Department of Computer Science and Engineering

A.Y.2023-24

Ethical Hacking

Lab4: Creating a Trojan using Social-Engineer Toolkit

Student Name: Adwait Purao Sem: 6 Date: 18/3/24

Objective: Creating a Trojan using Social-Engineer Toolkit

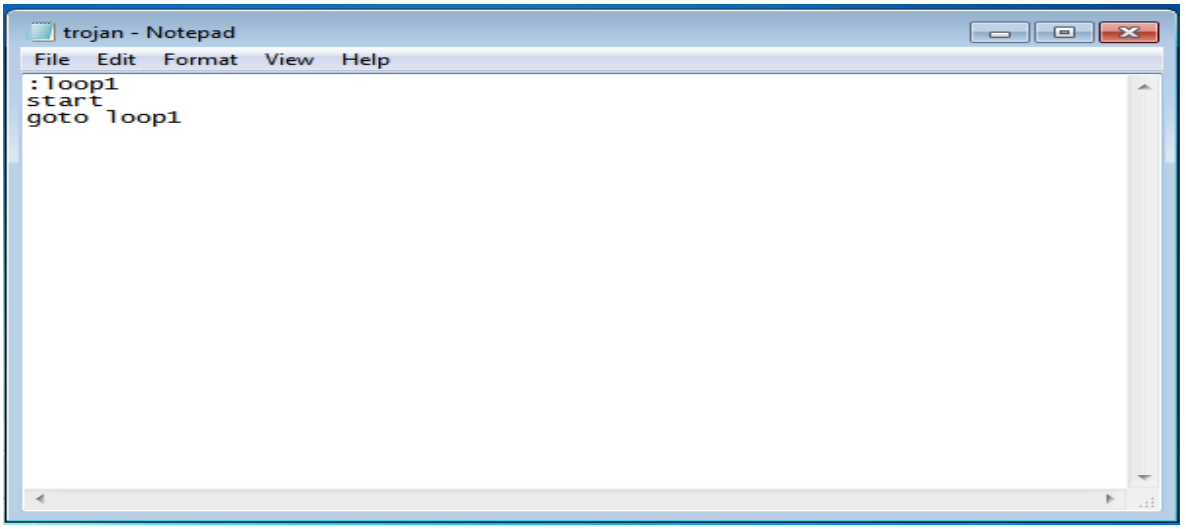
Outcomes:

1. Created a batch file virus in Windows 7 that spawned multiple instances of command prompt windows, potentially leading to system instability.
2. Developed a PowerShell-based alphanumeric shellcode injector Trojan using the Social-Engineer Toolkit (SEToolkit).
3. Demonstrated the ability to remotely access and control the victim machine after the Trojan payload was executed.
4. Highlighted the importance of implementing robust security measures and adopting a proactive stance to safeguard against such cyber threats.

