S9L5

Traccia:

Durante la lezione teorica, abbiamo visto la **Threat Intelligence** e gli indicatori di compromissione.
Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

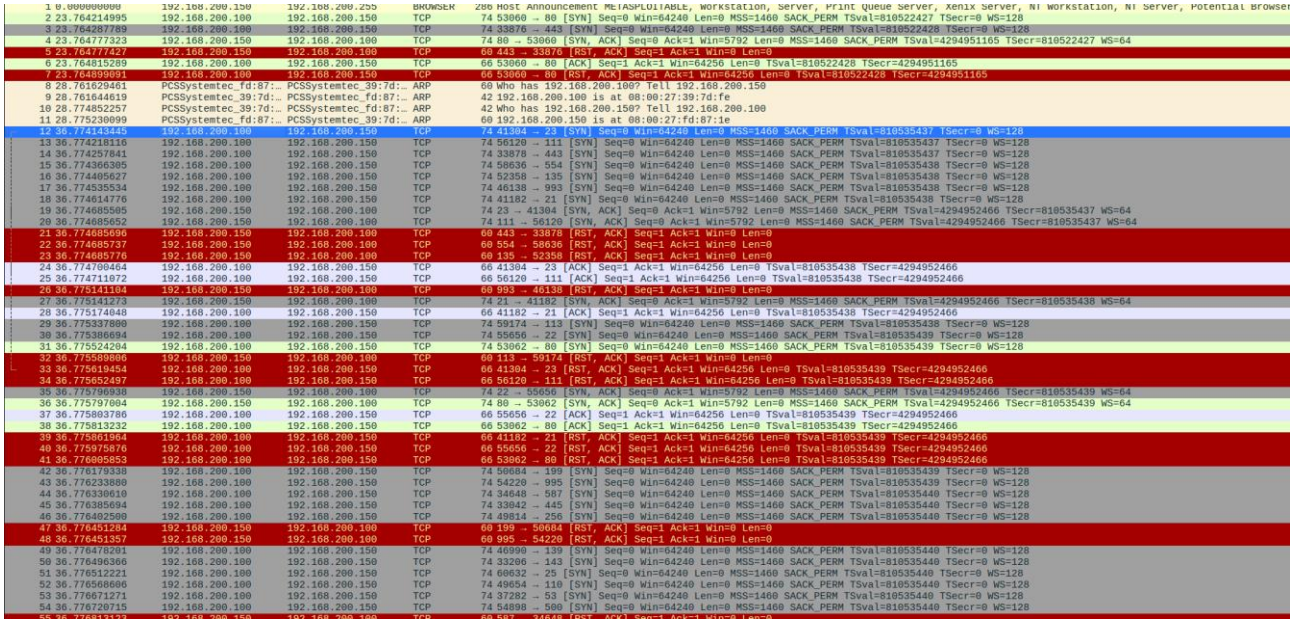
Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. **Analizzate** la cattura attentamente e rispondere ai seguenti quesiti:

- 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

Cattura_U3_W1_L3.pcapng

Al giorno d'oggi le minacce informatiche si evolvono costantemente, l'analisi proattiva è la nostra migliore difesa. Partendo dai concetti di **Threat Intelligence** e **Indicatori di Compromissione**, la traccia di oggi ci porterà nel vivo dell'investigazione. Attraverso una cattura di rete effettuata con l'ausilio di **Wireshark**, cercheremo di svelare le tracce di un'attività malevola. L'obiettivo è quello di individuare gli **IOC**, formulare ipotesi sui potenziali **vettori di attacco** e, infine, proporre azioni concrete per mitigare l'impatto e prevenire le minacce.

Identificazione ed analisi di potenziali IOC



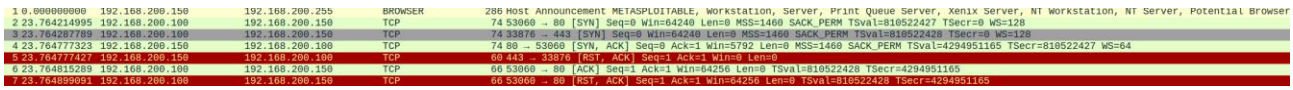
Tramite una prima analisi all'esame di Wireshark fornito, possiamo identificare la macchina con IP 192.168.200.150 come vittima/target e la macchina con IP 192.168.200.100 come attaccante. Si può capire da diversi fattori:

L'annuncio nella prima riga "ANNOUNCEMENT **METASPOITABLE**" è una prova inconfutabile che la macchina .150 è un target vulnerabile creato appositamente per i test.

L'IP .100, in molte righe è la *Source*, sta inviando dei pacchetti con il flag SYN, traducibili in tentativi di apertura TCP a molte porte di .150 che è la *Destination* in rapida successione.

