

UNIT3 S9/L5 - Threat intelligence

Obiettivo:

Data la cattura di rete effettuata con Wireshark (file in allegato <https://shorturl.at/hESXt>) 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

Scenario:

Il file in allegato è una cattura di rete effettuata con Wireshark dalla quale è possibile vedere sin da subito alcune informazioni molto interessanti.

Gli indirizzi IPv4 presenti sulla scansione sono due,

- **192.168.200.100 (macchina attaccante)**
- **192.168.200.150. (macchina vittima)**

No.	Time	Source	Destination	Protocol	Length	Info
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55862 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva1=810535439 Tscr=4294952466
41	36.776095853	192.168.200.100	192.168.200.150	TCP	66	53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsva1=810535439 Tscr=4294952466
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 - 199 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535439 Tscr=0 WS=128
43	36.776180028	192.168.200.100	192.168.200.150	TCP	74	54594 - 199 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	51640 - 567 [SYN] Seq=0 Win=64249 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33942 - 445 [SYN] Seq=0 Win=64249 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
46	36.776402590	192.168.200.100	192.168.200.150	TCP	74	49814 - 259 [SYN] Seq=0 Win=64249 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
47	36.776451284	192.168.200.150	192.168.200.100	TCP	66	190 - 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	66	994 - 54226 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478261	192.168.200.100	192.168.200.150	TCP	74	46996 - 139 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
50	36.776512221	192.168.200.100	192.168.200.150	TCP	74	46996 - 139 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	69632 - 25 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
52	36.776568666	192.168.200.100	192.168.200.150	TCP	74	49054 - 119 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
53	36.776612717	192.168.200.100	192.168.200.150	TCP	74	37282 - 53 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
54	36.776615115	192.168.200.100	192.168.200.150	TCP	74	54989 - 569 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
55	36.776615132	192.168.200.100	192.168.200.150	TCP	69	36136 - 34684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776634243	192.168.200.100	192.168.200.150	TCP	74	51534 - 349 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
57	36.776994828	192.168.200.100	192.168.200.150	TCP	74	445 - 33842 [SYN, ACK] Seq=0 Ack=1 Win=5729 Len=0 MSS=1460 PERM=1 Tsva1=4294952466 Tscr=810535440 WS=64
58	36.776994922	192.168.200.150	192.168.200.100	TCP	66	250 - 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776994961	192.168.200.150	192.168.200.100	TCP	74	139 - 46994 [SYN, ACK] Seq=0 Ack=1 Win=5729 Len=0 MSS=1460 SACK_PERM=1 Tsva1=4294952466 Tscr=810535440 WS=64
60	36.776995004	192.168.200.150	192.168.200.100	TCP	66	143 - 33269 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776995032	192.168.200.150	192.168.200.100	TCP	74	139 - 46994 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62	36.776995082	192.168.200.150	192.168.200.100	TCP	69	110 - 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776995123	192.168.200.150	192.168.200.100	TCP	74	53 - 37282 [SYN, ACK] Seq=0 Ack=1 Win=5729 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=64
64	36.776995162	192.168.200.150	192.168.200.100	TCP	66	500 - 54893 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.776994772	192.168.200.100	192.168.200.150	TCP	66	33942 - 445 [SYN] Seq=1 Ack=1 Win=64256 Len=0 Tsva1=810535440 Tscr=4294952466 Tsva1=4294952466 Tscr=810535440 WS=64
66	36.776995228	192.168.200.100	192.168.200.150	TCP	66	46994 - 33842 [SYN] Seq=0 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=4294952466 Tsva1=4294952466 Tscr=810535440 WS=64
67	36.776995235	192.168.200.100	192.168.200.150	TCP	66	69632 - 79 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=4294952466 Tsva1=4294952466 Tscr=810535440 WS=64
68	36.776993874	192.168.200.100	192.168.200.150	TCP	66	37282 - 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=4294952466 Tsva1=4294952466 Tscr=810535440 WS=64
69	36.777118481	192.168.200.150	192.168.200.100	TCP	69	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	56999 - 707 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
71	36.777186821	192.168.200.100	192.168.200.150	TCP	74	35538 - 438 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
72	36.777186821	192.168.200.100	192.168.200.150	TCP	74	35538 - 438 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
73	36.777337934	192.168.200.100	192.168.200.150	TCP	74	49 - 79 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535440 Tscr=0 WS=128
74	36.777430632	192.168.200.150	192.168.200.100	TCP	60	707 - 56999 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777430741	192.168.200.150	192.168.200.100	TCP	66	430 - 35632 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777473918	192.168.200.100	192.168.200.150	TCP	74	36138 - 589 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535441 Tscr=0 WS=128
77	36.777522494	192.168.200.100	192.168.200.150	TCP	74	52428 - 969 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 SACK_PERM=1 Tsva1=810535441 Tscr=0 WS=128
78	36.777439852	192.168.200.150	192.168.200.100	TCP	66	98 - 34129 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Gli indirizzi Ip quindi fanno parte della stessa rete e la prima macchina invia un continuo flusso di pacchetti TCP verso la seconda macchina.

L'IOC principale è proprio questo numero elevato di **pacchetti TCP SYN** inviati tutti quanti in sequenza con brevissimi lassi di tempo, che fanno presupporre uno scan sistematico di tutte le porte da parte dell'attaccante nei confronti della macchina vittima, settandolo forse con un -T4 o -T5.

L'attaccante sta eseguendo uno **scan** tramite Nmap o un altro scan con le stesse funzioni, per capire quali siano le **porte aperte**. Probabilmente è ancora nella fase di information gathering più che di exploit.

Nello specifico è possibile vedere come la tecnica utilizzata sia quella dell'Half open scan, ossia il metodo per essere più difficilmente rilevabili dai log applicativi, resettando la connessione il prima possibile, senza completare la **Three-way handshake** sulle porte chiuse.

Source	Destination	Protocol	Length	Info
192.168.200.100	192.168.200.150	TCP	74	34782 → 26 [SYN] Seq=0 Win=64240
192.168.200.150	192.168.200.100	TCP	60	26 → 34782 [RST, ACK] Seq=1 Ack=1

(esempio con porta 26 chiusa)

Source	Destination	Protocol	Length	Info
192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1
192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0
192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256

(esempio con porta 25 aperta)

Soluzioni immediate:

Una volta analizzata la cattura di rete la prima cosa da fare è sicuramente **bloccare** l'indirizzo IP 192.168.200.100 dalle iptables della macchina vittima o dal firewall . Poi nell'immediato, essendo un IP facente parte della rete bisogna avviare **un'indagine interna** per cercare di **isolarlo**, bloccando ogni tentativo di scan anche per le altre macchine presenti sulla rete.

Soluzioni lungo termine:

- Una soluzione estremamente utile sarebbe sicuramente installare un sistema di rilevamento intrusione **IDS/IPS** in primis, così da poter rilevare subito un potenziale port scanning e bloccare automaticamente l'IP attaccante.
- Per difendersi da un movimento laterale post exploit è bene **segmentare** la rete interna, così da impedire all'attaccante di raggiungere asset critici.
- Implementare nel **firewall** politiche di “default deny” permetterebbero poi di chiudere tutte le **porte non necessarie**, per ridurre ancora di più la superficie di attacco.
- Per quanto riguarda invece le singole macchine o le singole persone, la **formazione** costante sui principi di sicurezza informatica e **l'aggiornamento** costante dei **sistemi** e delle applicazioni in uso complicherebbero maggiormente la vita di un hacker malevolo.