Esercizio settimanale.

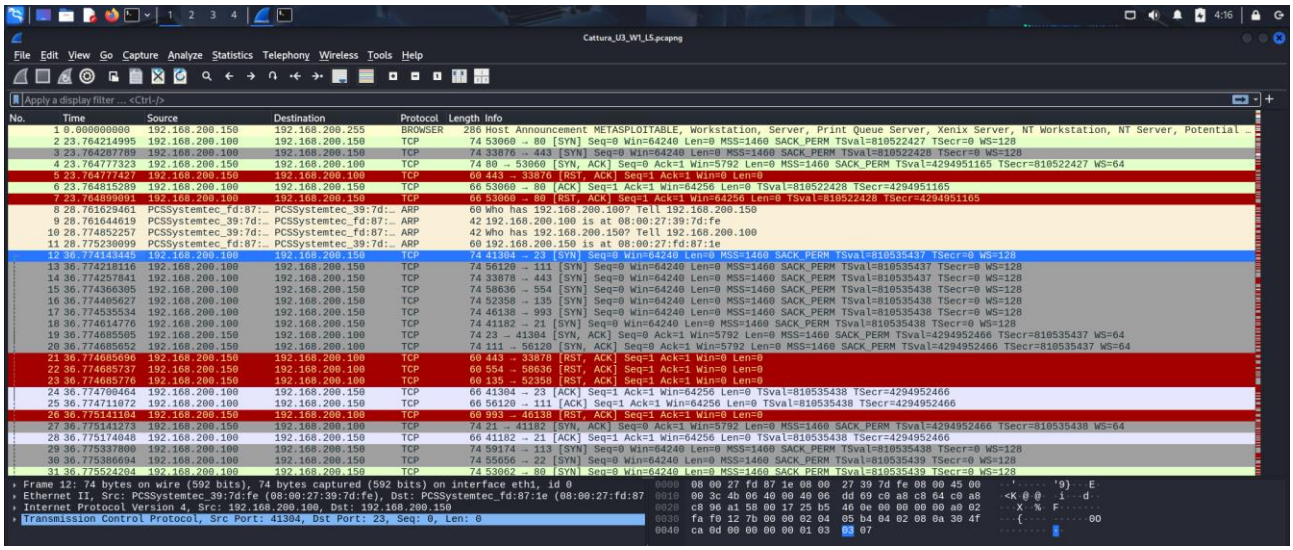
Threat Intelligence & IOC.

Traccia: Analizzate la cattura attentamente con wireshark

Obiettivi:

- 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.

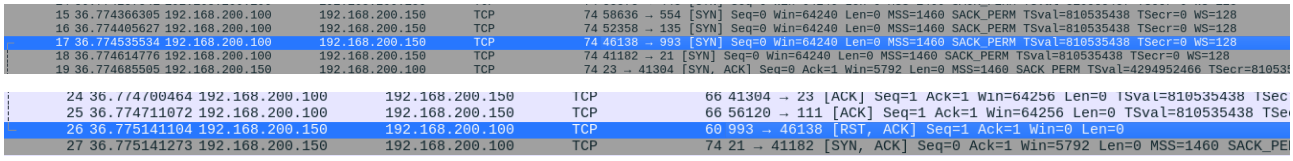
1) Importiamo la cattura sulla macchina Kali Linux.



2) Analisi preliminare della cattura.

In base ad una prima analisi, la cattura mostra un tipo di scansione delle porte attraverso l'uso di nmap -sT -p- in quanto risultano segnali di una connessione TCP completa.

Una scansione TCP connect (-sT) tenta di stabilire una connessione TCP con ogni porta della macchina target e alle porte ed aspetta una risposta. Essa completa l'handshake a tre vie.



Di per sé questo tipo di scansione non è un attacco vero e proprio in quanto non compromette il sistema ma è decisiva per trovare eventuali porte aperte e servizi attivi da sfruttare. Il fatto che non ci sia la rate limiting per quanto riguarda il numero di pacchetti SYN che possono essere ricevuti, espone

il server a pericoli di attacchi Denial of Service (DoS) e Distribuited Denial of Service (DDoS) di tipo SYN flood o reset flood.

3) Attacco SYN flood.

Il SYN flood è un tipo di attacco che sfrutta il protocollo TCP. L'attaccante invia un flusso continuo di pacchetti SYN senza mai completare l'handshake a tre vie utile per stabilire una connessione TCP.

Il server resta inutilmente in attesa di una risposta da queste connessioni semiaperte compilando le tabelle di sessione e saturando le risorse di sistema.

Spesso i pacchetti di SYN provengono da indirizzi IP falsificati, rendendo difficile il tracciamento dell'attaccante e il loro invio massiccio può causare il blocco del server, rendendolo non disponibile agli altri utenti legittimi.

4) Attacco reset flood.

L'attacco reset flood è un tipo di attacco che sfrutta l'uso di pacchetti reset del protocollo TCP per chiudere in modo imprevisto e forzato la connessione.

L'interruzione del tentativo della connessione e le risorse richieste per provare a ristabilirla causano il rallentamento o il blocco del server, rendendo il servizio non disponibile.

5) IoC (Indicatori di compromissione).

Nella cattura possono essere riscontrati diversi IoC (indicatori di compromissione):

- L'invio massiccio di richieste di connessione TCP su molteplici porte diverse;
- Il fatto che le richieste siano state inviate in successione e con intervalli di tempo ravvicinati;
- Il completamento dell'handshake a tre vie che mostra l'effettiva connessione riuscita.

6) Azioni consigliate.

Le azioni di mitigazione che possono essere intraprese:

- Rate limiting: limitare la ricezione del numero di pacchetti SYN da una singola sorgente;
- Impostare regole di Firewall per impedire l'attacco SYN flood/RST flood;
- Implementare dispositivi di sicurezza come IDS/IPS per rilevare e bloccare il traffico dannoso;
- Tecnica SYN cookies nella quale il server invia un cookie nel pacchetto SYN-ACK invece di allocare immediatamente le risorse.