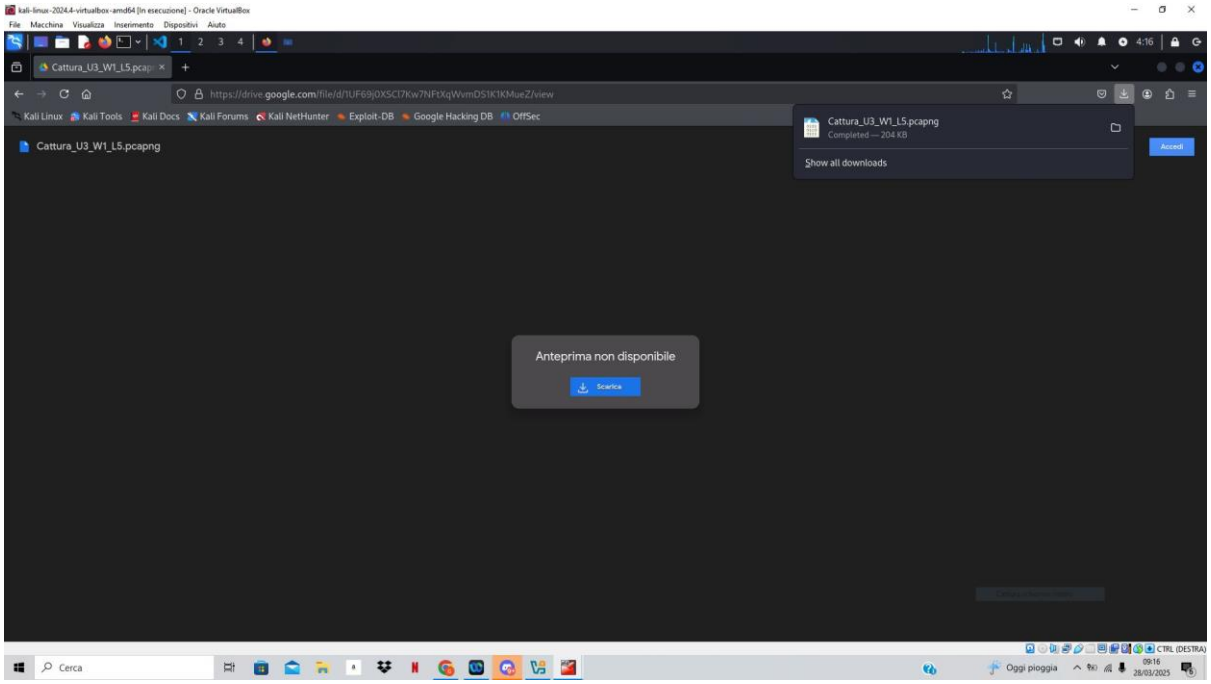
Traccia

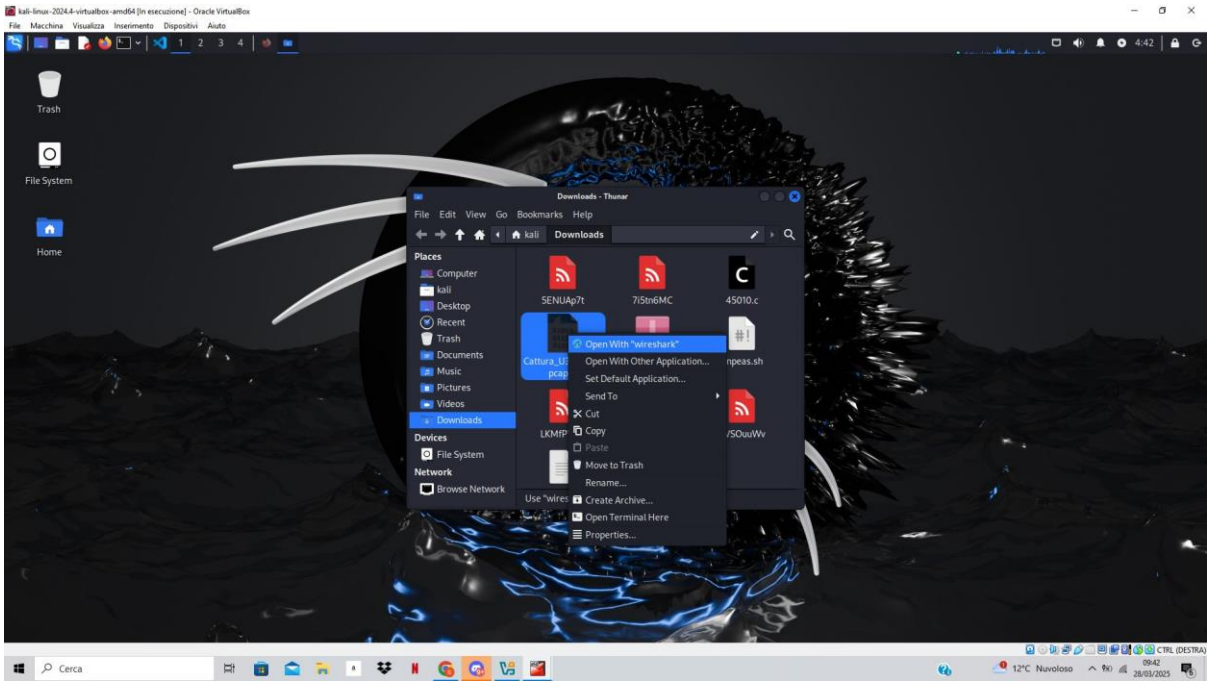
Esercizio **Threat Intelligence & IOC**. Durante la lezione teorica, abbiamo visto la **Threat Intelligence** e gli indicatori di compromissione. Abbiamo visto che gli **IOC** sono evidenze o eventi di un attacco in corso, oppure già avvenuto. Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con **Wireshark**. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

