Analisi di Rete

Sommario

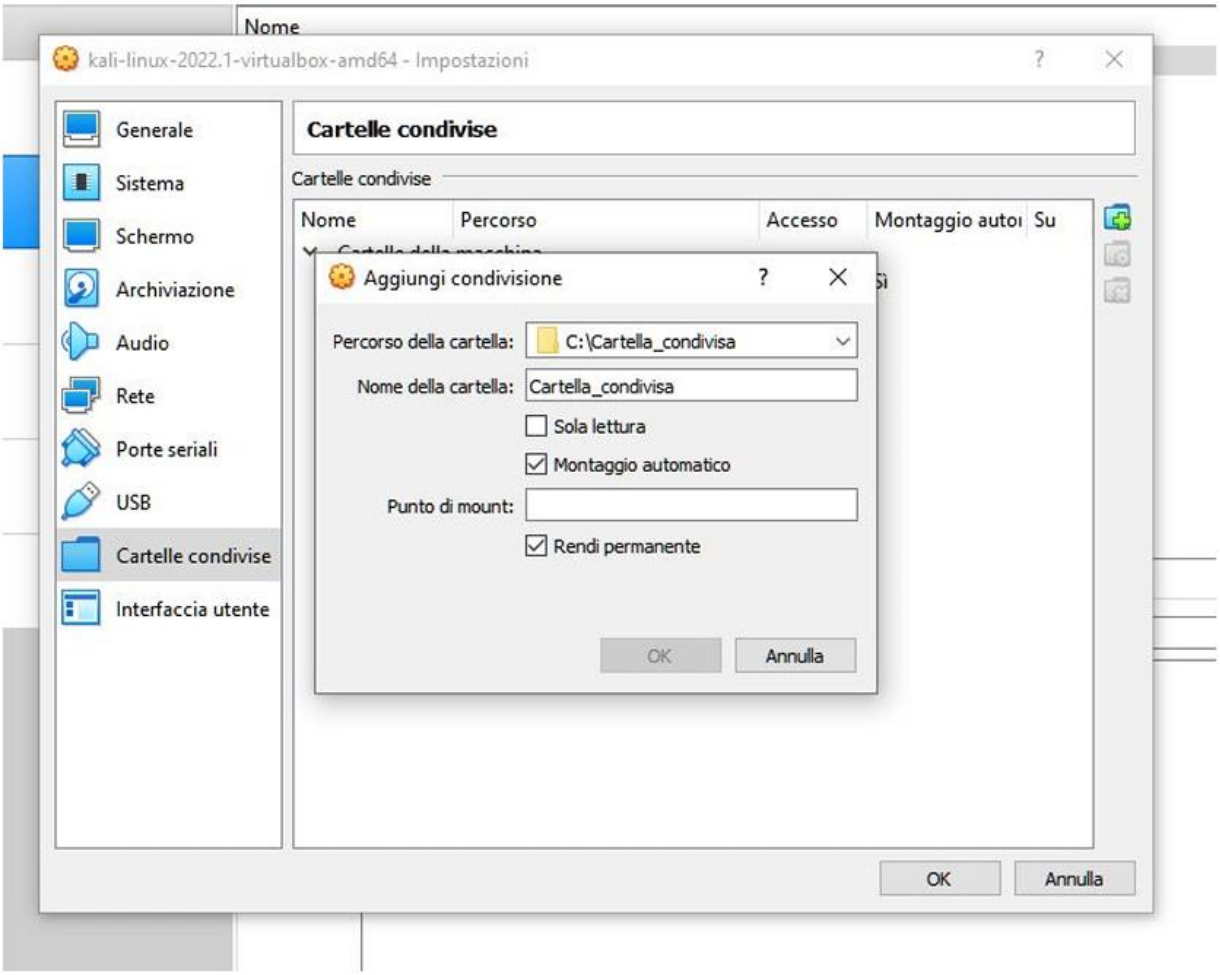
Traccia esercizio principale

Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.
Trovate in allegato una cattura di rete effettuata con Wireshark.
Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

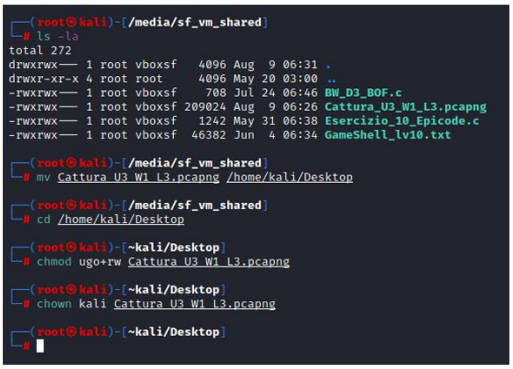
- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

