Module 07: Malware Threats

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.

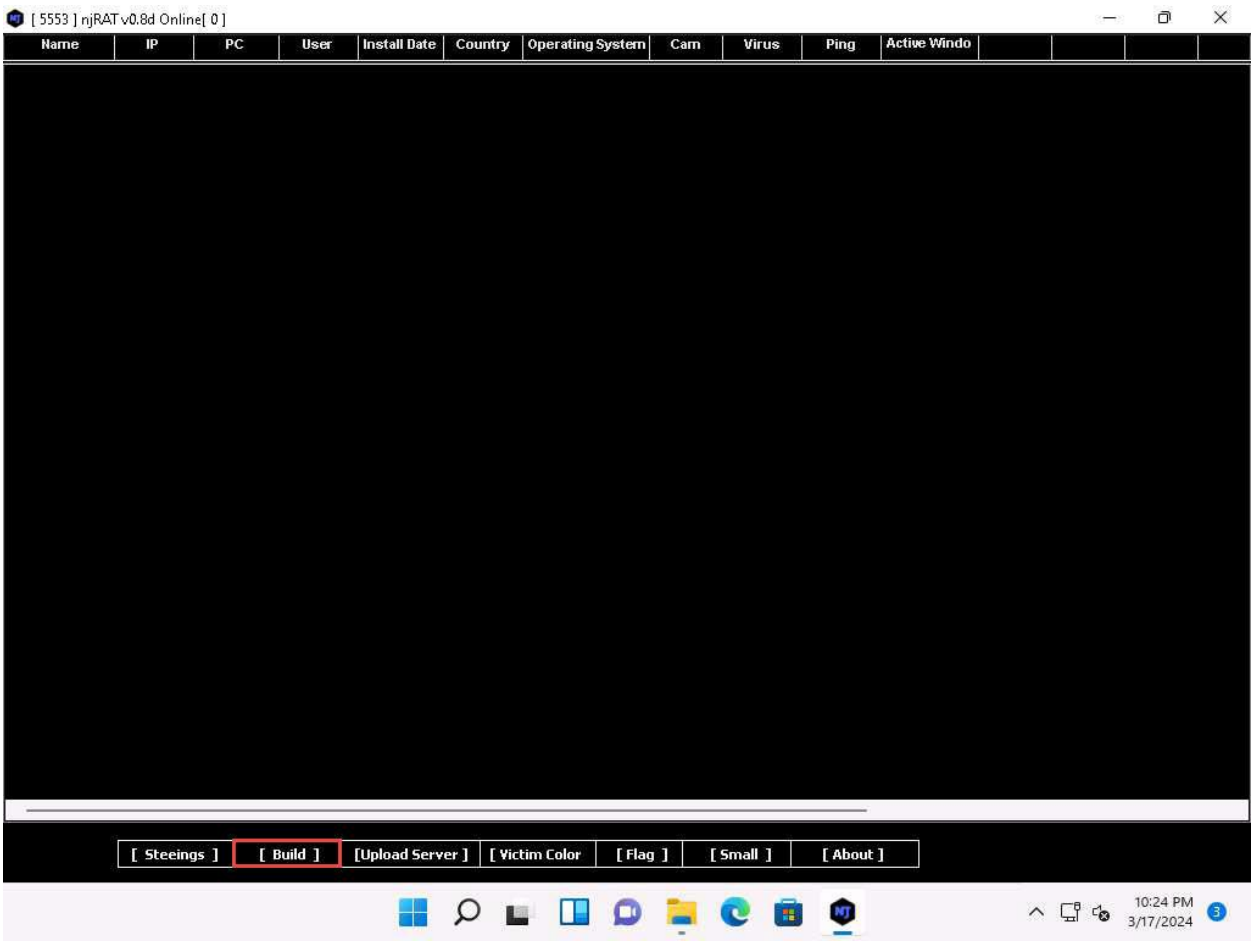
Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

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**.

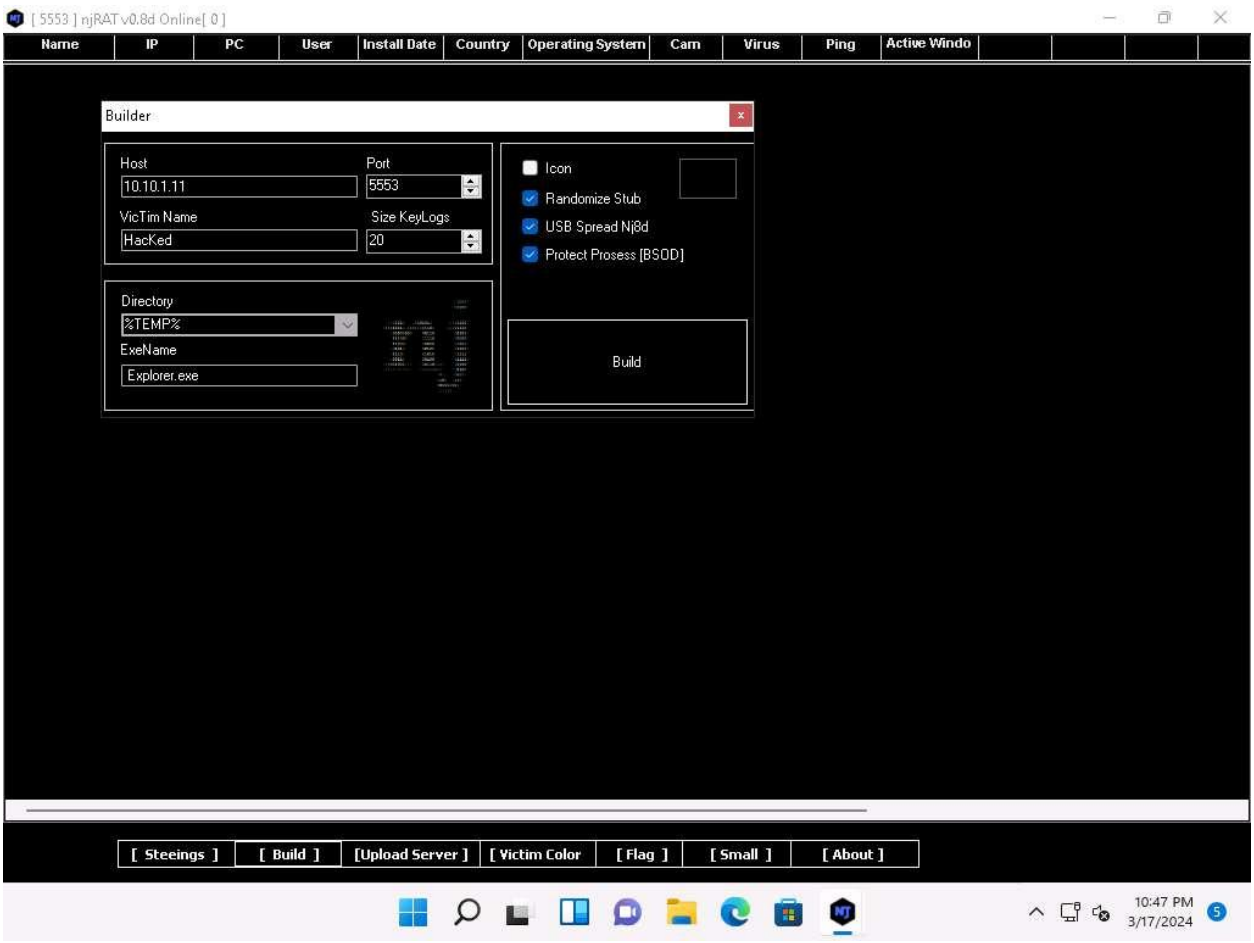
If an **Open File - Security Warning** pop-up appears, click **Run**.

