Module 7 **Malware Threats**

Module 07: Malware Threats

Scenario

Malware poses a major security threat to information security. Malware writers explore new attack vectors to exploit vulnerabilities in information systems. This leads to ever more sophisticated malware attacks, including drive-by malware, "maladvertising" (or "malvertising") and advanced persistent threats. Although organizations try hard to defend themselves using comprehensive security policies and advanced anti-malware controls, the current trend indicates that malware applications are targeting "lower-hanging fruit"; these include unsecured smartphones, mobile applications, social media, and cloud services. This problem is further complicated, because of the challenges faced during threat prediction.

Assessing an organization's information system against malware threats is a major challenge today, because of the rapidly changing nature of malware threats. One needs to be well-versed in the latest developments in the field and understand the basic functioning of malware to select and implement the controls appropriate for an organization and its needs.

The lab activities in this module provide first-hand experience with various techniques that attackers use to write and propagate malware. You will also learn how to effectively select security controls to protect your information assets from malware threats.

Objective

The objective of the lab is to create malware and perform other tasks that include, but are not limited to:

- Create a Trojan and exploit a target machine
- Create a virus to infect the target machine
- Perform malware analysis to determine the origin, functionality, and potential impact of a given type of malware
- Detect malware

Overview of Malware

With the help of a malicious application (malware), an attacker gains access to stored passwords in a computer and is able to read personal documents, delete files, display pictures, or messages on the screen, slow down computers, steal personal information, send spam, and commit fraud. Malware can perform various malicious activities that range from simple email advertising to complex identity theft and password stealing.

Programmers develop malware and use it to:

- Attack browsers and track websites visited
- Affect system performance, making it very slow
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in substantial data losses
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

Lab Tasks

Ensure that the **Windows Defender Firewall is Turn off** on the machines you are using for the lab tasks in this module, as it blocks and deletes malware as soon as it is executed.

Attackers, as well as ethical hackers or pen testers, use numerous tools and techniques to gain access to the target network or machine. Recommended labs that will assist you in learning various malware attack techniques include:

1. Gain access to the target system using Trojans
    - Gain control over a victim machine using the njRAT RAT Trojan
2. Infect the target system using a virus
    - Create a virus using the JPS Virus Maker Tool and infect the target system
3. Perform static malware analysis
    - Perform malware scanning using Hybrid Analysis
    - Analyze ELF executable file using Detect It Easy (DIE)
    - Perform malware disassembly using IDA and OllyDbg
4. Perform dynamic malware analysis
    - Perform port monitoring using TCPView and CurrPorts
    - Perform process monitoring using Process Monitor

Lab 1: Gain Access to the Target System using Trojans

Lab Scenario

Attackers use digital Trojan horses to trick the victim into performing a predefined action on a computer. Trojans are activated upon users' specific predefined actions, like unintentionally installing a piece of malicious software or clicking on a malicious link, and upon activation, it can grant attackers unrestricted access to all data stored on compromised information systems and cause potentially immense damage. For example, users could download a file that appears to be a movie, but, when opened, it unleashes a dangerous program that erases the hard drive or sends credit card numbers and passwords to the attacker.

Trojan horses work on the same level of privileges as victims. For example, if a victim has the privileges to delete files, transmit information, modify existing files, and install other programs (such as programs that provide unauthorized network access and execute privilege elevation attacks), once the Trojan infects that system, it will possess the same privileges. Furthermore, it can attempt to exploit vulnerabilities to increase its level of access, even beyond the user running it. If successful, the Trojan could use the increased privileges to install other malicious code on the victim's machine.

An expert security auditor or ethical hacker needs to ensure that the organization's network is secure from Trojan attacks by finding machines vulnerable to these attacks and making sure that antivirus tools are properly configured to detect such attacks.

The lab tasks in this exercise demonstrate how easily hackers can gain access to the target systems in the organization and create a covert communication channel for transferring sensitive data between the victim computer and the attacker.

Lab Objectives

- Gain control over a victim machine using the njRAT RAT Trojan

Overview of Trojans

In Ancient Greek mythology, the Greeks won the Trojan War with the aid of a giant wooden horse that the Greeks built to hide their soldiers. The Greeks left the horse in front of the gates of Troy. The Trojans, thinking that it was a gift from the Greeks that they had left before apparently withdrawing from the war, brought the horse into their city. At night, the hidden Greek soldiers emerged from the wooden horse and opened the city's gates for their soldiers, who eventually destroyed the city of Troy.

Thus, taking its cue from this myth, a computer Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can gain control and cause damage such as ruining the file allocation table on your hard disk.

Task 1: Gain Control over a Victim Machine using the njRAT RAT Trojan

Attackers use Remote Access Trojans (RATs) to infect the target machine to gain administrative access. RATs help an attacker to remotely access the complete GUI and

control the victim's computer without his/her awareness. They can perform screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and other tasks. The virus infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

This RAT can be used to control botnets (networks of computers), allowing the attacker to update, uninstall, disconnect, restart, and close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the Command and Control server software.

Here, we will use the njRAT Trojan to gain control over a victim machine.

The versions of the created client or host and appearance of the website may differ from what it is in this task. However, the actual process of creating the server and the client is the same, as shown in this task.
In this lab task, we will use the **Windows 11** (**10.10.1.11**) machine as the attacker machine and the **Windows Server 2022** (**10.10.1.22**) machine as the victim machine.

1. By default, **Windows 11** machine selected, click Ctrl+Alt+Delete. Login with **Admin**/**Pa$$w0rd**.

   Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 11** machine thumbnail in the **Resources** pane.

   Alternatively, you can also click **Pa$$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane.

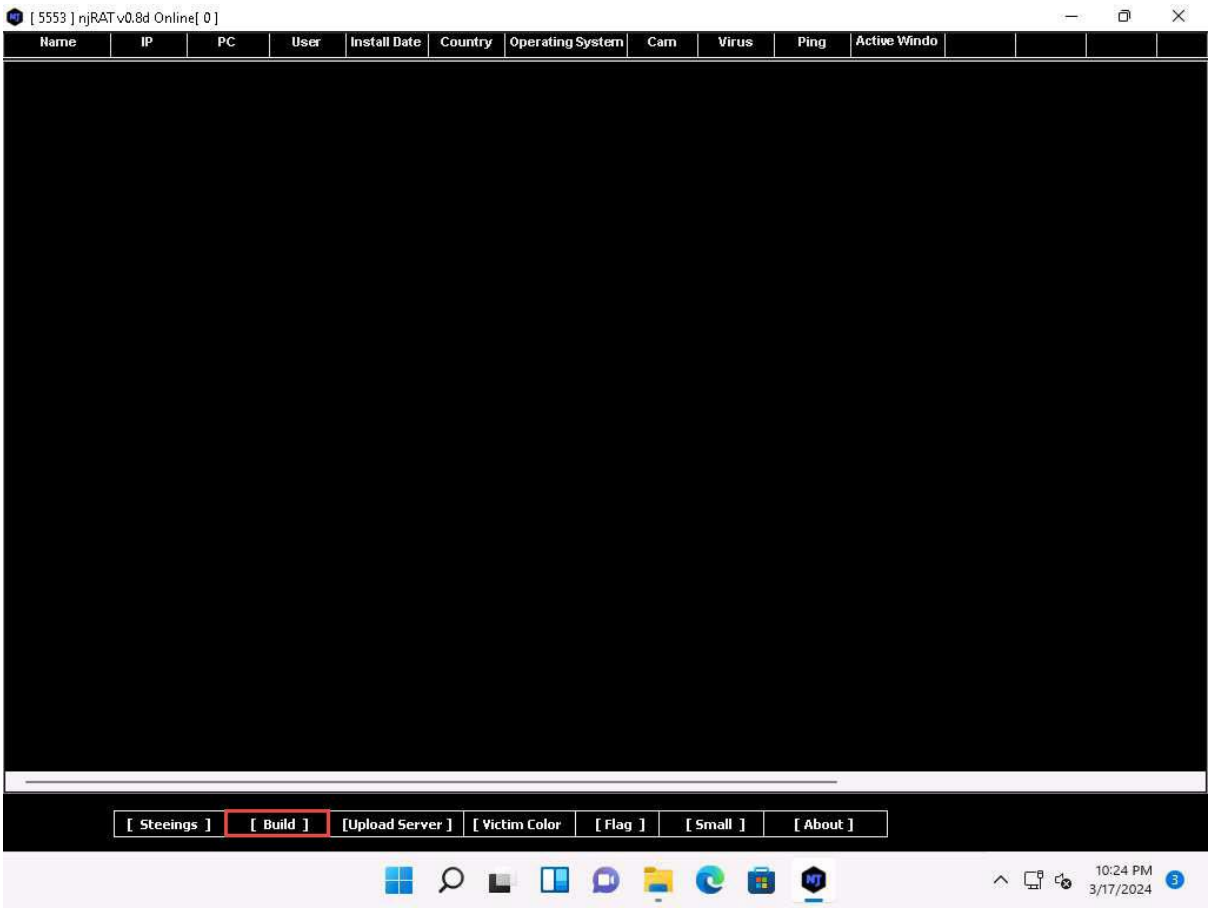
   Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

2. Navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.8d.exe**.

   If a **User Account Control** window appears, click **Yes**.
   If an **Open File - Security Warning** pop-up appears, click **Run**.

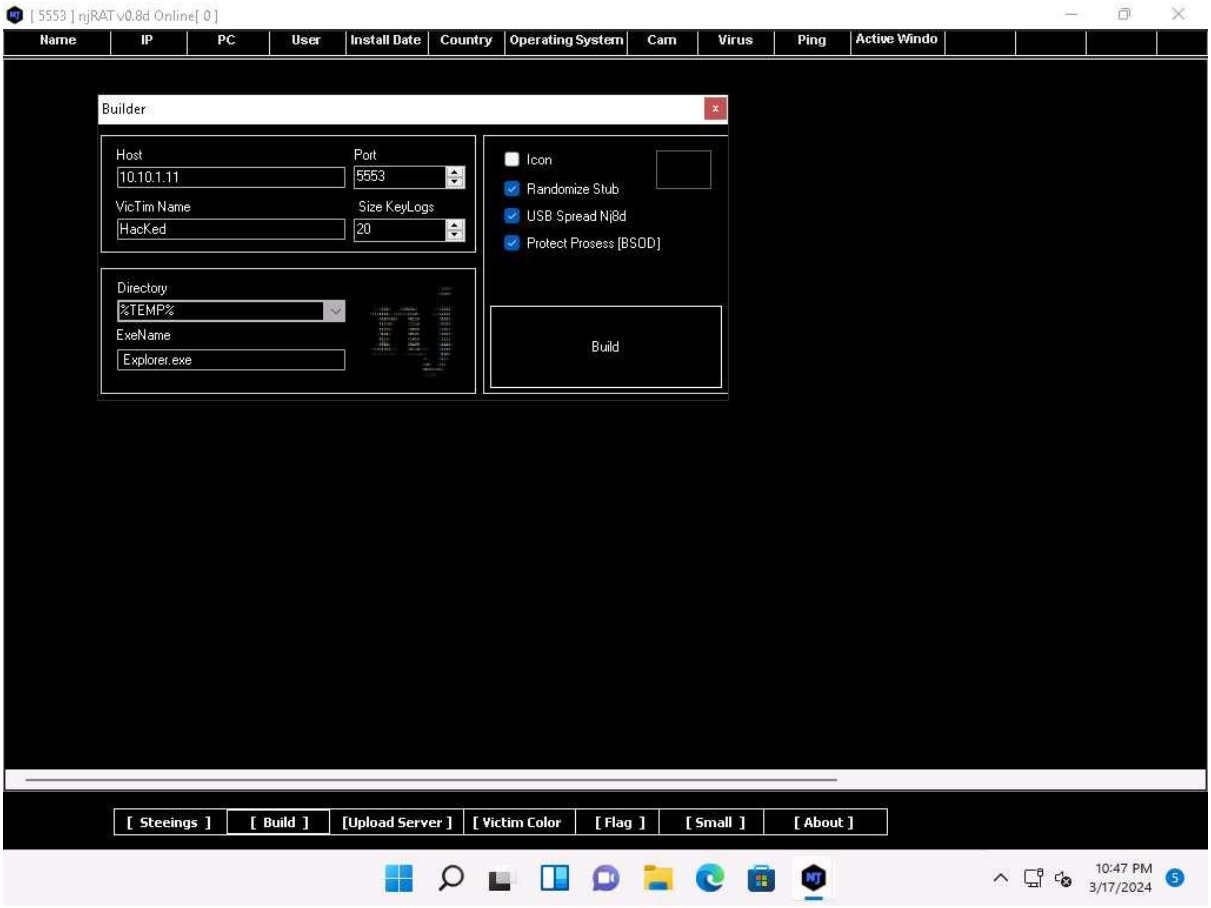
3. A **[Port Now]** pop-up appears, leave the port number to default and click on **OK**.

4. The njRAT GUI appears; click the **[Build]** button located in the lower-left corner of the GUI to configure the exploit details.



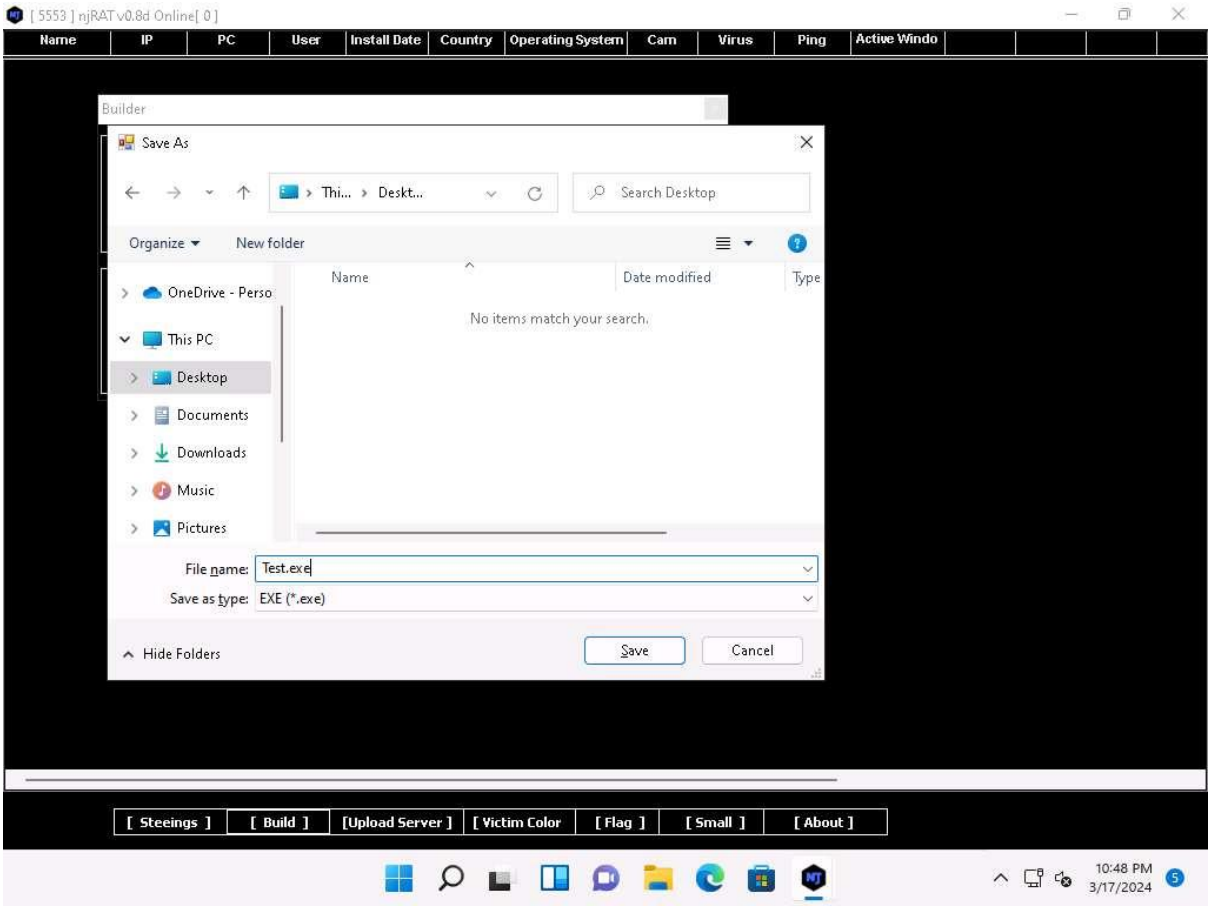
5. The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, check the options **Randomize Stub**, **USB Spread Nj8d, Protect Prosess [BSOD]**, leave the other settings to default, and click **Build**.

   In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.



6. The **Save As** window appears; specify a location to store the server, rename it, and click **Save**.

7. In this lab, the destination location chosen is **Desktop**, and the file is named **Test.exe**.

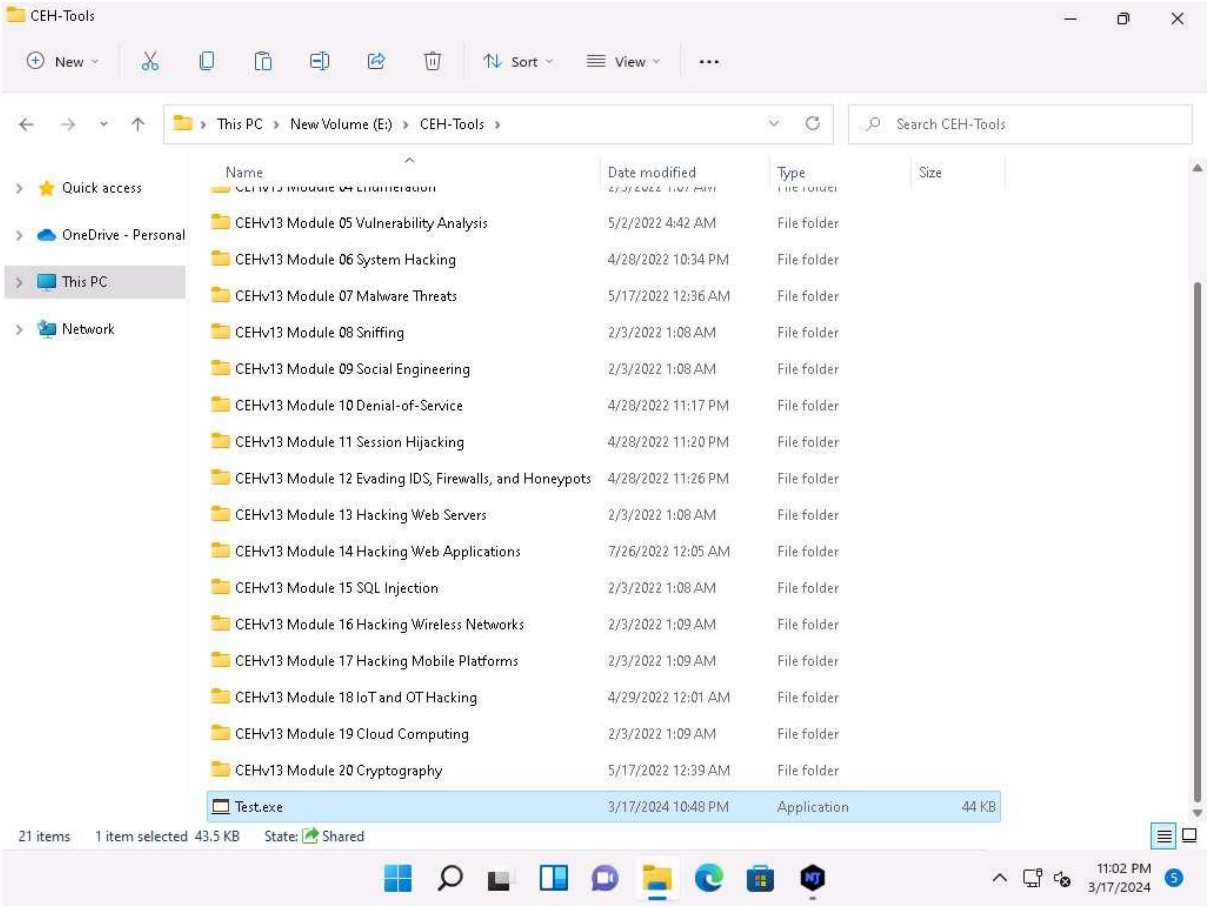


8. Once the server is created, the **Doen Successfully!** pop-up appears; click **OK**.

   A **Server** pop-up appears, click **OK**.

9. Now, use any technique to send this server to the intended target through email or any other source (in real-time, attackers send this server to the victim).

   In this task, we copied the **Test.exe** file to the shared network location (**CEH-Tools**) to share the file.



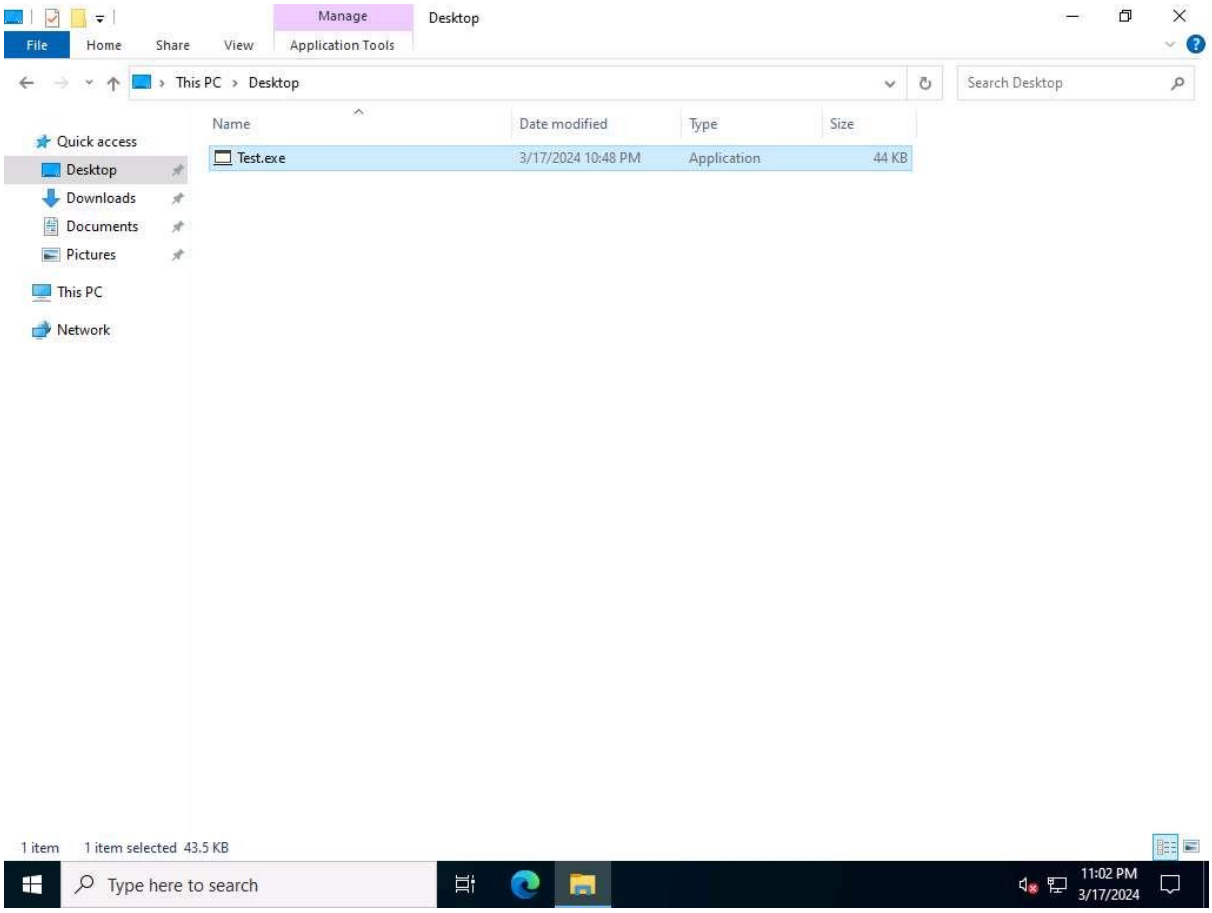
10. Click Windows Server 2022 to switch to the **Windows Server 2022** machine. Click Ctrl+Alt+Delete to activate the machine, login with **CEH\Administrator/Pa$$w0rd**.

    Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

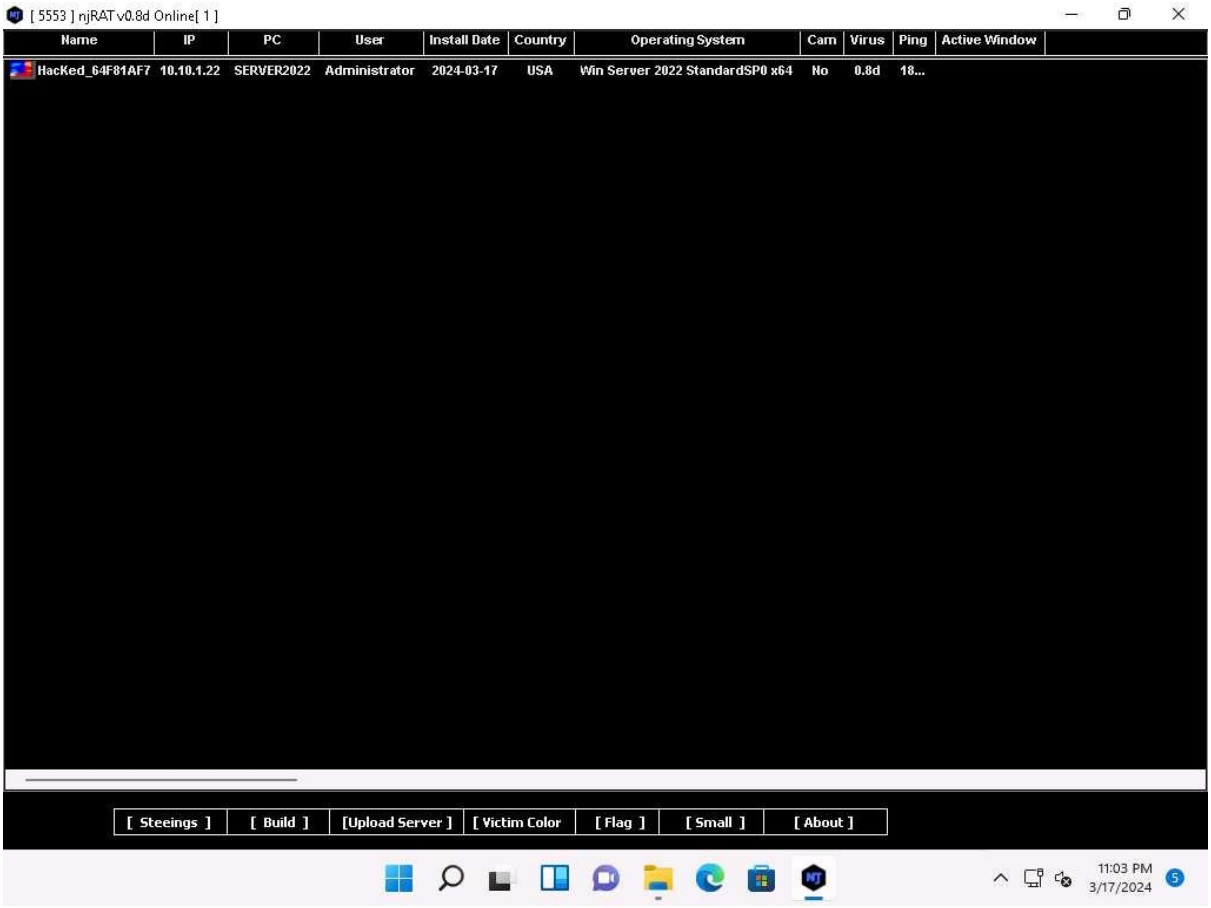
11. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**Test.exe**) onto the **Desktop** of **Windows Server 2022**.

12. Here, you are acting both as an **attacker** who logs into the **Windows 11** machine to create a malicious server, and as a **victim** who logs into the **Windows Server 2022** machine and downloads the server.

13. Double-click the server (**Test.exe**) to run this malicious executable.



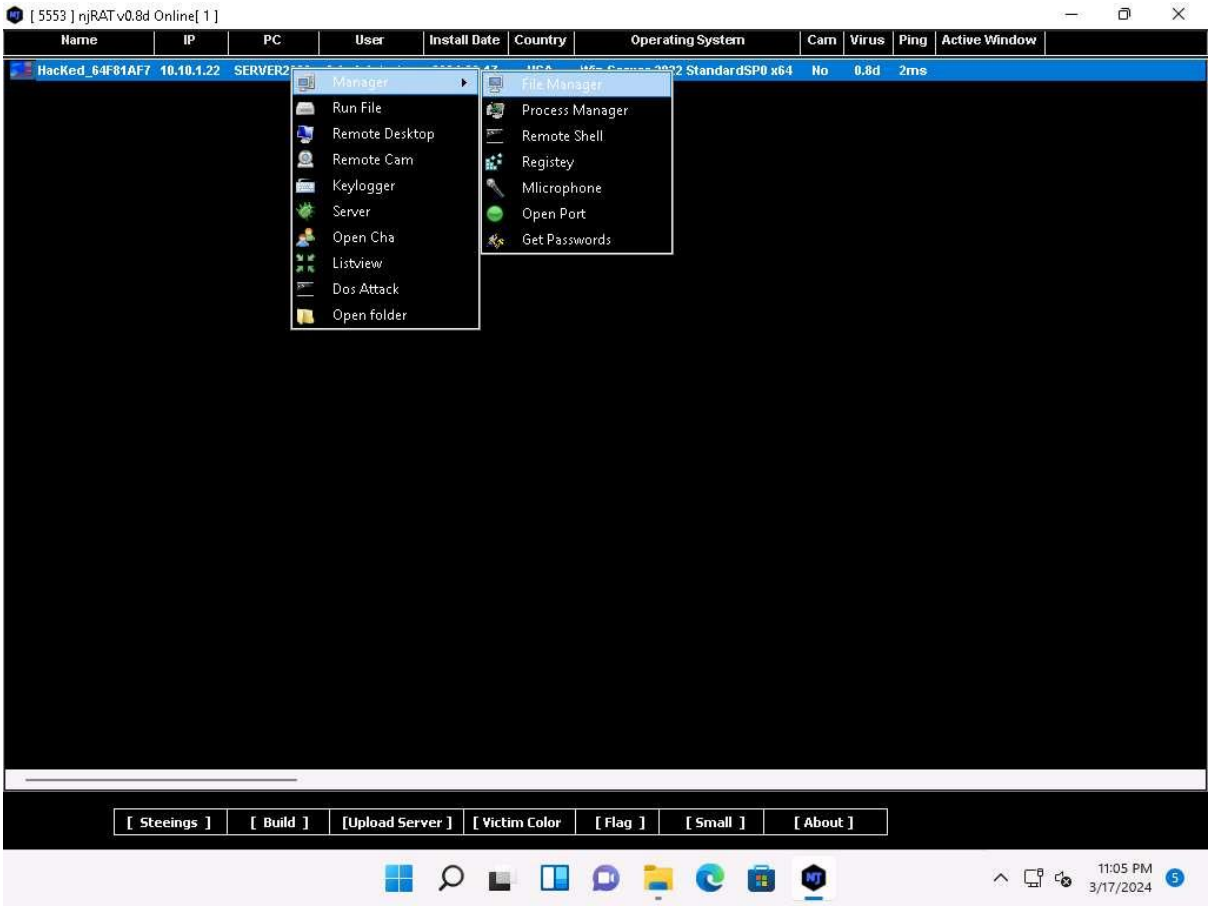
14. Click Windows 11 to switch back to the **Windows 11** machine. Maximize njRAT GUI window. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in **Windows 11** establishes a persistent connection with the victim machine, as shown in the screenshot.



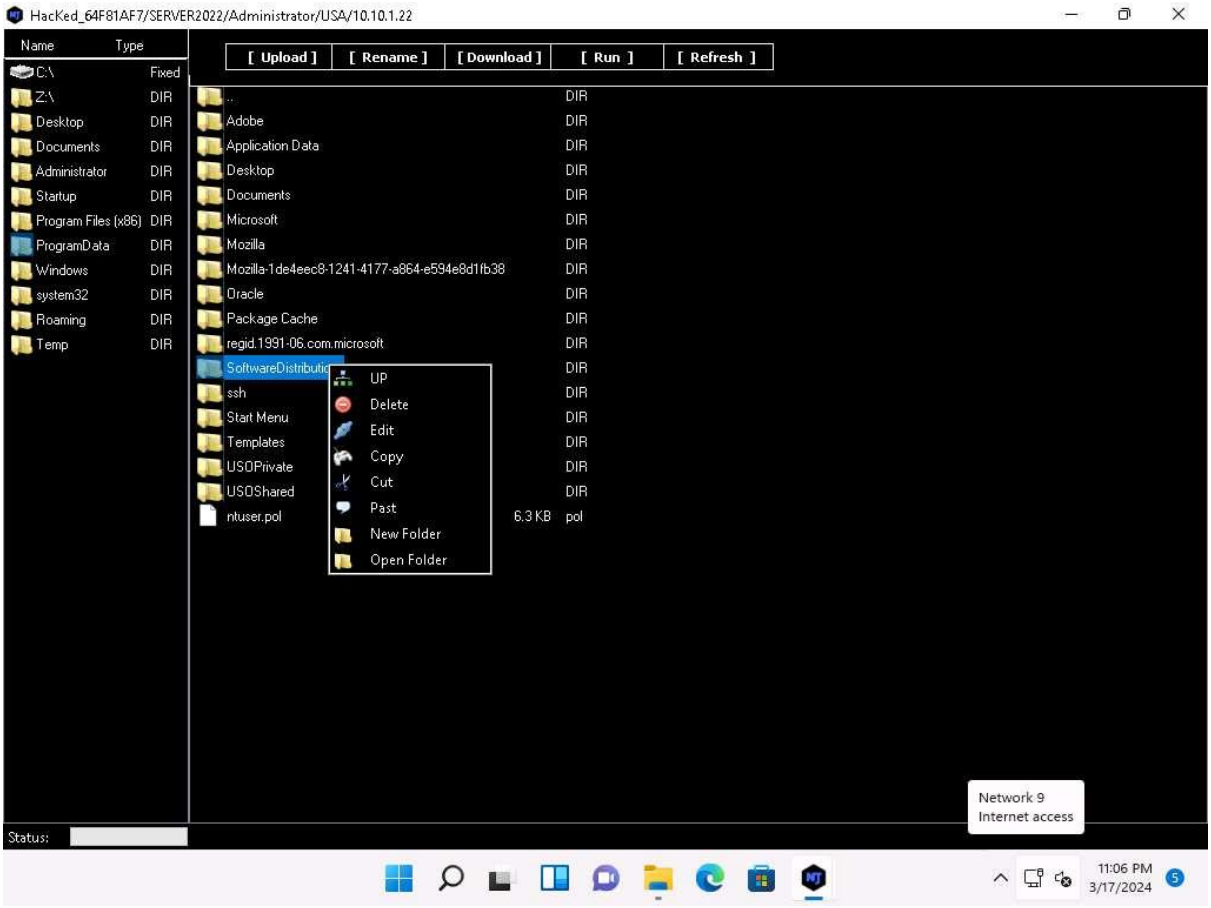
15. Unless the attacker working on the **Windows 11** machine disconnects the server on their own, the victim machine remains under their control.

16. The GUI displays the machine's basic details such as the IP address, User name, and Type of Operating system.

17. Right-click on the detected victim name and hover the cursor over **Manager** and click **File Manager** from context menu.

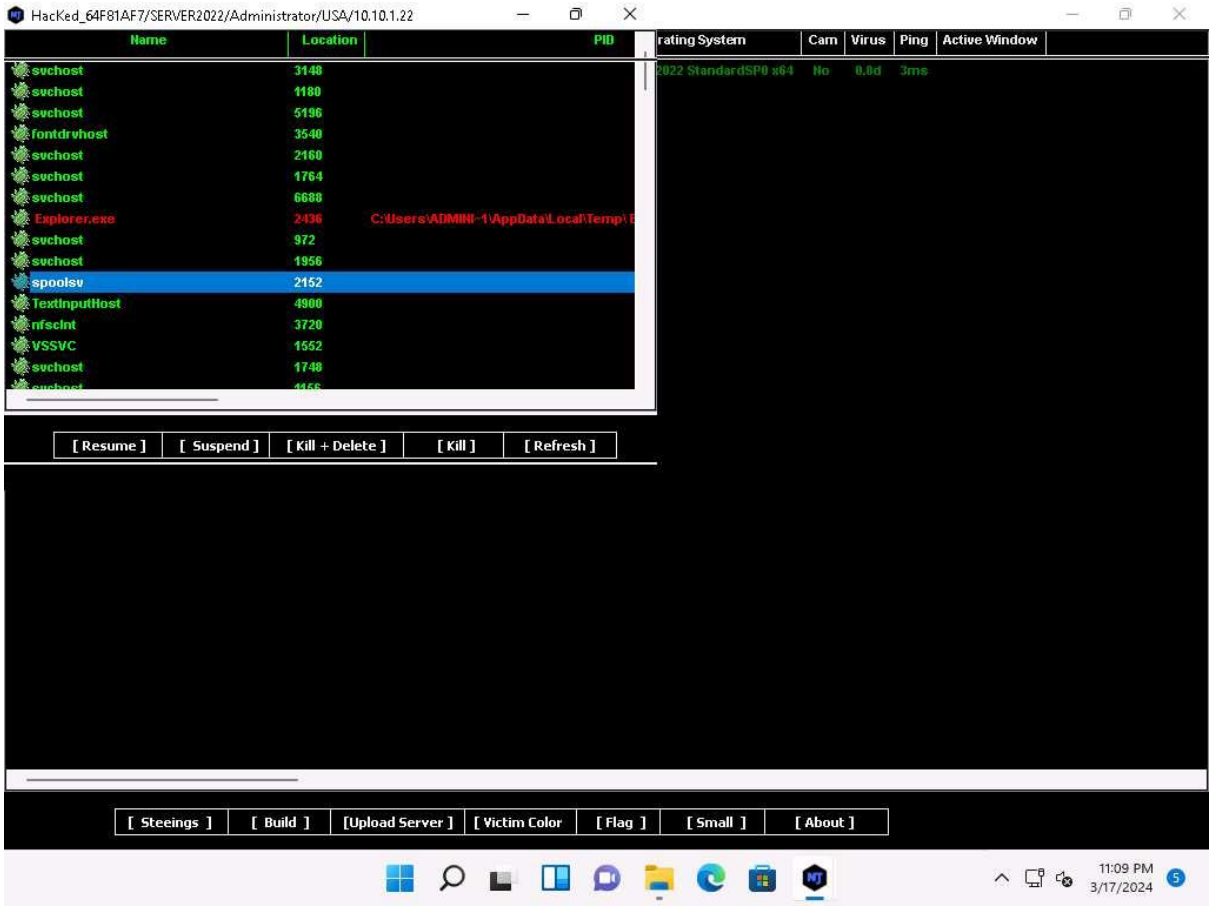


18. The **File Manager** window appears. Double-click any directory in the left pane (here, **ProgramData**); all its associated files and directories are displayed in the right pane. You can right-click a selected directory and manipulate it using the contextual options. Close the **File Manager** window.



19. Right-click on the detected victim name and click hover the cursor over **Manager** and click **Process Manager** from context menu.

20. You will be redirected to the Process Manager, where you can click on a selected process and perform actions such as **Suspend**, **Kill + Delete**, **Kill**, and **Refresh**.

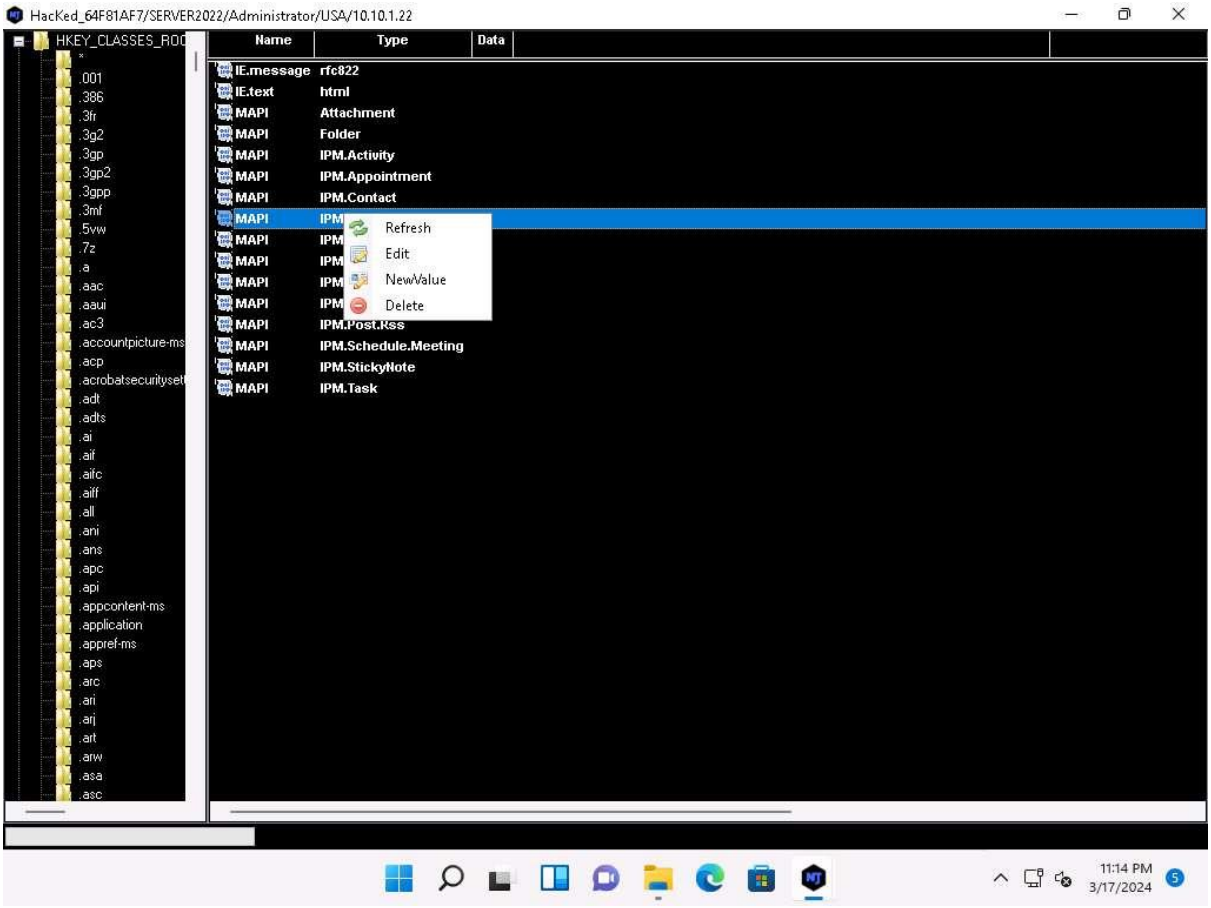


21. Close the **Process Manager** window.

22. Right-click on the detected victim name and click hover the cursor over **Manager** and click **Registey** from context menu.

23. Window showing the registries folders will be opened, choose a registry directory from the left pane, and right-click on its associated registry files.

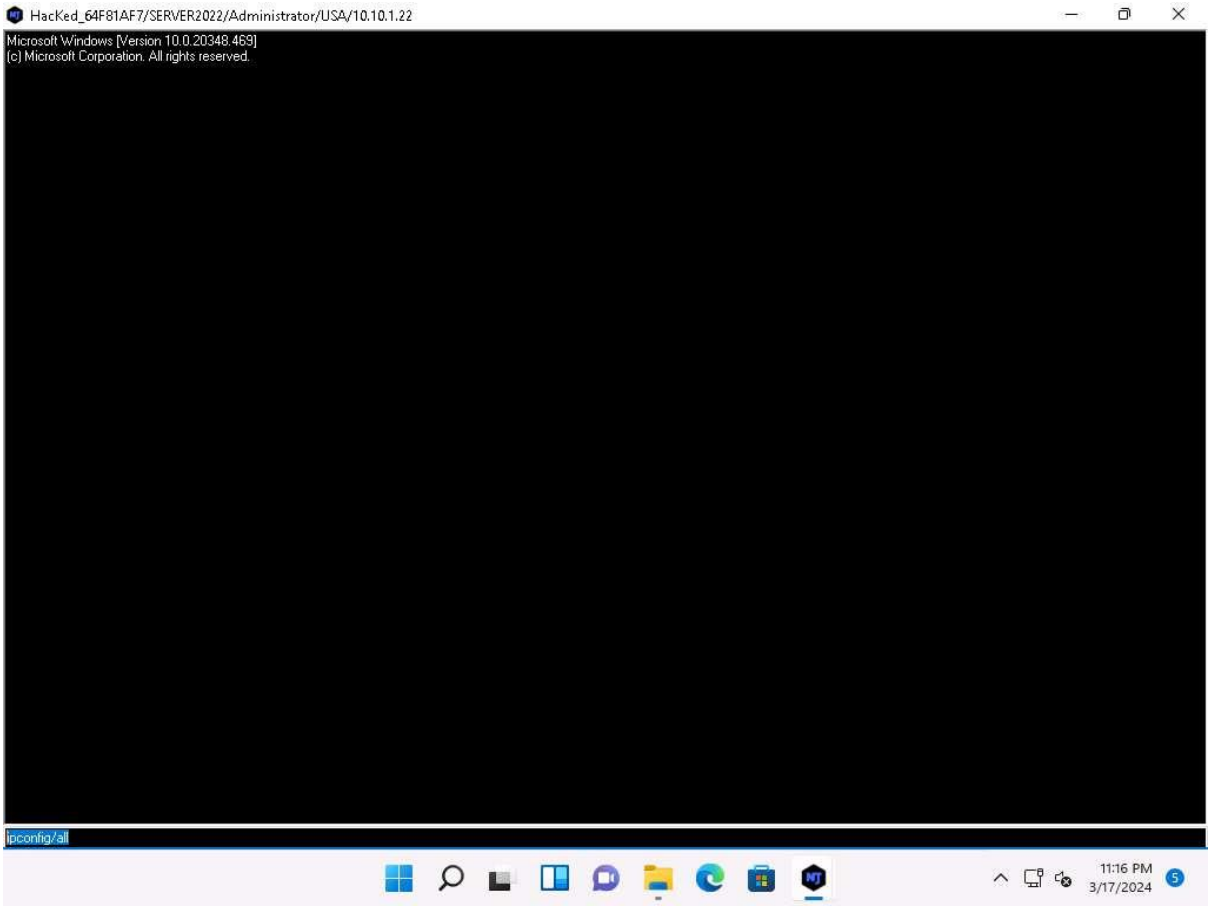
24. A few options appear for the files; you can use these to manipulate them. Close the window displaying Registry folders.



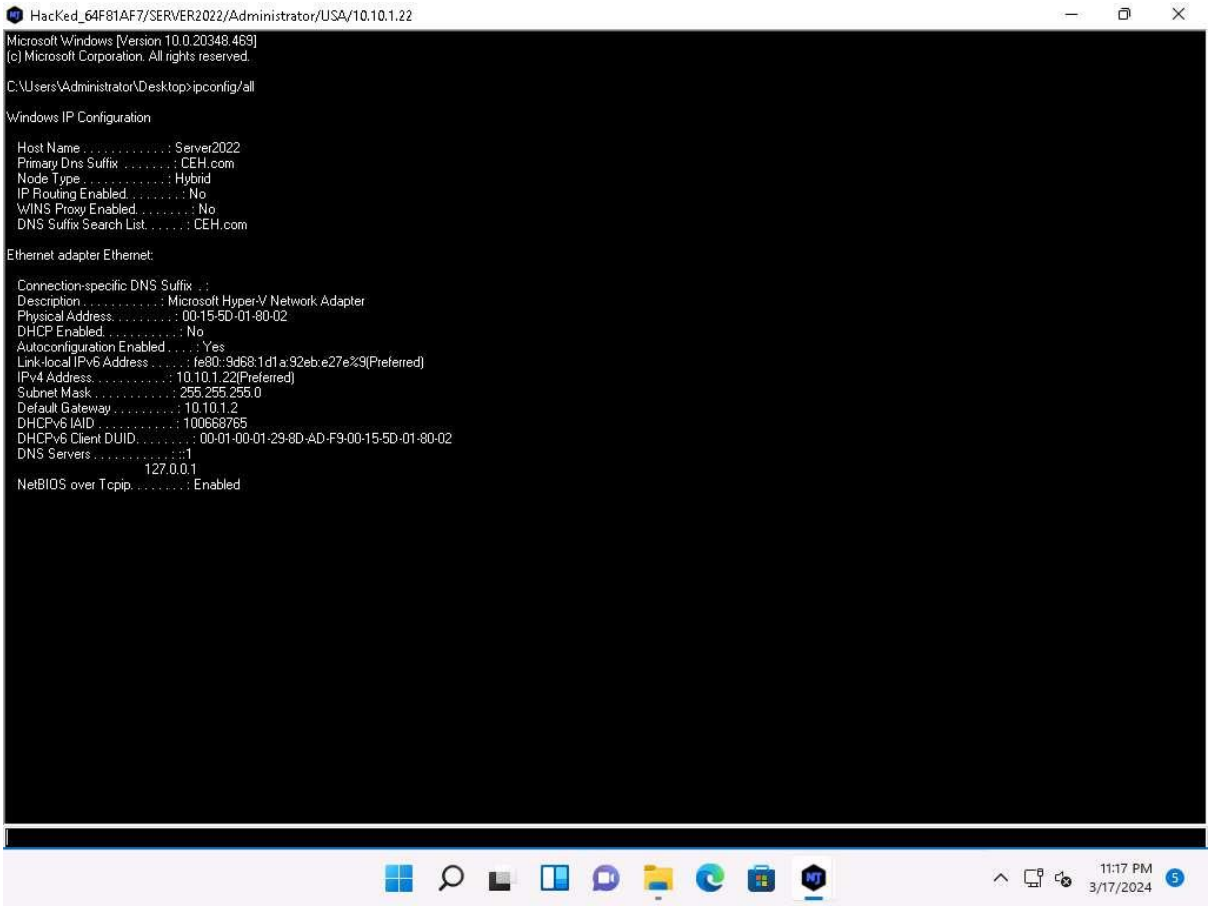
25. Right-click on the detected victim name and hover the cursor over **Manager** and click **Remote Shell** from context menu.