Cattura_U3_W1_L3.pcapng

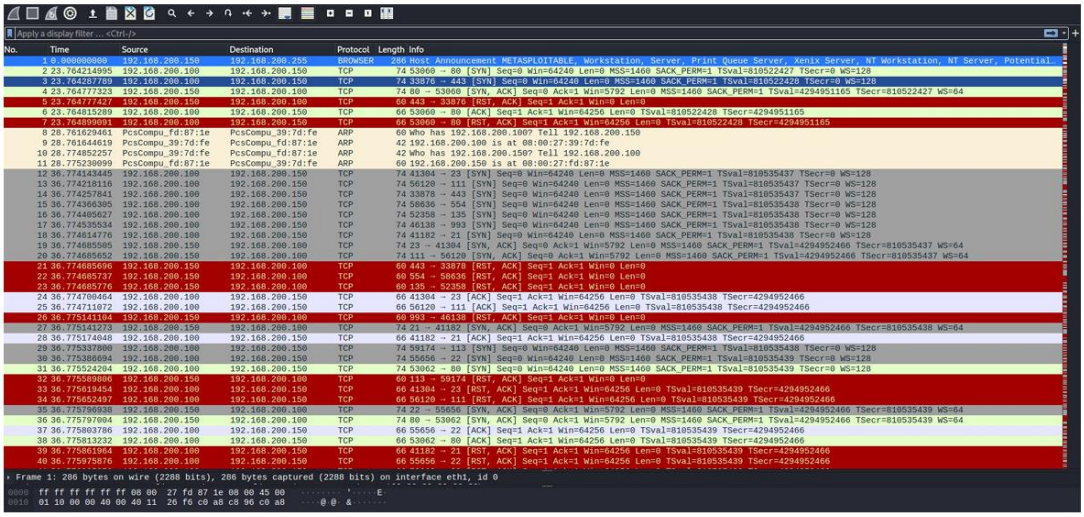
Per analizzare la cattura, spostate il file sulla vostra Kali Linux, e fate doppio-click, vi aprirà la cattura direttamente con Wireshark, dopo aver configurato i permessi per l'utente Kali.
Potete spostare il file sulla vostra Kali creando una cartella condivisa tra il vostro host e la Kali come la figura a destra.
Vi basterà creare la cartella sul vostro sistema operativo, e configurare la cartella sulla macchina virtuale, specificando il percorso della cartella sul vostro Host ed il nome della cartella.
Configurate la cartella con le opzioni in figura.