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.

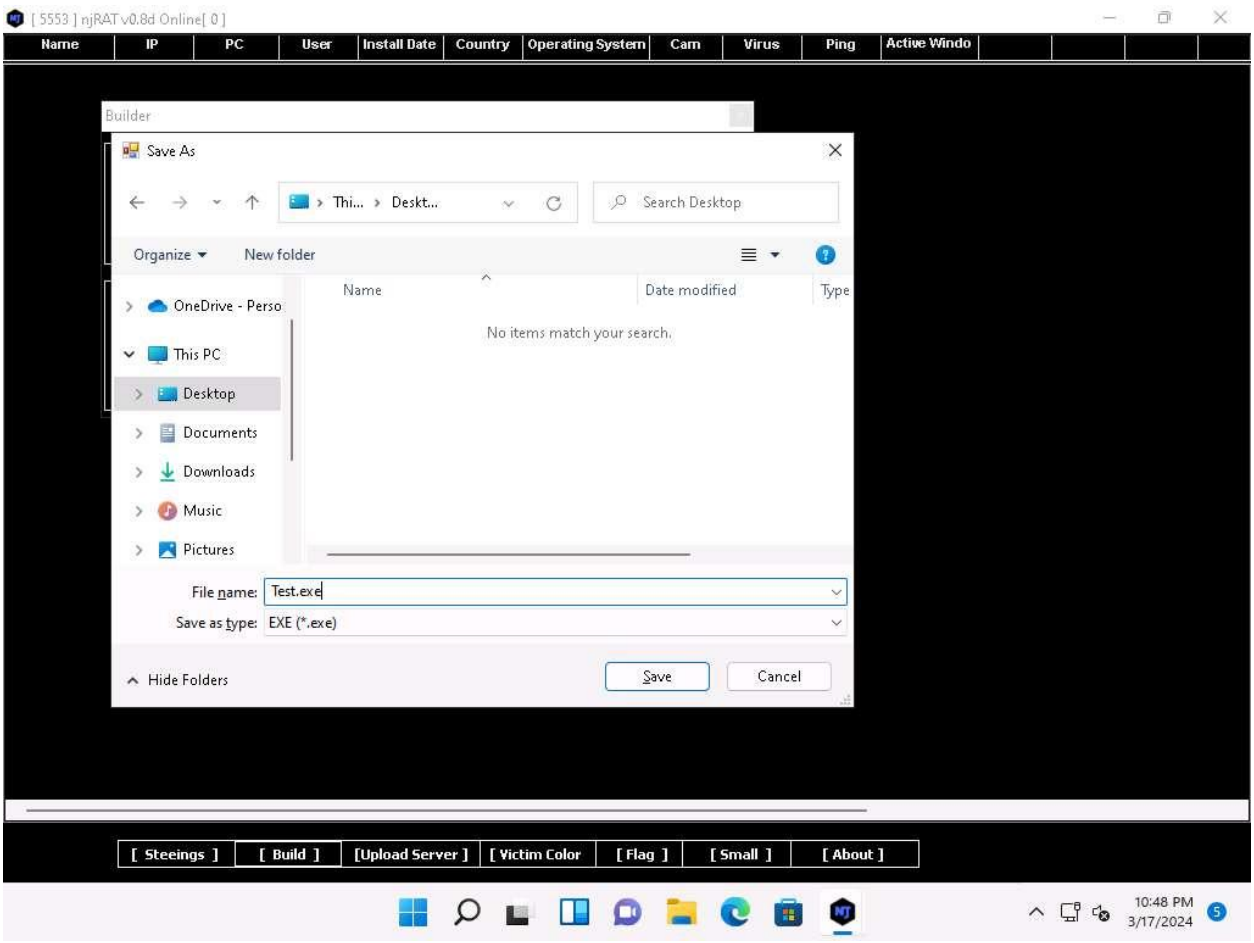


5. The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, check the options **Randomize Stub**, **USB Spread Nj8d, Protect Prosess [BSOD]**, leave the other settings to default, and click **Build**.

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**.

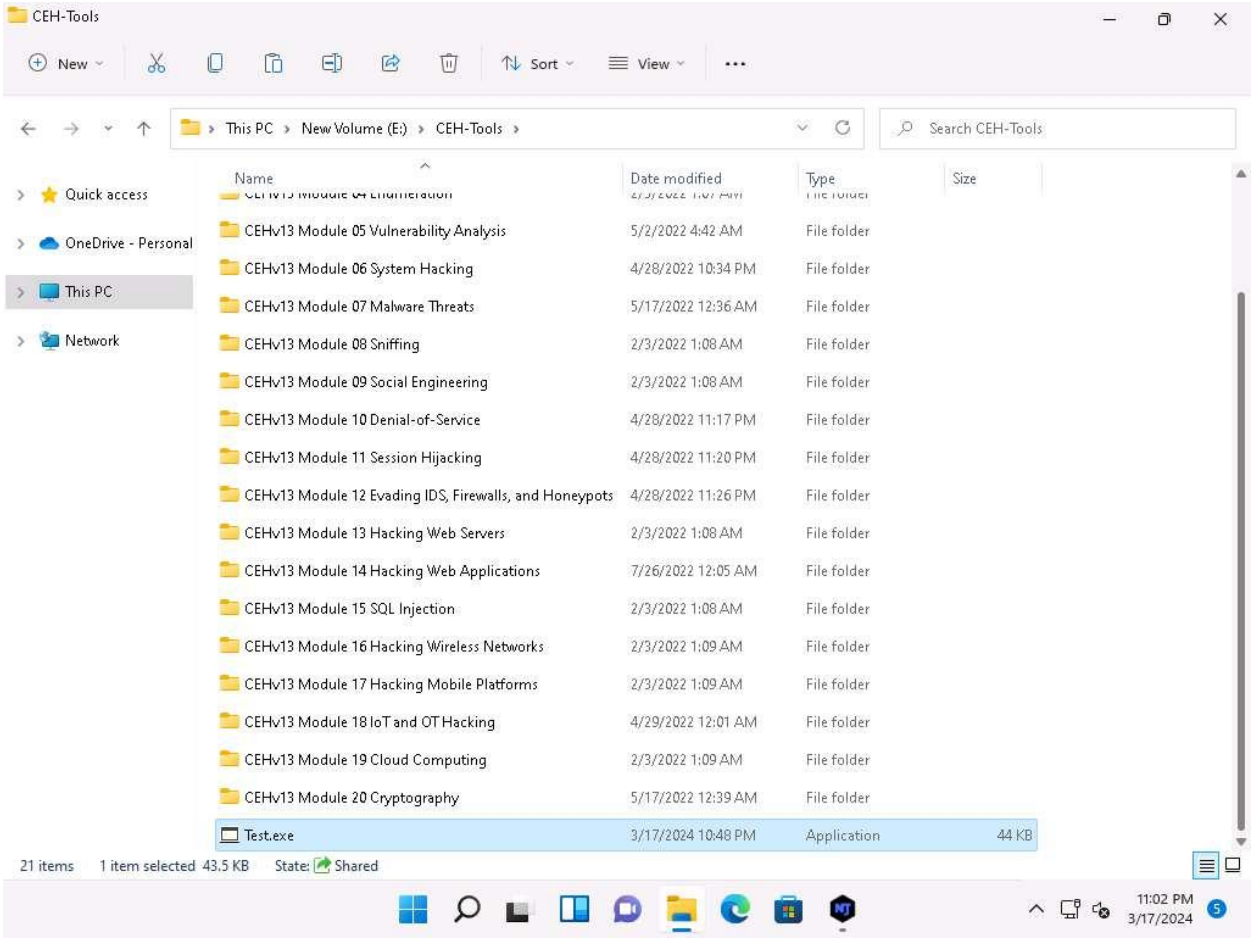


8. Once the server is created, the **Doen Successfully!** pop-up appears; click **OK**.

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).

