

EPICODE-CS0124

S9/L3 - Pratica

Flaviano Sedici

Indice

1. Traccia	3
1.1. Definizioni e impostazioni laboratorio	4
1.1.1. Definizioni	4
1.1.2. Impostazioni di laboratorio	4
1.2. Analisi del file Wireshark	4
1.2.1. Identificazione del tipo di richieste	4
1.2.2. Supposizione sulla tipologia di attacco	5
1.2.3. Consigli per operazioni di remediation	5

Riferimenti e versioni

Responsabile del documento: Flaviano Sedici

Versionamento

Versione	Descrizione	Riferimento	Data
1.0	Redazione documento	Responsabile	20/03/2024

1. 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 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.

1.1. Definizioni e impostazioni laboratorio

Prima di iniziare le scansioni richieste, definiamo il contesto operativo e gli strumenti utilizzati.

1.1.1. Definizioni

Wireshark

Wireshark è un software di analisi del traffico di rete open-source ampiamente utilizzato per catturare, visualizzare e analizzare il traffico di pacchetti in una rete. Consente agli utenti di esaminare il traffico in tempo reale o di analizzare i file di cattura esistenti per identificare problemi di rete, diagnosticare guasti, individuare attività sospette o analizzare la sicurezza della rete. Wireshark supporta una vasta gamma di protocolli di rete e offre potenti funzionalità di filtraggio, ricerca e analisi dei pacchetti, rendendolo uno strumento fondamentale per gli amministratori di rete, gli ingegneri di sicurezza e gli analisti di rete.

TCP

Il protocollo TCP (Transmission Control Protocol) è un protocollo di comunicazione affidabile e orientato alla connessione utilizzato per il trasferimento di dati su reti di computer. TCP suddivide i dati in segmenti e fornisce funzionalità di controllo di flusso, controllo di congestione e garanzia di consegna dei dati. Utilizza un meccanismo di handshaking a tre vie per stabilire e terminare le connessioni tra i dispositivi di comunicazione. TCP è ampiamente utilizzato per applicazioni che richiedono trasmissioni di dati affidabili e ordinate, come il trasferimento di file, la navigazione web e le comunicazioni email.

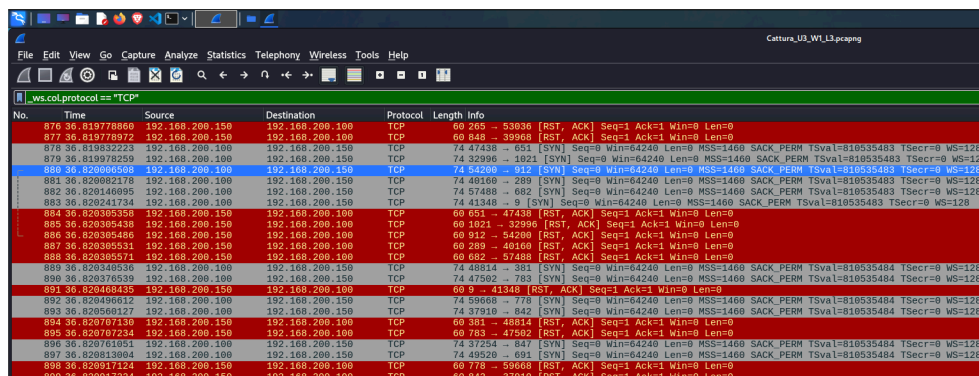
1.1.2. Impostazioni di laboratorio

Analizzando il file fornito dalla traccia, possiamo dedurre che la macchina attaccante ha un indirizzo IP 192.168.200.100 e la macchina target 192.168.200.150.

1.2. Analisi del file Wireshark

1.2.1. Identificazione del tipo di richieste

Analizzando i pacchetti presenti all'interno del file è evidente come la macchina con indirizzo IP 192.168.200.100 stia effettuando una scansione delle porte aperte sulla macchina target 192.168.200.150. Le richieste sono effettuate con protocollo TCP.



