



Federico
Cuccu

Threat Intelligence e analisi IOC con Wireshark

Pratica S9/L5



Obiettivo dell'esercizio

L'obiettivo di questo esercizio è comprendere la natura di un potenziale attacco osservabile dal file .pcapng, un file di Wireshark che ci mostra il log di **tutti gli eventi di connessione TCP** registrati in un determinato lasso di tempo.

Tramite questo file andremo ad:

- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, ipotizzare i vettori di attacco utilizzati

In questo modo possiamo condividere un report di Threat Intelligence per migliorare le difese del sistema aziendale e prevenire / mitigare attacchi futuri simili.

Cos'è la Threat Intelligence

Cos'è la Threat Intelligence

La Threat Intelligence si focalizza sull'**identificazione, analisi e mitigazione delle minacce**, migliorando la capacità delle organizzazioni di rispondere a eventi malevoli.

Nello specifico, è il processo di **raccolta, analisi e condivisione** di informazioni riguardanti minacce attuali o potenziali alla sicurezza informatica.

L'obiettivo della TI è quello di consentire alle organizzazioni di:

- **Comprendere le minacce** che possono colpire l'organizzazione
- Implementare misure di sicurezza proattive per **mitigare i rischi** prima che si concretizzino.
- **Reagire in modo rapido ed efficace** agli incidenti di sicurezza, riducendo l'impatto e accelerando il recupero.

Cattura del traffico TCP tramite Wireshark

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
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=1 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=1 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=1 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	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	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=1 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=1 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=1 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=1 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=1 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=1 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=1 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=1 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=1 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=1 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=1 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=1 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=1 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
33	36.775619454	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
34	36.775652497	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
35	36.775796938	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
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=1 TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	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
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
39	36.775861964	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
40	36.775975876	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

▶ Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0

```

0000  ff ff ff ff ff ff 08 00  27 fd 87 1e 08 00 45 00  .....E.
0010  01 10 00 00 40 00 40 11  26 f6 c0 a8 c8 96 c0 a8  ....@.@.&.....

```

Una parte del log della connessione TCP tra i dispositivi coinvolti, su Wireshark.

Indicatori di compromissione

Indicatori di Compromissione (IOC)

Dall'analisi dei log forniti, emergono diversi indicatori:

1. Elevato numero di pacchetti TCP con flag SYN e RST/ACK:

- Osserviamo molte connessioni interrotte con pacchetti TCP aventi il flag RST (Reset). Questo indica che il server di destinazione sta rispondendo negativamente in modo frequente all'attaccante, chiudendo la connessione.

2. Connessioni incomplete con flag SYN:

- Numerosi pacchetti presentano il flag SYN senza completare il processo di handshake.
- Il pattern può ricordare un SYN Flood, una tecnica comune in attacchi DoS, dove l'aggressore invia una quantità massiva di richieste iniziali (SYN) senza completarle.
- Il pattern può ricordare anche una scansione SYN (stealth), dove l'attaccante scansiona le porte del server senza mai rispondere con un pacchetto ACK.

Indicatori di Compromissione (IOC)

3. Indirizzi IP coinvolti:

- IP sorgente (attaccante): 192.168.200.100 – IP destinazione (vittima): 192.168.200.150
- Entrambi gli indirizzi sono locali, indicando che si tratta di un attacco dall'interno.

4. Porta di destinazione:

- Le porte di destinazione variano continuamente, tra porte note e porte dinamiche, non andando a colpire quindi una porta e un servizio specifico.
- Può indicare una scansione completa con il parametro `-p-` per scansionare tutte le porte da 1 a 65535.

Indicatori di Compromissione (IOC)

5. Presenza di pacchetti ACK

- In un attacco DoS, l'attaccante non dovrebbe rispondere con dei pacchetti ACK, in quanto di norma l'obiettivo è quello di mandare in down il servizio, a meno che non sia parte di un attacco più complesso.
- In una scansione stealth non possono esserci pacchetti ACK, in quanto anche in caso le porte siano aperte, l'attaccante risponde sempre con un pacchetto RST per fare meno "rumore" a livello di rete.

tcp.flags.ack == 1 && tcp.flags.syn == 0 && tcp.flags.reset == 0									
No.	Time	Source	Destination	Protocol	Length	Info			
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	
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	
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	
37	36.775803786	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	
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	
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66	33042 → 445	[ACK]	Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466	
66	36.776941020	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	36.776962320	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	36.776983878	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	
165	36.781512468	192.168.200.100	192.168.200.150	TCP	66	45648 → 512	[ACK]	Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466	
268	36.788833247	192.168.200.100	192.168.200.150	TCP	66	51396 → 514	[ACK]	Seq=1 Ack=1 Win=64256 Len=0 TSval=810535452 TSecr=4294952467	
997	36.825733008	192.168.200.100	192.168.200.150	TCP	66	42048 → 513	[ACK]	Seq=1 Ack=1 Win=64256 Len=0 TSval=810535489 TSecr=4294952471	

Indicatori di Compromissione (IOC)

5. Connessioni non permanenti

- Ogni connessione viene chiusa poco dopo con un pacchetto RST, di conseguenza l'attaccante non esegue mai accesso a dei servizi aperti (come ftp o telnet).
- In caso di connessione permanente, ad esempio sulla porta ftp, avremo notato diversi pacchetti tutti inviati/ricevuti sulla stessa porta, dimostrando dunque che l'attaccante sta eseguendo diverse azioni su quel servizio.

