

S9L5

Traccia:

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 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



Cattura_U3_W1_L3.pcapng

Al giorno d'oggi le minacce informatiche si evolvono costantemente, l'analisi proattiva è la nostra migliore difesa. Partendo dai concetti di **Threat Intelligence** e **Indicatori di Compromissione**, la traccia di oggi ci porterà nel vivo dell'investigazione. Attraverso una cattura di rete effettuata con l'ausilio di **Wireshark**, cercheremo di svelare le tracce di un'attività malevola. L'obiettivo è quello di individuare gli **IOC**, formulare ipotesi sui potenziali **vettori di attacco** e, infine, proporre azioni concrete per mitigare l'impatto e prevenire le minacce.

Identificazione ed analisi di potenziali IOC

1.0.0.0.0.0.0.0.0.0	192.168.200.150	192.168.200.250	BROWSER	290 Host Announcement RELIABLE, workstation, Server, Print Queue server, Xenix server, NI workstation, NI server, Potential browser
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
4.23.764777323	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=4294951105 TSecr=810522427 WS=64
5.23.764777323	192.168.200.150	192.168.200.100	TCP	66.53060 - 53060 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6.23.764915269	192.168.200.100	192.168.200.150	TCP	66.53060 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951105
7.23.764999091	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=4294951105
8.28.761629461	PCSSystemtec.fid:87...	PCSSystemtec.39:7d...	ARP	69 Who has 192.168.200.100? Tell 192.168.200.150
9.28.761644613	PCSSystemtec.39:7d...	PCSSystemtec.fid:87...	ARP	42 Who has 192.168.200.100? Tell 192.168.200.150
10.28.774852257	PCSSystemtec.39:7d...	PCSSystemtec.fid:87...	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
11.28.775230909	PCSSystemtec.fid:87...	PCSSystemtec.39:7d...	ARP	69 192.168.200.150 is at 08:00:27:fd:87:1e
12.30.774244444	192.168.200.100	192.168.200.150	TCP	74.53060 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13.30.774218110	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
14.30.774257841	192.168.200.100	192.168.200.150	TCP	74.33876 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15.30.774366305	192.168.200.100	192.168.200.150	TCP	74.56636 - 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16.30.774409227	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
17.30.774535534	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
18.30.774614776	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 TSecr=0 WS=128
19.30.774685595	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
20.30.774685652	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
21.30.774685696	192.168.200.150	192.168.200.100	TCP	69.443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22.30.774685737	192.168.200.150	192.168.200.100	TCP	69.354 - 36888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23.30.774685776	192.168.200.150	192.168.200.100	TCP	69.135 - 52368 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24.30.774706464	192.168.200.100	192.168.200.150	TCP	66.41304 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25.30.774711072	192.168.200.100	192.168.200.150	TCP	66.56120 - 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26.30.774711101	192.168.200.150	192.168.200.100	TCP	69.53060 - 53060 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27.30.775141273	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=4294952466 TSecr=810535438 WS=64
28.30.775174048	192.168.200.100	192.168.200.150	TCP	66.41182 - 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
29.30.775337080	192.168.200.100	192.168.200.150	TCP	74.50974 - 115 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30.30.775386694	192.168.200.100	192.168.200.150	TCP	74.56566 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31.30.775524264	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 TSecr=0 WS=128
32.30.775580896	192.168.200.150	192.168.200.100	TCP	69.115 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33.30.775619444	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=4294952466
34.30.775652497	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=4294952466
35.30.775696938	192.168.200.150	192.168.200.100	TCP	74.22 - 59556 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36.30.775719104	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=4294952466 TSecr=810535439 WS=64
37.30.775803786	192.168.200.100	192.168.200.150	TCP	66.55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38.30.775813232	192.168.200.100	192.168.200.150	TCP	66.53062 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39.30.775813584	192.168.200.100	192.168.200.150	TCP	66.41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40.30.775975876	192.168.200.100	192.168.200.150	TCP	66.55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41.30.776095853	192.168.200.100	192.168.200.150	TCP	66.53062 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42.30.776179338	192.168.200.100	192.168.200.150	TCP	74.50684 - 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43.30.776233080	192.168.200.100	192.168.200.150	TCP	74.54228 - 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44.30.776330610	192.168.200.100	192.168.200.150	TCP	74.34648 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45.30.776385694	192.168.200.100	192.168.200.150	TCP	74.33842 - 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46.30.776492590	192.168.200.100	192.168.200.150	TCP	74.48814 - 258 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47.30.776451284	192.168.200.150	192.168.200.100	TCP	69.199 - 50604 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48.30.776451357	192.168.200.150	192.168.200.100	TCP	69.995 - 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49.30.776478201	192.168.200.100	192.168.200.150	TCP	74.46990 - 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50.30.776496366	192.168.200.100	192.168.200.150	TCP	74.33206 - 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
51.30.776512221	192.168.200.100	192.168.200.150	TCP	74.60632 - 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
52.30.776509696	192.168.200.100	192.168.200.150	TCP	74.49654 - 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
53.30.776671271	192.168.200.100	192.168.200.150	TCP	74.37282 - 52 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
54.30.776720715	192.168.200.100	192.168.200.150	TCP	74.54898 - 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
55.30.776741143	192.168.200.150	192.168.200.100	TCP	69.507 - 57648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Tramite una prima analisi all'esame di Wireshark fornito, possiamo identificare la macchina con IP 192.168.200.150 come vittima/target e la macchina con IP 192.168.200.100 come attaccante. Si può capire da diversi fattori:

L'annuncio nella prima riga "ANNOUNCEMENT METASPOITABLE" è una prova inconfutabile che la macchina .150 è un target vulnerabile creato appositamente per i test.

L'IP .100, in molte righe è la *Source*, sta inviando dei pacchetti con il flag SYN, traducibili in tentativi di apertura TCP a molte porte di .150 che è la *Destination* in rapida successione.

Questo è un comportamento tipico di un **port scanning** (ad esempio **nmap**). In risposta il .150 manda dei RST, ACK che si traducono in rifiuti o servizio non attivo su quella porta. Un altro fattore interessante è l'ordine temporale delle richieste SYN da parte del .100 verso molte porte del .150, queste richieste hanno in comune un intervallo di tempo nelle righe, tipica caratteristica di scanner automatici o tool di enumerazione.

Inoltre possiamo notare che l'attaccante inizialmente prova una scansione completa sulla porta 80 e 443, ricevendo in risposta un SYN, ACK completando il triple-hand-shake sulla porta 80. Successivamente procede con una scansione stealth (Half-open), incrementando la velocità e la copertura delle richieste TCP, effettuando un port scan verso 192.168.200.150 — molti SYN in rapida successione verso porte multiple, con risposte RST/ACK dal target.

1 0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
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=64	
3 23.764897768	192.168.200.100	192.168.200.150	TCP	74 53076 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=64	
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=4294951165 TSecr=810522427 WS=64	
5 23.764777427	192.168.200.150	192.168.200.100	TCP	60 443 → 53076 [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	

(Quando si ottiene la risposta RST/ACK si traduce in servizio non aperto. Quando invece non si ottiene risposta dopo il SYN quella porta è filtrata)

Sembrerebbe che l'intenzione dell'attaccante è quella di sondare determinate porte (443,80,445,139,21,22) probabilmente mirando a servizi come http/https, smb e ssh. Tramite **nmap** sarà semplice per l'attaccante ottenere informazioni riguardo ai servizi utilizzati e alle rispettive versioni; questo indica un campanello d'allarme soprattutto se questi servizi non sono stati configurati correttamente e aggiornati con le ultime versione fornite dai **provider**.