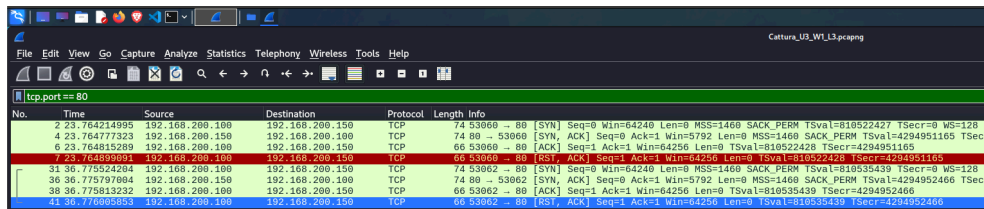
No.	Time	Source	Destination	Protocol	Length	Info
876	36.819778860	192.168.200.150	192.168.200.100	TCP	60	265 → 53936 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
877	36.819778972	192.168.200.150	192.168.200.100	TCP	60	648 → 39968 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
878	36.819832223	192.168.200.150	192.168.200.150	TCP	74	42485 → 6551 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535483 TSecr=0 WS=128
879	36.819978259	192.168.200.100	192.168.200.150	TCP	74	32996 → 1021 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535483 TSecr=0 WS=128
880	36.820006508	192.168.200.100	192.168.200.150	TCP	74	54200 → 612 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535483 TSecr=0 WS=128
881	36.820002176	192.168.200.100	192.168.200.150	TCP	74	40160 → 289 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535483 TSecr=0 WS=128
882	36.820146895	192.168.200.100	192.168.200.150	TCP	74	57488 → 682 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535483 TSecr=0 WS=128
883	36.820241734	192.168.200.100	192.168.200.150	TCP	74	41348 → 3 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535483 TSecr=0 WS=128
884	36.820305350	192.168.200.150	192.168.200.100	TCP	60	6551 → 47439 [EST, ACK] Seq=1 Ack=1 Win=0 Len=0
885	36.820305438	192.168.200.150	192.168.200.100	TCP	60	1021 → 32996 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
886	36.820305486	192.168.200.150	192.168.200.100	TCP	60	912 → 54200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
887	36.820305531	192.168.200.150	192.168.200.100	TCP	60	289 → 40160 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
888	36.820305571	192.168.200.150	192.168.200.100	TCP	60	682 → 57488 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
889	36.820305536	192.168.200.100	192.168.200.150	TCP	74	48814 → 381 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535484 TSecr=0 WS=128
890	36.820370539	192.168.200.100	192.168.200.150	TCP	74	47992 → 783 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535484 TSecr=0 WS=128
891	36.820408435	192.168.200.150	192.168.200.100	TCP	60	9 → 41348 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
892	36.820406612	192.168.200.100	192.168.200.150	TCP	74	59668 → 778 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535484 TSecr=0 WS=128
893	36.820506027	192.168.200.100	192.168.200.150	TCP	74	37910 → 842 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535484 TSecr=0 WS=128
894	36.820707130	192.168.200.150	192.168.200.100	TCP	60	381 → 48814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
895	36.820707234	192.168.200.150	192.168.200.100	TCP	60	783 → 47502 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
896	36.820810051	192.168.200.100	192.168.200.150	TCP	74	57254 → 447 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535484 TSecr=0 WS=128
897	36.820813084	192.168.200.100	192.168.200.150	TCP	74	49520 → 691 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535484 TSecr=0 WS=128
898	36.820917124	192.168.200.150	192.168.200.100	TCP	60	778 → 59668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
899	36.820917224	192.168.200.150	192.168.200.100	TCP	60	842 → 37910 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Analisi preliminare del file

1.2.2. Supposizione sulla tipologia di attacco

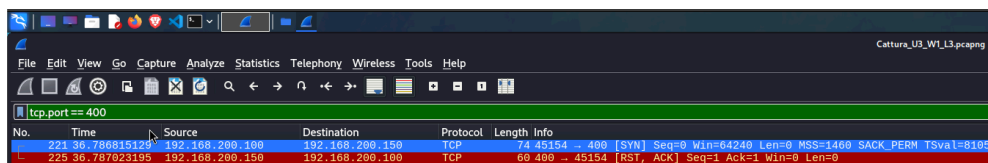
La grande mole di richieste TCP ci fa pensare ad una scansione presumibilmente effettuata con nmap con l'utilizzo di impostazioni standard.

Possiamo affermare che non sia stato utilizzato lo switch -sS in quando le richieste effettuate sono complete e comprendono tutte le fasi del three-way handshake.



No.	Time	Source	Destination	Protocol	Length	Info
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 Wnd=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=4294951165 TSecr=
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
23	764090001	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
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 TSecr=0 Wnd=128
36	36.775797004	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=
38	36.775813232	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
41	36.776000053	192.168.200.150	192.168.200.100	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Filtro sulla porta 80



No.	Time	Source	Destination	Protocol	Length	Info
221	36.786815129	192.168.200.100	192.168.200.150	TCP	74	45154 → 400 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8105
225	36.787023195	192.168.200.150	192.168.200.100	TCP	60	400 → 45154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Filtro sulla porta 400

1.2.3. Consigli per operazioni di remediation

L'attacco potrebbe essere contenuto nell'immediato applicando una regola sul firewall per bloccare l'indirizzo IP dell'attaccante.

Effettuato il contenimento dell'attacco nell'immediato, si potrebbe implementare una regola del firewall che impedisca il passaggio di pacchetti sulle porte che non necessariamente dovrebbero essere aperte per l'utilizzo dei regolari servizi esposti dalla macchina target.