THREAT INTELLIGENCE & IOC

Cyber Security & Ethical Hacking

Progetto

S9.L5

- Traccia:

Esercizio Threat Intelligence & IOC 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.

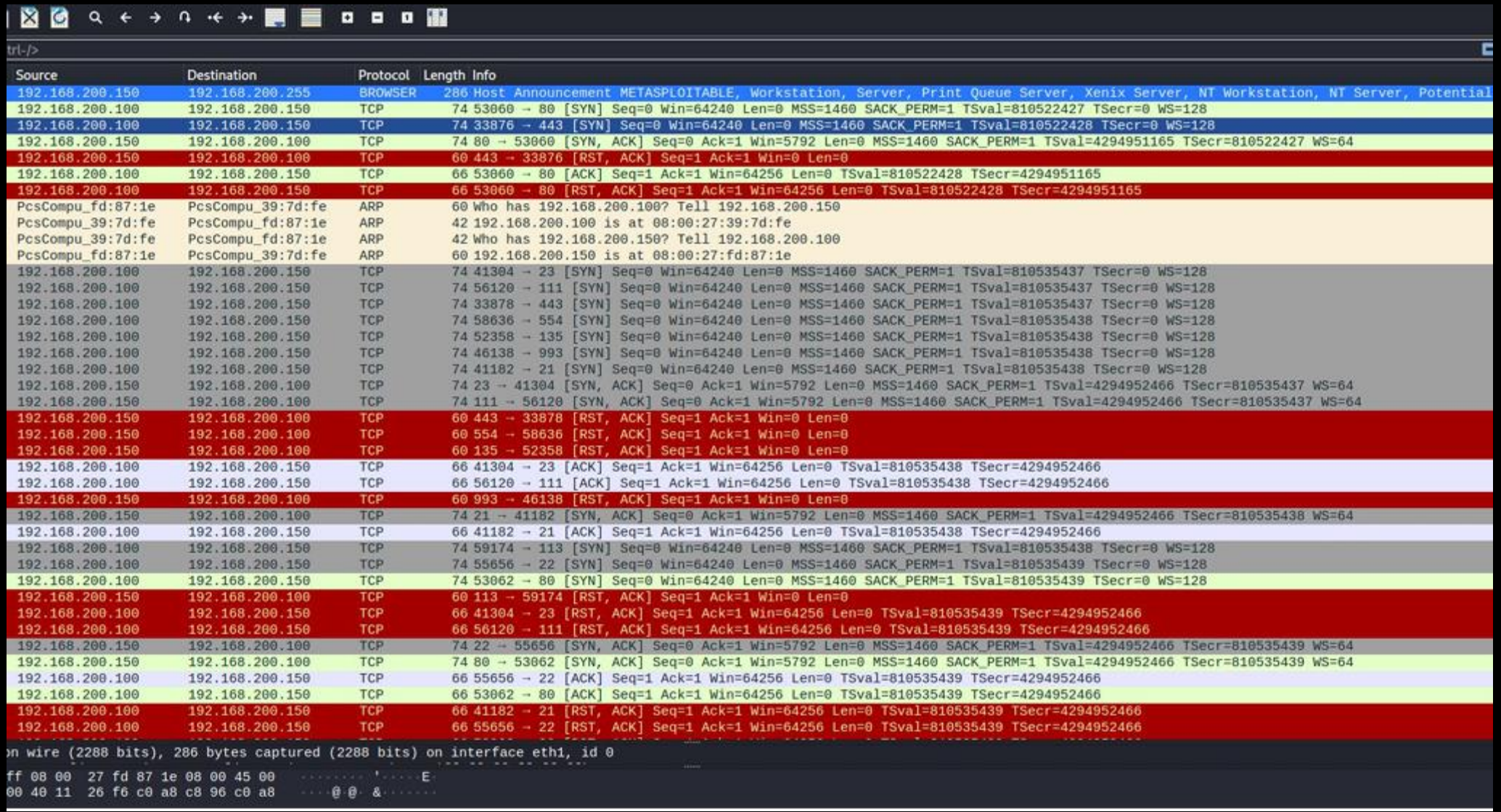
Introduzione.

Per l'esercizio di oggi, ci è stata fornita una cattura di rete analizzata tramite Wireshark al fine di individuare possibili IOC.

Dopo aver esaminato il file, siamo riusciti a determinare cosa sia accaduto, formulando diverse ipotesi che non abbiamo potuto verificare a causa della mancanza di ulteriori dati e risorse insufficienti.

In questo esercizio, ci concentreremo sul parlare di ciò che è accaduto realmente, fornendo dei consigli per mitigare i rischi emersi. Inoltre, dedicheremo anche uno spazio per illustrare le ipotesi che ho sviluppato.

Passiamo ora all'analisi del file, allego uno screenshot nella slide successiva.



