REPORT MONITORAGGIO

ATTACCANTE: 192.168.200.100
TARGET VITTIMA: 192.168.200.150

TIPO DI ATTACCO: Scansione delle porte

Parrebbe che l'attaccante stia effettuando un attacco Dos di tipo Syn Flood, ma si è esclusa tale analisi per la dimensione dei pacchetti non coerenti con la dimensione di un tipico payload. Infatti da un'analisi più dettagliata, l'attaccante sta facendo una scansione di tipo Syn Scan per comprendere quali porte siano aperte.
Nello specifico l'attaccante sta inviando pacchetti di tipo SYN a diverse porte della macchina target. Se l'attaccante riceve come risposta un SYN-ACK, allora il servizio su quella porta sarà in ascolto.

In caso contrario riceverà un RST-ACK.

Dall'analisi dei pacchetti inviati dalla macchina target, si riscontra che le porte in ascolto siano le seguenti:

80, 23, 111, 22, 445, 139, 25, 53, 512, 514, 513.

Nello specifico si può dedurre che la macchina target sia una Windows Server, in quanto sono presenti i servizi tipicamente associati alle relative porte.

Porta	Protocollo	Descrizione breve
80	TCP	**HTTP**
23	TCP	**Telnet**
111	TCP/UDP	**RPCbind / Portmapper**
22	TCP	**SSH**
445	TCP	**Microsoft-DS (SMB over TCP)**
139	TCP	**NetBIOS Session Service**
25	TCP	**SMTP**
53	TCP/UDP	**DNS**
512	TCP	**exec**
514	TCP/UDP	**syslog**
513	TCP	**login**

MITIGAZIONE

Un SYN scan è un tipo di scansione usata dagli strumenti come **nmap** per vedere quali porte sono aperte su un sistema. In questa scansione, l'attaccante invia pacchetti **SYN** e aspetta la risposta (SYN-ACK o RST) per capire se la porta è aperta, chiudendo poi la connessione senza completarla.

1) Firewall

Usare un firewall per bloccare pacchetti SYN in ingresso alle porte non necessarie.

2) Port Knocking o Port Security

Tecniche come il **port knocking** possono nascondere porte sensibili finché un client legittimo non "bussa" con pacchetti speciali. Sui dispositivi di rete, implementare il **port security** per limitare la connessione a dispositivi autorizzati.

3) IDS/IPS

Strumenti di IDS/IPS rilevano scansioni SYN sospette e possono bloccare l'IP dell'attaccante.

4) Aggiornamenti di sistema

Mantenere i sistemi sempre aggiornamenti secondo le direttive dei vendor

Screenshot di preconfigurazione della macchina per lo svolgimento dell’esame pratico: