U3W1L5 – Progetto Settimanale

Analisi Traffico di Rete (Wireshark)

Autore: Elena Pagnacco

Identificazione del Reperto

Dati del Reperto (Chain of Custody)

Al fine di garantire l'integrità dell'analisi, è stata calcolata l'impronta digitale del file di cattura originale.

- **Nome File:** Cattura_U3_W1_L3
- **Hash SHA256:** 9a922718bd0f88433ad58ab82f2e40e50ae0413e3dfbb04a20dc38a0e5c7e7e9
- **Dimensione:** 205K

Sintesi

Il presente documento riporta **l'analisi forense** di un file di cattura di rete **(.pcapng)** volto a identificare attività anomale all'interno del perimetro locale. L'analisi ha permesso di isolare e confermare un'attività di ***Network Scanning*** massiva (***Port Scan***) condotta da un host interno verso un server target. L'attaccante ha utilizzato tecniche automatizzate per mappare i servizi esposti, rivelando numerose criticità su protocolli non sicuri (Telnet, FTP, SMB). L'analisi dei protocolli di livello 2 (ARP) ha inoltre permesso di identificare la natura virtualizzata dell'ambiente di test (Oracle VirtualBox).

Scopo del test e analisi dello scenario

Scenario e Obiettivi

L'attività si svolge in un ambiente di laboratorio virtuale su sottorete 192.168.200.0/24. L'obiettivo è analizzare i log di rete per identificare gli **Indicatori di Compromissione (IOC)**, ricostruire la catena degli eventi e proporre azioni di mitigazione.

- **Attacker:** 192.168.200.100 (Macchina che origina le connessioni).
- **Target:** 192.168.200.150 (Hostname: ***METASPLOITABLE***).
- **Contesto:** Entrambe le macchine operano in ambiente virtuale, come evidenziato dai **MAC Address OUI** 08:00:27 (PCS Systemtechnik / VirtualBox).

Cronologia Temporale

L'analisi temporale dei pacchetti ha permesso di delimitare la finestra temporale dell'attività sospetta:

- **Inizio attività:** 2022-08-09 05:58:59.893817491 – Earliest packet time
- **Fine attività:** 2022-08-09 05:59:36.772714239 – Last packet time
- **Durata complessiva:** 36.878896748 seconds

Analisi Tecnica

1. Identificazione del Volume di Traffico

In prima analisi, è stata verificata la statistica delle conversazioni per isolare gli host maggiormente attivi. È emerso uno scambio asimmetrico di pacchetti tra l'IP .100 e l'IP .150, indicativo di un'attività di scansione automatizzata.

Ethernet · 2 | IPv4 · 2 | IPv6 | TCP · 1026 | UDP · 1

Address A	Address B	Packets	Bytes	Stream ID	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	2,078	139 kB	1	1,052	78 kB	1,026	62 kB	23.764214995	13.114682	47 kbps	37 kbps
192.168.200.150	192.168.200.255	1	286 bytes	0	1	286 bytes	0	0 bytes	0.000000000	0.000000		

Figura 1 Panoramica delle conversazioni IPv4: evidenziato l'alto volume di traffico tra attaccante e vittima.

2. Analisi del Vettore di Attacco (TCP Connect Scan)

Al fine di isolare univocamente i tentativi di connessione generati dall'attaccante, è stato applicato il seguente filtro di visualizzazione:

```
tcp.flags.syn == 1 and tcp.flags.ack == 0
```

Il filtro è stato progettato per isolare la **fase iniziale del Three-Way Handshake TCP**.

- Il parametro `tcp.flags.syn == 1` seleziona i pacchetti di richiesta sincronizzazione (SYN), utilizzati per avviare una nuova sessione.
- La condizione `tcp.flags.ack == 0` esclude le risposte provenienti dal target (pacchetti SYN-ACK), permettendo di visualizzare esclusivamente il flusso proattivo originato dall'attaccante.

L'analisi dei risultati evidenzia l'invio massivo di tali pacchetti verso un ampio range di porte di destinazione, con intervalli temporali ridotti (ordine dei millisecondi).

Tale comportamento conferma l'uso di uno strumento di scansione automatizzato (**Nmap**) in modalità "Connect Scan", caratterizzata dal completamento della connessione TCP prima dell'invio di un reset (RST) di chiusura.

tcp.flags.syn == 1 and tcp.flags.ack == 0

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=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
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
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
42	36.776179338	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

Figura 2 Evidenza dei pacchetti SYN inviati in rapida successione verso porte multiple.

Ipotesi di Comando

Basandosi sulla natura della scansione (Three-Way Handshake completo, alta velocità, scansione su tutte le porte), è possibile ipotizzare con alto grado di confidenza che il comando eseguito dall'attaccante sia stato: nmap -sT -p- -T4 192.168.200.150 L'opzione -sT forza la connessione TCP completa (rilevata nei log), mentre la densità dei pacchetti suggerisce un timing aggressivo (-T4).

