




S9/L3 Epicode Cybersecurity

Threat Intelligence & IOC



● Introduzione	3
● Ipotesi ed identificazione IOC	4
● Analisi approfondita	5
● Conclusioni	7



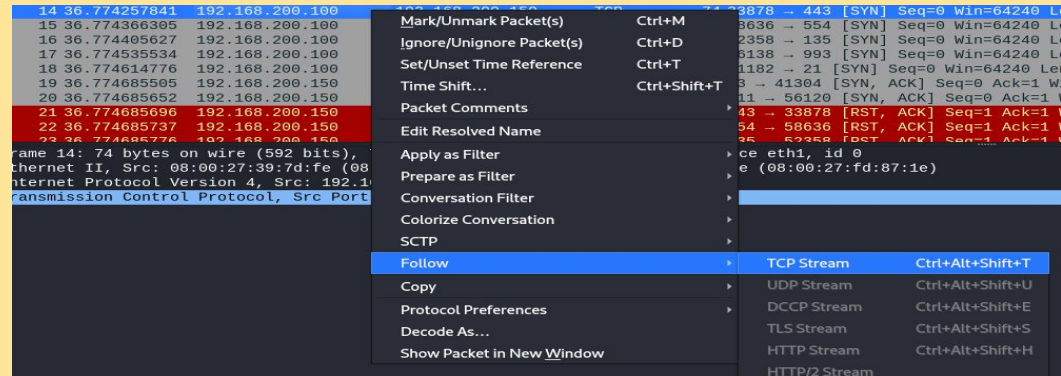
Nella lezione di oggi ci viene fornita una cattura su WireShark, che dobbiamo analizzare per capire se ci siano degli IOC, cosa sia avvenuto e quali remediation potremmo attuare per ovviare al problema. Iniziamo quindi la nostra analisi.

Nella schermata principale possiamo subito vedere come l'indirizzo IP 192.168.200.100 stia effettuando richieste di "three-way handshake" in molte porte dell'indirizzo IP 192.168.200.150. Questo ci fa ipotizzare che l'attaccante stia effettuando un port-scanning sulla vittima per controllare quali porte completino il three-way handshake e siano quindi aperte.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.100	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential B...
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	23.764287769	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	23.764777333	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	23.764777421	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	08:00:27:fd:87:1e	08:00:27:39:7d:fe	ARP	60	who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	08:00:27:39:7d:fe	08:00:27:fd:87:1e	ARP	42	who has 192.168.200.150? Tell 192.168.200.100
11	28.775230909	08:00:27:fd:87:1e	08:00:27:39:7d: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	36.774614775	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	36.774685595	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

Per capire meglio cosa ci troviamo davanti, andiamo ad analizzare a campione una richiesta TCP su una porta a scelta, cliccando col tasto destro > Follow > TCP Stream.


Da qui possiamo verificare per intero l'andamento della richiesta, quindi capire se la porta scelta sia in ascolto oppure no. In questo caso la porta risulterà chiusa.



No.	Time	Source	Destination	Protocol	Length	Info
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
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

Per comprendere meglio cosa ci troviamo davanti ed eliminare ogni dubbio, dalla schermata principale clicchiamo su Statistics > Conversations. Dalla schermata che ci appare possiamo vedere come sia stata scansionata ogni porta dalla 1 alla 1024 e, guardando quanti pacchetti la porta abbia ricevuto, capire quali siano le porte aperte.

Ethernet · 2		IPv4 · 2	IPv6	<u>TCP · 1026</u>	UDP · 1							
Address A	Port A	Address B	<u>Port B</u>	Packets	Bytes	Stream ID	<u>Packets A → B</u>	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
192.168.200.100	41182	192.168.200.150	21	4	280 bytes	8	3	206 bytes	1	74 bytes	36.774615	0.0012
192.168.200.100	55656	192.168.200.150	22	4	280 bytes	10	3	206 bytes	1	74 bytes	36.775387	0.0006
192.168.200.100	41304	192.168.200.150	23	4	280 bytes	2	3	206 bytes	1	74 bytes	36.774143	0.0015
192.168.200.100	60632	192.168.200.150	25	4	280 bytes	19	3	206 bytes	1	74 bytes	36.776512	0.0015
192.168.200.100	37282	192.168.200.150	53	4	280 bytes	21	3	206 bytes	1	74 bytes	36.776671	0.0014
192.168.200.100	53060	192.168.200.150	80	4	280 bytes	0	3	206 bytes	1	74 bytes	23.764215	0.0007
192.168.200.100	53062	192.168.200.150	80	4	280 bytes	11	3	206 bytes	1	74 bytes	36.775524	0.0005
192.168.200.100	56120	192.168.200.150	111	4	280 bytes	3	3	206 bytes	1	74 bytes	36.774218	0.0014
192.168.200.100	46990	192.168.200.150	139	4	280 bytes	17	3	206 bytes	1	74 bytes	36.776478	0.0014
192.168.200.100	33042	192.168.200.150	445	4	280 bytes	15	3	206 bytes	1	74 bytes	36.776386	0.0015
192.168.200.100	45648	192.168.200.150	512	4	280 bytes	68	3	206 bytes	1	74 bytes	36.781357	0.0006
192.168.200.100	42048	192.168.200.150	513	4	280 bytes	480	3	206 bytes	1	74 bytes	36.825398	0.0039
192.168.200.100	51396	192.168.200.150	514	4	280 bytes	118	3	206 bytes	1	74 bytes	36.788600	0.0011
192.168.200.100	37396	192.168.200.150	1	2	134 bytes	874	1	74 bytes	1	60 bytes	36.864770	0.0002



Grazie a questo controllo possiamo quindi evincere che le porte

21-22-23-25-53-80-111-139-445-512-513-514 siano aperte. Cosa possiamo fare, quindi, per ridurre l'impatto dell'attacco?

La soluzione più adatta sarebbe quindi quella di creare una regola nel firewall che chiuda quelle porte o una che blocchi l'accesso all'IP attaccante.