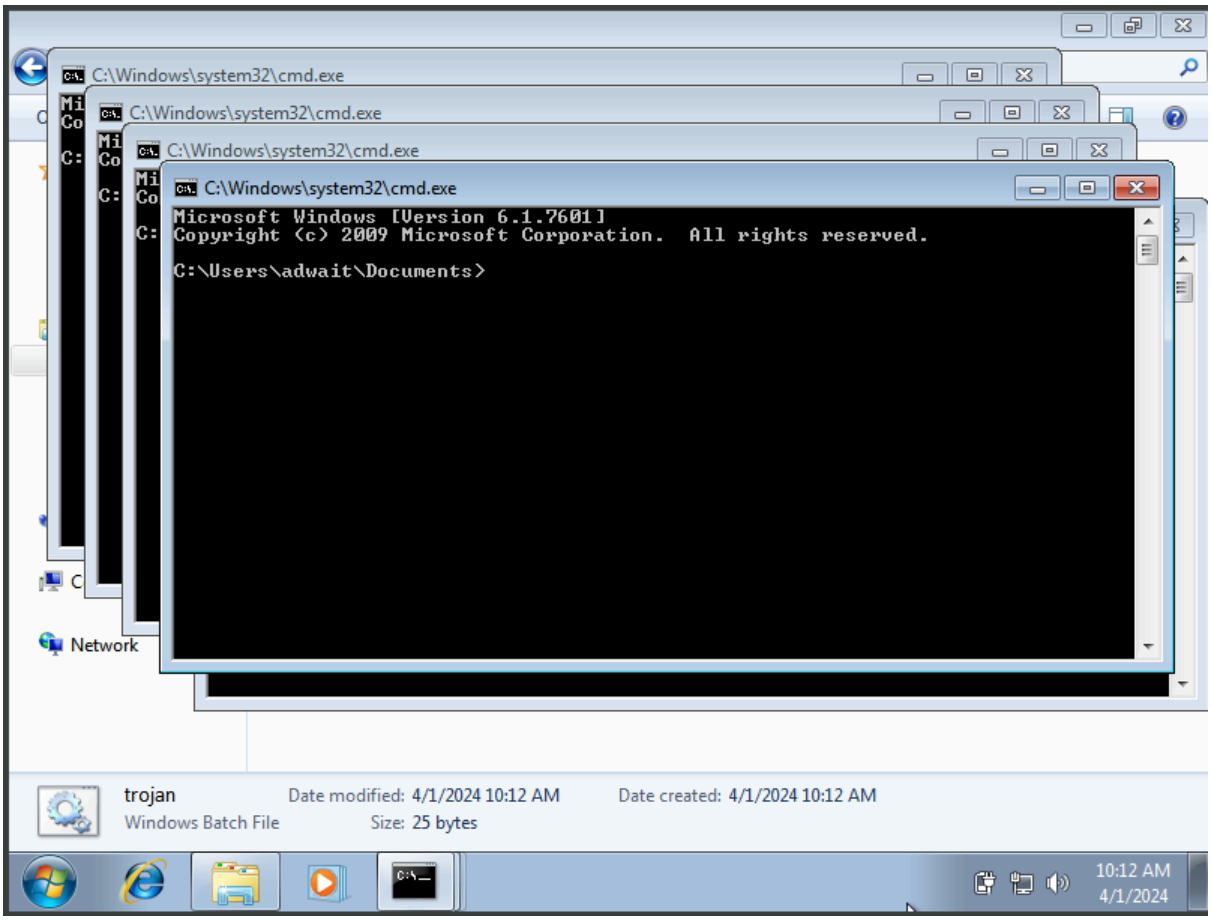
Procedure:

A. Task 1- creating .batch file virus in windows 7
Step 1- Create a new notepad file
Step 2- Write a code in the notepad file and save the file as filename.bat

```
:loop1
start
goto loop1
```



Step 3- Run the bat file and observe the finding.



