Relazione sull'Esercizio di Oggi: Creazione di un Malware con Msfvenom

Obiettivo dell'Esercizio

L'obiettivo dell'esercizio è creare un malware con msfvenom che sia più difficile da rilevare rispetto a quello analizzato in classe. I passaggi principali prevedono la preparazione dell'ambiente di lavoro, la creazione del malware e il confronto dei risultati per vedere quanto è efficace.

Preparazione dell'Ambiente

- Abbiamo utilizzato una macchina virtuale per creare il malware. Questo permette di mantenere al

sicuro il nostro sistema principale e lavorare in un ambiente isolato.

Creazione del Malware con msfvenom

- Le immagini mostrano l'utilizzo del comando msfvenom per generare il malware. È stato usato un metodo chiamato shikata_ga_nai che aiuta a nascondere il malware. Ciò è stato fatto più volte per ottenere una versione finale del file chiamato polimorficommm.exe.
- Questo metodo di nascondere il malware serve a renderlo meno rilevabile dagli antivirus.

Test del Malware

- Dopo aver creato il malware, il file è stato caricato su VirusTotal, una piattaforma che verifica se vari antivirus riescono a identificarlo come pericoloso.
- I risultati mostrano che 59 su 72 antivirus hanno rilevato il file come malware, dandogli nomi diversi, come Trojan.CryptZ.Marte.1.Gen o Backdoor:Win/meterpreter.A. Questo significa che la maggior parte degli antivirus ha riconosciuto che il file era sospetto.

Analisi dei Risultati

- Anche se abbiamo cercato di nascondere il malware, è stato comunque rilevato da molti antivirus (59 su 72). Solo alcuni antivirus non lo hanno identificato, ma questo non è sufficiente per considerare il nostro esperimento un successo.
- Il malware analizzato in classe aveva una rilevabilità simile, il che significa che dobbiamo migliorare ulteriormente il nostro metodo per renderlo meno rilevabile.

Migliorie Possibili

1. **Aumentare il Numero di Tentativi di Offuscamento**: Provare a ripetere il processo di

nascondere il malware più volte potrebbe migliorare il risultato.

2. **Aggiungere Ulteriori Tecniche di Nascondimento**: Utilizzare tecniche di cifratura o modifiche manuali potrebbe rendere il malware più difficile da rilevare.
3. **Creare Versioni Diverse del Malware**: Cambiare i parametri durante la creazione del malware o combinarli con altri metodi potrebbe far sì che il malware venga rilevato meno frequentemente.