

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

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ cd /media
(kali㉿kali)-[/media]
$ ls
sf_cartella_condivisa
(kali㉿kali)-[/media]
$ sf_cartella_condivisa
(kali㉿kali)-[/media/sf_cartella_condivisa]
$ ls
Cattura_U3_W1_L3.pcapng
(kali㉿kali)-[/media/sf_cartella_condivisa]
$ ls -la
total 212
drwxrwx--- 1 root vboxsf    0 Mar 14 20:40 .
drwxr-xr-x 3 root root    4096 Mar 14 20:43 ..
-rwxrwx--- 1 root vboxsf 209024 Nov  8 18:51 Cattura_U3_W1_L3.pcapng
(kali㉿kali)-[/media/sf_cartella_condivisa]
$ mv Cattura_U3_W1_L3.pcapng /home/kali/Desktop
(kali㉿kali)-[/media/sf_cartella_condivisa]
$ cd /home/kali/Desktop
(kali㉿kali)-[~/Desktop]
$ chmod ugo+rw Cattura_U3_W1_L3.pcapng
(kali㉿kali)-[~/Desktop]
$ chown kali Cattura_U3_W1_L3.pcapng
```

The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A display filter is applied: 'Apply a display filter ... <Ctrl-/>'. The packet list table shows the following data:

No.	Time	Source	Destination	Protocol	Length	Info
99	36.778663064	192.168.200.150	192.168.200.100	TCP	60	1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721080	192.168.200.150	192.168.200.100	TCP	60	206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36.778759636	192.168.200.100	192.168.200.150	TCP	74	40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=64240 Tsvr=0
102	36.778781327	192.168.200.100	192.168.200.150	TCP	74	51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=64240 Tsvr=0
103	36.778826294	192.168.200.150	192.168.200.100	TCP	60	131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778864493	192.168.200.100	192.168.200.150	TCP	74	39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=64240 Tsvr=0
105	36.778939327	192.168.200.150	192.168.200.100	TCP	60	392 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	36.778939427	192.168.200.150	192.168.200.100	TCP	60	677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	36.778963153	192.168.200.100	192.168.200.150	TCP	74	47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=64240 Tsvr=0
108	36.779029210	192.168.200.150	192.168.200.100	TCP	60	856 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.779055243	192.168.200.100	192.168.200.150	TCP	74	56542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=64240 Tsvr=0
110	36.779122299	192.168.200.150	192.168.200.100	TCP	60	84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145004	192.168.200.100	192.168.200.150	TCP	74	40138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=64240 Tsvr=0
112	36.779252884	192.168.200.150	192.168.200.100	TCP	60	807 → 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36.779273781	192.168.200.100	192.168.200.150	TCP	74	43140 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=64240 Tsvr=0
114	36.779309462	192.168.200.100	192.168.200.150	TCP	74	46886 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=64240 Tsvr=0
115	36.779354564	192.168.200.150	192.168.200.100	TCP	60	948 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	36.779378636	192.168.200.100	192.168.200.150	TCP	74	50204 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=64240 Tsvr=0

At the bottom, the packet details for Frame 106 are shown: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0. The packet structure is: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

- Multiple richieste TCP su ampi intervalli di porte, generalmente evidenzia una scansione in corso.
- Quando si osservano molteplici richieste TCP su ampi intervalli di porte, ci sono diverse ipotesi sui potenziali vettori di attacco che potrebbero essere utilizzati da parte degli aggressori:

1. Scansione delle porte per individuare vulnerabilità: Gli aggressori potrebbero effettuare una scansione delle porte per individuare servizi o protocolli aperti su un sistema. Questo potrebbe essere un precursore per individuare eventuali vulnerabilità note o configurazioni non sicure sui servizi in esecuzione.

2. Preparazione per un attacco mirato: Una scansione delle porte può essere utilizzata come fase preliminare per preparare un attacco mirato. Gli aggressori potrebbero cercare di individuare servizi specifici o applicazioni vulnerabili che possono essere sfruttate in seguito per compromettere il sistema o la rete.

3. Ricerca di punti di ingresso: Gli aggressori potrebbero essere alla ricerca di possibili punti di ingresso nella rete, come porte aperte o servizi non protetti, che possono essere utilizzati per ottenere accesso non autorizzato ai sistemi o per diffondere malware all'interno dell'ambiente aziendale.

4. Raccolta di informazioni per futuri attacchi: La scansione delle porte può essere utilizzata per raccogliere informazioni sulle infrastrutture di rete e sulle configurazioni dei sistemi. Queste informazioni possono essere utilizzate per pianificare attacchi più mirati e sofisticati in futuro.

- Quando si rileva un alto numero di richieste TCP su ampi intervalli di porte, ciò potrebbe indicare un comportamento tipico di scansione di rete da parte di un attaccante. Per ridurre gli impatti di tale attacco, è consigliabile adottare diverse azioni:

1. Monitoraggio del traffico di rete: Implementare un sistema di monitoraggio del traffico di rete per rilevare e analizzare le attività di scansione. Questo può aiutare a identificare rapidamente gli indirizzi IP sospetti o le serie di porte coinvolte nell'attività di scansione.

2. Blocco degli indirizzi IP sospetti: Utilizzare firewall o sistemi di rilevamento delle intrusioni per bloccare gli indirizzi IP che sono coinvolti nell'attività di scansione. Questo può limitare l'accesso dell'attaccante alla rete e ridurre l'impatto degli attacchi.

3. Limitazione dei tentativi di connessione: Impostare politiche per limitare il numero di tentativi di connessione per unità di tempo da parte di singoli indirizzi IP. Questo può aiutare a prevenire attacchi di scansione che tentano di individuare servizi aperti o vulnerabilità di sicurezza.

4. Implementazione di sistemi di autenticazione e accesso sicuri: Utilizzare sistemi di autenticazione robusti e meccanismi di accesso sicuri come VPN (Virtual Private Network) per proteggere l'accesso alla rete e ai servizi interni. Ciò può ridurre la possibilità che gli attaccanti utilizzino le scansioni di rete per individuare punti deboli nell'infrastruttura di sicurezza.