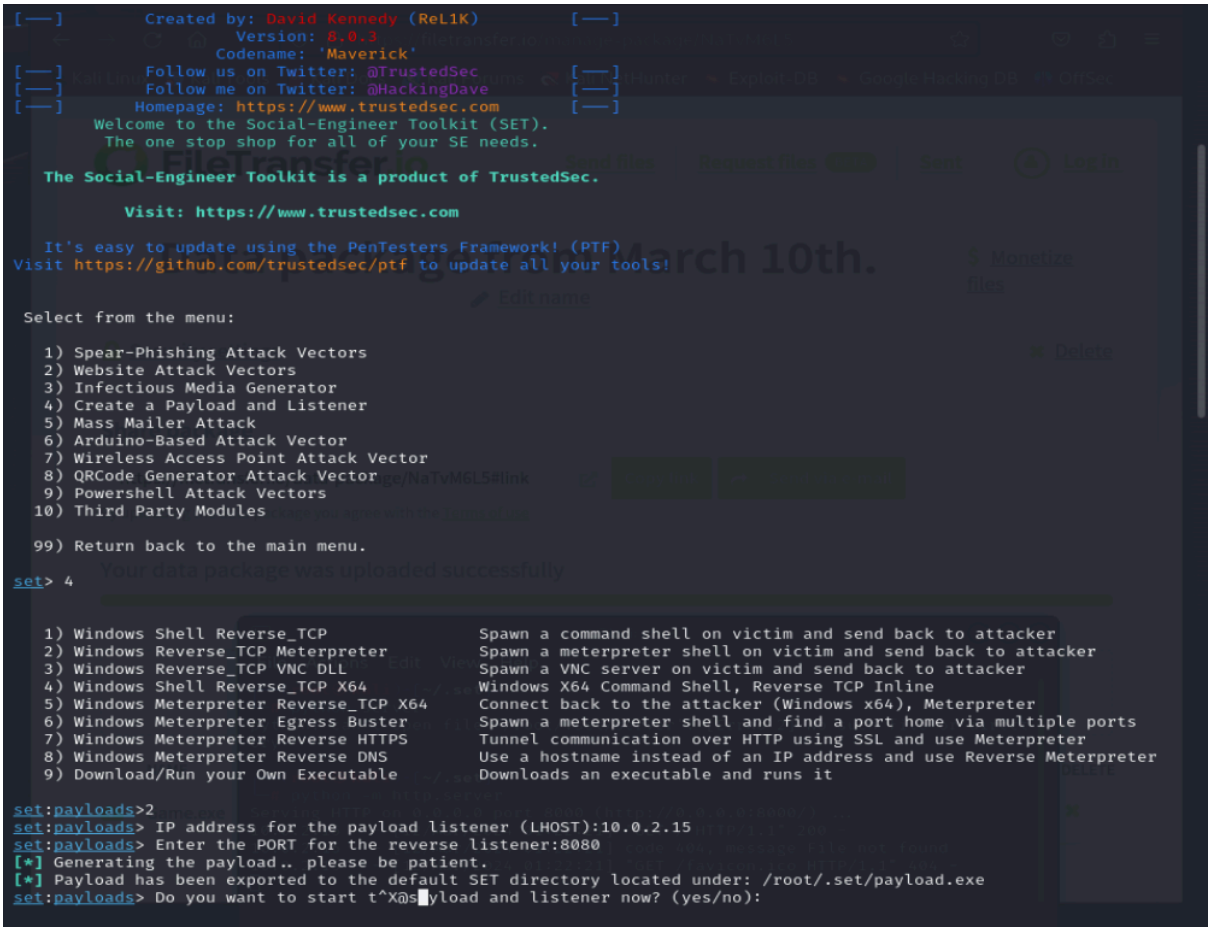
Observation:
This batch script exhibits a looping behavior that spawns multiple instances of the default program associated with a specific file type. Consequently, it initiates a cascade of command prompt windows opening continuously. Such a script can significantly drain system resources, potentially leading to performance degradation and even system instability if allowed to persist. It is strongly discouraged to develop or deploy scripts with such disruptive characteristics as they pose risks to the smooth operation of the system.

B.Task 2

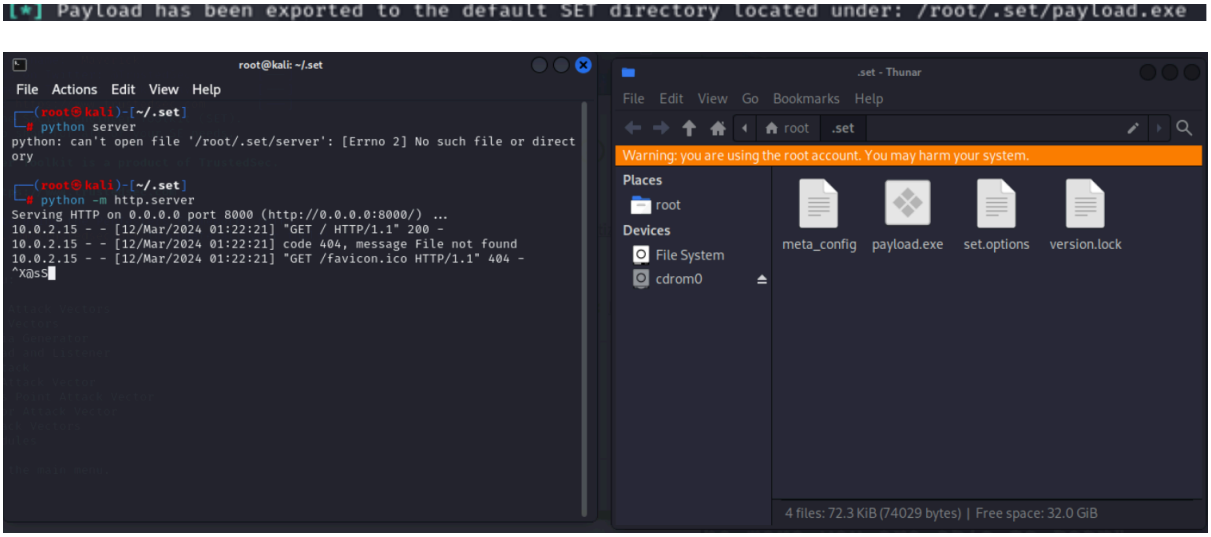
Create powershell alphanumeric shellcode injector trojan using SE toolkit