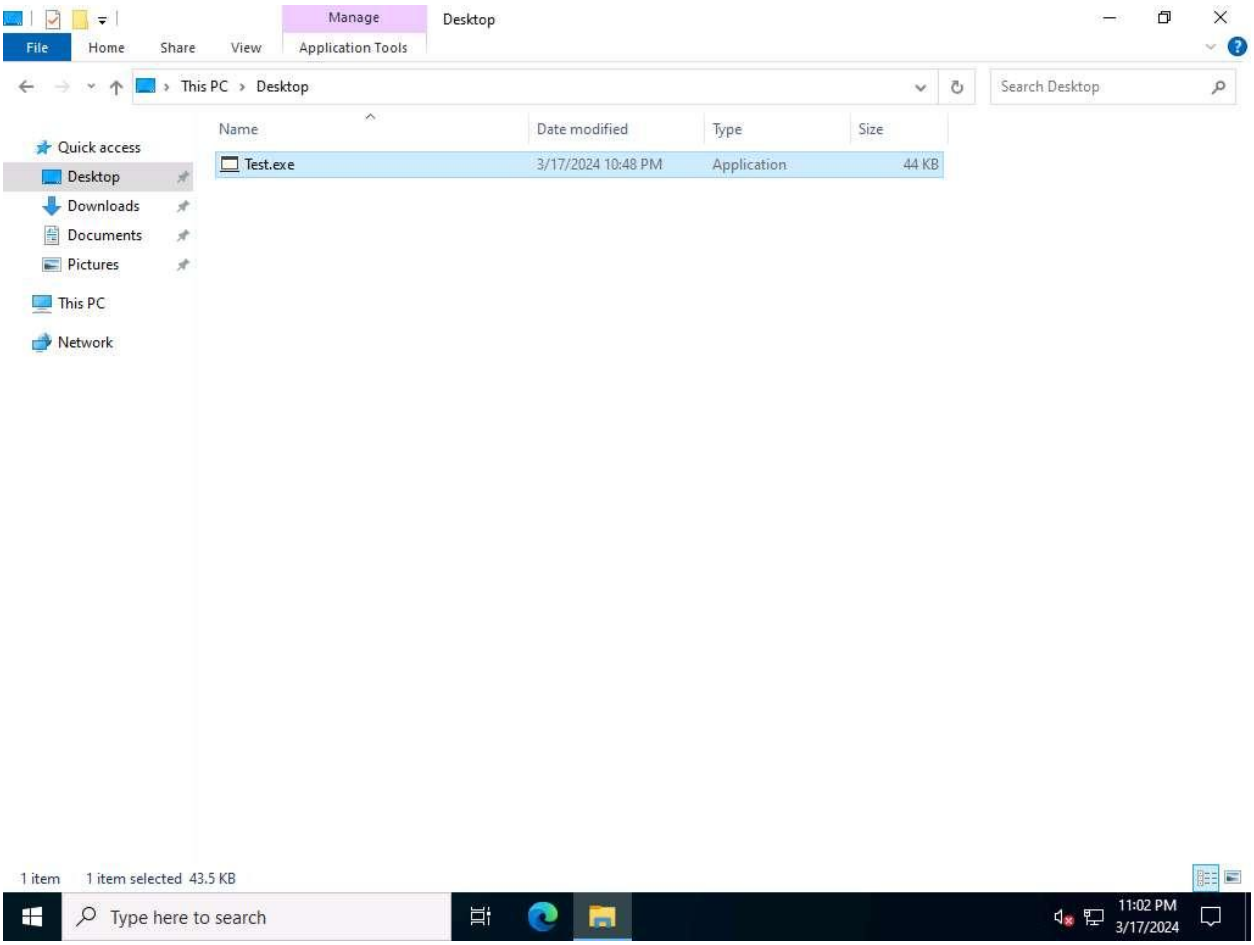
In this task, we copied the **Test.exe** file to the shared network location (**CEH-Tools**) to share the file.



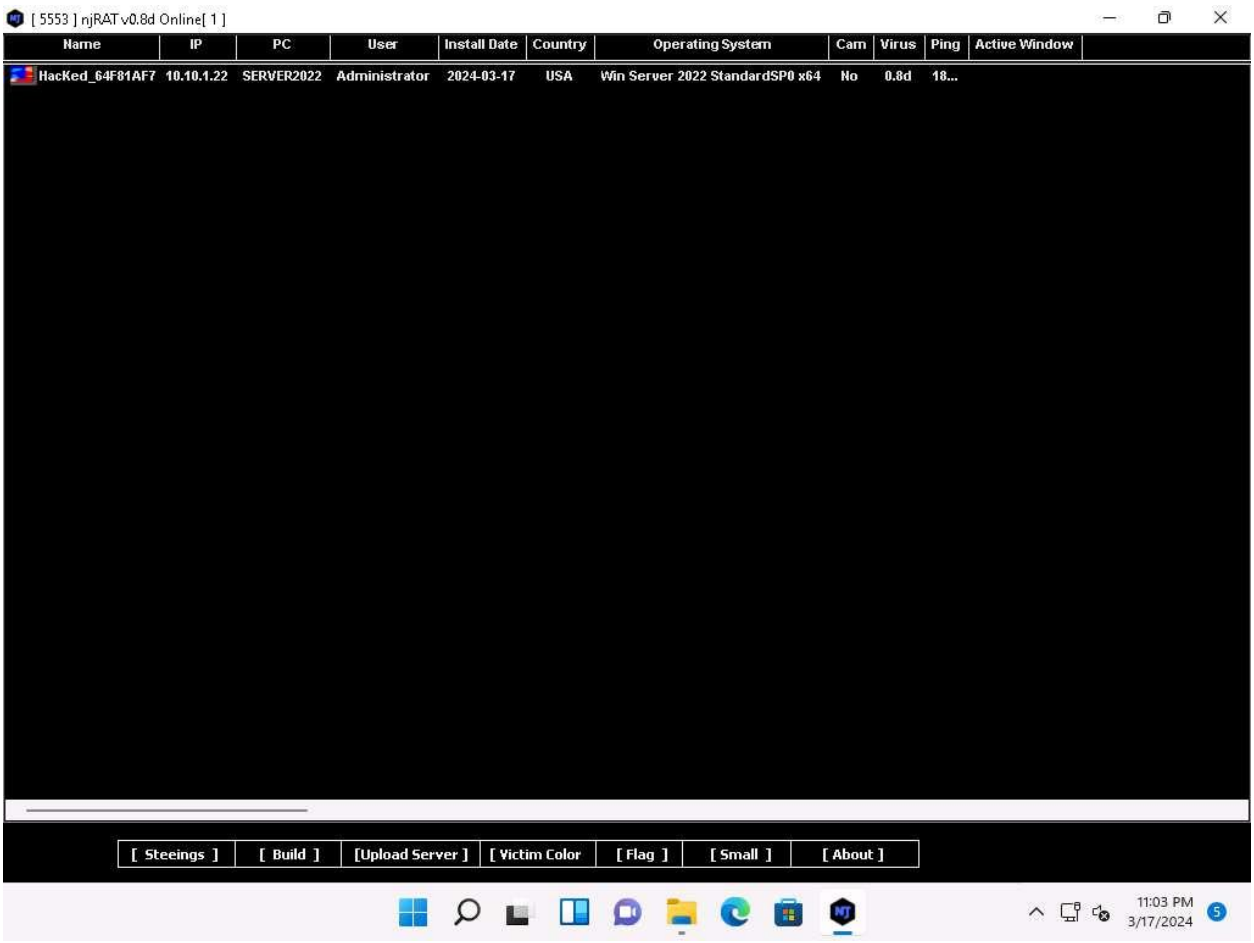
10. Click Windows Server 2022 to switch to the **Windows Server 2022** machine.
    Click Ctrl+Alt+Delete to activate the machine, login with **CEH\Administrator/Pa$$w0rd**.