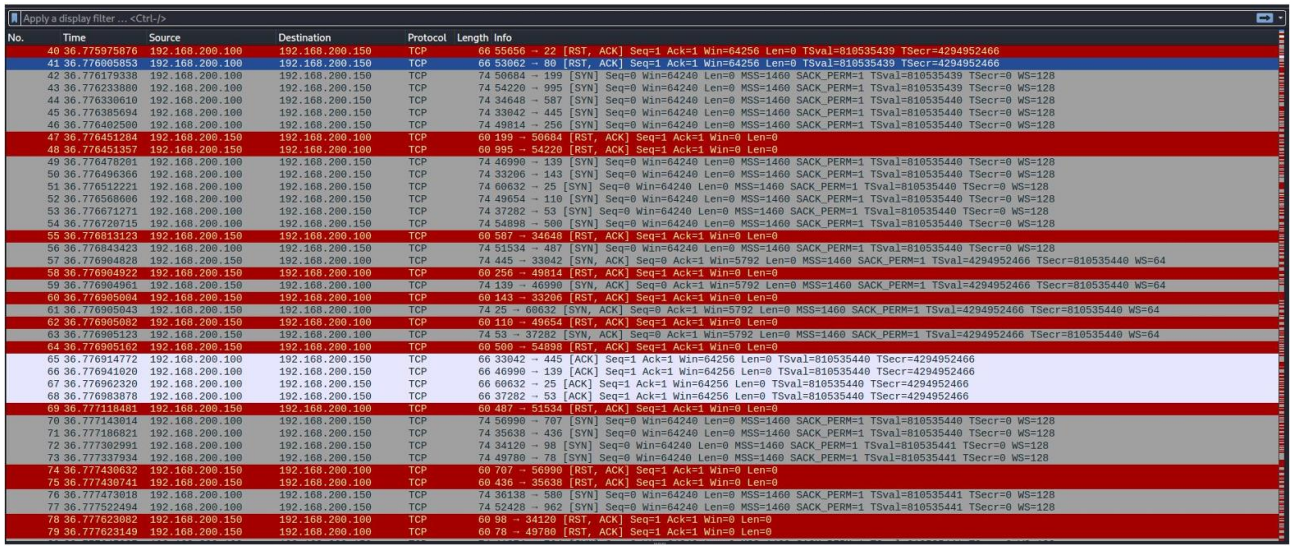


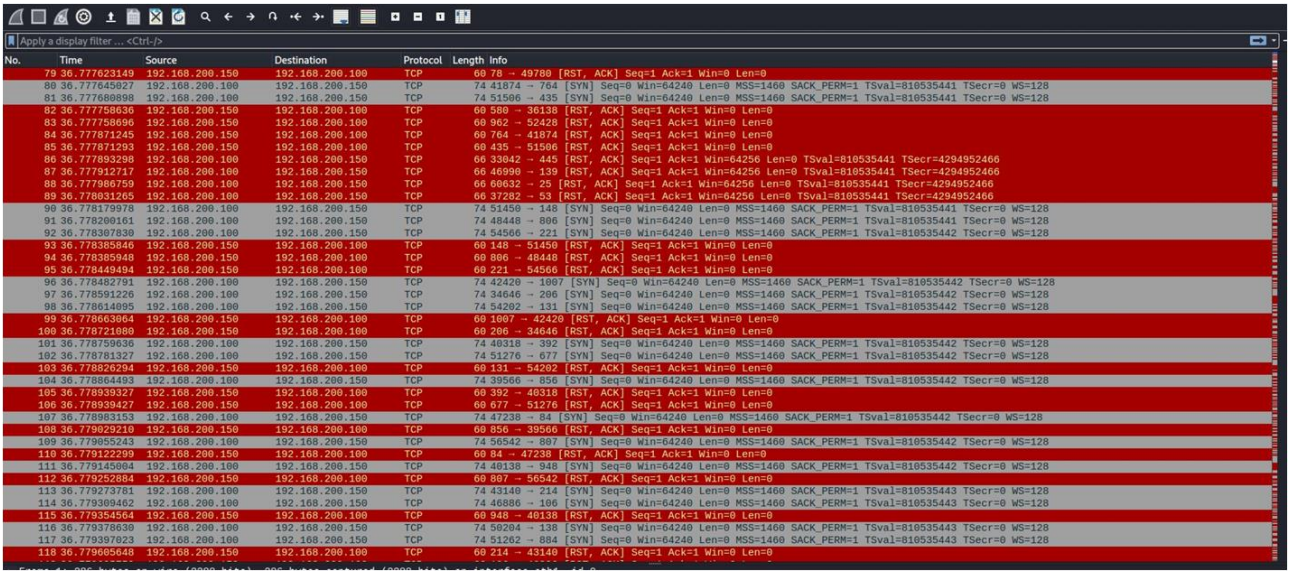
Da Kali potete accedere alla cartella (ed ai file in essa contenuti) navigando il file system alla directory /media come da figura seguente. Come vedete il nostro file è nella cartella condivisa. Da qui possiamo spostare il file sul desktop con il comando «mv» specificando il nome del file ed il path di destinazione, come visto nelle lezioni sul file system di Linux (il comando che abbiamo usato noi è nella figura a destra). Successivamente assicuratevi che l'utente Kali possa aprire il file assegnando i permessi necessari - riferimento figura in a destra. A questo punto fate doppio click per analizzare la cattura.



Qualora doveste avere problemi per spostare il file su Kali, trovate una prima parte della cattura negli screenshot di seguito, sufficienti per completare l'esercizio.

