RAPPORTO DI INTELLIGENCE SULLE MINACCE: Ricognizione della Rete Interna

Gravità: Alta (Rilevata Ricognizione Attiva)

Stato: Confermato

1. Sintesi Esecutiva (Executive Summary)

L'analisi del traffico di rete interno, catturato nel file Cattura_U3_W1_L5.pcapng, ha identificato una campagna di ricognizione attiva sostenuta, diretta contro un'infrastruttura critica.

L'analisi del traffico ha rivelato che un host con indirizzo IP 192.168.200.100 ha avviato una rapida scansione **TCP SYN** contro un asset vulnerabile (192.168.200.150). La scansione ha enumerato con successo diversi servizi aperti, inclusi protocolli legacy non crittografati (Telnet, FTP) e servizi amministrativi critici (SMB).

Se non mitigata, questa attività rappresenta il precursore di uno sfruttamento (exploit), che porterà probabilmente ad attacchi di forza bruta (brute-force) o all'esecuzione di codice in remoto (RCE) tramite vulnerabilità note come EternalBlue.

---

2. Panoramica dell'Incidente

Metrica	**Dettagli**
Tipo di Minaccia	Ricognizione di Rete / Port Scanning
IP Attaccante	192.168.200.100
IP Vittima	192.168.200.150 (Identificato come "METASPLOITABLE")
Timestamp Inizio	T+ 36.774s
Protocollo	TCP
Firma dello Strumento	Coerente con scanner automatizzati (es. Nmap, Masscan)

L'analisi del traffico mostra un volume anomalo di richieste di connessione TCP generate in un brevissimo lasso di tempo.

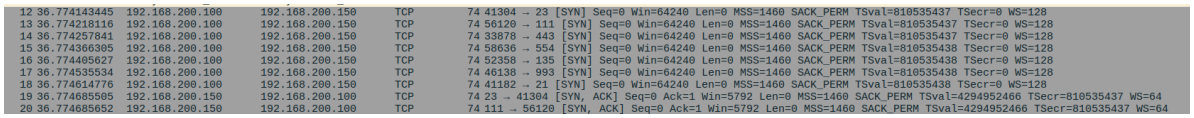

Figura 1: *Analisi del traffico di rete che evidenzia un alto volume di richieste SYN in sequenza rapida (Network Scanning Signature).*

---

3. Analisi Tecnica: Meccaniche TCP

L'attaccante ha utilizzato una scansione **SYN "Half-Open"** per mappare la superficie di attacco della vittima. Questa tecnica consente all'attaccante di determinare lo stato di una porta senza stabilire completamente una connessione, riducendo così la registrazione dei log a livello applicativo.

3.1 La Logica della Scansione

I log mostrano due distinti comportamenti TCP a seconda dello stato della porta di destinazione:

Caso A: Porta Aperta (Vulnerabile)

- **Comportamento:** L'Attaccante invia un pacchetto [SYN]. La Vittima risponde con [SYN, ACK].
- **Osservazione:** Il traffico verso la alcune porte, ad esempio **Porta 23 (Telnet)** e la **Porta 445 (SMB)** ha generato una risposta SYN, ACK.
- **Significato:** L'attaccante ora sa che su queste porte sono attivi dei servizi e li prenderà di mira per lo sfruttamento.

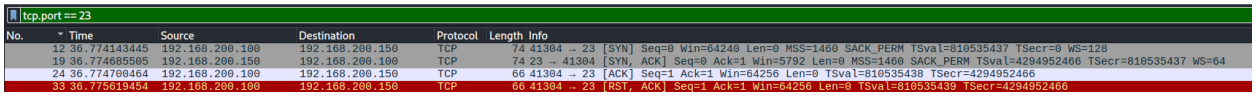

Figura 3: *Handshake TCP completo sulla porta 23, che conferma il servizio Telnet attivo e raggiungibile.*

Caso B: Porta Chiusa (Rifiutata)

- **Comportamento:** L'Attaccante invia un pacchetto [SYN]. La Vittima rifiuta immediatamente la connessione con [RST, ACK] (Reset/Acknowledgment).
- **Osservazione:** Il traffico verso porte chiuse ha generato un immediato RST, ACK.
- **Significato:** Il sistema operativo della vittima ha attivamente rifiutato la connessione, indicando che nessun servizio è in ascolto.