3. Enumerazione dei Servizi Esposti (Porte Aperte)

Al fine di identificare i servizi attivi che hanno risposto positivamente alla scansione, è stato applicato il seguente filtro di visualizzazione per isolare la seconda fase del Three-Way Handshake TCP:

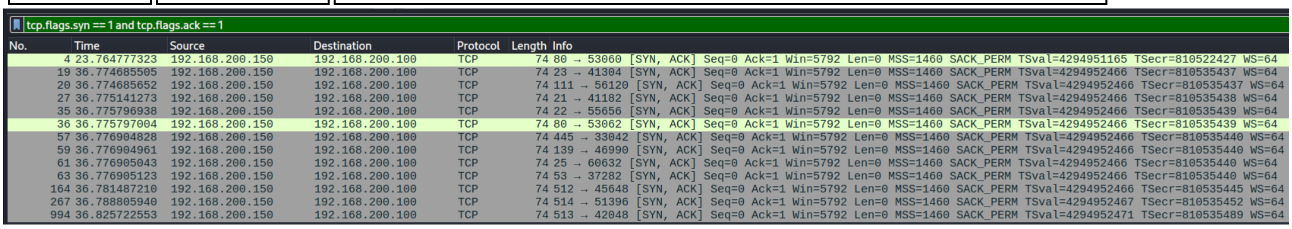
```
tcp.flags.syn == 1 and tcp.flags.ack == 1
```

Il filtro è progettato per evidenziare esclusivamente le **risposte affermative** del target.

- Il parametro `tcp.flags.syn == 1` combinato con `tcp.flags.ack == 1` (SYN-ACK) indica che la porta di destinazione è aperta e il servizio è in ascolto.
- Questa vista permette di scartare i tentativi falliti (pacchetti RST o nessun traffico di ritorno), focalizzando l'analisi sulla superficie di attacco effettiva esposta dalla vittima.

L'analisi dei pacchetti di risposta provenienti dall'host .150 rivela la presenza di numerose porte critiche aperte. Di seguito il dettaglio dei servizi identificati:

Porta (TCP)	Servizio	Analisi della Criticità
21	FTP	Servizio non cifrato, probabile presenza di Backdoor (vsftpd).
22	SSH	Esposto a Brute-Force.
23	Telnet	**Critico:** Accesso remoto in chiaro (senza cifratura).
25	SMTP	Server di posta, potenziale enumerazione utenti.
53	DNS	Servizio di risoluzione nomi.
80	HTTP	Web Server, vettore per attacchi applicativi.
111	RPCbind	Mappa i servizi RPC, utile per enumerazione avanzata.
139 / 445	NetBIOS/SMB	**Critico:** Vulnerabile a exploit RCE (Samba/EternalBlue).
512	exec	**R-Services:** Permette esecuzione comandi remoti (r-commands).
513	login	**R-Services:** Accesso remoto senza password forte (rlogin).
514	shell	**R-Services:** Shell remota insicura (rsh).


tcp.flags.syn == 1 and tcp.flags.ack == 1

No.	Time	Source	Destination	Protocol	Length	Info
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
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
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
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 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 TSval=4294952466 TSecr=810535439 WS=64
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64
267	36.788805940	192.168.200.150	192.168.200.100	TCP	74	514 → 51396 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64
994	36.825722553	192.168.200.150	192.168.200.100	TCP	74	513 → 42048 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64

Figura 3 Risposte SYN-ACK dal target che confermano i servizi attivi e raggiungibili.

4. Fingerprinting dell'Ambiente (Information Disclosure)

Un'analisi approfondita del traffico iniziale ha rivelato un pacchetto di protocollo **BROWSER** (NetBIOS Host Announcement). Il target annuncia in broadcast il proprio hostname come **METASPLOITABLE**, fornendo all'attaccante un'indicazione immediata sulla natura del sistema operativo e sulle potenziali vulnerabilità intrinseche, senza necessità di scansioni attive.

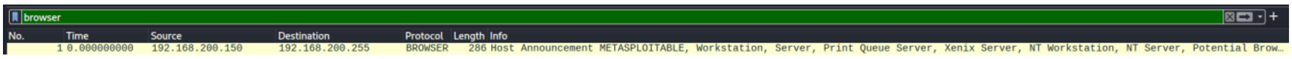


Figura 4 Pacchetto NetBIOS che rivela l'hostname e la tipologia del target.

Verifica Post-Exploitation

A seguito dell'identificazione delle porte critiche aperte (in particolare Telnet - porta 23), è stata condotta un'analisi approfondita per verificare eventuali accessi non autorizzati riusciti.

È stato applicato il filtro tcp.port == 23 && tcp.len > 0 per isolare eventuali scambi di dati (payload) successivi alla connessione.

L'analisi non ha evidenziato traffico dati significativo o sessioni interattive (shell) stabilite. Si conferma che l'attività si è limitata alla fase di **Reconnaissance** (Scansione) e non è evoluta in una **Exploitation** attiva nel periodo osservato.

Conclusioni e Raccomandazioni

L'analisi ha confermato che la macchina 192.168.200.150 è un sistema deliberatamente vulnerabile (***Metasploitable***) esposto all'interno di una rete virtuale. La presenza di protocolli obsoleti e non cifrati (**Telnet, R-Services**) e di servizi critici (**SMB**) la rende soggetta a compromissione immediata tramite exploit remoti o attacchi brute-force.

Si raccomandano le seguenti azioni correttive (**Hardening**):

1. **Isolamento di Rete:** Mantenere la macchina in una VLAN isolata (Host-Only o Internal Network) per evitare che possa essere attaccata o usata come ponte verso l'host fisico.
2. **Disabilitazione Servizi Insicuri:** Disattivare immediatamente i servizi **Telnet (23)** e **R-login (512-514)**, imponendo l'uso esclusivo di SSH configurato con autenticazione a chiave pubblica.
3. **Filtraggio del Traffico:** Implementare regole firewall per bloccare il traffico NetBIOS/SMB (Porte 139, 445) verso l'esterno, riducendo il rischio di exploit RCE (Remote Code Execution).
4. **Monitoraggio IDS:** Configurare un sistema di Intrusion Detection (es. Snort) per rilevare pattern di port scanning e bloccare preventivamente l'IP sorgente tramite regole di *drop* automatico.