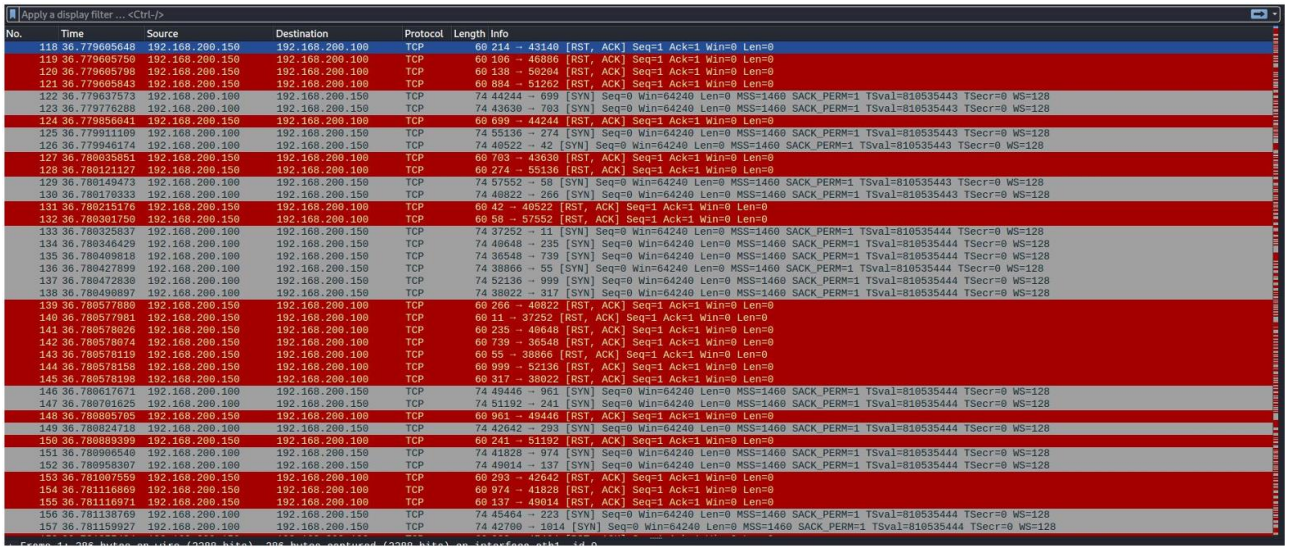






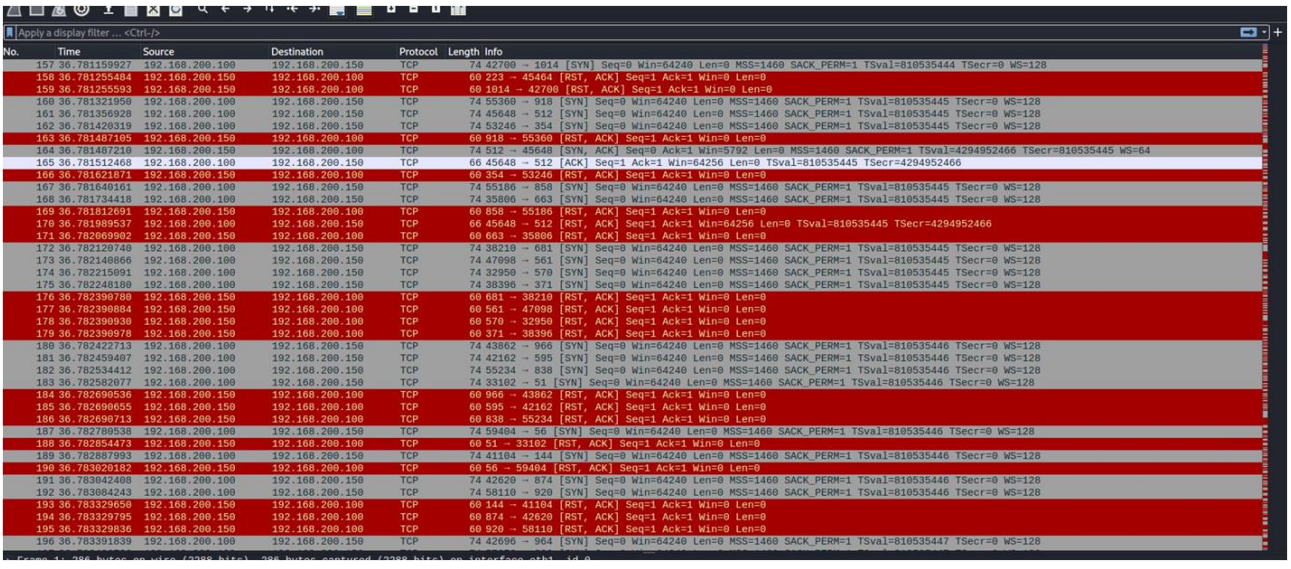
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
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_PERM=1 TSval=810535441 TSecr=0 WS=128
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_PERM=1 TSval=810535441 TSecr=0 WS=128
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=810535441 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
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=810535441 TSecr=4294952466
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=810535441 TSecr=4294952466
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_PERM=1 TSval=810535441 TSecr=0 WS=128
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_PERM=1 TSval=810535441 TSecr=0 WS=128
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_PERM=1 TSval=810535442 TSecr=0 WS=128
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_PERM=1 TSval=810535442 TSecr=0 WS=128
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_PERM=1 TSval=810535442 TSecr=0 WS=128
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_PERM=1 TSval=810535442 TSecr=0 WS=128
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	36.778759630	192.168.200.100	192.168.200.150	TCP	74	40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
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_PERM=1 TSval=810535442 TSecr=0 WS=128
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_PERM=1 TSval=810535442 TSecr=0 WS=128
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=1 TSval=810535442 TSecr=0 WS=128
108	36.779029210	192.168.200.150	192.168.200.100	TCP	60	856 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.779055243	192.168.200.100	192.168.200.150	TCP	74	56542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
110	36.779122299	192.168.200.150	192.168.200.100	TCP	60	84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145004	192.168.200.100	192.168.200.150	TCP	74	40138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
112	36.779252884	192.168.200.150	192.168.200.100	TCP	60	807 → 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36.779273781	192.168.200.100	192.168.200.150	TCP	74	43140 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
114	36.779309462	192.168.200.100	192.168.200.150	TCP	74	46886 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
115	36.779354564	192.168.200.150	192.168.200.100	TCP	60	948 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	36.779378630	192.168.200.100	192.168.200.150	TCP	74	50204 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
117	36.779397023	192.168.200.100	192.168.200.150	TCP	74	51202 → 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
118	36.779605648	192.168.200.150	192.168.200.100	TCP	60	214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