26. This launches a remote command prompt for the victim machine (**Windows Server 2022**).

27. In the text field present in the lower section of the window, type the command **ipconfig/all** and press **Enter**.

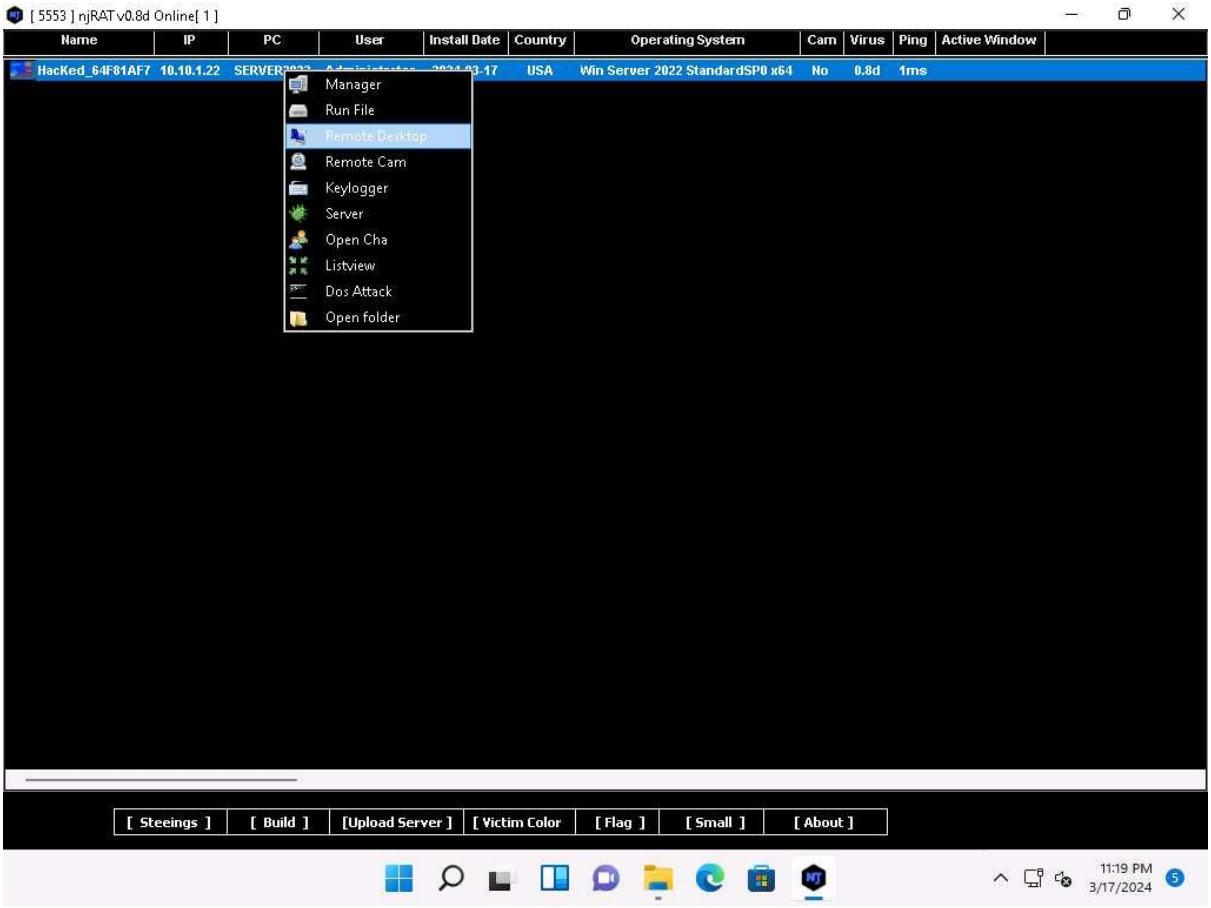


28. This displays all interfaces related to the victim machine, as shown in the screenshot.



29. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine. Close the **Remote Shell** window.

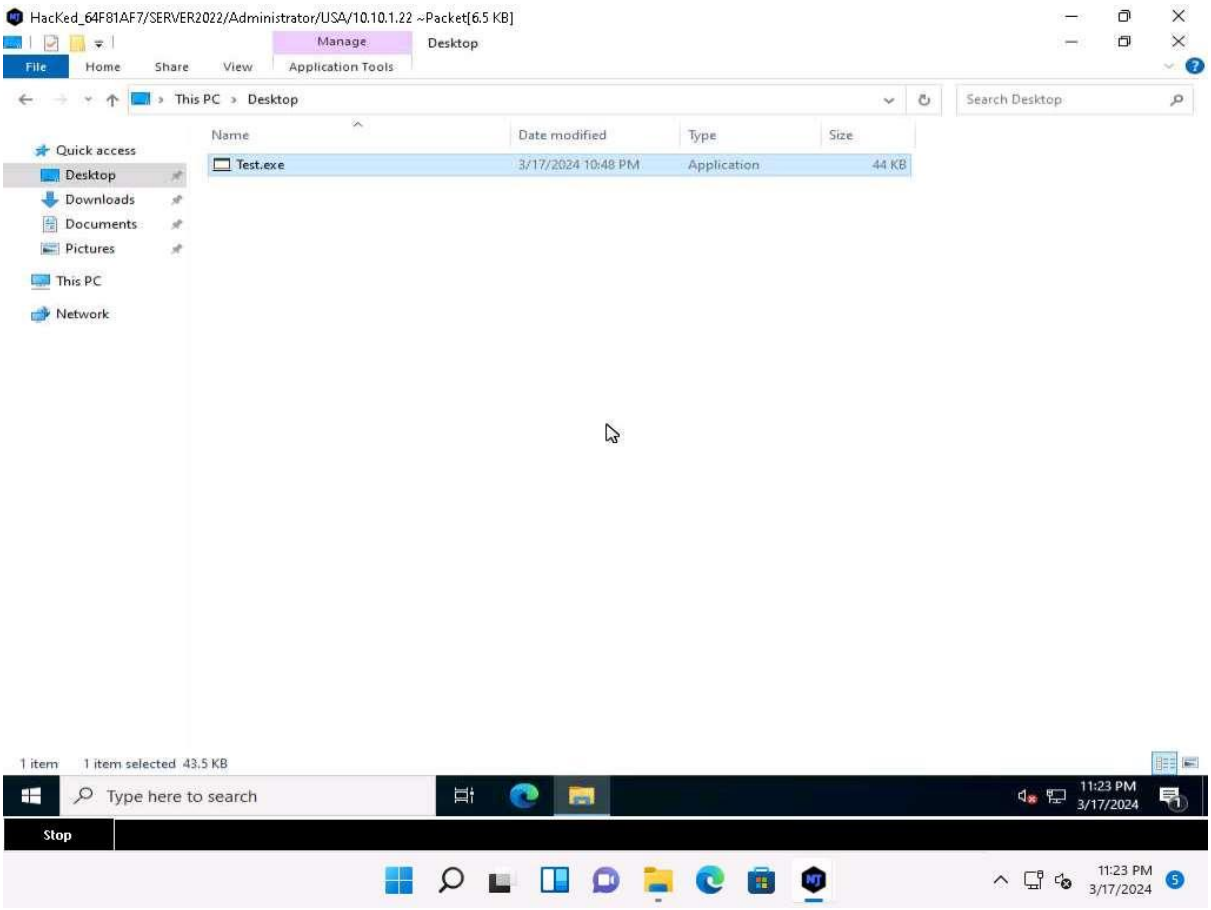
30. Right-click on the victim name, and then select **Remote Desktop**.



31. This launches a remote desktop connection without the victim's awareness.

    It might take a while for the screen to appear. If the screen is blank then switch to **Windows Server 2022** machine and unlock the machine.

32. A remote desktop window appears.

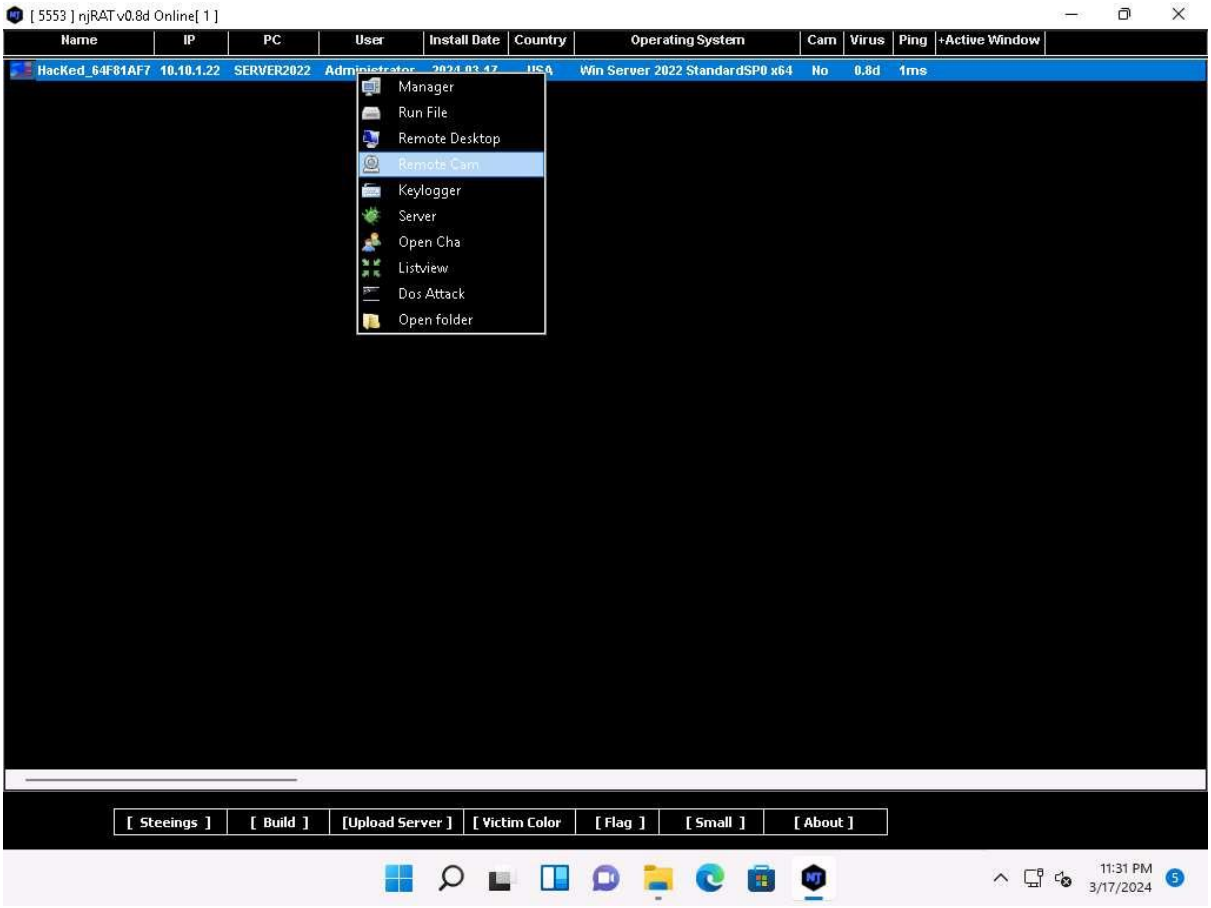


33. Now, you will be able to remotely spy the activities performed on the victim machine.

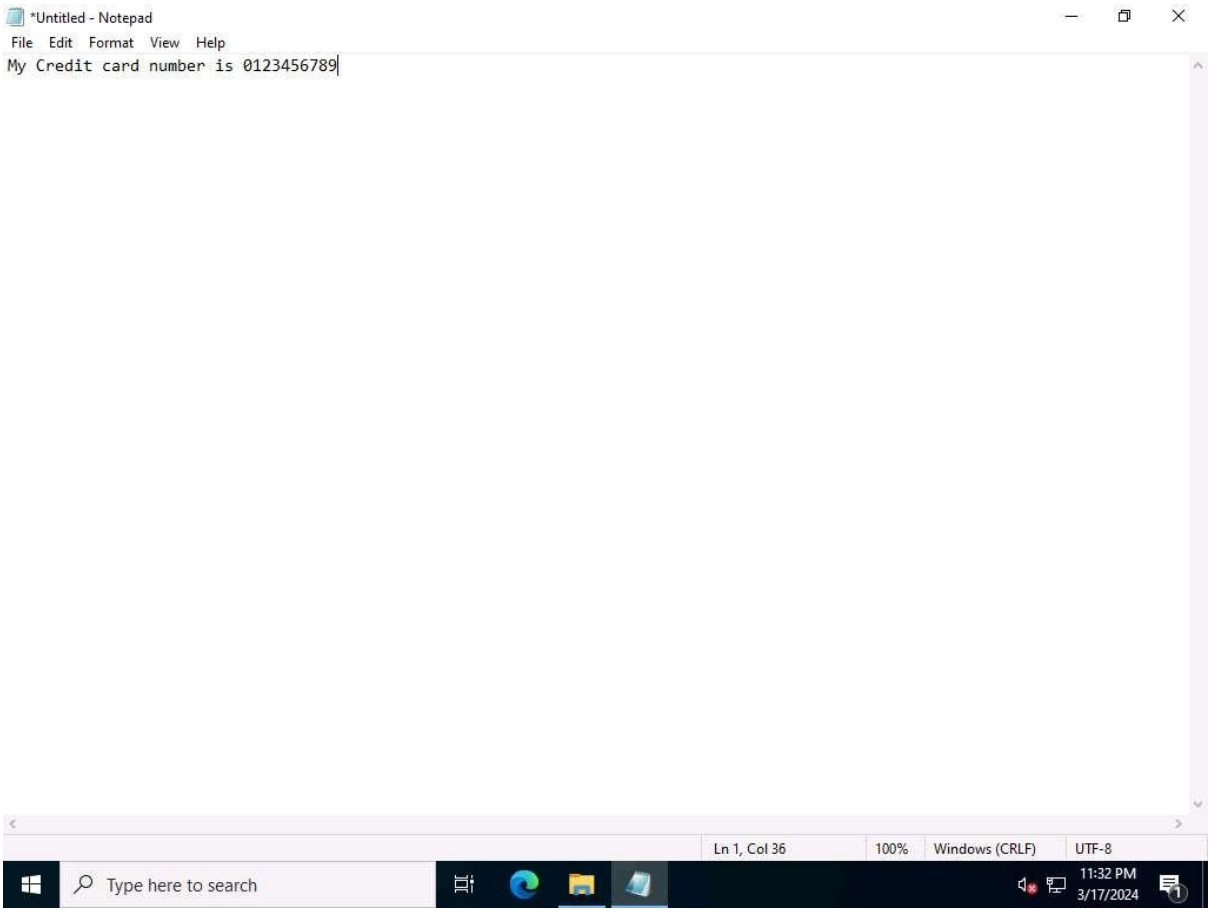
34. On completing the task, close the **Remote Desktop** window.

    If a Hacked pop-up appears, click Continue to close it.

35. In the same way, right-click on the victim name, and select **Remote Cam** to spy on them and track voice conversations.



36. Click Windows Server 2022 to switch to the **Windows Server 2022** machine. Assume that you are a legitimate user and perform a few activities such as logging into any website or typing some text in text documents.

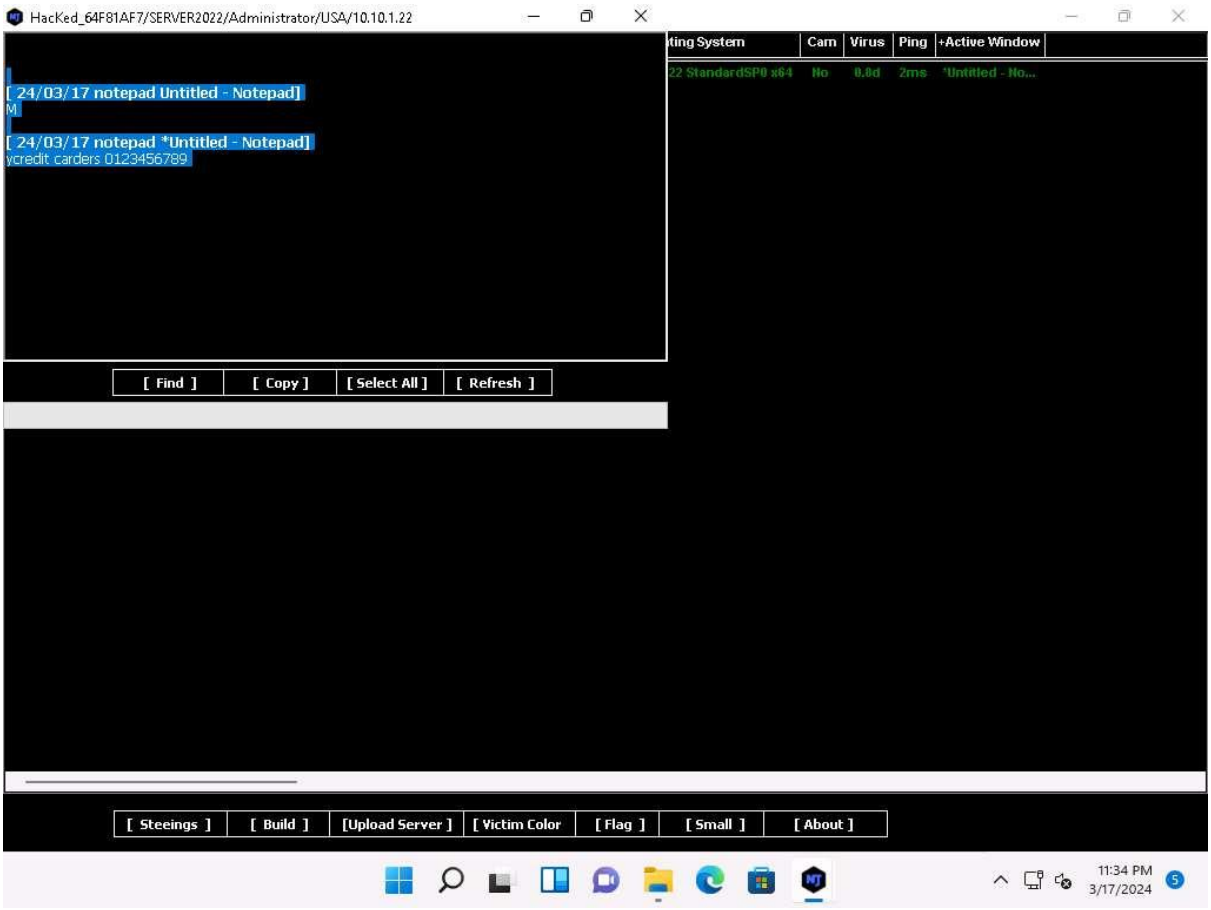


37. Click Windows 11 to switch back to the **Windows 11** machine, right-click on the victim name, and click **Keylogger**.

38. The Keylogger window appears; wait for the window to load.

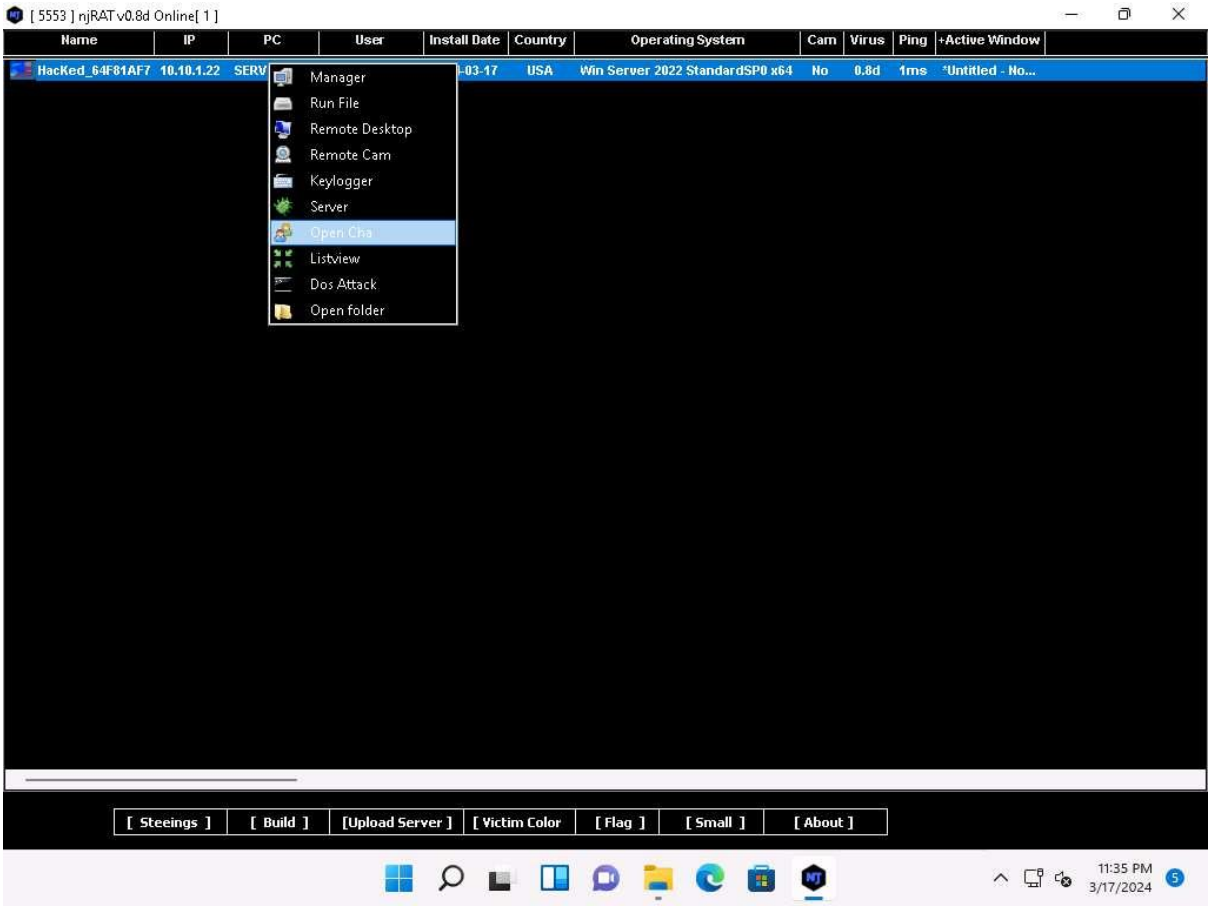
39. The window displays all the keystrokes performed by the victim on the **Windows Server 2022** machine, as shown in the screenshot.

    Select the text manually to view the keystrokes that were, typed.



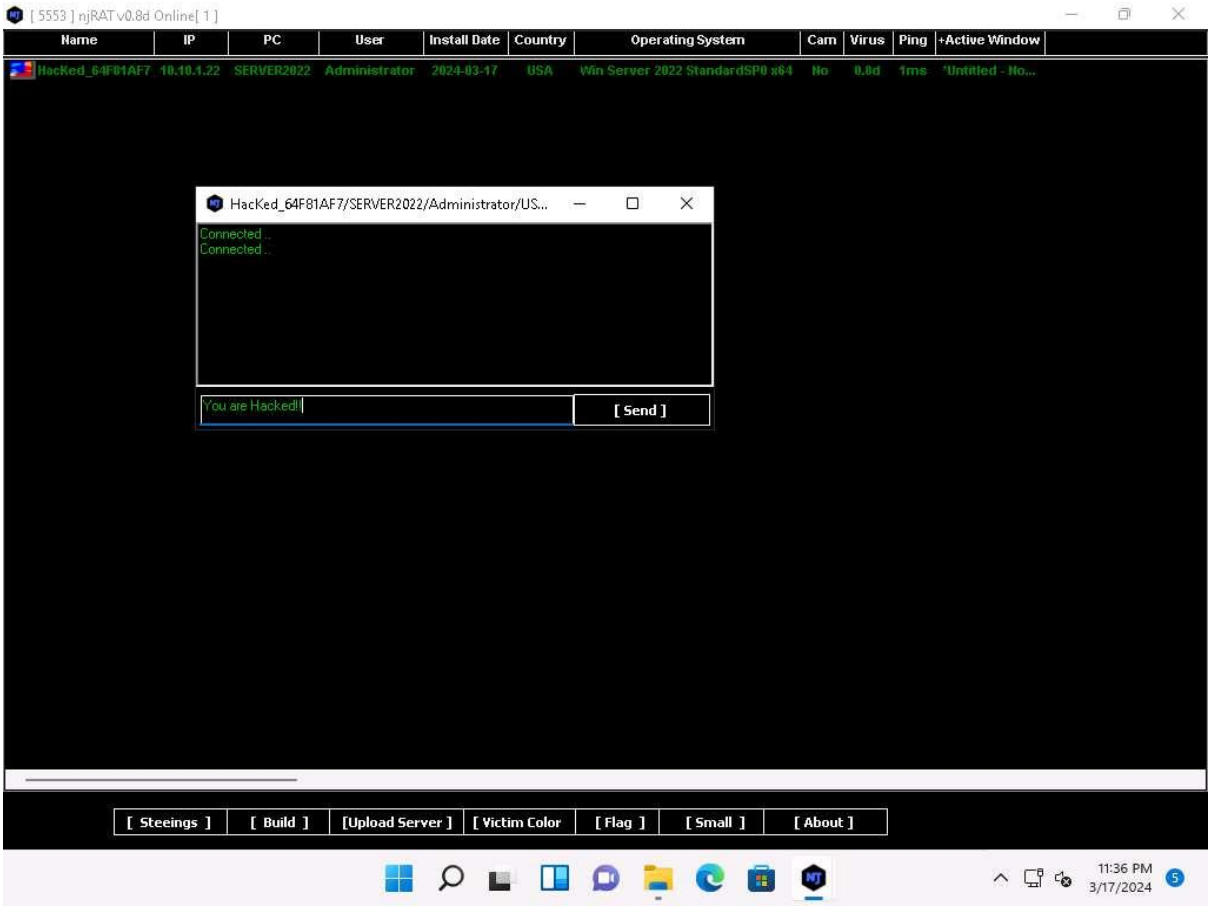
40. Close the **Keylogger** window.

41. Right-click on the victim name, and click **Open Cha**.



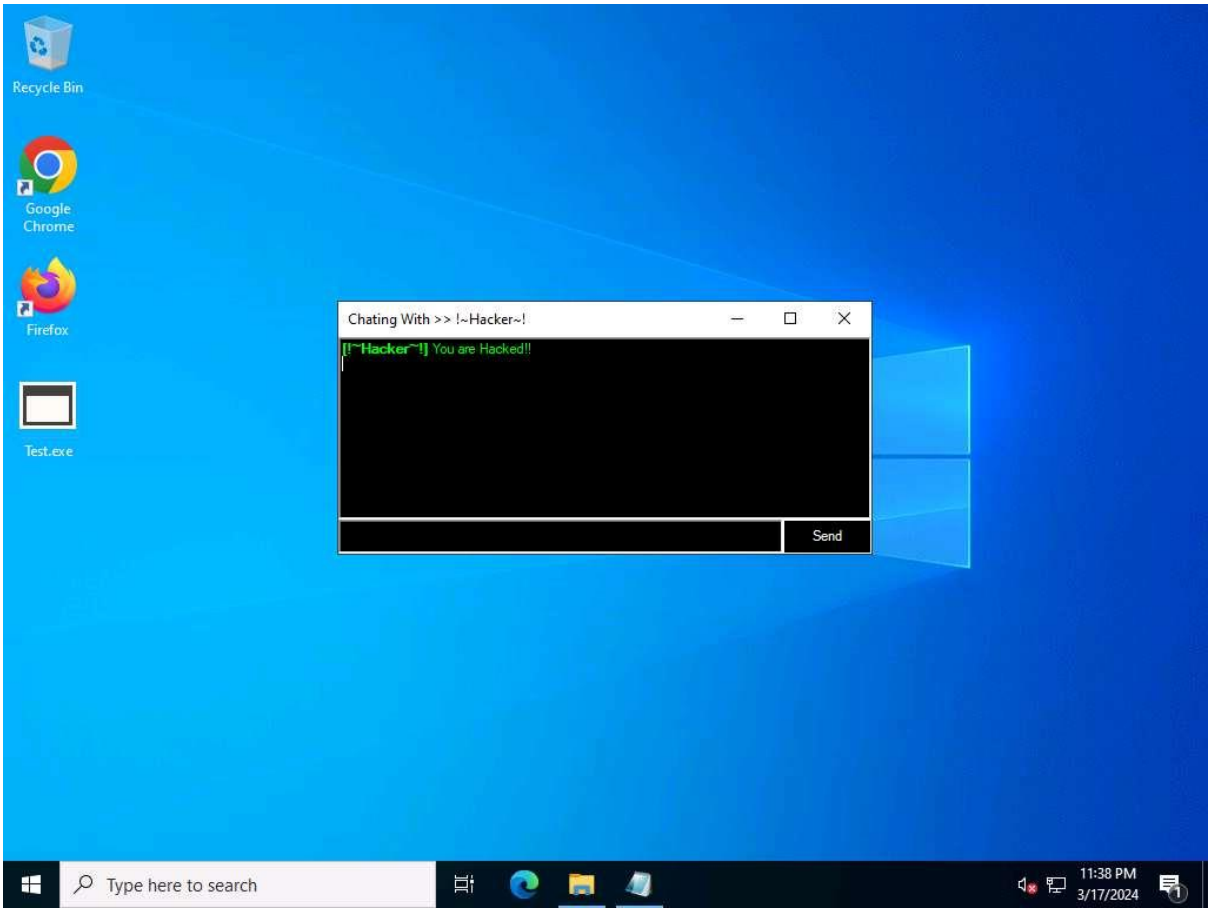
42. A **Chat** pop-up appears; enter a nickname (here, **Hacker**) and click **OK**.

43. A chat box appears; type a message, and then click **Send**.



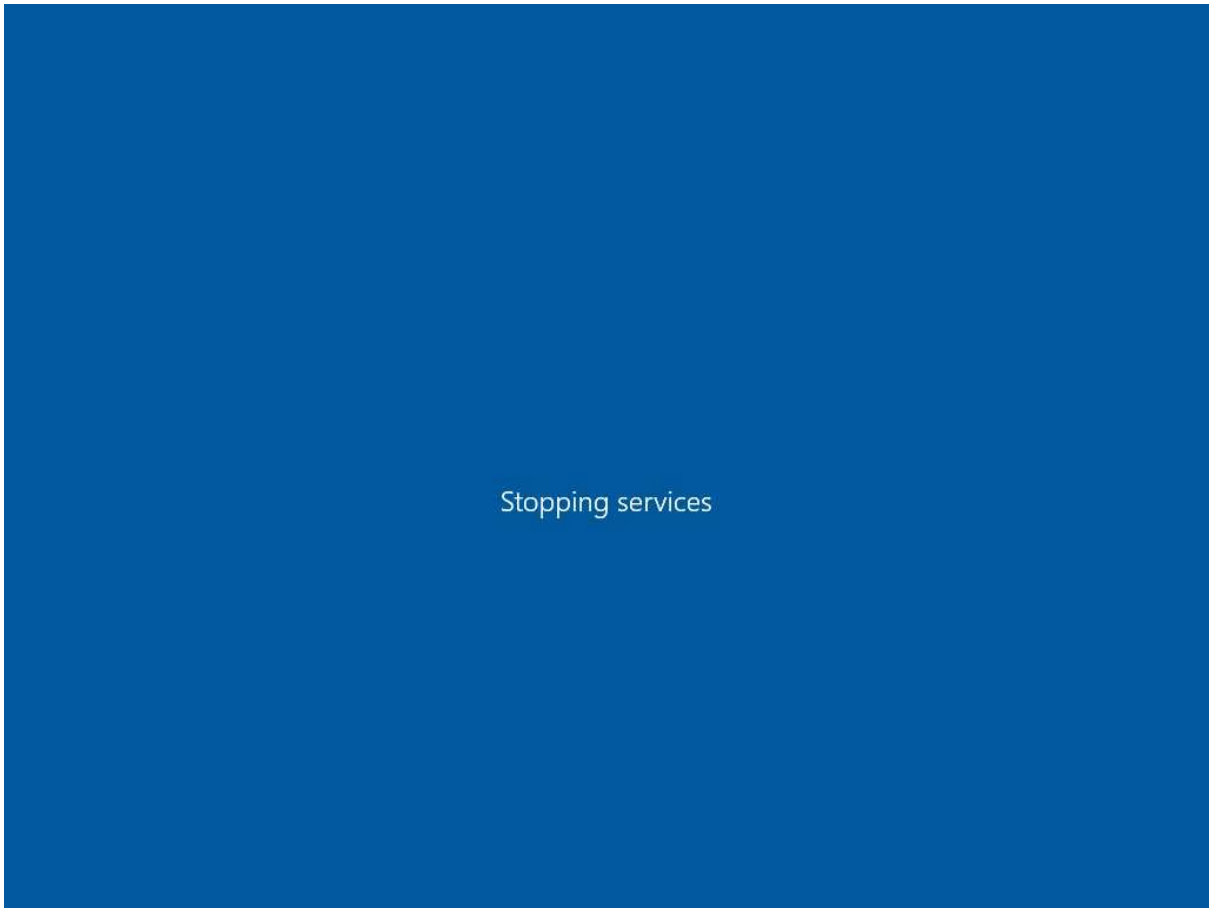
44. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows Server 2022**), as demonstrated in the screenshot.

45. Click Windows Server 2022 to switch to the **Windows Server 2022** machine, you can observe the message from the hacker appears on the screen.

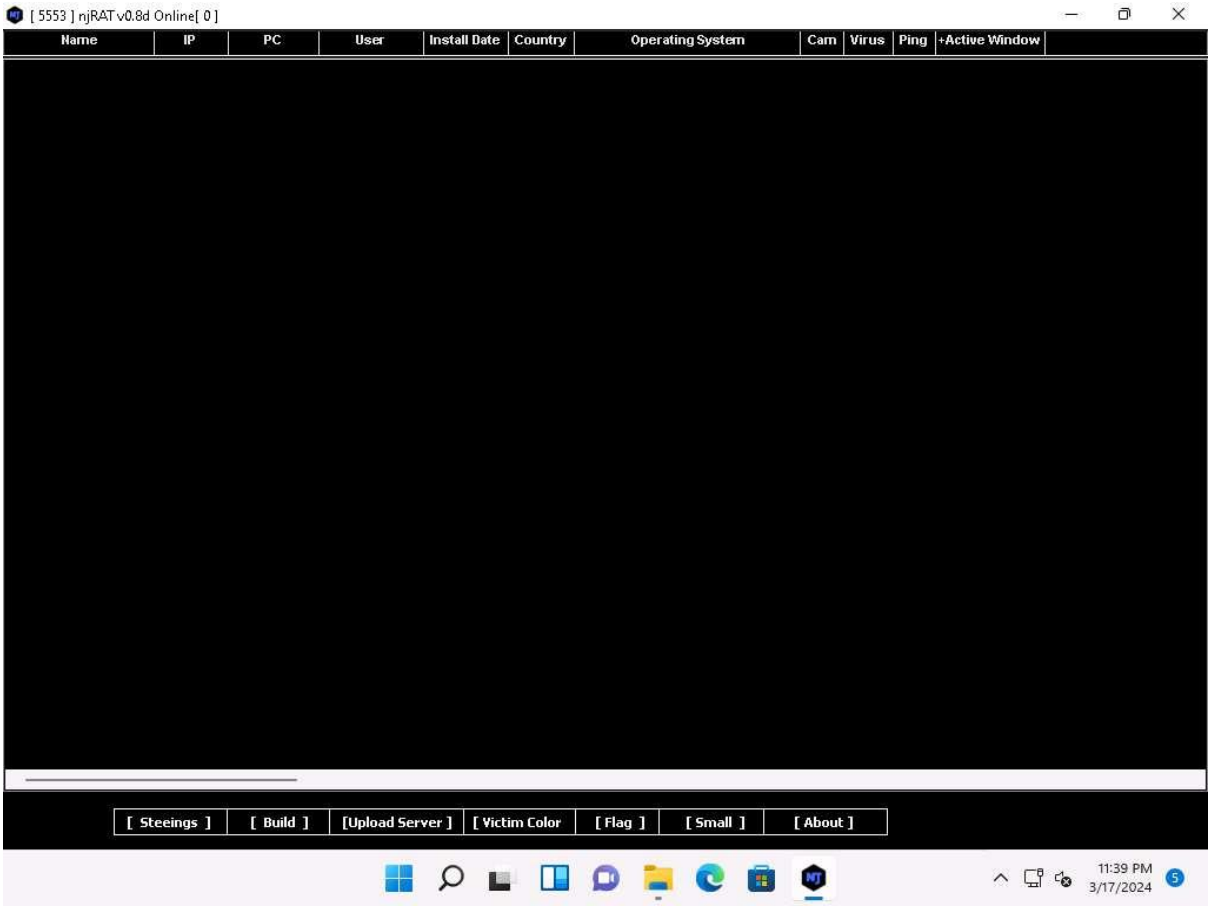


46. Seeing this, the victim becomes alert and attempts to close the chatbox. Irrespective of what the victim does, the chat box remains for open as long as the attacker uses it.

47. Surprised by the behavior, the victim (you) attempts to break the connection by restarting the machine. As soon as this happens, njRAT loses its connection with **Windows Server 2022**, as the machine is shut down in the process of restarting.

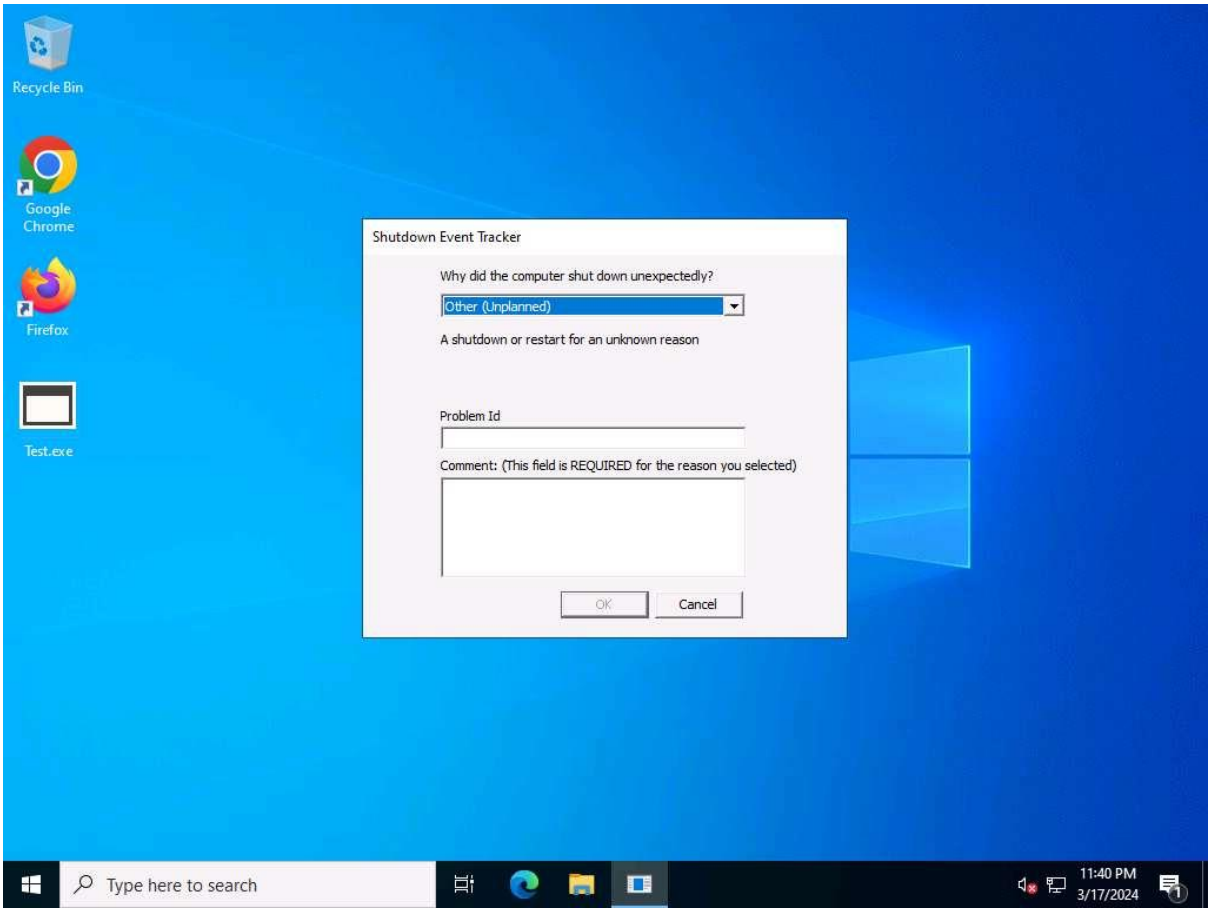


48. Click Windows 11 to switch back to the attacker machine (**Windows 11**); you can see that the connection with the victim machine is lost.



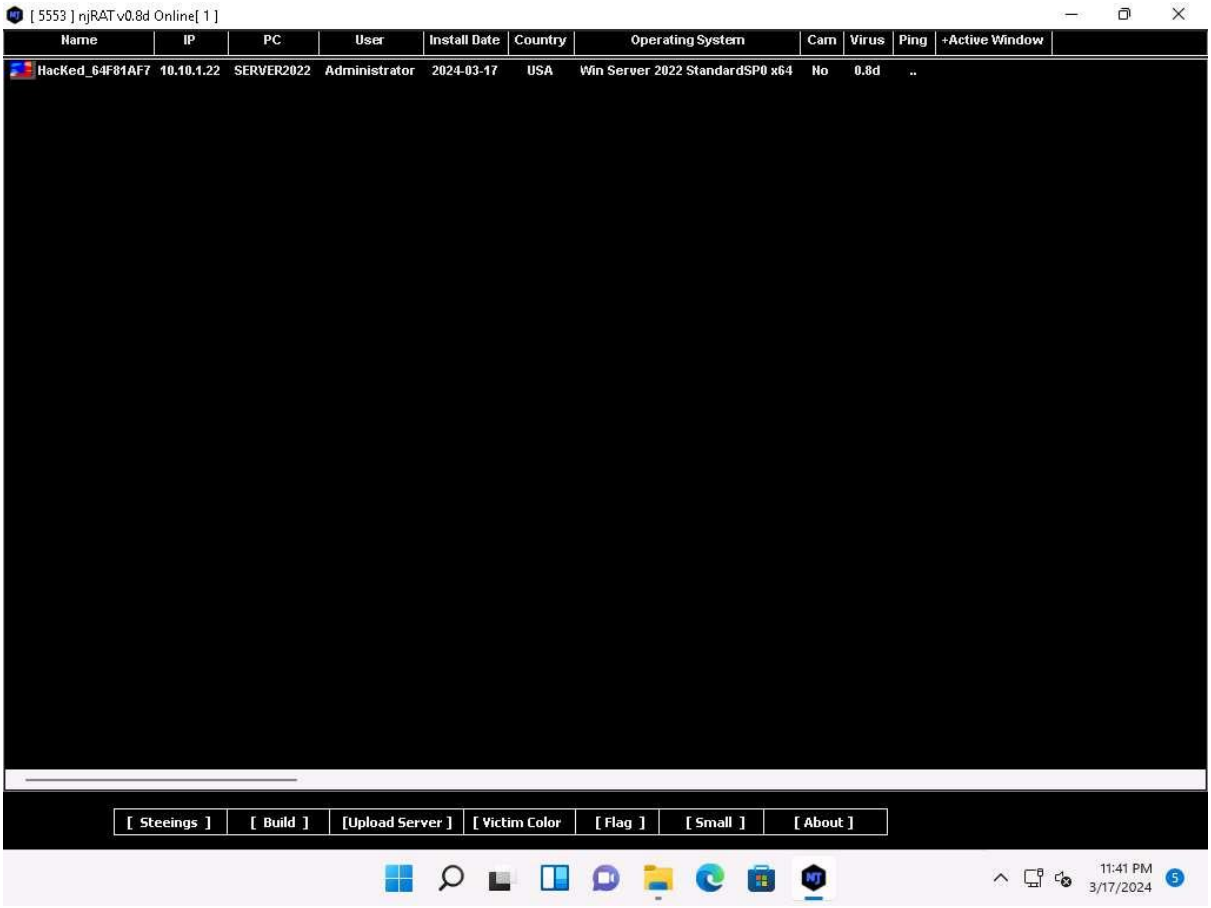
49. However, as soon as the victim logs in to their machine, the njRAT client automatically establishes a connection with the victim.

50. Click Windows Server 2022 to switch to the victim machine (**Windows Server 2022**). Click Ctrl+Alt+Delete to activate the machine and login with **CEH\Administrator / Pa$$w0rd**.



51. Click Windows 11 to switch back to the attacker machine (**Windows 11**); you can see that the connection has been re-established with the victim machine.

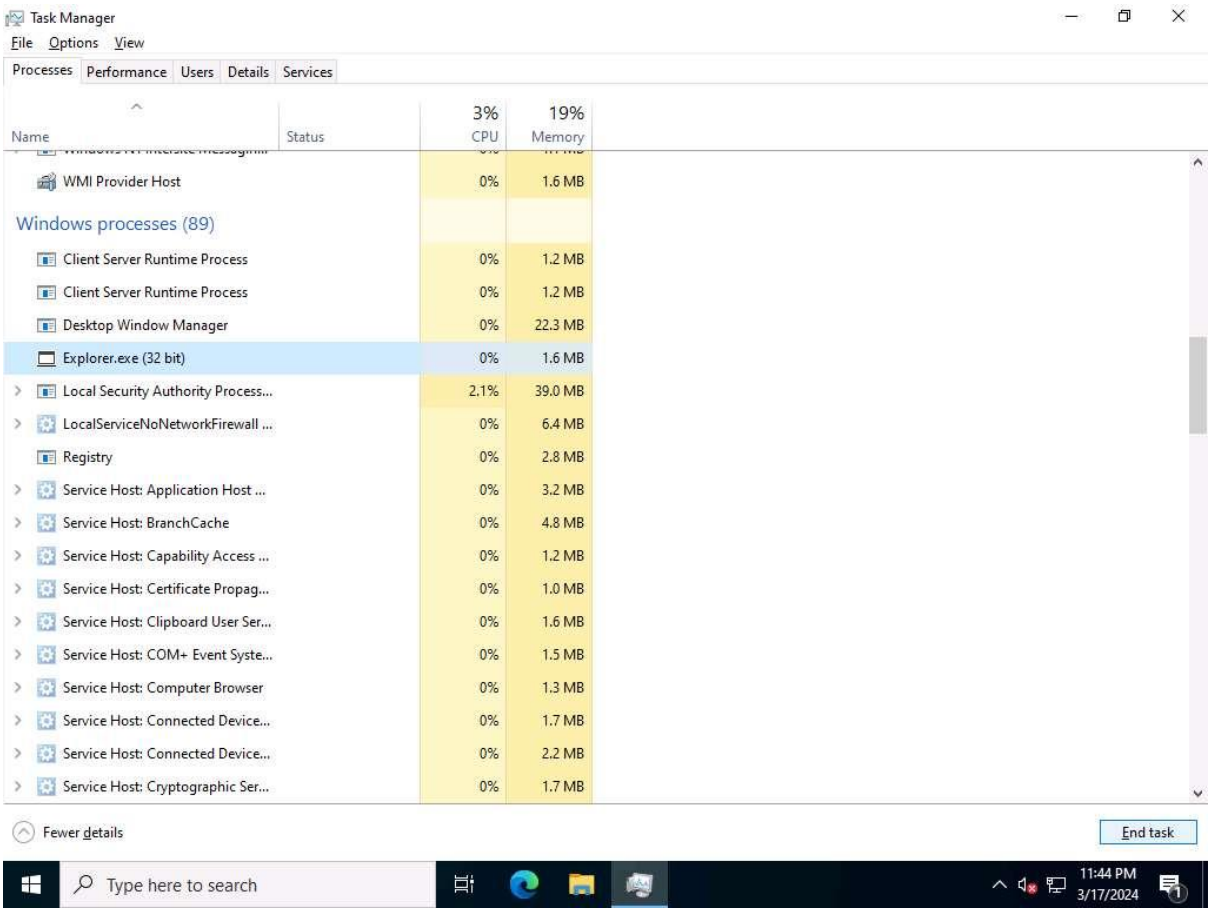
    It might take some time to establish a connection with the victim.



