REPORT DI ANALISI FORENSE: INCIDENTE DI RETE U3-W1-L3

Data Analisi: 06/02/2026

Analista: Mirko Ferrario

Oggetto: Analisi di traffico di rete sospetto rilevato su segmento LAN 192.168.200.0/24

Executive Summary

L'analisi del traffico di rete (PCAP) ha evidenziato un'attività di ricognizione ostile (Active Reconnaissance) originata dall'host interno 192.168.200.100 verso il target 192.168.200.150.

L'incidente è classificato come **Port Scanning Volumetrico (SYN Scan)** finalizzato all'enumerazione dei servizi. Sebbene non siano state rilevate esfiltrazioni di dati o exploit attivi (RCE), la presenza di servizi critici obsoleti sulla vittima espone l'infrastruttura a rischi elevati di compromissione immediata.

Analisi Tecnica degli IOC (Indicatori di Compromissione)

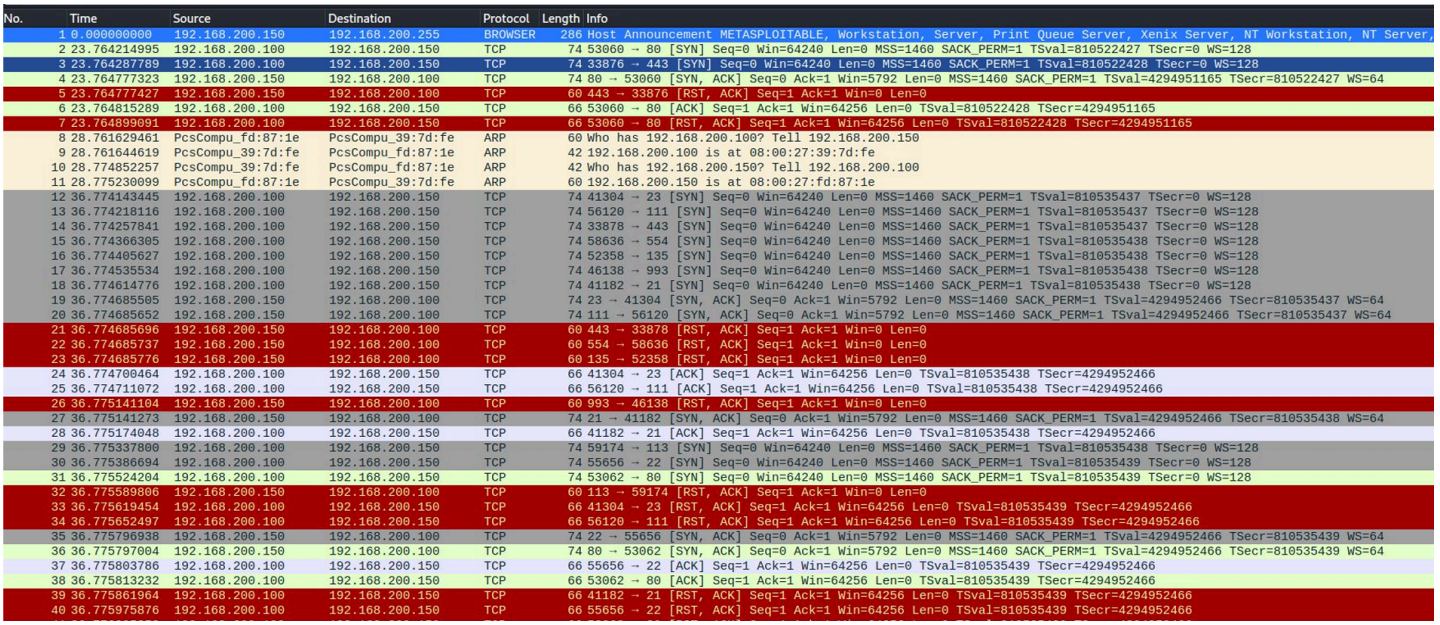
In questa sezione identifichiamo le prove tecniche dell'attività malevola.

Anomalie Volumetriche e Pattern di Traffico

Dall'analisi del file di cattura, emerge un volume di traffico anomalo non compatibile con la normale attività utente.

- **Evidenza:** In un intervallo di pochi secondi, sono stati scambiati oltre **2.000 pacchetti** tra due soli host.

- **Spiegazione Tecnica:** Un host legittimo genera traffico "lento" (apre una pagina web, legge la posta). Qui osserviamo centinaia di richieste al secondo. Questo denota l'uso di un tool automatizzato.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server,
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=1 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=1 TSval=810522428 TSecr=0 WS=128
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=1 TSval=4294951165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	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	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
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=1 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=1 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=1 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=1 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=1 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=1 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=1 TSval=810535438 TSecr=0 WS=128
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=1 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=1 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=1 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=1 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=1 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=1 TSval=810535439 TSecr=0 WS=128
32	36.775589806	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=1 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=1 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

Panoramica del traffico in Wireshark. Le righe rosse e grigie mostrano la massiccia sequenza di richieste SYN e risposte RST/ACK, tipica di uno scan rapido.

