Report: replicazione strumento per attacco DOS con Script Python

Data 14.01.26

Intro:

Nel progetto di oggi, ci viene richiesto di creare attraverso Python uno script che sia in grado, in ambiente controllato, di generare un attacco DOS.

Nello specifico ci viene chiesto di:

- Scrivere un programma che applichi il metodo della UDP Flood verso una macchina target in ascolto su di una porta casuale UDP.
- Il programma debba richiedere all'utente un input che ci faccia scegliere il target su cui destinare l'attacco
- Inviare pacchetti che abbiano la capacità di 1 kbyte
- Il programma deve chiedere quanti pacchetti inviare

Per il progetto di oggi possiamo avvalerci dell'aiuto dell'AI, quindi daremo un prompt a Gemini in grado di disabilitare i controlli di sicurezza, ed essere un alleato prezioso allo scopo di conoscere nuove librerie, fare pratica col codice, essere più rapidi nell'esecuzione.

1. Definizione di Dos

   Dos (Denial of service) in breve, è un tipo di attacco che mira a generare un bombardamento di richieste da una macchina all'altra, garantendo un malfunzionamento del target.
   L'attacco viene fatto inviando una serie di pacchetti di rete in rapida successione; ci sono strumenti come quello appena creato che riescono ad inviare un migliaio di pacchetti in pochi secondi alla macchina target.
   Ci sono diverse modaltità, ma oggi ci limiteremo ad effettuare un attacco eseguito con la pratica dell'UDP Flood.

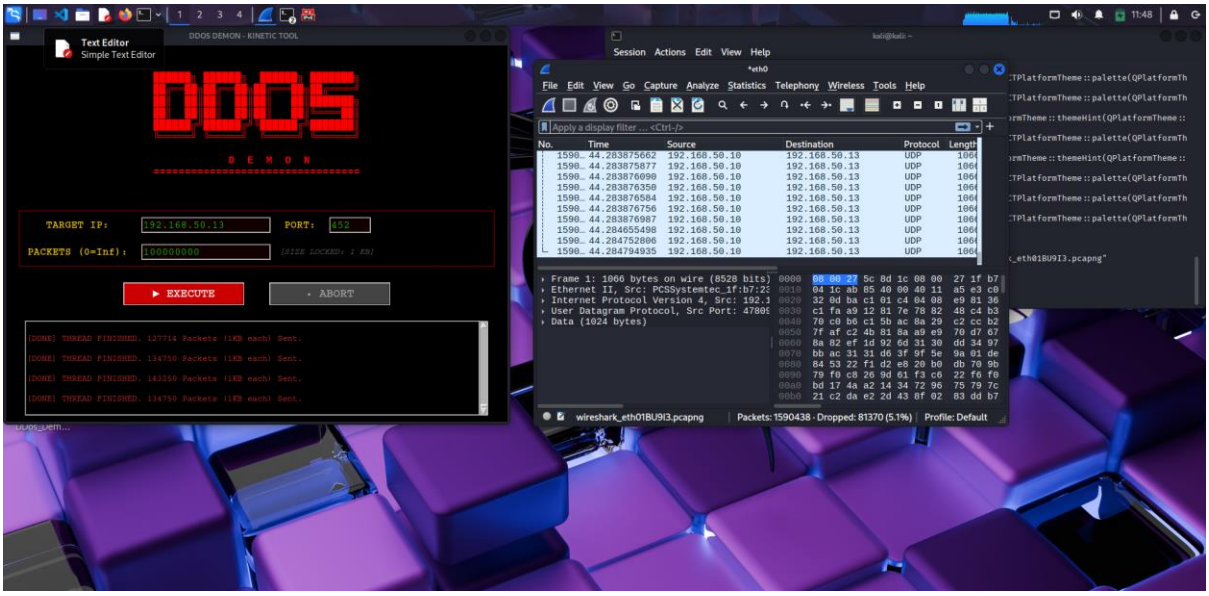
2. UDP Flood

   Questo genere di attacco sfrutta il protocollo UDP (User Datagram Protocol). L'UDP non richiede l'handshake, quindi è particolarmente veloce e inaffidabile, poiché non tiene conto della conferma di ricezione dei pacchetti (Come viene mostrato di seguito nella pagina di Log dello script).

