

### Esercizio per il progetto settimanale Unit 3 - S9 - L5

Data una cattura di rete effettuata con **Wireshark**. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare ed analizzare 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 attuale ed eventualmente un simile attacco futuro



### Threat Intelligence (TI)

La **Threat Intelligence (TI)** è la **raccolta**, **l'analisi** e la condivisione di **informazioni** su minacce attuali e potenziali alla sicurezza informatica. Queste informazioni provengono da diverse fonti e includono **dettagli** sui cyber attacchi, sulle **vulnerabilità** dei sistemi, sulle tattiche degli attaccanti e sugli indicatori di compromissione (IoC).

### Indicatori di Compromissione (IoC)

**Gli Indicatori di Compromissione (IoC)** sono **segnali** specifici che indicano che un sistema o una rete è stata **compromessa** da un attacco informatico. Tra i principali tipi di IoC si trovano indirizzi IP e **domini malevoli**, hash di file sospetti, **processi anomali** e modifiche non autorizzate ai file. Questi indicatori sono essenziali per la sicurezza informatica, poiché aiutano a **rilevare** le minacce, a guidare le azioni di **risposta** agli incidenti e a **prevenire** attacchi futuri attraverso l'uso di liste di controllo aggiornate.



La traccia di rete mostra un **attacco** in corso dove l'attaccante (192.168.200.100) sta eseguendo un attacco **brute-force** (data la ripetizione) contro un server (192.168.200.150), identificato come una macchina Metasploitable.

Oltre ad un attacco brute-force la traccia mostra la sequenza di pacchetti con flag **SYN, ACK e RST, ACK**, questo è il comportamento tipico di una **scansione di porte** automatizzata, in cui un attaccante cerca di identificare quali porte sono **aperte** su un host bersaglio.

I pacchetti inviati al server Metasploitable mirano a ottenere accesso **non autorizzato** al sistema.

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 Se
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53908 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81052
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=8105
4	23.764777323	192.168.200.100	192.168.200.150	TCP	74	80 -> 53908 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM T
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	53908 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=42
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53908 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSe
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	28.775230899	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=81053
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=8105
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=8105
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=8105
16	36.774495627	192.168.200.100	192.168.200.150	TCP	74	52358 -> 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8105
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=8105
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=81053
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 T
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

Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0  
Ethernet II, Src: PCSSystemtec\_fd:87:1e (08:00:27:fd:87:1e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255  
User Datagram Protocol, Src Port: 138, Dst Port: 138  
NetBIOS Datagram Service  
SMB (Server Message Block Protocol)  
SMB MailSlot Protocol  
Microsoft Windows Browser Protocol



La stringa TCP 66 53908 -> 80 mostra che l'attaccante sta tentando di **scansionare** le porte aperte sul server Metasploitable per trovare una vulnerabilità.

Il traffico mostra numerosi tentativi di connessione, in particolare verso la **porta 445**, che è la porta standard del protocollo Server Message Block (**SMB**). Ciò indica che l'attaccante ha identificato il servizio SMB come un potenziale punto debole mirando l'attacco brute-force nel sfruttare una potenziale **vulnerabilità** in questo servizio.

Il protocollo **SMB** (Server Message Block) usato per la condivisione di file è spesso preso di mira negli attacchi brute-force per tentare di accedere a cartelle condivise o altri servizi. Molti attacchi di malware e **ransomware** (come WannaCry) hanno sfruttato in passato vulnerabilità in SMB.



### Dettagli sull'attacco:

L'attaccante ha iniziato una scansione di porte per capire quali servizi sono attivi sul server 192.168.200.255. Troviamo pacchetti con i flag SYN inviati a diverse porte, come la porta 80 (HTTP) e la porta 445 (SMB). La scansione della porta 80, è un tentativo per capire se c'è un server web in esecuzione.

La scansione della porta 445 e il traffico SMB che abbiamo visto successivamente indicano che l'attaccante ha identificato il servizio SMB come un potenziale **punto debole**.

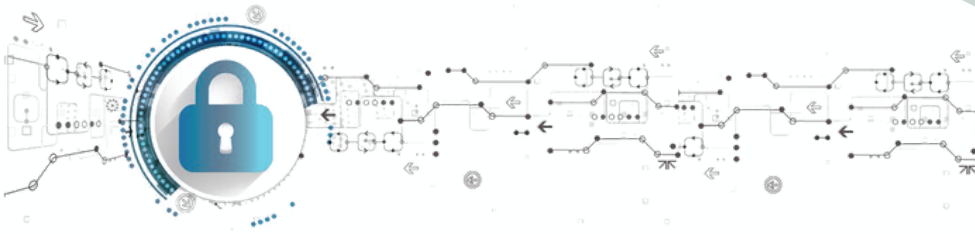
Il pacchetto **RST** viene usato per interrompere una connessione in modo anomalo. Se l'attaccante sta eseguendo una scansione stealth (-sS), dopo aver ricevuto un SYN, ACK dal server, invia un RST per chiudere la connessione prima che sia completamente stabilita. L'obiettivo è sondare una porta aperta senza lasciare tracce nei log del server. In questo caso, l'attaccante ha ottenuto le informazioni che cercava e non ha bisogno di continuare la connessione.

Per esempio nella port 80 dopo la scansione full connect (-sT) usa RST per chiudere immediatamente la connessione che ha appena stabilito. Questo è un modo per minimizzare il tempo di connessione e nascondere la sua attività.

No.	Time	Source	Destination	Protocol	Length	Info
19	36.774685565	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=42949
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=4294
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=42949
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

No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=0 Len=0
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=1 Ack=0 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=0 Win=0 Len=0
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=0 Win=0 Len=0

Per un attacco di successo era necessaria la mancanza di RST così che dopo la risposta con un pacchetto ACK per completare l'handshake a tre vie (three-way handshake) si sarebbe stabilita la connessione e l'attaccante avrebbe iniziato a scambiare dati con il server. Questo poteva includere l'invio di comandi, il download di dati sensibili o l'upload di **malware**.



## Vettori di attacco



- **Attacco di forza bruta (brute-force):** La serie di tentativi di connessione falliti indica un attacco di forza bruta.
- **Sfruttamento di vulnerabilità:** L'attaccante sta tentando di sfruttare una vulnerabilità nel protocollo SMB per ottenere l'accesso non autorizzato al server.
- **Scansione di porta:** L'attaccante sta cercando una porta aperta per penetrare nel sistema.



## Azioni di prevenzione



- **Bloccare** l'indirizzo IP dell'attaccante sul firewall per interrompere immediatamente la scansione e l'attacco.
- **Isolare** il server compromesso dalla rete per evitare che possa essere usato come punto di partenza per ulteriori attacchi.
- **Applicare patch di sicurezza:** Verificare che il sistema operativo e i servizi esposti (in questo caso, SMB) siano completamente aggiornati con le ultime patch di sicurezza per correggere eventuali vulnerabilità note.
- **Configurare un firewall:** Impostare regole sul firewall per limitare il traffico in entrata solo alle porte e agli indirizzi IP necessari, bloccando tutto il resto.
- **Implementare un IPS:** Utilizzare un Intrusion Prevention System (IPS) per rilevare e bloccare automaticamente comportamenti sospetti come le scansioni di porte. In aggiunta implementare un **EDR o XDR** per rilevare e rispondere a minacce che bypassano l'IPS.