6. Protocollo ARP

- Oltre all'indirizzo IP privato, abbiamo la doppia conferma che l'attaccante è all'interno della rete in quanto il protocollo ARP agisce tra il livello 2 e il livello 3 del modello ISO/OSI e associa IP e indirizzi Mac, che vengono utilizzati solamente all'interno della rete locale. Non sono presenti tracce di ARP poisoning.

Ipotesi sui vettori di attacco

Vettore di attacco

Basandosi sugli IOC rilevati, l'attacco osservato non è un vero e proprio attacco, bensì una **scansione non stealth mirata sul dispositivo vittima**.

L'attaccante ha utilizzato una scansione come questa: `nmap -sT -p-`, che sfrutta interamente il three-way handshake previsto dal protocollo TCP.

Questo tipo di scansione, completa la connessione TCP (SYN, SYN/ACK, ACK) con ogni porta aperta, rendendola facilmente rilevabile nei log.

Per quanto riguarda le porte chiuse, invece, il server invierà un pacchetto RST come risposta subito dopo il SYN.

Vettore di attacco

Inoltre con il parametro **-p-** l'attaccante scansiona tutte le porte, da 1 a 65535, anziché solo le porte note, risultando in una scansione più aggressiva.

È importante sottolineare anche la **quantità di pacchetti** tra il dispositivo attaccante e il dispositivo vittima, ovvero nella norma in una scansione di questo tipo, e di gran lunga inferiore a quello che sarebbe stato un ipotetico attacco DoS.

È comunque un **atteggiamento sospetto**, dato che la scansione è un prerequisito fondamentale che precede la fase di attacco.

Sono necessarie dunque maggiori indagini sull'avvenimento, insieme a delle limitazioni per mitigare questa possibile minaccia.

Azioni di mitigazione

Azioni di mitigazione

Per gestire efficacemente la scansione rilevata, è essenziale adottare contromisure che limitino l'azione dell'attaccante senza interferire con le normali attività lavorative.

1. Miglioramento delle regole del firewall:

- La configurazione del firewall è fondamentale: è possibile limitare la frequenza delle richieste TCP, oppure bloccare le richieste sulle porte a cui il dispositivo non può avere accesso.

2. Isolamento logico:

- Se la rete è suddivisa in VLAN, si può inserire il dispositivo sospetto in una VLAN dedicata con regole di accesso più restrittive, permettendo solo l'accesso ai servizi necessari per il suo ruolo, fino al termine dell'indagine.

Azioni di mitigazione

3. Installazione di dispositivi di rilevamento delle intrusioni:

- Sebbene non prevenga direttamente una scansione come quella rilevata, un IDS può analizzare i pacchetti nel traffico e confrontarli con un database alla ricerca di attività malevola, lanciando l'allarme.
- L'IPS, oltre a lanciare l'allarme, blocca in autonomia il traffico malevolo, ma potrebbe ridurre l'accessibilità al sistema e bloccare il lavoro di uno o più dipendenti temporaneamente.

4. Formazione del personale:

- Sensibilizzare il personale sull'uso improprio degli strumenti di rete, spiegando le possibili conseguenze di attività come scansioni o altre attività di rete non autorizzate.

Azioni di mitigazione

5. Verifica del dispositivo:

- Analizzare il dispositivo in questione per verificare la presenza di software o strumenti potenzialmente pericolosi.
- Analizzare i log presenti sul dispositivo utilizzato per la scansione per ricercare ulteriori indizi sulle eventuali intenzioni dell'attaccante.

Conclusioni

Conclusioni

L'analisi del traffico ha rivelato una scansione non stealth mirata. L'attività, proveniente da un dispositivo interno, indica un **intento esplorativo sospetto**, ma non ha compromesso servizi o iniettato pacchetti malevoli.

Le azioni di mitigazione mirano a migliorare le regole del firewall, isolare il dispositivo sospetto, utilizzare strumenti di rilevamento delle intrusioni e sensibilizzare il personale sull'uso appropriato delle risorse di rete.

L'evento sottolinea l'importanza di **monitorare e rispondere prontamente** ai comportamenti anomali, bilanciando la sicurezza con la continuità operativa. Sarà essenziale indagare ulteriormente le motivazioni del responsabile per prevenire futuri incidenti.