Introduzione

Il presente report si basa sull'analisi di un dump di traffico di rete fornito in formato Wireshark.
L'obiettivo è identificare potenziali attacchi o attività malevole presenti nel traffico e correlare eventuali vulnerabilità sfruttate.

Sommario dell'Analisi

1. Volume di Traffico

- **Totale pacchetti TCP**: 2.078
- **Tentativi di connessione SYN**: 1.026
- **Porte bersagliate**: 8 principali
- **Pacchetti ARP**: 4 (2 richieste, 2 risposte)

2. Destinazione Bersagliata

- **IP di destinazione principale**: 192.168.200.150
- **Totale traffico verso questa destinazione**: 1.052 pacchetti

Dettaglio delle Attività Sospette

Attività TCP e SYN Flood

- **Tentativi SYN**: 1.026 tentativi, concentrati da un'unica sorgente 192.168.200.100.
- **Segni di port scanning**: Sono stati scansionati servizi comuni e porte critiche.

Porta	Servizio	Tentativi	Potenziali Vulnerabilità
21	FTP	1	Brute force, trasferimenti non autorizzati
23	Telnet	1	Dati in chiaro, intercettazioni
53	DNS	1	Tunneling DNS, attacchi DDoS
80	HTTP	2	SQL injection, directory traversal
443	HTTPS	2	SSL stripping, vulnerabilità applicative
135	RPC	1	Esecuzione remota
139	NetBIOS	1	Enumerazione di rete
445	SMB	1	Exploit EternalBlue

Attività ARP

- **Richieste ARP**: 2 ("Who has")
    - Una richiesta proveniente da PCSSystemtec_fd:87:1e
    - Una richiesta proveniente da PCSSystemtec_39:7d:fe
- **Risposte ARP**: 2 ("is at")
    - Corrispondenza 1:1 tra richieste e risposte.
- **Conclusione**: Non ci sono segni evidenti di ARP spoofing.

Potenziali Exploit Identificati

Porta	Exploit Potenziale
21	Attacchi brute force FTP
23	Intercettazioni su Telnet
80	Attacchi applicativi (SQL, XSS)
443	SSL stripping
135	Exploit RPC
445	EternalBlue
53	Tunneling DNS
139	Enumerazione risorse di rete

Identificazione di IOC (Indicatori di Compromissione)

Gli indicatori di compromissione (IOC) osservati includono:

- **Traffico sospetto verso porte vulnerabili**: Specificamente porte 445 (SMB), 80 (HTTP), 443 (HTTPS), 21 (FTP) e 23 (Telnet).
- **Tentativi SYN ripetuti da una singola sorgente** (192.168.200.100), indicativo di un potenziale SYN flood o port scanning.
- **Assenza di completamento delle connessioni TCP**: Non ci sono pacchetti ACK successivi ai SYN, suggerendo un tentativo di esaurire le risorse del bersaglio.

Ipotesi sui Potenziali Vettori di Attacco

1. **Port Scanning e Ricognizione**:
    - Probabile tentativo di identificare servizi vulnerabili attivi sul sistema bersaglio.

2. **SYN Flood**:
    - Tentativo di sovraccaricare le risorse di rete del bersaglio saturando la tabella delle connessioni.
3. **Exploit mirati su porte specifiche**:
    - Porta 445 (SMB): Potenziale utilizzo di EternalBlue.
    - Porte 80/443: Sfruttamento di vulnerabilità applicative (SQL injection, XSS).

Raccomandazioni e Azioni Mitigative

Azioni Immediate

1. **Bloccare IP sospetti**:
    - Configurare regole firewall per bloccare traffico proveniente da 192.168.200.100.
2. **Isolare il sistema bersaglio**:
    - Se possibile, rimuovere 192.168.200.150 dalla rete per analisi forense.
3. **Monitoraggio attivo**:
    - Implementare strumenti di monitoraggio per rilevare ulteriori tentativi di connessione sospetta.

Azioni a Lungo Termine

1. **Aggiornare le patch di sicurezza**:
    - Applicare aggiornamenti per proteggere servizi vulnerabili come SMB e HTTP.
2. **Implementare IDS/IPS**:
    - Utilizzare un sistema di rilevamento/prevenzione delle intrusioni per bloccare attacchi futuri.
3. **Limitare l'esposizione delle porte**:
    - Chiudere porte non necessarie e applicare politiche di accesso ristretto.
4. **Addestramento del personale**:
    - Formare il team IT per riconoscere e rispondere tempestivamente a minacce simili.

Conclusione

L'analisi del traffico indica che l'host 192.168.200.150 è stato soggetto a una ricognizione mirata e a tentativi di sfruttamento di vulnerabilità. Misure immediate devono essere prese per mitigare l'impatto dell'attacco in corso e prevenire futuri attacchi simili. Una combinazione di aggiornamenti, monitoraggio attivo e formazione del personale sarà fondamentale per migliorare la resilienza della rete.