

CS0424IT — ESERCITAZIONE S9L3
THREAT INTELLIGENCE & INDICATORS OF COMPROMISE (IOC)

Simone La Porta



24 luglio 2024

1 TRACCIA

Durante la lezione teorica, abbiamo esaminato la Threat Intelligence e gli Indicators of Compromise (IoC). Abbiamo visto che gli IoC sono evidenze o eventi di un attacco in corso, oppure già avvenuto. Per l'esercizio pratico di oggi, è stata fornita una cattura di rete effettuata con Wireshark.

Questo report analizza tale cattura e risponde ai seguenti quesiti:

- Identificare eventuali IoC, ovvero evidenze di attacchi in corso.
- Ipotesi sui potenziali vettori di attacco utilizzati in base agli IoC trovati.
- Consigli su azioni per ridurre gli impatti dell'attacco.

2 SVOLGIMENTO

2.1 Identificazione degli IoC

Aprendo il file .pcapng in Wireshark si possono osservare i pacchetti inviati (con il flag SYN) e i pacchetti ricevuti (con il flag ACK).

Analizzando il traffico catturato, si rileva subito la presenza di soli due host: 192.168.200.100 e 192.168.200.150. Continuando l'analisi, si osserva una grande quantità di richieste SYN provenienti dall'host 192.168.200.100 verso 192.168.200.150. È interessante notare che queste richieste vengono inviate ogni volta su una porta diversa, il che indica chiaramente che non si tratta di un normale tentativo di connessione, ma è molto probabile che questo host stia eseguendo una scansione per individuare vulnerabilità, servizi attivi o porte aperte da sfruttare.

L'host 192.168.200.150, invece, risponde alle richieste con un messaggio di tipo [RST, ACK] se la porta è chiusa, [SYN, ACK] se la porta è aperta.

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-08-09	192.168.200.100	192.168.200.150	BROW.	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
2	2022-08-09	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	2022-08-09	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	2022-08-09	192.168.200.100	192.168.200.150	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	2022-08-09	192.168.200.150	192.168.200.100	TCP	60	443 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	2022-08-09	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	2022-08-09	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	2022-08-09	PCSSystemtec_f...	PCSSystemtec_f...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	2022-08-09	PCSSystemtec_f...	PCSSystemtec_f...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	2022-08-09	PCSSystemtec_f...	PCSSystemtec_f...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	2022-08-09	PCSSystemtec_f...	PCSSystemtec_f...	ARP	60	192.168.200.150 is at 08:00:27:39:7d:fe
12	2022-08-09	192.168.200.100	192.168.200.150	TCP	74	41384 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	2022-08-09	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	2022-08-09	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	2022-08-09	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	2022-08-09	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	2022-08-09	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	2022-08-09	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	2022-08-09	192.168.200.100	192.168.200.150	TCP	74	23 → 41384 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	2022-08-09	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	2022-08-09	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	2022-08-09	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	2022-08-09	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	2022-08-09	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	2022-08-09	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	2022-08-09	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	2022-08-09	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	2022-08-09	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	2022-08-09	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	2022-08-09	192.168.200.100	192.168.200.150	TCP	74	56566 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	2022-08-09	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	2022-08-09	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	2022-08-09	192.168.200.100	192.168.200.150	TCP	66	41384 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	2022-08-09	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	2022-08-09	192.168.200.150	192.168.200.100	TCP	74	22 → 56566 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	2022-08-09	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=810535439 WS=64
37	2022-08-09	192.168.200.100	192.168.200.150	TCP	66	56566 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	2022-08-09	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	2022-08-09	192.168.200.150	192.168.200.100	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	2022-08-09	192.168.200.100	192.168.200.150	TCP	66	56566 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	2022-08-09	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	2022-08-09	192.168.200.100	192.168.200.150	TCP	74	50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43	2022-08-09	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44	2022-08-09	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	2022-08-09	192.168.200.100	192.168.200.150	TCP	74	33842 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	2022-08-09	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
47	2022-08-09	192.168.200.150	192.168.200.100	TCP	60	199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	2022-08-09	192.168.200.100	192.168.200.150	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	2022-08-09	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
50	2022-08-09	192.168.200.100	192.168.200.150	TCP	74	33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128

Figura 1: Pacchetti inviati/ricevuti

2.2 Ipotesi sui potenziali vettori di attacco

2.2.1 Port Scanning

La presenza di numerosi pacchetti SYN e RST/ACK suggerisce che un port scanning potrebbe essere in corso. Un aggressore potrebbe cercare di identificare porte aperte sull'host 192.168.200.150.

2.2.2 TCP Reset Attack

I numerosi pacchetti RST/ACK possono indicare un attacco TCP reset. Questo tipo di attacco è utilizzato per interrompere le connessioni TCP legittime tra host.

