

Report di Analisi del Traffico di Rete

1) Introduzione e obiettivo

L'attuale scenario della sicurezza informatica richiede un'analisi dettagliata del traffico di rete per identificare tempestivamente tentativi di intrusione e attività di cognizione. Il presente report analizza una cattura di pacchetti (file **Cattura_U3_W1_L5.pcapng**) effettuata tramite l'applicativo **Wireshark** all'interno di un ambiente di laboratorio controllato. La sessione di monitoraggio ha intercettato un flusso di dati tra un host attaccante (Kali Linux, IP **192.168.200.100**) e un target vulnerabile (**Metasploitable**, IP **192.168.200.150**).

L'analisi si focalizza sulle prime fasi della **Cyber Kill Chain**, ovvero la ricognizione e l'identificazione degli asset, analizzando le anomalie nei protocolli TCP, ARP e NetBIOS.

L'attività di indagine si pone i seguenti obiettivi principali:

- **Identificazione della Metodologia di Scansione:** Determinare la tecnica utilizzata dall'attaccante per mappare la rete, analizzando la struttura dei flag TCP e la frequenza dei pacchetti.
- **Mappatura della Superficie di Attacco:** Individuare quali servizi e quali porte del target sono state sollecitate per determinare, in base alle risposte dell'host (**SYN/ACK vs RST/ACK**), quali risultino effettivamente esposte.
- **Rilevamento di Anomalie di Rete:** Documentare eventuali errori di protocollo, ritrasmissioni o tentativi di connessione falliti che possano indicare la presenza di sistemi di difesa o configurazioni di rete specifiche.

1) Riepilogo dell'Attività

L'analisi del traffico evidenzia un'interazione intensa tra due host principali sulla sottorete **192.168.200.0/24**. L'attività predominante è costituita da tentativi di connessione TCP rapidi verso diverse porte, molti dei quali terminano con un reset della connessione.

- **Sorgente (Attaccante/Scanner):** **192.168.200.100**
- **Destinazione (Target):** **192.168.200.150**

2) Analisi dei Protocolli e Flussi

-Host Discovery (Pacchetto 1)

Il primo pacchetto mostra un annuncio browser (protocollo BROWSER) dove l'host **.150** si identifica esplicitamente come **METASPOITABLE**. Questo indica che il target è una macchina vulnerabile intenzionale, spesso usata per laboratori di penetration testing.

No.	Time	Source	Destination	Protocol	Description
1	0.0899999999	192.168.200.150	192.168.200.255	BROWSER	286 Host Announcement METASPOITABLE, Workstation Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential...
2	0.0900000000	192.168.200.100	192.168.200.150	TCP	74.5386 - 80 [SYN] Seq=0 Win=1468 MSS=1468 SACK_PERM Tsvl=810522428 Tsecr=4294951165 WS=64
3	0.23.76477739	192.168.200.100	192.168.200.150	TCP	74.53876 - 84 [SYN] Seq=0 Win=1468 MSS=1468 SACK_PERM Tsvl=810522428 Tsecr=4294951165 WS=64
4	23.76477732	192.168.200.150	192.168.200.100	TCP	74.80 - 53608 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1468 SACK_PERM Tsvl=4294951165 Tsecr=810522428 WS=64
5	23.76477742	192.168.200.150	192.168.200.100	TCP	68.443 - 33876 [RST, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1468 SACK_PERM Tsvl=4294951165 Tsecr=810522428 WS=64
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66.53860 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810522428 Tsecr=4294951165
7	23.764815290	192.168.200.100	192.168.200.150	TCP	66.53861 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810522428 Tsecr=4294951165
8	28.761629461	PCSystemtec_fd:87:..	PCSystemtec_39:7d:..	ARP	68 who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSystemtec_39:7d:..	PCSystemtec_fd:87:..	ARP	42.192.168.200.100 is at 08:00:27:39:7d:fe

-Port Scanning (TCP SYN Scan)

A partire dal **pacchetto n. 12**, si osserva una sequenza di pacchetti **TCP SYN** provenienti dall'host .**100** verso l'host .**150** su diverse porte (es. 23, 111, 443, 554, 135, 993, 21, 110, ecc.).

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 Tsvl=810535437 Tscr=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 Tsvl=810535437 Tscr=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 Tsvl=810535437 Tscr=0 WS=128
15 36.774363709 192.168.200.100	192.168.200.150	TCP	74 56120 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535437 Tscr=0 WS=128
16 36.774485607 192.168.200.100	192.168.200.150	TCP	74 56120 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535437 Tscr=0 WS=128
17 36.774525534 192.168.200.100	192.168.200.150	TCP	74 56120 - 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535437 Tscr=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 Tsvl=810535438 Tscr=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 Tsvl=4294952466 Tscr=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 Tsvl=4294952466 Tscr=810535437 WS=64

- Comportamento:** La sorgente invia **SYN**; se la porta è chiusa, la destinazione risponde con **RST, ACK** (le righe rosse, es. pacchetti 21, 26, 32).