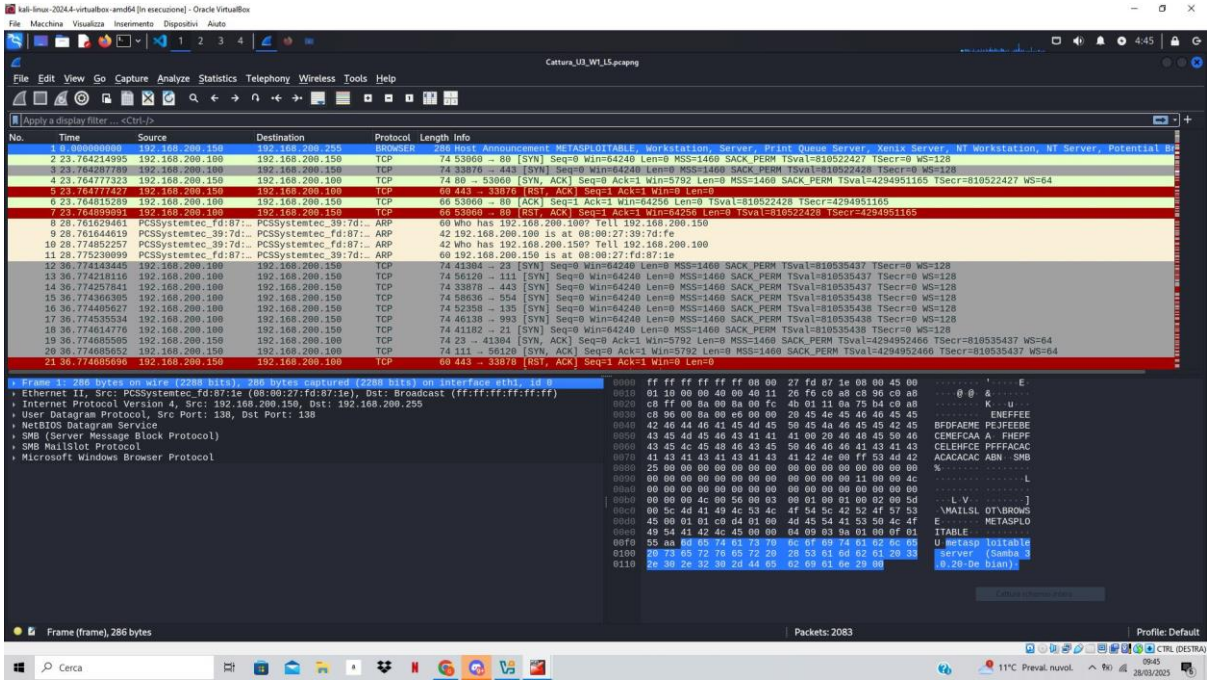
- Identificare ed analizzare eventuali **IOC**, ovvero evidenze di attacchi in corso;
- In base agli **IOC** trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati.

Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.