52. The attacker, as usual, makes use of the connection to access the victim machine remotely and perform malicious activity.

53. On completion of this lab, click Windows Server 2022 to switch to the **Windows Server 2022** machine, launch **Task Manager**, click on **More details** and look for the **Explorer.exe (32 bit)** process, and click **End task**.

    If a pop-up appears, check the **Abandon unsaved data and shut down** checkbox. and click on **Shut down**.



54. The **Windows Server 2022** machine will restart.

55. This concludes the demonstration of how to create a Trojan using njRAT Trojan to gain control over a victim machine.

56. Close all open windows in all machines.

Question 7.1.1.1

Use the Windows 11 machine (10.10.1.11) as the attacker machine and the Windows Server 2022 machine (10.10.1.22) as the victim machine. Run the njRAT Trojan from the attacker machine and gain control over the victim machine. What is the default port used for njRAT in this lab?

Question 7.1.1.2

Use the Windows 11 machine (10.10.1.11) as the attacker machine and the Windows Server 2022 machine (10.10.1.22) as the victim machine. Enter the Host Name of the victim machine displayed in njRAT Remote Shell.

Lab 2: Infect the Target System using a Virus

Lab Scenario

Viruses are the scourges of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce. Therefore, attackers design every virus code in such a manner that the virus replicates itself n number of times, where n is a number specified by the attacker. Worldwide, most businesses have been infected by a virus at some point. Like a biological virus, a computer virus is contagious and can contaminate other files; however, viruses can only infect outside machines with the assistance of computer users.

Like viruses, computer worms are standalone malicious programs that independently replicate, execute, and spread across network connections, without human intervention. Worms are a subtype of virus. Intruders design most worms to replicate and spread across a network, thus consuming available computing resources and, in turn, causing network servers, web servers, and individual computer systems to become overloaded and stop responding. However, some worms also carry a payload to damage the host system.

An ethical hacker and pen tester during an audit of a target organization must determine whether viruses and worms can damage or steal the organization's information. They might need to construct viruses and worms and try to inject them into the target network to check their behavior, learn whether an anti-virus will detect them, and find out whether they can bypass the firewall.

Lab Objectives

- Create a virus using the JPS Virus Maker Tool and infect the target system

Overview of Viruses and Worms

Viruses can attack a target host's system using a variety of methods. They can attach themselves to programs and transmit themselves to other programs by making use of specific events. Viruses need such events to take place, since they cannot self-start, infect hardware, or transmit themselves using non-executable files. "Trigger" and "direct attack" events can cause a virus to activate and infect the target system when the user triggers attachments received through email, Web sites, malicious advertisements, flashcards, pop-ups, or other methods. The virus can then attack a system's built-in programs, antivirus software, data files, and system startup settings, or perform other malicious activities.

Like a virus, a worm does not require a host to replicate, but in some cases, the worm's host machine also infects. At first, Blackhat professionals treated worms as a mainframe problem. Later, with the introduction of the Internet, they concentrated and targeted Windows OSes using the same worms by sharing them by email, IRC, and other network functions.

Task 1: Create a Virus using the JPS Virus Maker Tool and Infect the Target System

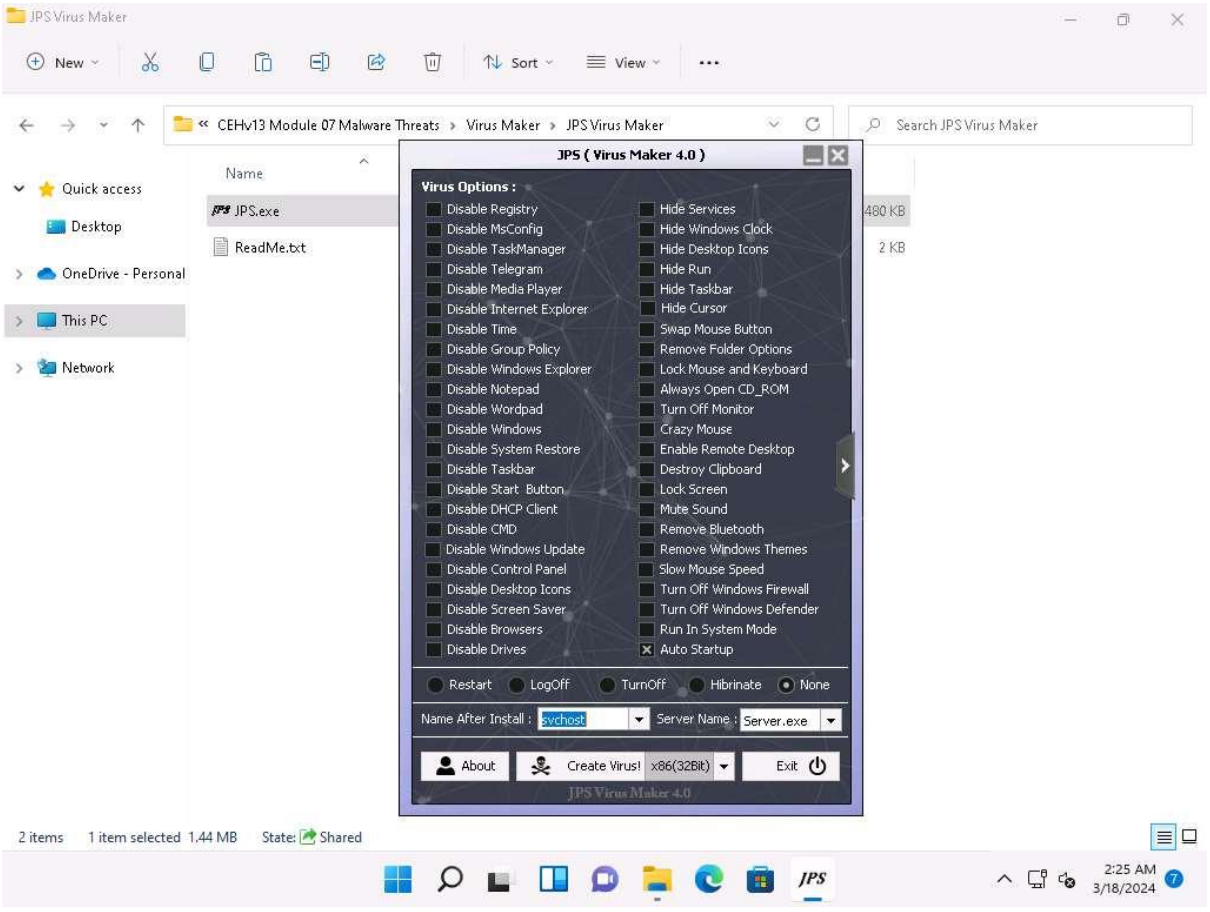
The JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool's features are auto-start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows. An ethical hacker and pen-tester can use the JPS Virus Maker Tool as a proof of concept to audit perimeter security controls in an organization.

After performing this task, we will revert the machine to its initial state, as the **Windows Server 2019** machine will be infected by the virus. To do this, click on the Power and Display button and select the **Revert Machine**. If the Revert Machine option is not working, end the lab and re-launch it to reset the machines. To do this, click the Exit Lab option and select End lab from the drop-down menu.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **JPS.exe**.

   If an **Open File - Security** Warning pop-up appears, click **Run**.

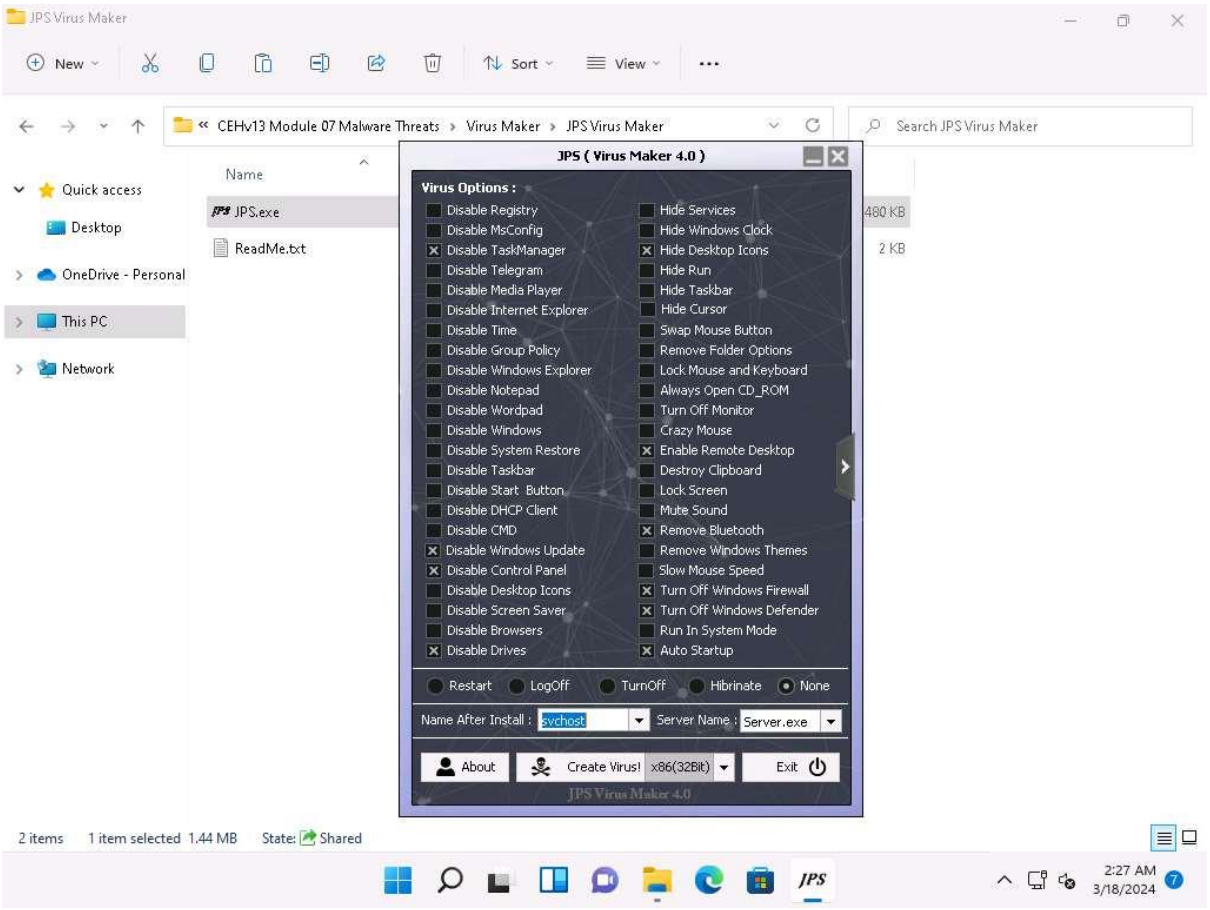
2. The **JPS (Virus Maker 4.0)** window appears; tick the **Auto Startup** checkbox.



3. The window displays various features and options that can be chosen while creating a virus file.

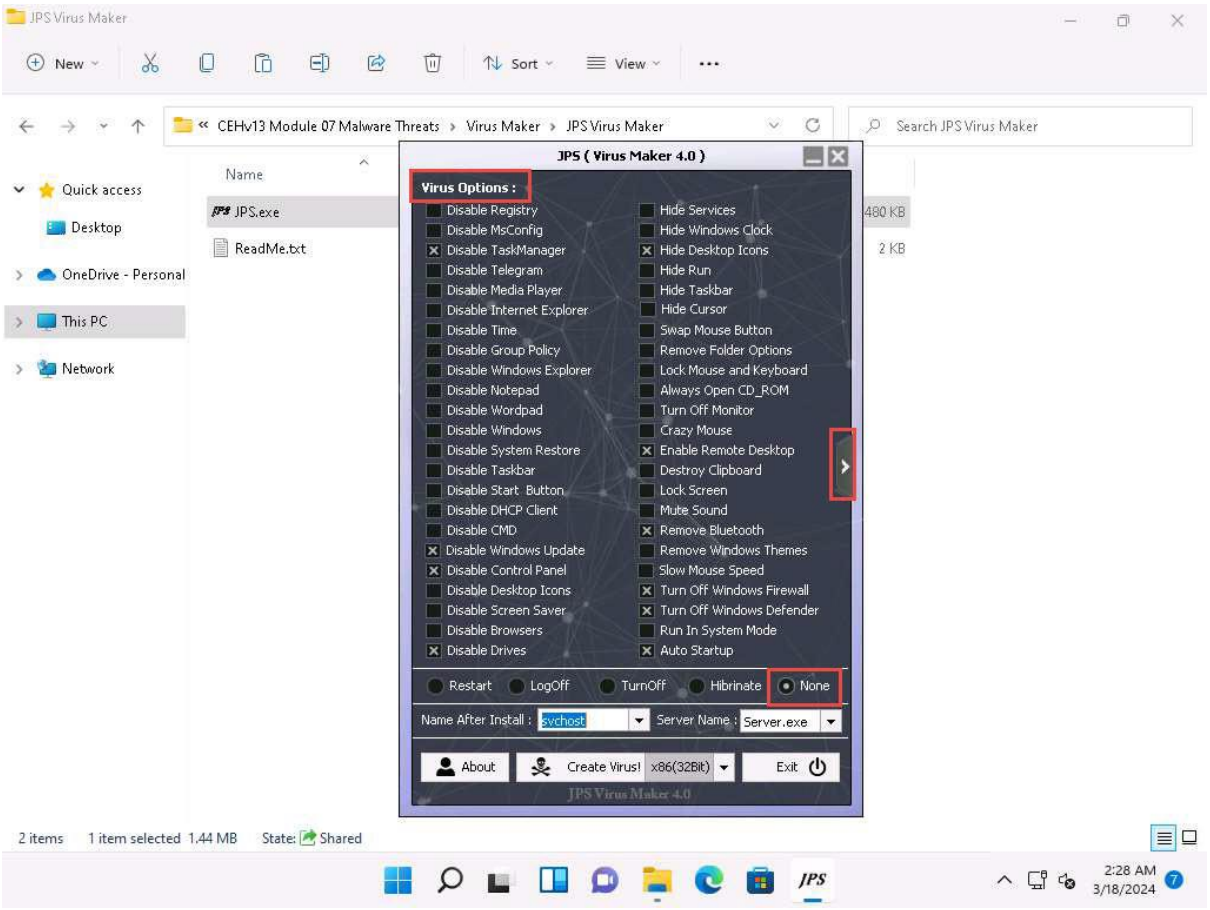
4. From the **Virus Options**, check the **options** that you want to embed in a new virus file.

5. In this task, the options embedded in the virus file are **Disable TaskManager**, **Disable Windows Update**, **Disable Control Panel**, **Disable Drives**, **Hide Desktop Icons**, **Enable Remote Desktop**, **Remove Bluetooth**, **Turn Off Windows Firewall**, **Turn Off Windows Defender**, and **Auto Startup**.



6. Ensure that the **None** radio button is selected to specify the trigger event when the virus should start attacking the system after its creation.

7. Now, click the right arrow icon from the right-hand pane of the window to configure the virus options.



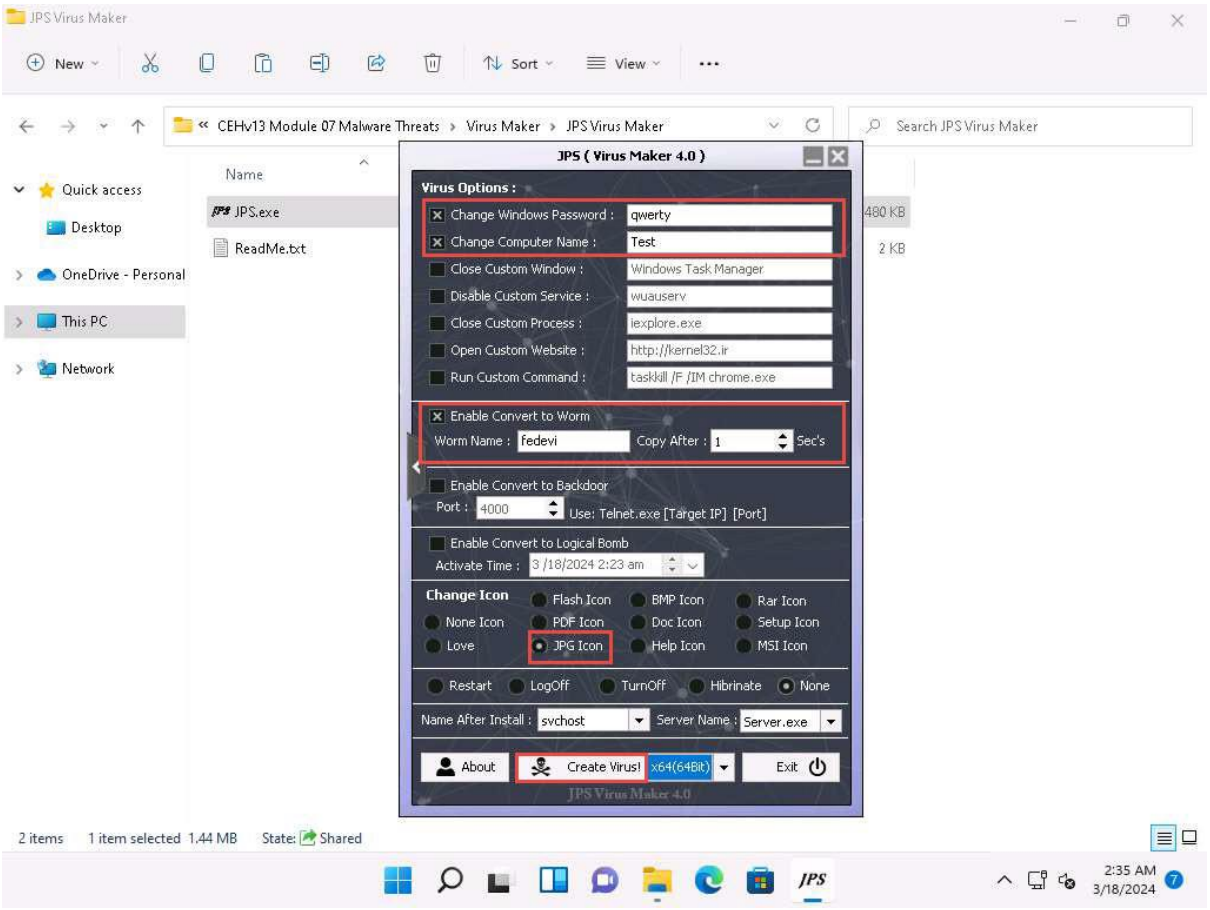
8. A **Virus Options** window appears.

9. Check the **Change Windows Password** option, and enter a password (here, **qwerty**) in the text field. Check the **Change Computer Name** option, and type **Test** in the text field.

10. You can even configure the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox, and provide a **Worm Name** (here, **fedevi**). For the worm to self-replicate after a particular time, specify the time in seconds (here, **1 second**) in the **Copy After** field.

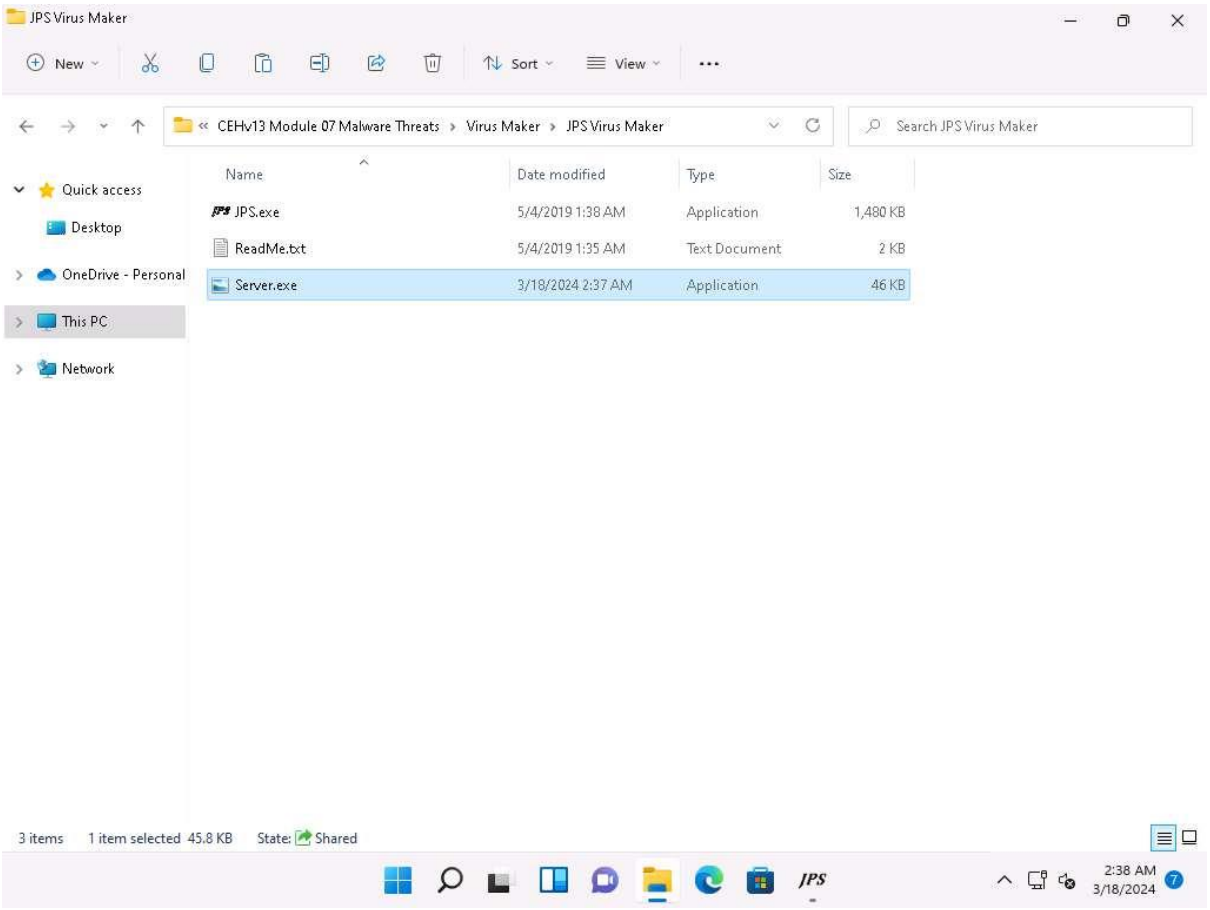
11. Ensure that the **JPG Icon** radio button is selected under the **Change Icon** section. Ensure that the **None** radio button is selected in the lower part of the window.

12. After completing your selection of options, click the drop-down icon next to the **Create Virus!** button and select **x64(64Bit)**; click **Create Virus!**



13. A **Virus Created Successful!** pop-up appears; click **OK**.

14. The newly created virus (server) is placed automatically in the **folder** where jps.exe is located, but with the name **Server.exe**. Navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and observe that the newly created virus with the name **Server.exe** is available at the specified location.



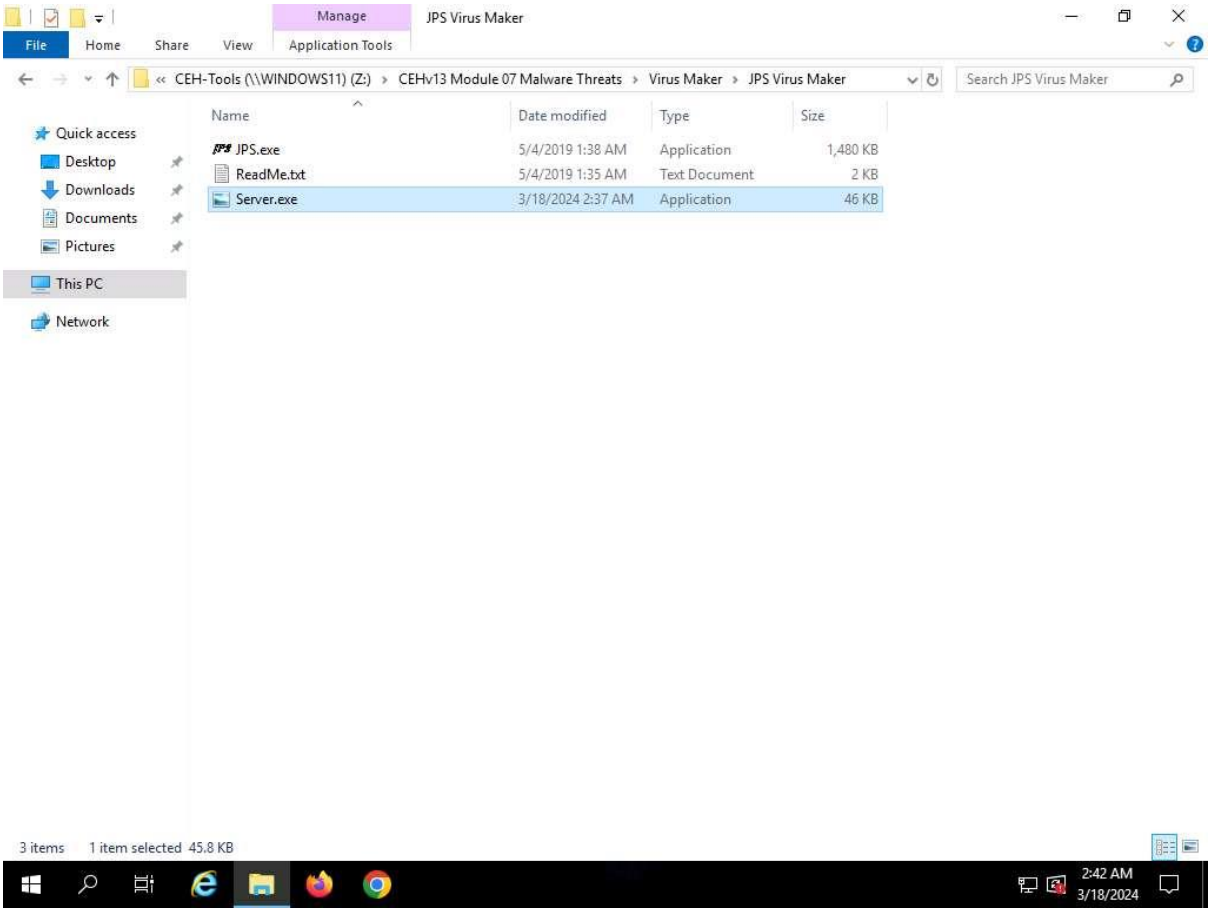
15. Now, pack this virus with a binder or virus packager and send it to the victim machine through email, chat, a mapped network drive, or other method.

16. In this task, we are using a mapped network drive to share the virus file to the victim machine. Assume that you are a victim and that you have received this file.

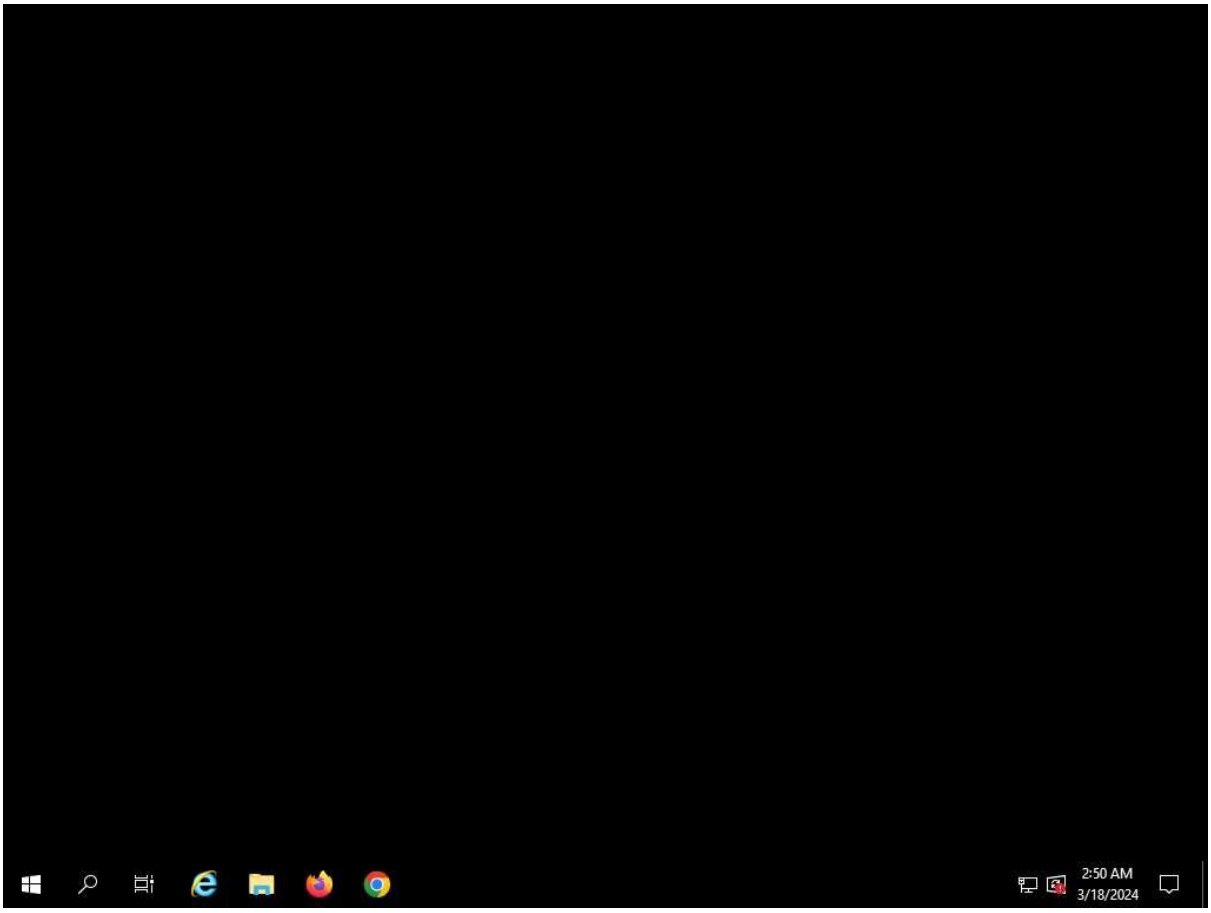
17. Click Windows Server 2019 to switch to the **Windows Server 2019** machine. Click Ctrl+Alt+Delete to activate the machine, login with **Administrator/Pa$$w0rd**.

    Here, we are logging into the machine as a victim.

18. Navigate to **Z:\CEHv13 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **Server.exe** file to execute the virus.

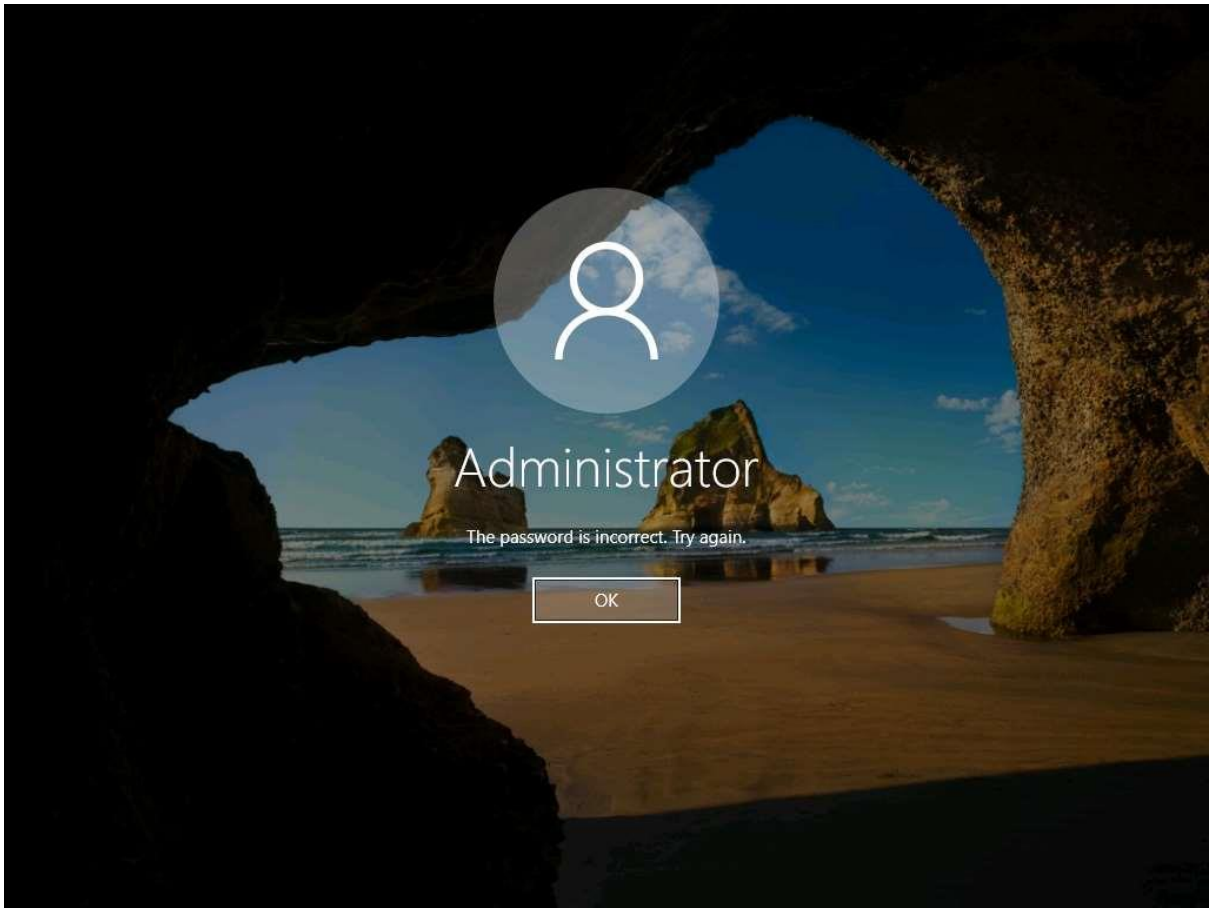


19. Once you have executed the virus, close the window and you can observe that the **Desktop** screen goes blank, indicating that the virus has infected the system, as shown in the screenshot.

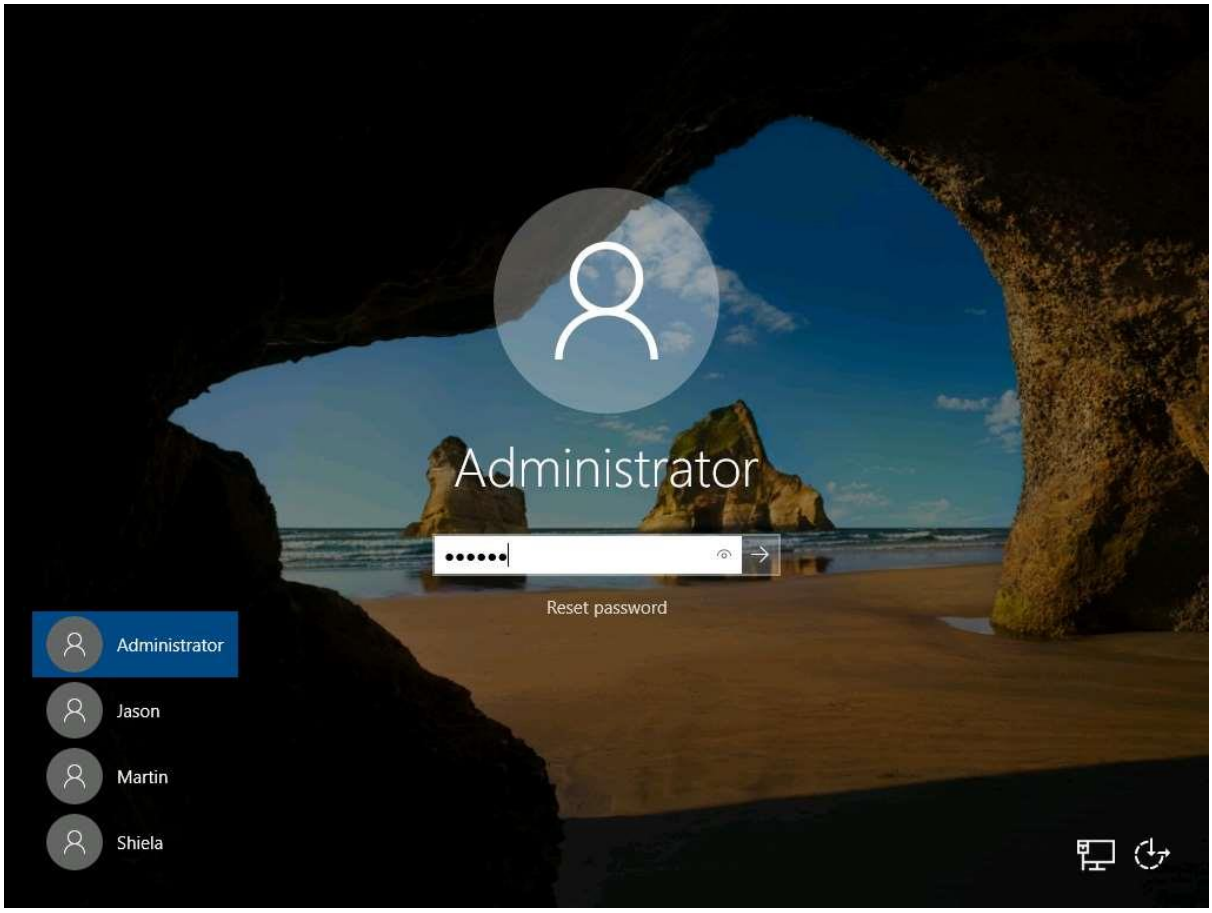


20. Surprised by the system behavior, the victim (you) attempts to fix the machine by restarting it. Once the machine has rebooted, try to log in to the machine with the provided **Username** and **Password**. You should receive the error message "the password is incorrect. Try again."

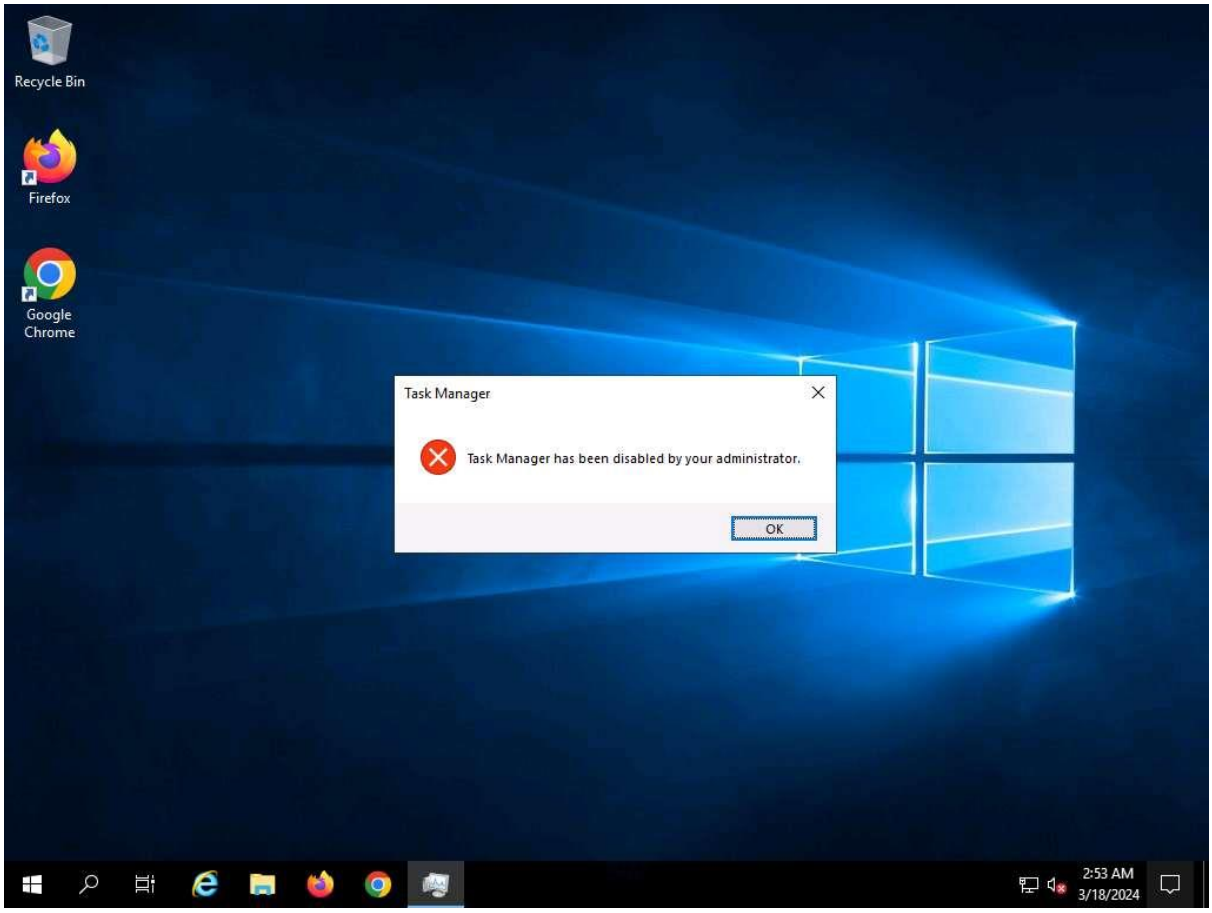
21. Click Ctrl+Alt+Delete to activate the machine, login with **Administrator/Pa$$w0rd**.



22. Click **OK** and login with the password that you provided at the time of virus creation (i.e., **qwerty**). You should log in to the machine with the new password.



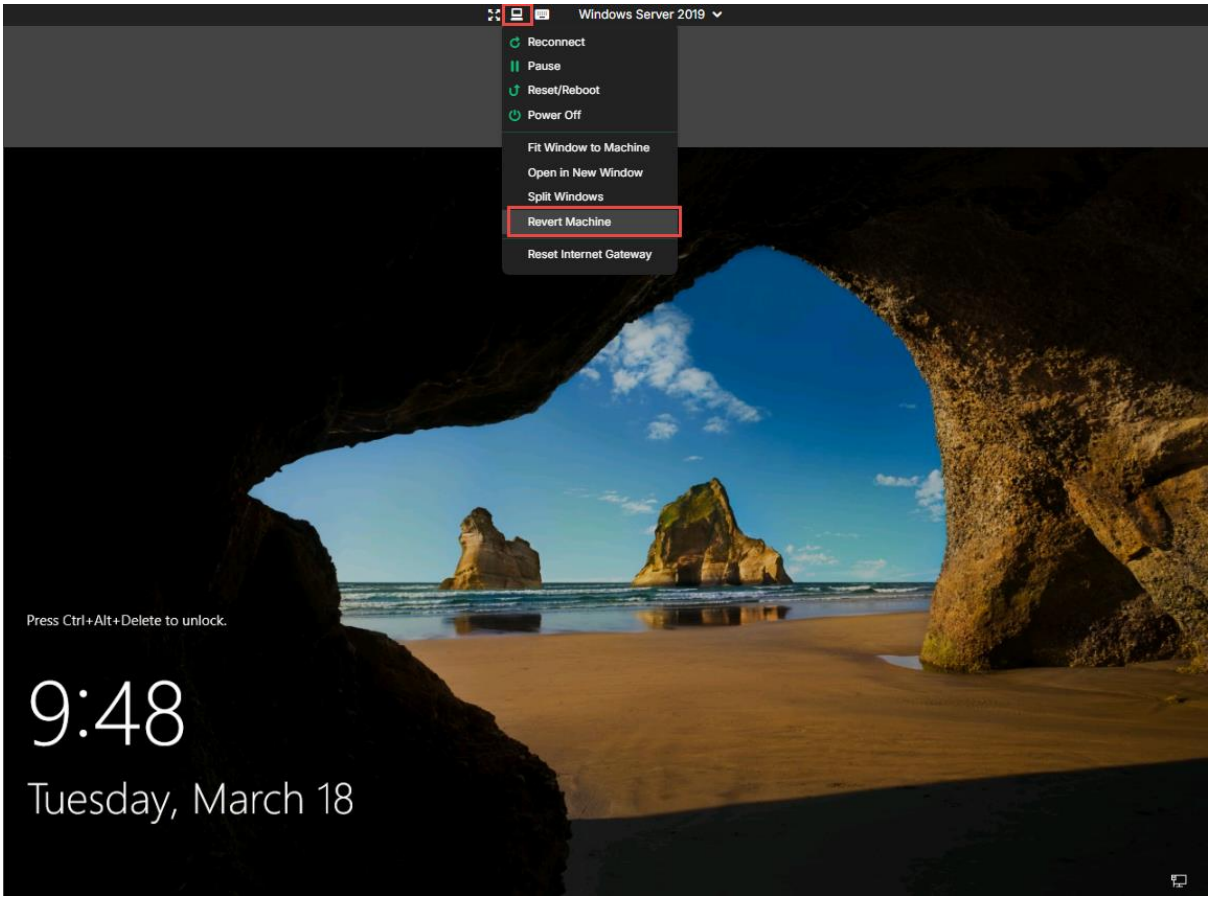
23. Now, try to open **Task Manager**; observe that an opening error pop-up appears, and then click **OK**.



24. You will get a similar error for all the applications that are disabled by the virus.

25. This is how attackers infect a system with viruses. Now before proceeding to the next task, revert the Windows Server 2019 Windows 11 machines to its initial state. To do this, click on the **Power and Display** button and select the **Revert Machine** option from the drop-down list as shown in the screenshot.

    If **Revert Machine** option is not working, end the lab and re-launch it to reset the machines. To do so, click the **Exit Lab** option and click **End lab** from the drop-down options.
    Before relaunching the lab, it is recommended to save all obtained answers. You can continue from next task by placing all the answers in their respective flags.



Question 7.2.1.1

In the Windows 11 machine, create a virus using the JPS Virus Maker tool and infect the Windows Server 2019 machine. What is the default custom website used by JPS Virus Maker 4.0?

Lab 3: Perform Static Malware Analysis

Lab Scenario

Attackers use sophisticated malware techniques as cyber weapons to steal sensitive data. Malware can inflict intellectual and financial losses on the target, be it an individual, a group of people, or an organization. The worst part is that it spreads from one system to another with ease and stealth.

Malware such as viruses, Trojans, worms, spyware, and rootkits allow an attacker to breach security defenses and subsequently launch attacks on target systems. Thus, to find and cure the existing infections and thwart future problems, it is necessary to perform malware analysis. Many tools and techniques exist to perform such tasks. Malware analysis provides an in-depth understanding of each individual sample and identifies emerging technology trends from large collections of malware samples without executing them. The samples of malware are mostly compatible with the Windows binary executable.

By performing malware analysis, detailed information regarding the malware can be extracted. This information includes items like the malicious intent of the malware, indicators of compromise, complexity level of the intruder, exploited vulnerability, extent of damage caused by the intrusion, perpetrator accountable for installing the malware, and system vulnerability the malware has exploited. An ethical hacker and pen tester must perform malware analysis to understand the workings of the malware and assess the damage that it may cause to the information system. Malware analysis is an integral part of any penetration testing process.

It is very dangerous to analyze malware on production devices connected to production networks. Therefore, one should always analyze malware samples in a testing environment on an isolated network.

Lab Objectives

- Perform malware scanning using Hybrid Analysis
- Analyze ELF executable file using Detect It Easy (DIE)
- Perform malware disassembly using IDA and OllyDbg

Overview of Static Malware Analysis

Static Malware Analysis, also known as code analysis, involves going through the executable binary code without executing it to gain a better understanding of the malware and its purpose. The process includes the use of different tools and techniques to determine the malicious part of the program or a file. It also gathers information about malware functionality and collects the technical pointers or simple signatures it generates. Such pointers include file name, MD5 checksums or hashes, file type, and file size. Analyzing the binary code provides information about the malware's functionality, network signatures, exploit packaging technique, dependencies involved, as well as other information.

