

REPORT S9/L5: Analisi Threat Intelligence & IOC

Studente: Vincenzo Zarola

Corso: Cybersecurity Specialist

Oggetto: Analisi di una cattura di rete per l'identificazione di Indicatori di Compromissione (IOC).

1. Obiettivo dell'Esercitazione

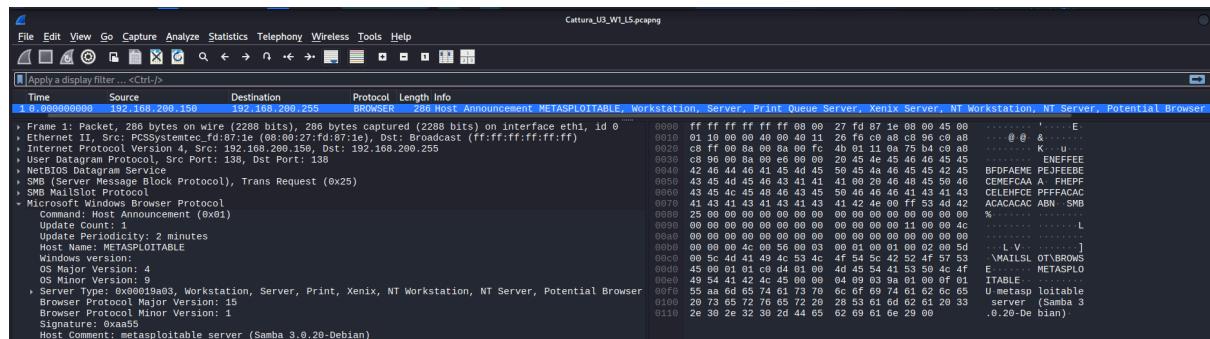
L'attività si concentra sull'analisi di un file di cattura (**Cattura_U3_W1_L5.pcapng**). L'obiettivo è identificare e analizzare eventuali IOC (Indicators of Compromise), ipotizzare i potenziali vettori di attacco e proporre strategie di difesa proattiva.

2. Identificazione e Analisi degli IOC

Dall'analisi approfondita dei pacchetti tramite Wireshark, sono stati isolati i seguenti indicatori di compromissione:

Information Leakage (Broadcast)

Il Pacchetto n°1 mostra un evento di "Host Announcement" inviato dall'indirizzo IP **192.168.200.150** verso il broadcast **192.168.200.255**.



The screenshot shows a single packet captured by Wireshark. The packet details are as follows:

- Time: 0.000000000000
- Source: 192.168.200.150
- Destination: 192.168.200.255
- Protocol: BROWSER
- Length: 260 bytes on wire (208 bits), 260 bytes captured (228 bits) on interface eth1, id 0
- Frame 1: Packet 1: 260 bytes on wire (208 bits), 260 bytes captured (228 bits) on interface eth1, id 0 (0.000000000000) at Fri, 27 Apr 2018 10:40:00 +0000 (Local Time)
Ethernet II, Src: Microsoft (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
Session Message Block Protocol, Trans Request (0x25)
SMB Mailslot Protocol
Microsoft Windows Browser Protocol
Command: Host Announcement (0x01)
Update Count: 1
Periodicity: 2 minutes
Host Name: METASPLOITABLE
Windows version:
OS Major Version: 4
OS Minor Version: 0
Server Type: 0x00019a03
Browser Protocol Major Version: 15
Browser Protocol Minor Version: 1
Signature: 0xa505
Host Comment: Metasploitable server (Samba 3.0.20-Dbian)

- Analisi:** Nel pannello di dettaglio del pacchetto, sotto il protocollo *Microsoft Windows Browser Protocol*, il sistema rivela in chiaro il proprio nome: **METASPLOITABLE**. Inoltre, il campo "Server Type" elenca servizi come *Workstation* e *Server*, esponendo la natura del sistema a chiunque sia in ascolto nella rete locale (Passive Reconnaissance).

