

THREAT INTELLIGENCE & IOC

MATTIA PASTORELLI



COMANDA:

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

64 36.7776905162	192.168.200.150	192.168.200.100	TCP	60 500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
65 36.7776914772	192.168.200.100	192.168.200.150	TCP	66 22042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466	
66 36.7776941020	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 36.7776962320	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 36.7776983878	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 TSval=810535440 TSecr=0 WS=128	
71 36.777186821	192.168.200.100	192.168.200.150	TCP	74 35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM 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 TSval=810535441 TSecr=0 WS=128	
73 36.777337934	192.168.200.100	192.168.200.150	TCP	74 49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128	
74 36.777430632	192.168.200.150	192.168.200.100	TCP	60 707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
75 36.777430741	192.168.200.150	192.168.200.100	TCP	60 436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
76 36.777473018	192.168.200.100	192.168.200.150	TCP	74 36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128	
77 36.777522494	192.168.200.100	192.168.200.150	TCP	74 52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128	
78 36.777623082	192.168.200.150	192.168.200.100	TCP	60 98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
79 36.777623149	192.168.200.150	192.168.200.100	TCP	60 78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
80 36.777645027	192.168.200.100	192.168.200.150	TCP	74 41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128	
81 36.777680898	192.168.200.100	192.168.200.150	TCP	74 51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535441 TSecr=0 WS=128	
82 36.777758636	192.168.200.150	192.168.200.100	TCP	60 580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	

Scansione con Wireshark

Scansione di Attacco in Corso: Analisi di un Risultato Wireshark
L'immagine qui sotto rappresenta un possibile tentativo di attacco, rilevato attraverso una scansione con Wireshark.
In questo caso, l'attacco consiste in una "semplificata" scansione dei servizi attivi su un obiettivo specifico (ad es. Nmap).

Un'analisi più attenta mostra una forte evidenza di attacco: un'intensa attività di richiesta SYN su molte porte, tutte in un breve lasso di tempo.
Le risposte visibili a schermo includono due scenari possibili:

- Il completamento del three-way handshake (SYN, SYN/ACK, ACK, RST/ACK).
- La richiesta di SYN seguita immediatamente da una risposta di RST, ACK.

200.150	TCP	66 33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS
200.150	TCP	66 46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS
200.150	TCP	66 60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS
200.150	TCP	66 37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS
200.100	TCP	60 487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200.150	TCP	74 56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=146
200.150	TCP	74 35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=146
200.150	TCP	74 34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
200.150	TCP	74 49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
200.100	TCP	60 707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200.100	TCP	60 436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200.150	TCP	74 36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=146
200.150	TCP	74 52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=146
200.100	TCP	60 98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200.100	TCP	60 78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200.150	TCP	74 41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=146
200.150	TCP	74 51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=146
200.100	TCP	60 550 → 55150 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

ER	286	Host Announcement METASPLOITA	LE, Workstation, Server, Print
	74 53060 → 80 [SYN] Seq=0 Win=64	40 Len=0 MSS=1460 SACK_PERM TS	
	74 33876 → 443 [SYN] Seq=0 Win=6	240 Len=0 MSS=1460 SACK_PERM	
	74 80 → 53060 [SYN, ACK] Seq=0 A	k=1 Win=5792 Len=0 MSS=1460 S	
	60 443 → 33876 [RST, ACK] Seq=1	ck=1 Win=0 Len=0	
	66 53060 → 80 [ACK] Seq=1 Ack=1	in=64256 Len=0 TSval=810522428	
	66 53060 → 80 [RST, ACK] Seq=1 A	k=1 Win=64256 Len=0 TSval=810	
	60 Who has 192.168.200.100? Tell	192.168.200.150	
	42 192.168.200.100 is at 08:00:02:39:7d:fe		

Due possibili scenari di connessione di porta

Analizzando il flusso di connessione tra le porte 35638 e 436, possono verificarsi due situazioni:

1. Tentativo di connessione: nel caso in cui venga inviata una richiesta SYN dalla porta 35638 alla porta 436, ma viene immediatamente chiusa con un messaggio RST, ACK, questo indica che la porta 436 è chiusa e non può essere scansionata.

2. Completamento della connessione: se invece la connessione viene completata con successo, significa che la porta è aperta e può essere scansionata. Tuttavia, la comunicazione può essere interrotta istantaneamente dal primo host con un messaggio RST, che indica la chiusura forzata della connessione.

COME PROTEGGERSI?

- CHIUDERE LE RICHIESTE DI PING DEL PROTOCOLLO ICMP
- ATTIVARE IL FIREWALL PER FILTRARE LE RICHIESTE
- IMPOSTARE UN NUMERO MASSIMO DI RICHIESTE CHE IL SERVER PUÒ GESTIRE E A CUI DEBBA RISPONDERE
- CREARE UNA ACL CHE VADA A BLOCCARE GLI IP SOSPETTI
- UTILIZZARE SERVIZI IN STILE CLOUDFLARE, CHE POSSONO FUNGERE DA PROXY, O DEI VERI PROXY
- CREARE UN HONEYPOT UTILIZZARE UNA VPN