*(Si raccomanda vivamente di eseguire gli aggiornamenti del software e dei sistemi operativi **esclusivamente** tramite i canali ufficiali e i link forniti direttamente dai rispettivi provider)*

Time	Source	Destination	Protocol	Length	Info
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=4294951165 TSecr=810522427 WS=64	
19 36.774405595	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 36.774405652	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	
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=4294952466 TSecr=810535438 WS=64	
35 36.775796938	192.168.200.150	192.168.200.100	TCP	74 22 → 56566 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64	
36 36.775797064	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=4294952466 TSecr=810535439 WS=64	
57 36.776904828	192.168.200.150	192.168.200.100	TCP	74 445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64	
59 36.776904961	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 TSval=4294952466 TSecr=810535440 WS=64	
61 36.776905043	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 TSval=4294952466 TSecr=810535440 WS=64	
63 36.776905123	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 TSval=4294952466 TSecr=810535440 WS=64	
164 36.781407210	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 TSval=4294952466 TSecr=810535445 WS=64	
267 36.788005940	192.168.200.150	192.168.200.100	TCP	74 514 → 51396 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64	
994 36.825722553	192.168.200.150	192.168.200.100	TCP	74 513 → 42048 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64	
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	
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=4294952466	
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=4294952466	
39 36.775861964	192.168.200.100	192.168.200.150	TCP	66 41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466	
40 36.775975876	192.168.200.100	192.168.200.150	TCP	66 56566 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466	
41 36.776005053	192.168.200.100	192.168.200.150	TCP	66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466	
86 36.777892928	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	
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	
273 36.789681130	192.168.200.100	192.168.200.150	TCP	66 51396 → 514 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535453 TSecr=4294952467	
1075 36.829275924	192.168.200.100	192.168.200.150	TCP	66 42048 → 513 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535493 TSecr=4294952471	

Consapevoli che la macchina vittima è una Metasploitable, possiamo subito identificare alcune vulnerabilità note corrispondenti con le porte scannate dall'attaccante:

- **SMB:** Le porte **139** e **445** sono particolarmente vulnerabili in Metasploitable.

Vulnerabilità EternalBlue: Metasploitable è suscettibile a questa vulnerabilità critica di Windows (CVE-2017-0144), sfruttata dall'exploit EternalBlue della NSA. Questo permette a un attaccante di eseguire codice in remoto sul sistema. È stata resa famosa dall'attacco ransomware globale di WannaCry.

Accesso anonimo: È possibile ottenere accesso alle condivisioni di file SMB senza credenziali, consentendo all'attaccante di visualizzare o modificare file di sistema sensibili.

- **Apache (Web Server):** Le porte **80** (HTTP) e **443** (HTTPS) sono aperte e indicano un server web.

Moduli non sicuri: Metasploitable contiene moduli Apache non configurati correttamente o vulnerabili, come **mod_cgi**, che possono consentire l'esecuzione di script malevoli.

Direttive di configurazione deboli: Le configurazioni predefinite del server web possono esporre informazioni sensibili, come versioni del software e liste di directory.

- **SSH (Secure Shell):** La porta **22** è vulnerabile a diversi tipi di attacco.

Attacco Brute Force: Il servizio SSH su Metasploitable è configurato per consentire tentativi di login ripetuti. Questo permette a un attaccante di utilizzare tool automatici per indovinare la password di un utente, come "root", provando un gran numero di combinazioni.

Credenziali di default: Metasploitable ha credenziali di accesso predefinite e deboli, come msfadmin / msfadmin, che sono facili da indovinare e offrono un punto di ingresso immediato per un attaccante.

Indicatore di compromissione (IOC)

In questo scenario, un potenziale **Indicatore di Compromissione** è l'indirizzo IP **192.168.200.100**, in quanto è la sorgente del traffico anomalo e potenzialmente ostile. L'invio di pacchetti **SYN** in rapida successione verso porte multiple del bersaglio (**192.168.200.150**) è una chiara firma di **port scanning**, una fase di ricognizione di un attacco. L'indirizzo **.100** è costantemente la **sorgente** dei pacchetti che iniziano le connessioni. Questo lo identifica come il sistema che sta attivamente conducendo l'attacco, rendendolo un elemento di rischio immediato.

