REPORT S9/L5

Obiettivo: 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.

SVOLGIMENTO

Pacchetti TCP con flag RST

Osservando le immagini si può notare una quantità elevata di pacchetti TCP (evidenziati in rosso) inviati tra gli IP 192.168.200.100 e 192.168.200.150.
L'alta quantità di pacchetti RST indica che uno degli host sta cercando attivamente di chiudere le connessioni, questo comportamento potrebbe essere dovuto a un tentativo di evasione da parte di un attaccante o a una misura difensiva adottata da un IDS/IPS in risposta a un attacco.
Un'altra possibile spiegazione è che una scansione delle porte stia cercando di stabilire connessioni, ma venga costantemente bloccata.

Anomalie nel traffico ARP

Nella prima immagine si possono osservare pacchetti ARP scambiati tra gli indirizzi IP 192.168.200.100, 192.168.200.150 e altri dispositivi con alcune richieste che sembrano sospette
Se questi pacchetti sono risposte ARP non richieste o richieste dirette a indirizzi non autorizzati si potrebbe trattare di un tentativo di Spoofing, tecnica spesso utilizzata per intercettare il traffico tra un host e il gateway. Un comportamento simile potrebbe anche segnalare un possibile attacco Man-in-the-Middle in cui un attaccante cerca di

intercettare e manipolare le comunicazioni tra due dispositivi all’interno della rete.

Indirizzi IP sospetti nella rete interna

Il traffico tra 192.168.200.100 e 192.168.200.150 mostra un numero insolito di pacchetti SYN seguiti da RST e ACK, il che potrebbe indicare una scansione delle porte.
L’host 192.168.200.150 sta rifiutando attivamente le connessioni segno che potrebbe esserci un firewall che sta bloccando il traffico.

Pacchetti contenenti dati potenzialmente anomali o sospetti

Alcuni pacchetti hanno lunghezza anomala (74 bytes, 66 bytes) che potrebbero far pensare a possibili scansioni o attacchi flood.

Bloccare l’attacco in corso

Se l’host 192.168.200.100 sta conducendo l’attacco o è compromesso bisogna bloccare temporaneamente la sua comunicazione nella rete tramite firewall e attivare il logging del traffico anomalo per analizzare i pacchetti inviati e ricevuti dall’IP sospetto individuando eventuali pattern malevoli.

Prevenire attacchi futuri

Per prevenire attacchi futuri, è fondamentale implementare un sistema di rilevamento e prevenzione delle intrusioni (IDS/IPS) per monitorare il traffico di rete e bloccare eventuali attività sospette. Inoltre, è utile limitare la velocità delle connessioni TCP, impostando restrizioni sulla frequenza delle connessioni simultanee dallo stesso indirizzo IP per prevenire attacchi di tipo flood o scansioni aggressive.
Se un dispositivo all'interno della rete risulta compromesso, è importante isolarlo temporaneamente e analizzare i log di sistema per individuare l'origine dell'attacco. Infine, è consigliabile effettuare un analisi delle vulnerabilità della rete per verificare se altri dispositivi interni sono

esposti a rischi di sicurezza, controllando i servizi aperti e possibili punti deboli.

BONUS

Possibili vulnerabilità

Il software sviluppato in C99 potrebbe essere vulnerabile a diversi tipi di attacchi, tra cui buffer overflow e injection attack, se il codice non è stato scritto seguendo pratiche di sicurezza avanzate, potrebbe rappresentare un punto di ingresso per gli attaccanti. Inoltre, anche se la partizione del sistema operativo è bloccata, un attaccante con accesso fisico al dispositivo potrebbe tentare di avviare il sistema da un supporto alternativo.
La presenza di porte USB attive, nonostante il blocco delle pendrive, lascia aperta la possibilità di attacchi tramite dispositivi rogue, come tastiere USB modificate o Rubber Ducky, che potrebbero eseguire comandi malevoli compromettendo la sicurezza del sistema.

Proposte di sicurezza

Per migliorare la sicurezza del software, è importante adottare misure efficaci contro i buffer overflow nel codice C99, la validazione degli input è altrettanto essenziale, utilizzare funzioni più sicure e controllare sempre i dati in ingresso può prevenire vulnerabilità.
Il software di gestione dovrebbe essere isolato limitando i permessi di accesso ai file critici nella seconda partizione mentre per proteggere l'accesso fisico al sistema, è consigliabile bloccare qualsiasi dispositivo USB non autorizzato tramite il controllo degli ID hardware. Inoltre, per impedire avvii da supporti esterni, bisogna disabilitare il boot da dispositivi non autorizzati e proteggerlo con una password.

Progetto di sistema di monitoraggio del traffico

Soluzione più economica (500€)
Hardware: Raspberry Pi 5 (circa 100€)
Software: Suricata (IDS/IPS open-source)
Il Raspberry Pi viene collegato a uno switch in modalità mirroring analizzando tutto il traffico in tempo reale.

Soluzione più costosa(2500€)
Hardware: Firewall come pfSense Netgate o Fortinet FortiGate (1500-2000€)
Software: IDS/IPS avanzato con funzioni di deep packet inspection e analisi AI.
Il firewall viene posizionato tra la rete del cliente e il macchinario analizzando e filtrando il traffico sospetto.

*Nei prezzi sono comprese anche le spese relative alla configurazione, installazione e montaggio del sistema.