Source	Destination	Protocol	Length	Info
192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential
192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522427 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522428 TSecr=0 WS=128
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=1 TSval=4294951165 TSecr=810522427 WS=64
192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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
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
PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
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=1 TSval=4294952466 TSecr=810535437 WS=64
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=1 TSval=4294952466 TSecr=810535437 WS=64
192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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
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
192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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=1 TSval=4294952466 TSecr=810535438 WS=64
192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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
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
192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64
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=1 TSval=4294952466 TSecr=810535439 WS=64
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
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
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
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

```
on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0
ff 08 00  27 fd 87 1e 08 00 45 00    ·····'····E
00 40 11  26 f6 c0 a8 c8 96 c0 a8    ·@·@ &·····
```

Prima di passare allo svolgimento vero e proprio dell'esercizio, vorrei dedicare qualche parola agli IOC, ovvero agli indicatori di compromissione. Questi indicatori sono segnali che suggeriscono una possibile violazione del sistema. Possono includere indirizzi IP sospetti, hash di file maligni, URL dannosi e così via.

Tali segnali vengono utilizzati dai professionisti della sicurezza per identificare, prevenire o mitigare le minacce, e sono essenziali per il monitoraggio delle reti e per garantire una risposta rapida agli incidenti.

Svolgimento!

Analizzando la cattura di Wireshark, individuiamo subito dei dati sospetti.

Come possiamo osservare, notiamo numerosi pacchetti SYN inviati da un unico indirizzo IP (192.168.200.100) verso diverse porte su un bersaglio specifico, in questo caso la macchina vittima (192.168.200.150). Possiamo quindi dire con certezza che la scansione viene effettuata da un dispositivo interno alla rete (ergo potrebbe trattarsi di un PC infetto, di una scansione fatta da qualcuno all'interno dell'azienda con fini malevoli, o da qualcuno nelle vicinanze che è riuscito ad accedere alla rete aziendale). Possiamo anche vedere che ci sono diverse porte prese di mira, come la 80 (HTTP), la 443 (HTTPS), la 21 (FTP) ecc, ma tutte appartenenti alle prime 1024, ovvero le porte note. Successivamente possiamo osservare che la stretta di mano a tre vie (three-way handshake) non è stata completata, il che conferma che si tratta di una scansione Nmap con l'opzione –sS (in questo caso nmap invia pacchetti SYN, ma non completa la connessione limitandosi a raccogliere le risposte). Proseguendo con la visione del file, notiamo che in alcuni casi la stretta di mano a tre vie viene conclusa, il che ci fa ipotizzare che sia stata effettuata una scansione Nmap anche con l'opzione -sT.

Mitigazione dei rischi.

Per mitigare i rischi, si consiglia di isolare immediatamente il dispositivo dalla rete aziendale (dato che conosciamo quale sia il PC) per evitare ulteriori attività dannose.

Successivamente, è fondamentale verificare l'integrità del PC compromesso per determinare se sia stato effettivamente infettato o se la scansione sia stata effettuata in modo consapevole.

Inoltre, si suggerisce di utilizzare strumenti specifici per monitorare la rete, al fine di individuare altre possibili anomalie.

Se non già implementato, si raccomanda di sviluppare un piano strategico con le relative procedure operative, per poter rispondere rapidamente a eventuali attacchi in futuro.

Ipotesi!

Oltre ad aver analizzato i dati, sono state sviluppate diverse ipotesi (che non è possibile confermare a causa della scarsità di dati a disposizione).

Tra queste, sono state ipotizzate le seguenti:

- ARP poisoning (spoofing)
- Infezione tramite malware
- Attaccho SYN flood (DoS), poiché se l'attaccante invia continuamente pacchetti SYN senza completare l'handshake TCP, può saturare le risorse del sistema bersaglio, impedendo la normale comunicazione.
- Tentativi di exploit: le porte scansionate potrebbero indicare il tentativo di sfruttare vulnerabilità conosciute su quei servizi.

Ma poiché i dati disponibili non consentono una conferma definitiva, le ipotesi devono rimanere come possibili scenari fino a quando non verranno raccolte ulteriori informazioni.

Conclusione.

In conclusione, possiamo affermare che l'analisi ha rivelato una scansione SYN effettuata tramite Nmap, proveniente da un dispositivo interno, con l'obiettivo di individuare le porte aperte. Questo comportamento rientra nella fase di ricognizione di un attacco (anche se, in questo caso, è stato eseguito in modo rumoroso).

Le azioni raccomandate includono il rafforzamento della sicurezza della rete e l'implementazione di misure di protezione avanzate.

Inoltre, se l'attacco non fosse stato eseguito intenzionalmente, ma piuttosto il dispositivo fosse stato compromesso, ad esempio, da malware, si suggerisce di concentrarsi anche sulla formazione del personale per prevenire attacchi futuri, come quelli provenienti da link dannosi o email di phishing.

GRAZIE PER L'ATTENZIONE!