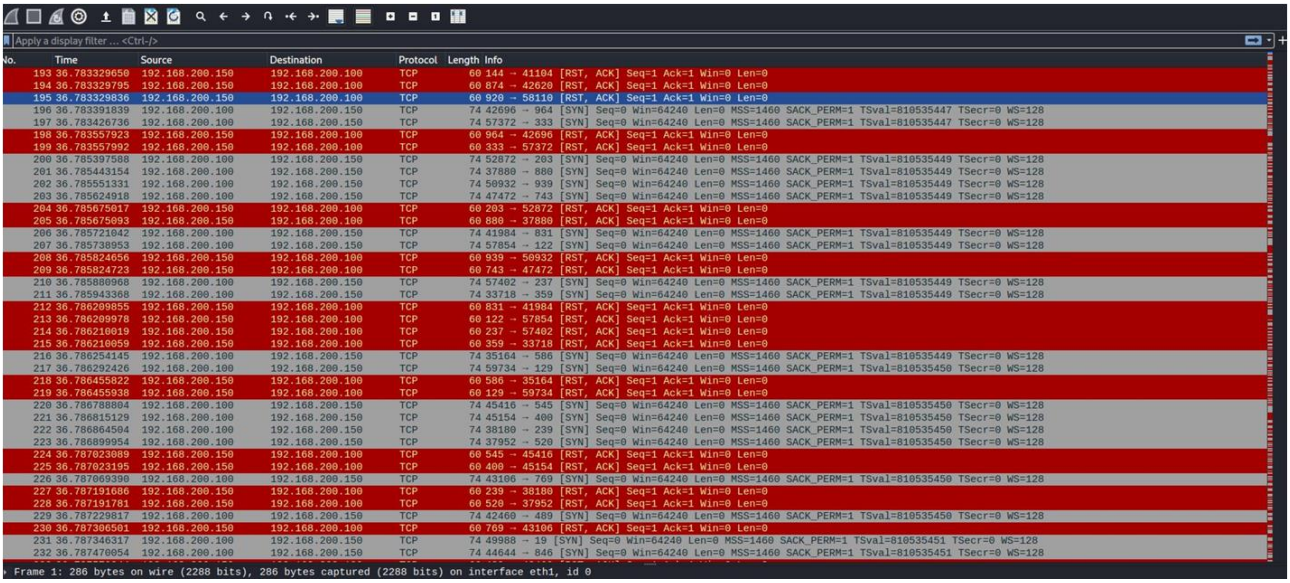
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
118	36.779605648	192.168.200.150	192.168.200.100	TCP	60	214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	36.779605750	192.168.200.150	192.168.200.100	TCP	60	106 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
120	36.779605798	192.168.200.150	192.168.200.100	TCP	60	138 → 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121	36.779605843	192.168.200.150	192.168.200.100	TCP	60	884 → 51202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122	36.779637573	192.168.200.100	192.168.200.150	TCP	74	44244 → 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
123	36.779776288	192.168.200.100	192.168.200.150	TCP	74	43630 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
124	36.779856041	192.168.200.150	192.168.200.100	TCP	60	699 → 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	36.779911109	192.168.200.100	192.168.200.150	TCP	74	55136 → 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
126	36.779946174	192.168.200.100	192.168.200.150	TCP	74	40522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
127	36.780035851	192.168.200.150	192.168.200.100	TCP	60	703 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128	36.780121127	192.168.200.150	192.168.200.100	TCP	60	274 → 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	36.780149473	192.168.200.100	192.168.200.150	TCP	74	57552 → 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
130	36.780170333	192.168.200.100	192.168.200.150	TCP	74	40822 → 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
131	36.780215176	192.168.200.150	192.168.200.100	TCP	60	42 → 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132	36.780301750	192.168.200.150	192.168.200.100	TCP	60	58 → 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133	36.780325837	192.168.200.100	192.168.200.150	TCP	74	37252 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
134	36.780346429	192.168.200.100	192.168.200.150	TCP	74	40648 → 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
135	36.780409818	192.168.200.100	192.168.200.150	TCP	74	36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
136	36.780427899	192.168.200.100	192.168.200.150	TCP	74	38866 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
137	36.780472830	192.168.200.100	192.168.200.150	TCP	74	52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
138	36.780490897	192.168.200.100	192.168.200.150	TCP	74	38022 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
139	36.780577880	192.168.200.150	192.168.200.100	TCP	60	266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577981	192.168.200.150	192.168.200.100	TCP	60	11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780578026	192.168.200.150	192.168.200.100	TCP	60	235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	36.780578074	192.168.200.150	192.168.200.100	TCP	60	739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	36.780578119	192.168.200.150	192.168.200.100	TCP	60	55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	36.780578165	192.168.200.150	192.168.200.100	TCP	60	999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	36.780578198	192.168.200.150	192.168.200.100	TCP	60	317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146	36.780617671	192.168.200.100	192.168.200.150	TCP	74	49446 → 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
147	36.780701625	192.168.200.100	192.168.200.150	TCP	74	51192 → 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
148	36.780805705	192.168.200.150	192.168.200.100	TCP	60	961 → 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149	36.780824718	192.168.200.100	192.168.200.150	TCP	74	42642 → 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
150	36.780889399	192.168.200.150	192.168.200.100	TCP	60	241 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151	36.780908540	192.168.200.100	192.168.200.150	TCP	74	41828 → 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
152	36.780958307	192.168.200.100	192.168.200.150	TCP	74	49014 → 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
153	36.781007559	192.168.200.150	192.168.200.100	TCP	60	293 → 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
154	36.781116869	192.168.200.150	192.168.200.100	TCP	60	974 → 41828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155	36.781116971	192.168.200.150	192.168.200.100	TCP	60	137 → 49014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
156	36.781138769	192.168.200.100	192.168.200.150	TCP	74	45464 → 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
157	36.781159927	192.168.200.100	192.168.200.150	TCP	74	42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
