S9 L5

Daniele Paolone

# Threat Intelligence & IOC

# THREAT INTELLIGENCE

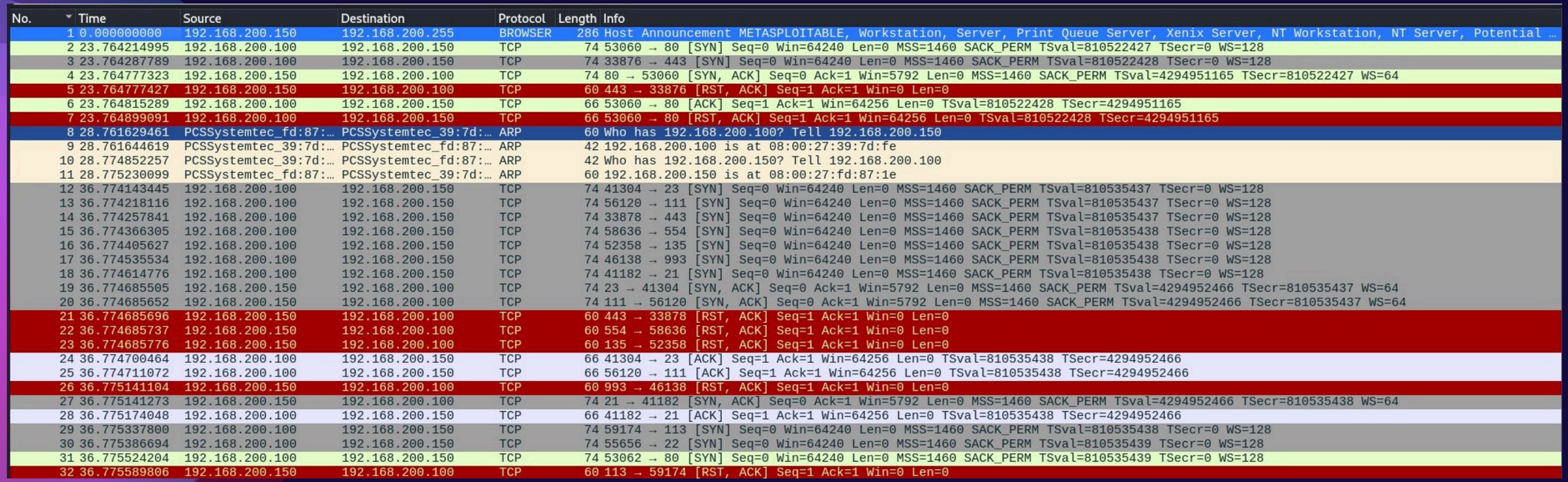
Si basa sulla raccolta, analisi e utilizzo di informazioni relative alle minacce informatiche. L'obiettivo principale è fornire una conoscenza approfondita e contestualizzata delle minacce, permettendo alle organizzazioni di prendere decisioni informate per proteggere i propri asset.

Ed è proprio applicando i metodi e le procedure della Threat Intelligence, che si andrà a svolgere l’ esercizio proposto.

# SVOLGIMENTO ESERCIZIO

L’ immagine seguente rappresenta una cattura di rete effettuata tramite Wireshark. L’ esercizio richiede di:

- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fare delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliare un’azione per ridurre gli impatti dell’attacco attuale ed eventualmente un simile attacco futuro



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 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 … |
| 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 | 23.764287789 | 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=4294951165 TSecr=810522427 WS=64 |
| 5 | 23.764777427 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 443 → 33876 [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 |
| 8 | 28.761629461 | PCSSystemtec_fd:87:… | PCSSystemtec_39:7d:… | ARP | 60 | Who has 192.168.200.100? Tell 192.168.200.150 |
| 9 | 28.761644619 | PCSSystemtec_39:7d:… | PCSSystemtec_fd:87:… | ARP | 42 | 192.168.200.100 is at 08:00:27:39:7d:fe |
| 10 | 28.774852257 | PCSSystemtec_39:7d:… | PCSSystemtec_fd:87:… | ARP | 42 | Who has 192.168.200.150? Tell 192.168.200.100 |
| 11 | 28.775230099 | PCSSystemtec_fd:87:… | PCSSystemtec_39:7d:… | ARP | 60 | 192.168.200.150 is at 08:00:27:fd:87:1e |
| 12 | 36.774143445 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128 |
| 13 | 36.774218116 | 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 | 36.774257841 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128 |
| 15 | 36.774366305 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128 |
| 16 | 36.774405627 | 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 | 36.774535534 | 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 | 36.774614776 | 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 | 36.774685505 | 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 | 36.774685652 | 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 | 36.774685696 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 22 | 36.774685737 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 23 | 36.774685776 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 24 | 36.774700464 | 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 | 36.774711072 | 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 | 36.775141104 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 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 |
| 28 | 36.775174048 | 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 |
| 29 | 36.775337800 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128 |
| 30 | 36.775386694 | 192.168.200.100 | 192.168.200.150 | TCP | 74 | 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128 |
| 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 WS=128 |
| 32 | 36.775589806 | 192.168.200.150 | 192.168.200.100 | TCP | 60 | 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |

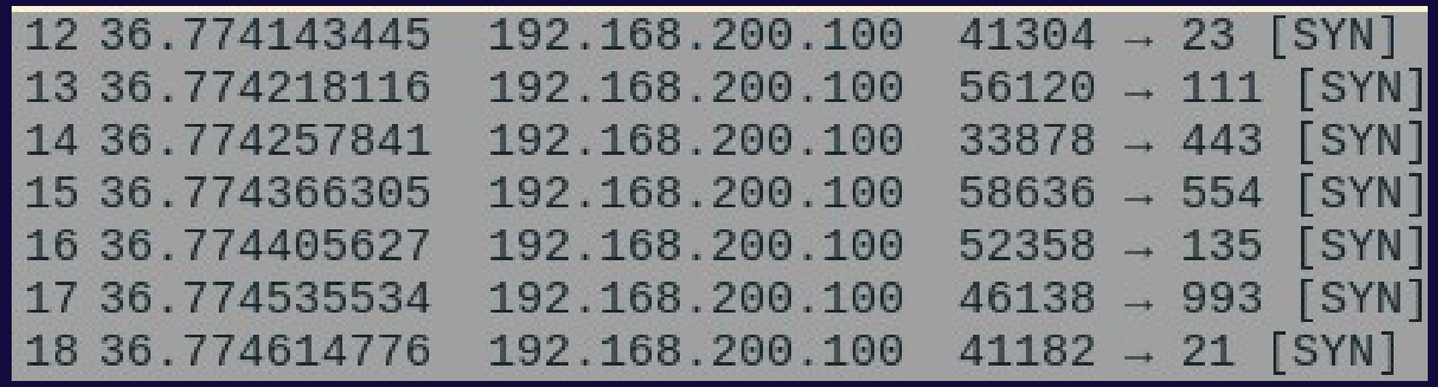
# IOC - INDICATORI DI COMPROMISSIONE

Sono evidenze o tracce che indicano la possibile compromissione di un sistema informatico o di una rete. Rappresentano segnali tangibili che possono essere utilizzati per rilevare attività malevole, indagare incidenti di sicurezza e prevenire ulteriori attacchi.

Nel caso specifico del traffico monitorato tramite Wireshark, un IOC da prendere in considerazione, sono i pacchetti SYN.

# ANALISI

Come si può notare nell' immagine, questi pacchetti sono invitati di continuo dall' indirizzo ip mittente 192.168.200.100, senza mai chiudere il three-way handshake con la ricezione e l' invio di nuovo degli altri pacchetti SYN/ACK e ACK.




Di conseguenza, un altro parametro che può essere preso come IOC, è il tempo stimato in secondi. Tutto ciò avviene in pochissimi istanti.

Queste evidenze possono destare dei sospetti, perchè può essere considerato come un comportamento anomalo.

# VETTORI DI ATTACCO

La presenza di molti tentativi su porte diverse in un breve lasso di tempo potrebbe indicare un'attività di scansione delle porte (port scan), spesso effettuata per individuare servizi attivi o vulnerabilità.

Si può avanzare l’ ipotesi che questa scansione sia stata effettuata tramite Nmap. Inoltre, l’ indirizzo da cui parte la scansione, è interno. Questo sta a significare che l’ attaccante è dentro la rete aziendale.

# MITIGAZIONE

Come prima azione da intraprende, si deve limitare l' operatività di quell' indirizzo ip tramite la configurazione di regole sul firewall. Cioè proibire la possibilità di effettuare quel tipo di scansione o l' invio di quel tipo di pacchetti.

Successivamente, capire se è un' azione volontaria o involontaria. Questo perchè è un indirizzo ip interno. Non si può impedire ad un dipendente di continuare la propria attività, andando a bloccare l'indirizzo ip e tagliarlo fuori dalla rete aziendale. Perciò ci si deve assicurare se sia un vero e proprio attacco o una richiesta accidentale.

Infine, una volta verificata la casistica di appartenenza, si procederà con l'applicazione di una misura definitiva per ripristinare la situazione di normalità