Analisi e report del traffico di rete
Cattura effettuata con Wireshark

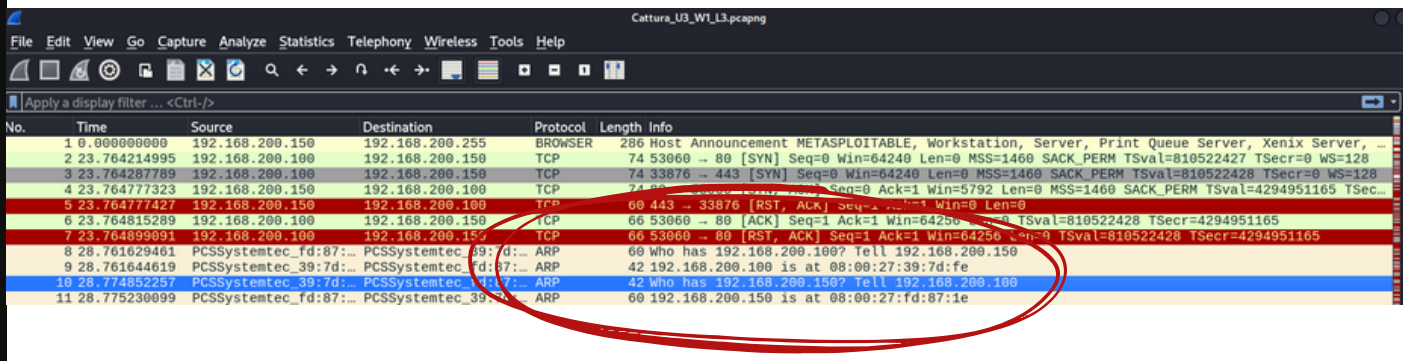
Introduzione

Gli Indicatori di Compromissione (IOC) sono evidenze che suggeriscono la presenza di un'attività malevola o di un attacco informatico in corso. Analizzando i pacchetti catturati con Wireshark, possiamo identificare vari IOC che possono indicare tentativi di attacco o comportamenti sospetti

Analisi dei pacchetti

Durante l'analisi del traffico di rete con Wireshark, sono stati osservati numerosi pacchetti TCP con flag SYN inviati da un IP (192.168.200.100) verso un altro IP (192.168.200.150), seguiti da risposte con flag RST. Tuttavia, su alcune porte specifiche, la risposta ai pacchetti SYN è positiva, con pacchetti SYN-ACK seguiti da pacchetti ACK, completando così l'handshake TCP a tre vie.

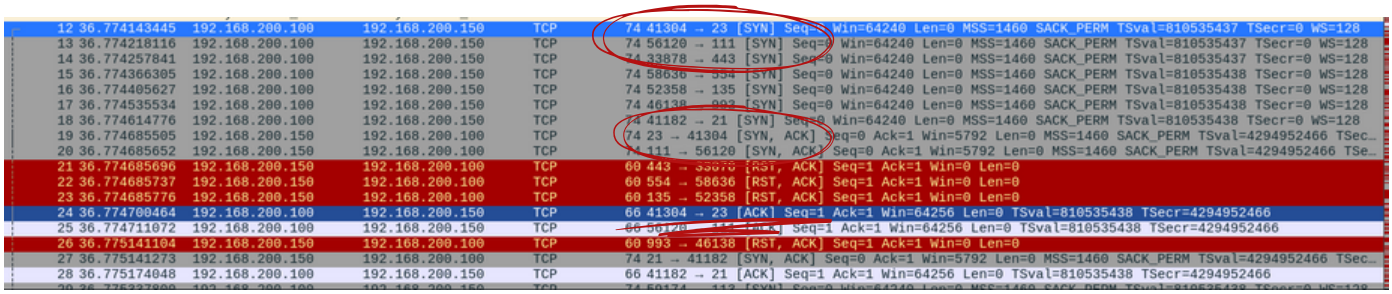
Per prima cosa andando ad analizzare i primi pacchetti della cattura

