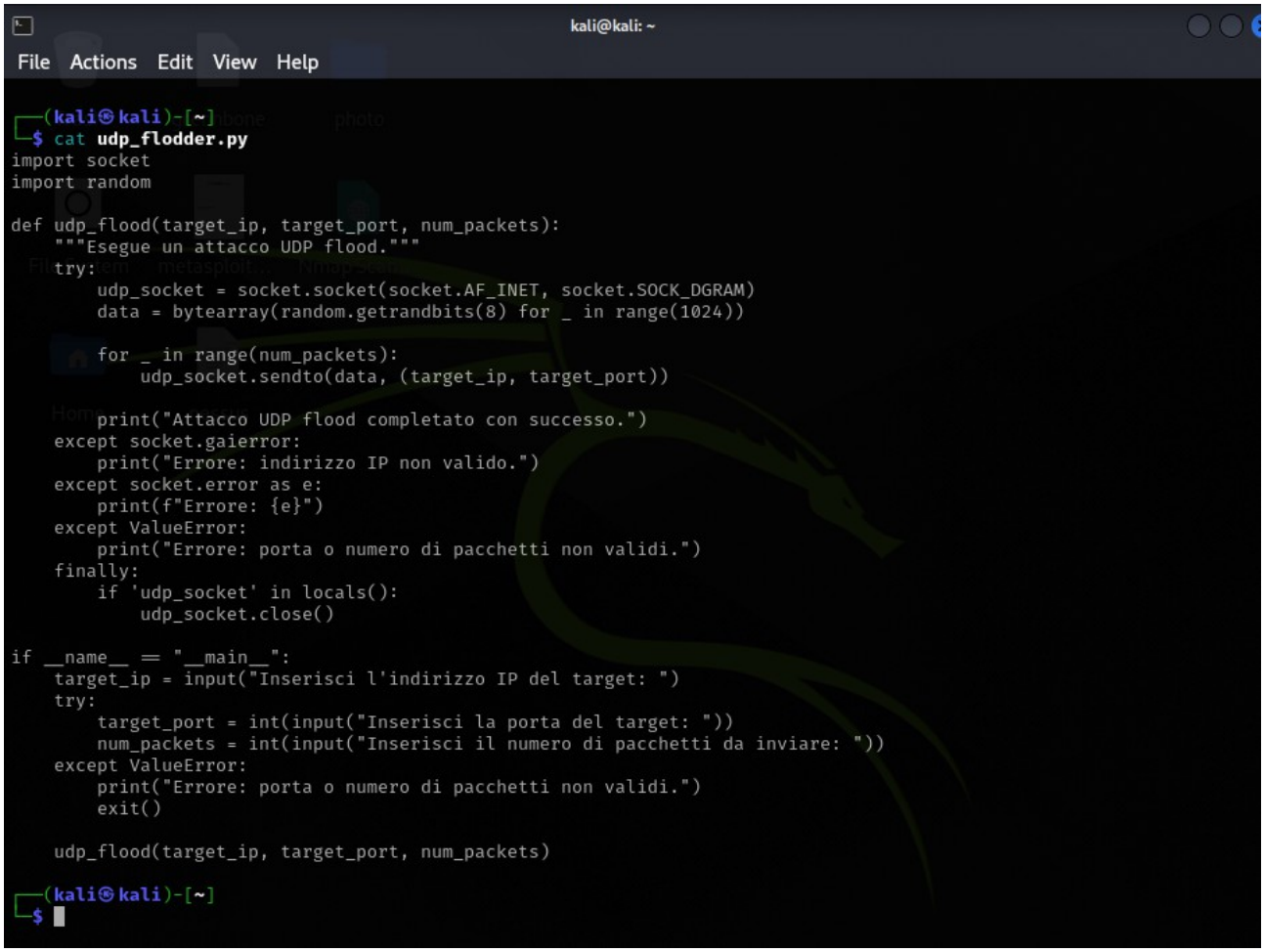
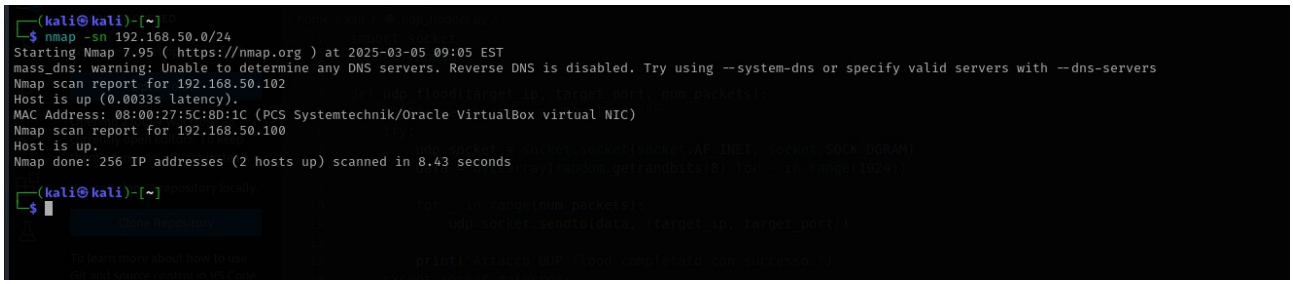
## Simulazione di un UDP Flood

