

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.

tcp.stream eq 2					
No.	Tim	Source	Destination	Protocol	Length Info
12	3...	192.168.200.100	192.168.200.150	TCP	74 41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
19	3...	192.168.200.150	192.168.200.100	TCP	74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=
24	3...	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=81
33	3...	192.168.200.100	192.168.200.150	TCP	66 41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSV

In caso contrario riceverà un RST-ACK.

tcp.stream eq 23					
No.	Tim	Source	Destination	Protocol	Length Info
56	3...	192.168.200.100	192.168.200.150	TCP	74 51534 → 487 [SYN] Seq=0 Win=64240
69	3...	192.168.200.150	192.168.200.100	TCP	60 487 → 51534 [RST, ACK] Seq=1 Ack=1

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:

```
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# cd /media

(root@kali)-[/media]
# ls
sf_Cartella_condivisa_esame

(root@kali)-[/media]
# cd sf_Cartella_condivisa_esame

(root@kali)-[/media/sf_Cartella_condivisa_esame]
# ls
Cattura_U3_W1_L5.pcapng
```

```
(root@kali)-[/media/sf_Cartella_condivisa_esame]
# ls -la
total 212
drwxrwx--- 1 root vboxsf  0 May 30 05:53 .
drwxr-xr-x 3 root root   4096 May 30 05:55 ..
-rwxrwx--- 1 root vboxsf 209024 May 30 03:10 Cattura_U3_W1_L5.pcapng

(root@kali)-[/media/sf_Cartella_condivisa_esame]
# mv Cattura_U3_W1_L5.pcapng /home/kali/Desktop

(root@kali)-[/media/sf_Cartella_condivisa_esame]
# cd /home/kali/Desktop

(root@kali)-[/home/kali/Desktop]
# chmod ugo+rw Cattura_U3_W1_L5.pcapng

(root@kali)-[/home/kali/Desktop]
# chown kali Cattura_U3_W1_L5.pcapng

(root@kali)-[~/kali/Desktop]
#
```