Step 1:

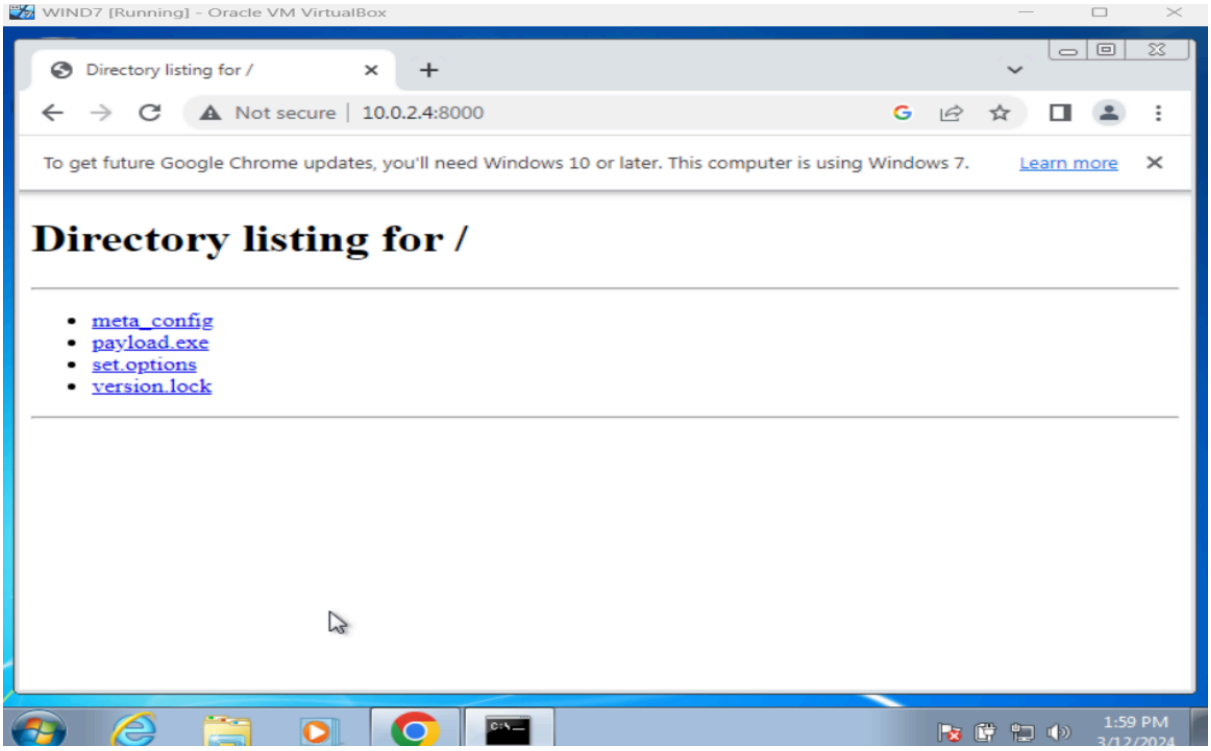
- **In Kali linux run SEtoolKit.**
- **Then select option 4(create a payload and listener).**
- **Then select option 2 (Windows Reverse_TCP Meterpriter).**
- **Then it will ask for LHost which is the attacker IP for listening the calls from victim machines.**