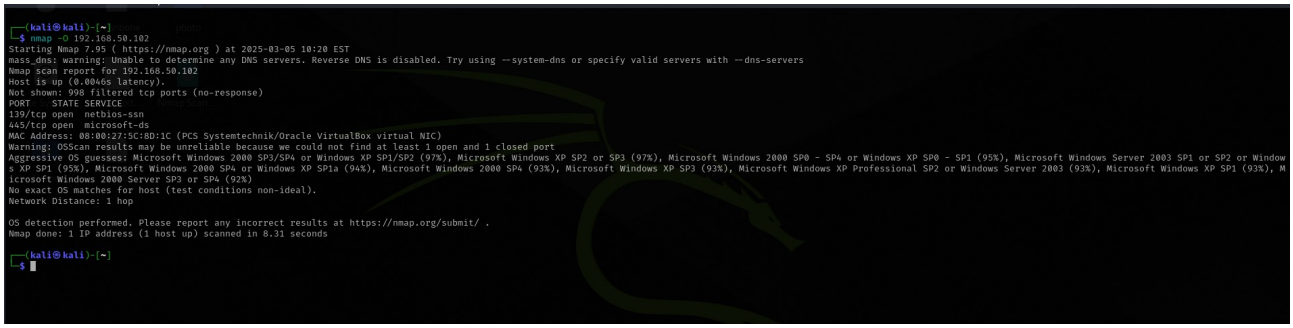
Per simulare un attacco UDP Flood utilizzeremo due macchine, Kali Linux da cui partirà l'attacco e Windows XP come macchina target.
Prima di tutto prepariamo il programma in Python che utilizzeremo per effettuare l'attacco



