

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 targetinput
- 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

The screenshot displays a Kali Linux terminal window on the left and a Wireshark network capture window on the right. The terminal shows the execution of a Python script named `client_server.py` which performs a UDP flood attack. The user has entered the target IP `192.168.32.100` and port `80`, and specified `10` packets. The terminal output shows the script sending UDP packets to the target.

The Wireshark window shows the captured network traffic. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_cb:7e:f5		ARP	44	Who has 192.168.117.109
2	0.005580732	e2:f7:20:24:8b:71		ARP	62	192.168.117.109
3	0.255396564	192.168.117.109	192.168.32.100	TCP	76	49582 → 80 [S
4	6.681525134	e2:f7:20:24:8b:71		ARP	62	Who has 192.168.117.109
5	6.682875279	e2:f7:20:24:8b:71		ARP	62	Who has 192.168.117.109
6	6.683750510	e2:f7:20:24:8b:71		ARP	62	Who has 192.168.117.109
7	13.271666739	192.168.117.109	192.168.117.159	DHCP	344	DHCP Request
8	19.700632390	192.168.117.109	192.168.117.159	DHCP	344	DHCP Request
9	24.831296735	PcsCompu_cb:7e:f5		ARP	44	Who has 192.168.117.109
10	24.836494003	e2:f7:20:24:8b:71		ARP	62	192.168.117.109
11	25.525050037	e2:f7:20:24:8b:71		ARP	62	Who has 192.168.117.109
12	33.927199660	192.168.117.109	192.168.117.159	DHCP	344	DHCP Request
13	48.775273062	192.168.117.109	192.168.117.159	DHCP	344	DHCP Request
14	48.778136156	e2:f7:20:24:8b:71		ARP	62	Who has 192.168.117.109
15	48.779446433	e2:f7:20:24:8b:71		ARP	62	Who has 192.168.117.109

The packet details pane for the first packet (Frame 1) shows:

- Frame 1: 44 bytes on wire (352 bits)
- Linux cooked capture v1
- Address Resolution Protocol (request)

The packet bytes pane shows the raw data: `0000 00 04 00 01 00 06 08 00 27 cb 7e f5 00 00 08 06 0010 00 01 08 00 06 04 00 01 08 00 27 cb 7e f5 c0 a8 0020 75 6d 00 00 00 00 00 00 c0 a8 75 9f`