Federico
Cuccu

Threat Intelligence e analisi IOC con Wireshask

Pratica S9/L5

Obiettivo dell’esercizio

L'obiettivo di questo esercizio è comprendere la natura di un potenziale attacco osservabile dal file .pcapng, un file di Wireshark che ci mostra il log di **tutti gli eventi di connessione TCP** registrati in un determinato lasso di tempo.

Tramite questo file andremo ad:

- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, ipotizzare i vettori di attacco utilizzati

In questo modo possiamo condividere un report di Threat Intelligence per migliorare le difese del sistema aziendale e prevenire / mitigare attacchi futuri simili.

Cos’è la Threat Intelligence

Cos’è la Threat Intelligence

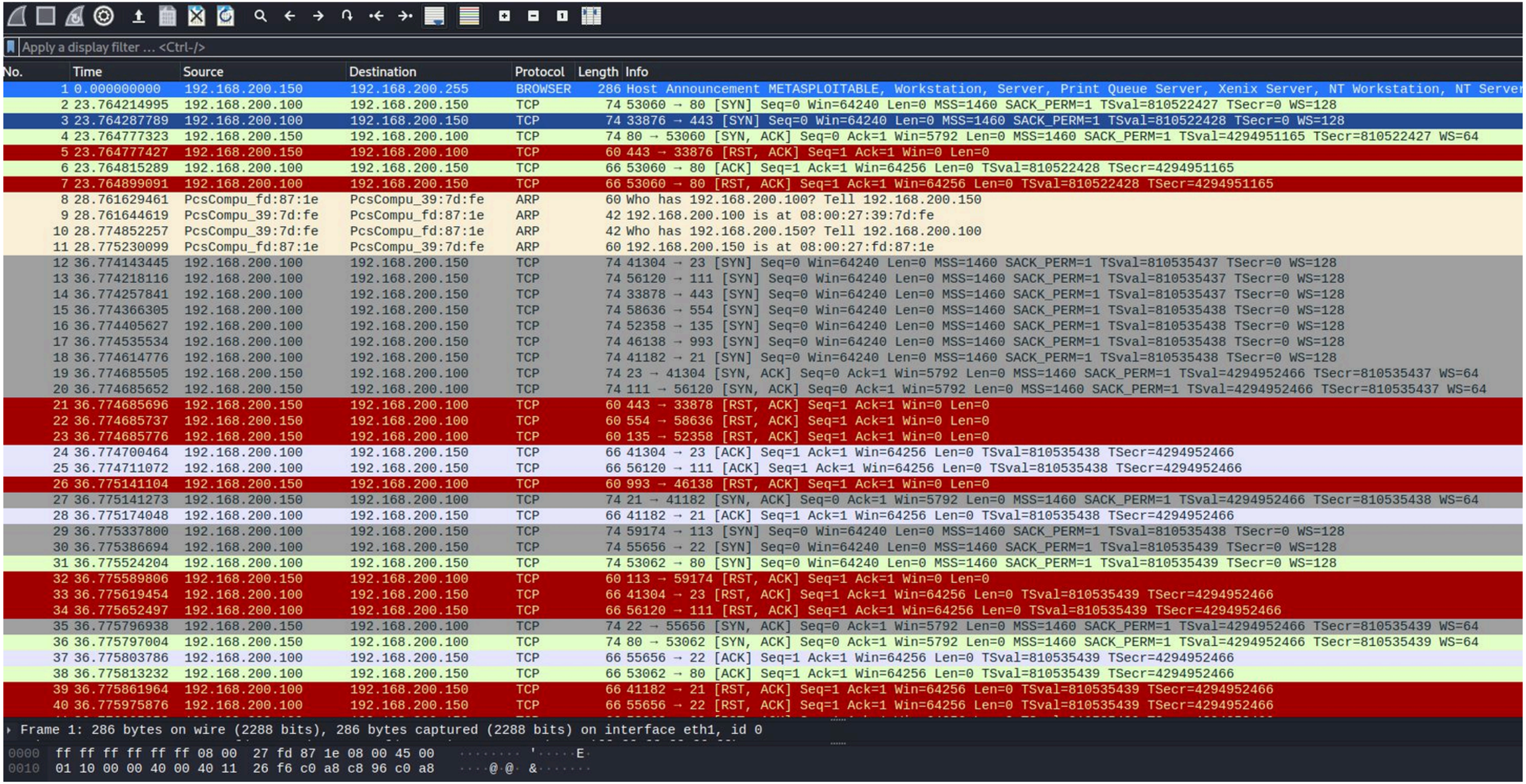
La Threat Intelligence si focalizza sull'**identificazione**, **analisi** e **mitigazione delle minacce**, migliorando la capacità delle organizzazioni di rispondere a eventi malevoli.