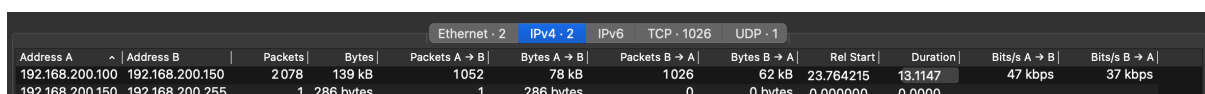
2.2.3 Tentativi di connessione illegittimi

Potrebbero esserci tentativi di brute-force o altri tipi di attacchi di connessione da parte dell'IP 192.168.200.100 verso l'IP 192.168.200.150.

3 STRUMENTI E COMANDI UTILIZZATI PER L'ANALISI

3.1 Wireshark

Per ottenere una panoramica dettagliata degli indirizzi IP coinvolti nello scambio di pacchetti registrato in un file .pcapng, basta cliccare su **Statistics > Conversations** e selezionare IPv4 per vedere gli indirizzi IP coinvolti nella conversazione, il numero totale di pacchetti scambiati, il numero di pacchetti inviati da un IP all'altro e viceversa ed anche la loro dimensione.



Ethernet - 2 IPv4 - 2 IPv6 TCP - 1026 UDP - 1											
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.200.100	192.168.200.150	2078	139 kB	1052	78 kB	1026	62 kB	23.764215	13.1147	47 kbps	37 kbps
192.168.200.150	192.168.200.255	1	286 bytes	1	286 bytes	0	0 bytes	0.000000	0.0000		

Figura 2: Statistics → Conversations

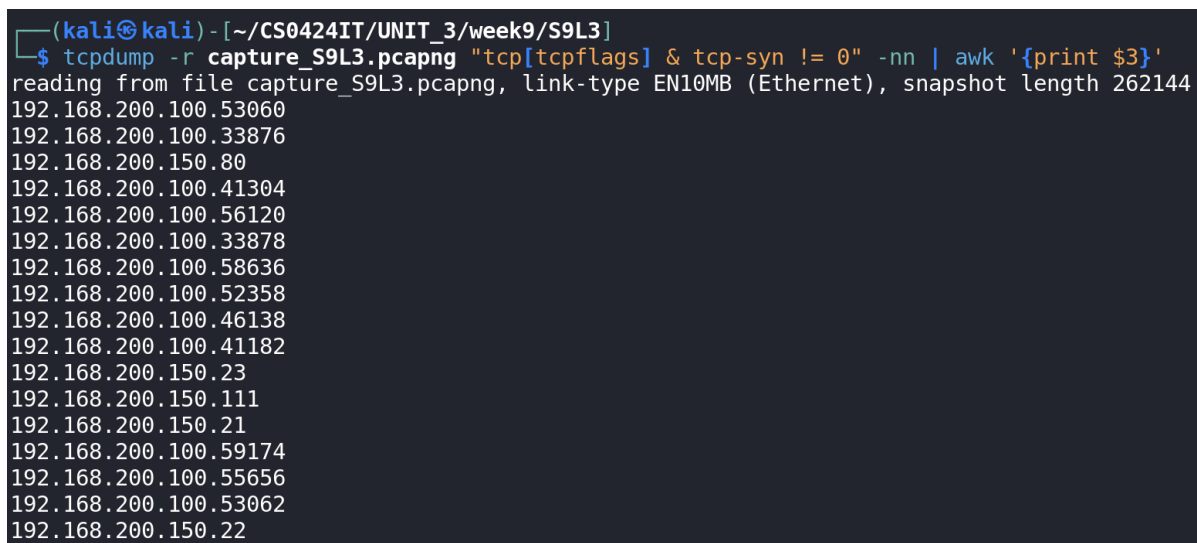
3.2 TCPDump

TCPDump è uno strumento molto pratico per analizzare i file .pcapng e può essere utilizzato da riga di comando. Per contare i pacchetti inviati con i flag SYN-ACK e RST-ACK e determinare quanti corrispondono a porte aperte e chiuse, possiamo utilizzare tcpdump e analizzare i flag dei pacchetti TCP. Ricordiamo che i pacchetti SYN-ACK indicano una porta aperta, mentre RTS-ACK una porta chiusa.