CATTURA





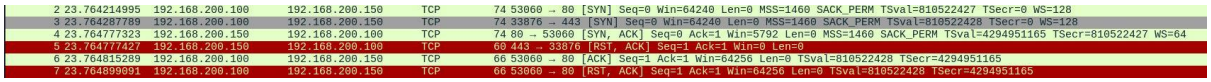


Analisi dello scambio pacchetti

Analizzando il traffico di rete, la prima riga presenta un'annuncio di host che coinvolge il sistema **Metasploitable**, insieme ad altri dispositivi e server di rete:

- **IP di origine**: `192.168.200.150` – L'indirizzo IP da cui è originato il pacchetto.
- **IP di destinazione**: `192.168.200.255` – Questo è un indirizzo di broadcast, il che significa che il pacchetto viene inviato a tutti i dispositivi nella sottorete **`192.168.200.0`**.
- **Protocollo**: Il protocollo utilizzato per l'annuncio, che fa parte del servizio **NetBIOS** su TCP/IP (NBT), viene utilizzato da Windows per la navigazione in rete.
- **Annuncio host**: Il pacchetto sta annunciando la presenza di vari servizi, tra cui Metasploitable, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server e un potenziale browser.

Questo tipo di pacchetto può far parte di una scansione o enumerazione della rete.

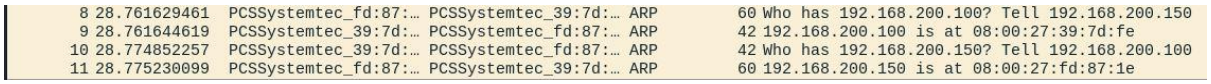


Di seguito inizia una connessione TCP su porta 80 da parte del dispositivo con IP `192.168.200.100` verso il dispositivo, con IP `192.168.200.150.` Il primo inviato è un pacchetto di tipo **SYN**:

- **Porta di origine**: `53060` – La porta da cui il pacchetto è stato inviato.
- **Porta di destinazione**: `80` – La porta di destinazione, che è tipicamente usata per il traffico **HTTP**.
- **Tipo di pacchetto**: `[SYN]` – Questo è un pacchetto di sincronizzazione, che fa parte della fase di **three-way handshake** per stabilire una connessione TCP.

Questo è solo il primo passo del processo di **handshake**, in cui il client (IP `192.168.200.150`) invia il pacchetto **SYN** per iniziare la connessione, poi viene inviato un pacchetto TCP da IP `192.168.200.150 [SYN, ACK],` questo è il secondo passo **dell'handshake** TCP. Con il flag **ACK**, il dispositivo riconosce la richiesta di connessione. Tuttavia, alla riga successiva con il flag **RST**, il dispositivo sta rifiutando la connessione (o per un motivo di errore o per altre politiche di sicurezza). che rappresenta una **risposta di reset** (RST) a una connessione già stabilita:

- **Porta di origine**: 443 – La porta di origine è la 443, tipicamente utilizzata per il traffico **HTTPS**.
- **Porta di destinazione**: 33876 – La porta di destinazione a cui il pacchetto è stato inviato.
- **Tipo di pacchetto**: `[RST, ACK]` – Il pacchetto è un **RST** (Reset) con **ACK** (**Acknowledge**). Il pacchetto RST viene inviato per interrompere una connessione TCP in modo anomalo o per segnalare che la connessione non può essere stabilita o è stata interrotta.



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	28.775230099	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e

Questo pacchetto è un **ARP (Address Resolution Protocol)**, utilizzato per mappare un indirizzo IP a un indirizzo MAC all'interno di una rete locale:

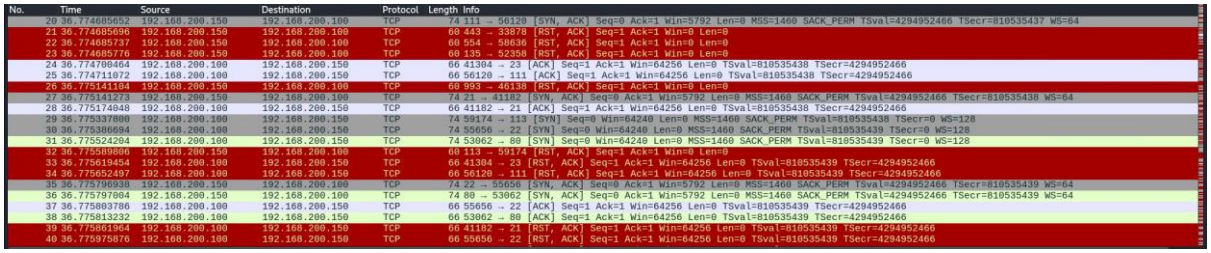
Messaggio ARP: “`Who has 192.168.200.150? Tell 192.168.200.100”,` questo è il contenuto del pacchetto ARP. Il dispositivo con indirizzo IP `192.168.200.100` sta chiedendo "Chi ha l'indirizzo IP `192.168.200.150`? Rispondete a `192.168.200.100`".