Questo è un comportamento tipico di un **port scanning** (ad esempio **nmap**). In risposta il .150 manda dei RST, ACK che si traducono in rifiuti o servizio non attivo su quella porta. Un altro fattore interessante è l'ordine temporale delle richieste SYN da parte del .100 verso molte porte del .150, queste richieste hanno in comune un intervallo di tempo nelle righe, tipica caratteristica di scanner automatici o tool di enumerazione.

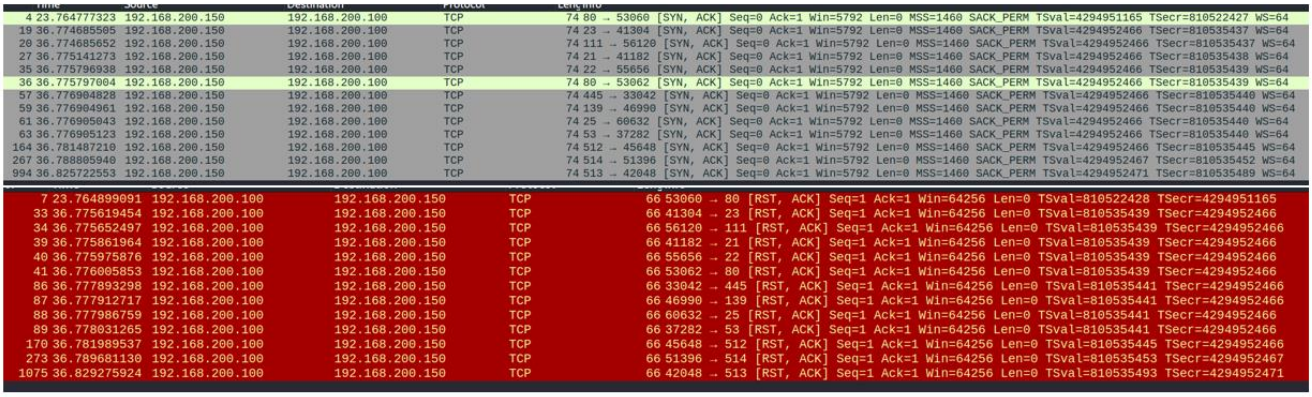
Inoltre possiamo notare che l'attaccante inizialmente prova una scansione completa sulla porta 80 e 443, ricevendo in risposta un SYN, ACK completando il triple-hand-shake sulla porta 80. Successivamente procede con una scansione stealth (Half-open), incrementando la velocità e la copertura delle richieste TCP, effettuando un port scan verso 192.168.200.150 — molti SYN in rapida successione verso porte multiple, con risposte RST/ACK dal target.



(***Quando si ottiene la risposta RST/ACK si traduce in servizio non aperto. Quando invece non si ottiene risposta dopo il SYN quella porta è filtrata***)

Sembrerebbe che l'intenzione dell'attaccante è quella di sondare determinate porte (443,80,445,139,21,22) probabilmente mirando a servizi come http/https, smb e ssh. Tramite **nmap** sarà semplice per l'attaccante ottenere informazioni riguardo ai servizi utilizzati e alle rispettive versioni; questo indica un campanello d'allarme soprattutto se questi servizi non sono stati configurati correttamente e aggiornati con le ultime versione fornite dai ***provider***.

(*Si raccomanda vivamente di eseguire gli aggiornamenti del software e dei sistemi operativi **esclusivamente tramite i canali ufficiali e i link forniti direttamente dai rispettivi provider***)



Consapevoli che la macchina vittima è una Metaspoitable, possiamo subito identificare alcune vulnerabilità note corrispondenti con le porte scannate dall'attaccante:

- **SMB:** Le porte **139** e **445** sono particolarmente vulnerabili in Metasploitable.

  Vulnerabilità EternalBlue: Metasploitable è suscettibile a questa vulnerabilità critica di Windows (CVE-2017-0144), sfruttata dall'exploit EternalBlue della NSA. Questo permette a un attaccante di eseguire codice in remoto sul sistema. È stata resa famosa dall'attacco ransomware globale di WannaCry.

  Accesso anonimo: È possibile ottenere accesso alle condivisioni di file SMB senza credenziali, consentendo all'attaccante di visualizzare o modificare file di sistema sensibili.

- **Apache (Web Server):** Le porte **80** (HTTP) e **443** (HTTPS) sono aperte e indicano un server web.

  Moduli non sicuri: Metasploitable contiene moduli Apache non configurati correttamente o vulnerabili, come **mod_cgi**, che possono consentire l'esecuzione di script malevoli.

  Direttive di configurazione deboli: Le configurazioni predefinite del server web possono esporre informazioni sensibili, come versioni del software e liste di directory.

- **SSH (Secure Shell)**: La porta **22** è vulnerabile a diversi tipi di attacco.

