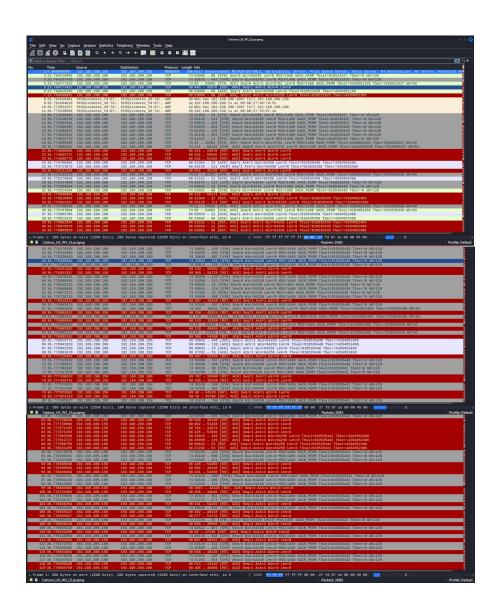
Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro



ANALISI

È stato rilevato un possibile attacco in corso sulla rete locale, caratterizzato da attività di scansione di porte, tentativi di sfruttamento di vulnerabilità note e potenziali manipolazioni del traffico di rete. L'attacco sembra essere mirato a ottenere accesso non autorizzato ai sistemi e ai dati sensibili presenti sulla rete.Notiamo tentativi di connessione TCP (SYN) da 192.168.200.100 verso 192.168.200.150 su porte come 80 (HTTP), 443 (HTTPS), 21, 22, 111, 135, 993 e altre. Si può dedurre che l'Host con indirizzo Ip 192.168.200.100 stia tentando di connettersi su di una macchina METASPLOITABLE, un tool usato per fare penetration test, e quindi per trovare vulnerabilità nei sistemi.

Indicatori di Compromissione (IOC):

- Indirizzo IP sospetto: 192.168.200.100
- Scansione di porte: Numerosi tentativi di connessione SYN verso varie porte.
- Tentativi di connessione a porte sensibili: 445 (SMB), 139(NetBIOS), 3306 (MySQL), 80 (HTTP), 443 (HTTPS) etc.
- Connessione riuscita: 21, 22,23, 25, 53, 80, 111,139, 445, 512, 513, 514.
- Traffico TCP anomalo: Pacchetti RST, ACK.
- Richieste ARP
- **Stringhe rilevanti:** "METASPLOITABLE", "BROWSER", "Xenix Server NT workstation NT Server Potential".

Vettori di Attacco Potenziali:

- Scansione di porte e servizi: In un ipotesi negativa, l'attaccante sta mappando la rete per identificare servizi vulnerabili.
- Sfruttamento di vulnerabilità note: Tentativi di sfruttare vulnerabilità in SMB, NetBIOS, MySQL, HTTP, HTTPS, altre porte e browser web.

Azioni Consigliate:

- 1. **Isolamento dell'host compromesso:** Disconnettere immediatamente 192.168.200.100 dalla rete.
- 2. **Analisi dei log:** Esaminare i log di sistema, delle applicazioni e del firewall di tutti gli host coinvolti.

- 3. **Scansioni antimalware:** Eseguire scansioni approfondite su tutti i sistemi.
- 4. **Aggiornamenti di sicurezza:** Aggiornare sistemi operativi e applicazioni con le patch più recenti.
- 5. **Rafforzamento della sicurezza:** Rafforzare la sicurezza di tutti i servizi utilizzati e chiudere i servizi che non risultano indispensabili.
- 6. **Monitoraggio della rete:** Monitorare il traffico per rilevare ulteriori attività sospette.
- 7. **Analisi forense:** Effettuare un'analisi forense dell'host compromesso.
- 8. **Cambio password:** Cambiare tutte le password di account utente e di servizio.
- 9. **Formazione degli utenti:** Educare gli utenti sulla sicurezza informatica.

Conclusioni:

L'isolamento dell'host 192.168.200.100 è fondamentale per contenere il possibile danno. Un'analisi approfondita è necessaria per identificare la causa principale e prevenire futuri incidenti.

Raccomandazioni Aggiuntive:

- Considerare l'implementazione di un sistema SIEM per la correlazione dei log.
- Utilizzare strumenti di analisi forense per ricostruire la sequenza degli eventi.
- Condurre un'analisi del possibile malware per comprendere le sue funzionalità.
- Implementare un piano di risposta agli incidenti per gestire futuri possibili attacchi.
- Incrementare sistemi di sicurezza informatica come IDS/IPS per riconoscere automaticamente comportamenti sospetti permettendo di intervenire in tempo reale.