Sebbene l'indirizzo IP **192.168.200.100** sia l'IOC principale, il tipo di attacco e le vulnerabilità che sta cercando di sfruttare ci forniscono ulteriori IOC specifici.

- **Scansione del protocollo SMB (porte 139, 445):** Il traffico mostra che l'attaccante sta sondando attivamente queste porte, che sono tipicamente utilizzate per la condivisione di file. Questa attività suggerisce che l'attaccante sta cercando vulnerabilità note come **EternalBlue**, spesso presente in sistemi come Metasploitable.

- **Attacco Brute-Force SSH (porta 22):** Visto il particolare interesse da parte dell'attaccante alla porta **22**, un altro indice di compromissione potrebbe essere un numero elevato di tentativi di accesso al servizio ssh, probabilmente dato da un brute-force attack
- **Sondaggio dei servizi web (porte 80, 443):** I tentativi di connessione alle porte **80** (HTTP) e **443** (HTTPS) indicano che l'attaccante sta cercando vulnerabilità in un server web. Un **IOC** in questo caso potrebbe essere una richiesta HTTP che contiene un payload insolitamente lungo o una firma di codice malevolo, che suggerisce un tentativo di **code injection**.

Misure di sicurezza consigliate

Le contromisure consigliate saranno suddivise in tre categorie principali: **difesa immediata**, **prevenzione a lungo termine** e **risposta agli incidenti**.

Difesa Immediata:

- **Blocco dell'IP dell'attaccante:** La prima misura è quella di bloccare l'indirizzo IP di origine dell'attacco (**192.168.200.100**). Questo può essere fatto tramite un **firewall** o una **lista di controllo degli accessi (ACL)**. Il blocco impedisce ulteriori tentativi di scansione o attacco, isolando temporaneamente la minaccia.
- **Attivazione degli alert:** Creare alert basati su volume, comportamento e tipo di pacchetto. Questi alert dovrebbero essere configurati in un **sistema di rilevamento delle intrusioni (IDS)** o in un **SIEM** (*Security Information and Event Management*) per notificare immediatamente il team di sicurezza di attività sospette, come scansioni di rete o tentativi di brute-force.

Prevenzione a Lungo Termine:

- **Patching e Aggiornamenti:** Le vulnerabilità che l'attaccante sta sondando (SMB, SSH, HTTP) sono spesso risolvibili con patch e aggiornamenti. È fondamentale che tutti i servizi di rete siano regolarmente aggiornati per correggere le falle di sicurezza note.
- **Indurimento dei Servizi:**
 - **SMB:** Disabilitare il supporto per le versioni obsolete e non sicure del protocollo SMB e bloccare il traffico su alcune porte se non sono strettamente necessarie o inutilizzate.
 - **SSH:** Implementare l'autenticazione con una pass-phrase anziché la semplice password. Disabilitare l'accesso root diretto e utilizzare password complesse per tutti gli account. ***E' consigliato bloccare l'IP dopo un massimo di tentativi falliti***
 - **Servizi Web:** Assicurarsi che il server web sia configurato correttamente, che non esponga informazioni sensibili (come le versioni del software) e che sia protetto da un **Web Application Firewall (WAF)**.

Risposta agli Incidenti:

- **Analisi Forense:** Una volta che l'attacco è stato mitigato, è necessario condurre un'analisi forense sulla macchina **192.168.200.150** per determinare se la compromissione è avvenuta, identificare i file compromessi e valutare i potenziali danni.
- **Revisione dei Log:** Analizzare i log di sistema e di rete per cercare altre attività sospette che potrebbero essere state compiute dall'attaccante prima del rilevamento.

Con l'implementazione di queste misure sarà possibile fermare l'attacco in corso, e grazie alla prevenzione proposta si potrà rendere il sistema più resiliente e protetto da futuri attacchi.