Some of the static malware analysis techniques are:

- File fingerprinting
- Local and online malware scanning
- Performing strings search
- Identifying packing and obfuscation methods
- Finding portable executable (PE) information
- Identifying file dependencies
- Malware disassembly

Task 1: Perform Malware Scanning using Hybrid Analysis

Hybrid Analysis is a free service that analyzes suspicious files and URLs and facilitates the quick detection of unknown threats such as viruses, worms, Trojans, and other kinds of malware.

It helps ethical hackers and penetration testers to examine files and URLs, enabling the identification of viruses, worms, Trojans, and other malicious content detected by anti-virus engines and website scanners.

This task will demonstrate how to analyze malware using online Hybrid Analysis services.

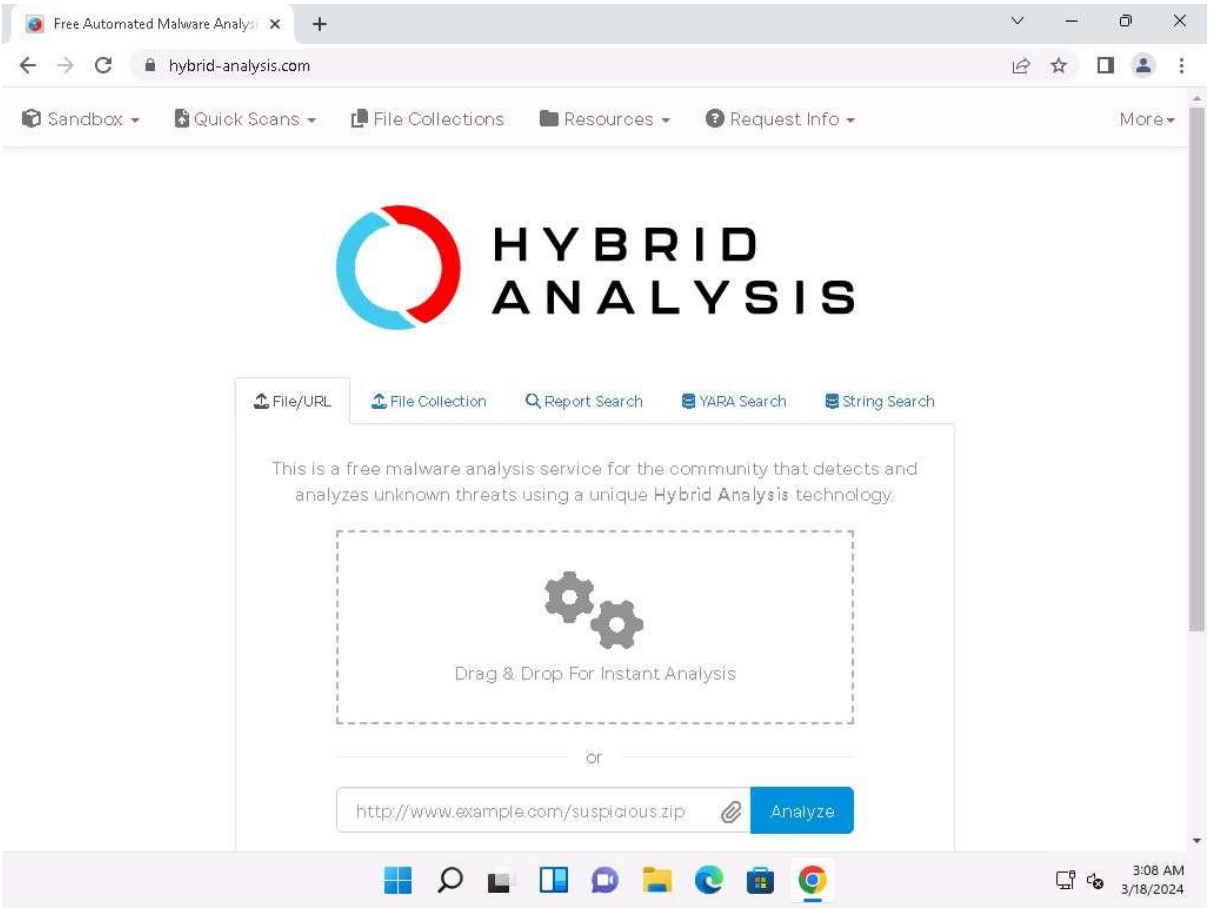
1. By default, **Windows 11** machine selected, click Ctrl+Alt+Delete. Login with **Admin/Pa$$w0rd**.

   Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

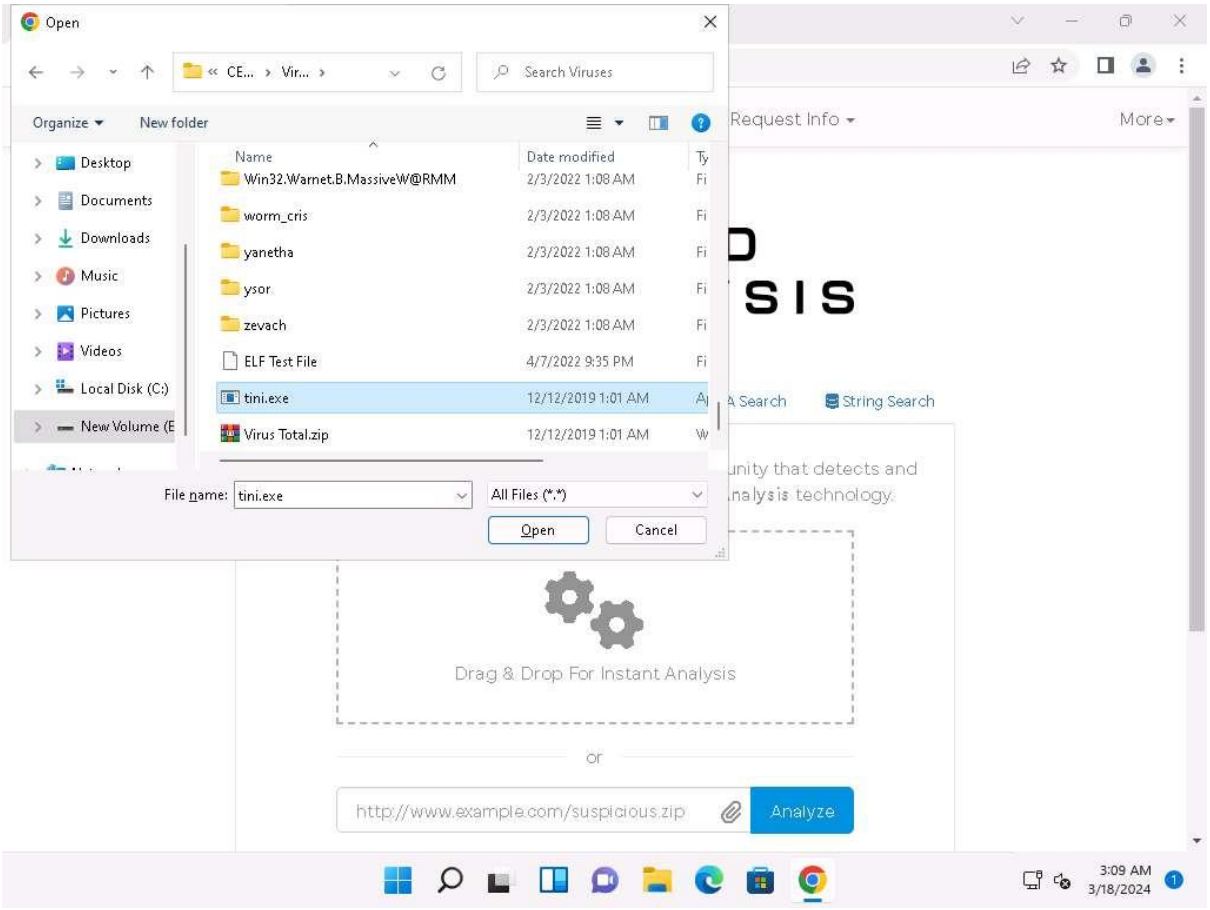
2. Open any web browser (here, **Google Chrome**) and go to **https://www.hybrid-analysis.com** and press **Enter**.

   If a cookie notification appears in the lower section of the page, then click **ACCEPT**.

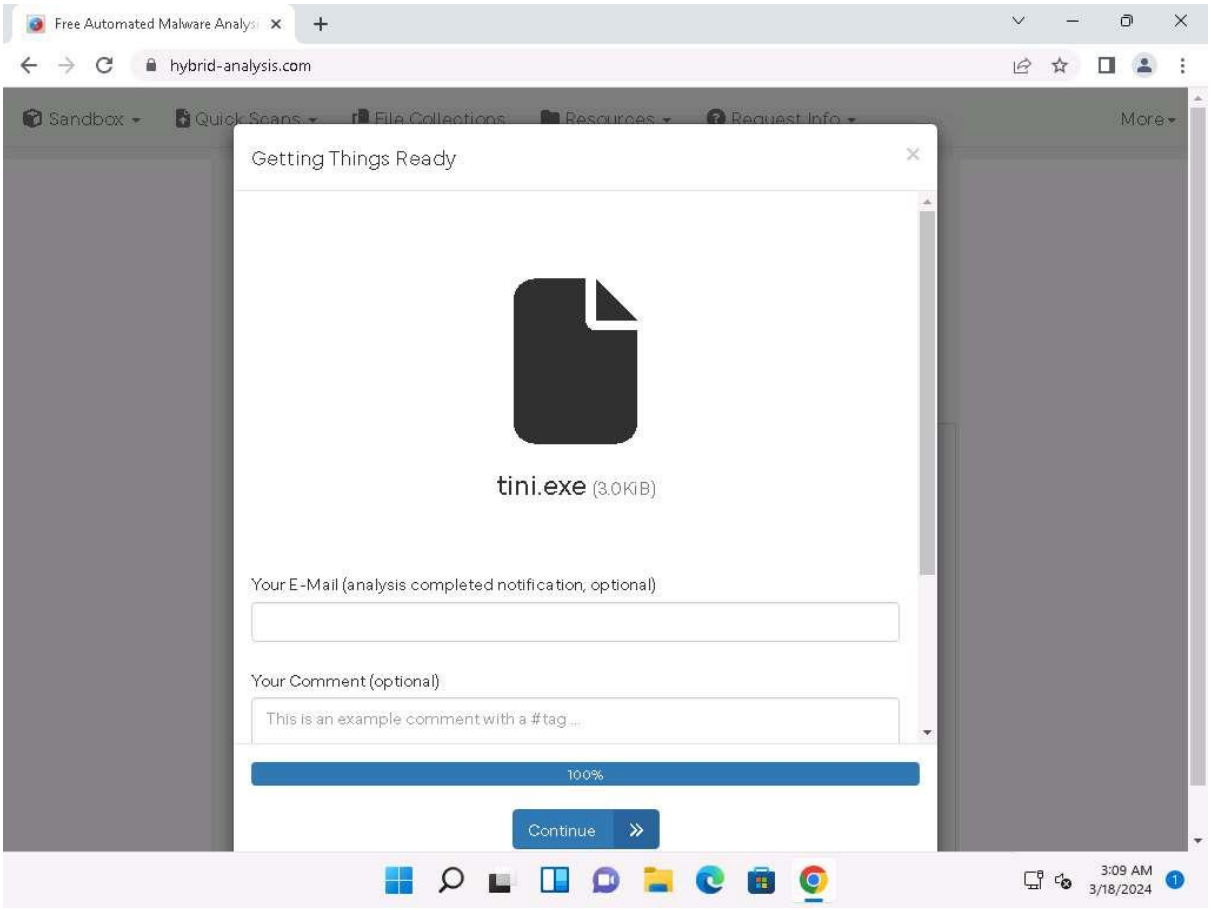
3. The **HYBRID ANALYSIS** main page appears; click **Drag & Drop For Instant Analysis** section to upload a virus file.



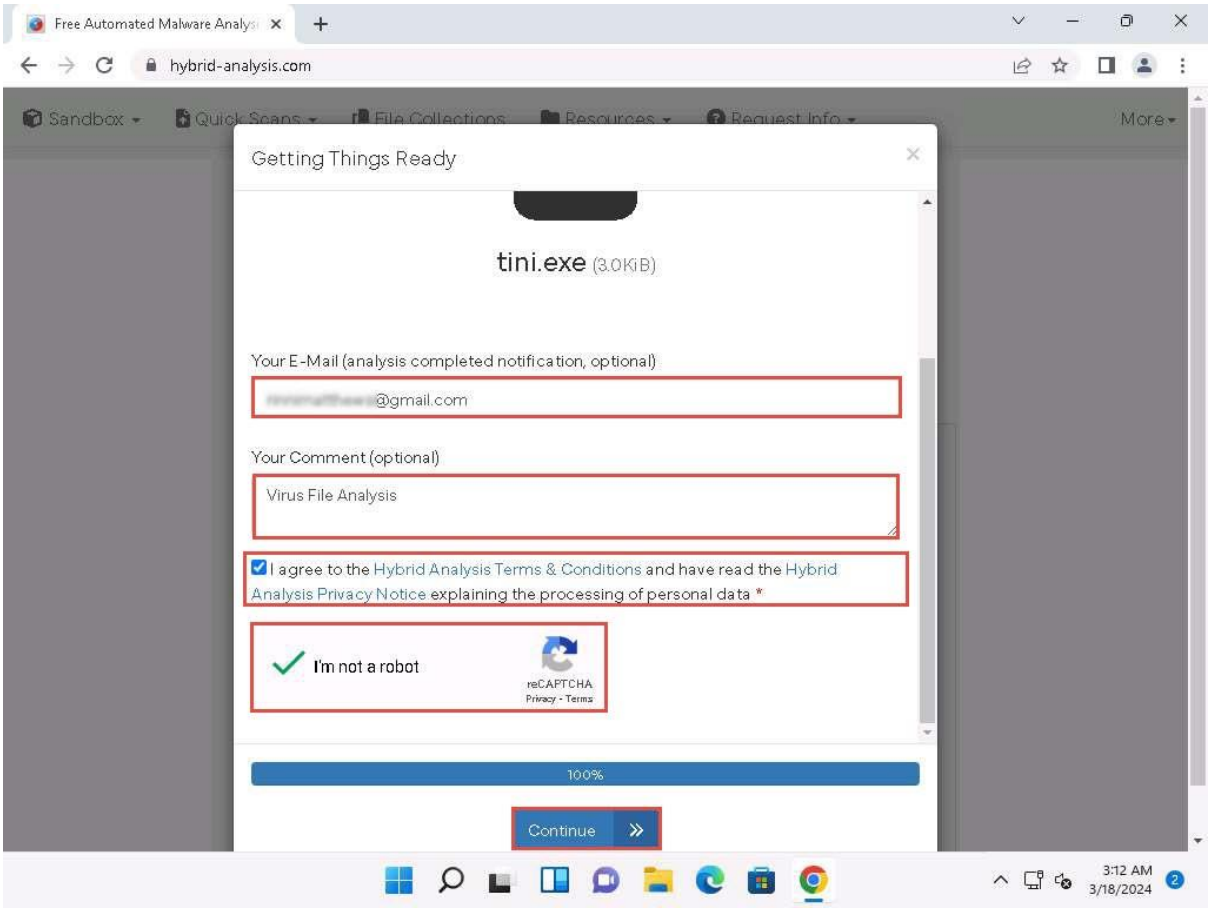
4. The **Open** window appears; navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.



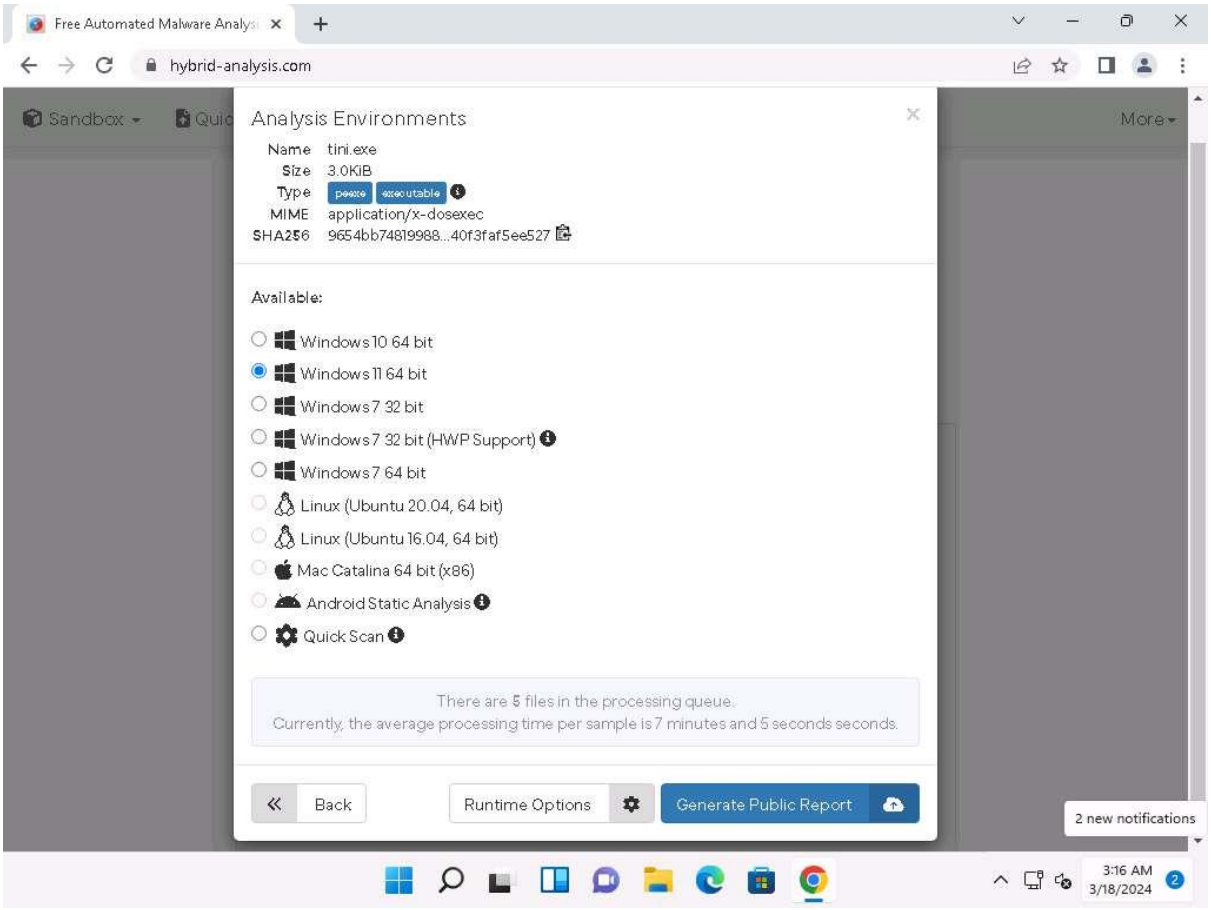
5. **Getting Things Ready** page appears and the virus file begins to upload. Once it is uploaded, the status bar reaches **100%**, as shown in the screenshot.



6. Now, enter your personal mail in **Your E-mail** field and enter a comment in **Your Comment** field. Scroll-down to check the **I agree to the Hybrid Analysis Terms & Conditions and have read the Hybrid Analysis Privacy Notice explaining the processsing of personal data** checkbox and **I'm not a robot** checkbox. Click **Continue**.



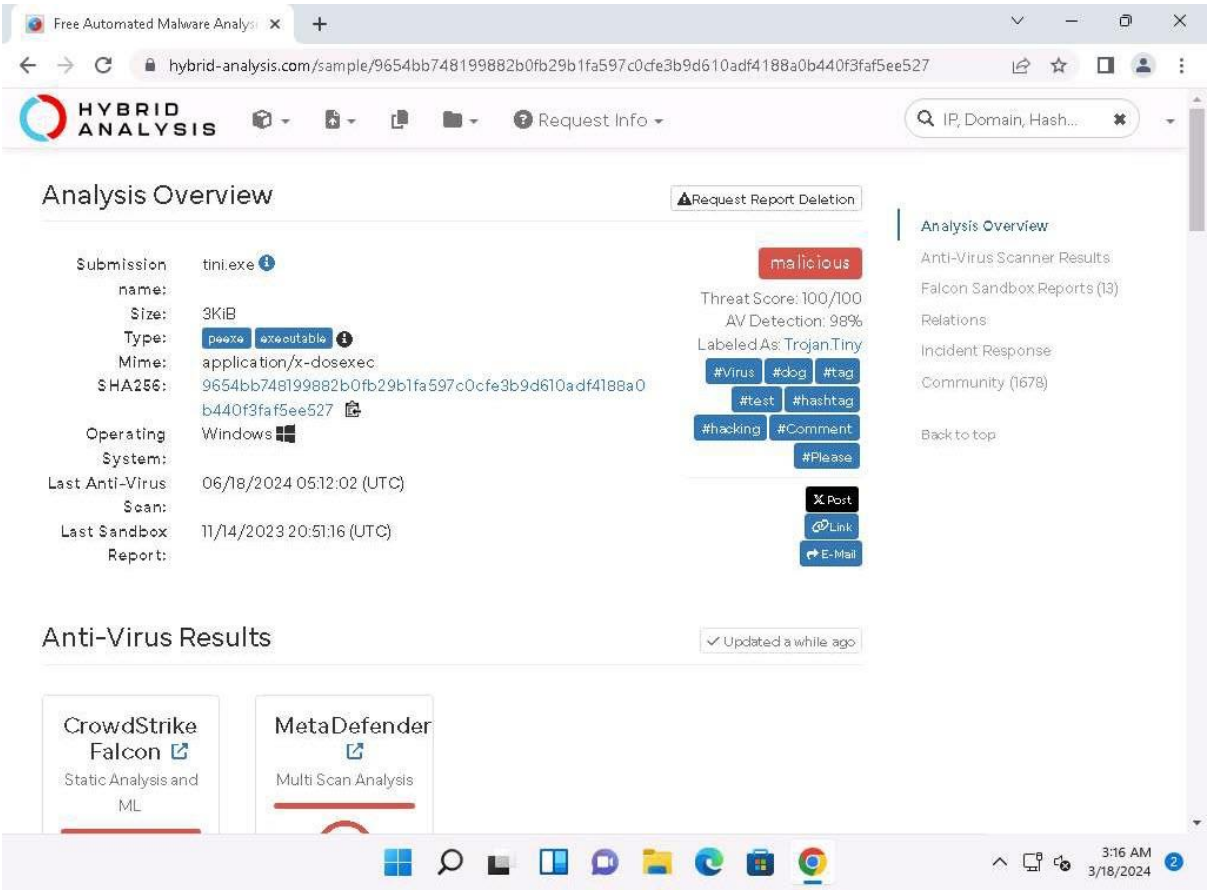
7. **Analysis Environments** page appears, select **Windows 11 64 bit** radio-button and click **Generate Public Report**.



8. The report generation process initializes and after it completes, **Analysis Overview** page appears.

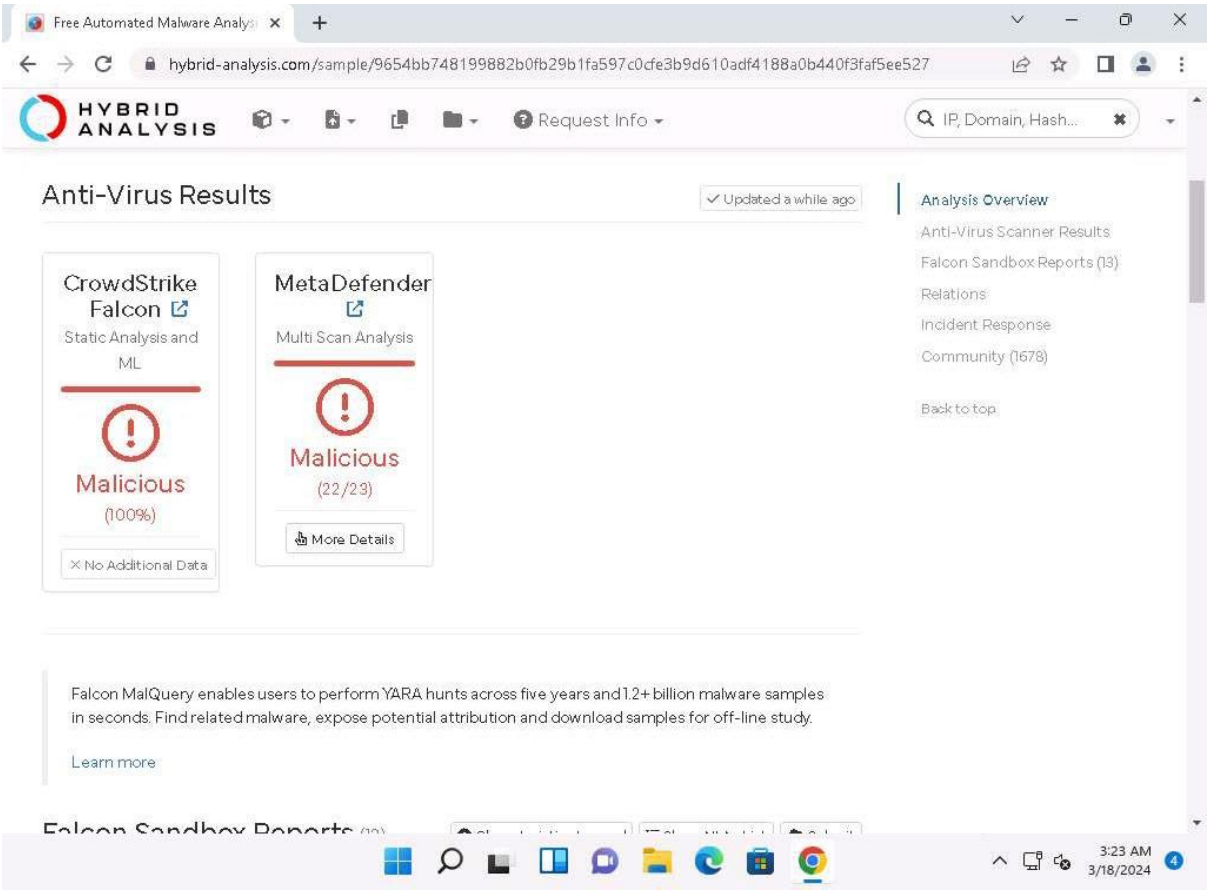
   If you receive an error in the webpage, then reload the page to obtain the result.

9. You can observe that the file is detected as **malicious** with threat score at 100 along with the additional information such as SHA value.

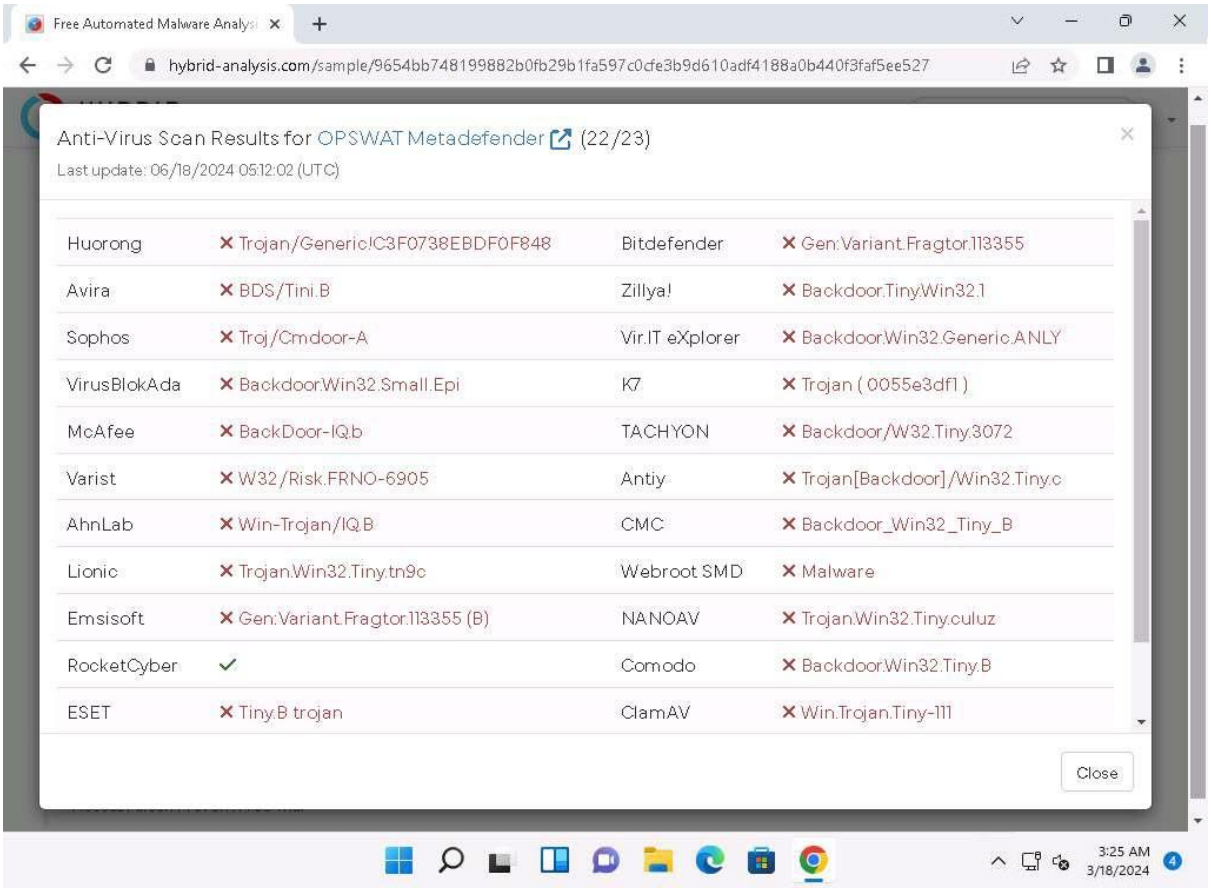


10. In the **Anti-Virus Results** section, you can observe the AV results obtained from different online resources such as **CrowdStrike Falcon** and **MetaDefender**.

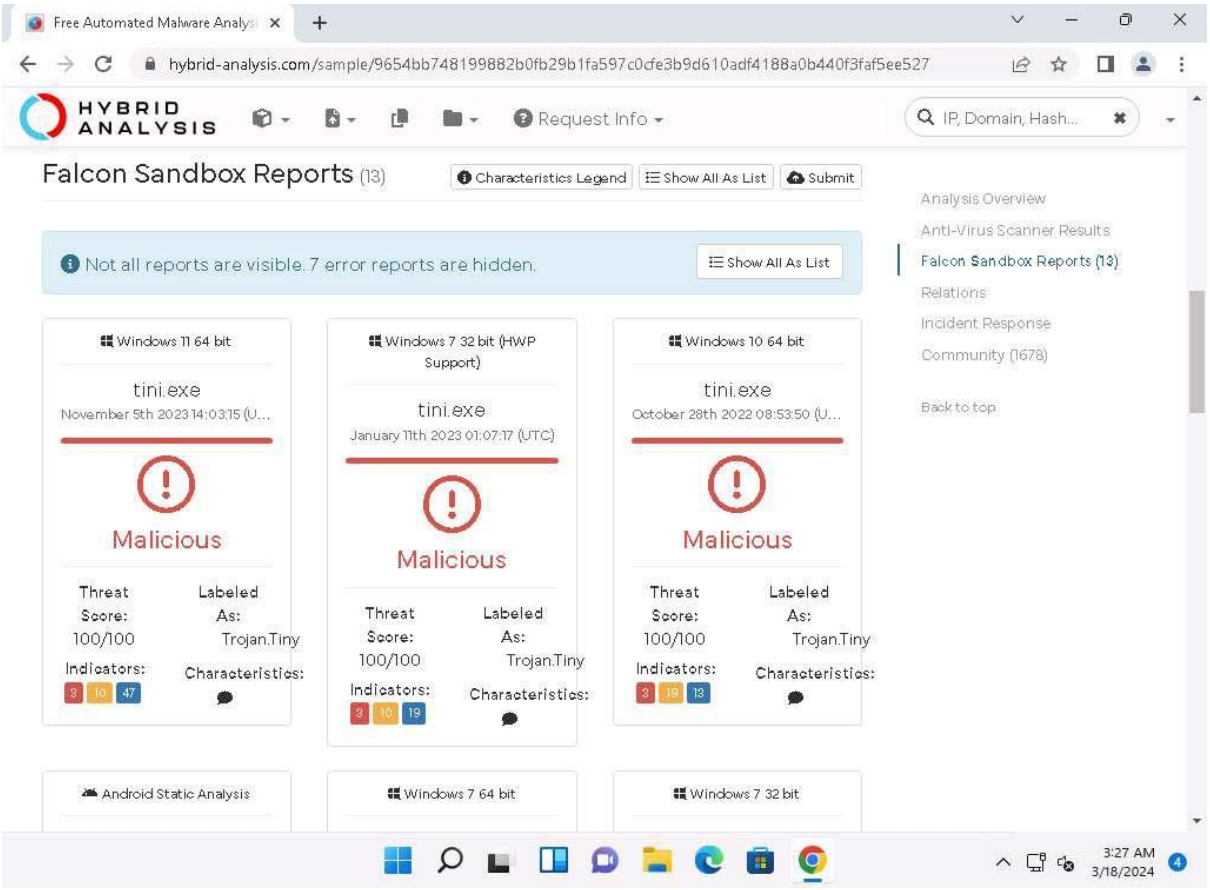
11. To further view the complete information obtained by the online resources you can click this icon ( ). Here, we will view the AV results obtained by the **MetaDefender**. Click **More Details** to open the result in the new tab.

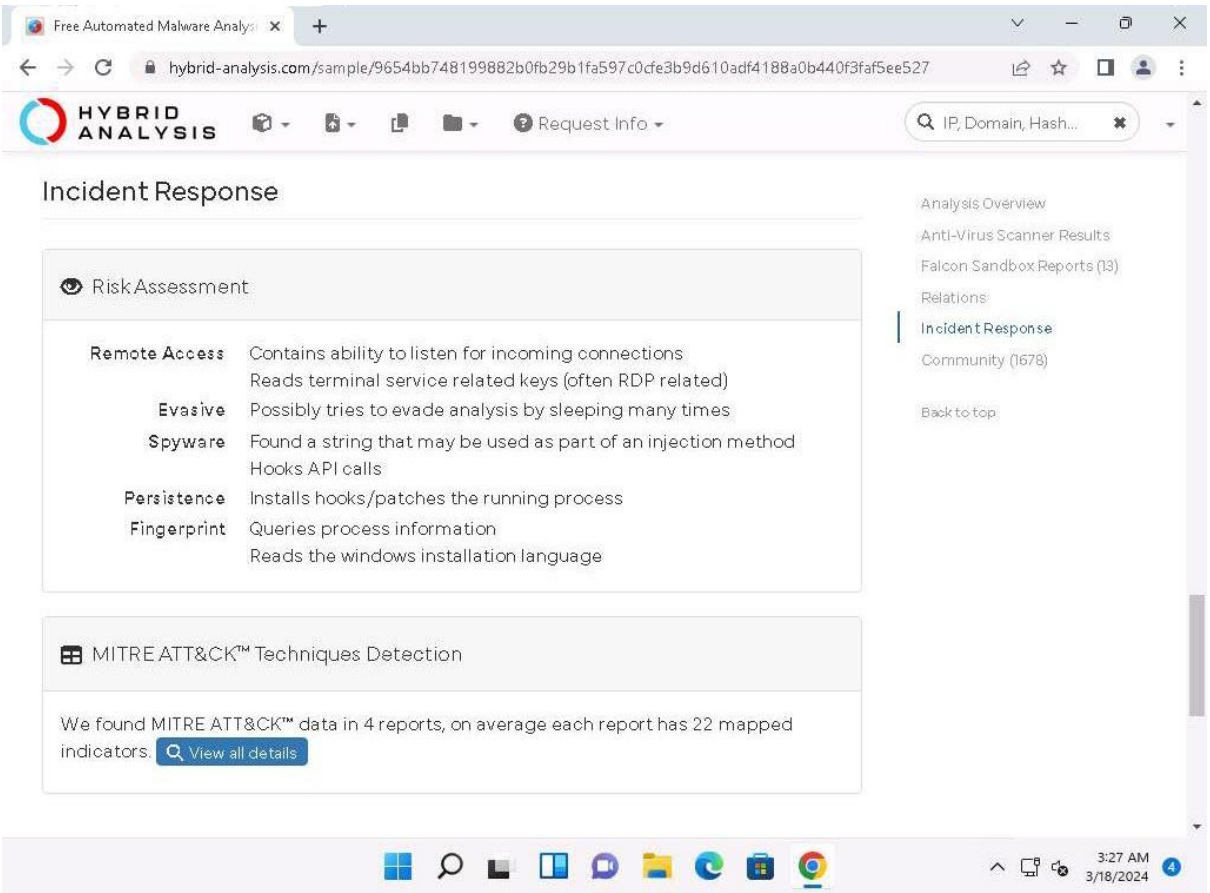


12. A pop-up appears showing the **Anti-Virus Scan Results for OPSWAT Metadefender**. Close the pop-up window.



13. You can further scroll-down in the results page to view information related to Falcon reports and Incident Response.


Free Automated Malware Analysis
hybrid-analysis.com/sample/9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527
HYBRID ANALYSIS
Request Info
IP, Domain, Hash...
Falcon Sandbox Reports (13)
Characteristics Legend
Show All As List
Submit
Not all reports are visible. 7 error reports are hidden.
Show All As List
Windows 11 64 bit
tini.exe
November 5th 2023 14:03:15 (U...
Malicious
Threat Score: 100/100
Labeled As: Trojan.Tiny
Indicators: 3 10 47
Characteristics:
Windows 7 32 bit (HWP Support)
tini.exe
January 11th 2023 01:07:17 (UTC)
Malicious
Threat Score: 100/100
Labeled As: Trojan.Tiny
Indicators: 3 10 19
Characteristics:
Windows 10 64 bit
tini.exe
October 28th 2022 08:53:50 (U...
Malicious
Threat Score: 100/100
Labeled As: Trojan.Tiny
Indicators: 3 10 13
Characteristics:
Android Static Analysis
Windows 7 64 bit
Windows 7 32 bit
Analysis Overview
Anti-Virus Scanner Results
Falcon Sandbox Reports (13)
Relations
Incident Response
Community (1678)
Back to top
3:27 AM
3/18/2024


Free Automated Malware Analysis
hybrid-analysis.com/sample/9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527
HYBRID ANALYSIS
Request Info
IP, Domain, Hash...
Incident Response
Risk Assessment
Remote Access
Contains ability to listen for incoming connections
Reads terminal service related keys (often RDP related)
Evasive
Possibly tries to evade analysis by sleeping many times
Spyware
Found a string that may be used as part of an injection method
Hooks API calls
Persistence
Installs hooks/patches the running process
Fingerprint
Queries process information
Reads the windows installation language
MITRE ATT&CK™ Techniques Detection
We found MITRE ATT&CK™ data in 4 reports, on average each report has 22 mapped indicators.
View all details
Analysis Overview
Anti-Virus Scanner Results
Falcon Sandbox Reports (13)
Relations
Incident Response
Community (1678)
Back to top
3:27 AM
3/18/2024

14. This concludes the demonstration of malware scanning using Hybrid Analysis.

15. Close all open windows.

16. You can also use other local and online malware scanning tools such as **Any.Run** (https://app.any.run) **Valkyrie Sandbox** (https://valkyrie.comodo.com), **JOESandbox Cloud** (https://www.joesandbox.com), **Jotti** (https://virusscan.jotti.org) to perform online malware scanning.

Question 7.3.1.1

Analyze malware using online Hybrid Analysis services. What the name of the Analysis Environment that was selected in this task?

Question 7.3.1.2

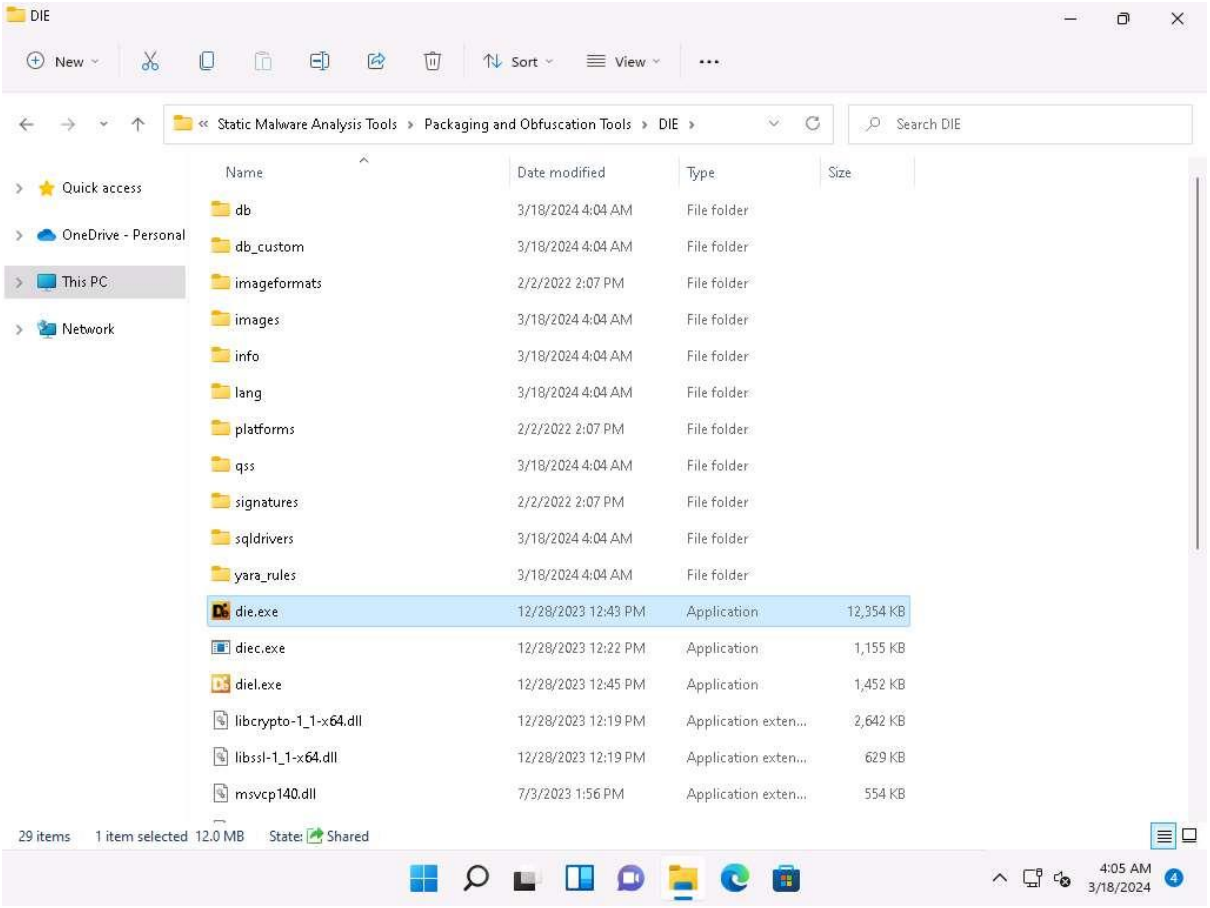
Analyze malware using online Hybrid Analysis services. Enter the name of the malicious file that was uploaded for analysis in this lab.

Task 2: Analyze ELF Executable File using Detect It Easy (DIE)

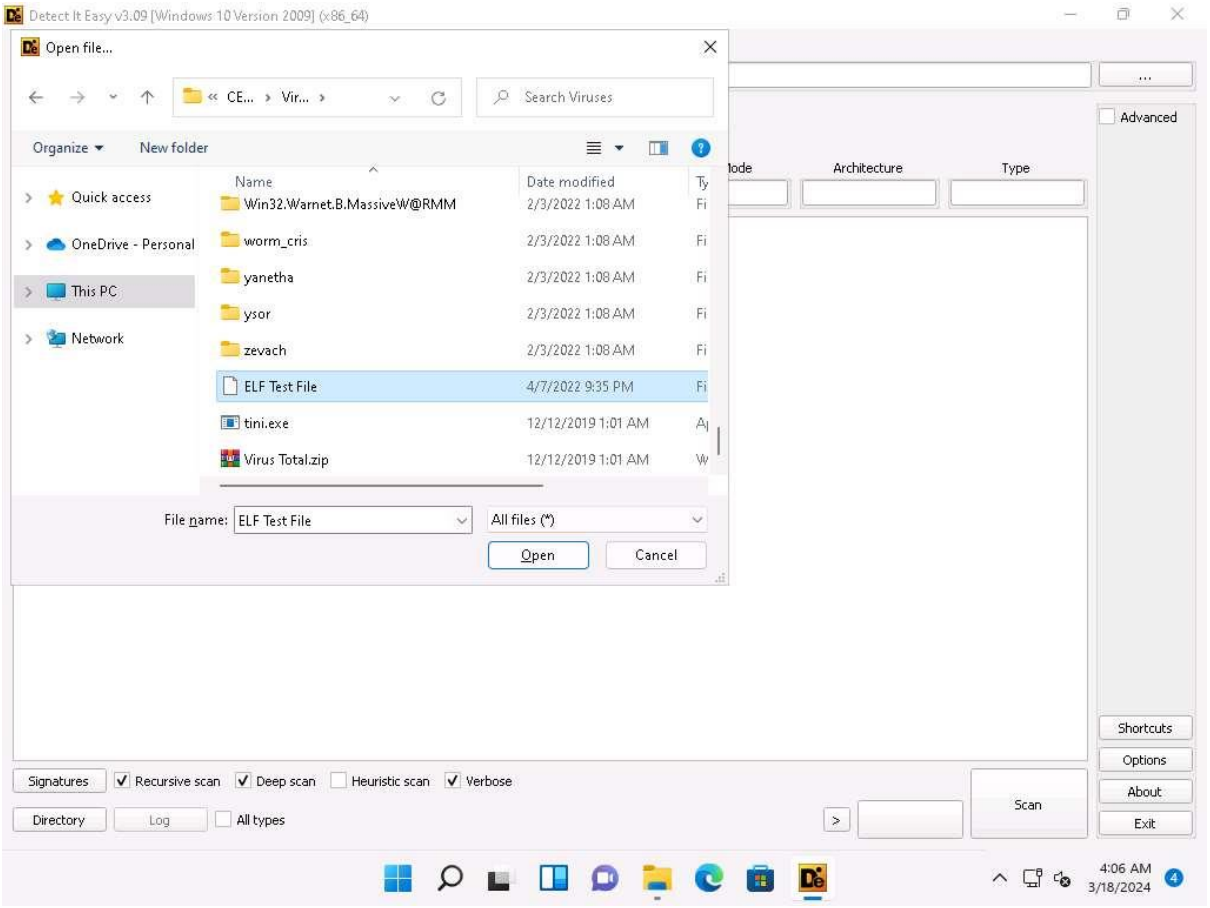
The Executable and Linkable Format (ELF) is a generic executable file format in Linux environment. It contains three main components including ELF header, sections, and segments. Each component plays an independent role in the loading and execution of ELF executables. The static analysis of an ELF file involves investigating an ELF executable file without running or installing it. It also involves accessing the binary code and extracting valuable artifacts from the program. Numerous tools can be used to perform static analysis on ELF files. In this task, we will be using Detect It Easy (DIE) tool to analyze ELF file.

Detect It Easy (DIE) is an application used for determining the types of files. Apart from the Windows, DIE is also available for Linux and Mac OS. It has a completely open architecture of signatures and can easily add its own algorithms for detecting or modifying the existing signatures. It detects a file's compiler, linker, packer, etc. using a signature-based detection method.