In pratica, il dispositivo con IP `192.168.200.100` sta cercando di scoprire l'indirizzo MAC associato all'indirizzo IP `192.168.200.150` in modo da poter inviare correttamente i pacchetti a quell'indirizzo.

Di seguito una **risposta ARP:**

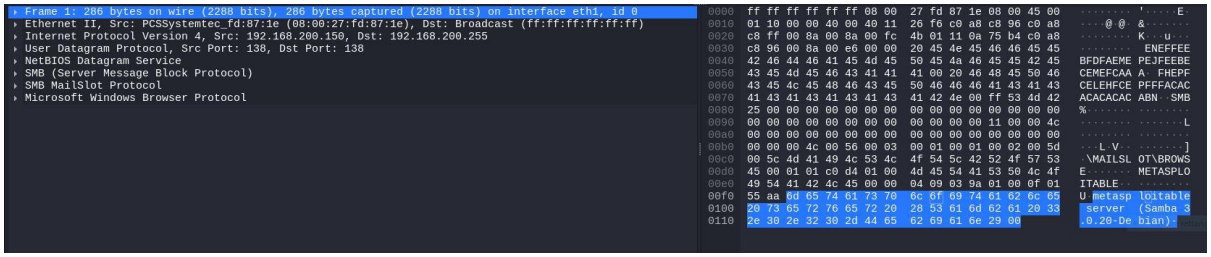
Messaggio ARP: `192.168.200.150 is at 08:00:27:fd:87:1e` , questo è il contenuto del pacchetto ARP, in cui il dispositivo con l'indirizzo IP `192.168.200.150` risponde alla richiesta ARP, dicendo che il suo indirizzo MAC è `08:00:27:fd:87:1e`.

Questo pacchetto è una risposta al messaggio ARP precedente in cui il dispositivo con IP `192.168.200.100` aveva chiesto chi avesse l'indirizzo IP `192.168.200.150`. Ora, il dispositivo con IP `192.168.200.150` ha risposto, comunicando il suo indirizzo MAC.



No.	Time	Source	Destination	Protocol	Length	Info
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56128 [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
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=4294952466 TSecr=810535438 WS=64
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
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	36.775380694	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
32	36.775589886	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
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
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

Dopo inizia una sequenza da 192.168.200.100 di TCP [SYN] e 192.168.200.150 di TCP [SYN, ACK/RST ACK]



```
▸ 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
```

```
0000  ff ff ff ff ff ff 08 00  27 fd 87 1e 08 00 45 00   ........ '.....E.
0010  01 10 00 00 40 00 40 11  26 f6 c0 a8 c8 96 c0 a8   ....@.@. &.......
0020  c8 ff 00 8a 00 8a 00 fc  4b 01 11 0a 75 b4 c0 a8   ........ K...u...
0030  c8 96 00 8a 00 e6 00 00  20 45 4e 45 46 46 45 45   ........  ENEFFEE
0040  42 46 44 46 41 45 4d 45  50 45 4a 46 45 45 42 45   BFDFAEME PEJFEEBE
0050  43 45 4d 45 46 43 41 41  41 00 20 46 48 45 50 46   CEMEFCAA A. FHEPF
0060  43 45 4c 45 48 46 43 45  50 46 46 46 41 43 41 43   CELEHFCE PFFFACAC
0070  41 43 41 43 41 43 41 43  41 42 4e 00 ff 53 4d 42   ACACACAC ABN..SMB
0080  25 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   %....... ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 11 00 00 4c   ........ .......L
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 4c 00 56 00 03  00 01 00 01 00 02 00 5d   ...L.V.. .......]
00c0  00 5c 4d 41 49 4c 53 4c  4f 54 5c 42 52 4f 57 53   .\MAILSL OT\BROWS
00d0  45 00 01 01 c0 d4 01 00  4d 45 54 41 53 50 4c 4f   E....... METASPLO
00e0  49 54 41 42 4c 45 00 00  04 09 03 9a 01 00 0f 01   ITABLE.. ........
00f0  55 aa 0d 65 74 61 73 70  6c 6f 69 74 61 62 6c 65   U..metasp loitable
0100  20 73 65 72 76 65 72 20  28 53 61 6d 62 61 20 33    server  (Samba 3
0110  2e 30 2e 32 30 2d 44 65  62 69 61 6e 29 00         .0.20-De bian).
```

Questo pacchetto rappresenta una **comunicazione di tipo broadcast** utilizzando il **protocollo NetBIOS (Network Basic Input/Output System)**. Analizziamo i dettagli del pacchetto per identificare eventuali **Indicators of Compromise (IOC)** e determinare se possa essere indicativo di un attacco o comportamento sospetto.