157	36.781159927	192.168.200.100	192.168.200.150	TCP	74	42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
158	36.781255484	192.168.200.150	192.168.200.100	TCP	60	223 → 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159	36.781255593	192.168.200.150	192.168.200.100	TCP	60	1014 → 42700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
160	36.781321950	192.168.200.100	192.168.200.150	TCP	74	55360 → 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
161	36.781356928	192.168.200.100	192.168.200.150	TCP	74	45648 → 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
162	36.781420319	192.168.200.100	192.168.200.150	TCP	74	53246 → 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
163	36.781487105	192.168.200.150	192.168.200.100	TCP	60	918 → 55360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164	36.781487219	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535445 WS=64
165	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
166	36.781621871	192.168.200.150	192.168.200.100	TCP	60	354 → 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167	36.781640161	192.168.200.100	192.168.200.150	TCP	74	55186 → 858 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
168	36.781734418	192.168.200.100	192.168.200.150	TCP	74	35806 → 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
169	36.781812691	192.168.200.150	192.168.200.100	TCP	60	858 → 55186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170	36.781989537	192.168.200.100	192.168.200.150	TCP	66	45648 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
171	36.782069902	192.168.200.150	192.168.200.100	TCP	60	663 → 35806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172	36.782120748	192.168.200.100	192.168.200.150	TCP	74	38210 → 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
173	36.782140866	192.168.200.100	192.168.200.150	TCP	74	47098 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
174	36.782215091	192.168.200.100	192.168.200.150	TCP	74	32950 → 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
175	36.782248180	192.168.200.100	192.168.200.150	TCP	74	38396 → 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
176	36.782390780	192.168.200.150	192.168.200.100	TCP	60	681 → 38210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177	36.782390884	192.168.200.150	192.168.200.100	TCP	60	561 → 47098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
178	36.782390930	192.168.200.150	192.168.200.100	TCP	60	570 → 32950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179	36.782390978	192.168.200.150	192.168.200.100	TCP	60	371 → 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
180	36.782422713	192.168.200.100	192.168.200.150	TCP	74	43862 → 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
181	36.782459407	192.168.200.100	192.168.200.150	TCP	74	42162 → 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
182	36.782534412	192.168.200.100	192.168.200.150	TCP	74	55234 → 838 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
183	36.782582077	192.168.200.100	192.168.200.150	TCP	74	33102 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
184	36.782690536	192.168.200.150	192.168.200.100	TCP	60	966 → 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185	36.782690655	192.168.200.150	192.168.200.100	TCP	60	595 → 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	36.782690713	192.168.200.150	192.168.200.100	TCP	60	838 → 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187	36.782780538	192.168.200.100	192.168.200.150	TCP	74	59404 → 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
188	36.782854473	192.168.200.150	192.168.200.100	TCP	60	51 → 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
189	36.782887993	192.168.200.100	192.168.200.150	TCP	74	41104 → 144 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
190	36.783020182	192.168.200.150	192.168.200.100	TCP	60	56 → 59404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
191	36.783042408	192.168.200.100	192.168.200.150	TCP	74	42620 → 874 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
192	36.783084243	192.168.200.100	192.168.200.150	TCP	74	58110 → 920 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
193	36.783329650	192.168.200.150	192.168.200.100	TCP	60	144 → 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
194	36.783329795	192.168.200.150	192.168.200.100	TCP	60	874 → 42620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
195	36.783329836	192.168.200.150	192.168.200.100	TCP	60	920 → 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
196	36.783391839	192.168.200.100	192.168.200.150	TCP	74	42696 → 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128



