

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	60	55056 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776095853	192.168.200.100	192.168.200.150	TCP	60	55062 → 60 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	55684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
44	36.776338610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33842 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
46	36.776492580	192.168.200.100	192.168.200.150	TCP	74	48614 → 250 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
47	36.776451924	192.168.200.150	192.168.200.100	TCP	60	150 → 55064 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33200 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
52	36.776568666	192.168.200.100	192.168.200.150	TCP	74	49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
54	36.776728715	192.168.200.100	192.168.200.150	TCP	74	54890 → 589 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
57	36.776904830	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=1 TSval=4294952466 TSecr=810535440 WS=64
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	250 → 48614 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.77694961	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=1 TSval=4294952466 TSecr=810535440 WS=64
60	36.776959004	192.168.200.150	192.168.200.100	TCP	60	143 → 33200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776959043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
62	36.776959082	192.168.200.150	192.168.200.100	TCP	60	110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776959123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
64	36.776959102	192.168.200.150	192.168.200.100	TCP	60	500 → 54890 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66	33842 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66	36.776941020	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
67	36.776962320	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68	36.776983870	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69	36.777118481	192.168.200.150	192.168.200.100	TCP	60	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	56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
71	36.777180621	192.168.200.100	192.168.200.150	TCP	74	35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
72	36.777302991	192.168.200.100	192.168.200.150	TCP	74	34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
73	36.77737934	192.168.200.100	192.168.200.150	TCP	74	49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
74	36.777438632	192.168.200.150	192.168.200.100	TCP	60	707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777438741	192.168.200.150	192.168.200.100	TCP	60	436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777475016	192.168.200.150	192.168.200.100	TCP	74	35153 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
77	36.777522484	192.168.200.100	192.168.200.150	TCP	74	52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
78	36.777623982	192.168.200.150	192.168.200.100	TCP	60	98 → 34120 [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 L
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 192.16.8.200.100 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.