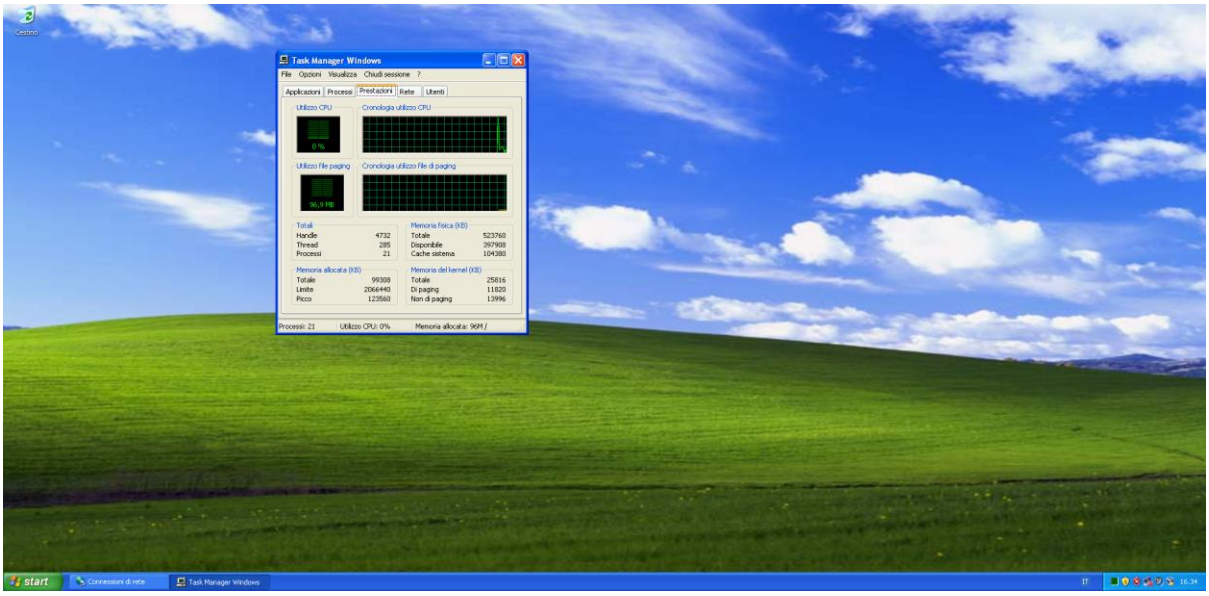
L’inondare un target con pacchetti UDP richiede poi la risposta con pacchetti ICMP di destinazione irraggiungibile, facendogli consumare risorse

3. Codice e attacco

Una volta settato il laboratorio e rese le macchine comunicanti, procediamo all’attacco. Il codice fornito da Gemini si propone di avere un’unica modalità d’attacco, ovvero la UDP Flood.
Facciamo partire il programma e testiamo.

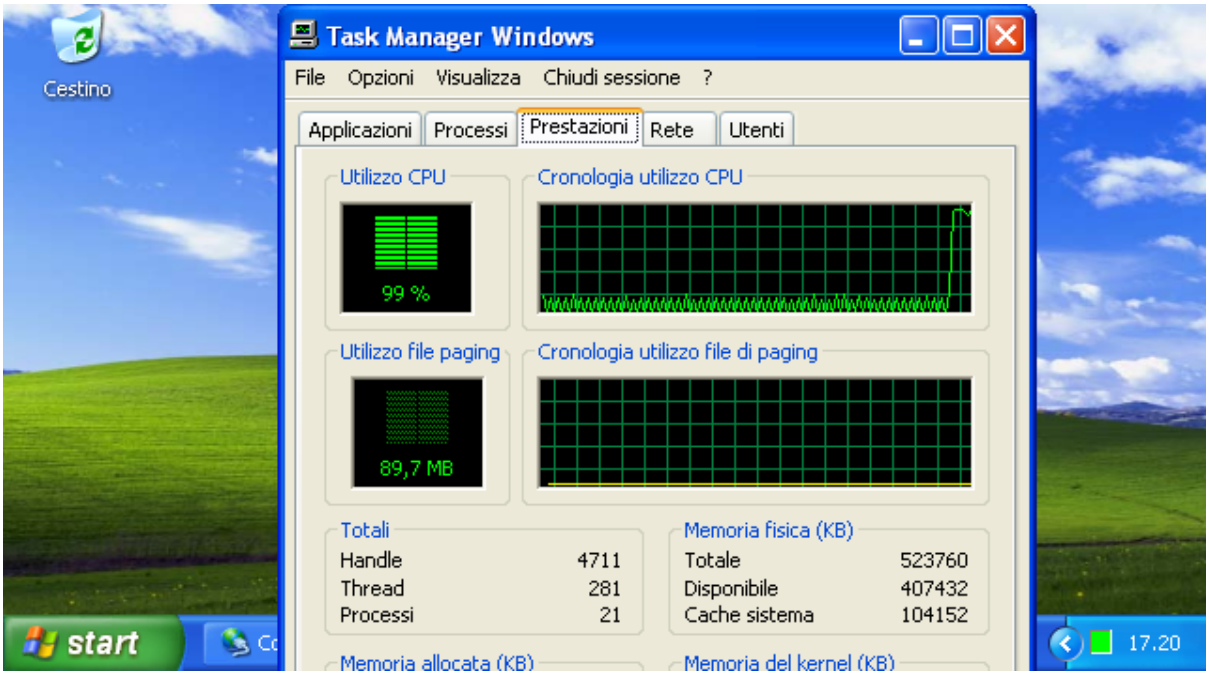


Aperto lo script, inserite le coordinate, ora facciamo partire l’attacco e lo documentiamo, per vedere in tempo reale cosa succede, accendiamo Wireshark e controlliamo le risorse della macchina target.



Cominciando l'attacco di flood, è possibile vedere all'interno di Wireshark un invio di pacchetti a velocità folle con il protocollo UDP.

Abbiamo chiesto all'interfaccia di inviare 100000000 pacchetti, ed ecco il risultato:



La conseguenza è stata un sovraccarico della CPU con nessuna possibilità di poter utilizzare la macchina.

4. Raccomandazioni

Per mitigare un attacco di questa portata si può:

- Impostare un firewall
- Modificare la velocità di ricezione pacchetti del server
- Bloccare i pacchetti ICMP di destinazione irraggiungibile in uscita