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

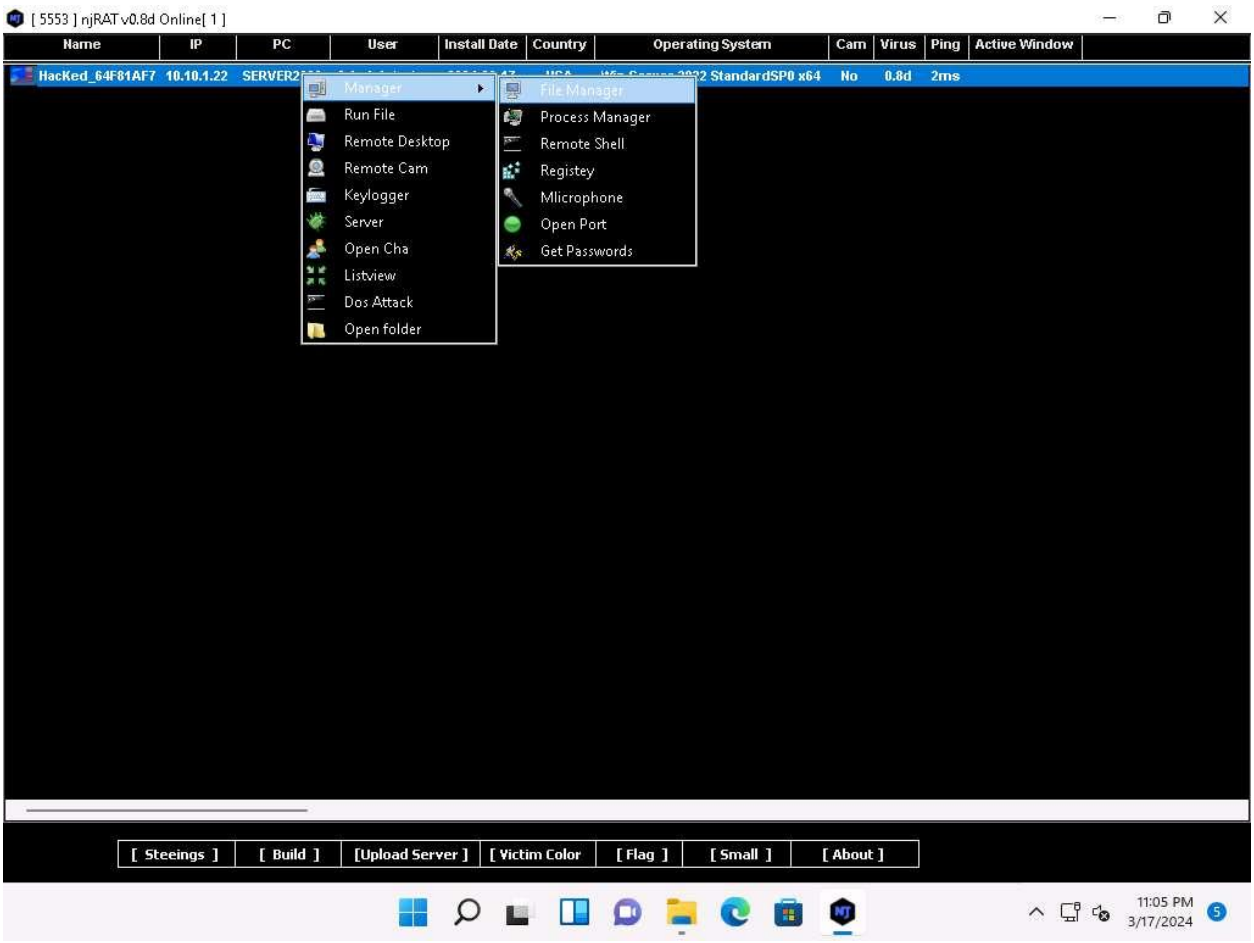
11. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**Test.exe**) onto the **Desktop** of **Windows Server 2022**.
12. Here, you are acting both as an **attacker** who logs into the **Windows 11** machine to create a malicious server, and 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.



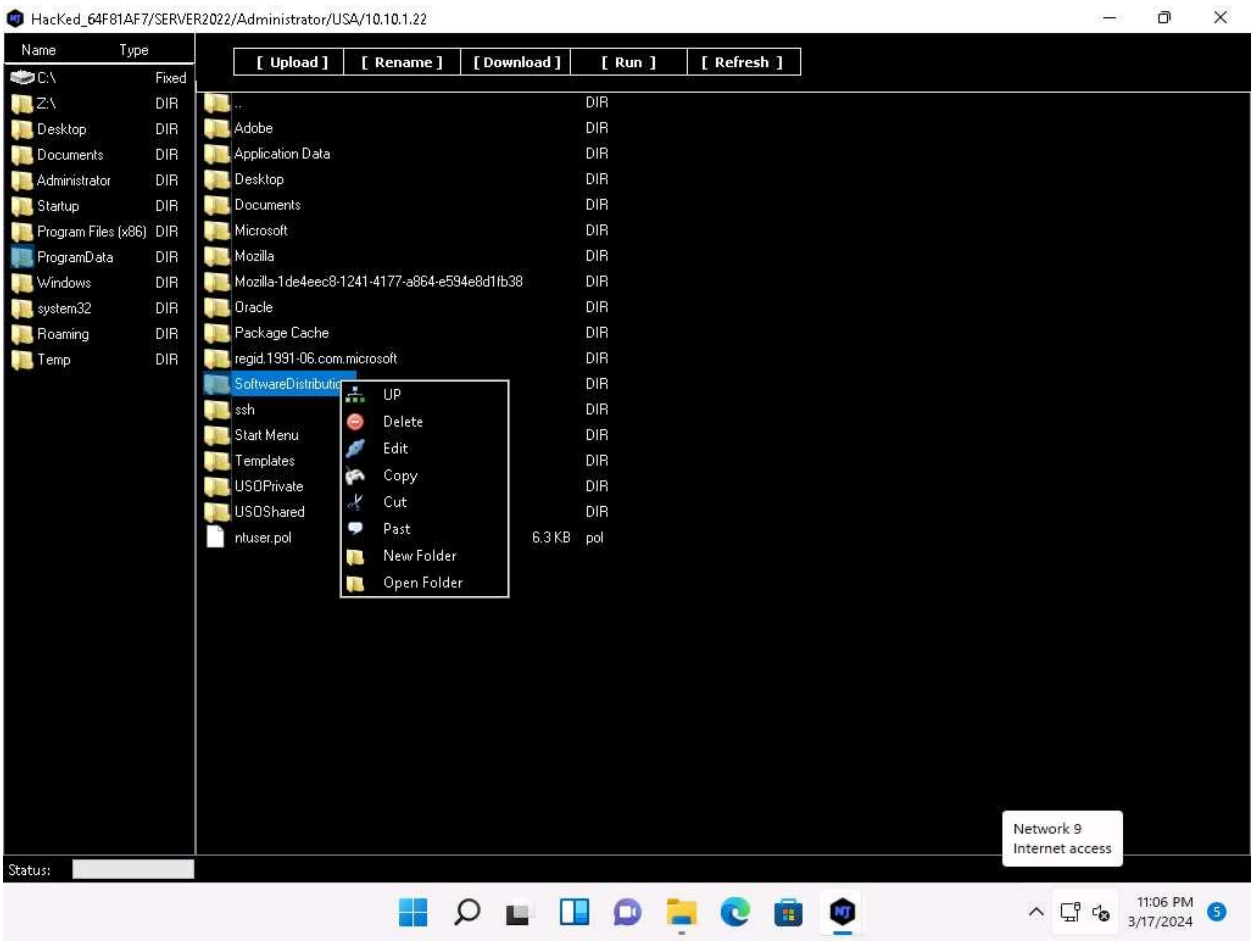
14. Click Windows 11 to switch back to the **Windows 11** machine. Maximize njRAT GUI window. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in **Windows 11** establishes a persistent connection with the victim machine,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