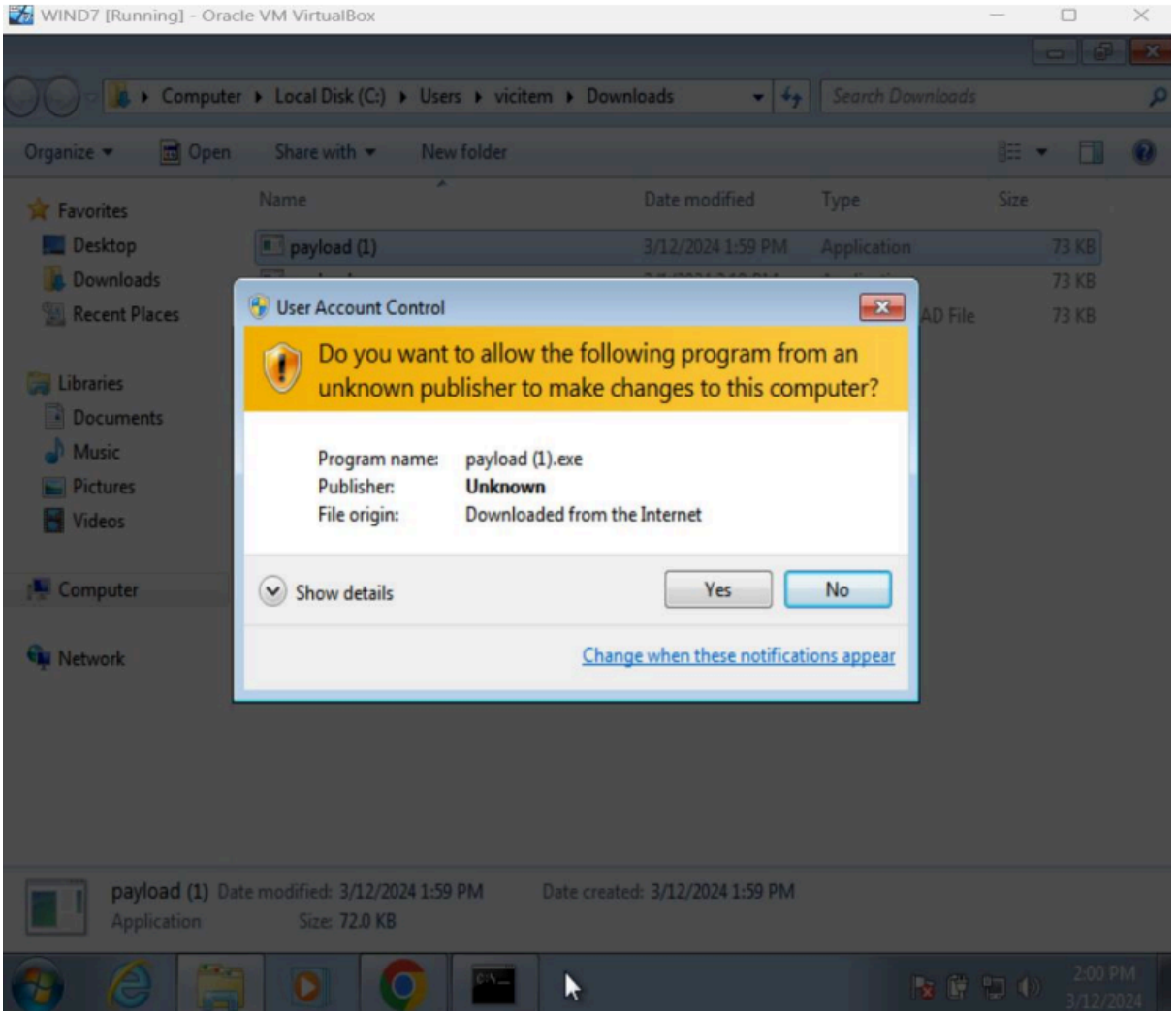
I have shared the file location using Python Server



