

# PROGETTO SETTIMANA 9.

Per l'esercizio pratico di oggi, in allegato avremo una cattura di rete effettuata con Wireshark.

Obiettivi:

1. Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso.
2. In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati.
3. Consigliare un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.

Il file in questione è:

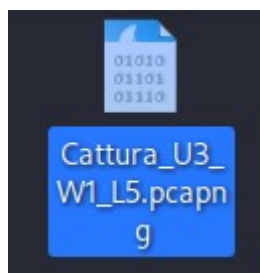
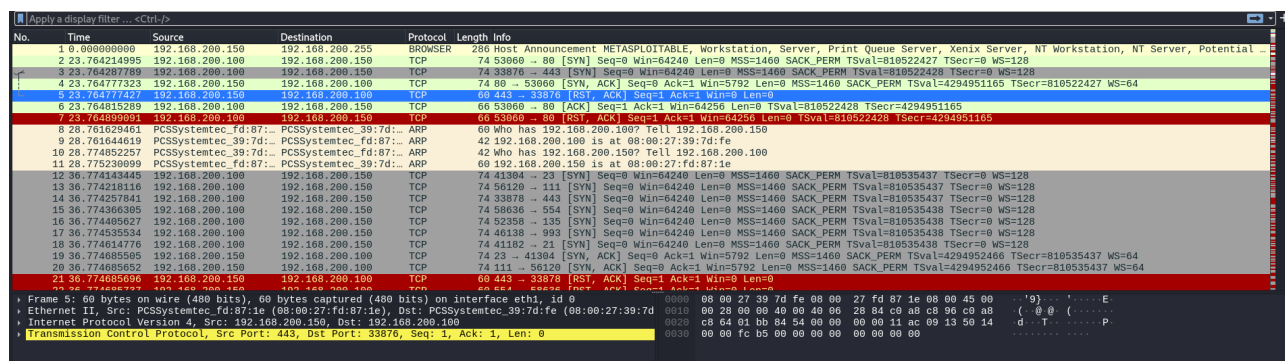


Fig.1

## 1. Identificazione e analisi degli IOC.

L'analisi del traffico di rete tramite Wireshark ha evidenziato un'attività anomala caratterizzata da intenso traffico TCP tra l'host sorgente con IP 192.168.200.150 e target con IP 192.168.200.100 (Fig.2).



No.	Time	Source	Destination	Protocol	Length	Info
10	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	3.764214995	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	3.764297789	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	60	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899991	192.168.200.100	192.168.200.150	TCP	60	80 → 53060 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PCSSystemtec_39:7d:...	PCSSystemtec_39:7d:...	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:...	PCSSystemtec_39:7d:...	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:...	PCSSystemtec_39:7d:...	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230809	PCSSystemtec_39:7d:...	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	50120 → 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	36.774366385	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	40138 → 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	36.774685595	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 → 50120 [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

Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth1, id 0  
Ethernet II, Src: PCSSystemtec\_fd:87:1e (08:00:27:fd:87:1e), Dst: PCSSystemtec\_39:7d:fe (08:00:27:39:7d:fe)  
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100  
Transmission Control Protocol, Src Port: 443, Dst Port: 33876, Seq: 1, Ack: 1, Len: 0

Fig.2

Si evince appunto un elevato numero di connessioni TCP in tempi molto ravvicinati sulle porte che superano la numero 60000 utilizzate tipicamente per Port Scanning o Backdoor ma le connessioni terminano bruscamente con il flag “RST, ACK”. Questi flag, a primo impatto, sono appunto il segnale di un Port scanning aggressivo con tentativi continui falliti che vengono confermati dai svariati pacchetti SYN-ACK assenti dove l’handshake non viene concluso. (Fig.3)

No.	Time	Source	Destination	Protocol	Length	Info
		Source Address: 192.168.200.150 Destination Address: 192.168.200.100 [Stream index: 1]				
▼		Transmission Control Protocol, Src Port: 765, Dst Port: 60588, Seq: 1, Ack: 1, Len: 0				
		Source Port: 765 Destination Port: 60588 [Stream index: 936] [Stream Packet Number: 2]				
		▼ [Conversation completeness: Incomplete (37)]				
		..1. .... = RST: Present ...0 .... = FIN: Absent .... 0... = Data: Absent .... .1.. = ACK: Present .... ..0. = SYN-ACK: Absent .... ...1 = SYN: Present [Completeness Flags: R..A.S]				
		[TCP Segment Len: 0] Sequence Number: 1 (relative sequence number) Sequence Number (raw): 0 [Next Sequence Number: 1 (relative sequence number)] Acknowledgment Number: 1 (relative ack number) Acknowledgment number (raw): 3446022271 0101 .... = Header Length: 20 bytes (5)				
		▼ Flags: 0x014 (RST, ACK)				
		000. .... = Reserved: Not set ...0 .... = Accurate ECN: Not set .... 0... = Congestion Window Reduced: Not set .... .0.. = ECN-Echo: Not set .... ..0. = Urgent: Not set .... ...1 = Acknowledgment: Set .... ....0... = Push: Not set				
		▼ .... ..1.. = Reset: Set				
		▶ [Expert Info (Warning/Sequence): Connection reset (RST)]				
		.... ....0... = Syn: Not set .... ....0... = Fin: Not set [TCP Flags: .....A.R..] Window: 0 [Calculated window size: 0] [Window size scaling factor: -1 (unknown)] Checksum: 0xbff4 [unverified] [Checksum Status: Unverified] Urgent Pointer: 0 ▶ [Timestamps] ▶ [SEQ/ACK analysis]				