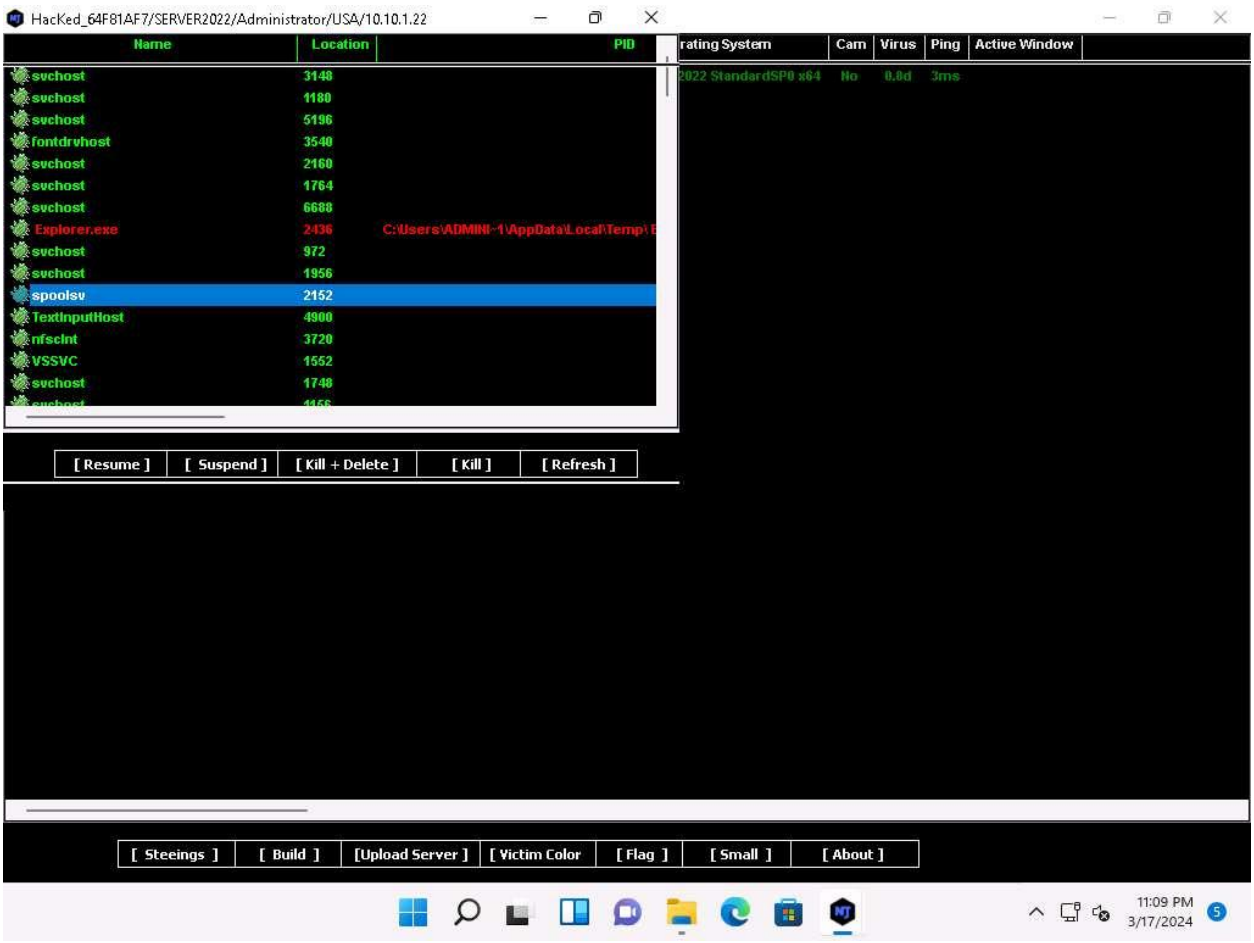


18. The **File Manager** window appears. Double-click any directory in the left pane (here, **ProgramData**); all its associated files and directories are displayed in the right pane. You can right-click a selected directory and manipulate it using the contextual options. Close the **File Manager** window.