Analisi degli IOC

1.Protocolli SMB e NetBIOS: L'uso di **SMB** e **NetBIOS** insieme potrebbe suggerire che i dispositivi stiano cercando di scoprire o accedere a risorse condivise nella rete. SMB è stato frequentemente sfruttato in attacchi di tipo **ransomware** (come il caso di

WannaCry). L'uso di NetBIOS per scoprire dispositivi sulla rete è anche un possibile segno di un attacco di **scansione della rete** o un tentativo di **enumerazione**.

2.Attività ARP: In particolare, la richiesta ARP potrebbe suggerire un tentativo di **ARP Spoofing** o **Man-in-the-Middle**. In un attacco ARP Spoofing, un attaccante invia risposte ARP false per associarsi a indirizzi IP legittimi, dirottando il traffico verso il proprio dispositivo. Se il traffico tra i dispositivi fosse intercettato, potrebbe esserci il rischio di **esfiltrazione dei dati** o **modifica del traffico.**

3.Pacchetti TCP con SYN e RST: Potrebbe indicare un **attacco DoS (Denial of Service)** o un tentativo di **scannerizzazione di porte** per identificare vulnerabilità.

Ipotesi sui potenziali vettori di attacco

1.Enumerazione della rete: Il pacchetto di broadcast potrebbe essere parte di un processo di **enumerazione della rete**. L'attaccante potrebbe essere alla ricerca di dispositivi vulnerabili o risorse condivise (ad esempio, cartelle di rete o stampanti) che possono essere sfruttate.

2.Attacco tramite SMB: Poiché SMB è utilizzato per condividere file e stampanti, un attaccante potrebbe tentare di sfruttare una vulnerabilità in un dispositivo che espone servizi SMB. Se il traffico SMB è mal configurato o non adeguatamente protetto, un attacco come **EternalBlue potrebbe essere possibile.**

3.ARP Spoofing (Man-in-the-Middle): Se stiamo osservando un tentativo di **ARP Spoofing**, l'attaccante potrebbe voler intercettare o dirottare il traffico di rete per raccogliere informazioni sensibili o iniettare dati dannosi nelle comunicazioni tra

dispositivi. Il vettore di attacco è una **vulnerabilità nel protocollo ARP**, che non prevede alcuna forma di autenticazione.

4.Denial of Service (DoS) / Port Scanning: Il pacchetto con flag **RST** potrebbe essere una tecnica di **DoS** mirata a interrompere le connessioni legittime. Un attaccante potrebbe anche essere utilizzando una scansione delle porte per identificare servizi vulnerabili, facendo uso di pacchetti SYN per sondare le porte aperte, per poi inviare pacchetti **RST** per interrompere le connessioni.

Azioni consigliate per ridurre l'impatto

1.Limitare l'esposizione di SMB e NetBIOS: se i servizi SMB e NetBIOS non sono necessari, disabilitarli sui dispositivi della rete per ridurre la superficie di attacco. Se SMB è necessario, si può **usare SMBv3** (che è più sicuro) e assicurarsi che le risorse siano protette con **autenticazione forte** e **crittografia**.

2.Segmentazione della rete: segmentare la rete in sottoreti per isolare i dispositivi più sensibili e ridurre la portata degli attacchi. I dispositivi che non necessitano di interagire con SMB dovrebbero essere isolati da quelli che lo utilizzano.

3.Monitoraggio del traffico di rete: Configurare un sistema di rilevamento delle intrusioni (IDS) per monitorare il traffico di rete alla ricerca di pacchetti sospetti, come quelli che utilizzano NetBIOS o SMB. Monitorare i pacchetti broadcast, in particolare quelli diretti a **tutti i dispositivi** (indirizzo MAC di broadcast), per rilevare eventuali tentativi di enumerazione della rete.

4.Aggiornamenti di sicurezza: assicurarsi che tutti i dispositivi di rete siano aggiornati con le ultime patch di sicurezza, in particolare per i vulnerabili servizi SMB (come **EternalBlue**).

5.Autenticazione a più fattori: implementare l'autenticazione a più fattori (MFA) per l'accesso a risorse di rete sensibili, come file condivisi, per ridurre il rischio di compromissione in caso di attacco