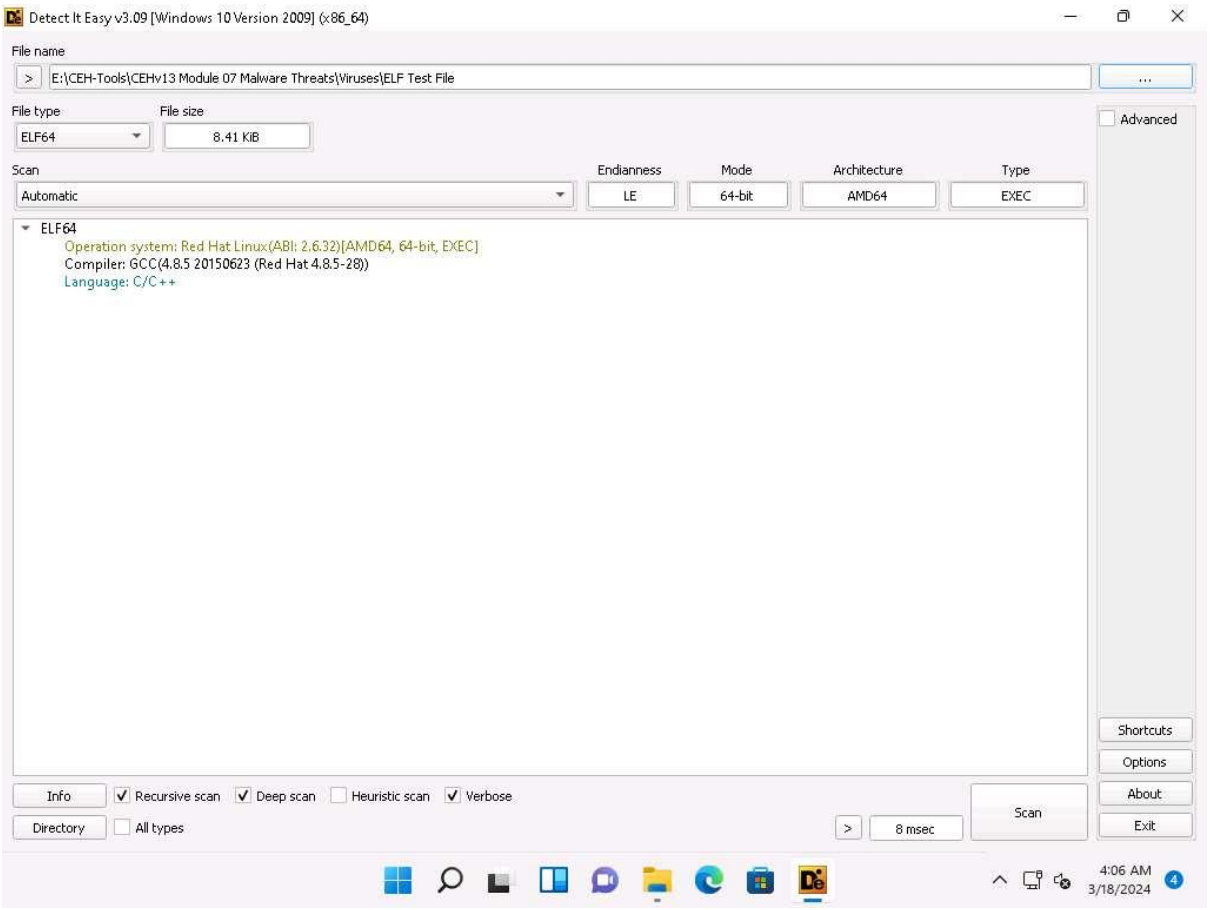
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\DIE** and double-click **die.exe**.



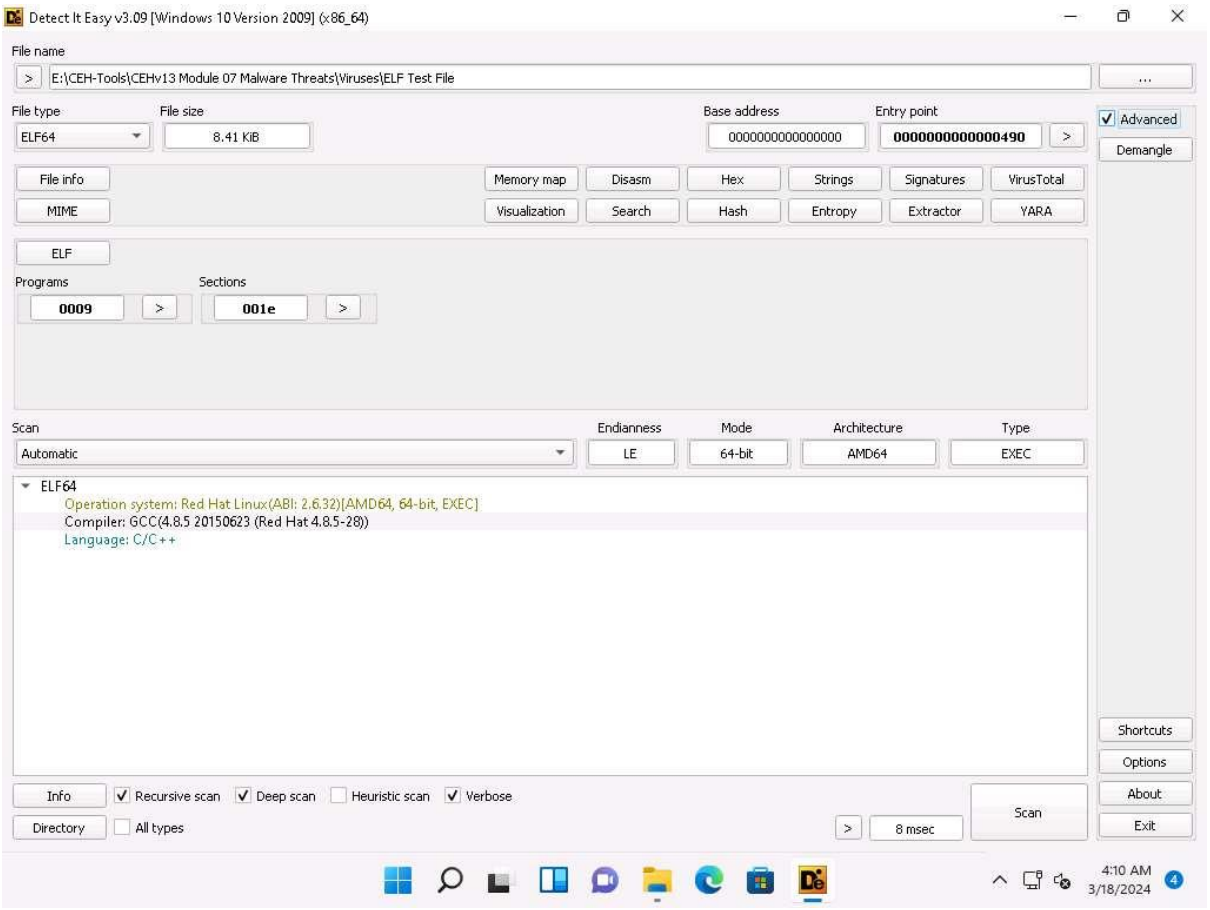
2. **Open File - Security Warning** appears, click **Run**.
3. **Detect It Easy** window appears. Click ellipses icon next to the **File name** text field.
4. The **Open file…** window appears; navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Viruses**, select **ELF Test File**, and click **Open**.



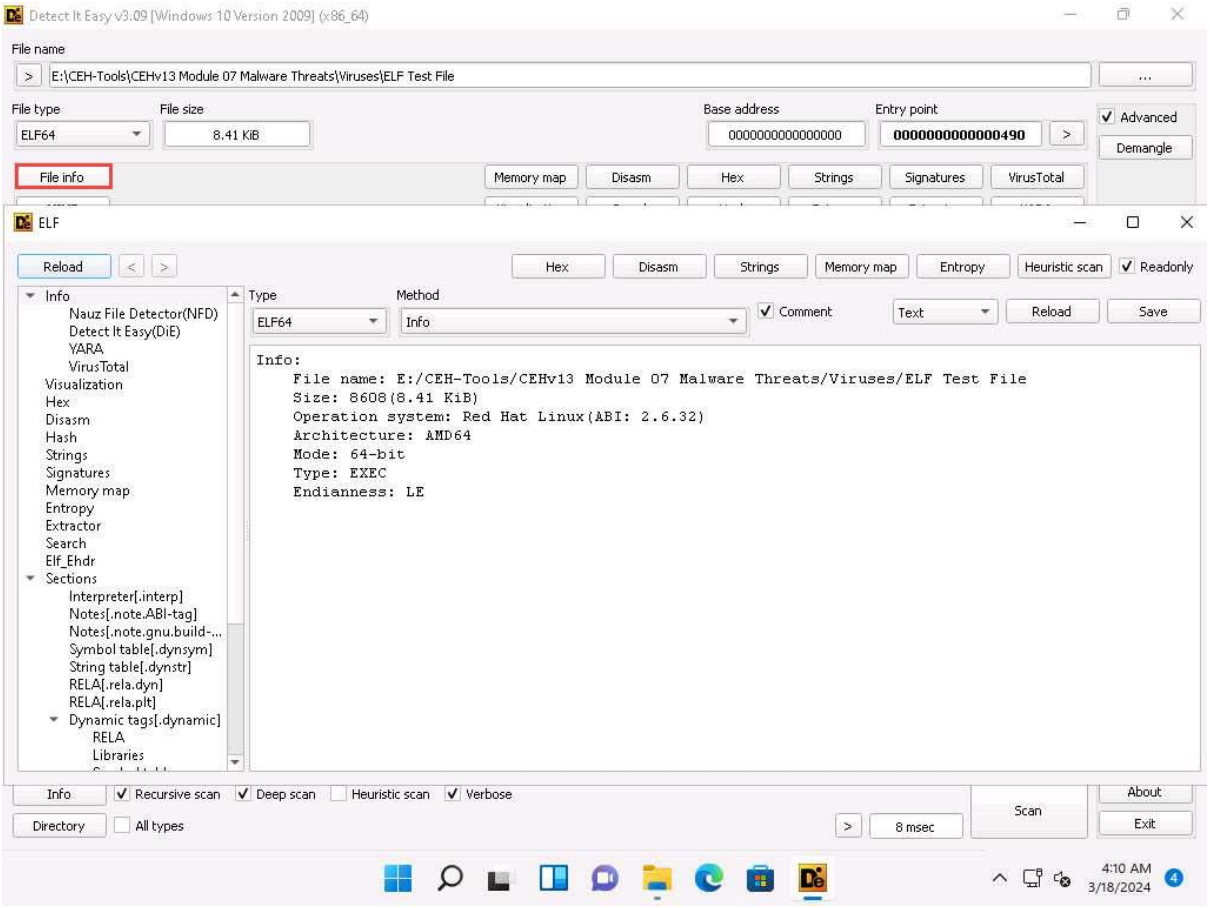
5. **Detect It Easy** automatically scans the file and result appears showing the Operating system, compiler and language details in the middle pane, as shown in the screenshot.



6. Now, check the **Advanced** checkbox present at the right pane.

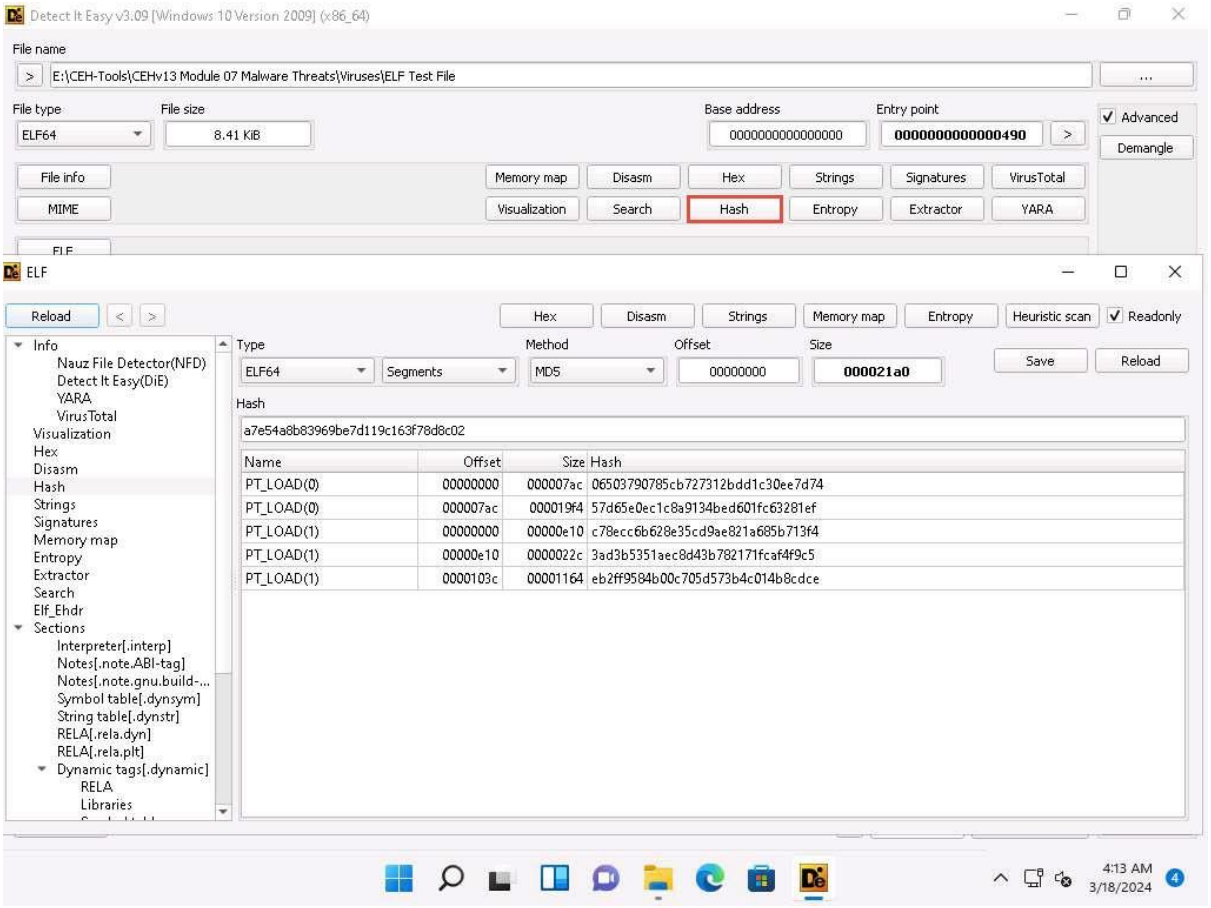


7. Click **File info** button from the top left corner of the window. Info window appears, you can observe information such as File name, size, MD5, SHA1, Entropy, entry points, etc.

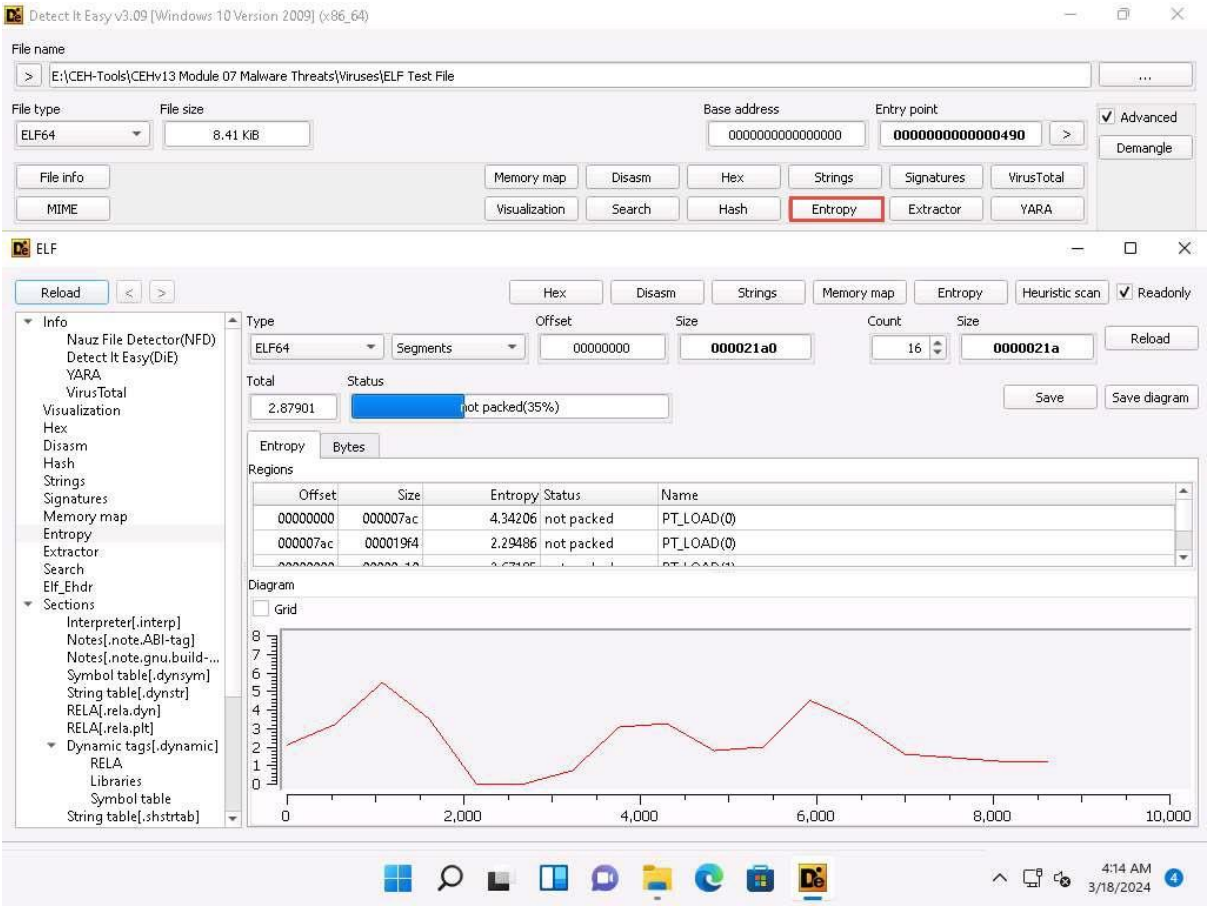


8. After viewing the information, close the window.

9. Similarly, click **Hash** button from the top right corner of the window to view the information related to hash. Close the window after viewing the information.



10. Click **Entropy** button from the top right corner of the window. Here, you can observe the status, size and graph of entropy. Close the window after viewing the Entrophy information.



11. Similarly, you can further explore other functions such as MIME, Hex, Signatures and Demangle.

12. This concludes the demonstration of ELF file analysing using Detect It Easy (DIE).

13. Close all the open windows.

14. You can also use other packaging/obfuscation tools such as **Macro_Pack** (https://github.com), **UPX** (https://upx.github.io), **ASPack** (http://www.aspack.com), or **VMprotect** (https://vmpsoft.com) to identify packing/obfuscation methods.

Question 7.3.2.1

Detect a file's compiler, linker, packer, etc. using Detect It Easy (DIE). Enter the name of the operating system that was detected from the ELF file in this task.

Task 3: Perform Malware Disassembly using IDA and OllyDbg

Static analysis also includes the dismantling of a given executable into binary format to study its functionalities and features. This process helps identify the language used for programming the malware, look for APIs that reveal its function, and retrieve other information. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process uses debugging tools such as IDA Pro and OllyDbg.

IDA As a disassembler, IDA explores binary programs, for which the source code might not be available, to create maps of their execution. The primary purpose of a disassembler is to display the instructions actually executed by the processor in a symbolic representation called "assembly language." However, in real life, things are not always simple. Hostile code usually does not cooperate with the analyst. Viruses, worms, and Trojans are often armored and obfuscated; as such, more powerful tools are required. The debugger in IDA complements the static analysis capabilities of the disassembler. By allowing an analyst to single-step through the code being investigated, the debugger often bypasses the obfuscation. It helps obtain data that the more powerful static disassembler will be able to process in depth.

OllyDbg OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is unavailable. It traces registers, recognizes procedures, API calls switches, tables, constants, and strings, and locates routines from object files and libraries.

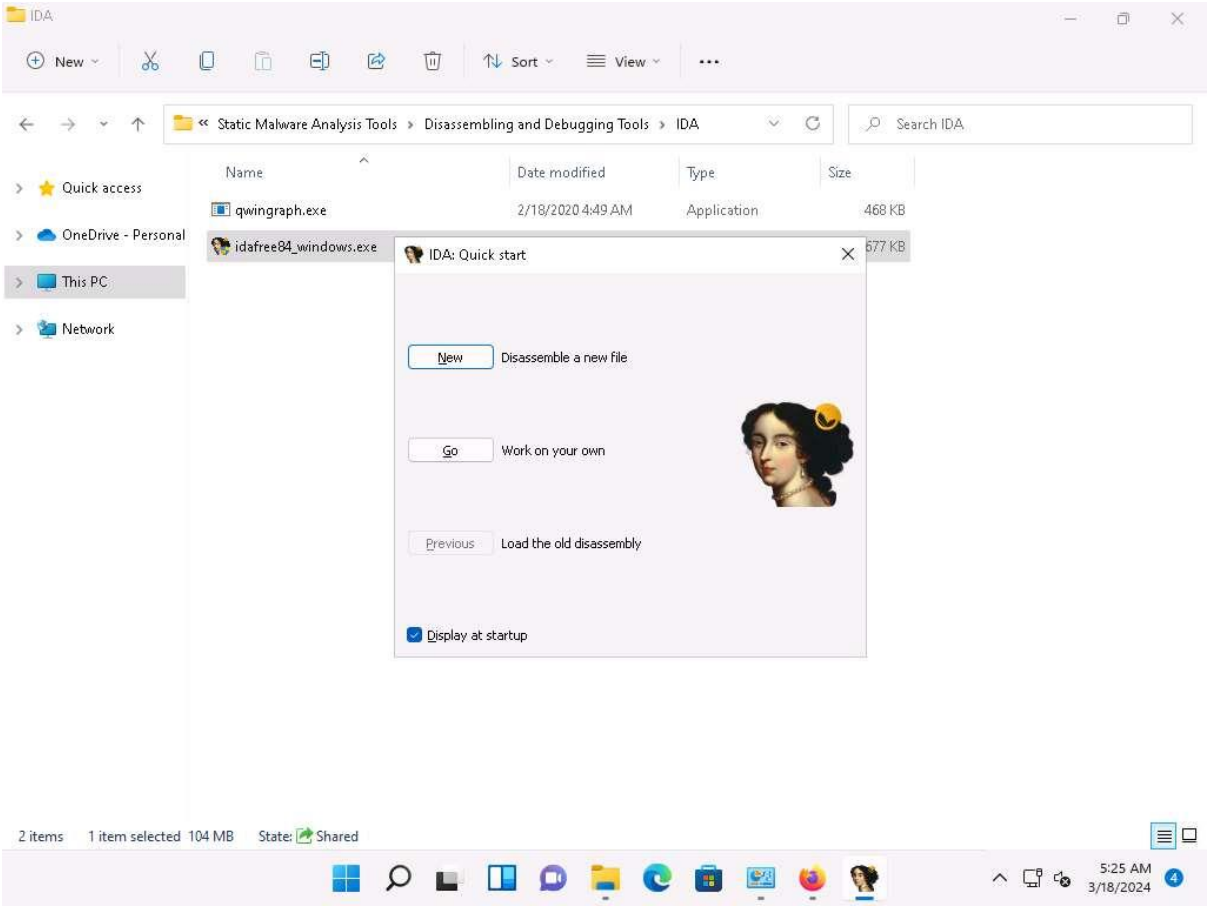
There is a new debugging option, "Set permanent breakpoints on system calls." When active, it requests OllyDbg to set breakpoints on KERNEL32.UnhandledExceptionFilter(), NTDLL.KiUserExceptionDispatcher(), NTDLL.ZwContinue(), and NTDLL.NtQueryInformationProcess().

1. In the **Windows 11** machine, search for **ida** in the Windows search, the **IDA Freeware 8.4** appears in the result, click **Open** to launch it.

2. If the **IDA License** window appears, click on **I Agree**.

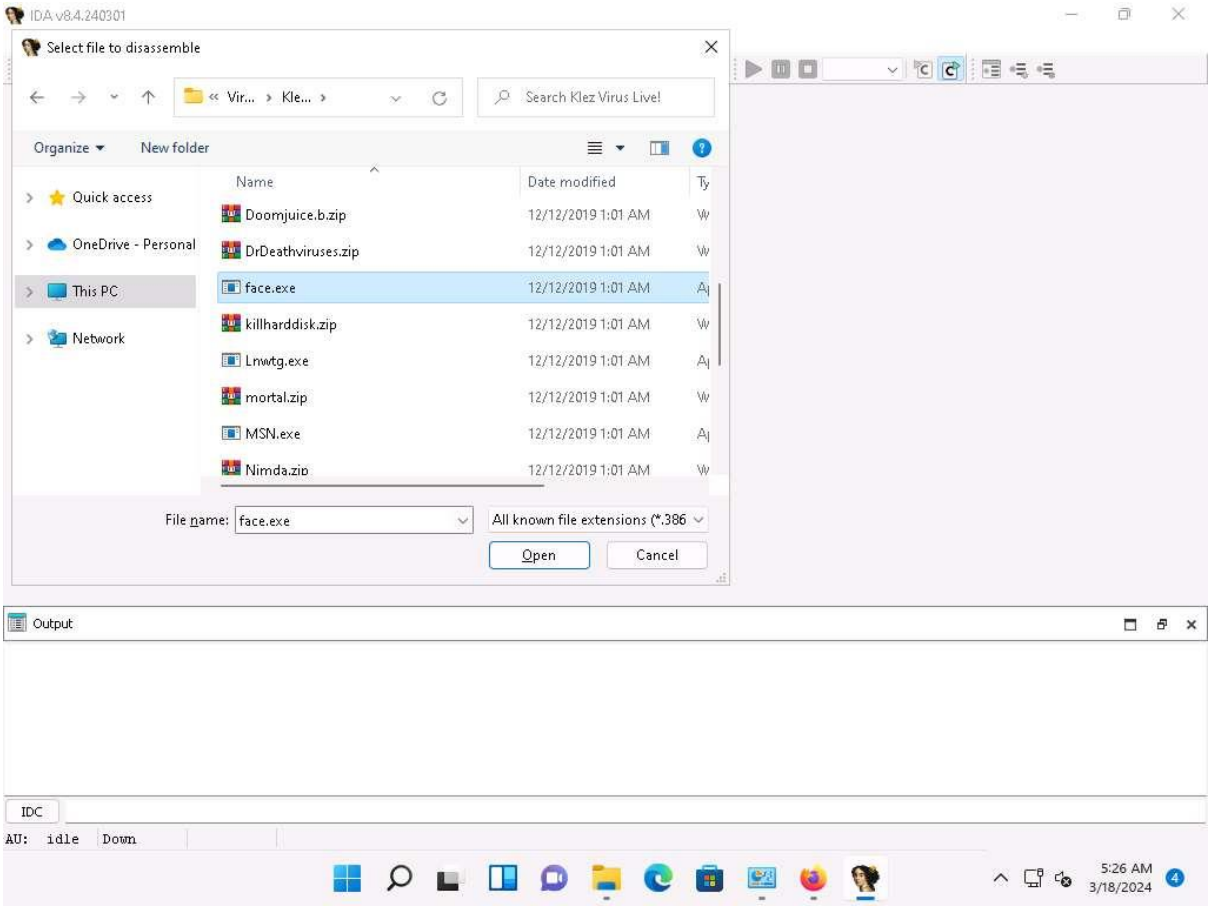
3. **User interface telemetry** window appears, uncheck **Yes, I want to help improve IDA** checkbox and click **OK**.

4. The **IDA: Quick start** pop-up appears; click on **New** to select a malicious file for disassembly.

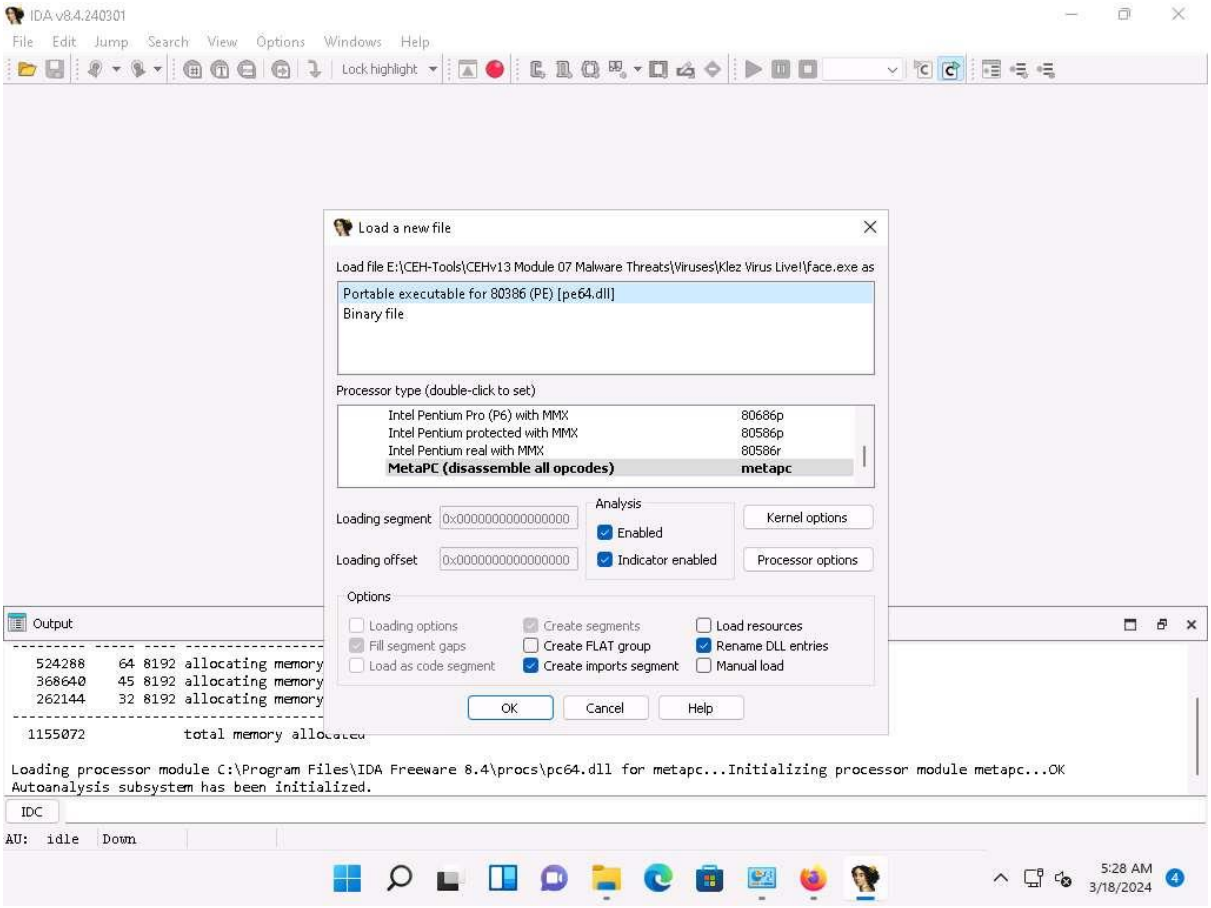


5. The **IDA** main window appears, along with the **Select file to disassemble** window.

6. In the **Select file to disassemble** window, navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select **face.exe**, and click **Open**.

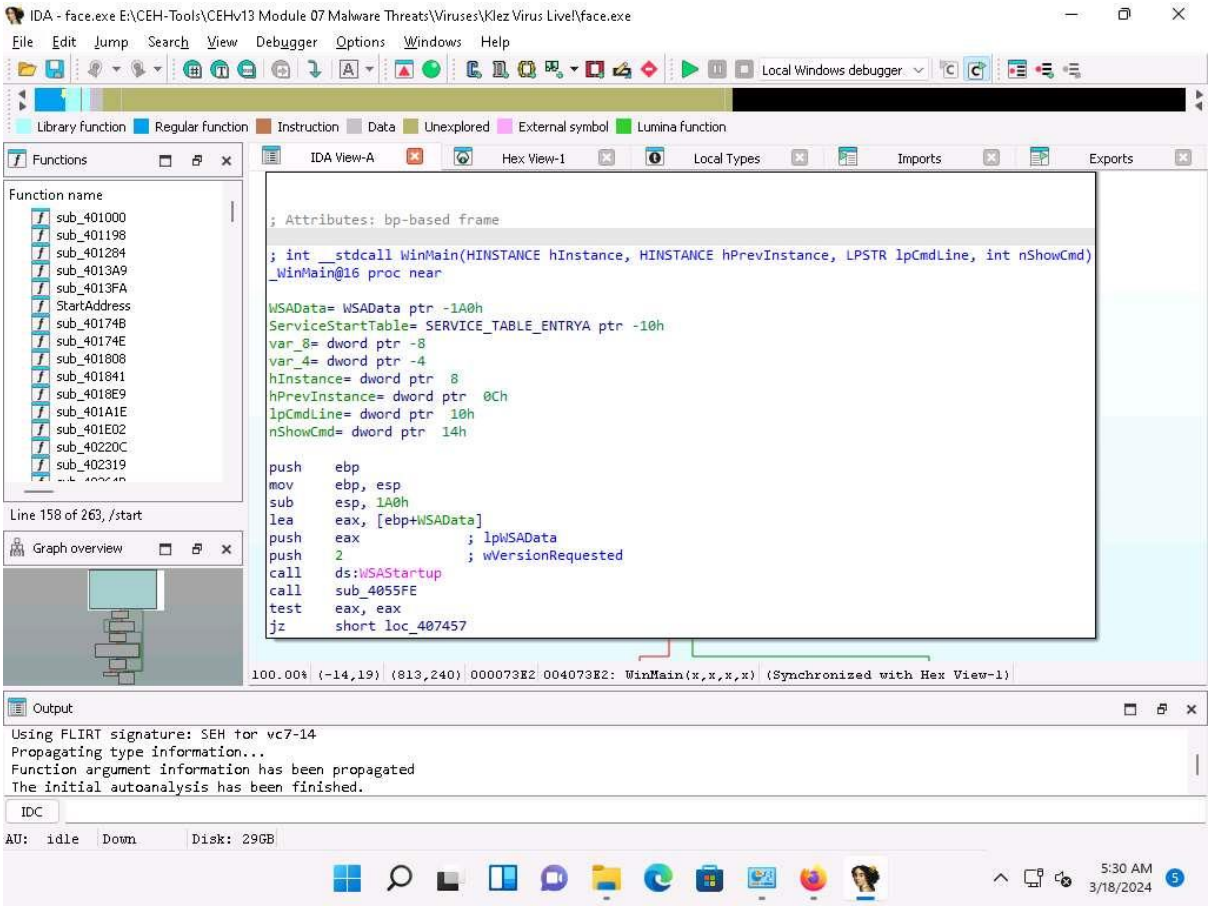


7. The **Load a new file** window appears; by default, the **Portable executable for 80386 (PE) [pe64.dll]** option selected; click **OK**.

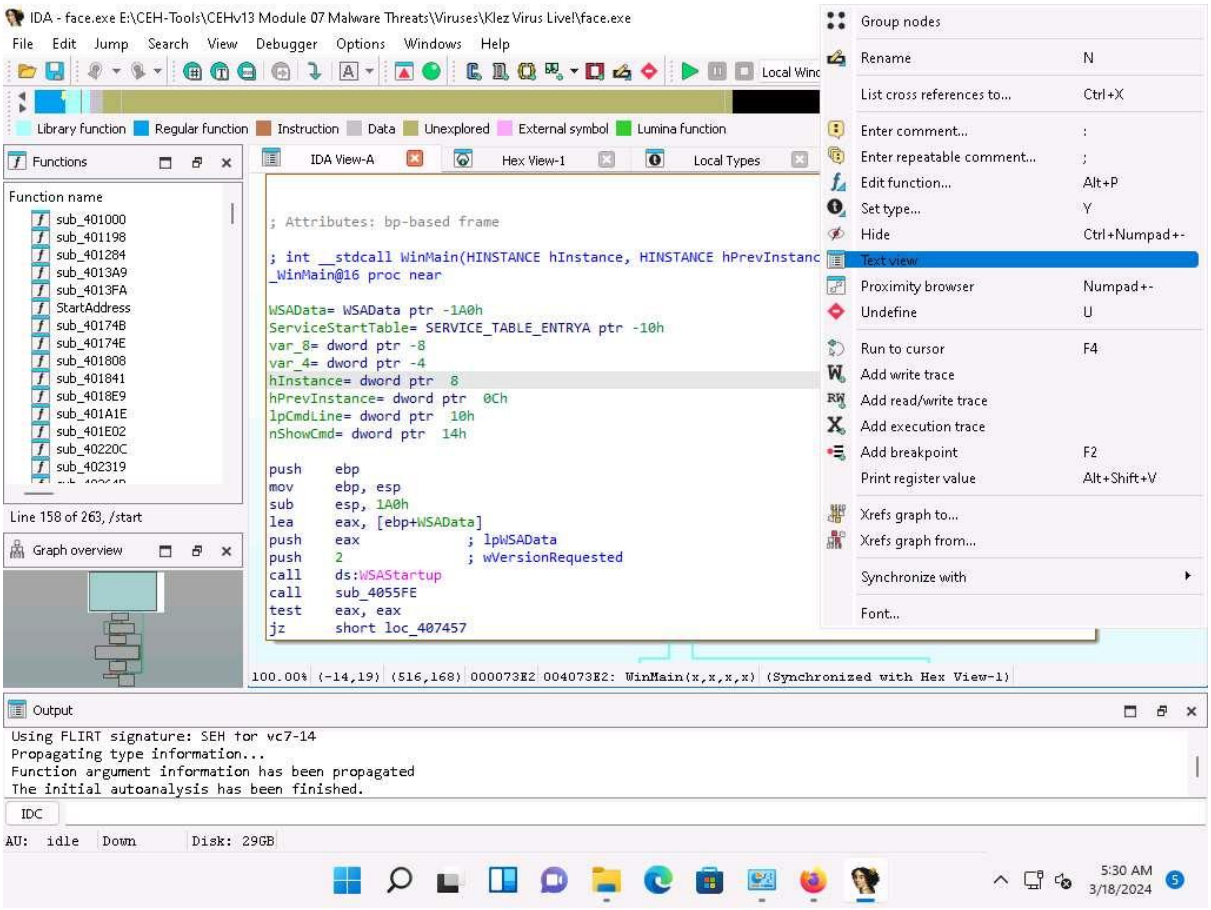


If a **Warning** pop-up appears, click **OK**.
If a **Please confirm** dialog-box appears, read the instructions carefully, and then click **Yes**.

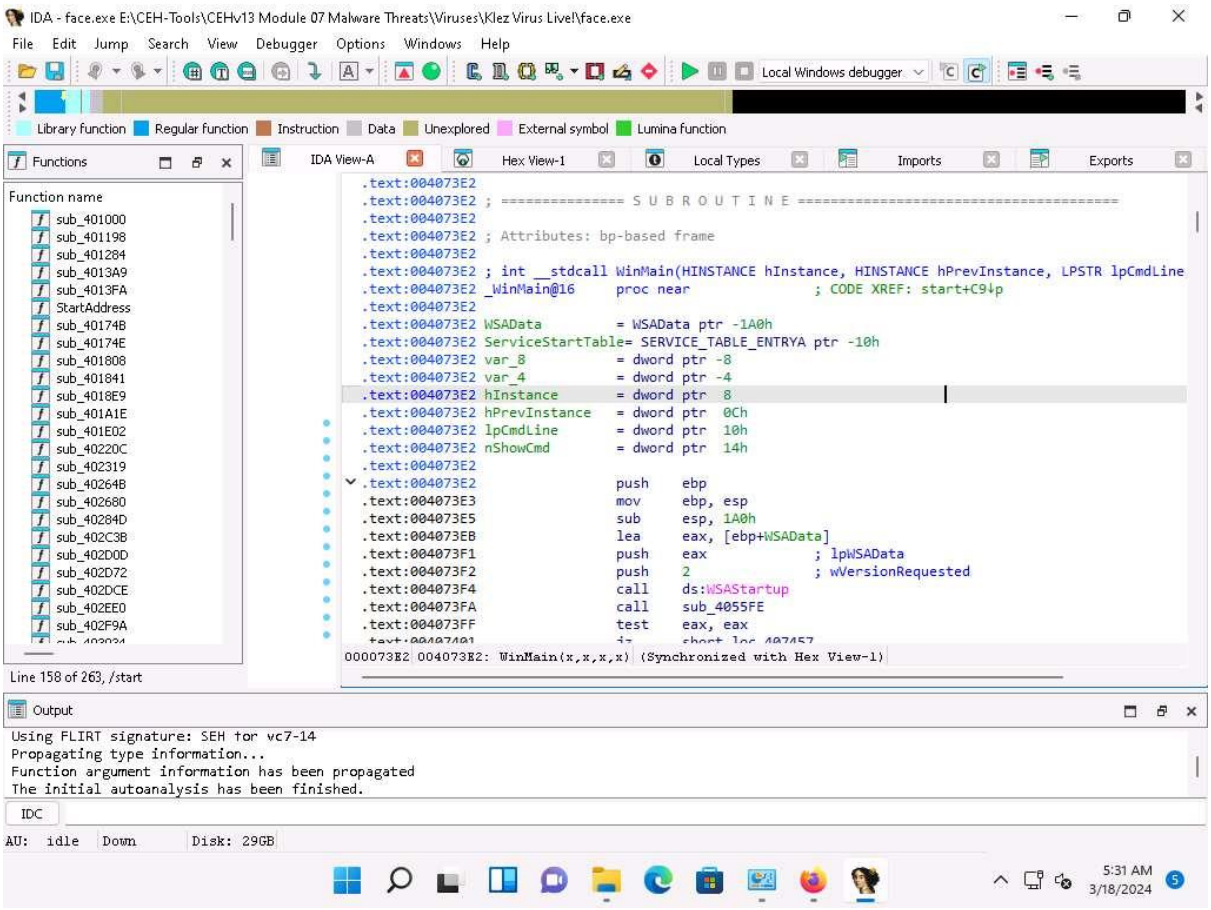
8. IDA completes the analysis of the imported malicious file and displays the results in the **IDA View-A** tab, as shown in the screenshot.



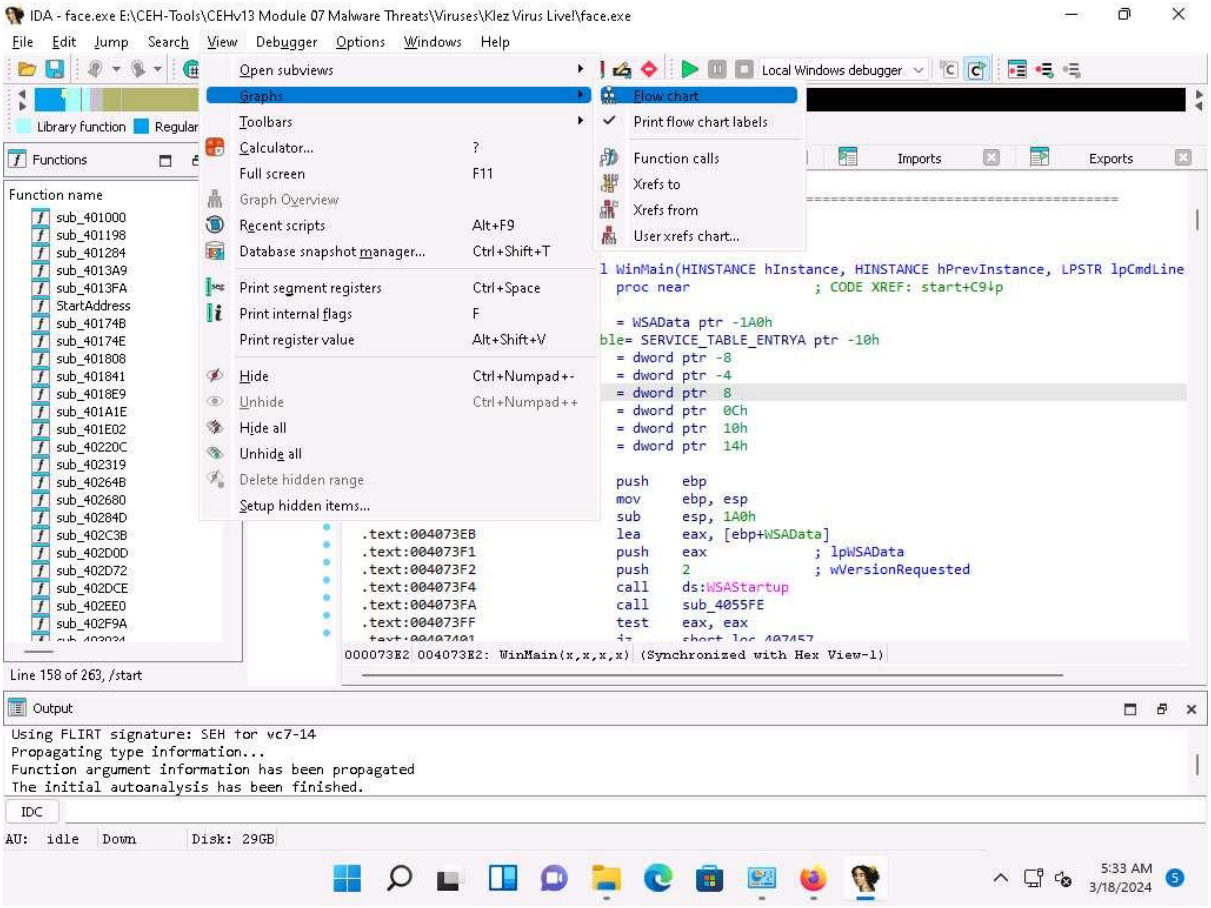
9. In the **IDA View-A** section, right-click anywhere and choose **Text view** from the context menu to view the text information of the malicious file uploaded to IDA for analysis.



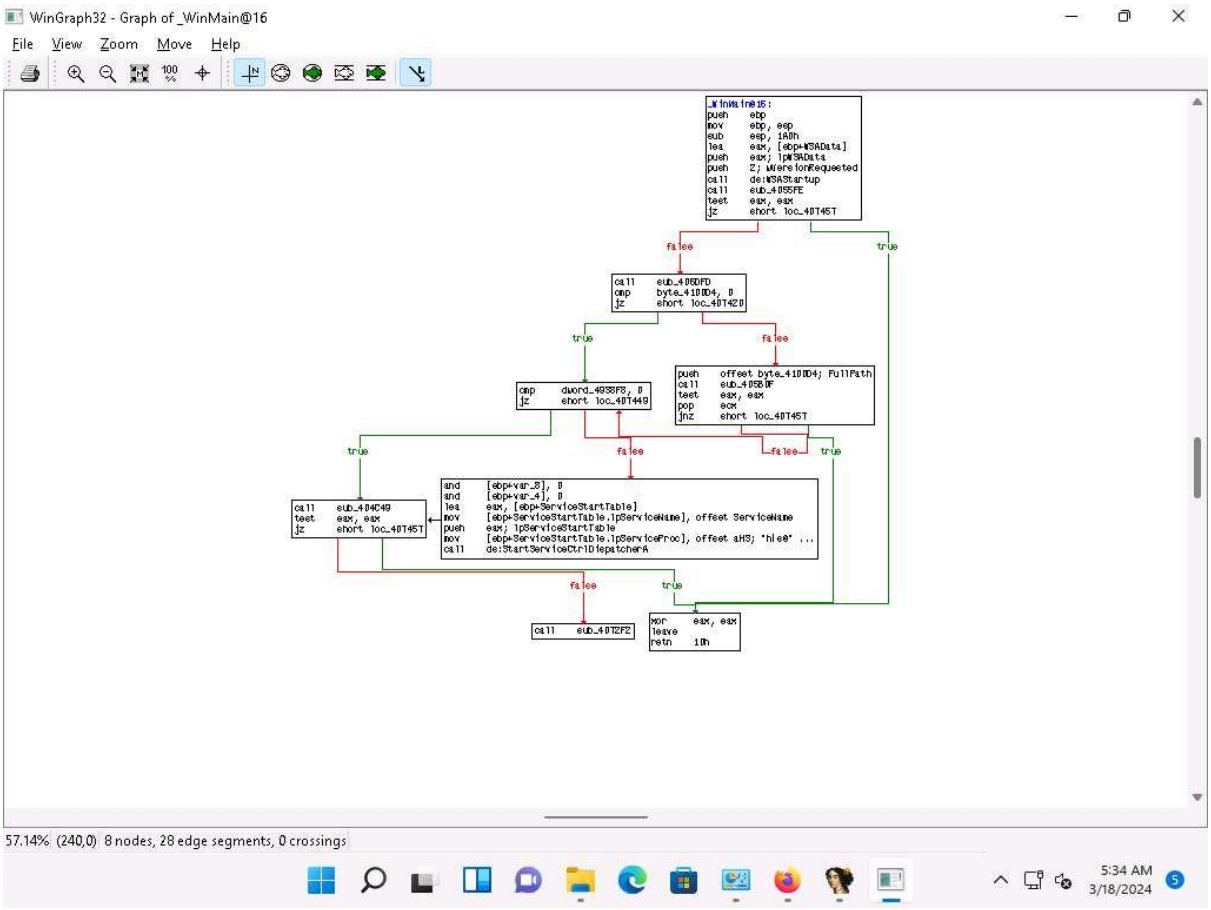
10. This reveals the text view of the malicious file, allowing analysis of its information.



