

Report Tecnico: Analisi Threat Intelligence & IOC

Studente: Giuseppe Monaco

1. Introduzione

Il presente report documenta i risultati dell'analisi condotta sul file di log di rete fornito. L'obiettivo primario è isolare eventuali anomalie di traffico, identificare le entità coinvolte nella comunicazione e determinare se siano in corso tentativi di intrusione o attività di ricognizione ostile. L'esame è stato svolto mediante l'ausilio di *Wireshark* per l'ispezione dei pacchetti.

2. Identificazione degli Attori di Rete

L'analisi dei metadati e dei payload dei pacchetti ha permesso di delineare la topologia della comunicazione, individuando due nodi principali:

- **Host Sorgente (Minaccia): 192.168.200.100**
 - Questo IP è l'iniziatore di quasi tutte le connessioni TCP, inviando richieste ad alta frequenza. Identificato come la macchina attaccante (Kali Linux).
- **Host Destinazione (Bersaglio): 192.168.200.150**
 - Questo IP risponde passivamente alle sollecitazioni.
 - *Information Leakage*: Al pacchetto n. 1, l'host invia un broadcast SMB rivelando il proprio hostname: **METASPLOITABLE**. Questo ha permesso l'identificazione immediata della natura vulnerabile del sistema

No.	Time	Source	Destination	Protocol	Length	Info
18	0.0000000	192.168.200.150	192.168.200.255	Broadcast	286	Host Announcement: METASPLOITABLE, Workstation, Server, Print Queue Server, Xerox Server, NT Workstation, NT Server, Potential S
233	0.64214995	192.168.200.100	192.168.200.150	TCP	74	53800 → 80 [RST] Seq=9 Win=0 Len=0 MSS=1460 SACK_PERM TSval=618522427 TSecr=0 WS=328

▶ Frame 1: Packet, 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), Trans Request (0x25)

 ▶ SMB Header

 Server Component: SMB

 SMB Command: Trans (0x25)

 Error Class: Success (0x00)

 Reserved: 00

 Error Code: No Error

 ▶ Flags: 0x00

 ▶ Flags2: 0x0000

- **Protocollo:** BROWSER (SMB)
- **Info:** Il pacchetto contiene la stringa "*Host Announcement METASPLOITABLE, Workstation, Server...*".
- **Dettaglio Tecnico:** La vittima (192.168.200.150) sta inviando un pacchetto broadcast (192.168.200.255) rivelando il proprio Hostname (**METASPLOITABLE**) e il servizio utilizzato (**SMB**). Questo permette all'attaccante di identificare il bersaglio senza toccarlo attivamente.

Successivamente, si osserva un traffico massivo TCP indicativo di una scansione delle porte automatizzata.

S. Time	Source	Destination	Protocol	Length	Info
1	192.168.200.150	192.168.200.255	TCP	60	Host Announcemnt MT:DISPATCHABLE, MORTIFICATION, SERVER, PRIN, Queue Server, MOIS, Server, MT:DISPATCHABLE, MT:SERVER, POCUNTIAL bro
2	23.74.147.93	192.168.200.150	TCP	74	53600 - 80 [SYN] Seq=1642426 Lenn=1502-1503 SACK PERM Tsva1=180522428 Tsvcr=424949150
3	23.74.147.93	192.168.200.150	TCP	74	53600 - 80 [SYN] Seq=1642426 Lenn=1502-1503 SACK PERM Tsva1=180522428 Tsvcr=424949150
4	23.74.147.93	192.168.200.150	TCP	74	53600 - 80 [SYN] Seq=1642426 Lenn=1502-1503 SACK PERM Tsva1=180522428 Tsvcr=424949150
5	23.74.147.93	192.168.200.150	TCP	74	53600 - 80 [SYN] Seq=1642426 Lenn=1502-1503 SACK PERM Tsva1=180522428 Tsvcr=424949150
6	23.74.147.93	192.168.200.150	TCP	74	53600 - 80 [SYN] Seq=1642426 Lenn=1502-1503 SACK PERM Tsva1=180522428 Tsvcr=424949150
7	23.74.147.93	192.168.200.150	TCP	74	53600 - 80 [SYN] Seq=1642426 Lenn=1502-1503 SACK PERM Tsva1=180522428 Tsvcr=424949150
8	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	60 who has 192.168.200.150? len 192.168.200.150
9	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
10	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
11	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
12	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
13	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
14	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
15	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
16	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
17	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
18	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
19	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
20	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
21	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
22	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
23	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
24	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
25	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
26	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
27	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
28	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
29	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
30	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
31	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
32	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
33	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
34	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
35	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
36	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
37	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
38	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
39	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
40	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
41	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
42	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
43	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
44	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
45	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
46	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
47	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
48	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
49	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
50	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
51	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
52	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
53	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
54	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
55	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
56	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
57	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
58	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
59	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
60	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
61	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
62	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
63	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
64	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
65	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
66	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
67	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
68	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
69	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
70	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
71	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
72	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
73	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
74	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
75	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
76	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
77	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
78	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
79	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
80	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
81	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
82	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
83	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
84	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
85	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
86	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
87	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
88	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
89	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
90	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
91	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
92	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
93	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
94	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
95	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
96	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
97	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
98	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
99	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150
100	78.162.94.61	PCSystemtec.f87:	PCSystemtec.f87:	ARP	42 who has 192.168.200.150? len 192.168.200.150

