Esercizio S9-L3

Traccia:

Analizzare la cattura di Wire Shark e rispondere ai seguenti quesiti:

- Identificare 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.

IOC Analizzati:

Con l'analisi del file wireshark notiamo che la scansione e una **Router-based Monitoring** e gli IOC che ci permettono di notare ciò sono i seguenti:

1. Vengono inviati più pacchetti TCP/SYN da vari indirizzi IP sorgente a diverse porte di destinazione su 192.168.200.150.
2. Il target risponde con pacchetti SYN-ACK per alcuni dei pacchetti SYN in ingresso, indicando che sta cercando di stabilire una connessione TCP.
3. Tuttavia, nella maggior parte dei casi, l'attaccante invia pacchetti RST (reset) immediatamente dopo aver ricevuto i pacchetti SYN-ACK, il che impedisce l'instaurazione di una connessione TCP completa.

Vettori di attacco utilizzati:

Possiamo da ciò dedurre che il target stia subendo una scansione su diverse porte o che si può trattare di un attacco DoS.

Consigli e conclusioni:

Si possono adottare misure per mitigare questi attacchi:

1. Implementare regole nella policy dei firewall;
2. Limitare la velocità dei pacchetti SYN;
3. Implementare sistemi di prevenzione delle intrusioni (IPS o IDS).