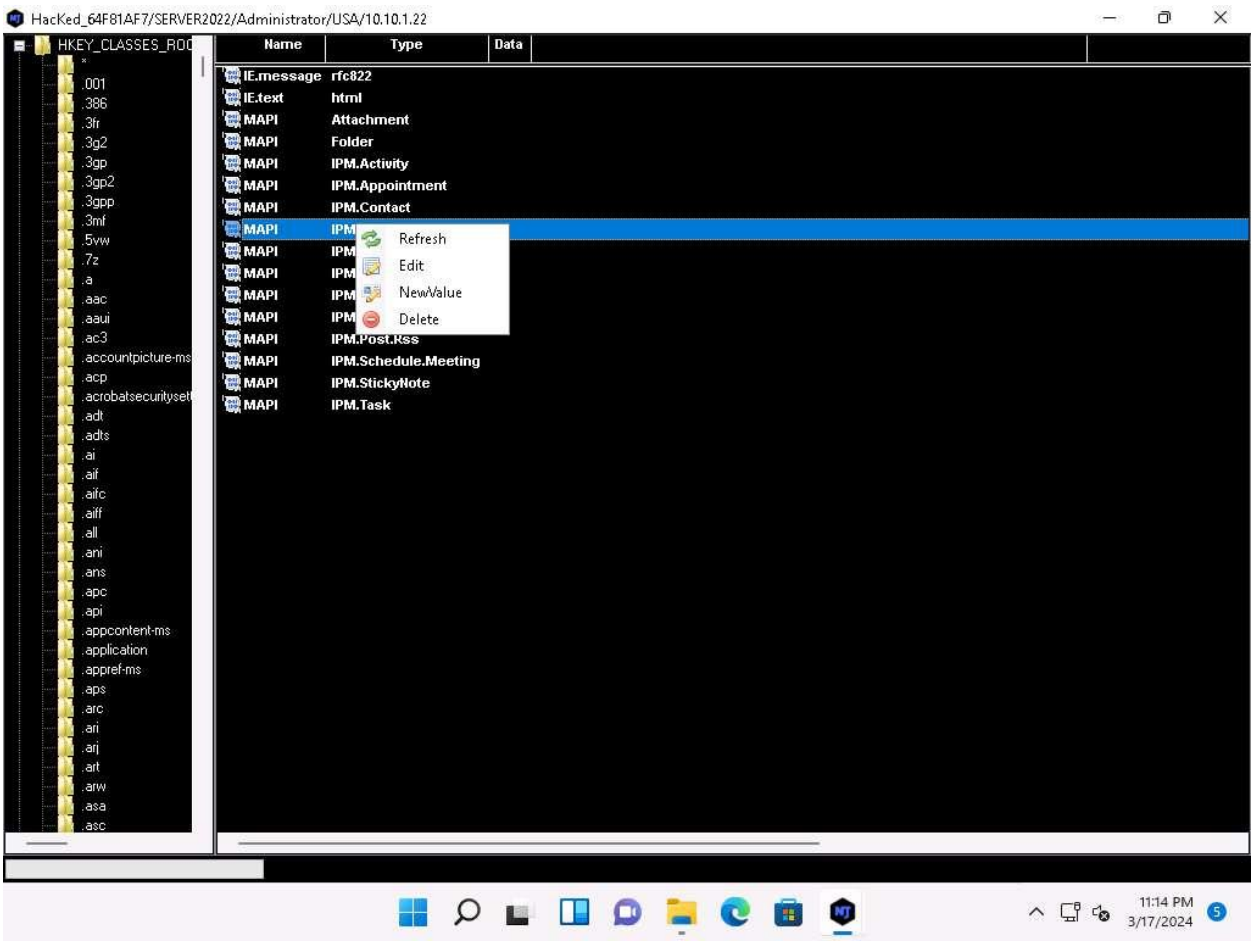


19. Right-click on the detected victim name and click hover the cursor over **Manager** and click **Process Manager** from context menu.

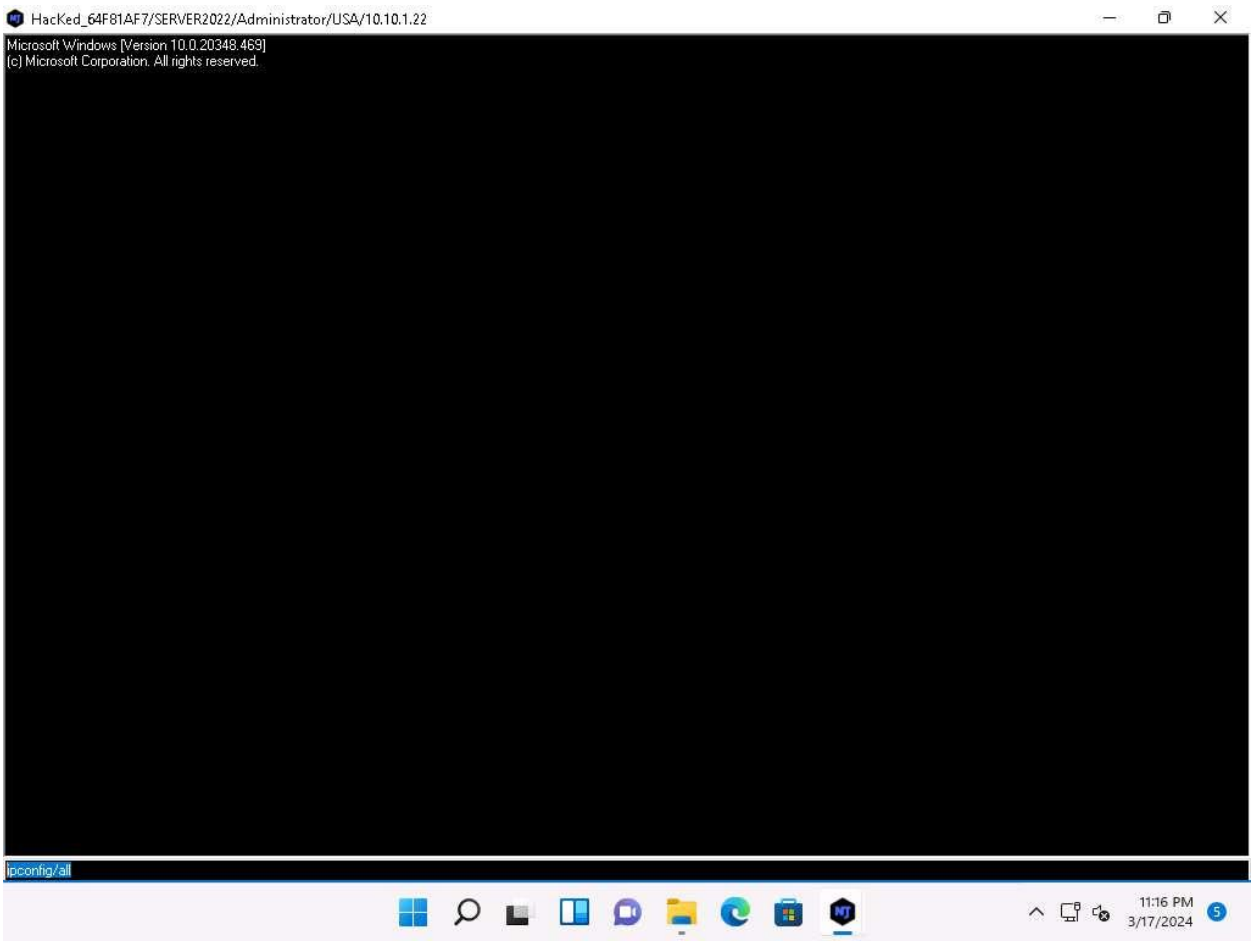
20. You will be redirected to the Process Manager, where you can click on a selected process and perform actions such as **Suspend**, **Kill + Delete**, **Kill**, and **Refresh**.



