PROGETTO S9L5

ANALISI DI WIRESHARK

Data: 24 Maggio 2024
studente: Cappellozza Daniele
Anno: 2025-2026
Corso: Cybersecurity

1. Identificazione ed Analisi degli IOC

Dall'analisi dei pacchetti catturati, sono stati identificati i seguenti IOC che indicano un **attacco in corso**:

- **Ip Sospetto:** 192.168.200.100 (Attaccante)
- **Target:** 192.168.200.150 (Vittima)
- **Attacco:** Si osserva un elevato numero di pacchetti **TCP SYN** inviati in rapida successione dall'ip sospetto verso una moltitudine di porte diverse sulla macchina target (es. porte 80, 443, 22, 21, 23, 25, 445, 110, 139, ecc.).
- **Risposta del Target:** Molti pacchetti ricevono in risposta **RST, ACK**. Questo indica che le porte sul target sono chiuse, ma l'attaccante sta continuando a tentare la connessione.
- **Informazione Critica:** Nel pacchetto n. 1 si nota un NetBIOS che identifica quale macchina si sta cercando di attaccare ovvero la **METASPLOITABLE**. Questo conferma uno scenario di penetration testing.

Conclusione: Siamo di fronte a un scansione delle porte aperte

2. Ipotesi sui Potenziali Vettori di Attacco

Sulla base degli IOC rilevati (scansione massiva di porte standard), si possono ipotizzare i seguenti vettori e finalità:

1. **Ricognizione:** L'attaccante sta utilizzando tool automatizzati (molto probabilmente **Nmap** o il modulo scanner di **Metasploit**) per identificare porte aperte (es. SSH sulla 22, Telnet sulla 23, SMB sulla 445).
2. **Fingerprinting dei Servizi:** Una volta identificate le porte aperte, l'attaccante tenterà di determinare la versione dei software in esecuzione (Banner Grabbing) per cercare exploit specifici.
3. **Sfruttamento di Vulnerabilità Note:** Dato che il target è identificato come "Metasploitable", i vettori probabili includono lo sfruttamento di servizi obsoleti o malconfigurati (es. backdoor su FTP, vulnerabilità Samba/SMB, o vulnerabilità su applicativi web).
4. **Brute Force:** La scansione delle porte 22 (SSH) e 23 (Telnet) suggerisce un possibile successivo tentativo di attacco a forza bruta per ottenere credenziali di accesso.

3. Azioni Consigliate

Per gestire l'evento attuale e prevenire incidenti futuri, si consigliano le seguenti azioni:

Azioni Immediate (Contenimento)

- **Interruzione della sorgente:** Configurare una regola sul Firewall o sull'IPS per bloccare (drop) temporaneamente tutto il traffico proveniente dall'IP `192.168.200.100`.
- **Isolamento:** Se il target `192.168.200.150` non è un honeypot o un ambiente di test autorizzato, isolarlo dalla rete principale fino al termine della bonifica.

Azioni a Lungo Termine (Prevenzione)

- Chiudere tutte le porte e i servizi non strettamente necessari al business
- Implementare ids/ips
- Eseguire scansioni di vulnerabilità regolari per identificare e patchare i servizi prima che lo faccia un attaccante.
- Separare i sistemi critici da quelli meno sicuri o di test tramite VLAN e firewall interni.
- Centralizzare i log di sistema e di rete su un SIEM per correlare tentativi di scansione con potenziali accessi anomali.