1. **Righe Grigie (Richiesta SYN):** L'attaccante (192.168.200.100) invia pacchetti **SYN** in rapida successione verso porte diverse della vittima (es. porte 199, 995, 587). È il tentativo di connessione iniziale.
2. **Righe Rosse (Risposta RST - Porta Chiusa):** La vittima (192.168.200.150) risponde con **RST, ACK** (Reset). Il colore rosso in Wireshark indica che la connessione è stata rifiutata, confermando all'attaccante che la porta è **CHIUSA**.
3. **Righe Grigio Chiaro/Verdi (Risposta SYN/ACK - Porta Aperta):** Dove la vittima risponde con **SYN, ACK**, indica che un servizio è in ascolto (Porta **APERTA**).

L'attività massiva osservata nei log identifica una tecnica specifica nota come **TCP SYN Scan** (o "Half-open scan").

- **SYN Scan:** È una tecnica di scansione in cui l'attaccante invia un pacchetto **SYN** (richiesta di sincronizzazione) come se volesse iniziare una connessione legittima. Tuttavia, non appena riceve una risposta positiva (**SYN-ACK**) dalla vittima, non completa il "three-way handshake" inviando l'ACK finale, ma tronca la comunicazione con un pacchetto **RST** (Reset).

L'obiettivo finale di questa operazione è il **Port Mapping** (mappatura delle porte). L'attaccante sta "bussando" a tutte le porte della macchina vittima per censire quali servizi sono attivi (es. Server Web, Database, File Sharing). Ogni porta aperta scoperta (evidenziata dai pacchetti SYN-ACK nei log) rappresenta una potenziale "porta d'ingresso" vulnerabile da attaccare nella fase successiva.

4. Valutazione della Superficie d'Attacco

Sulla base delle porte risultate aperte ("Open"), è stata stilata una lista dei vettori di rischio che l'attaccante potrebbe sfruttare nelle fasi successive:

1. **Accesso Remoto Insicuro (Porta 23 - Telnet):**
 - *Analisi:* Servizio critico obsoleto. A differenza di SSH, Telnet non cifra la connessione.
 - *Impatto:* Un attaccante in ascolto sulla rete può leggere username e password in chiaro.
2. **File Sharing Legacy (Porte 139/445 - SMB):**
 - *Analisi:* La versione rilevata (Samba) è spesso soggetta a vulnerabilità gravi (es. *Exploit Username Map Script*).
 - *Impatto:* Rischio elevatissimo di esecuzione remota di codice (RCE) e compromissione totale del server.
3. **Trasferimento File (Porta 21 - FTP):**
 - *Analisi:* Protocollo spesso configurato male (es. accesso anonimo abilitato).
 - *Impatto:* Possibile esfiltrazione di dati o caricamento di file malevoli.
4. **Servizi Web (Porta 80 - HTTP):**
 - *Analisi:* Presenza di un Web Server in chiaro. Su macchine come Metasploitable, questo ospita tipicamente applicazioni web vulnerabili (es. DVWA, Mutillidae).
 - *Impatto:* Esposizione a vulnerabilità applicative come SQL Injection, XSS o Remote File Inclusion (RFI).
5. **Gestione Remota Sicura (Porta 22 - SSH):**
 - *Analisi:* Sebbene sia il sostituto sicuro di Telnet , la sua presenza indica un punto di ingresso amministrativo.

- *Impatto*: Anche se il traffico è cifrato, il servizio rimane esposto ad attacchi di Brute-Force se protetto solo da password deboli (es. msfadmin:msfadmin).
-

5. Strategie di Difesa e Mitigazione

L'analisi conferma che la macchina **192.168.200.150** è un bersaglio attivo di ricognizione. L'attaccante ha identificato con successo la natura vulnerabile del sistema ("Metasploitable").

Azioni Consigliate:

- **Hardening dei Servizi**: Rimuovere immediatamente i protocolli che trasmettono in chiaro (**Telnet, FTP**) migrando verso alternative cifrate (**SSH, SFTP**).
- **Segmentazione e Firewalling**: Configurare regole di firewall per bloccare scansioni rapide (rate-limiting) e impedire l'accesso alle porte SMB (139, 445) da IP non amministrativi.
- **Gestione sicura di SMB**: La best practice prevede la chiusura delle porte 139 e 445 per prevenire vettori di attacco noti. Se l'infrastruttura richiede tale protocollo, è mandatorio eseguire l'upgrade all'ultima release stabile e imporre l'autenticazione obbligatoria per tutti gli utenti.