Nello specifico, è il processo di **raccolta**, **analisi** e **condivisione** di informazioni riguardanti minacce attuali o potenziali alla sicurezza informatica.

L'obiettivo della TI è è quello di consentire alle organizzazioni di:

- **Comprendere le minacce** che possono colpire l’organizzazione
- Implementare misure di sicurezza proattive per **mitigare i rischi** prima che si concretizzino.
- **Reagire in modo rapido ed efficace** agli incidenti di sicurezza, riducendo l'impatto e accelerando il recupero.

Cattura del traffico TCP tramite Wireshark



Una parte del log della connessione TCP tra i dispositivi coinvolti, su Wireshark.

Indicatori di compromissione

Indicatori di Compromissione (IOC)

Dall'analisi dei log forniti, emergono diversi indicatori:

1. **Elevato numero di pacchetti TCP con flag SYN e RST/ACK**:
   - Osserviamo molte connessioni interrotte con pacchetti TCP aventi il flag RST (Reset). Questo indica che il server di destinazione sta rispondendo negativamente in modo frequente all’attaccante, chiudendo la connessione.

2. **Connessioni incomplete con flag SYN**:
   - Numerosi pacchetti presentano il flag SYN senza completare il processo di handshake.
   - Il pattern può ricordare un SYN Flood, una tecnica comune in attacchi DoS, dove l'aggressore invia una quantità massiva di richieste iniziali (SYN) senza completarle.
   - Il pattern può ricordare anche una scansione SYN (stealth), dove l’attaccante scansiona le porte del server senza mai rispondere con un pacchetto ACK.

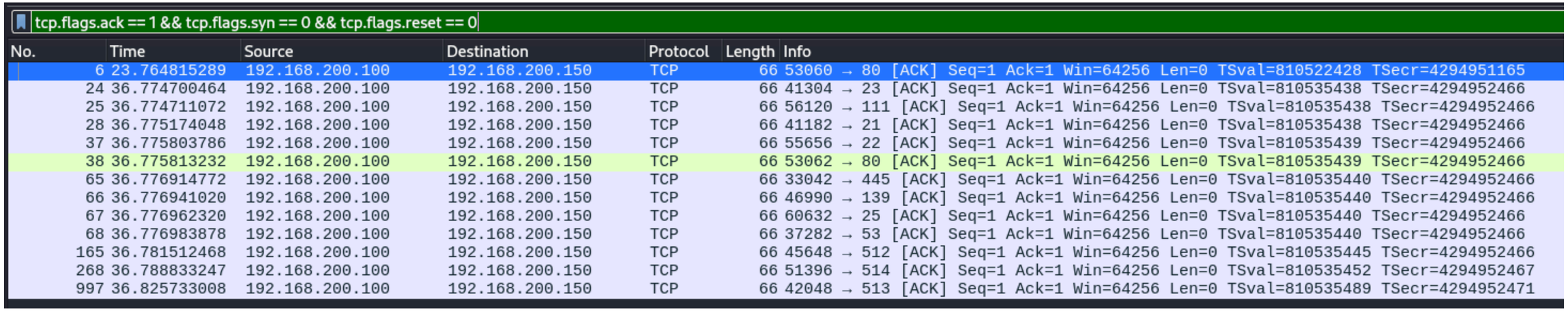
Indicatori di Compromissione (IOC)

3. **Indirizzi IP coinvolti**:
   - IP sorgente (attaccante): 192.168.200.100 - IP destinazione (vittima): 192.168.200.150
   - Entrambi gli indirizzi sono locali, indicando che si tratta di un attacco dall'interno.

4. **Porta di destinazione**:
   - Le porte di destinazione variano continuamente, tra porte note e porte dinamiche, non andando a colpire quindi una porta e un servizio specifico.
   - Può indicare una scansione completa con il parametro -p- per scansionare tutte le porte da 1 a 65535.

Indicatori di Compromissione (IOC)

5. **Presenza di pacchetti ACK**
   - In un attacco DoS, l'attaccante non dovrebbe rispondere con dei pacchetti ACK, in quanto di norma l'obiettivo è quello di mandare in down il servizio, a meno che non sia parte di un attacco più complesso.
   - In una scansione stealth non possono esserci pacchetti ACK, in quanto anche in caso le porte siano aperte, l'attaccante risponde sempre con un pacchetto RST per fare meno "rumore" a livello di rete.



