il macchinario è installato nelle varie aziende clienti

Analisi della situazione

1. Il fatto che la porta di rete (80) sia usata solo per gli aggiornamenti, non implica il fatto che sia chiusa. Se non adeguatamente protetta, potrebbe consentire intrusioni. La porta USB potrebbe essere soggetta da interazioni da parte di altri tipi di dispositivi come tastiere e driver HID (Human Interface Device).
2. La VPN seppur di norma considerata un canale "sicuro" perché cifrato, può diventare pericolosa se le credenziali di accesso alla VPN vengono rubate o indovinate da un attaccante dandogli un semplice modo di accesso alla rete da remoto.
3. Il blocco della partizione del sistema operativo riduce gli attacchi diretti contro Windows 10 ma per avere una buona sicurezza bisognerebbe aggiornare il sistema operativo frequentemente ed essendo bloccata la scrittura, questo non può accadere.
Se la partizione Windows non dovesse essere protetta adeguatamente, la partizione del software di gestione potrebbe subire attacchi di iniezione di codice malevolo nel software sfruttando eventuali vulnerabilità.
4. Il linguaggio di gestione C99 è soggetto ad alcune vulnerabilità come la possibilità di iniettare codice PHP malevolo per poter aprire una C99 Shell (<https://www.exploit-db.com/ghdb/420>)
5. Il macchinario è installato in diverse sedi di diversi clienti, ciascuna con la propria infrastruttura e livelli di sicurezza differenti. Se uno di essi fosse più esposto o meno protetto, potrebbe diventare un punto di ingresso per gli attacchi verso Mak o verso altre istanze del macchinario

Le vulnerabilità riscontrate si basano su diversi punti di vista:

Rete: mancato isolamento del macchinario con porte aperte

VPN: mancato controllo di sicurezza nelle credenziali di accesso

USB: potenziale bypass di sicurezza se la porta non è fisicamente bloccata

Sistema Windows: richiede piano di patch e aggiornamenti di sicurezza

C99: vulnerabilità nel codice

Installazioni multiple: possibili configurazioni non sicure

Soluzioni di sicurezza

Per rendere più sicura l'azienda, inizierei col proporre di mettere il macchinario in una VLAN con regole di firewall che limitano le connessioni solo a specifici indirizzi strettamente necessari.

Proporrei anche di acquistare una VPN con un forte sistema di crittografia, come ad esempio OpenVPN, implementare una MFA (Multi Factor Authentication) per accedere alla VPN per la diagnostica riducendo la probabilità che le credenziali rubate possano essere usate per accedere al macchinario.

(<https://www.linkedin.com/advice/0/how-can-you-secure-your-vpn-from-unauthorized-dbpbfb>)



Consiglierei anche di assicurarsi che Windows sia installato periodicamente e correttamente basandosi sulle patch di Microsoft.

Per quanto riguarda la porta USB, proporrei di aggiungere alla disabilitazione delle chiavette USB, una cover fisica prevista di lucchetti per evitarne l'utilizzo non autorizzato.

Per il linguaggio di gestione C99 proporrei di effettuare periodicamente delle analisi del codice, scansioni di vulnerabilità e test di penetrazione.

Infine, sarebbe il caso di stabilire una policy standard per l'implementazione del macchinario nelle aziende clienti della Mak.

Sistema di monitoraggio

Dato che Windows 10 è bloccato, l'unico modo per poter monitorare è agire esternamente dal sistema operativo implementando dei dispositivi hardware o, se i router dell'azienda è compatibile, una configurazione della rete per poter effettuare un mirroring del traffico della rete su una porta collegata ad un dispositivo di analisi (IDS o un pc con Wireshark in esecuzione).

Soluzione economica

Se la configurazione della rete non supportasse le **VLAN**, inserirei un piccolo switch economico da 50/80€ (<https://amzn.eu/d/7gL7Lyw>) così da poter configurare una VLAN dedicata per il macchinario. Per proteggere la porta **USB** si potrebbe acquistare un lucchetto per porte USB da 15/20€ (<https://amzn.eu/d/3AhMGjO>).

Per la **VPN**, il server di OpenVPN permette di integrare un secondo fattore di autenticazione tramite app OTP (Google Authenticator, Microsoft Authenticator). Il costo può essere nullo, se l'infrastruttura supporta questa funzionalità e se la VPN attuale non lo consente, almeno aumentare la complessità delle password e rinnovarle periodicamente.

Fare una revisione del codice manuale del software di gestione scritto in **C99**.

Eseguire backup offline periodici della partizione scrivibile e del software di gestione su un disco esterno (<https://amzn.eu/d/gzq6aeM> 80€) o NAS di base (<https://amzn.eu/d/0Yg2UWR> 150€) così, in caso di corruzione del codice (causa crash o errori umani) è possibile recuperare il codice.

E infine consiglierei di preparare brevi guide o sessioni da 1 o 2 ore sul tema della cybersecurity di base, phishing, uso corretto delle password e gestione degli account su materiale facilmente reperibile gratuitamente sul web.

Spesa totale: ~198€

Soluzione costosa

Implementerei un firewall che integra funzionalità di firewall, VPN, prevenzione delle intrusioni (IPS), controllo delle applicazioni e filtraggio web includendo nel prezzo il monitoraggio della rete.

(<https://www.aedgaming.com/it/firewall/fortigate-60f-hardware-plus-1-year-forticare-premi-p424456?src=trovaprezzi> 800€+1 anno di licenza gratuita)
(<https://a.co/d/3uNR8ac> licenza ~273\$/anno)

Implementerei dei software per l'analisi statica e periodica del codice come SonarQube
(<https://www.sonarsource.com/plans-and-pricing/> 384€/anno)

Server più capiente per poter immagazzinare altro dati oltre al backup del codice. Con almeno 4 hard disk da 2 TB con la possibilità di aggiungerne altri in futuro (<https://amzn.eu/d/0pM5TOI> 65€ l'uno)
(https://www.gigatrade.it/product_default.asp?idProdotto=31405 1.043€)

Spesa totale: ~2490€ (senza licenza del firewall annuale dopo primo anno gratuito)