Network Scanning (Active Reconnaissance)

A partire dal tempo **23.76s**, si osserva un traffico anomalo generato dall'host **192.168.200.100** verso **192.168.200.150**

Time	Source	Destination	Protocol	Length Info
1.0	0909090909	192.168.200.150	BROWSER	256 Host Announcement METASPOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential Browser
2.23	7.64214995	192.168.200.100	192.168.200.150	TCP 74 53060 → 80 [SYN] Seq=0
3.23	7.64287789	192.168.200.100	192.168.200.150	TCP 74 33876 → 443 [SYN] Seq=0
4.23	7.64777323	192.168.200.150	192.168.200.100	TCP 74 80 → 53060 [SYN, ACK] Seq=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810522428 Tscr=0 WS=128
5.23	7.64777427	192.168.200.150	192.168.200.100	TCP 60 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 MSS=1460 SACK_PERM Tsvl=810522428 Tscr=0 WS=64
6.23	7.64815289	192.168.200.100	192.168.200.150	TCP 66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=810522428 Tscr=0 WS=128
7.23	7.64899091	192.168.200.100	192.168.200.150	TCP 66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=810522428 Tscr=0 WS=128
8.23	7.74414774	192.168.200.100	192.168.200.150	TCP 66 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535437 Tscr=0 WS=128
9.28	7.61644019	PCSSystemte_c_39:7d:	ARP	42 192.168.200.100 Is at 08:09:27.3977:fe
10.28	7.74485257	PCSSystemte_c_39:7d:	ARP	42 Who has 192.168.200.100? Tell 192.168.200.100
11.28	7.75239099	PCSSystemte_c_39:7d:	ARP	42 192.168.200.100 Is at 08:09:27.41f1:87:1e
12.30	7.74414774	192.168.200.100	192.168.200.150	TCP 74 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535437 Tscr=0 WS=128
13.30	7.74238136	192.168.200.100	192.168.200.150	TCP 74 585120 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535437 Tscr=0 WS=128
14.36	7.74257843	192.168.200.100	192.168.200.150	TCP 74 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535437 Tscr=0 WS=128
15.36	7.74366308	192.168.200.100	192.168.200.150	TCP 74 58836 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=0 WS=128
16.36	7.74414774	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
17.36	7.74435534	192.168.200.100	192.168.200.150	TCP 74 48138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=0 WS=128
18.36	7.74414774	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	7.74485246	192.168.200.100	192.168.200.150	TCP 74 23 → 41394 [SYN, ACK] Seq=0 Win=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535437 Tscr=0 WS=64
20.36	7.74485246	192.168.200.100	192.168.200.150	TCP 74 41394 → 23 [ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535437 Tscr=0 WS=64
21.36	7.74485246	192.168.200.100	192.168.200.150	TCP 66 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22.36	7.74485246	192.168.200.100	192.168.200.150	TCP 66 554 → 58390 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23.36	7.74485246	192.168.200.100	192.168.200.150	TCP 66 135 → 52350 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24.36	7.74708077	192.168.200.100	192.168.200.150	TCP 66 41394 → 23 [ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=0 WS=128
25.36	7.74414774	192.168.200.100	192.168.200.150	TCP 66 41394 → 23 [ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=0 WS=128
26.36	7.74485246	192.168.200.100	192.168.200.150	TCP 66 41394 → 23 [ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=0 WS=128
27.36	7.75141273	192.168.200.100	192.168.200.150	TCP 74 21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=0 WS=64
28.36	7.75174048	192.168.200.100	192.168.200.150	TCP 66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=810535438 Tscr=0 WS=128
29.36	7.753386594	192.168.200.100	192.168.200.150	TCP 74 585120 → 113 [SYN] Seq=0 Win=64250 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=0 WS=128
30.36	7.753386594	192.168.200.100	192.168.200.150	TCP 74 55856 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535438 Tscr=0 WS=128
31.36	7.75524204	192.168.200.100	192.168.200.150	TCP 74 53862 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=810535439 Tscr=0 WS=128
32.36	7.75589889	192.168.200.100	192.168.200.150	TCP 66 513 → 59174 [RST, ACK] Seq=1 Win=0 Len=0
33.36	7.75619454	192.168.200.100	192.168.200.150	TCP 66 41394 → 23 [ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=810535439 Tscr=0 WS=128
34.36	7.75632507	192.168.200.100	192.168.200.150	TCP 66 56120 → 113 [RST, ACK] Seq=1 Ack=1 Win=64250 Len=0 Tsvl=810535439 Tscr=0 WS=128

- Analisi:** L'host attaccante genera un volume elevato di pacchetti TCP [SYN] in un lasso di tempo ridottissimo (millisecondi). Questo pattern è la firma tipica di un **Port Scanner** automatizzato (come Nmap).
- Risposta del Target:**
 - Porte Chiuse:** Numerose risposte [RST, ACK] (righe rosse), che indicano tentativi di connessione falliti su porte non attive (es. porte 445, 995, 587).
 - Porte Aperte:** Risposte [SYN, ACK] seguite da una chiusura immediata della connessione (RST) da parte dell'attaccante.