Traccia esercizio facoltativo

- Cos'è il CSIRT Italia ACN ?
- Quali sono i suoi compiti?
- Esamina l'allerta:
  - https://www.csirt.gov.it/contenuti/campagna-phishing-a-tema-sondaggio-trenitalia-al03-240322-csirt-ita
- Come puoi proteggere la tua organizzazione da questa campagna phishing?

Svolgimento esercizio principale

Questo report analizza il traffico di rete registrato tra i dispositivi 192.168.200.100 e 192.168.200.150, basato sui dati forniti nel file di Wireshark. Si ipotizza che il dispositivo target sia una macchina Metasploitable2, comunemente utilizzata come obiettivo per test di penetrazione.

Analisi del Traffico

Scansione delle Porte

L'attaccante ha probabilmente avviato una scansione delle porte. Le righe del file di Wireshark mostrano numerosi pacchetti TCP SYN inviati da 192.168.200.100 verso 192.168.200.150. Questa attività è tipica di una scansione stealth, come quella eseguita con Nmap utilizzando il flag -sS, che invia solo pacchetti SYN senza completare il three-way handshake.

Identificazione delle Porte Aperte e Chiuse

Le risposte RST ricevute dal dispositivo 192.168.200.150 (ad esempio, righe 5, 21, 26, e 47) indicano che molte delle porte tentate sono chiuse. Questo comportamento suggerisce che l'attaccante sta mappando le porte per identificare quali servizi sono attivi e quali potrebbero essere vulnerabili a exploit.

Richieste ARP

Le richieste ARP (righe 8-11) mostrano che i dispositivi stanno cercando di risolvere gli indirizzi IP associati ai propri indirizzi MAC. Questo è un passo necessario per la comunicazione nella rete locale e indica che il traffico è attivo.

Conclusioni

In sintesi, l'analisi del traffico, come evidenziato nel file di Wireshark, suggerisce che l'attaccante ha utilizzato una scansione delle porte per identificare il dispositivo Metasploitable2 come potenziale vittima. La scansione delle porte, probabilmente eseguita con Nmap utilizzando il flag -sS, ha rivelato porte chiuse tramite risposte RST.

Svolgimento esercizio facoltativo

Cos'è il CSIRT Italia (ACN)

Il **CSIRT Italia** è il team nazionale che si occupa della risposta agli incidenti informatici. Fa parte dell'Agenzia per la Cybersicurezza Nazionale (ACN) e ha il compito di supportare enti pubblici, aziende e cittadini nella gestione delle minacce informatiche.

Compiti del CSIRT Italia

I principali compiti del CSIRT Italia sono:

- **Monitoraggio**: Raccogliere e analizzare dati su minacce e vulnerabilità.
- **Risposta a Incidenti**: Offrire supporto tecnico in caso di attacchi informatici.
- **Prevenzione**: Sviluppare strategie per evitare attacchi.
- **Sensibilizzazione**: Informare e formare i cittadini e le aziende sulla sicurezza informatica.
- **Collaborazione**: Lavorare insieme ad altre agenzie internazionali e nazionali.

Analisi allerta Trenitalia

L'allerta riguardante una campagna di phishing a tema "sondaggio Trenitalia" avvisa gli utenti su email fraudolente che sembrano provenire da Trenitalia. Queste email invitano a partecipare a sondaggi e mirano a rubare informazioni personali.

Come Proteggere l'Organizzazione

Per difendersi da questa campagna di phishing, le organizzazioni possono adottare le seguenti misure:

1. **Formazione dei Dipendenti**: Educare i collaboratori a riconoscere email sospette.
2. **Filtri Antispam**: Utilizzare soluzioni per bloccare email pericolose.
3. **Verifica delle Comunicazioni**: Controllare sempre l'autenticità di email e link.
4. **Autenticazione a Due Fattori**: Implementare sistemi di sicurezza aggiuntivi per gli accessi.
5. **Aggiornamenti di Sicurezza**: Tenere software e sistemi operativi sempre aggiornati.
6. **Backup dei Dati**: Eseguire backup regolari per proteggere le informazioni aziendali.
7. **Segnalazione di Email Sospette**: Creare un protocollo interno per segnalare email o incidenti sospetti.

Adottando queste misure, le organizzazioni possono migliorare la loro sicurezza e ridurre il rischio di attacchi di phishing.

Cos'è il 4-Way Handshake

Il **4-Way Handshake** è un processo di autenticazione utilizzato nei protocolli di rete, in particolare nel protocollo Wi-Fi (802.11), per garantire una connessione sicura tra un client (come un computer o uno smartphone) e un punto di accesso (access point). Questo processo è fondamentale per stabilire una connessione sicura e per proteggere i dati trasmessi.

