Threat Intelligence & IOC

Profilo studente

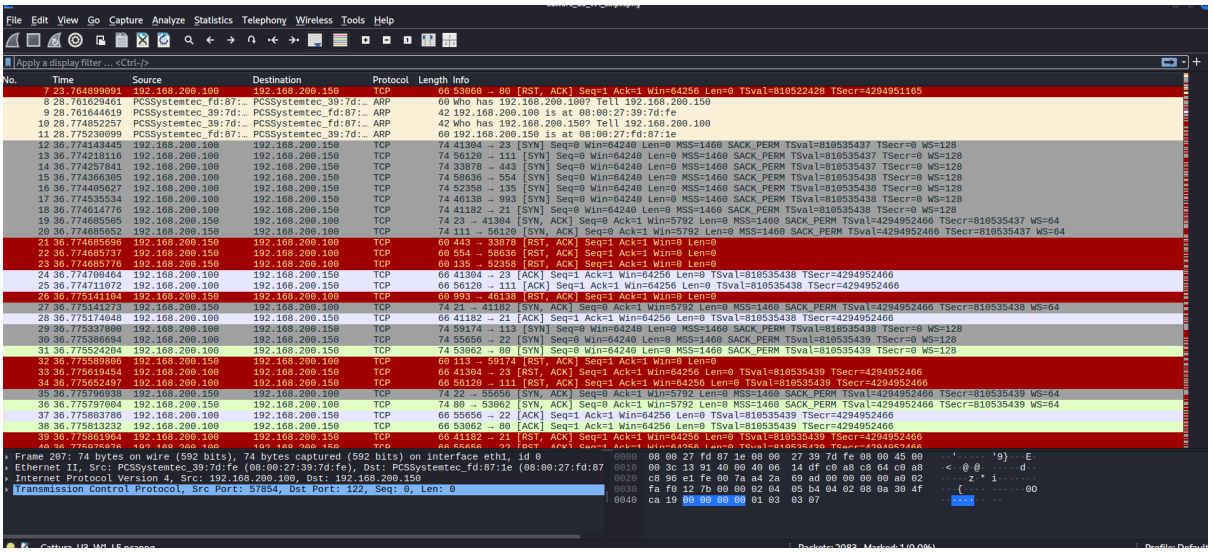
data:03/02/2026
studente: Gabriel Giustinelli 15/06/2004
Epicode classe: CS0525
Cyber Security Specialist

Obiettivo

In questo progetto ha l'obiettivo di analizzare il traffico di dati catturato di **Cattura_U3_W1_L3.pcapng** a noi affidato per identificare eventuali o potenziali minacce alla sicurezza del perimetro della macchina sottostante.
Il lavoro quindi si basa sull'analisi di dati grezzi per estrarre informazioni utili per mitigare o prevenire attacchi informatici.

Metodologia di Analisi

Tramite lo strumento di visualizzazione **Wireshark** possiamo condurre l'analisi dei pacchetti, andando a focalizzarsi sulla ricerca di eventuali indicatori di compromissione (**IOC**).
Il nostro compito di analisi comprende l'ispezione dei protocolli, l'analisi comportamentale e la valutazione dell'impatto .



1. Identificazione e analisi degli IOC

Dall'ispezione dei pacchetti sono stati rilevati i seguenti elementi critici:

1.1 Identificazione dell'attaccante e del target:

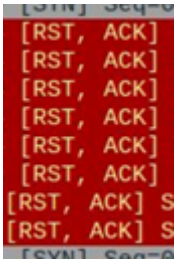
Nel primo pacchetto l'intercettazione del **protocollo BROWSER** ha rivelato **l'hostname** della vittima **"METASPLOITABLE"** questo è un dato fondamentale poiché identifica la macchina target orientando l'attaccante verso exploit delle vulnerabilità note.

- **IP sorgente:** 192.168.200.100
- **IP destinazione:** 192:168.200.150

1.2 Analisi del comportamento:

- **Scan aggressivo:** Dai dati è emersa una massiccia raffica di pacchetti con flag **[SYN]** diretti a porte sequenziali non standard.

- **Analisi risposte:** La costante presenza di risposte con flag **[RST,ACK]** evidenziate in rosso ci dice che l'host di destinazione sta rifiutando le connessioni su porte chiuse.



Lo scambio indica che tra i due host non è presente alcun firewall con politiche di dropping attivo, permettendo così una scansione libera.

- **Enumerazione servizi:** La presenza di traffico NBNS (NetBios Name Service) conferma che l'attaccante non sta solo cercando le porte aperte, ma sta cercando di trovare i nomi dei servizi e dei gruppi di lavoro per mappare la gerarchia della rete locale.

Sintesi dei Risultati

L'analisi ha permesso di rilevare un'attività di **ricognizione** ostile proveniente dall'IP **`192.168.200.100`**. L'attaccante invia un pacchetto **SYN** a migliaia di porte diverse in sequenza rapidissima senza mai concludere l'handshake a tre vie il che lo rende meno tracciabile, il sistema operativo risponde con un **RST** per chiudere immediatamente il tentativo di richiesta su porte chiuse. La prevalenza di questi pacchetti indica che l'attaccante sta effettuando un **brute-force di porte**, cercando di capire quali sono le porte aperte.

2. Ipotesi sui Vettori di Attacco e Metodologia

Sulla base dei dati raccolti, l'attacco è classificabile come una fase di **Ricognizione attiva ed aggressiva:**

1. **Vettore Principale:** Sfruttamento di falle nei servizi di rete (Network Service Exploitation).

2. **Automatizzazione:** La velocità dei millisecondi dell'invio dei pacchetti (nella colonna **Time**) e la graduazione numerica delle porte indicano l'uso di tool automatizzati come **Nmap** o il framework **Metasploit**.

3. **Strategia dell'Attaccante:** L'attaccante sta eseguendo un "**OS Fingerprinting**" e una mappatura dei servizi per identificare vettori di ingresso specifici **(**come backdoor o servizi obsoleti tipici dei sistemi Metasploitable**)** per una s**uccessiva fase di Exploitation**.

3. Piano di Mitigazione e Azioni Correttive

Per neutralizzare la minaccia e innalzare il livello di sicurezza, si propongono le seguenti misure:

- **Contenimento Immediato:** Implementazione di una regola di filtraggio (**ACL**) sul firewall per il blocco totale del traffico proveniente dall'IP **`192.168.200.100`**.

- **Rate Limiting:** Configurazione di soglie di rate limiting per le connessioni **SYN** entranti, al fine di mitigare gli effetti di scansioni massive e prevenire potenziali Denial of Service (DoS) sulle tabelle di stato dei servizi.

- **Network Hardening:** Disabilitazione dei protocolli legacy (**NetBIOS/LLMNR**) e configurazione del sistema affinché **non risponda** con pacchetti **RST** alle porte chiuse, adottando una **politica di "Silent Drop"** per rendere l'host invisibile agli scanner automatici.

- **Isolamento degli Asset Critici:** Spostamento di macchine vulnerabili (come Metasploitable) in reti isolate (VLAN dedicata) senza connettività verso gli asset di produzione.

5. Conclusioni

L'analisi dimostra che il monitoraggio tramite Wireshark consente di intercettare le fasi preparatorie di un attacco informatico.

L'identificazione precoce dei pattern di scansione e dell'enumerazione dei servizi è essenziale per implementare contromisure efficaci prima che l'attaccante possa procedere alla fase di infiltrazione vera e propria.