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 Tsvl=4294952466 Tscr=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 Tsvl=4294952466 Tscr=810535437 WS=64
21 36.774685696 192.168.200.150	192.168.200.100	TCP	69 443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 36.774685709 192.168.200.150	192.168.200.100	TCP	69 443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 36.774685776 192.168.200.150	192.168.200.100	TCP	69 135 - 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 Tsvl=810535438 Tscr=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 Tsvl=810535438 Tscr=4294952466
26 36.775141164 192.168.200.150	192.168.200.100	TCP	69 993 - 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 - 41102 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=4294952466 Tscr=810535438 WS=64

- Tecnica:** Questo pattern è probabilmente un **nmap -st** che chiede al sistema operativo di completare l'intera procedura di connessione standard con ogni porta che sta scansionando.

-SYN: Nmap invia un pacchetto di richiesta connessione.

-SYN/ACK: Se la porta è **aperta**, il bersaglio risponde accettando.

-ACK: Nmap risponde a sua volta, **completando la connessione** (handshake).

-RST: Subito dopo, Nmap chiude la connessione per passare così alla porta successiva.

-Analisi ARP (Pacchetti 8-11)

Si notano diverse richieste ARP ("Who has..."). Questo indica che gli host stanno risolvendo gli indirizzi MAC per comunicare nel segmento di rete locale.

7 23.764899691 192.168.200.100	192.168.200.150	TCP	66 53060 - 88 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=810522428 Tscr=4294951165
8 28.761644619	PCSSystemtec_39:7d:..	PCSSystemtec_39:7d:..	ARP
9 28.761644619	PCSSystemtec_39:7d:..	PCSSystemtec_39:7d:..	ARP
10 28.774852527	PCSSystemtec_39:7d:..	PCSSystemtec_39:7d:..	ARP
11 28.774852527	PCSSystemtec_39:7d:..	PCSSystemtec_39:7d:..	ARP
12 36.774143445	192.168.200.100	192.168.200.150	TCP
13 36.774143445	192.168.200.100	192.168.200.150	TCP
14 36.774218116	192.168.200.100	192.168.200.150	TCP
15 36.774218116	192.168.200.100	192.168.200.150	TCP
16 28.774852527	PCSSystemtec_39:7d:..	PCSSystemtec_39:7d:..	ARP
17 28.774852527	PCSSystemtec_39:7d:..	PCSSystemtec_39:7d:..	ARP
18 28.774852527	PCSSystemtec_39:7d:..	PCSSystemtec_39:7d:..	ARP
19 28.774852527	PCSSystemtec_39:7d:..	PCSSystemtec_39:7d:..	ARP
20 36.774685595	192.168.200.150	192.168.200.100	TCP
21 36.774685696	192.168.200.150	192.168.200.100	TCP
22 36.774685709	192.168.200.150	192.168.200.100	TCP
23 36.774685776	192.168.200.150	192.168.200.100	TCP
24 36.774700464	192.168.200.100	192.168.200.150	TCP
25 36.774711072	192.168.200.100	192.168.200.150	TCP
26 36.775141164	192.168.200.150	192.168.200.100	TCP
27 36.775141273	192.168.200.150	192.168.200.100	TCP

3) Analisi degli Alert (Righe Rosse)

Le righe evidenziate in **rosso** in Wireshark indicano pacchetti con flag **RST (Reset)** o problemi di ritrasmissione.

- Significato:** L'host .**150** sta attivamente rifiutando le connessioni sulle porte che non ha attive. Ad esempio, nel pacchetto 21, la porta 443 (HTTPS) risponde con un RST, indicando che il servizio non è disponibile o è filtrato.

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 Tsvl=4294952466 Tscr=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 Tsvl=4294952466 Tscr=810535437 WS=64
21 36.774685696 192.168.200.150	192.168.200.100	TCP	69 443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 36.774685709 192.168.200.150	192.168.200.100	TCP	69 443 - 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 36.774685776 192.168.200.150	192.168.200.100	TCP	69 135 - 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 Tsvl=810535438 Tscr=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 Tsvl=810535438 Tscr=4294952466
26 36.775141164 192.168.200.150	192.168.200.100	TCP	69 993 - 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 - 41102 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=4294952466 Tscr=810535438 WS=64

4) Conclusioni Tecniche

In conclusione, l'analisi del traffico catturato nel file **Cattura_U3_W1_L5.pcapng** evidenzia un'attività sistematica di **network scanning** e tentativi di connessione tra gli host della sottorete **192.168.200.0/24**.

I punti chiave emersi sono:

- **Scansione delle Porte:** Si osserva un elevato numero di pacchetti TCP con flag [SYN] diretti verso varie porte (come la 21, 22, 23, 80, 111, 135, 139, 443, 445 e altre) dell'host **192.168.200.150**. Questo comportamento è tipico di una fase di **Enumeration o Port Scanning**.
- **Risposte del Target:** Molte di queste richieste ricevono un pacchetto [RST, ACK] (evidenziato in rosso), il che indica che le porte corrispondenti sul target sono chiuse o che un firewall sta attivamente rifiutando la connessione.
- **Protocolli Identificati:** Oltre al traffico TCP, la presenza di pacchetti **ARP** per la risoluzione degli indirizzi MAC e di annunci **BROWSER/NetBIOS** suggerisce una fase di scoperta dei servizi Windows/Samba all'interno della rete locale.
- **Configurazione dell'Ambiente:** L'annuncio iniziale ("METASPLOITABLE, Workstation, Server...") conferma che l'analisi si sta svolgendo in un ambiente di test controllato, mirato all'identificazione di vulnerabilità su macchine bersaglio specifiche.