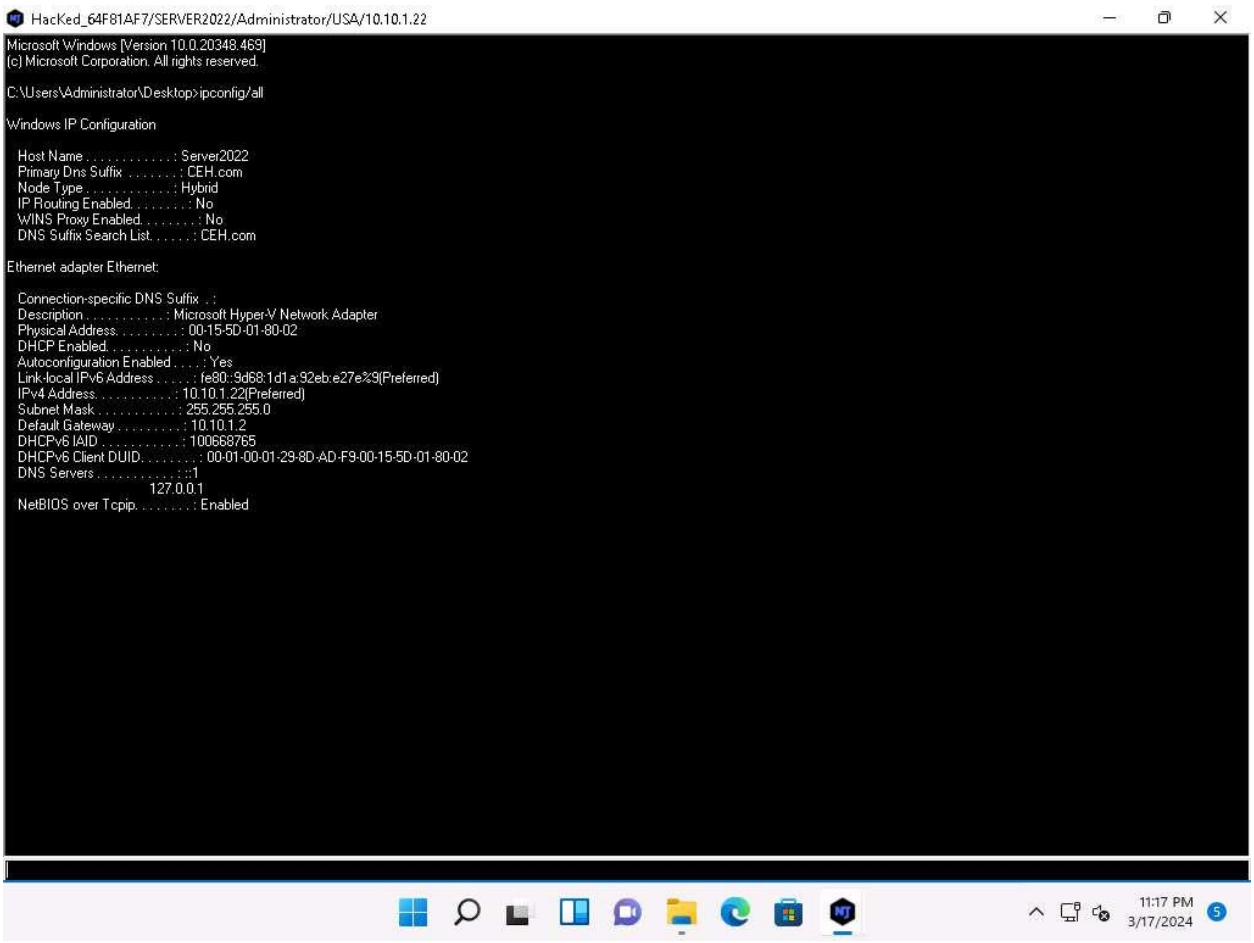
21. Close the **Process Manager** window.
22. Right-click on the detected victim name and click hover the cursor over **Manager** and click **Registey** from context menu.
23. Window showing the registries folders will be opened, choose a registry directory from the left pane, and right-click on its associated registry files.
24. A few options appear for the files; you can use these to manipulate them. Close the window displaying Registry folders.



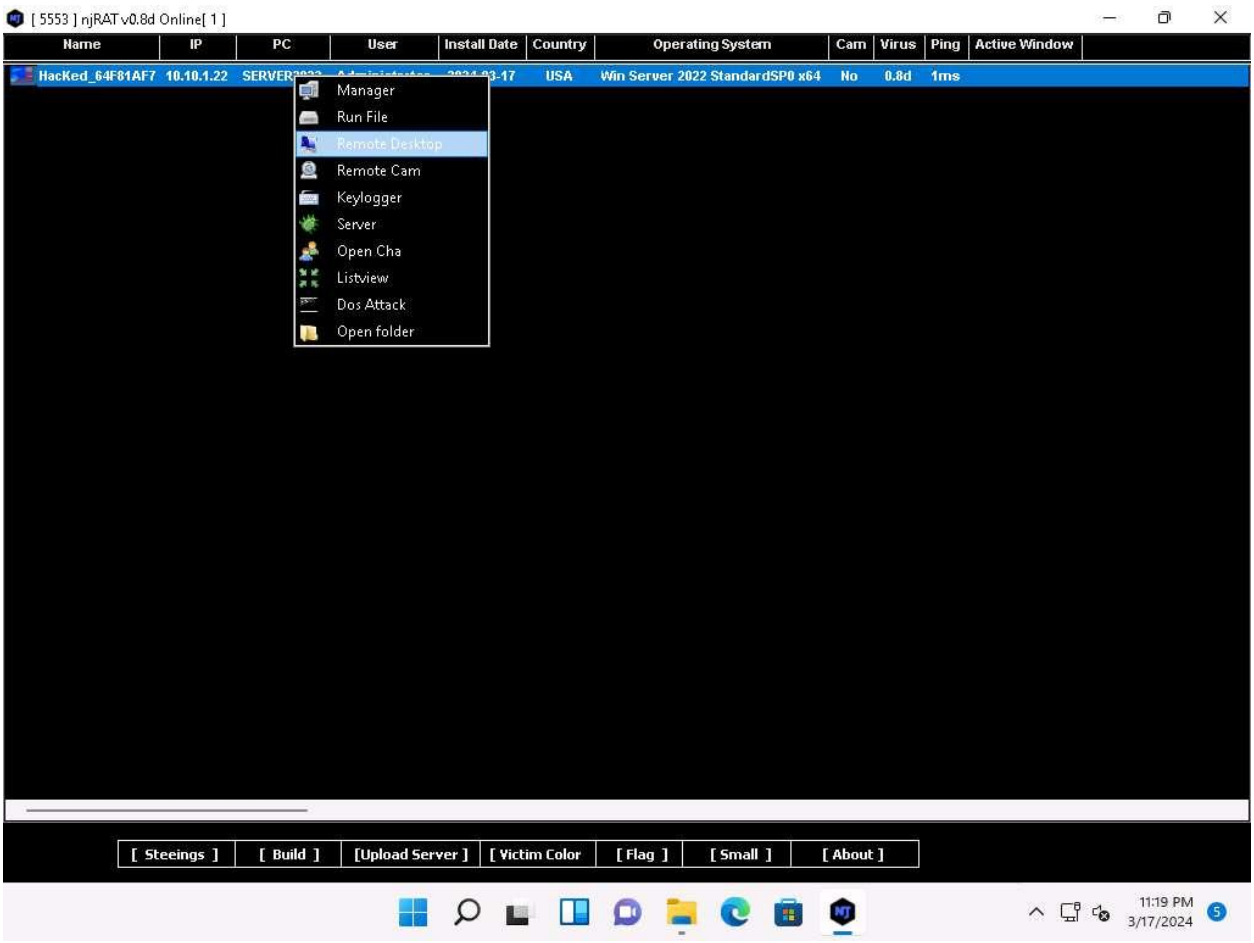
25. Right-click on the detected victim name and hover the cursor over **Manager** and click **Remote Shell** from context menu.
26. This launches a remote command prompt for the victim machine (**Windows Server 2022**).
27. In the text field present in the lower section of the window, type the command **ipconfig/all** and press **Enter**.



