

# 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 ricognizione. 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 **METASPLOITABLE**. Questo indica che il target è una macchina vulnerabile intenzionale, spesso usata per laboratori di penetration testing.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	284	Host Announcement: METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix, Seq=1, NT Workstation, NT Server, Potential
2	25.764239950	192.168.200.100	192.168.200.150	TCP	74	33860 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=818522428 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=818522428 TSecr=0 WS=128
4	23.76477323	192.168.200.100	192.168.200.100	TCP	74	80 → 53860 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=818522427 WS=64
5	23.764777424	192.168.200.100	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	53860 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=818522428 TSecr=4294951165
7	23.764899891	192.168.200.100	192.168.200.150	TCP	60	53860 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=818522428 TSecr=4294951165
8	28.761629461	PCSSystemtec_f8:197...	PCSSystemtec_39:7d1...	ARP	60	who has 192.168.200.100? tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d1...	PCSSystemtec_f8:197...	ARP	42	192.168.200.100 is at 66:00:27:39:7d1: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	41384	- 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	36.774366395	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
19	36.774685595	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	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

- **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	- 41384 [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
21	36.774685690	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	36.774709404	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	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=4294952466 TSecr=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	23.764890901	192.168.200.100	192.168.200.150	TCP	60	53060	- 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSval=810522428 TSecr=294951105
8	28.761029461	PCSystemtec_f0:87:	PCSystemtec_39:7d:	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150	
9	28.761644619	PCSystemtec_39:7d:	PCSystemtec_f0:87:	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe	
10	28.774852257	PCSystemtec_39:7d:	PCSystemtec_f0:87:	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100	
11	28.775239099	PCSystemtec_f0:87:	PCSystemtec_39:7d:	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e	
12	36.774343445	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

## 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	- 41384 [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
21	36.774685690	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	36.774709404	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	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=4294952466 TSecr=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 **Enumerazione** 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.