

Esercitazione WEEK 19 D4

Threat Intelligence & IOC

Ettore Farris

Descrizione sintetica

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 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

Svolgimento

Per prima cosa importiamo il file della cattura su wireshark dal menu file >>> open.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, X
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 TS
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 TS
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=42
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=429495116
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=4294
8	28.761629461	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_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 TS
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 TS
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 TS
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 TS
16	36.774495627	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 TS
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 TS
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 TS
19	36.774685505	192.168.200.100	192.168.200.100	TCP	74	23 -> 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=42
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=4
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 -> 33876 [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=429495246
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=42949524
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=42
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=429495246
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 TS
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TS
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 TS
32	36.775530906	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=4294
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=42
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=42
36	36.775797094	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=42
37	36.775803766	192.168.200.100	192.168.200.150	TCP	66	55656 -> 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=429495246

- **Identificare eventuali IOC, ovvero evidenze di attacchi in corso**

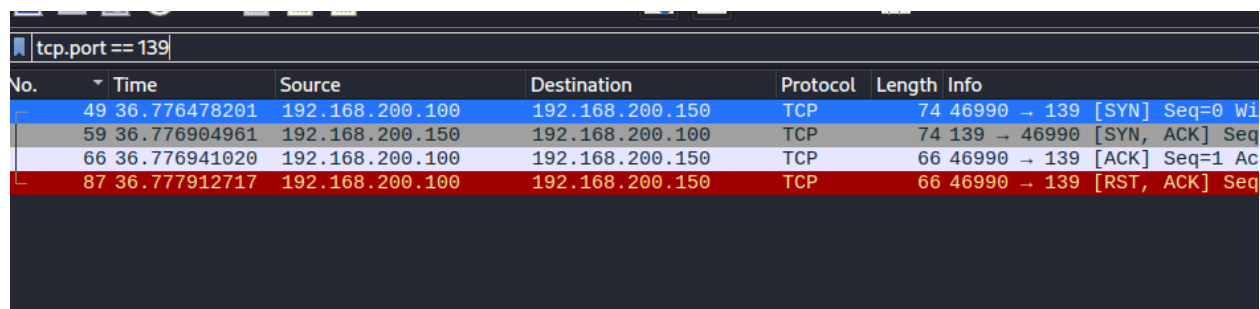
Analizzando i pacchetti, per prima cosa si può notare che il sistema con ip 192.168.200.150 è oggetto di multiple richieste TCP su un ampio intervallo di porte provenienti sempre dallo stesso indirizzo IP, ovvero 192.168.200.100.

- **In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati**

Le richieste oltretutto sono state effettuate in un tempo relativamente breve. Questo farebbe pensare a un'attività di scanning effettuata tramite dei tool automatici come nmap.

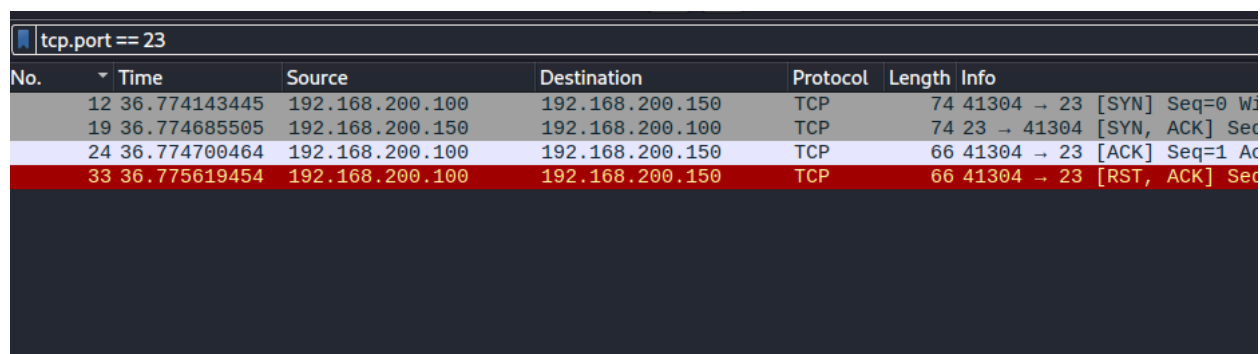
Filtrando i risultati per porta, possiamo notare il completamento di una *three-way-handshake* e la chiusura immediata della comunicazione. Questo farebbe pensare a una scansione nmap TCP (ovvero con flag -sT).

Filtro su porta 139:



No.	Time	Source	Destination	Protocol	Length	Info
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=0
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990 [SYN, ACK] Seq=1
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [ACK] Seq=1
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [RST, ACK] Seq=1

Filtro su porta 23:



No.	Time	Source	Destination	Protocol	Length	Info
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=0
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=1
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] Seq=1

- **Consigliate un'azione per ridurre gli impatti dell'attacco**

Una soluzione per impedire l'attività di scanning, potrebbe essere quella di configurare bene il firewall affinché questo blocchi il traffico in entrata.