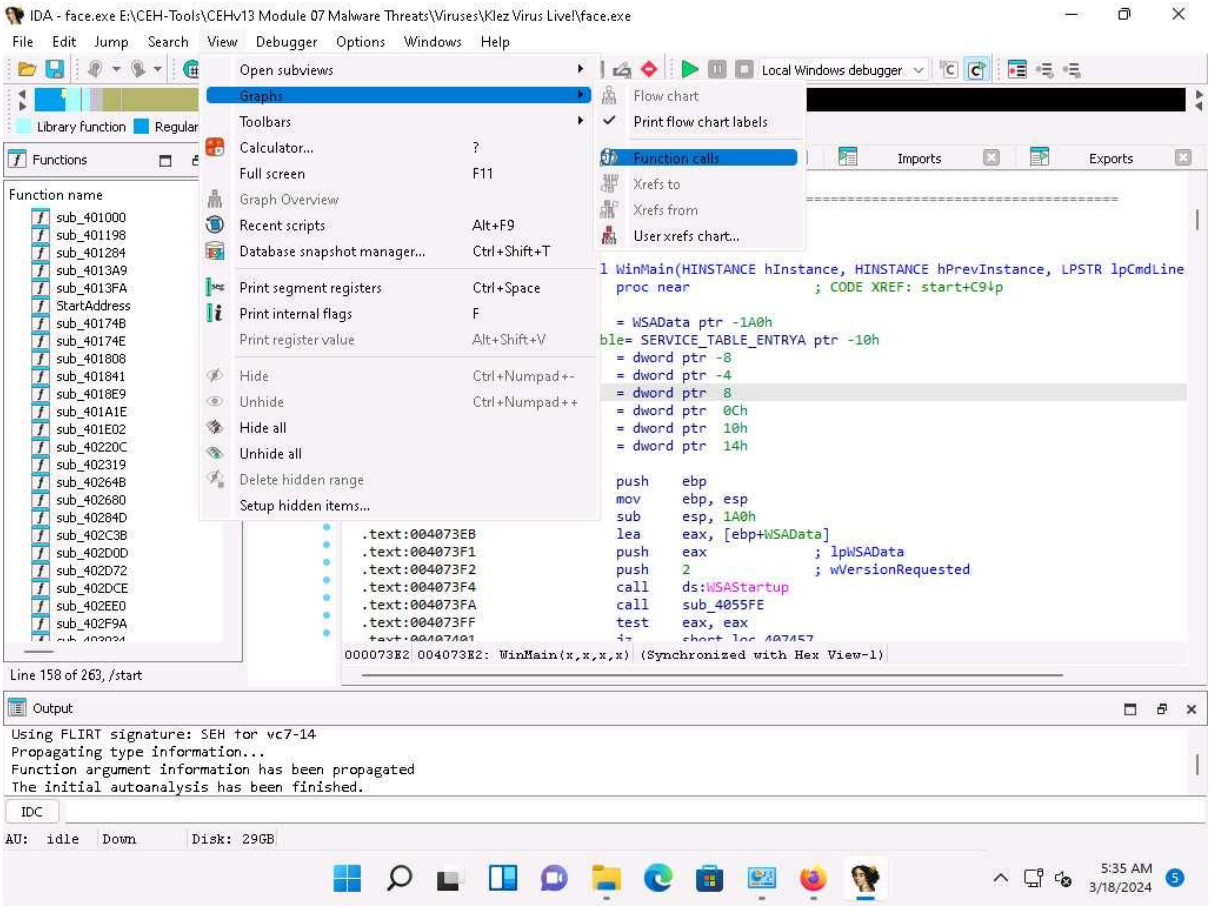
11. Maximize the IDA window. To view the flow of the uploaded malicious file, navigate to **View** --> **Graphs** and click **Flow chart**.



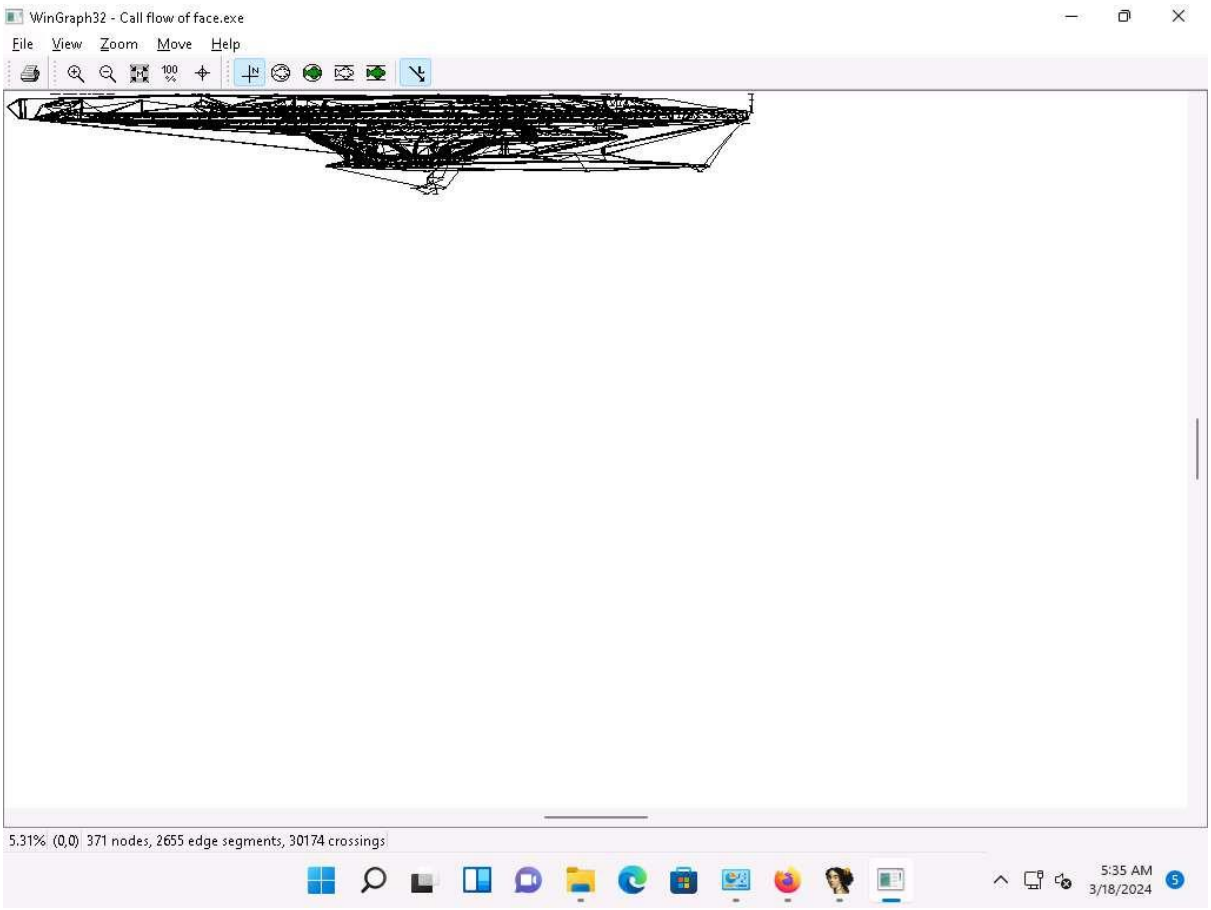
12. A **Graph** window appears with the flow. You may zoom in and adjust the screen to view this more clearly.

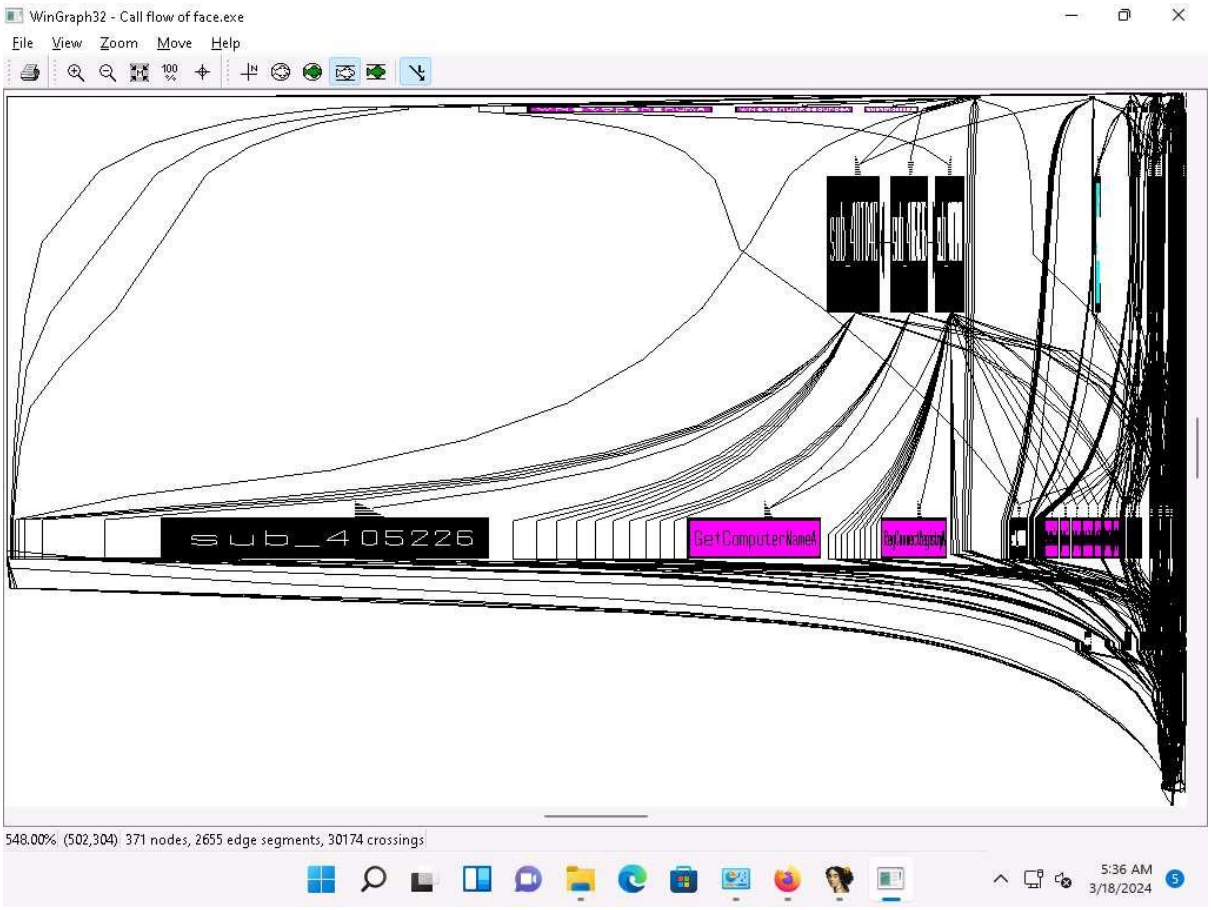


13. Close the **Graph** window, go to **View** --> **Graphs**, and click **Function calls** from the menu bar.

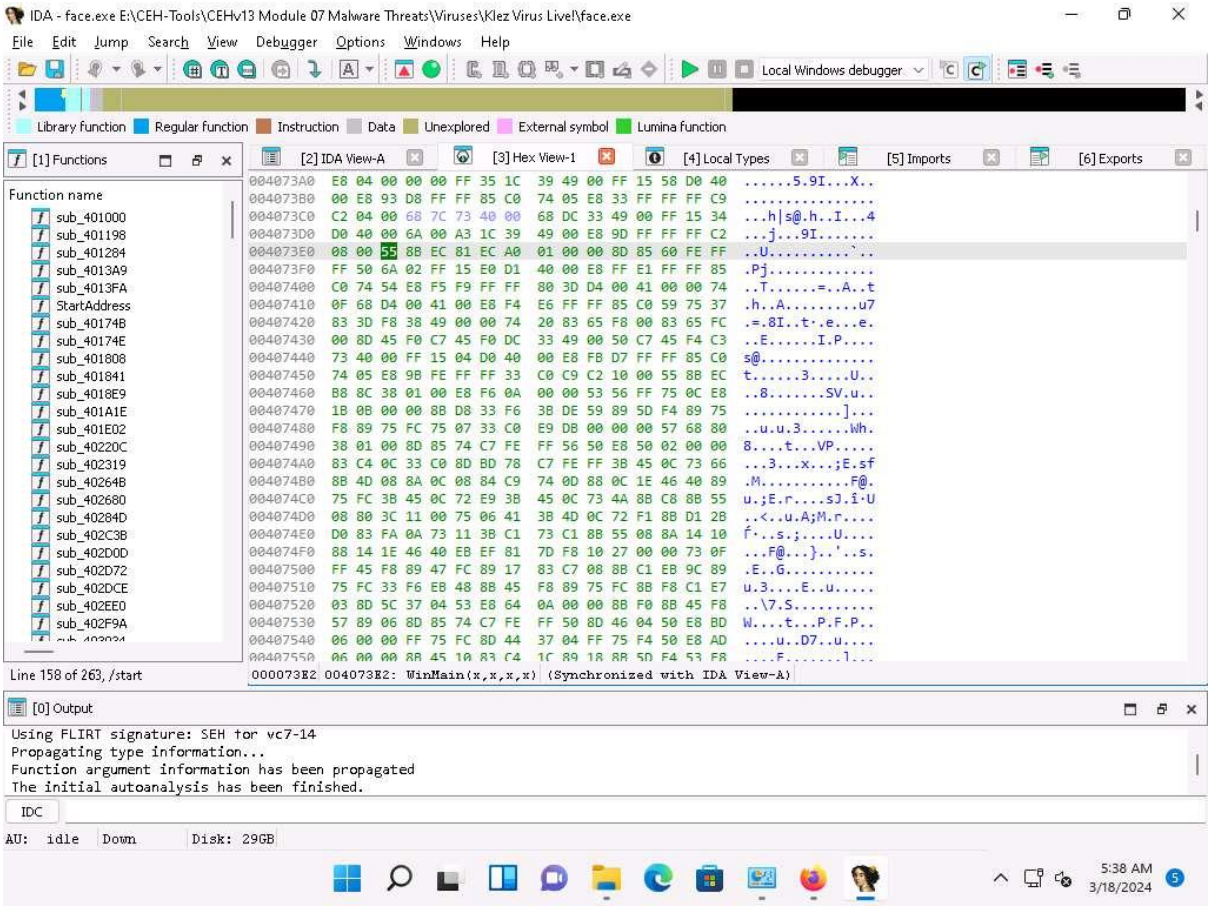


14. A window showing **call flow** appears; zoom in for a better view. Close the **WinGraph32 Call flow** window after completing the analysis.

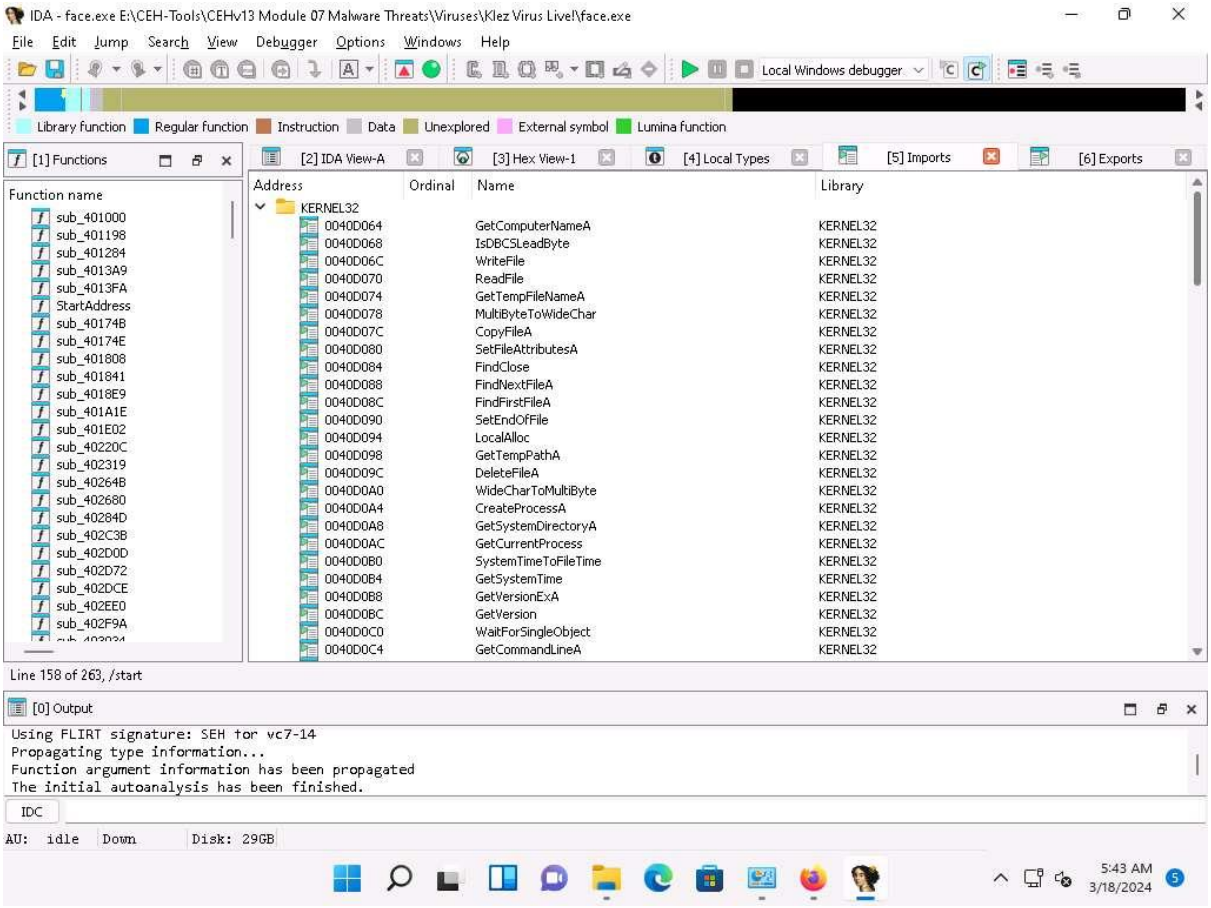

WinGraph32 - Call flow of face.exe
File View Zoom Move Help
5.31% (0,0) 371 nodes, 2655 edge segments, 30174 crossings
5:35 AM
3/18/2024


WinGraph32 - Call flow of face.exe
File View Zoom Move Help
sub_405226
GetComputerNameA
548.00% (502,304) 371 nodes, 2655 edge segments, 30174 crossings
5:36 AM
3/18/2024

15. Click the **HexView-1** tab to view the hex value of the malicious file.



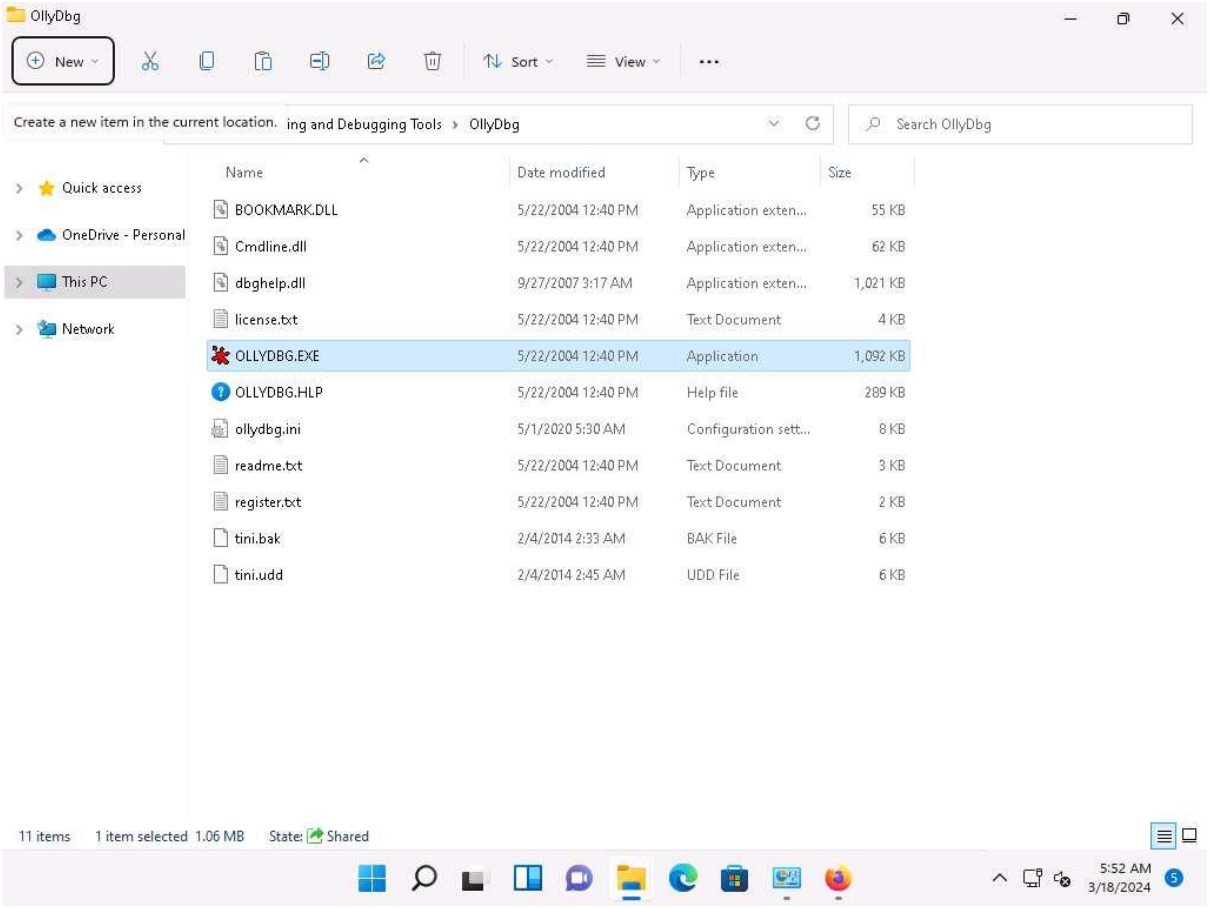
16. Click the **Imports** tab to view list of all functions that the executable calls.



17. Close all open windows. In the **Save database** pop-up, click **OK**.

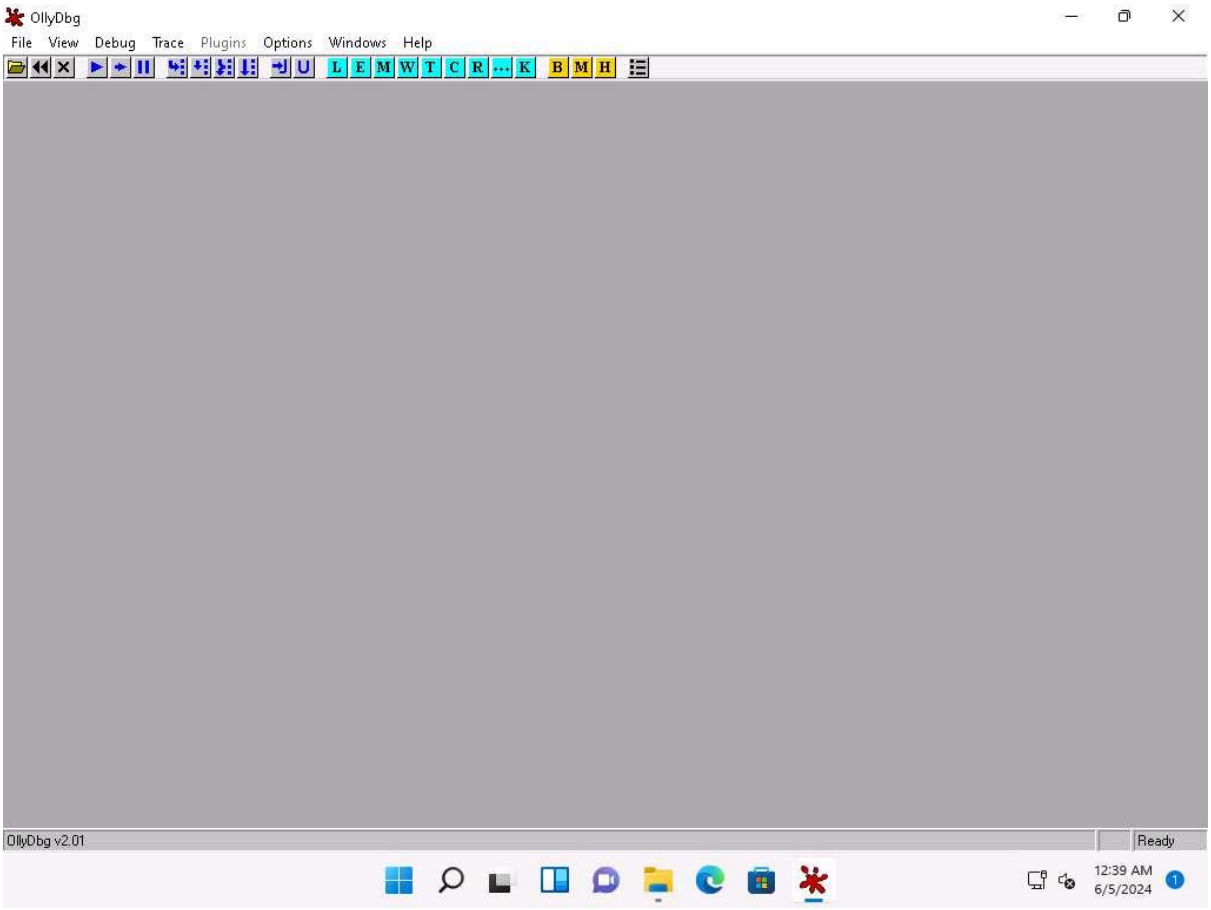
18. Navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg** and double-click **Ollydbg.exe**.

    If an **Open File - Security Warning** pop-up appears, click **Run**.



19. If a **Old DLL** dialog box appears, click **Yes**.
20. If an OllyDbg warning message appears, for administrative rights, click **OK**.
21. The **OllyDbg** main window appears, as shown in the screenshot.

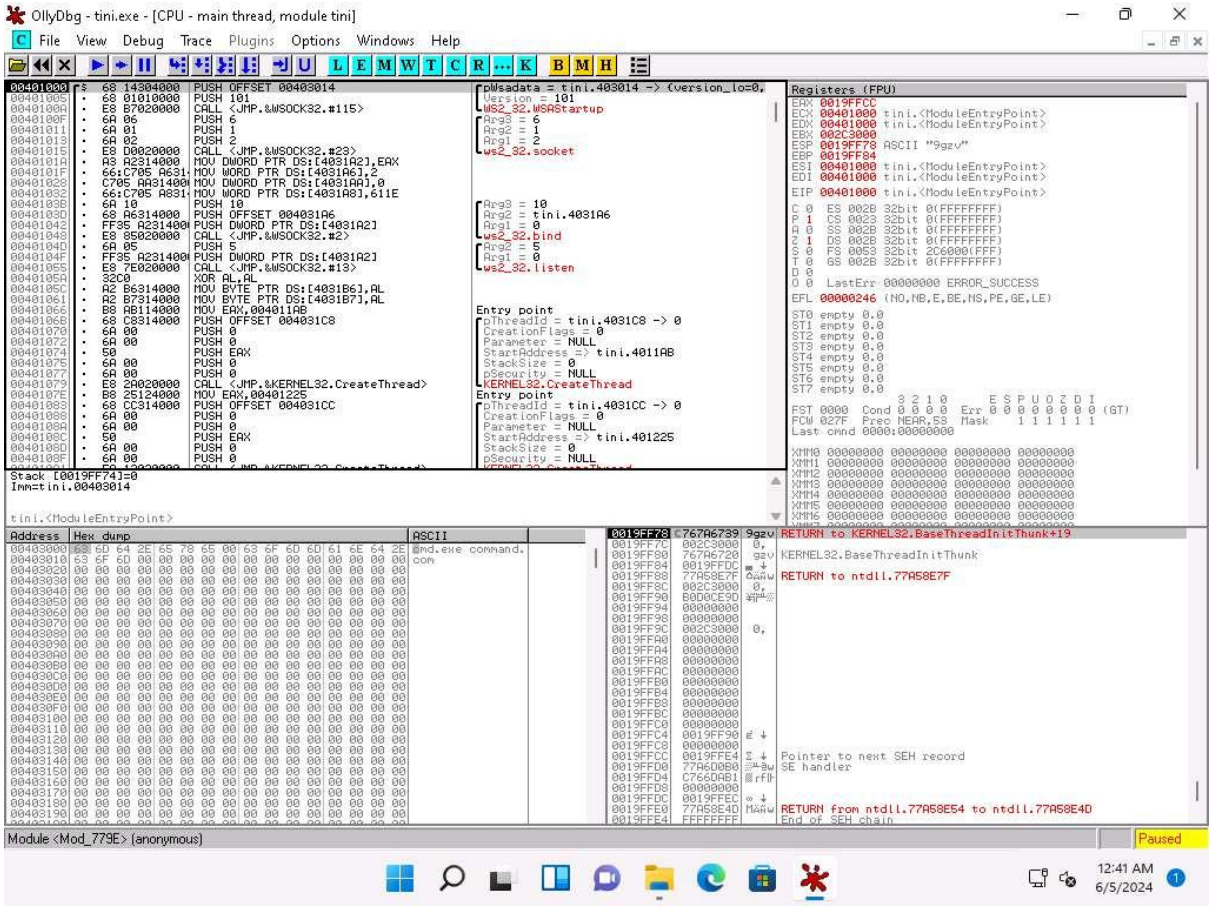
    When you launch OllyDbg for the first time, several sub-windows might appear in the main window of OllyDbg; close all of them.



22. Choose **File** from the menu bar, and then choose **Open**.

23. The **Select 32-bit executable** window appears; navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.

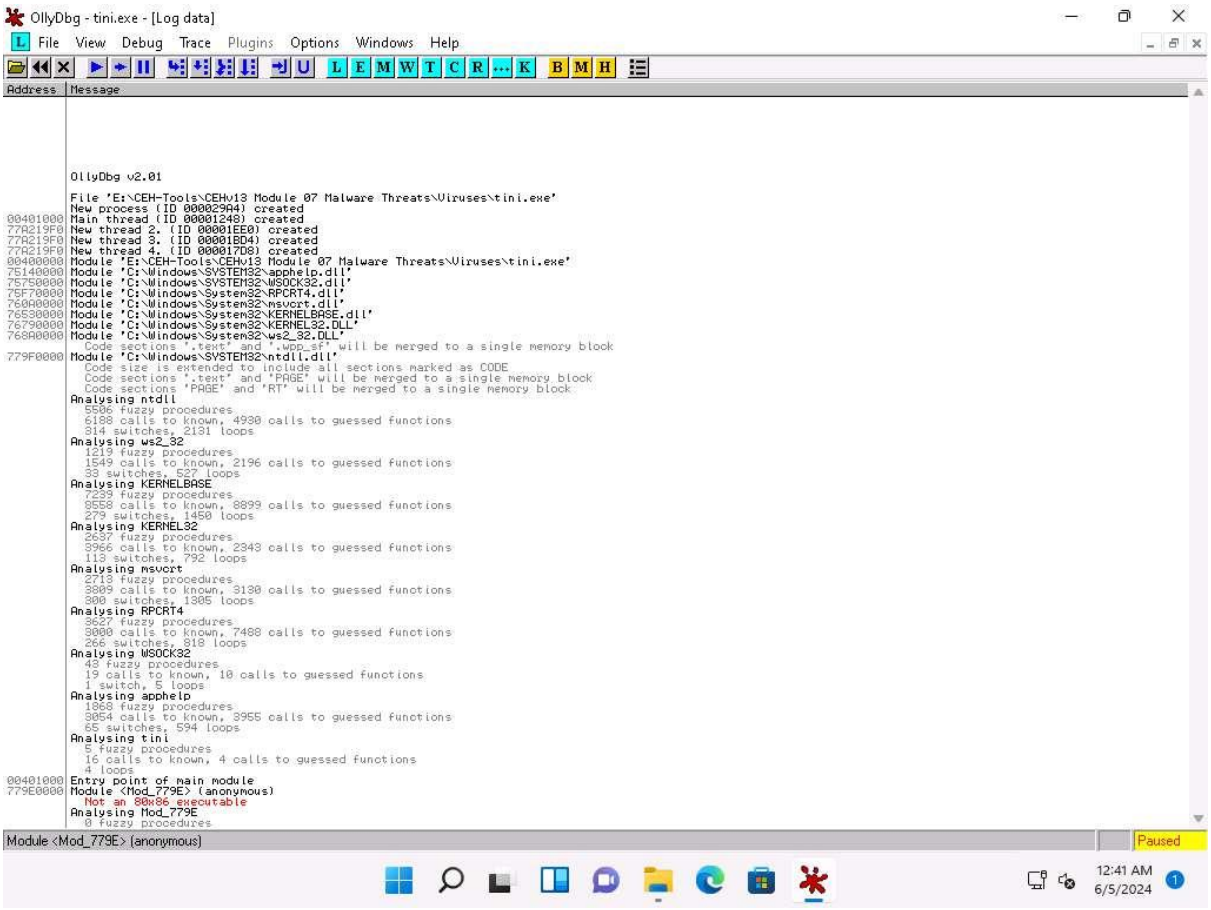
24. The output appears in a window named **CPU - main thread, module tini**, maximize the window.



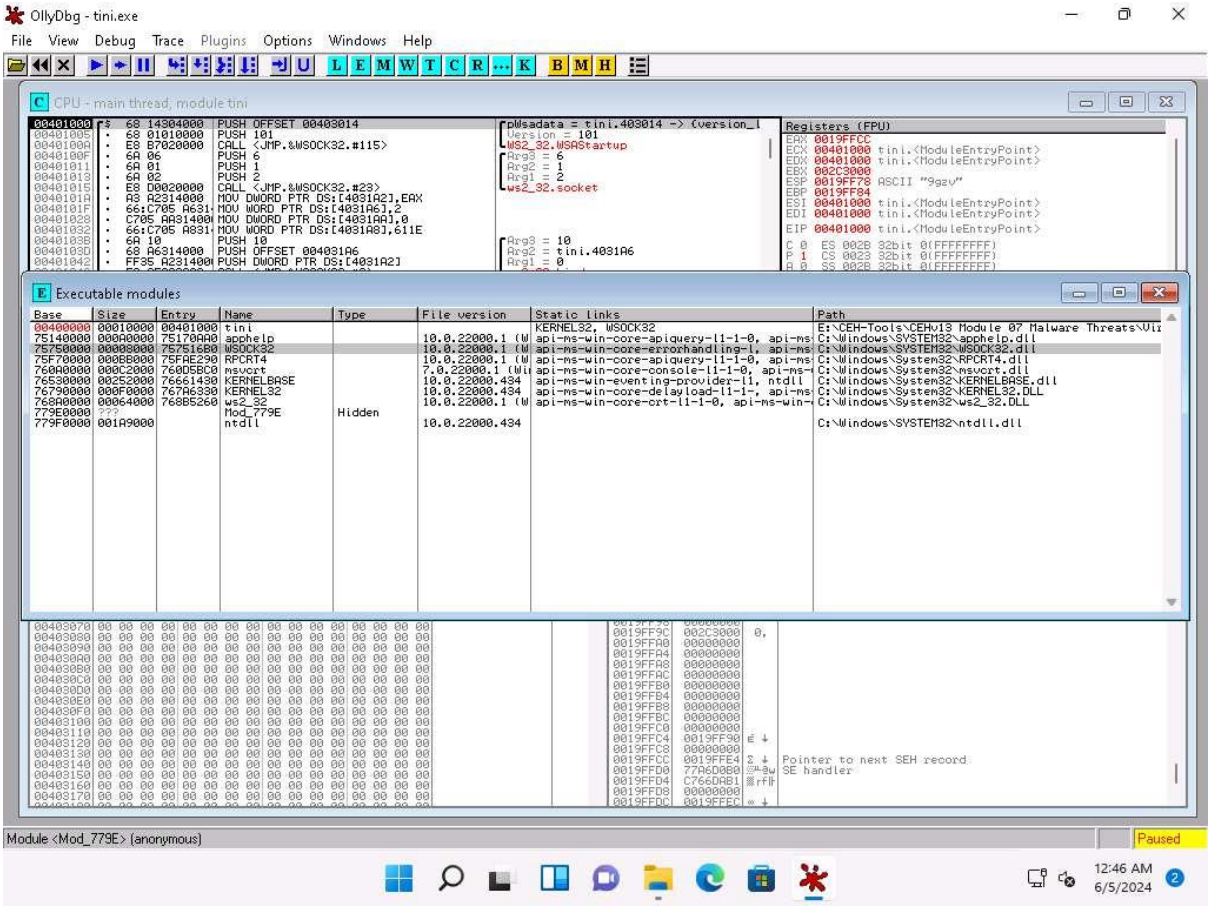
25. Choose **View** in the menu bar, and then choose **Log**.

26. A window named **Log data** appears in OllyDbg, displaying the log details.

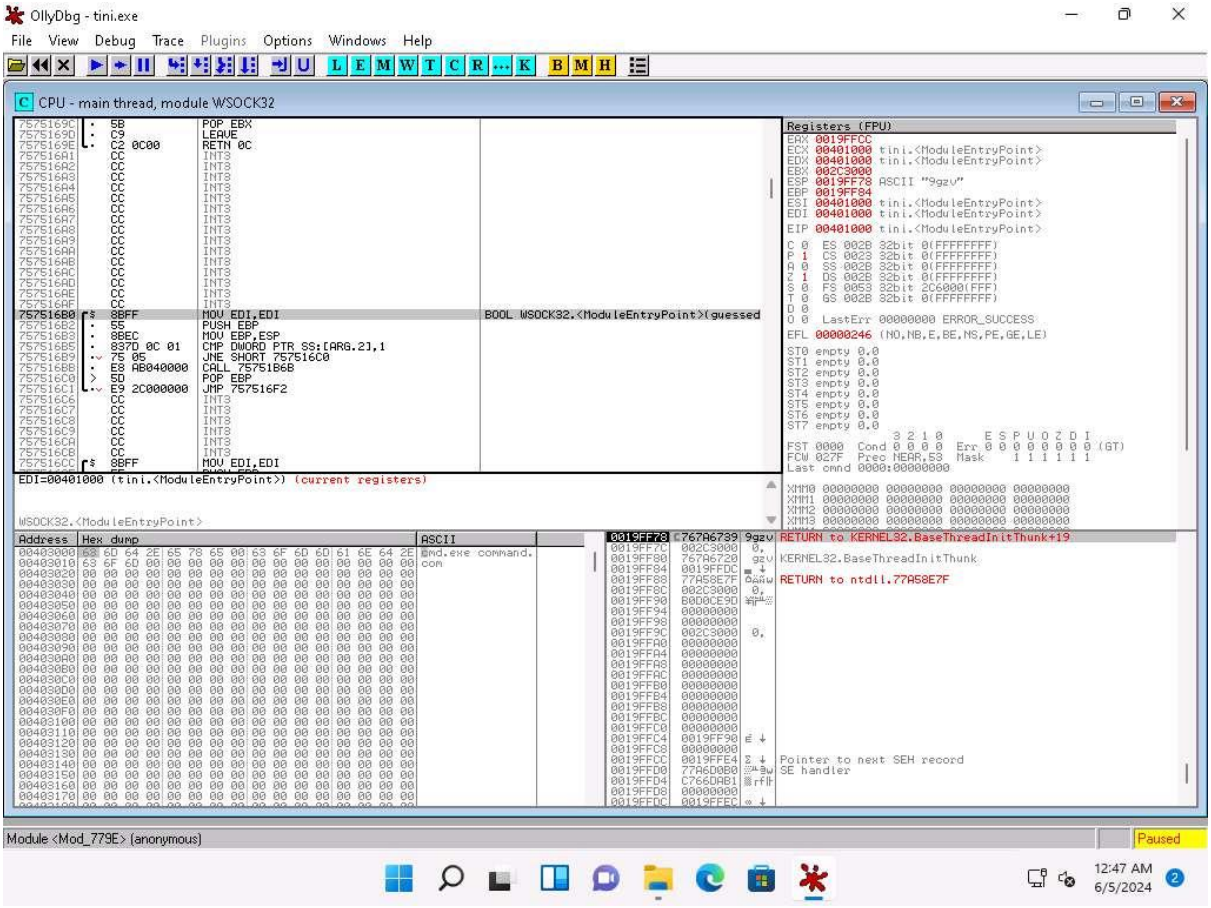
27. The **Log data** also displays the program entry point and its calls to known functions. Close the **Log data** window after completing the analysis.



28. Choose **View** in the menu bar, and then choose **Executable modules**.
29. A window named **Executable modules** appears in OllyDbg, displaying all executable modules.
30. Double-click any module to view the complete information of the selected module.
31. In this task, we are choosing the **75750000** module. The results might differ when you perform this task.

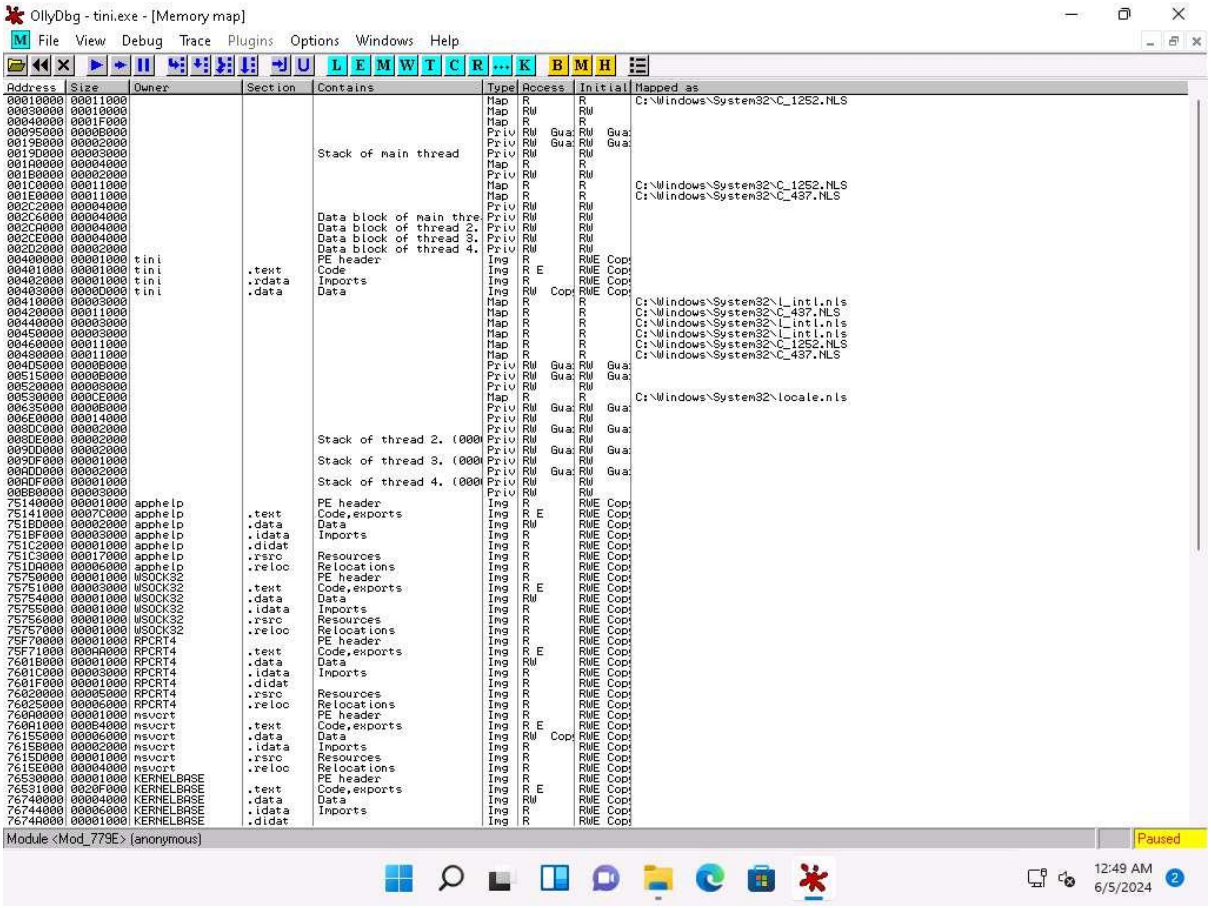


32. This will redirect you to the **CPU - main thread** window, as shown in the screenshot.



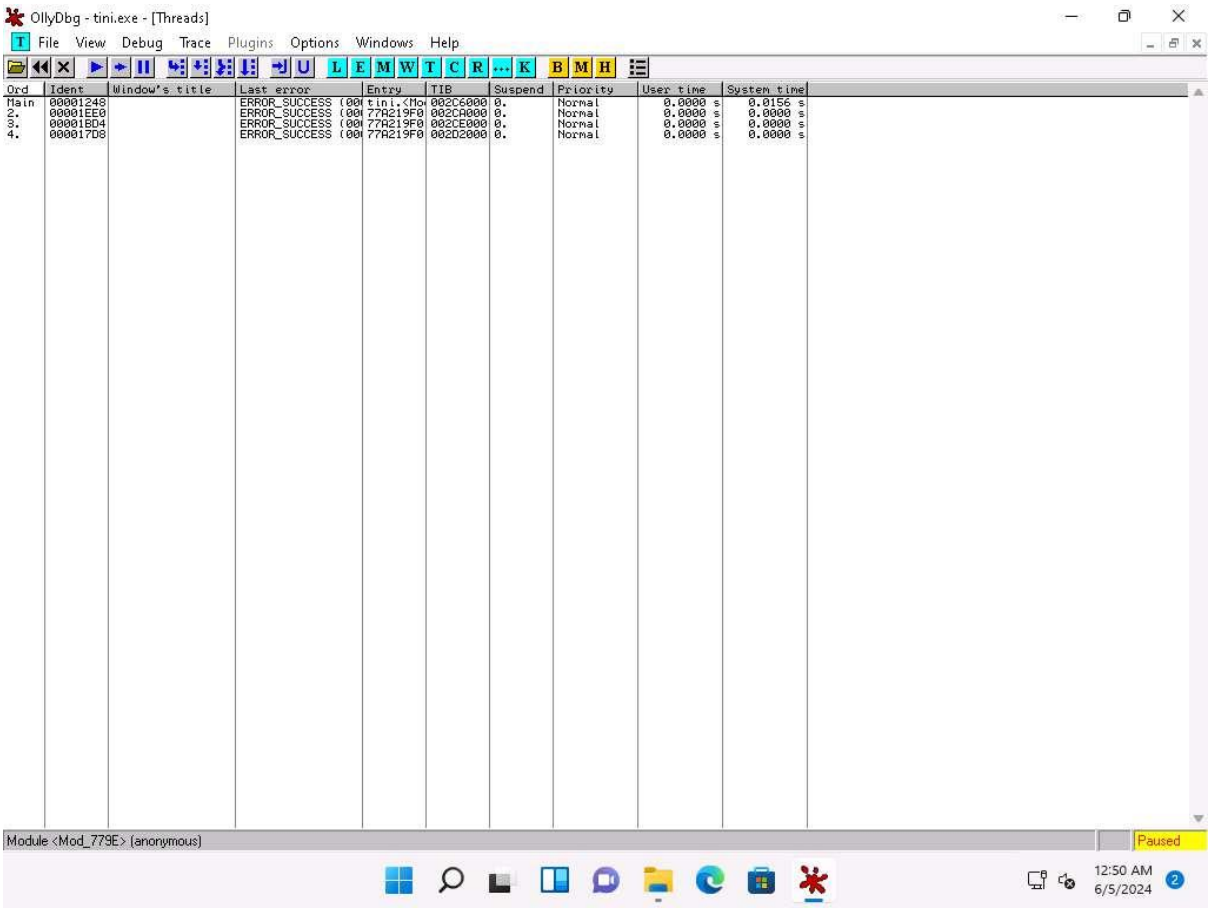
33. Choose **View** in the menu bar, and then choose **Memory map**.

34. A window named **Memory map** appears in OllyDbg, displaying all memory mappings, as shown in the screenshot. Close the **Memory map** window.



35. Choose **View** in the menu bar, and then choose **Threads**.

36. A window named **Threads** appears in OllyDbg, displaying all threads, as shown in the screenshot.



37. This way, you can scan files and analyze the output using OllyDbg.

38. Close all open windows.

Question 7.3.3.1

On the Windows 11 machine, use the IDA tool to analyze the file face.exe located in the directory E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!. What is the first subroutine function identified by IDA?

Lab 4: Perform Dynamic Malware Analysis

Lab Scenario

Dynamic Malware Analysis, also known as behavioral analysis, involves executing malware code to learn how it interacts with the host system and its impact after infecting the system.

Dynamic analysis involves the execution of malware to examine its conduct and operations and identify technical signatures that confirm the malicious intent. It reveals information such as

domain names, file path locations, created registry keys, IP addresses, additional files, installation files, and DLL and linked files located on the system or network.