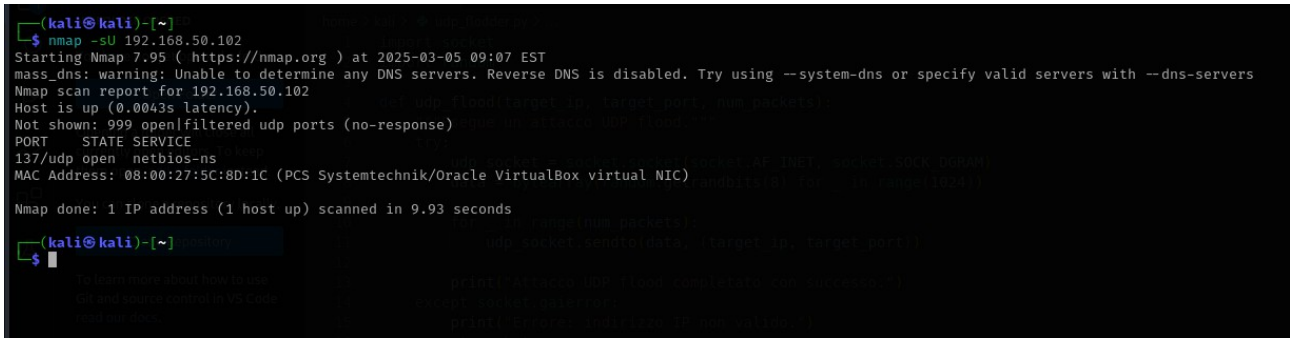

Il codice implementa un attacco UDP flood che consiste nell'inviare un gran numero di pacchetti UDP casuali a un target specificato, con l'obiettivo di sovraccaricarlo e renderlo non disponibile.L'utente inserisce l'indirizzo IP e la porta del server bersaglio, e il numero di pacchetti da inviare. Il programma crea un socket UDP, genera un pacchetto di dati casuali di 1 KB, invia il pacchetto UDP al server bersaglio, ripetendo l'operazione per il numero di pacchetti specificato dall'utente, dopo di chechiude il socket UDP.
Prima di effettuare l'attacco cerchiamo l'indirizzo IP del target sulla rete 50 col comando **nmap -sn 192.168.50.0/24**. Da qui vediamo che sono presenti due host, il nostro, cioè il 100 ed il target, il 102



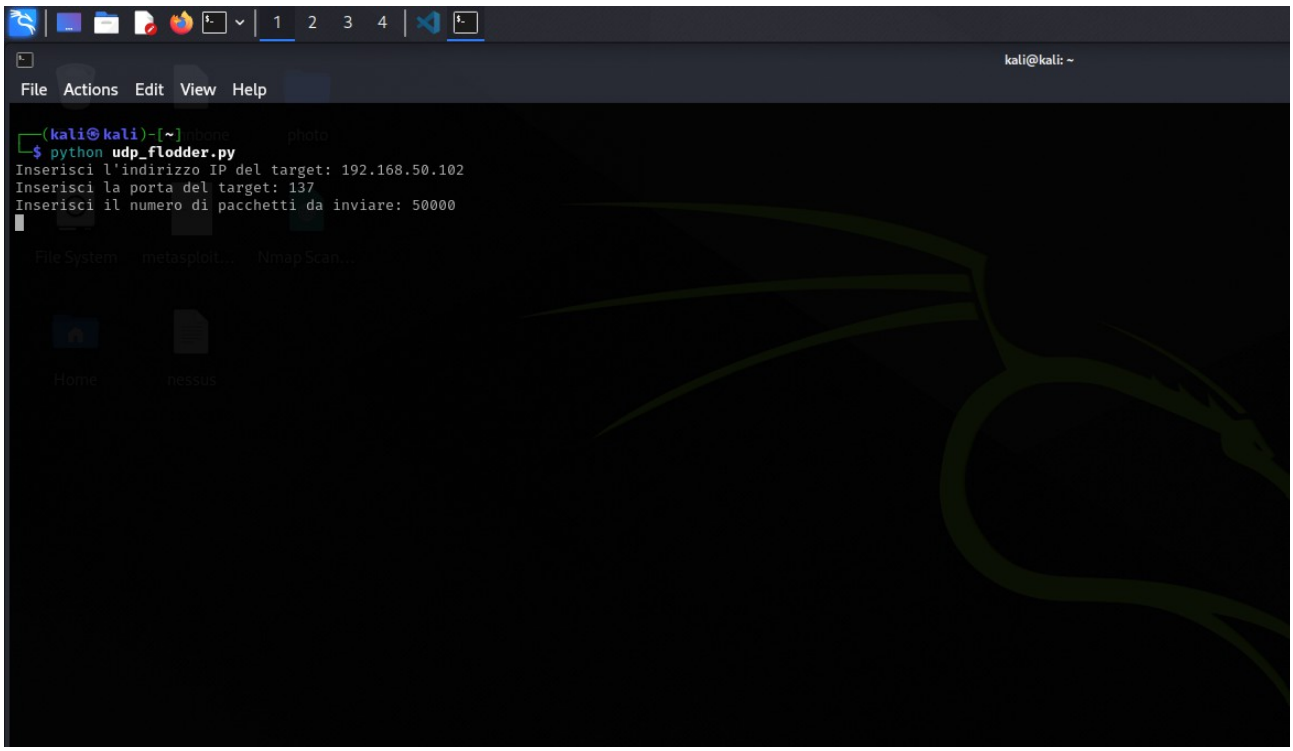
Per ulteriore conferma col comando **nmap -O 192.168.50.102** ci accertiamo che la macchina sia quella scelta per l'attacco.