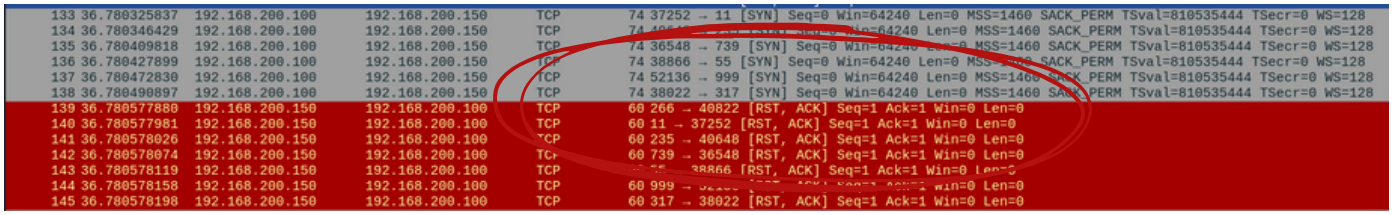


Possiamo notare dei pacchetti **ARP** seguiti da dei messaggi, "who has 192.168.200.100 tell 192.168.200.150" e "who has 192.168.200.150 tell 192.168.200.100" questi messaggi indicano che i dispositivi stanno cercando di risolvere gli indirizzi **IP** in indirizzi **MAC** per stabilire la comunicazione. Questo è un comportamento normale nelle reti locali e rappresenta il funzionamento di base di ARP per la risoluzione degli indirizzi.

Successivamente analizzando gli indirizzi ip 192.168.200.100 e 192.168.200.150 si può dedurre che appartengono alla stessa rete. La subnet mask utilizzata è /24 (255.255.255.0), che significa che i primi 24 bit degli indirizzi IP sono utilizzati per identificare la rete e gli ultimi 8 bit sono utilizzati per identificare gli host.
Siccome gli indirizzi rientrano nel range degli IP validi (da 192.168.200.1 a 192.168.200.254) significa che si trovano nella stessa rete.

Analizzando i successivi pacchetti si può osservare il seguente comportamento:





Numerosi Pacchetti **SYN**:

- Pacchetti con flag SYN inviati da 192.168.200.100 verso 192.168.200.150 su diverse porte.
- Questo potrebbe indicare una scansione delle porte, dove un attaccante tenta di trovare porte aperte e servizi attivi.

Risposte con flag **RST, ACK**:

- L'IP 192.168.200.150 risponde con pacchetti RST, ACK su alcune porte, indicando che queste porte sono chiuse.

Completamento di **Handshake TCP** su alcune porte:

- Su alcune porte specifiche, l'IP 192.168.200.150 risponde con pacchetti **SYN-ACK** e successivamente 192.168.200.100 completa l'handshake TCP con un pacchetto **ACK**.
- Questo indica che le connessioni su queste porte sono state stabilite correttamente, suggerendo che i servizi su queste porte sono attivi e accettano connessioni.

Identificazione degli IOC

Scansione delle Porte:

- La presenza di numerosi pacchetti SYN su diverse porte, con risposte miste di SYN-ACK e RST, è un chiaro indicatore di una scansione delle porte. Questo tipo di attività viene utilizzato per identificare quali servizi sono attivi su un host e quali porte sono aperte.

Connessioni Stabilite su Porte Specifiche:

- L'handshake TCP completato su alcune porte specifiche indica che i servizi su queste porte sono attivi e possono essere potenziali vettori di attacco se vulnerabili.

Ipotesi sui potenziali vettori d'attacco

Scansione delle Porte:

- Strumenti come Nmap potrebbero essere utilizzati per eseguire la scansione delle porte. L'attaccante invia pacchetti SYN a varie porte per determinare quali sono aperte e quali servizi sono in esecuzione.

Sfruttamento di Vulnerabilità dei Servizi Attivi:

- Una volta identificate le porte aperte e i servizi attivi, l'attaccante potrebbe tentare di sfruttare vulnerabilità note in quei servizi. Ad esempio, potrebbe utilizzare exploit specifici per il software in esecuzione su quelle porte.

Azioni consigliate

Monitoraggio delle scansioni delle porte

- Implementare sistemi di rilevamento delle intrusioni (IDS) per monitorare e rilevare attività di scansione delle porte, configurare avvisi per notificare gli amministratori di rete quando viene rilevata una scansione.

Aggiornamento e Patch dei Servizi

- Assicurarsi che tutti i servizi in esecuzione sui dispositivi di rete siano aggiornati con le ultime patch di sicurezza. Questo riduce la probabilità che gli attaccanti possano sfruttare vulnerabilità note.

Configurazione del Firewall

- Configurare il firewall per limitare l'accesso alle porte e ai servizi non necessari. Chiudere le porte non utilizzate e applicare regole di accesso restrittive per le porte aperte.

Segmentazione della Rete

- Implementare la segmentazione della rete per limitare il movimento laterale degli attaccanti, utilizzare VLAN e subnet per isolare segmenti di rete sensibili.

Analisi dei log

- Controllare regolarmente i log di sistema per rilevare attività sospette. Analizzare i log di connessione per identificare tentativi di accesso non autorizzati o comportamenti anomali.

L'implementazione delle azioni consigliate aiuterà a migliorare la sicurezza della rete e a mitigare i potenziali impatti degli attacchi, monitorare regolarmente il traffico di rete e mantenere aggiornati i sistemi sono pratiche essenziali per proteggere la rete da minacce e vulnerabilità.