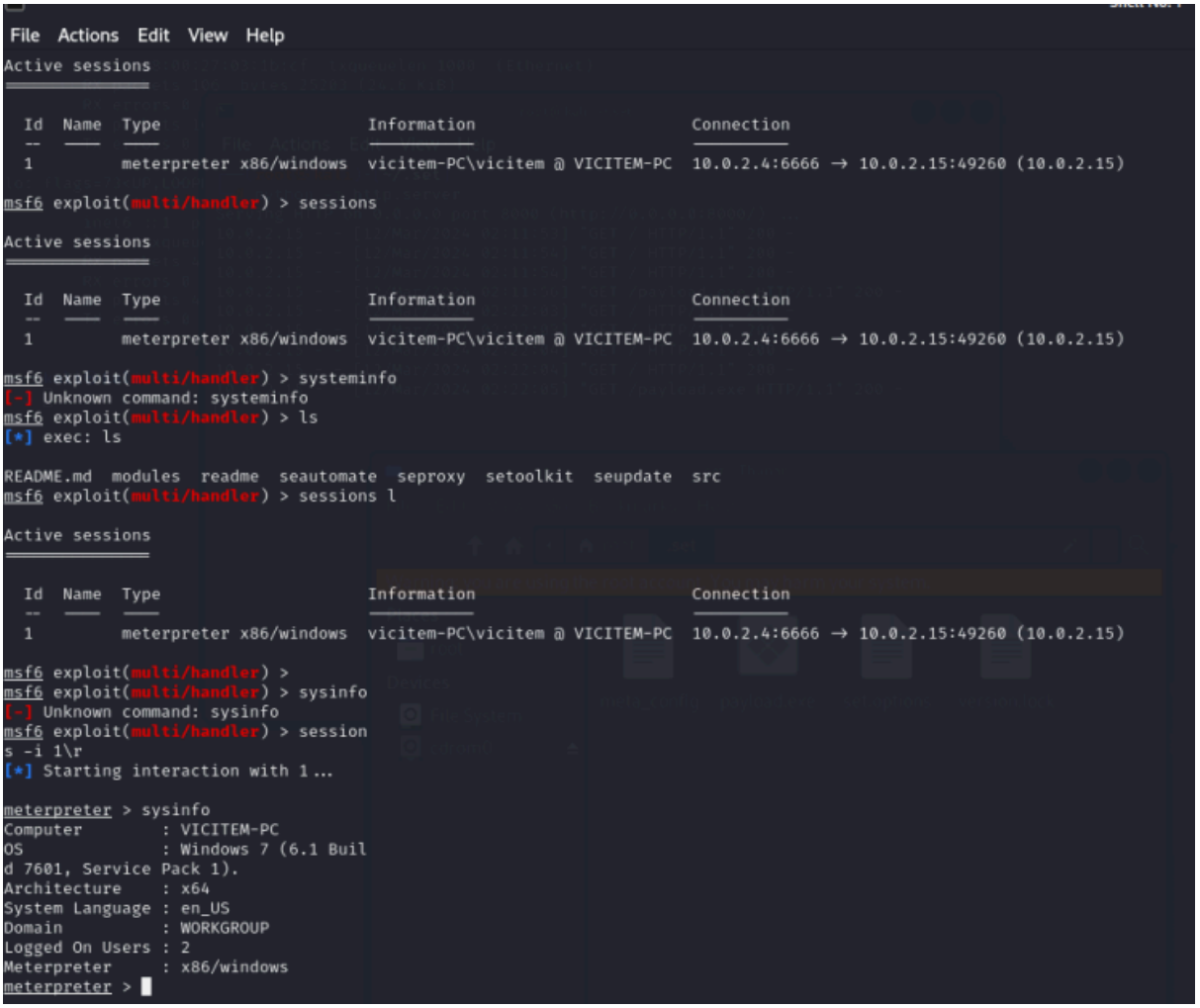
Open Chrome or any browser and Enter the server location for accessing files.



Download and run the Pyload.exe file in the victim machine.



Now the session will start and you can control the victim machine.



Conclusion:

In conclusion, our efforts have resulted in the successful deployment of a potent payload, leveraging SEtoolKit and Metasploit to gain control over the target machine. Moreover, we've implemented a vigilant monitoring mechanism through a bat file to closely track the execution process. These actions underscore our dedication to implementing robust security measures and adopting a proactive stance in safeguarding against cyber threats.