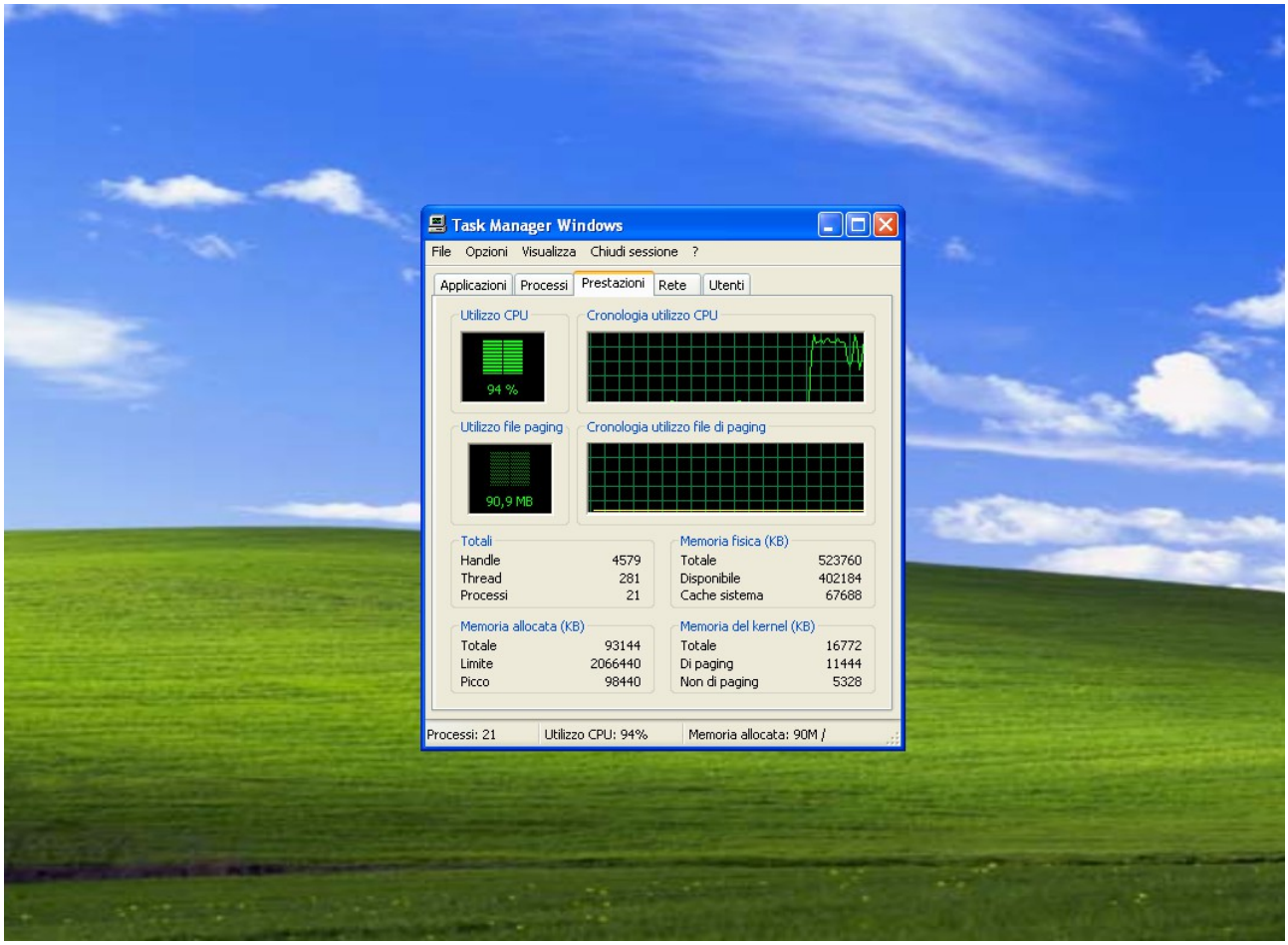



Col comando **nmap -sU 192.168.50.102** controlliamo lo stato e il numero della porta UDP, questo ultimo necessario per l'attacco. La porta UDP è la **137**.




Procediamo con l'attacco






Durante l'attacco noteremo sulla macchina con XP un **alto utilizzo della CPU** ed una graduale **diminuzione della memoria disponibile**.

Per completezza, schermata della configurazione di rete della Macchina con Windows XP