  Attacco Brute Force: Il servizio SSH su Metasploitable è configurato per consentire tentativi di login ripetuti. Questo permette a un attaccante di utilizzare tool automatici per indovinare la password di un utente, come "root", provando un gran numero di combinazioni.

  Credenziali di default: Metasploitable ha credenziali di accesso predefinite e deboli, come msfadmin / msfadmin, che sono facili da indovinare e offrono un punto di ingresso immediato per un attaccante.

Indicatore di compromissione (IOC)

In questo scenario, un potenziale **Indicatore di Compromissione** è l'indirizzo IP **192.168.200.100**, in quanto è la sorgente del traffico anomalo e potenzialmente ostile. L'invio di pacchetti **SYN** in rapida successione verso porte multiple del bersaglio (**192.168.200.150**) è una chiara firma di **port scanning**, una fase di ricognizione di un attacco. L'indirizzo **.100** è costantemente la **sorgente** dei pacchetti che iniziano le connessioni. Questo lo identifica come il sistema che sta attivamente conducendo l'attacco, rendendolo un elemento di rischio immediato.

Sebbene l'indirizzo IP **192.168.200.100** sia l'IOC principale, il tipo di attacco e le vulnerabilità che sta cercando di sfruttare ci forniscono ulteriori IOC specifici.

- **Scansione del protocollo SMB (porte 139, 445):** Il traffico mostra che l'attaccante sta sondando attivamente queste porte, che sono tipicamente utilizzate per la condivisione di file. Questa attività suggerisce che l'attaccante sta cercando vulnerabilità note come **EternalBlue**, spesso presente in sistemi come Metasploitable.

- **Attacco Brute-Force SSH (porta 22):** Visto il particolare interesse da parte dell'attaccante alla porta **22**, un altro indice di compromissione potrebbe essere un numero elevato di tentativi di accesso al servizio ssh, probabilmente dato da un brute-force attack
- **Sondaggio dei servizi web (porte 80, 443):** I tentativi di connessione alle porte **80** (HTTP) e **443** (HTTPS) indicano che l'attaccante sta cercando vulnerabilità in un server web. Un **IOC** in questo caso potrebbe essere una richiesta HTTP che contiene un payload insolitamente lungo o una firma di codice malevolo, che suggerisce un tentativo di **code injection**.

Misure di sicurezza consigliate

Le contromisure consigliate saranno suddivise in tre categorie principali: **difesa immediata**, **prevenzione a lungo termine** e **risposta agli incidenti**.

Difesa Immediata:

- **Blocco dell'IP dell'attaccante:** La prima misura è quella di bloccare l'indirizzo IP di origine dell'attacco (**192.168.200.100**). Questo può essere fatto tramite un **firewall** o una **lista di controllo degli accessi (ACL)**. Il blocco impedisce ulteriori tentativi di scansione o attacco, isolando temporaneamente la minaccia.
- **Attivazione degli alert:** Creare alert basati su volume, comportamento e tipo di pacchetto. Questi alert dovrebbero essere configurati in un **sistema di rilevamento delle intrusioni (IDS)** o in un **SIEM** (*Security Information and Event Management*) per notificare immediatamente il team di sicurezza di attività sospette, come scansioni di rete o tentativi di brute-force.

Prevenzione a Lungo Termine:

- **Patching e Aggiornamenti:** Le vulnerabilità che l'attaccante sta sondando (SMB, SSH, HTTP) sono spesso risolvibili con patch e aggiornamenti. È fondamentale che tutti i servizi di rete siano regolarmente aggiornati per correggere le falle di sicurezza note.
- **Indurimento dei Servizi:**
- **SMB:** Disabilitare il supporto per le versioni obsolete e non sicure del protocollo SMB e bloccare il traffico su alcune porte se non sono strettamente necessarie o inutilizzate.
- **SSH:** Implementare l'autenticazione con una pass-phrase anziché la semplice password. Disabilitare l'accesso root diretto e utilizzare password complesse per tutti gli account. ***E' consigliato bloccare l'IP dopo un massimo di tentativi falliti***
- **Servizi Web:** Assicurarsi che il server web sia configurato correttamente, che non esponga informazioni sensibili (come le versioni del software) e che sia protetto da un **Web Application Firewall (WAF)**.

Risposta agli Incidenti:

- **Analisi Forense:** Una volta che l'attacco è stato mitigato, è necessario condurre un'analisi forense sulla macchina **192.168.200.150** per determinare se la compromissione è avvenuta, identificare i file compromessi e valutare i potenziali danni.
- **Revisione dei Log:** Analizzare i log di sistema e di rete per cercare altre attività sospette che potrebbero essere state compiute dall'attaccante prima del rilevamento.

Con l’implementazione di queste misure sarà possibile fermare l'attacco in corso, e grazie alla prevenzione proposta si potrà rendere il sistema più resiliente e protetto da futuri attacchi.