75	36.777430741	192.168.200.150	192.168.200.100	TCP	60 436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78	36.777623082	192.168.200.150	192.168.200.100	TCP	60 98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60 78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60 580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60 962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60 764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	192.168.200.150	192.168.200.100	TCP	60 435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figura 4: *La vittima invia un pacchetto RST, ACK (Reset) in risposta a un tentativo di connessione su una porta chiusa.*

---

4. Approfondimento: Utilizzo delle Porte Effimere

Un aspetto critico di questa cattura è la varianza delle **Porte Sorgente** utilizzate dall'attaccante.

4.1 Osservazione

Mentre le **Porte di Destinazione** mirano a servizi standard (es. 23, 80, 445), le **Porte Sorgente** provengono da numeri alti e casuali (es. 37952, 45416, 43166).

4.2 Meccanica delle Porte Effimere

Nel networking TCP/IP, il sistema operativo assegna una **Porta Effimera** temporanea (porta a vita breve) a ogni richiesta di connessione in uscita per mantenere l'unicità dello stato.

1. **Tracciamento dello Stato:** Poiché l'attaccante invia centinaia di pacchetti al secondo, il sistema operativo dell'attaccante richiede un identificatore unico per ogni "conversazione".
2. **La Tupla a 5 elementi:** Il SO traccia le connessioni usando: [IP Sorgente, Porta Sorgente, IP Dest, Porta Dest, Protocollo].
3. **Prevenzione delle Collisioni:** Se l'attaccante usasse una porta sorgente statica (es. Porta 5000) per tutte le scansioni in uscita, il traffico di ritorno dalla vittima sarebbe indistinguibile: la macchina dell'attaccante non saprebbe se un SYN, ACK appartiene alla scansione sulla Porta 80 o sulla Porta 21.

Ciclando attraverso le Porte Effimere (Intervallo 49152–65535), la macchina dell'attaccante può mappare accuratamente le risposte in arrivo rispetto alla specifica sonda inviata.

---

5. Indicatori di Compromissione (IOC)

I seguenti indicatori sono stati confermati nei log di rete:

- **Firma di Rete:** Alta frequenza di pacchetti [SYN] da una singola sorgente (.100) verso multiple porte di destinazione su (.150) entro una finestra temporale inferiore a 1 secondo.
- **Firma della Risposta:** Alto volume di pacchetti [RST, ACK] in uscita dalla vittima (che indicano il sondaggio di porte chiuse).
- **Servizi Vulnerabili Esposti:**
  - Porta 21 (FTP)
  - Porta 22 (SSH)
  - Porta 23 (Telnet)
  - Porta 80 (HTTP)
  - Porta 445 (SMB)

---

6. Raccomandazioni e Mitigazione

Per neutralizzare la minaccia e rafforzare (hardening) l'ambiente, si raccomandano le seguenti azioni:

1. **Isolamento della Rete (Immediato):**
   - Implementare regole firewall per bloccare immediatamente tutto il traffico proveniente da 192.168.200.100.
   - Comando consigliato: ufw deny from 192.168.200.100
2. **Hardening del Sistema:**
   - **Disabilitare Telnet (Porta 23):** Transizione di tutta l'amministrazione remota su SSH (Porta 22).
   - **Patching SMB:** Assicurarsi che la macchina vittima sia aggiornata (patchata) contro MS17-010 (EternalBlue) per prevenire la propagazione stile worm.
3. **Miglioramento del Rilevamento:**
   - Dispiegare un IDS/IPS (es. Snort o Suricata) con regole configurate per allertare su firme di "TCP Port Scanning".