Per questa analisi, ho utilizzato i seguenti comandi:

- Legge il file .pcapng e filtra i pacchetti TCP con il flag SYN impostato, mostrando solamente gli indirizzi IP e le porte senza risolvere i nomi:

```
tcpdump -r file.pcapng "tcp[tcpflags] & tcp-syn != 0" -nn | awk "{print $3}"
```



```
(kali@kali)-[~/CS0424IT/UNIT_3/week9/S9L3]
$ tcpdump -r capture_S9L3.pcapng "tcp[tcpflags] & tcp-syn != 0" -nn | awk '{print $3}'
reading from file capture_S9L3.pcapng, link-type EN10MB (Ethernet), snapshot length 262144
192.168.200.100.53060
192.168.200.100.33876
192.168.200.150.80
192.168.200.100.41304
192.168.200.100.56120
192.168.200.100.33878
192.168.200.100.58636
192.168.200.100.52358
192.168.200.100.46138
192.168.200.100.41182
192.168.200.150.23
192.168.200.150.111
192.168.200.150.21
192.168.200.100.59174
192.168.200.100.55656
192.168.200.100.53062
192.168.200.150.22
```

Figura 3: TCPDump: filtro per pacchetti TCP con flag SYN

- Legge il file .pcapng e conta i pacchetti TCP con il flag SYN-ACK o RST-ACK impostato:

```
tcpdump -r file.pcapng "tcp[tcpflags] == (tcp-rst|tcp-ack)" --count
```

```
tcpdump -r file.pcapng "tcp[tcpflags] == (tcp-syn|tcp-ack)" --count
```

```
(kali㉿kali)-[~/CS0424IT/UNIT_3/week9/S9L3]
$ tcpdump -r capture_S9L3.pcapng "tcp[tcpflags] == (tcp-rst|tcp-ack)" --count
reading from file capture_S9L3.pcapng, link-type EN10MB (Ethernet), snapshot length 262144
1026 packets

(kali㉿kali)-[~/CS0424IT/UNIT_3/week9/S9L3]
$ tcpdump -r capture_S9L3.pcapng "tcp[tcpflags] == (tcp-syn|tcp-ack)" --count
reading from file capture_S9L3.pcapng, link-type EN10MB (Ethernet), snapshot length 262144
13 packets
```

Figura 4: TCPDump: conteggio pacchetti inviati TCP RTS-ACK e SYN-ACK

4 AZIONI DI MITIGAZIONE RACCOMANDATE

Per proteggersi efficacemente dalle scansioni delle porte in una rete informatica, è essenziale adottare misure preventive robuste per mantenere l'integrità e la sicurezza della rete. Di seguito sono elencate alcune azioni preventive specifiche:

- **Configurazione di regole di sicurezza:** Impostare regole di sicurezza stringenti sui dispositivi di rete come router, switch e firewall per limitare l'accesso solo alle porte e ai servizi necessari. L'uso di ACL (Access Control Lists) e altre tecniche di filtraggio consente di permettere solo il traffico autorizzato.
- **Monitoraggio del traffico interno:** Utilizzare strumenti di monitoraggio per analizzare il traffico di rete e rilevare attività sospette o non autorizzate, incluse le scansioni delle porte. Il monitoraggio interno aiuta a identificare rapidamente comportamenti anomali e a rispondere prontamente.
- **Segmentazione della rete:** Suddividere la rete in segmenti distinti per ridurre il traffico tra le diverse sezioni. Questo approccio limita la capacità di un dispositivo compromesso di esplorare o danneggiare altri segmenti della rete.
- **Politiche di autenticazione avanzate:** Implementare politiche di autenticazione robuste, come l'autenticazione a due fattori, per proteggere l'accesso ai dispositivi di rete e alle risorse sensibili.
- **Aggiornamenti frequenti:** Garantire che tutti i dispositivi di rete e il firmware siano regolarmente aggiornati con le ultime patch di sicurezza, per correggere le vulnerabilità note che potrebbero essere sfruttate durante una scansione delle porte o altri tipi di attacchi.

5 CONCLUSIONI

La Threat Intelligence e gli Indicatori di Compromissione (IoC) sono componenti fondamentali della strategia di sicurezza informatica moderna. La Threat Intelligence fornisce informazioni preziose sulle minacce attuali e potenziali, permettendo alle organizzazioni di anticipare, identificare e rispondere efficacemente agli attacchi. Gli IoC, d'altra parte, sono strumenti critici per rilevare e mitigare compromissioni, fornendo segnali specifici che indicano attività dannose all'interno della rete.

L'integrazione di Threat Intelligence e IoC nel framework di sicurezza consente una difesa proattiva e reattiva. La Threat Intelligence aiuta a comprendere il contesto delle minacce e a prendere decisioni informate, mentre gli IoC permettono una risposta rapida e precisa agli incidenti, limitando i danni e prevenendo future violazioni.

In un panorama di minacce in continua evoluzione, l'adozione di un approccio basato su Threat Intelligence e IoC è indispensabile. Questi strumenti non solo migliorano la visibilità e la consapevolezza delle minacce, ma rafforzano anche la capacità di difesa delle organizzazioni, proteggendo le risorse critiche e mantenendo la fiducia delle parti interessate.