Fig.3

## 2. Ipotesi sui vettori utilizzati.

Basandoci quindi sulle informazioni ottenute fin'ora dagli IOC, possiamo ipotizzare 4 tipi d'attacco utilizzati:

- **Port Scanning**: l'host cerca di stabilire una connessione inviando vari pacchetti di dati a diverse porte dell'IP del target per determinare quali servizi sono in esecuzione e accessibili per poi sfruttarle, infatti l'invio massivo di SYN lo conferma. Qui un vettore che può essere utilizzato è <nmap> o <telnet> o <nc> o ancora <metasploit>;
- **DoS (Denial of Service)**: l'host cerca di sovraccaricare il target con un traffico eccessivo allo scopo di rendere il sistema indisponibile all'utente causando crash o malfunzionamenti generali del sistema come ad esempio un semplice rallentamento delle risorse. Qui un vettore che può essere utilizzato è <Nping>;
- **Lateral Movement**: l'host si muove attraverso la rete compromessa del target cercando di accedere ai sistemi all'interno della rete ad esempio per scalare privilegi. Qui un vettore che può essere utilizzato è l'accesso tramite SHELL o PowerShell;
- **Brute Force**: l'host tenta sistematicamente di forzare credenziali sui servizi esposti (come ad esempio SSH). Qui un vettore che può essere utilizzato è <Hydra> o <Medusa>.

Potremmo scartare le ultime 3 ipotesi in quanto:

- DoS: il volume del traffico, anche se elevato, non mostra una saturazione costante sulle prestazioni di rete o del sistema e i pacchetti mirano a porte diverse;
- Lateral Movement: sono visibili solo un host e un solo target senza coinvolgere nuovi sistemi, quindi abbiamo un traffico che si limita solo in un'unica direzione;
- Brute Force: non sono presenti ripetute connessioni verso la stessa porta o nuovi tentativi di autenticazione, quindi manca il pattern tipico di un attacco tramite SSH.

L'analisi conferma un attacco di Port Scanning in quanto:

- Il traffico si indirizza verso una nuova porta diversa ogni volta che la precedente non presenta una risposta SYN-ACK (**Fig.4**);
- Le porte di destinazione dell'attacco sono elevate (superano le 60000 come visto prima);
- I pacchetti sono inviati in blocco e non in modo caotico o intenso e le tempistiche di risposta indica che il sistema non è sotto stress.

```
▼ Transmission Control Protocol, Src Port: 443, Dst P
Source Port: 443
Destination Port: 33878
[Stream index: 4]
[Stream Packet Number: 2]
▼ [Conversation completeness: Incomplete (37)]
  ..1. .... = RST: Present
  ...0 .... = FIN: Absent
  .... 0... = Data: Absent
  .... .1.. = ACK: Present
  .... ..0. = SYN-ACK: Absent
  .... ...1 = SYN: Present
[Completeness Flags: R..A..S]
```

Fig.4

### 3. Azioni consigliati per ridurre l'impatto di questo attacco.

Una delle azioni da svolgere immediatamente di sicuro è quella di isolare il target, bloccando poi il traffico aggiungendo nuove regole nel Firewall specifiche per l'IP dell'attaccante e continuare a monitorare l'intera rete per rilevare attività simili future.

Si passa poi a disattivare eventuali servizi non necessari e “chiudere” queste porte definitivamente, monitorare più costantemente gli eventi con sistemi SIEM e infine applicare sul sistema il Least Privilege (ovvero impostare privilegi minimi a utenti, applicazioni, database e rete riducendo il più possibile potenziali danni in caso di compromissione).

## CONCLUSIONE.

L'analisi mostra un tentativo d'attacco neutralizzato in quanto sono già presenti ottime contromisure quali un Firewall configurato correttamente, porte non necessarie chiuse e infine una risposta immediata alle sollecitazioni anomale senza degradazione dei servizi.

Questo attacco conferma l'importanza di un approccio alla sicurezza su più livelli e della necessità di mantenere una sorveglianza attiva per identificare tempestivamente future minacce simili e non.