2	23.764214995	192.168.200.100	192.168.200.150	TCP 74 53060 → 80 [SYN] Seq=0
3	23.764287789	192.168.200.100	192.168.200.150	TCP 74 33876 → 443 [SYN] Seq=0
4	23.764777323	192.168.200.150	192.168.200.100	TCP 74 80 → 53060 [SYN, ACK]
5	23.764777427	192.168.200.150	192.168.200.100	TCP 60 443 → 33876 [RST, ACK]
6	23.764815289	192.168.200.100	192.168.200.150	TCP 66 53060 → 80 [ACK] Seq=1
7	23.764899091	192.168.200.100	192.168.200.150	TCP 66 53060 → 80 [RST, ACK]

Dall'analisi del Three-Way Handshake (visibile ad esempio nei pacchetti 2, 4 e 6), si nota che la connessione TCP viene completamente stabilita prima di essere resettata. Questo identifica la scansione come una **TCP Connect Scan (Nmap -sT)** e non come una SYN Scan (-sS), poiché l'attaccante invia il pacchetto ACK finale di conferma. Questa tecnica è meno furtiva e più facilmente rilevabile dai log di sistema rispetto a una scansione Stealth.

3. Ipotesi sui Vettori di Attacco

Basandosi sugli IOC rilevati e sulle porte risultate "APERTE" durante la scansione, possiamo ipotizzare che l'attaccante stia preparando un attacco mirato sfruttando i seguenti vettori:

- Vettore Telnet (Porta 23):** È stato rilevato un handshake completo sulla porta 23. Poiché Telnet trasmette dati in chiaro, l'attaccante potrebbe tentare un attacco di *Sniffing* o un *Brute Force* per ottenere le credenziali di accesso.
- Vettore Web (Porta 80):** La presenza della porta 80 aperta suggerisce la possibilità di attacchi verso l'applicazione web (es. SQL Injection, XSS) o tentativi di enumerazione delle directory (Gobuster).
- Vettore SMB (Porta 445):** Anche se alcuni tentativi sembrano resettati, la presenza di traffico SMB (visibile nel pacchetto 1 come protocollo sottostante) suggerisce che

l'attaccante potrebbe tentare exploit noti come *EternalBlue* o tentativi di accesso anonimo alle share di rete.

4. Azioni di Mitigazione e Risposta (Remediation)

Per ridurre l'impatto dell'attacco attuale e prevenire incidenti futuri, si consigliano le seguenti azioni:

A. Azioni Immediate (Containment)

- **Blocco IP:** Configurare una regola sul Firewall del router per bloccare tutto il traffico proveniente dall'IP **192.168.200.100**.
- **Analisi dei Log:** Verificare i log di sistema (Syslog/Event Viewer) della macchina **192.168.200.150** per confermare se, oltre alla scansione, ci siano stati tentativi di login (Event ID 4625).

B. Azioni Preventive (Hardening)

- **Disabilitazione Servizi Insicuri:** Il servizio Telnet (porta 23) deve essere immediatamente disattivato e sostituito con SSH (porta 22).
- **Disabilitazione NetBIOS:** Per evitare l'Information Leakage, disabilitare il protocollo NetBIOS over TCP/IP sulle interfacce di rete per impedire alla macchina di annunciare il proprio nome e ruolo in broadcast.
- **Implementazione SIEM/IDS:** Implementare un sistema di rilevamento intrusioni con regole specifiche per rilevare pattern di "Port Scanning" e allertare il team di sicurezza in tempo reale.
- **Automazione della Risposta (SOAR):** Integrare una soluzione SOAR configurando un **Playbook** automatico che, alla ricezione dell'alert "**Port Scan Detected**" dal SIEM, blocchi immediatamente l'IP attaccante sul Firewall senza intervento umano.