Fasi del 4-Way Handshake

Il 4-Way Handshake si compone di quattro passaggi principali:

1. **Message 1: Il Client Richiede una Connessione**
    - Il client invia un messaggio al punto di accesso per iniziare la connessione. Questo messaggio contiene un identificatore unico (nonce) generato dal client.
2. **Message 2: Il Punto di Accesso Risponde**
    - Il punto di accesso riceve il messaggio e risponde con un proprio nonce, insieme a una chiave di sessione che è derivata dalla chiave pre-condivisa (la password) e dai nonce scambiati. Questo messaggio è crittografato.
3. **Message 3: Il Client Conferma la Connessione**
    - Il client riceve il secondo messaggio e utilizza le informazioni per generare la chiave di sessione. Poi invia un messaggio di conferma al punto di accesso, indicando che ha ricevuto correttamente il nonce e la chiave.
4. **Message 4: Il Punto di Accesso Conferma la Connessione**
    - Infine, il punto di accesso invia un messaggio di conferma al client, completando il processo di autenticazione. A questo punto, entrambi i dispositivi possono iniziare a comunicare in modo sicuro utilizzando la chiave di sessione condivisa.

Importanza del 4-Way Handshake

- **Sicurezza**: Il 4-Way Handshake aiuta a prevenire attacchi come il "replay attack" e garantisce che solo i dispositivi autorizzati possano connettersi alla rete.
- **Crittografia**: Stabilisce una chiave di sessione che viene utilizzata per crittografare i dati trasmessi tra il client e il punto di accesso.
- **Autenticazione**: Verifica che entrambi i lati (client e punto di accesso) possano fidarsi l'uno dell'altro prima di iniziare a scambiare dati sensibili.

In sintesi, il 4-Way Handshake è un componente essenziale per garantire la sicurezza delle connessioni Wi-Fi.

Report su Agent Tesla

Agent Tesla è un tipo di malware, specificamente un **trojan di accesso remoto (RAT)**, scritto in **.NET**. È attivo dal 2014 e si concentra su sistemi operativi **Microsoft Windows**. Questo malware è molto versatile e ha diverse funzioni, tra cui il furto di informazioni sensibili, la registrazione di tasti e la cattura di schermate.

Caratteristiche e Funzionalità

Agent Tesla ha una serie di funzioni che lo rendono pericoloso:

1. **Furto di Credenziali**: Può raccogliere password, nomi utente, informazioni finanziarie e cronologia di navigazione da più di 50 applicazioni, come client di posta elettronica e browser web.
2. **Cattura di Schermate**: È in grado di fare screenshot del computer della vittima, raccogliendo informazioni sensibili.
3. **Intercettazione di Comunicazioni**: Può monitorare email, messaggi di chat e altre forme di comunicazione online.
4. **Registrazione di Tasti**: Monitora i tasti premuti, registrando informazioni sensibili come password e nomi utente.
5. **Caricamento e Download di File**: Può trasferire file dal computer della vittima e installare moduli aggiuntivi.
6. **Diffusione a Altri Sistemi**: Può propagarsi ad altri computer sulla rete sfruttando vulnerabilità.

Dettagli Tecnici

Agent Tesla utilizza tecniche di offuscamento, come l'encoding Base64 e la crittografia XOR, per nascondere il proprio codice e rendere più difficile il rilevamento da parte dei software di sicurezza. Inoltre, ha meccanismi anti-analisi per evitare di essere scoperto.

Processo di Esecuzione

La maggior parte delle campagne di Agent Tesla avviene in più fasi:

1. **Consegna**: Il malware viene inviato come allegato a un'email di spam, spesso in forma di documento di Office o file zip.
2. **Esecuzione**: Una volta aperto l'allegato, viene eseguito un downloader che scarica la seconda fase del malware.
3. **Raccolta delle Informazioni**: Il malware raccoglie informazioni dal sistema della vittima e le invia all'attaccante.

Agent Tesla utilizza diversi protocolli di comunicazione per inviare dati al server di comando e controllo, come **HTTP**, **SMTP**, **FTP** e **Telegram**.

Incidenti e Diffusione

Agent Tesla è stato utilizzato in molti attacchi informatici nel corso degli anni. Ha visto un aumento significativo durante la pandemia di COVID-19, con campagne che sfruttavano temi legati alla salute per ingannare le vittime. Ad esempio, nel 2020 sono state segnalate campagne che distribuivano Agent Tesla attraverso falsi aggiornamenti per dispositivi di protezione personale.

Nel 2022, è stato identificato come uno dei malware più diffusi nel settore educativo, colpendo circa il 7% delle organizzazioni a livello globale.

Conclusione

Agent Tesla è un malware pericoloso e versatile che continua a rappresentare una minaccia significativa per utenti e organizzazioni. La sua capacità di rubare informazioni sensibili e di diffondersi attraverso email di phishing sottolinea l'importanza di pratiche di sicurezza informatica rigorose, come la formazione degli utenti e l'uso di software di sicurezza aggiornati.

Fonti: https://en.wikipedia.org/wiki/Agent_Tesla