This type of analysis requires a safe environment such as machines and sandboxes to deter the spreading of malware. The environment design should include tools that can capture every movement of the malware in detail and give feedback. Typically, systems act as a base for conducting such experiments.

An ethical hacker and pen tester must perform dynamic malware analysis to find out about the applications and processes running on a computer and remove unwanted or malicious programs that can breach privacy or affect the system's health.

Lab Objectives

- Perform port monitoring using TCPView and CurrPorts
- Perform process monitoring using Process Monitor

Overview of Dynamic Malware Analysis

Dynamic analysis is performed to gather valuable information about malware activity, including the files and folders created, ports and URLs accessed, called functions and libraries, applications and tools accessed, information transferred, settings modified processes, and services the malware started, and other items. You should design and set up the environment for performing the dynamic analysis in such a way that the malware cannot propagate to the production network, and ensure that the testing system can recover to an earlier set timeframe (prior to launching the malware) in case anything goes wrong during the test.

To achieve this, you need to perform the following:

- **System Baselining** Baselining refers to the process of capturing a system's state (taking snapshot of the system) at the time the malware analysis begins. This can be used to compare the system's state after executing the malware file, which will help understand the changes that the malware has made across the system. A system baseline involves recording details of the file system, registry, open ports, network activity, and other items.

- **Host Integrity Monitoring** Host integrity monitoring is the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents. It involves using the same tools to take a snapshot of the system before and after the incident or actions and analyzing the changes to evaluate the malware's impact on the system and its properties. In malware analysis, host integrity monitoring helps to understand the runtime behavior of a malware file as well as its activities, propagation techniques, URLs accessed, downloads initiated, and other characteristics.

  Host integrity monitoring includes:

  - Port monitoring

- Process monitoring
- Registry monitoring
- Windows services monitoring
- Startup program monitoring
- Event logs monitoring and analysis
- Installation monitoring
- Files and folder monitoring
- Device driver monitoring
- Network traffic monitoring and analysis
- DNS monitoring and resolution
- API calls monitoring

Task 1: Perform Port Monitoring using TCPView and CurrPorts

We know that the Internet uses a software protocol named TCP/IP to format and transfer data. Malware programs corrupt the system and open system input and output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks. These open ports can also act as backdoors or communication channels for other types of harmful malware and programs. They open unused ports on the victim's machine to connect back to the malware handlers.

You can identify the malware trying to access a particular port by installing port monitoring tools such as TCPView and CurrPorts.

TCPView TCPView is a Windows program that shows the detailed listings of all the TCP and UDP endpoints on the system, including the local and remote addresses, and the state of the TCP connections. It provides a subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.

CurrPorts CurrPorts is a piece of network monitoring software that displays a list of all the currently open TCP/IP and UDP ports on a local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, etc.), the time that the process was created, and the user that created it.

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP port information to an HTML file, XML file, or to tab-delimited text file.

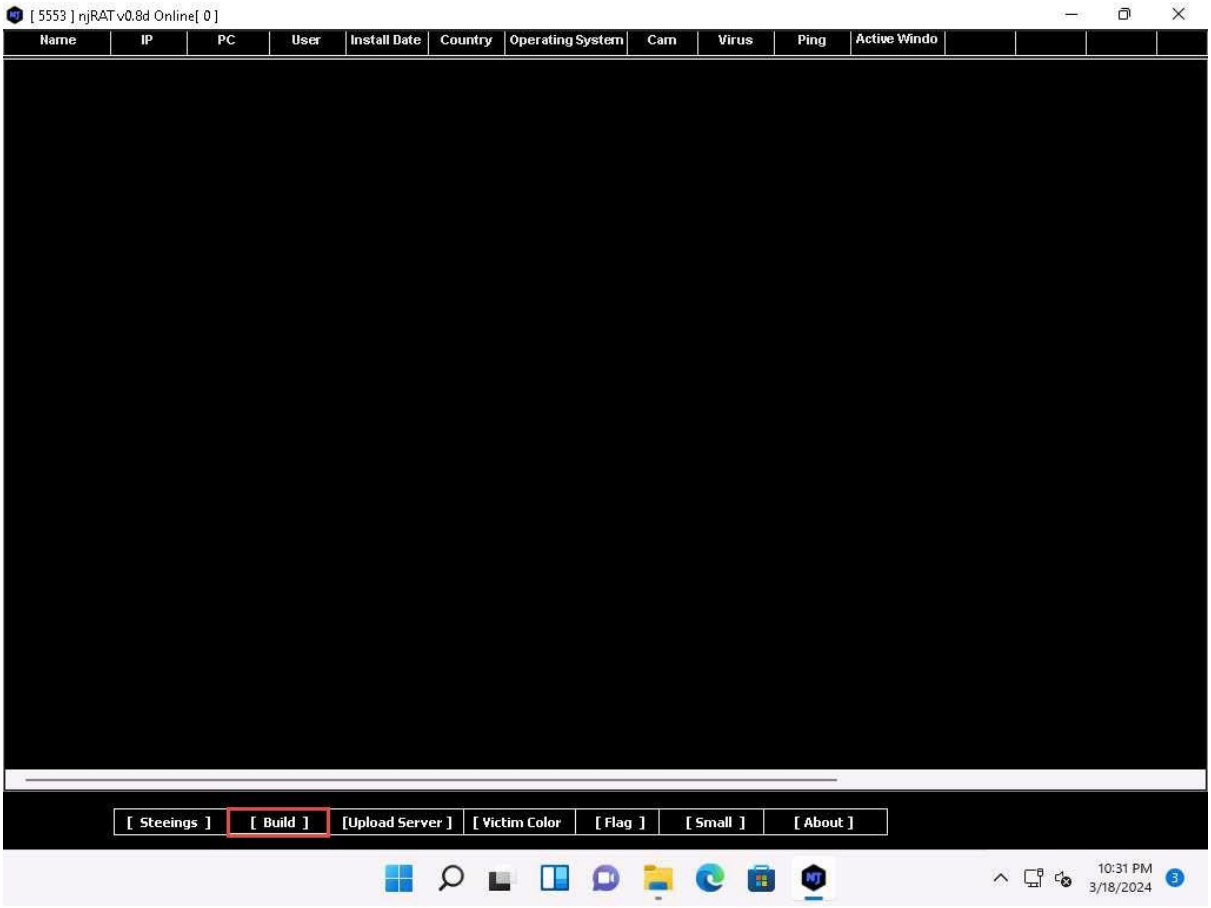
CurrPorts also automatically marks suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons) in pink.

This lab activity demonstrates how to analyze malicious processes running on a machine using TCPView and CurrPorts. Here, you will first create a server using njRAT, and then execute this server from the second machine. Later, you will run the TCPView and CurrPorts applications on the second machine and find that the process associated with the server is running on it.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.8d.exe** to launch **njRAT**.

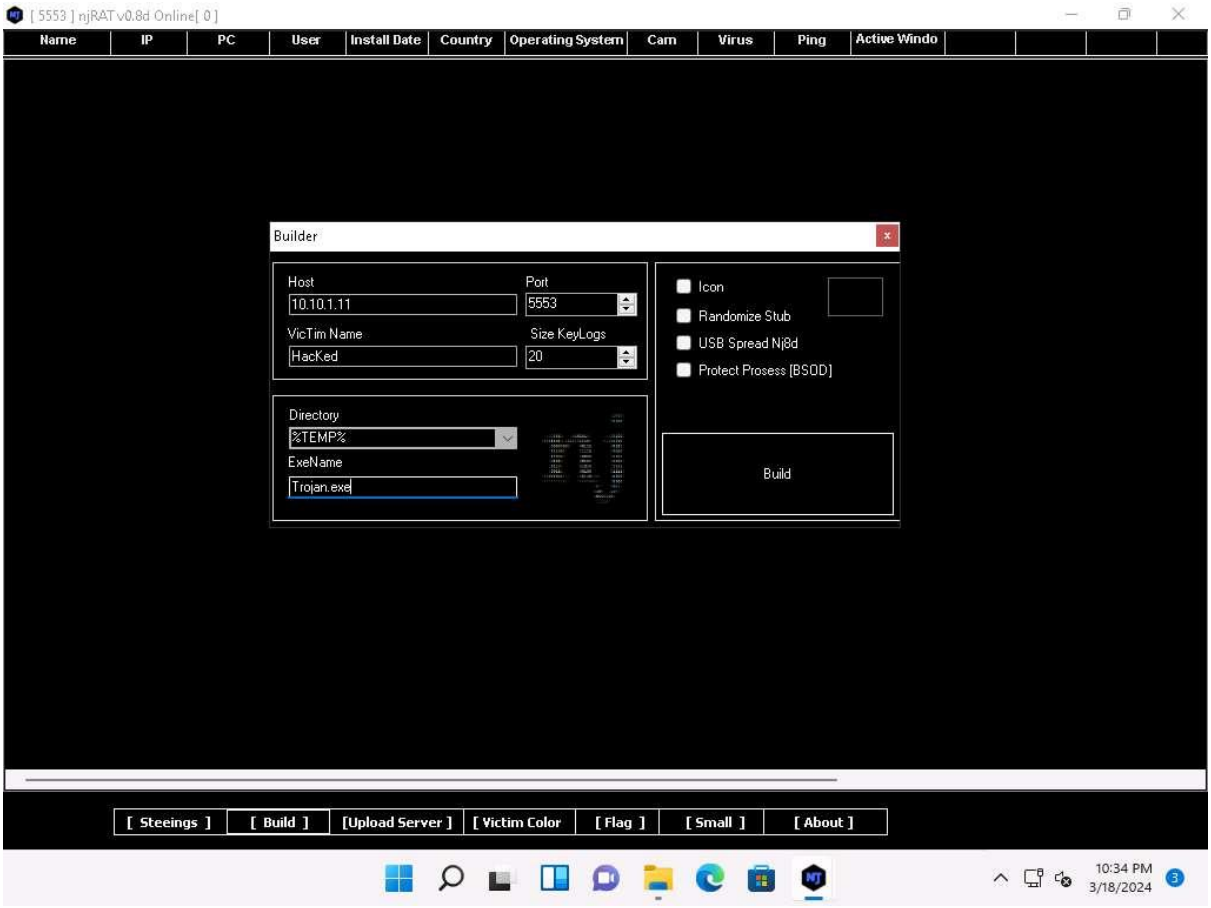
2. A **[Port Now]** pop-up appears, leave the port number to default and click on **OK**.

3. The njRAT GUI appears; click the **Build** link located in the lower-left corner of the GUI to configure the exploit details.

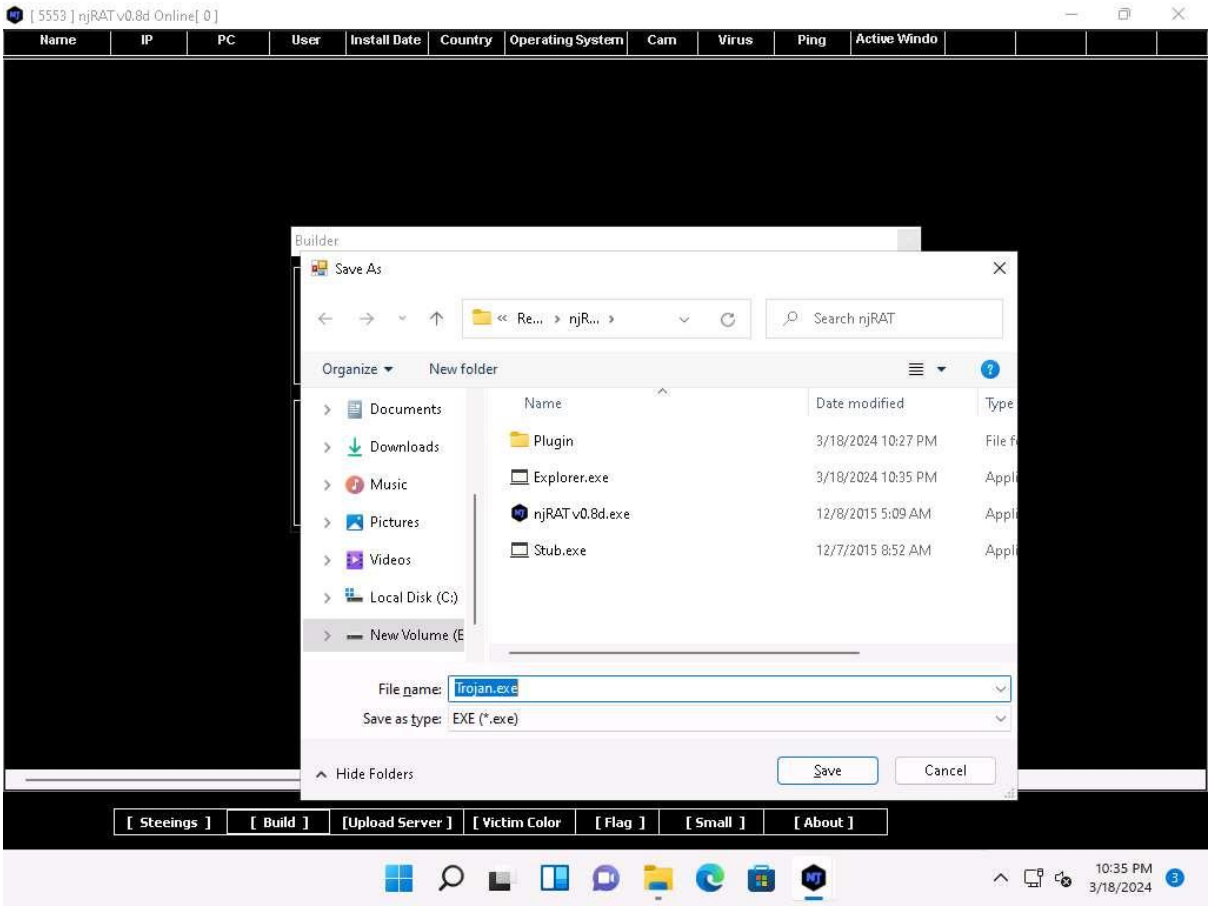


4. The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, rename **ExeName** as **Trojan.exe**. Leave the other settings to default, and click **Build**.

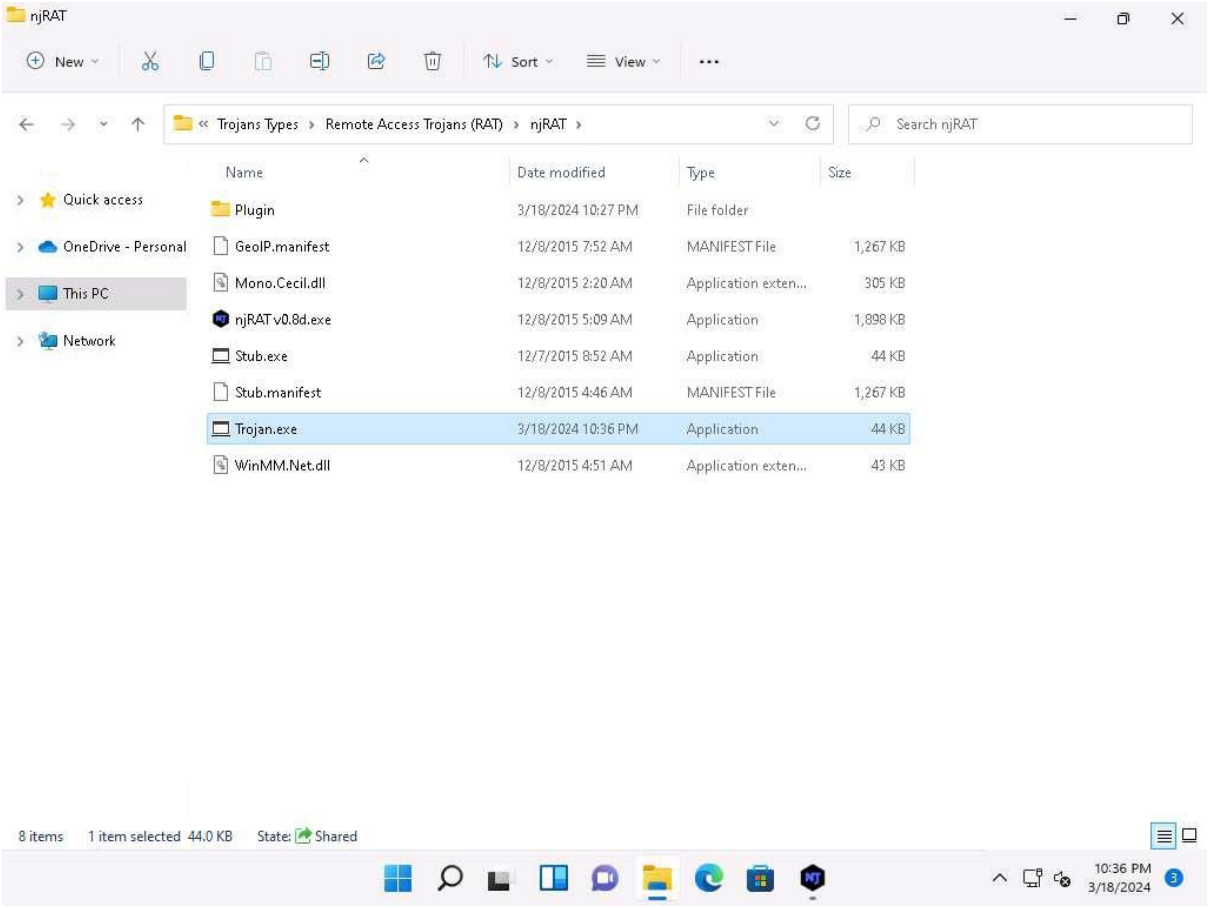
   In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.



5. **Save As** window appears, **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**. In the **File name**, enter **Trojan.exe** and click **Save**. **Done!** pop-up appears, click **OK**.



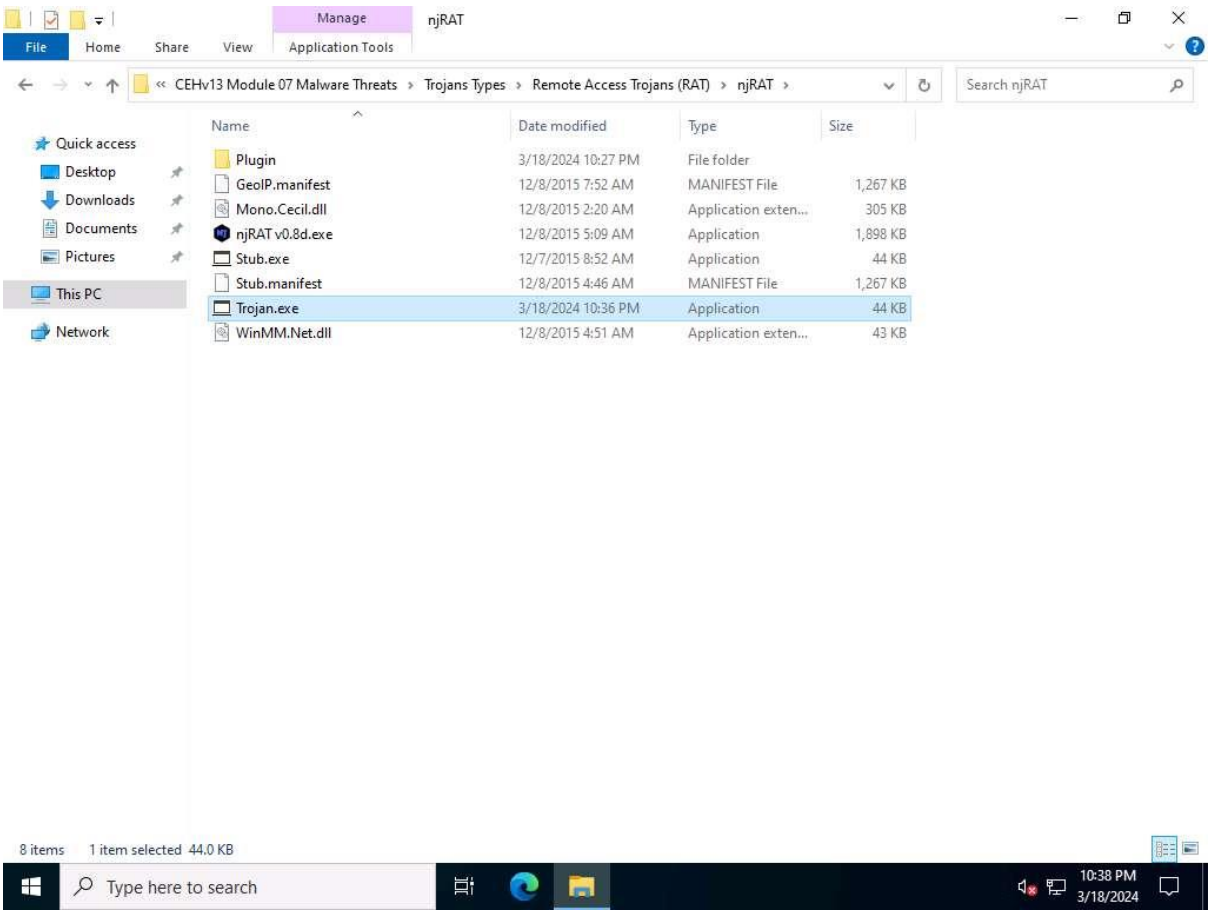
6. Minimize njRAT window. You can observe that a **Trojan.exe** file has been created at the location **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.



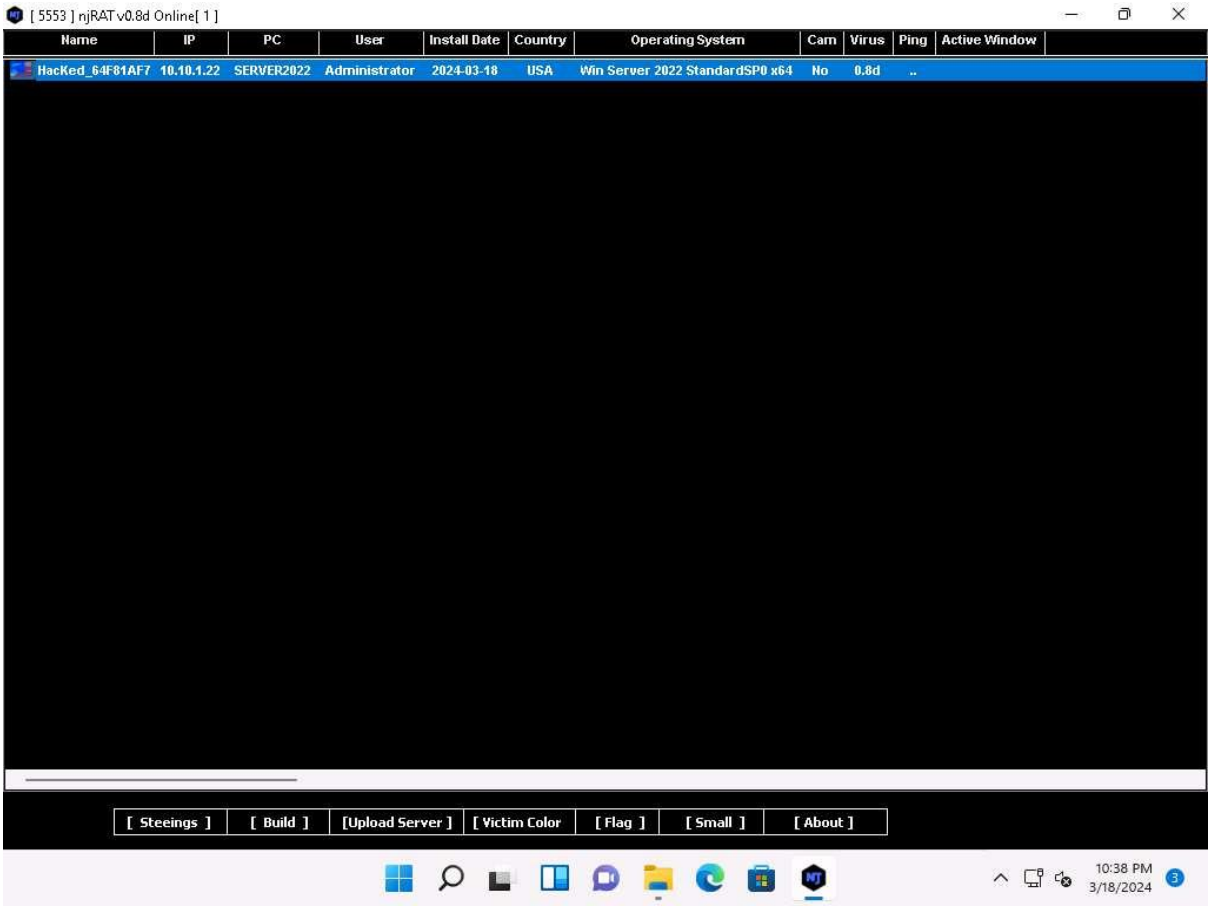
7. Click Windows Server 2022 to switch to the **Windows Server 2022** machine. Click Ctrl+Alt+Delete to activate the machine, login with **CEH\Administrator/Pa$$w0rd**.

   Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

8. Navigate to **Z:\CEHv13 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe**.



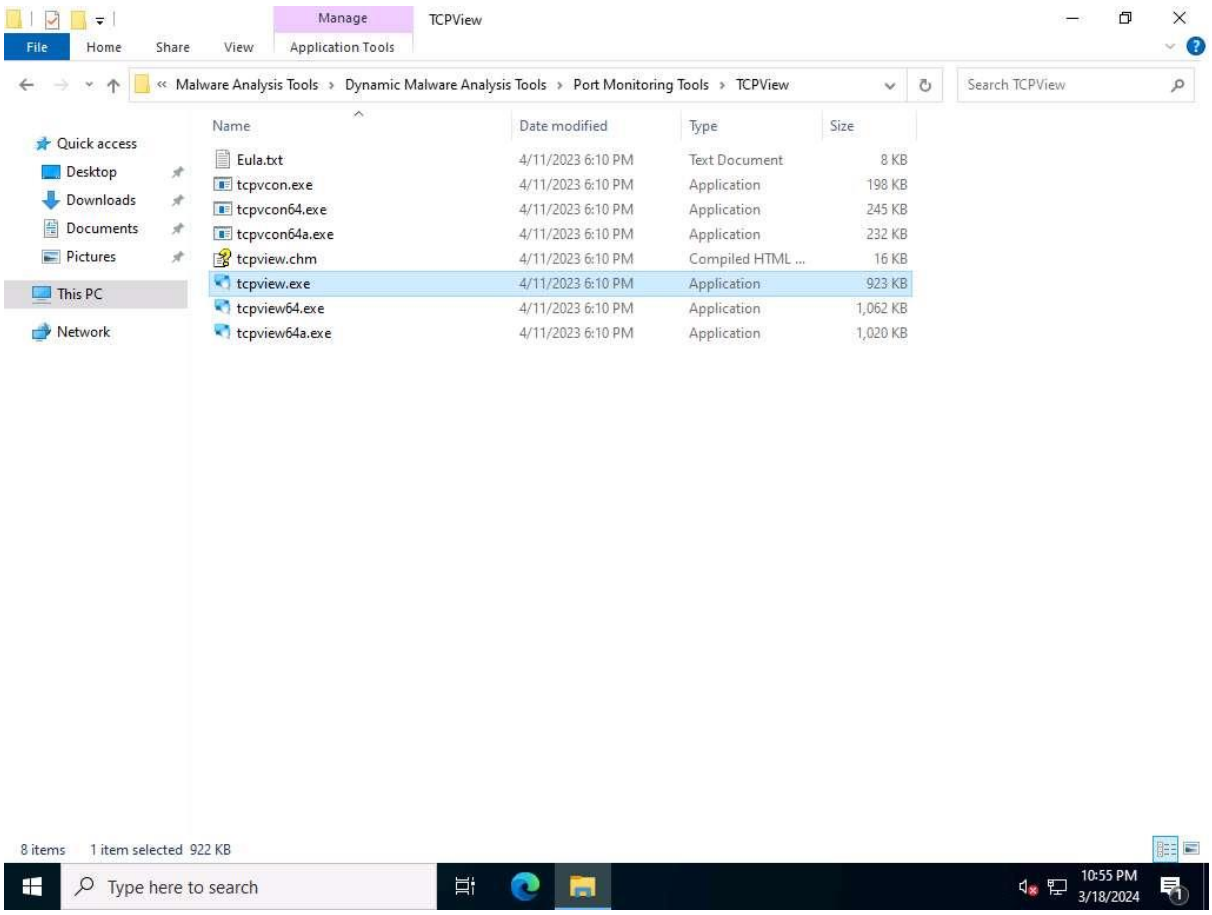
9. Observe that a connection has been established by the njRAT client. Click Windows 11 to switch to the **Windows 11** machine. Switch to **njRAT** window to observe the established connection.



10. Now, let us analyze this process on **Windows Server 2022** using **TCPView** tool. Click Windows Server 2022 to switch back to the **Windows Server 2022** machine.

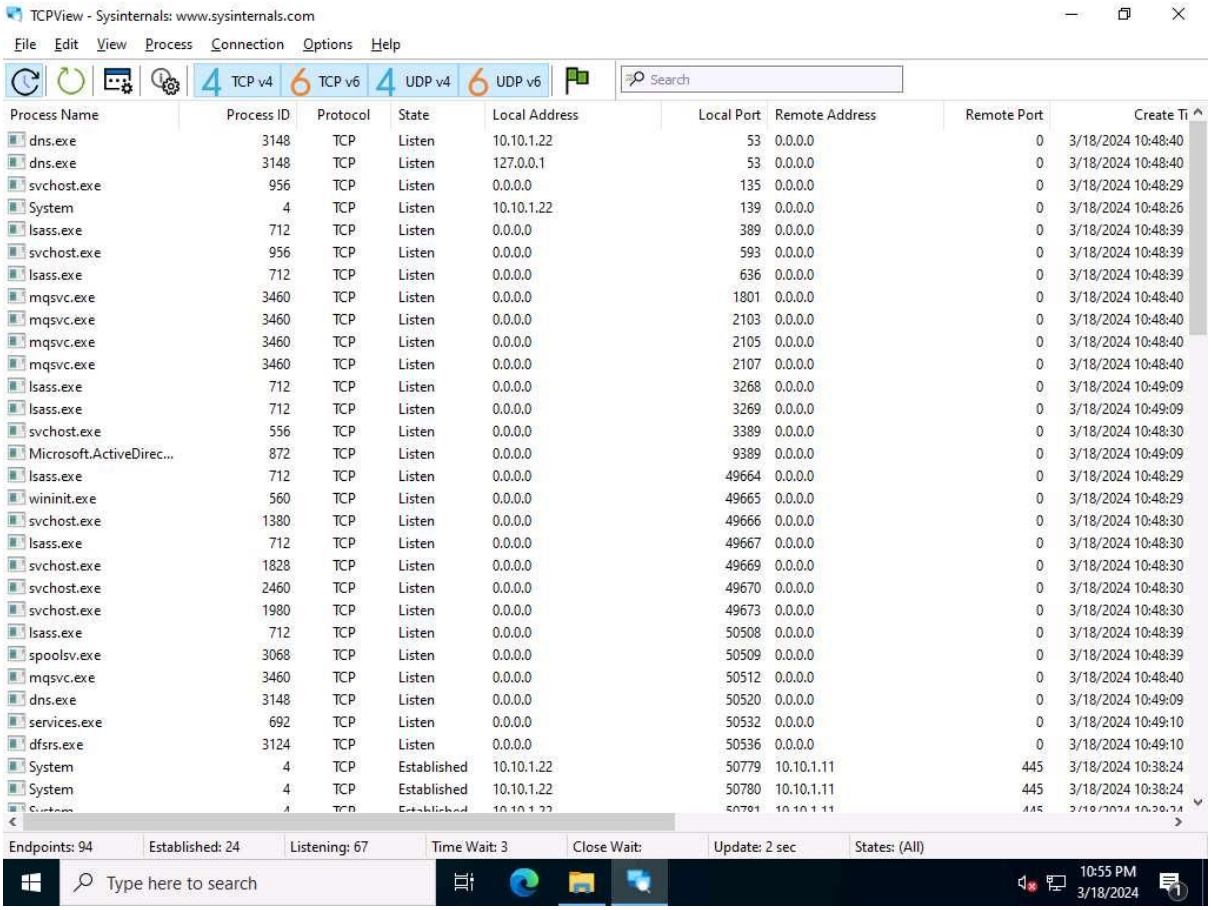
11. Navigate to **Z:\CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView** and double-click **tcpview.exe** to launch the application.

    If a **User Account Control** pop-up appears, click **Yes**.



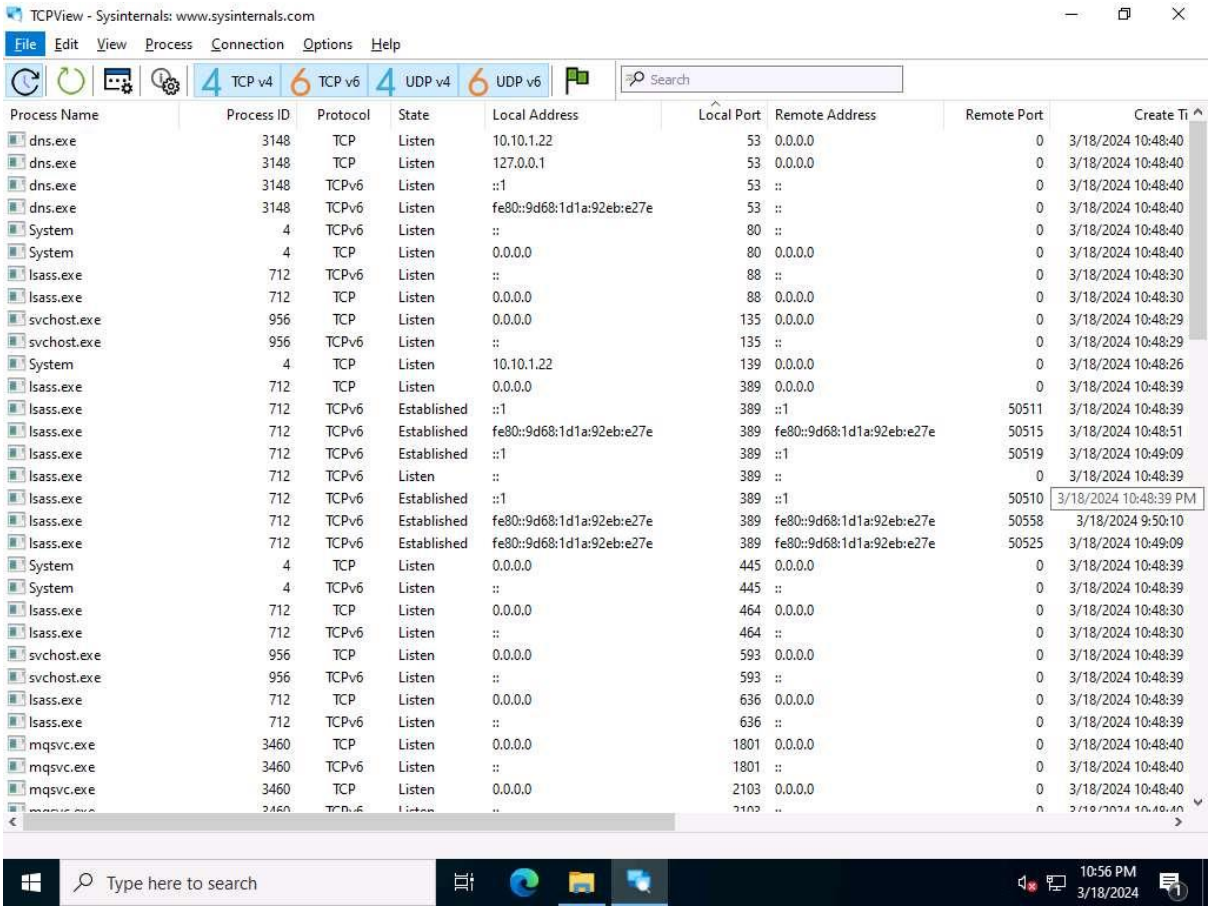
12. If a **TCPView License Agreement** window appears, click the **Agree** button to agree to the terms and conditions.

13. The **TCPView** main window appears, displaying the details such as Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, as shown in the screenshot.



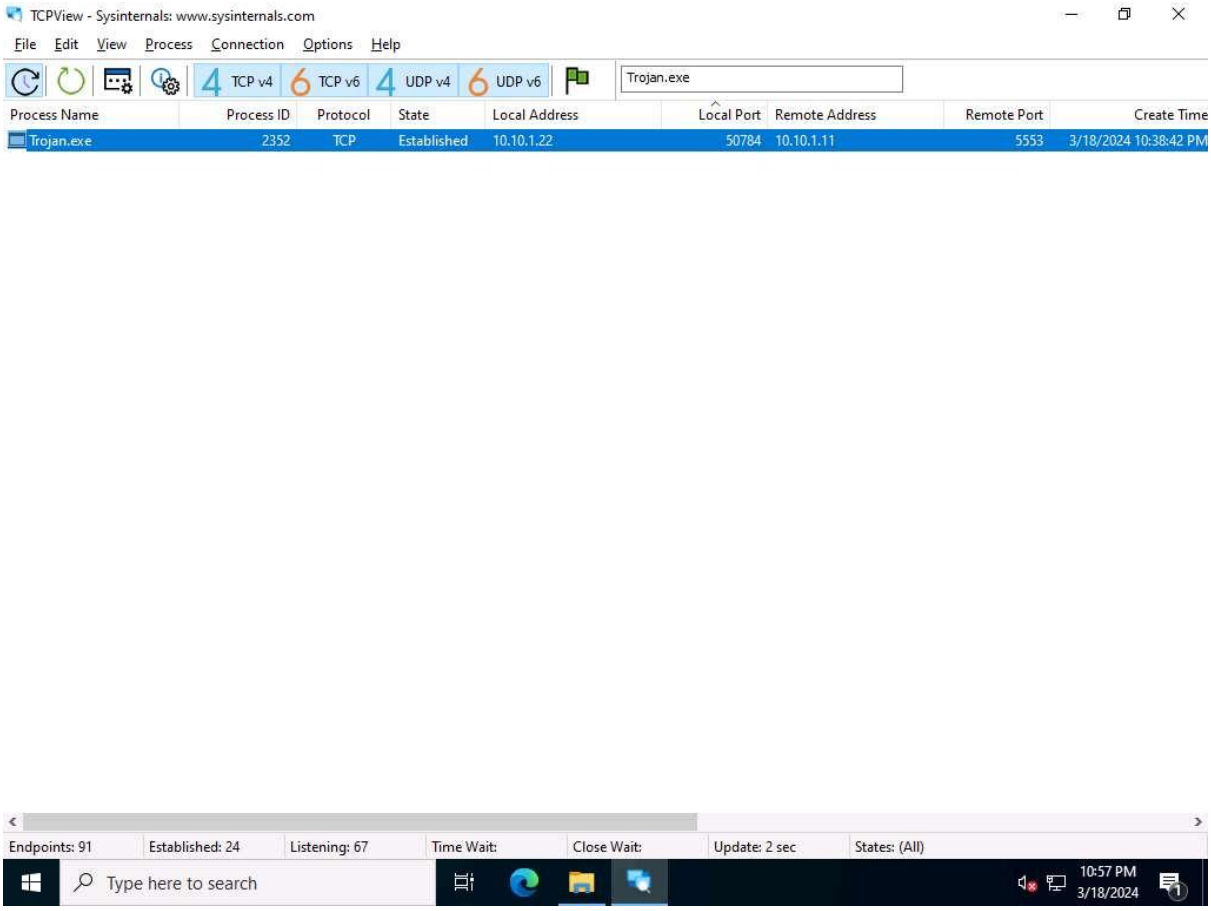
14. TCPView performs **Port monitoring**. Click the **Local Port** tab to view the ports in serial order.

15. Observe the protocols running on different ports under the **Protocol** column.

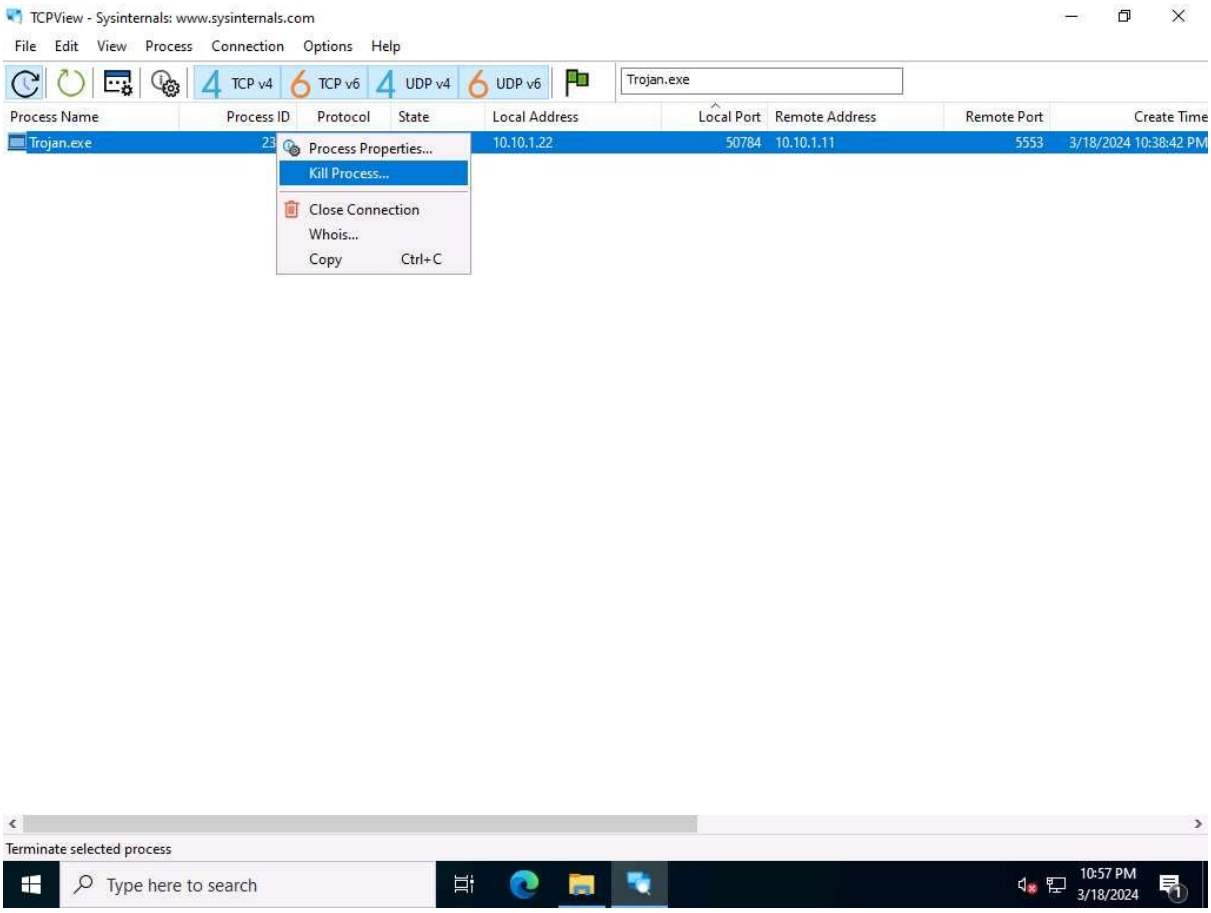


16. As you have executed a malicious application, now search for the **Trojan.exe** process in the TCPView.

17. You can observe that the **Trojan.exe** malicious program is running on the **Windows Server 2022** machine. You can see details such as **Remote Address** and **Remote Port**.

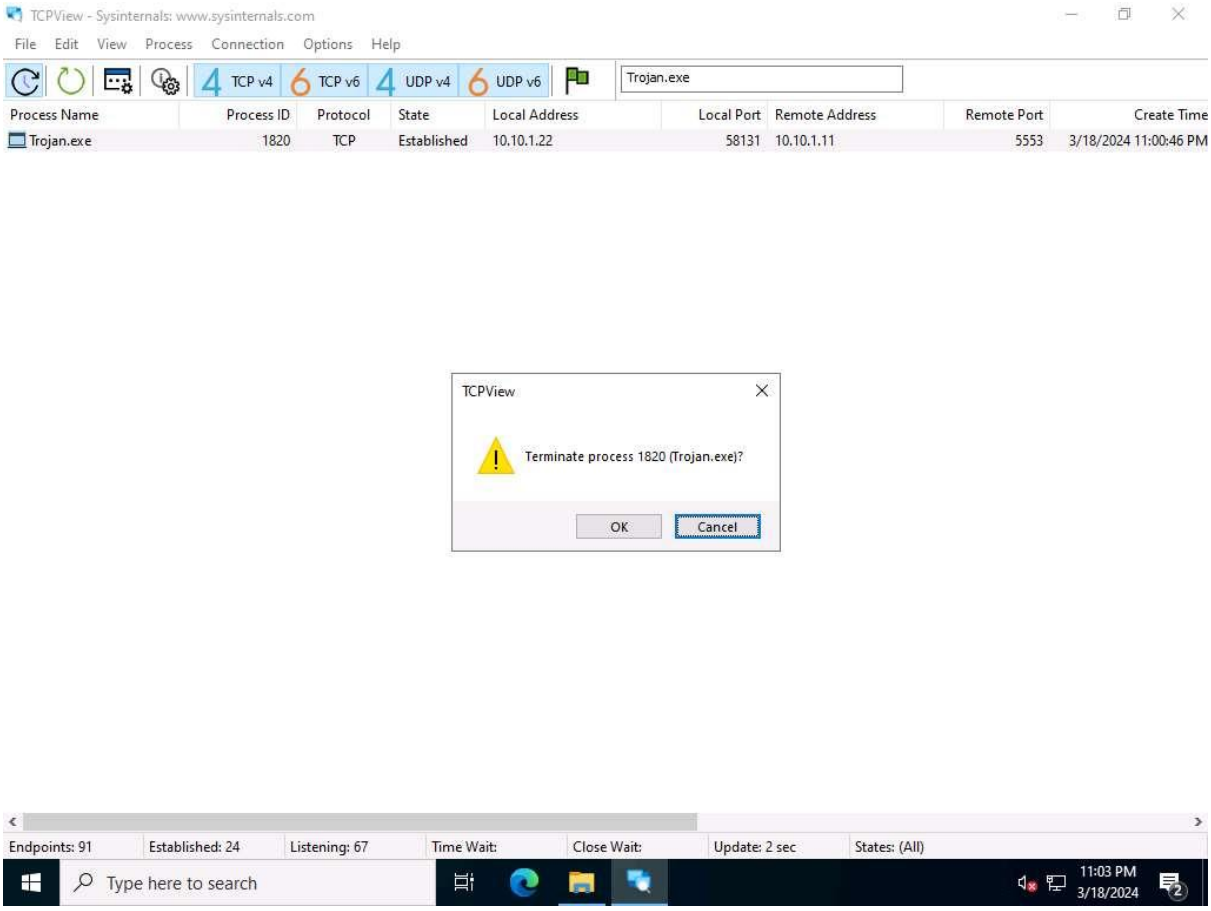


18. You can right-click the process **Trojan.exe**; select **Kill Process…** to end the running process.



19. For this task, do not Kill the process in this step as we are going to use this running process for the next task; click **Cancel**.

    Normally, if a **TCPView** dialog box appears, click **OK** to terminate the process.

