PROGETTO S9/L5

Introduzione

L’obiettivo di questa relazione è analizzare un file di cattura di rete (pcapng) effettuato con Wireshark per identificare eventuali Indicatori di Compromissione (IOC) e comprendere la natura dell’attacco in corso. Dall'analisi preliminare, si è ipotizzato che si tratti di un port scanning, una tecnica comunemente utilizzata per esplorare le porte di un dispositivo alla ricerca di vulnerabilità. L'esercizio mira a identificare le evidenze di un possibile attacco e suggerire contromisure adeguate.

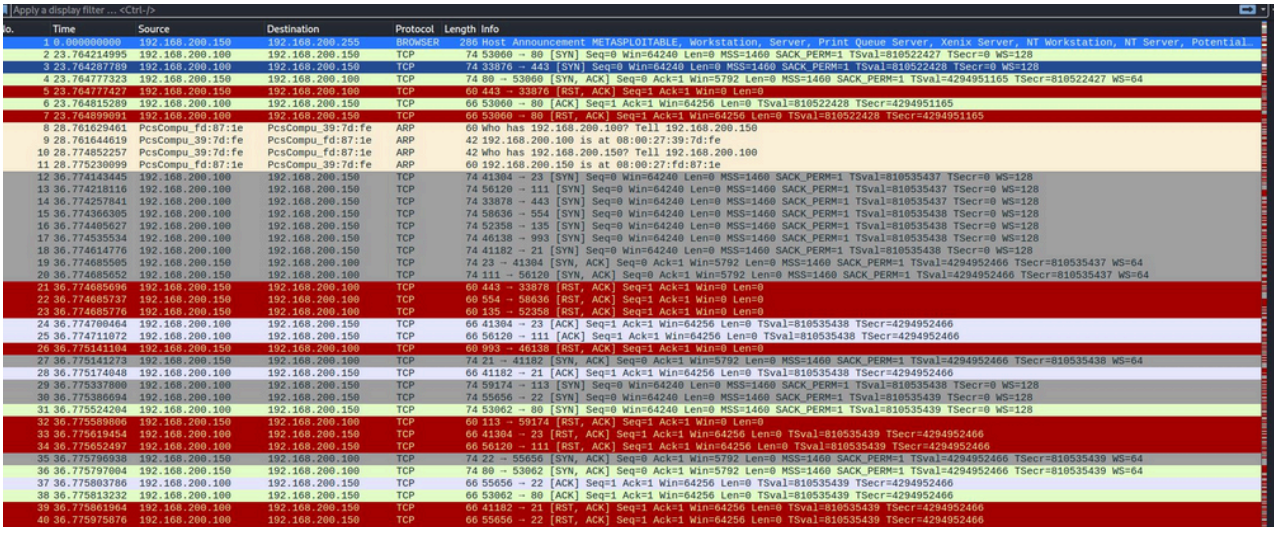
Identificazione degli IOC

Dall’analisi dei dati, emergono segnali che suggeriscono un’attività di port scanning. Si può riconoscere osservando i pacchetti TCP e le loro caratteristiche.

Il primo indicatore evidente è l’alto numero di pacchetti **TCP** con flag SYN inviati in rapida successione verso diverse porte su uno stesso host. Questo comportamento è tipico del port scanning, poiché l’attaccante cerca di individuare porte aperte e servizi in ascolto. Inoltre, molti di questi pacchetti sono seguiti da una risposta RST (Reset), il che indica che le porte non erano disponibili o che la connessione è stata rifiutata dal sistema target.

Un altro elemento che conferma la natura dell’attacco è il traffico sulle porte note, molte delle quali corrispondono a servizi critici come HTTP (porta 80), SMB (porta 445) e RDP (porta 3389). Questo suggerisce che l’attività non sia casuale, ma mirata a individuare vulnerabilità nei servizi più frequentemente utilizzati.

Infine, si osservano pacchetti **ARP** sospetti, che potrebbero indicare un tentativo di rilevare host attivi sulla rete locale prima di procedere con la scansione delle porte. Questo è un passaggio comune nelle fasi iniziali di un attacco, noto come "reconnaissance" (ricognizione).



Ipotesi sui vettori di attacco utilizzati

L’attacco rilevato sembra essere un tipico esempio di port scanning, un’attività preliminare utilizzata per raccogliere informazioni sulla configurazione della rete e identificare eventuali vulnerabilità. Gli strumenti più comuni per eseguire port scanning includono software come **Nmap**, che consente di identificare porte aperte e servizi attivi su un host. Inoltre, è possibile che l’attaccante abbia utilizzato script personalizzati per evitare di essere rilevato dai sistemi di monitoraggio.

Il port scanning è spesso un preludio a fasi successive di attacco. Una volta identificate le porte aperte, gli attaccanti possono sfruttare vulnerabilità specifiche associate ai servizi in esecuzione su tali porte. Ad esempio, una porta SMB aperta (445) potrebbe essere un punto d’ingresso per exploit noti come EternalBlue, mentre un servizio RDP non protetto (3389) potrebbe essere soggetto a tentativi di brute-force sulle credenziali.

Azioni consigliate per ridurre gli impatti dell'attacco attuale e futuri

Ridurre l’impatto dell’attacco **attuale**

- Configurare il firewall per rilevare e bloccare i tentativi di port scanning. Molti firewall moderni offrono funzionalità specifiche per rilevare pattern tipici di port scanning e per bloccare automaticamente questi tentativi.
- In alcuni casi si potrebbe bloccare l’IP sospetto, però in questo caso gli indirizzi sembrano essere nella stessa LAN, quindi bloccandolo, non conoscendo la natura di questa scansione, potremmo compromettere l’operabilità nell’azienda. Nel caso fosse stato un IP esterno poteva essere bloccato tramite il firewall, che può filtrare il traffico in ingresso da questi indirizzi IP sospetti.

Ridurre i rischi di attacchi **futuri**

- Un approccio efficace è limitare l’accesso alle porte critiche, permettendo solo a IP autorizzati di comunicare con tali servizi. Ad esempio, le porte SMB e RDP possono essere configurate per essere accessibili solo da specifici segmenti di rete o tramite VPN. È consigliabile configurare anche il rate limiting per limitare il numero di richieste di connessione provenienti da un singolo indirizzo IP.
- Implementare un sistema di rilevamento e risposta alle intrusioni (IDS/IPS) per monitorare continuamente la rete e rilevare tentativi di port scanning. L'IPS può anche bloccare automaticamente i pacchetti sospetti prima che raggiungano il sistema target.
- L'uso di honeypots può aiutare a identificare gli attaccanti. Questi sistemi sono configurati per sembrare porte vulnerabili e raccogliere informazioni sugli attacchi in corso, riducendo al minimo il rischio per il sistema reale.
- Assicurarsi che tutti i sistemi e le applicazioni siano regolarmente aggiornati per correggere eventuali vulnerabilità conosciute.

Conclusioni

L'analisi del file pcapng ha rivelato la presenza di un attacco di tipo port scanning, confermato dalla rilevazione di numerosi tentativi di connessione TCP a un ampio numero di porte. Sulla base di questi indicatori, è stato ipotizzato l'uso di tecniche come il SYN scan e l'utilizzo di strumenti automatizzati per esplorare le porte vulnerabili come Nmap.
Per mitigare gli effetti dell'attacco attuale e prevenire futuri tentativi, è fondamentale adottare misure di difesa come il rafforzamento dei firewall, l'implementazione di sistemi IDS/IPS, e l'adozione di politiche di sicurezza attive.