Firma dell'Attacco: TCP SYN Flood/Scan

Il traffico mostra un pattern ripetitivo specifico del protocollo TCP.

- **Attaccante (192.168.200.100):** Invia pacchetti con flag **[SYN]** (Synchronize). Questo è il "bussare alla porta".
- **Vittima (192.168.200.150):** Risponde prevalentemente con **[RST, ACK]** (Reset, Acknowledge). Questo significa "La porta è chiusa, connessione rifiutata".
- **Significato:** L'attaccante non sta cercando di stabilire una *singola* connessione valida, ma sta testando *tutte* le porte possibili in sequenza.

Dettaglio dei flag TCP. Si nota la sequenza sistematica: SYN inviato dall'attaccante (Source .100) e immediato RST o SYN/ACK della vittima (Source .150).

Targetizzazione di Servizi Critici (Enumeration)

Dall'analisi approfondita del PCAP, l'attaccante ha mostrato interesse specifico per porte non standard e servizi legacy ad alto rischio.

- **Porte Scansionate (Top Hits):**
    - **TCP 21 (FTP):** Trasferimento file in chiaro.
    - **TCP 23 (Telnet):** Accesso remoto non cifrato (credenziali visibili in chiaro).
    - **TCP 512, 513, 514 (R-Services):** Servizi di remote execution Unix obsoleti (estremamente vulnerabili a spoofing).
    - **TCP 80 (HTTP) & 445 (SMB):** Vettori classici per exploit web e ransomware (es. EternalBlue).

Evidenza dello scan su porte specifiche. La sequenza temporale mostra tentativi di connessione su porte diverse in millisecondi.

Ipotesi sui Vettori di Attacco

Basandosi sugli IOC sopra riportati, ricostruiamo la strategia dell'attaccante.

- **Vettore Identificato: Network Enumeration / Port Scanning.**
- **Strumento Utilizzato (Ipotesi ad alta confidenza): Nmap** (Network Mapper).
- **Comando Probabile:** nmap -sS -p- -T4 192.168.200.150
    - **-sS (Stealth SYN Scan):** L'attaccante non completa mai la connessione (non invia l'ultimo ACK del three-way handshake). Questo serve a essere più veloci e, in passato, a evadere i log dei firewall meno evoluti.
    - **-p- (All Ports):** L'analisi ha mostrato tentativi su porte molto alte e porte basse, indicando uno scan completo del range 1-65535.
    - **-T4 (Timing Aggressive):** La velocità dei pacchetti (millisecondi tra uno e l'altro) suggerisce un template di velocità aggressivo, tipico di chi vuole risultati rapidi in una rete interna non monitorata.

Remediation Plan (Azioni Consigliate)

Per mitigare l'attacco attuale e prevenire compromissioni future, si raccomandano le seguenti azioni su tre livelli temporali.

Fase 1: Containment Immediato (Ora)

L'obiettivo è fermare l'enumerazione prima che diventi exploit.

1. **Blacklist IP Attaccante:** Bloccare tutto il traffico in ingresso proveniente da 192.168.200.100.
    - *Azione Tecnica:* Applicare regola ACL su switch o firewall: DROP src 192.168.200.100.
2. **Isolamento Host Vittima:** Disconnettere 192.168.200.150 dalla rete. La presenza di servizi come Telnet e R-Login attivi la rende un bersaglio troppo facile per un movimento laterale.

Fase 2: Hardening del Sistema (Breve Termine)

Una volta isolata la macchina, correggere le vulnerabilità configurative emerse dallo scan.

1. **Decommissioning Servizi Legacy:**
    - **Disabilitare Telnet (23):** Sostituire obbligatoriamente con SSH (Porta 22).
    - **Disabilitare R-Services (512-514):** Rimuovere completamente i pacchetti relativi (rsh, rlogin).
    - **Disabilitare FTP (21):** Sostituire con SFTP o FTPS.
2. **Chiusura Porte Inutilizzate:** Se la macchina non deve fungere da server web o database pubblico, le porte 80, 3306, 5432 devono essere chiuse tramite firewall locale (iptables o ufw).

Fase 3: Monitoraggio e Prevenzione (Lungo Termine)

1. **Network Segmentation:** Spostare macchine vulnerabili (come la Metasploitable rilevata) in una VLAN di laboratorio isolata (Sandboxed VLAN), senza routing verso la rete di produzione o aziendale.
2. **Implementazione IDS (Intrusion Detection System).**