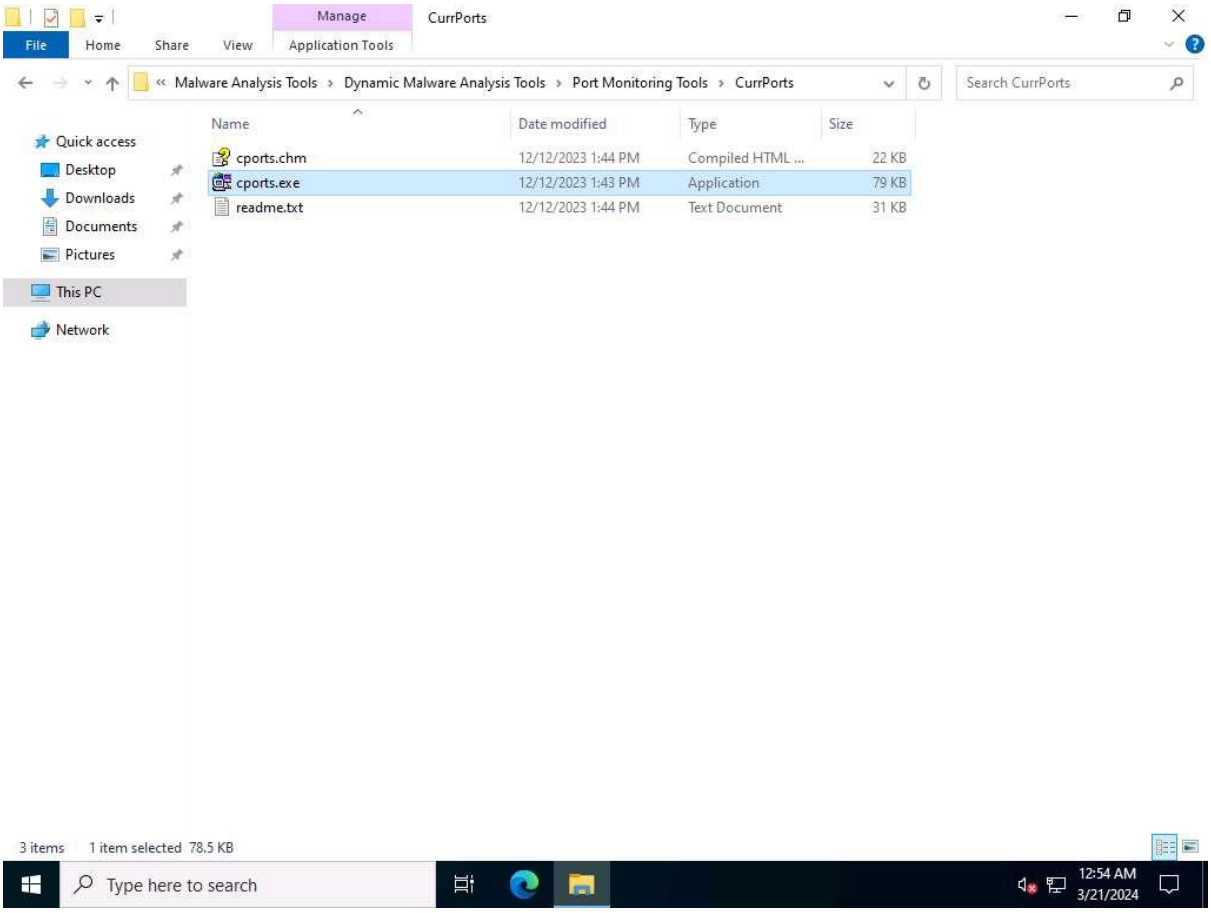


20. This way, you can view all processes running on the machine and stop unwanted or malicious processes that may affect your system. If you are unable to stop a process, you can view the port on which it is running and add a firewall rule to block the port.

21. Close the **TCPView** window.

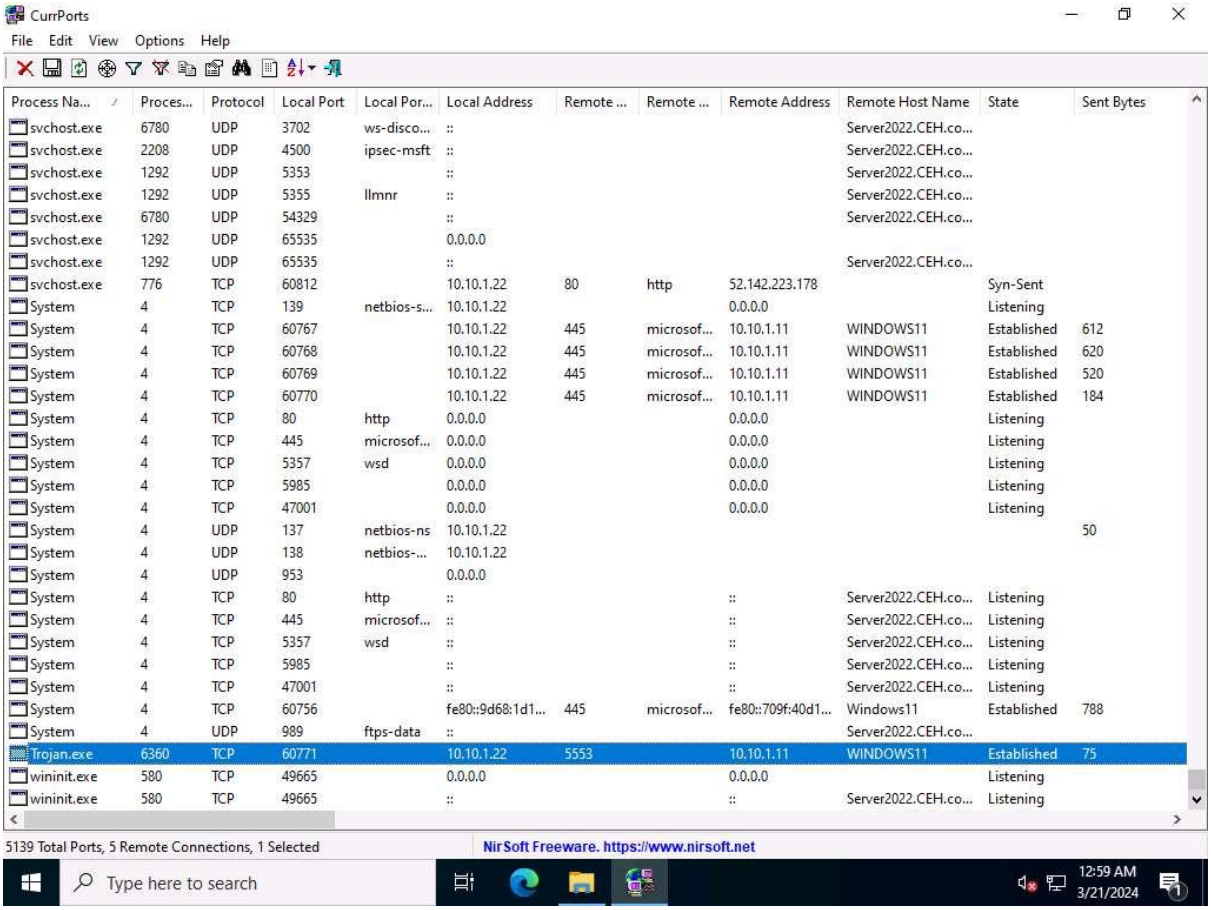
22. Now, let us analyze this process on **Windows Server 2022** using **CurrPorts**.

23. Navigate to **Z:\CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts** and double-click **cports.exe**.

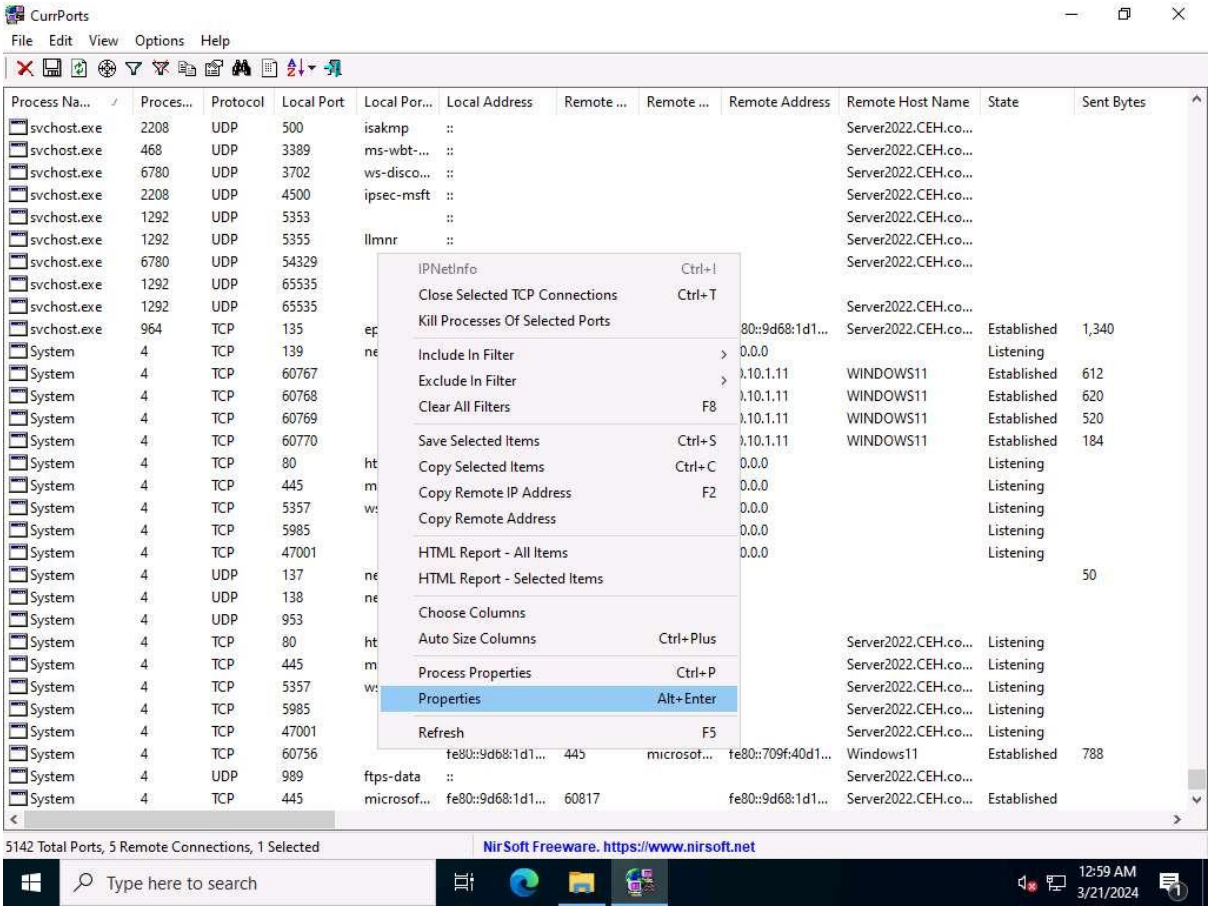


24. The **CurrPorts** window appears, displaying a list of currently open TCP/IP and UDP ports on the machine.

25. Scroll-down to search for **Trojan.exe** process running on the machine, as the shown in the screenshot. It is evident from the above screenshot that the process is connected to the machine on **port 5553**.

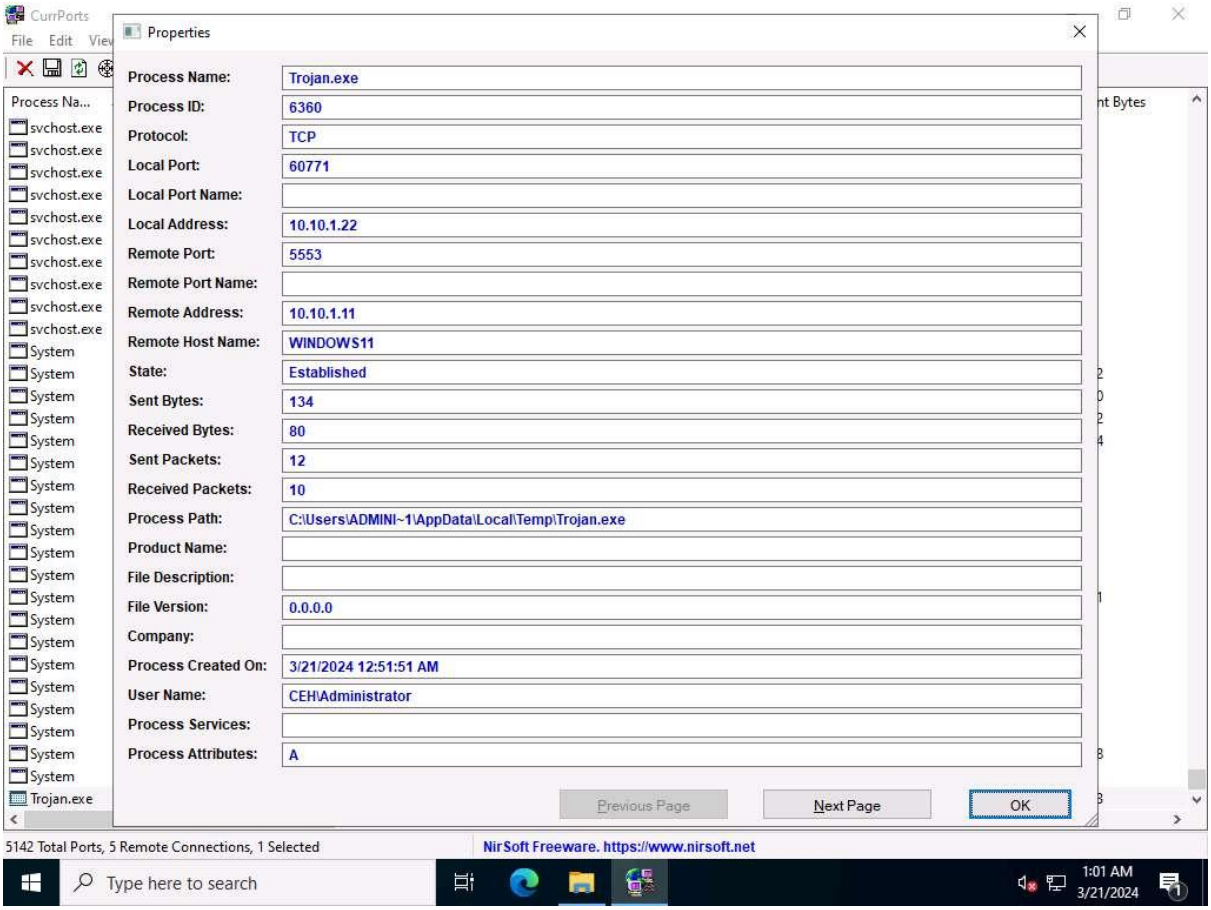


26. You can view the properties of the process by right-clicking on the process and clicking **Properties** from the **Context** menu.



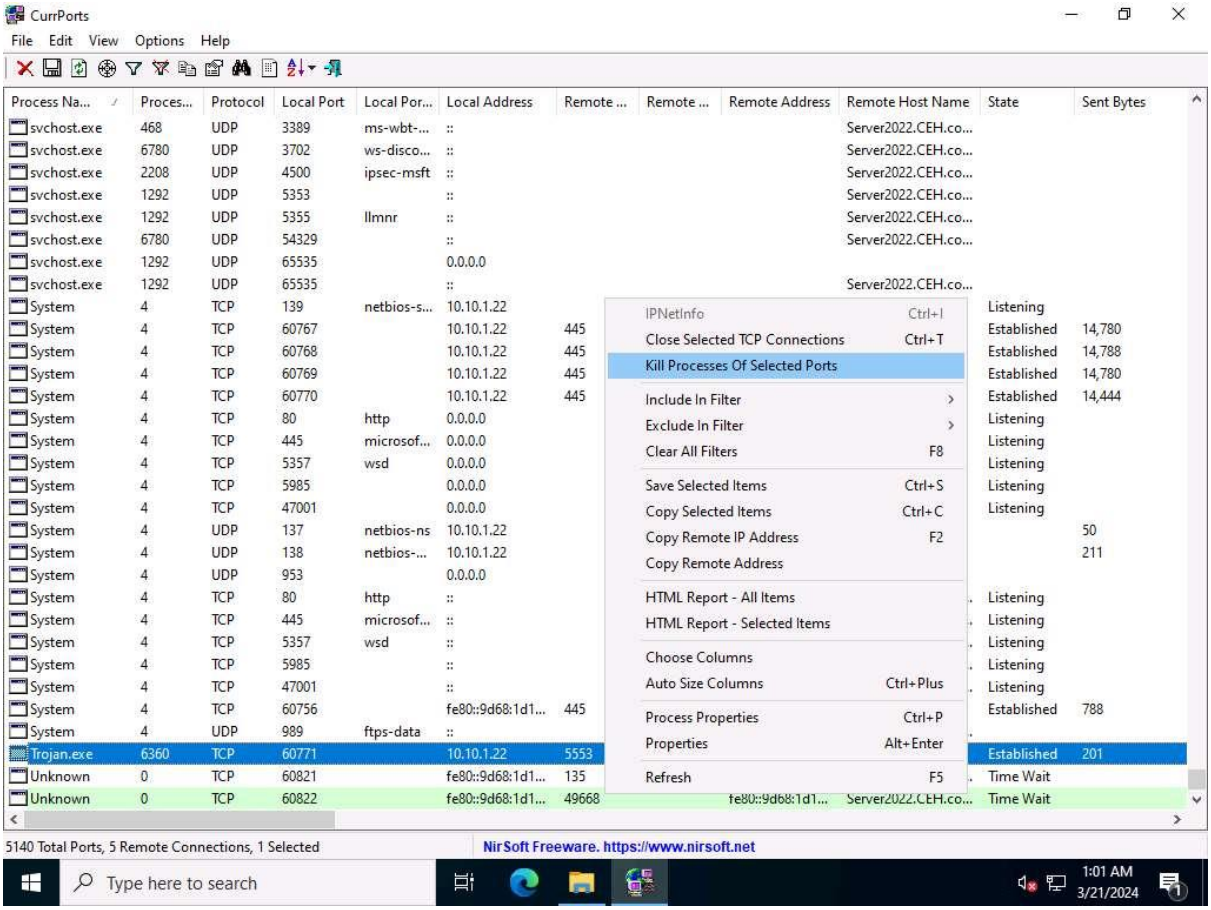
27. The **Properties** window appears, displaying information related to the process such as the name of the process, its process ID, Remote Address, Process Path, Remote Host Name, and other details.

28. Once you are done examining the properties associated with the process, click **OK**.



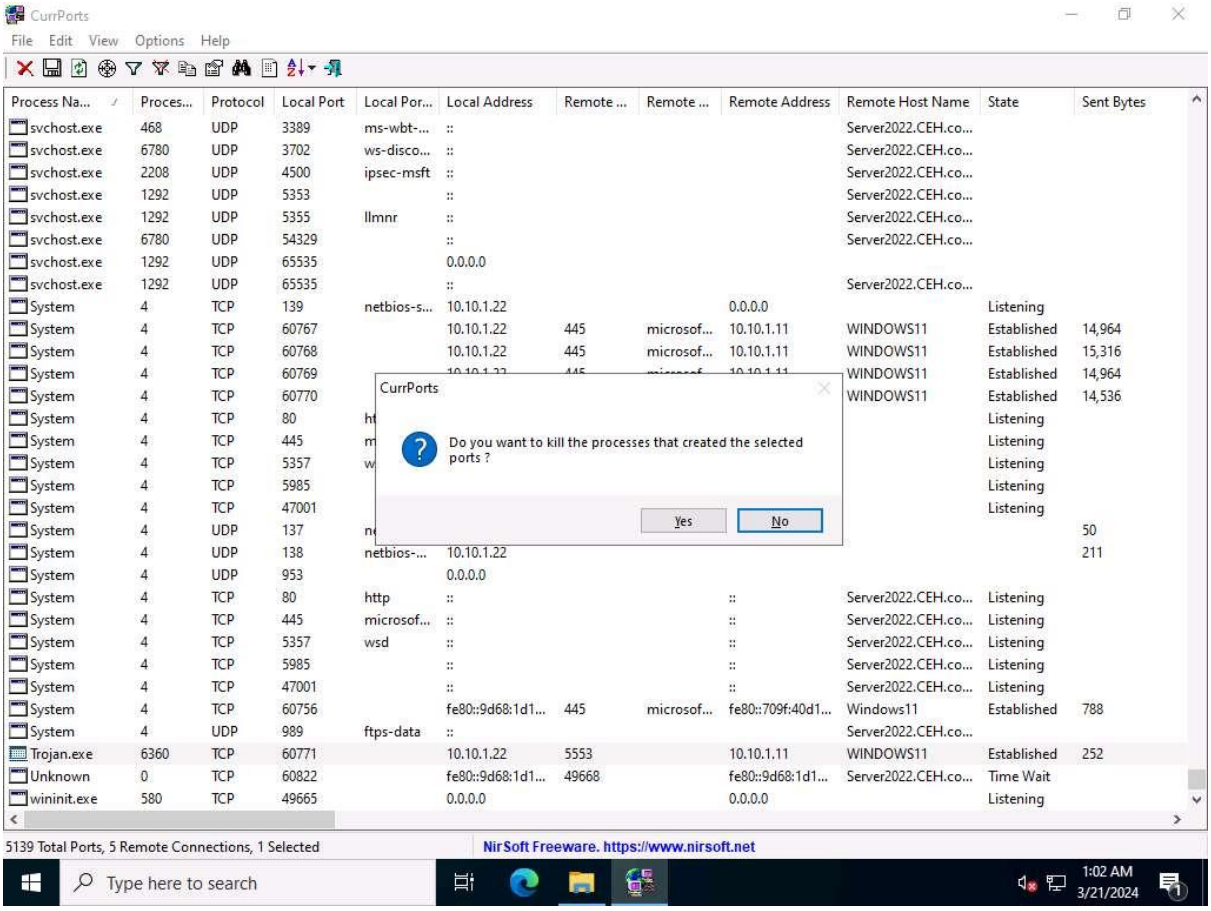
29. Because **Trojan.exe** is a malicious process, you may end the process by right-clicking on it and selecting **Kill Processes Of Selected Ports** from the context menu.

30. Alternatively, you may select **Close Selected TCP Connections**, so that the port closes, and the attacker can never regain connection through the port unless you open it.



31. Do not Kill the process at this step, as this running process will be used for the next task; when the **CurrPorts** dialog-box appears click **No**.

    Normally, when the **CurrPorts** dialog-box appears, you would click **Yes** to close the connection.



32. This way, you can analyze the ports open on a machine and the processes running on it.

33. If a process is found to be suspicious, you may either kill the process or close the port.

34. Close all open windows.

35. You can also use other port monitoring tools such as **TCP Port/Telnet Monitoring** (https://www.dotcom-monitor.com), **PRTG Network Monitor** (https://www.paessler.com), **SolarWinds Open Port Scanner** (https://www.solarwinds.com) or to perform port monitoring.

Question 7.4.1.1

Run njRAT from the attacker machine (Windows 11) and gain control over the victim machine (Windows Server 2022). On the Windows Server 2022 machine, use the TCPView tool to find the connections created by the Trojan. What is the remote port used by the Trojan server?

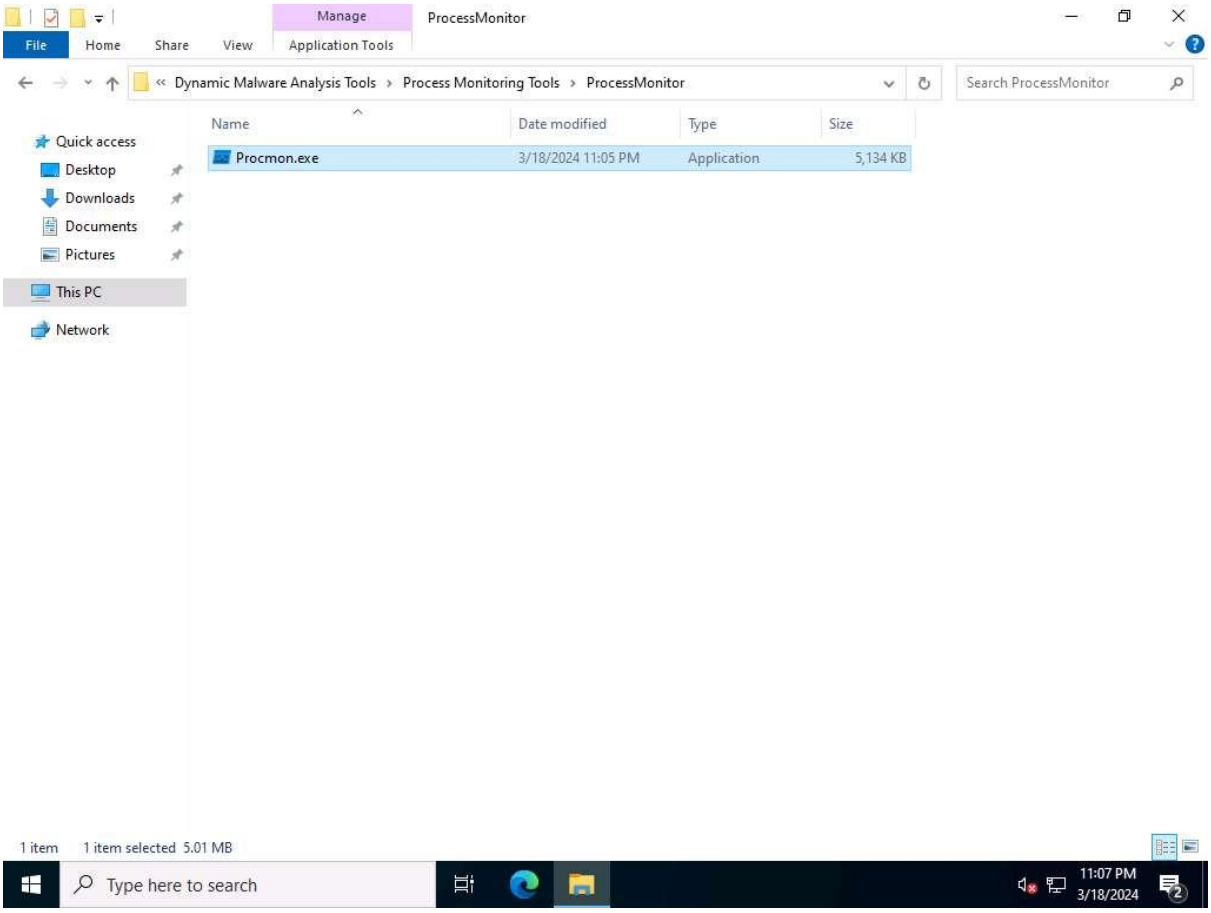
Task 2: Perform Process Monitoring using Process Monitor

Process monitoring will help in understanding the processes that malware initiates and takes over after execution. You should also observe the child processes, associated handles, loaded libraries, functions, and execution flow of boot time processes to define the entire nature of a file or program, gather information about processes running before the execution of the malware, and compare them with the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all processes that malware starts.

Process Monitor is a monitoring tool for Windows that shows the real-time file system, Registry, and process and thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon. It adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, and simultaneous logging to a file. Unique features of Process Monitor make it a core utility in system troubleshooting and vital to the malware hunting toolkit.

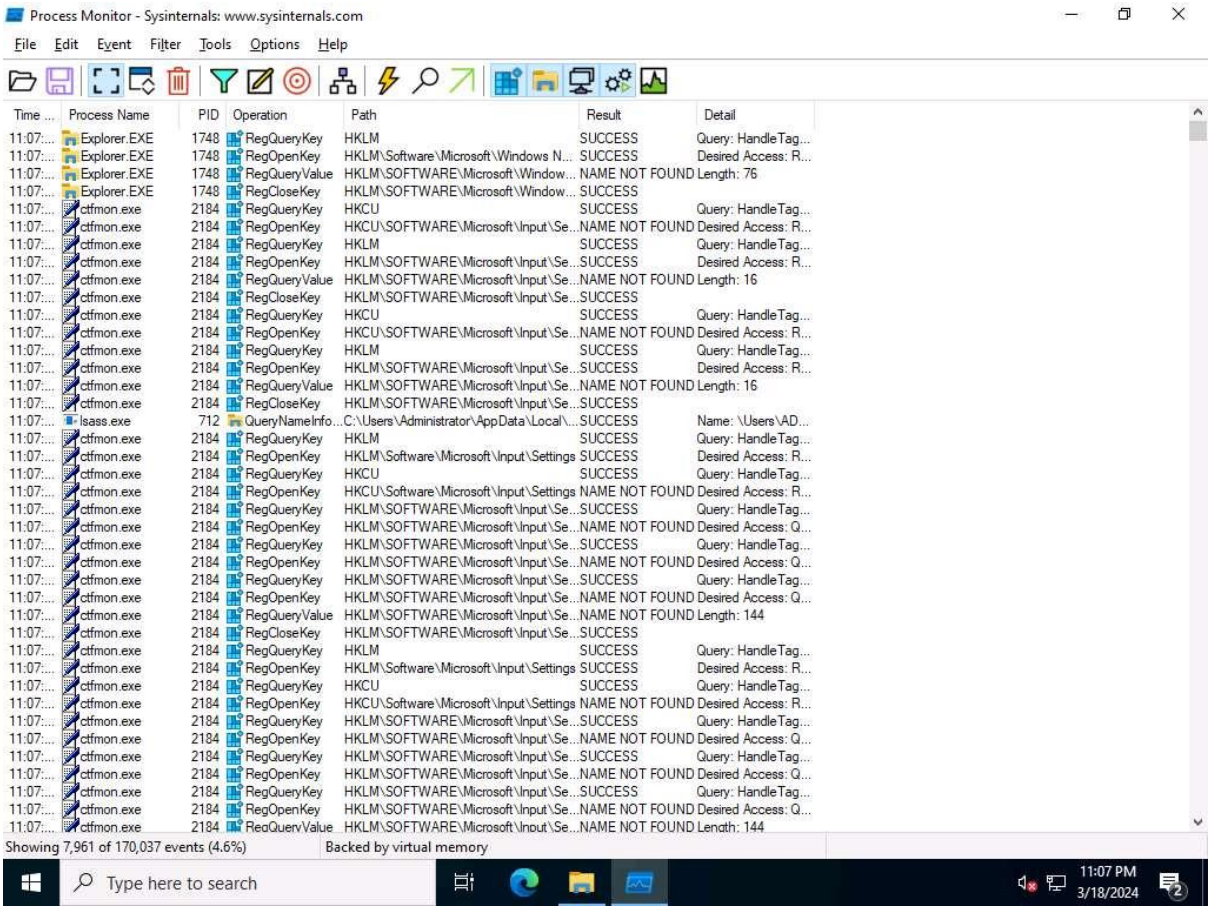
Here, we will use the Process Monitor tool to detect suspicious processes.

1. On the **Windows Server 2022** machine, navigate to **Z:\CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Process Monitoring Tools\ProcessMonitor** and double-click **Procmon.exe** to launch the Process Monitor tool.



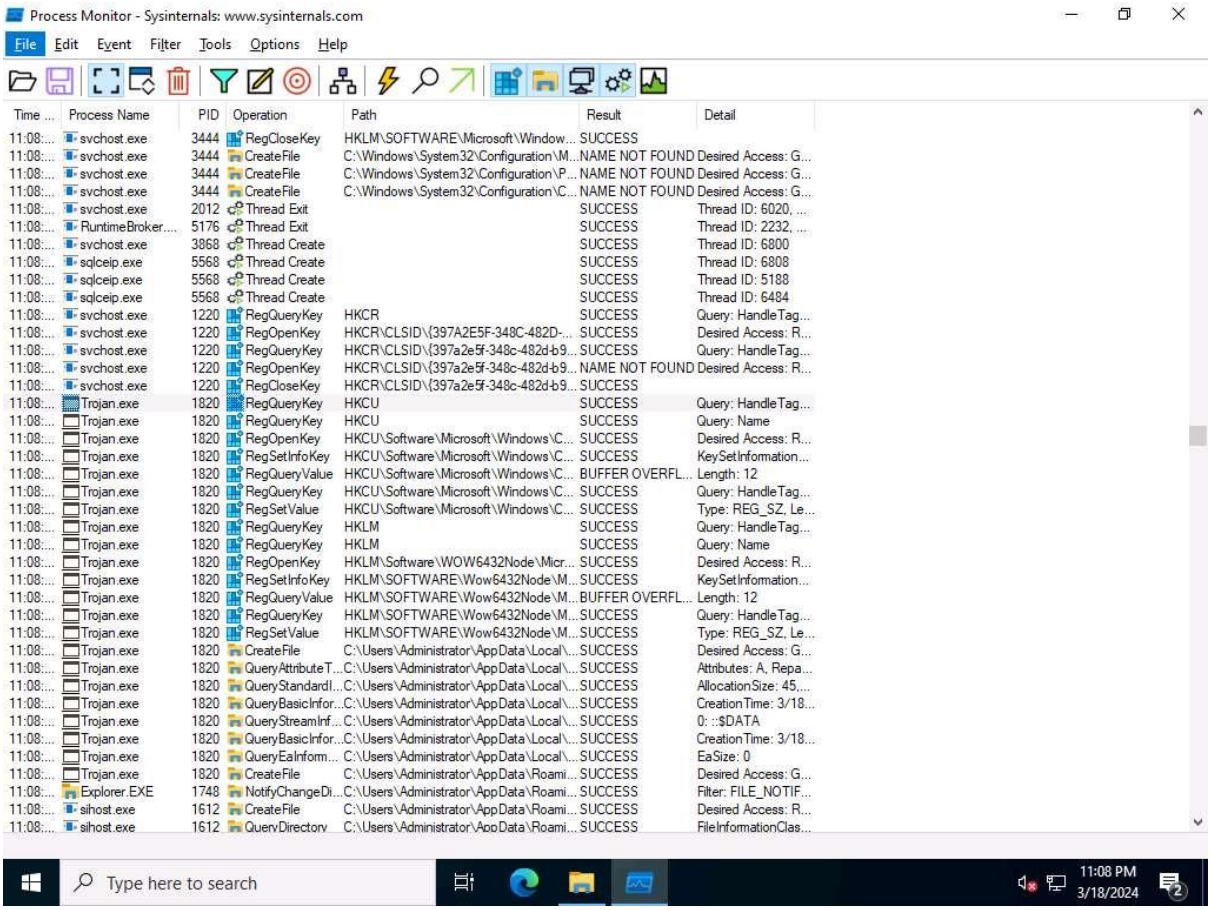
2. The **Process Monitor License Agreement** window appears; click **Agree**.

3. The **Process Monitor** main window appears, as shown in the screenshot, with the processes running on the machine.

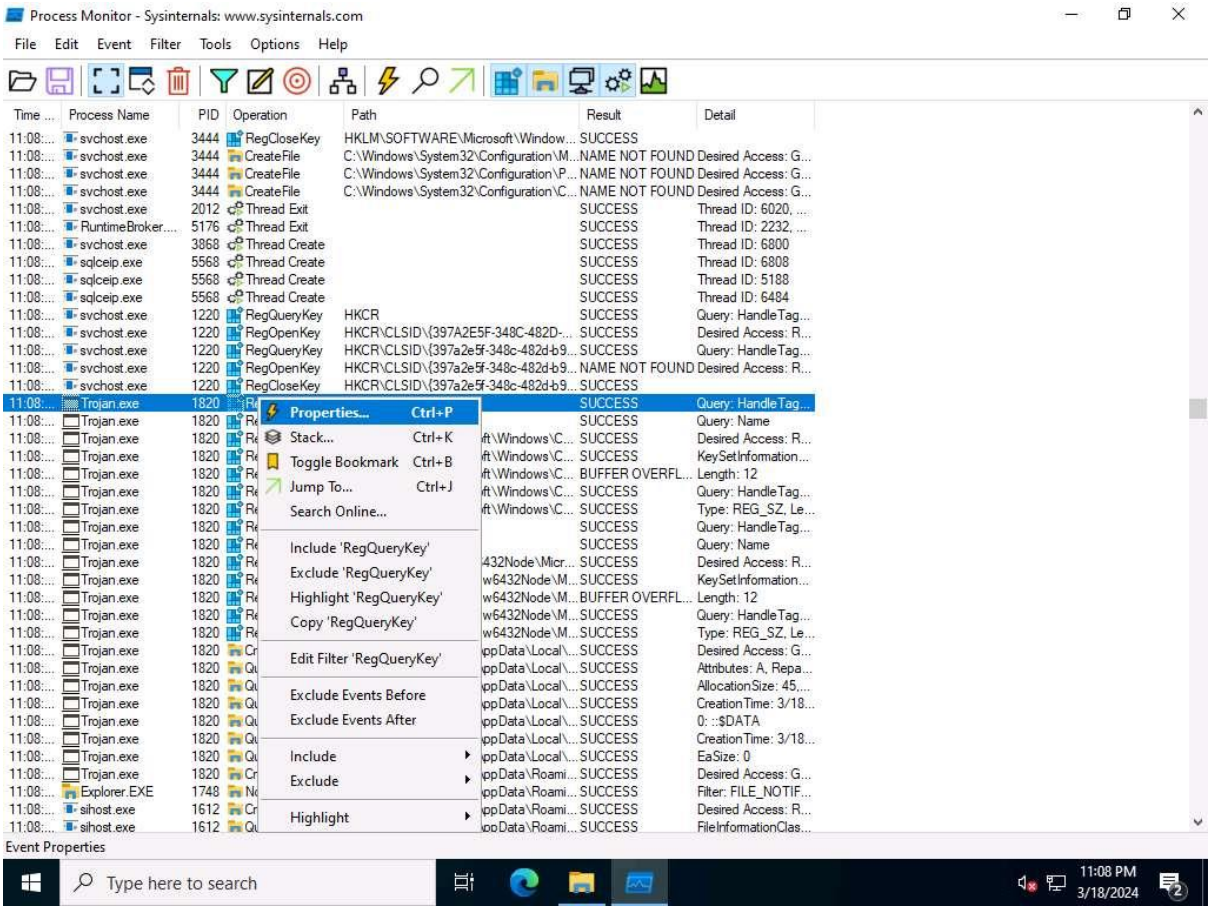


4. Scroll down to look for the **Trojan.exe** process that was executed in the previous task. If you killed the process at the end of the task, then navigate to **Z:\CEHv13 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe** to re-execute the malicious program.

5. Observe that the **Trojan.exe** process is running on the machine. Process Monitor shows the running process details such as the PID, Operation, Path, Result, and Details.

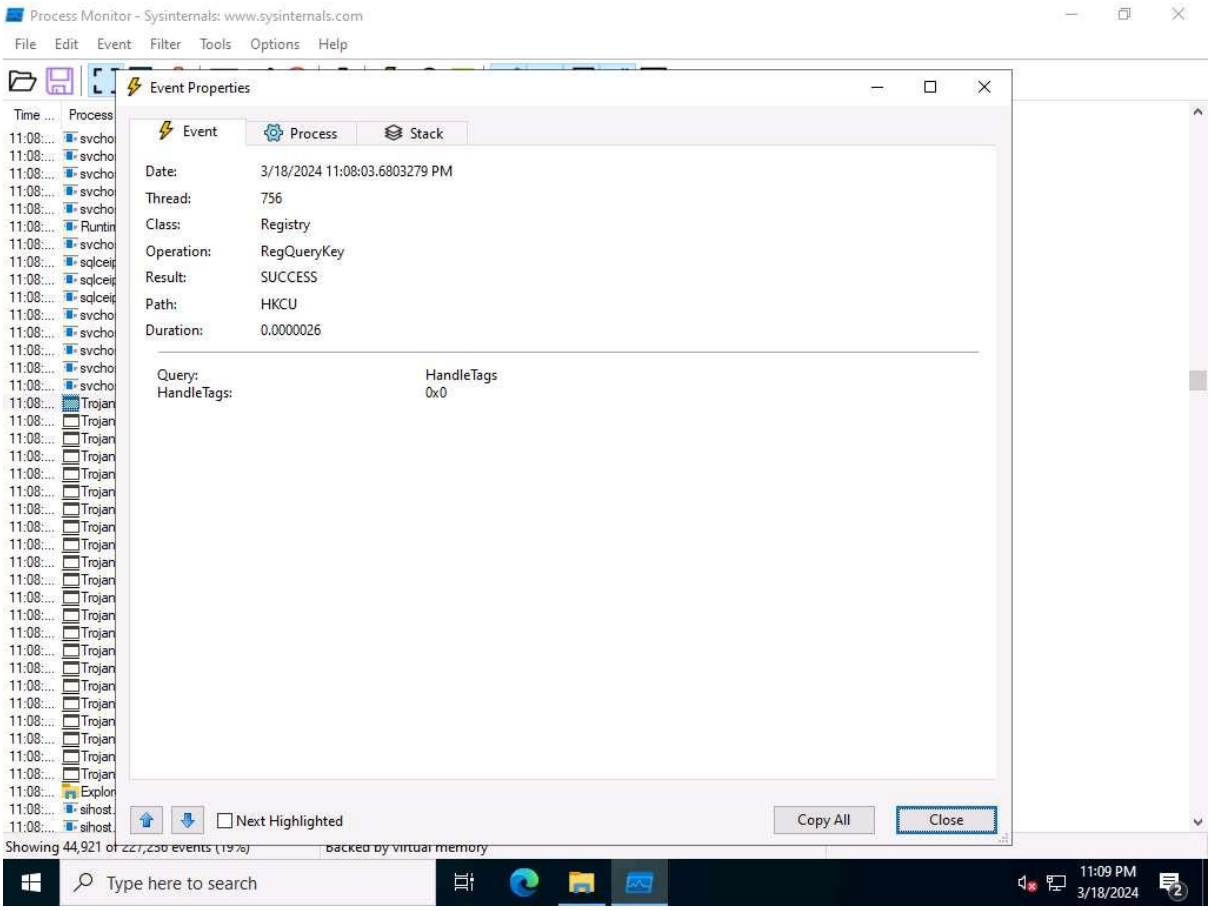


6. To view the properties of a running process, select the process (here, **Trojan.exe**), right-click on the process and select **Properties** from the context menu.



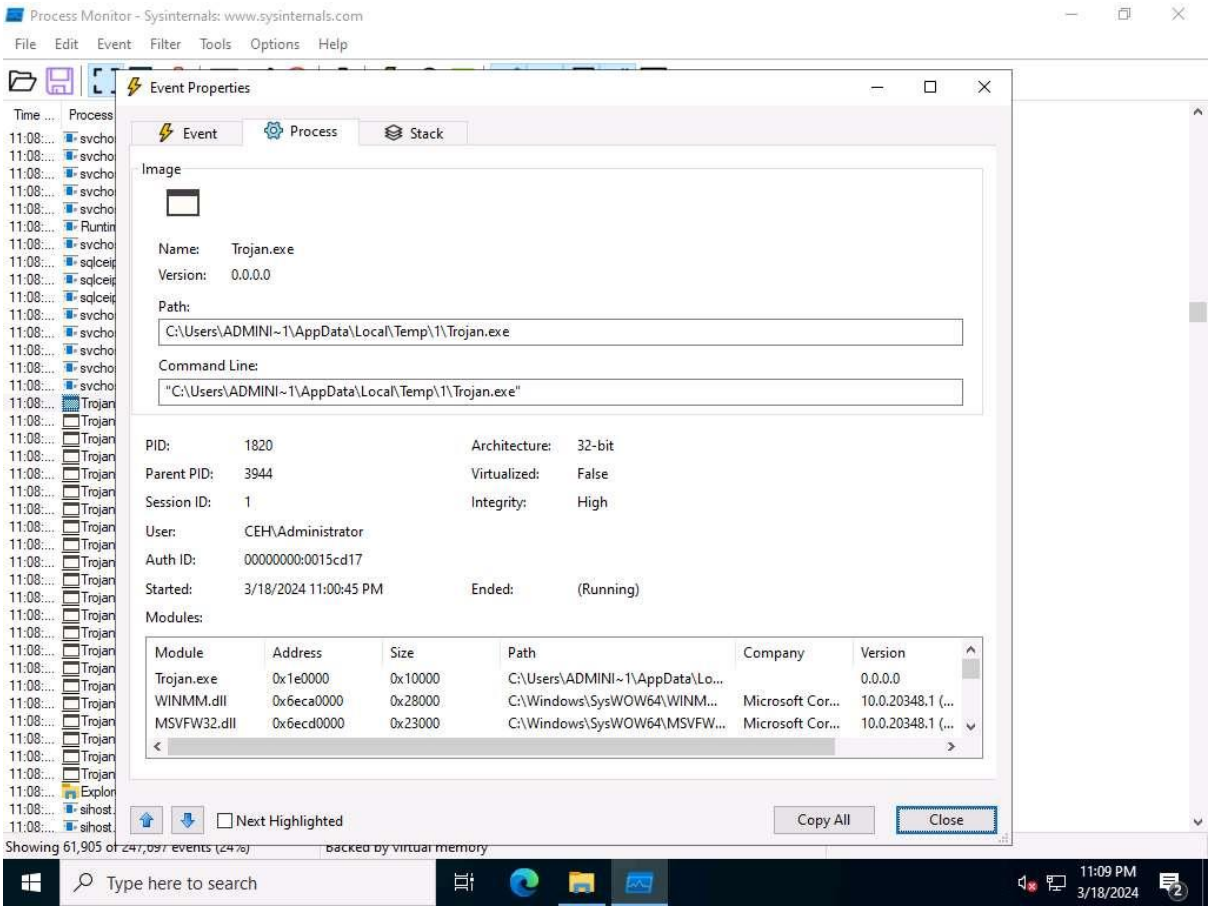
7. The **Event Properties** window appears with the details of the chosen process.

8. In the **Event** tab, you can see the complete details of the running process such as Date, Thread, Class, Operation, Result, Path, and Duration.

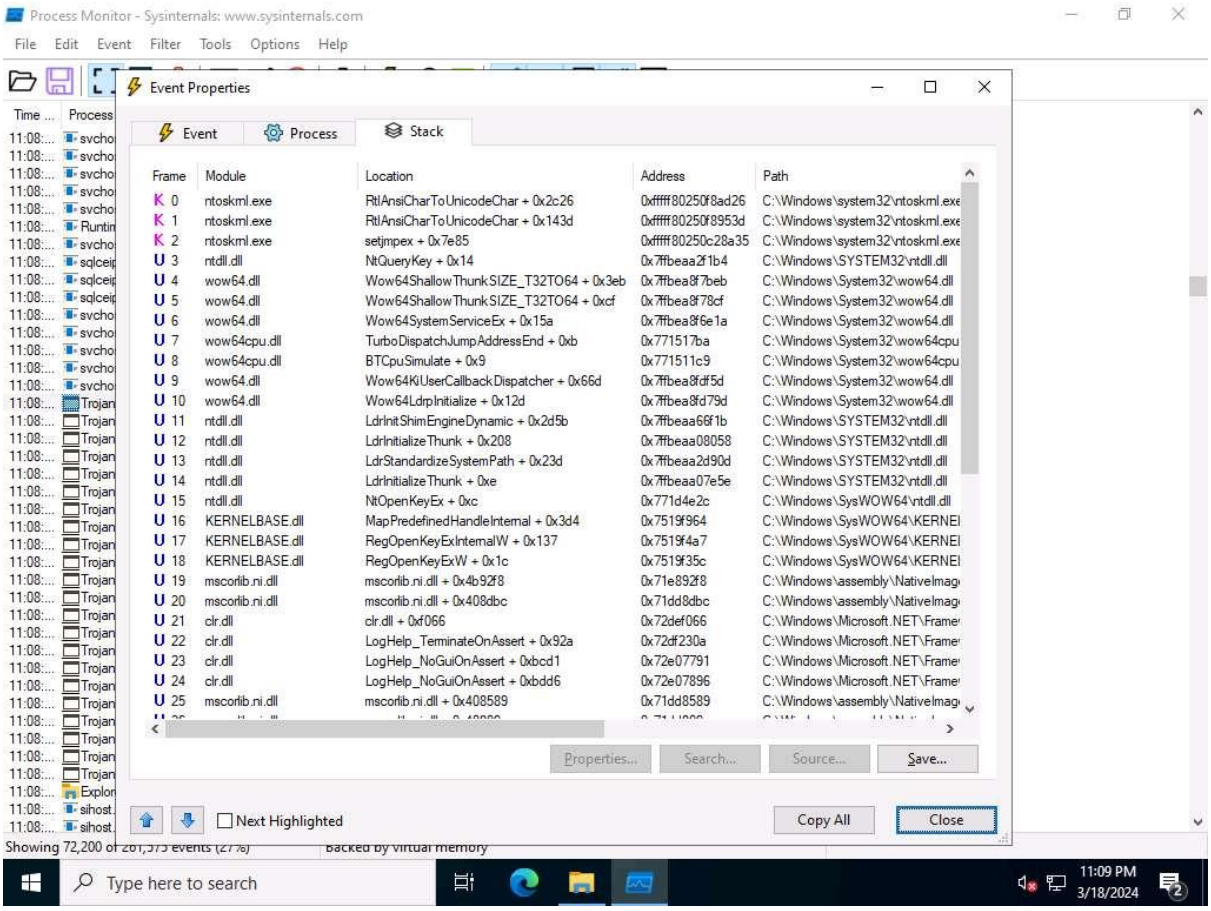


9. Once the analysis is complete, click the **Process** tab.

10. The **Process** tab shows the complete details of the process running, as shown in the screenshot.



11. Click the **Stack** tab to view the supported DLLs of the selected process. Once the analysis is done, click **Close**.



12. This way, you can analyze the processes running on a machine.

13. If a process is found to be suspicious, you may either kill the process or close the port.

14. Close all windows on the **Windows 11** and **Windows Server 2022** machines.

15. You can also use other process monitoring tools such as **Process Explorer** (https://docs.microsoft.com), **OpManager** (https://www.manageengine.com), **Monit** (https://mmonit.com), **ESET SysInspector** (https://www.eset.com), or **System Explorer** (https://systemexplorer.net) to perform process monitoring.

Question 7.4.2.1

Run njRAT from the attacker machine (Windows 11) and gain control over the victim machine (Windows Server 2022). On the Windows Server 2022 machine, use Process Monitor to detect suspicious processes created by the Trojan server. Determine the architecture of the malicious process that is running.