Indicatori di Compromissione (IOC)

5. **Connessioni non permanenti**
   - Ogni connessione viene chiusa poco dopo con un pacchetto RST, di conseguenza l'attaccante non esegue mai accesso a dei servizi aperti (come ftp o telnet).
   - In caso di connessione permanente, ad esempio sulla porta ftp, avremo notato diversi pacchetti tutti inviati/ricevuti sulla stessa porta, dimostrando dunque che l'attaccante sta eseguendo diverse azioni su quel servizio.

6. **Protocollo ARP**
   - Oltre all'indirizzo IP privato, abbiamo la doppia conferma che l'attaccante è all'interno della rete in quanto il protocollo ARP agisce tra il livello 2 e il livello 3 del modello ISO/OSI e associa IP e indirizzi Mac, che vengono utilizzati solamente all'interno della rete locale. Non sono presenti tracce di ARP poisoning.

Ipotesi sui vettori di attacco

Vettore di attacco

Basandosi sugli IOC rilevati, l'attacco osservato non è un vero e proprio attacco, bensì una **scansione non stealth mirata sul dispositivo vittima**.

L'attaccante ha utilizzato una scansione come questa: `nmap -sT -p-`, che sfrutta interamente il three-way handshake previsto dal protocollo TCP.

Questo tipo di scansione, completa la connessione TCP (SYN, SYN/ACK, ACK) con ogni porta aperta, rendendola facilmente rilevabile nei log.

Per quanto riguarda le porte chiuse, invece, il server invierà un pacchetto RST come risposta subito dopo il SYN.

Vettore di attacco

Inoltre con il parametro **-p-** l'attaccante scansiona tutta le porte, da 1 a 65535, anziché solo le porte note, risultando in una scansione più aggressiva.

È importante sottolineare anche la **quantità di pacchetti** tra il dispositivo attaccante e il dispositivo vittima, ovvero nella norma in una scansione di questo tipo, e di gran lunga inferiore a quello che sarebbe stato un ipotetico attacco DoS.

È comunque un **atteggiamento sospetto**, dato che la scansione è un prerequisito fondamentale che precede la fase di attacco.

Sono necessarie dunque maggiori indagini sull'avvenimento, insieme a delle limitazioni per mitigare questa possibile minaccia.

Azioni di mitigazione

Azioni di mitigazione

Per gestire efficacemente la scansione rilevata, è essenziale adottare contromisure che limitino l'azione dell'attaccante senza interferire con le normali attività lavorative.

1. **Miglioramento delle regole del firewall**:
   - La configurazione del firewall è fondamentale: è possibile limitare la frequenza delle richieste TCP, oppure bloccare le richieste sulle porte a cui il dispositivo non può avere accesso.

2. **Isolamento logico**:
   - Se la rete è suddivisa in VLAN, si può inserire il dispositivo sospetto in una VLAN dedicata con regole di accesso più restrittive, permettendo solo l'accesso ai servizi necessari per il suo ruolo, fino al termine dell’indagine.

Azioni di mitigazione

3. **Installazione di dispositivi di rilevamento delle intrusioni**:
   - Sebbene non prevenga direttamente una scansione come quella rilevata, un IDS può analizzare i pacchetti nel traffico e confrontarli con un database alla ricerca di attività malevola, lanciando l'allarme.
   - L'IPS, oltre a lanciare l'allarme, blocca in autonomia il traffico malevolo, ma potrebbe ridurre l'accessibilità al sistema e bloccare il lavoro di uno o più dipendenti temporaneamente.

4. **Formazione del personale**:
   - Sensibilizzare il personale sull'uso improprio degli strumenti di rete, spiegando le possibili conseguenze di attività come scansioni o altre attività di rete non autorizzate.

Azioni di mitigazione

5. **Verifica del dispositivo**:
   - Analizzare il dispositivo in questione per verificare la presenza di software o strumenti potenzialmente pericolosi.
   - Analizzare i log presenti sul dispositivo utilizzato per la scansione per ricercare ulteriori indizi sulle eventuali intenzioni dell’attaccante.

Conclusioni

Conclusioni

L'analisi del traffico ha rivelato una scansione non stealth mirata. L'attività, proveniente da un dispositivo interno, indica un **intento esplorativo sospetto**, ma non ha compromesso servizi o iniettato pacchetti malevoli.

Le azioni di mitigazione mirano a migliorare le regole del firewall, isolare il dispositivo sospetto, utilizzare strumenti di rilevamento delle intrusioni e sensibilizzare il personale sull'uso appropriato delle risorse di rete.

L'evento sottolinea l'importanza di **monitorare e rispondere prontamente** ai comportamenti anomali, bilanciando la sicurezza con la continuità operativa. Sarà essenziale indagare ulteriormente le motivazioni del responsabile per prevenire futuri incidenti.