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



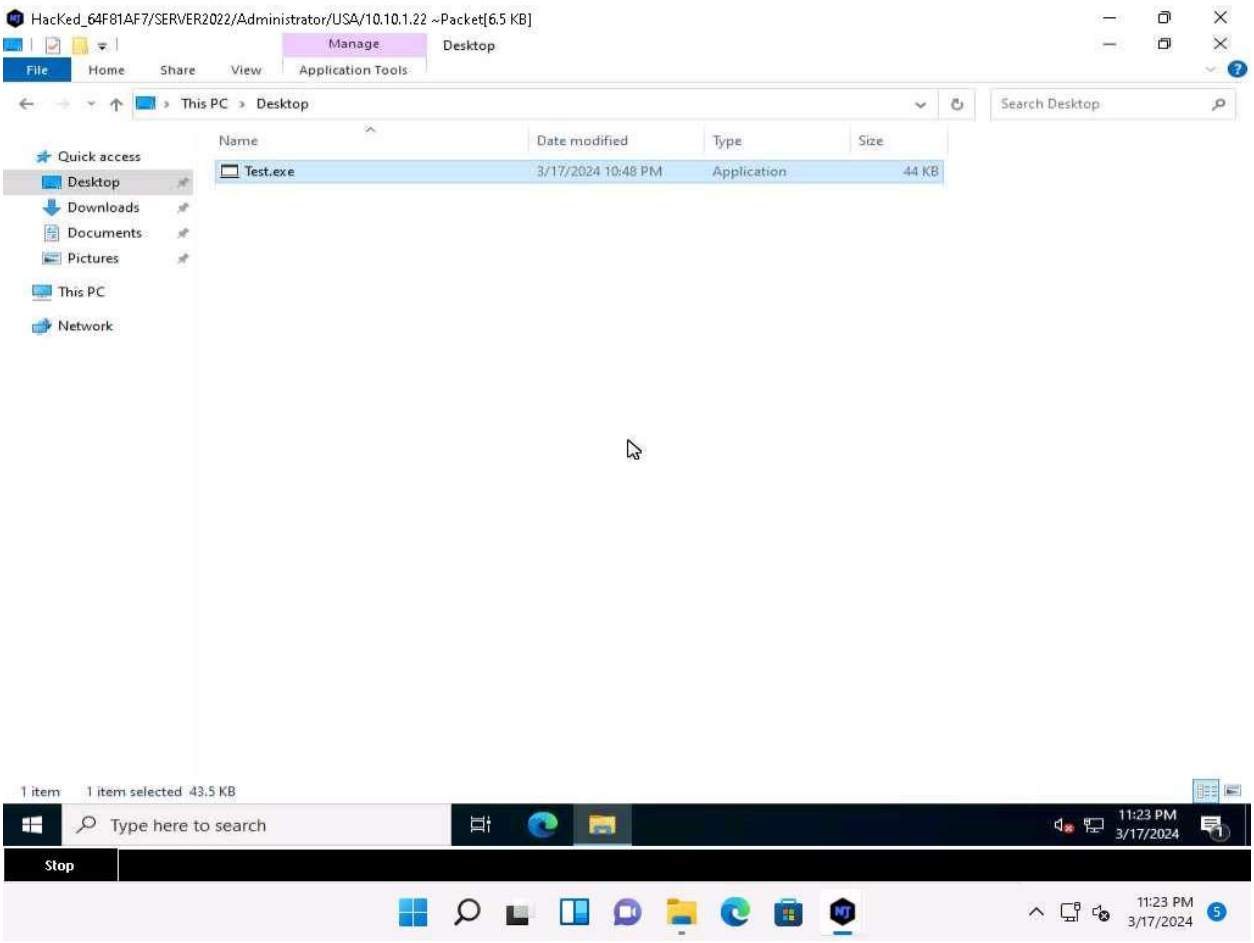
29. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine. Close the **Remote Shell** window.
30. Right-click on the victim name, and then select **Remote Desktop**.



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.

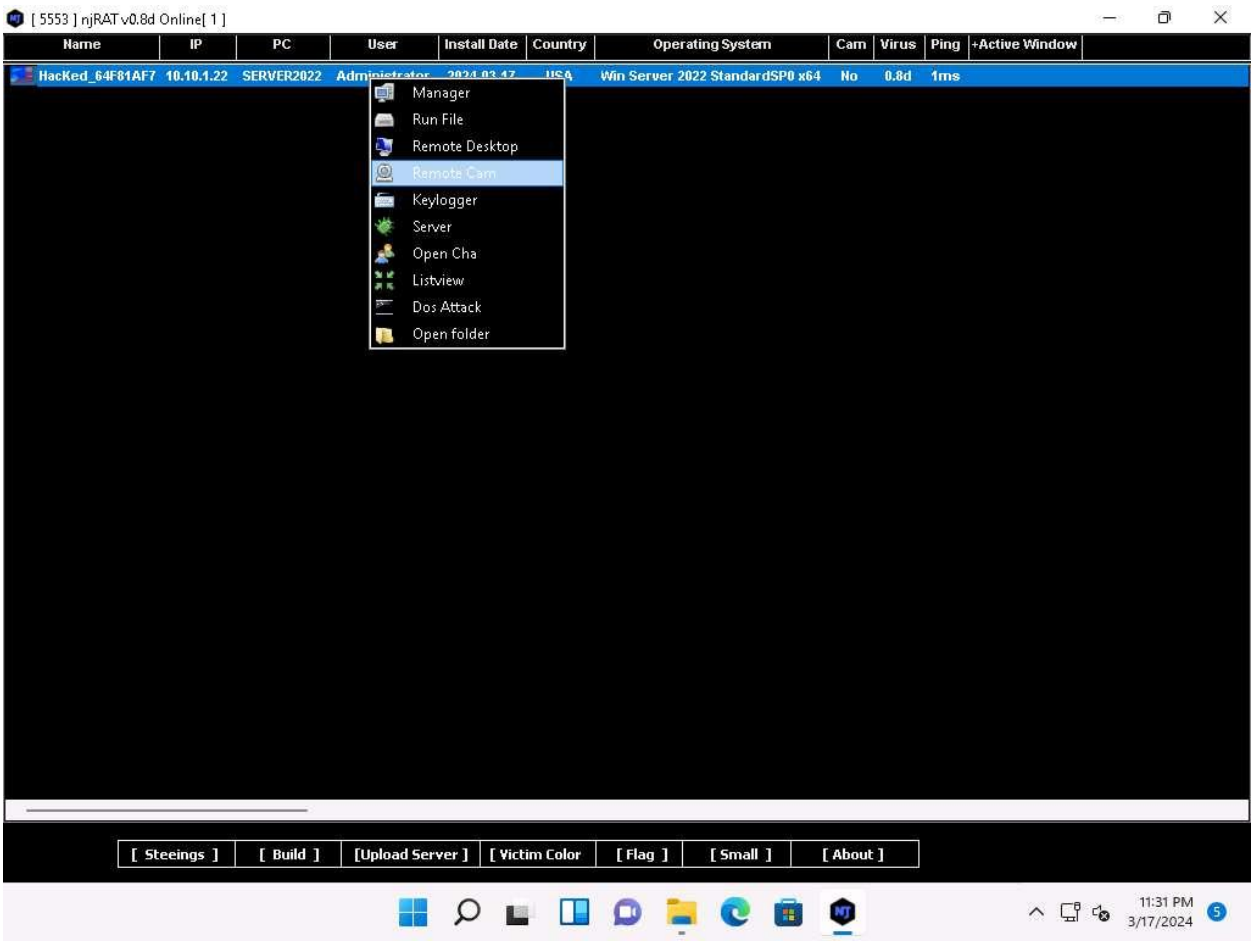
32. A remote desktop window appears.



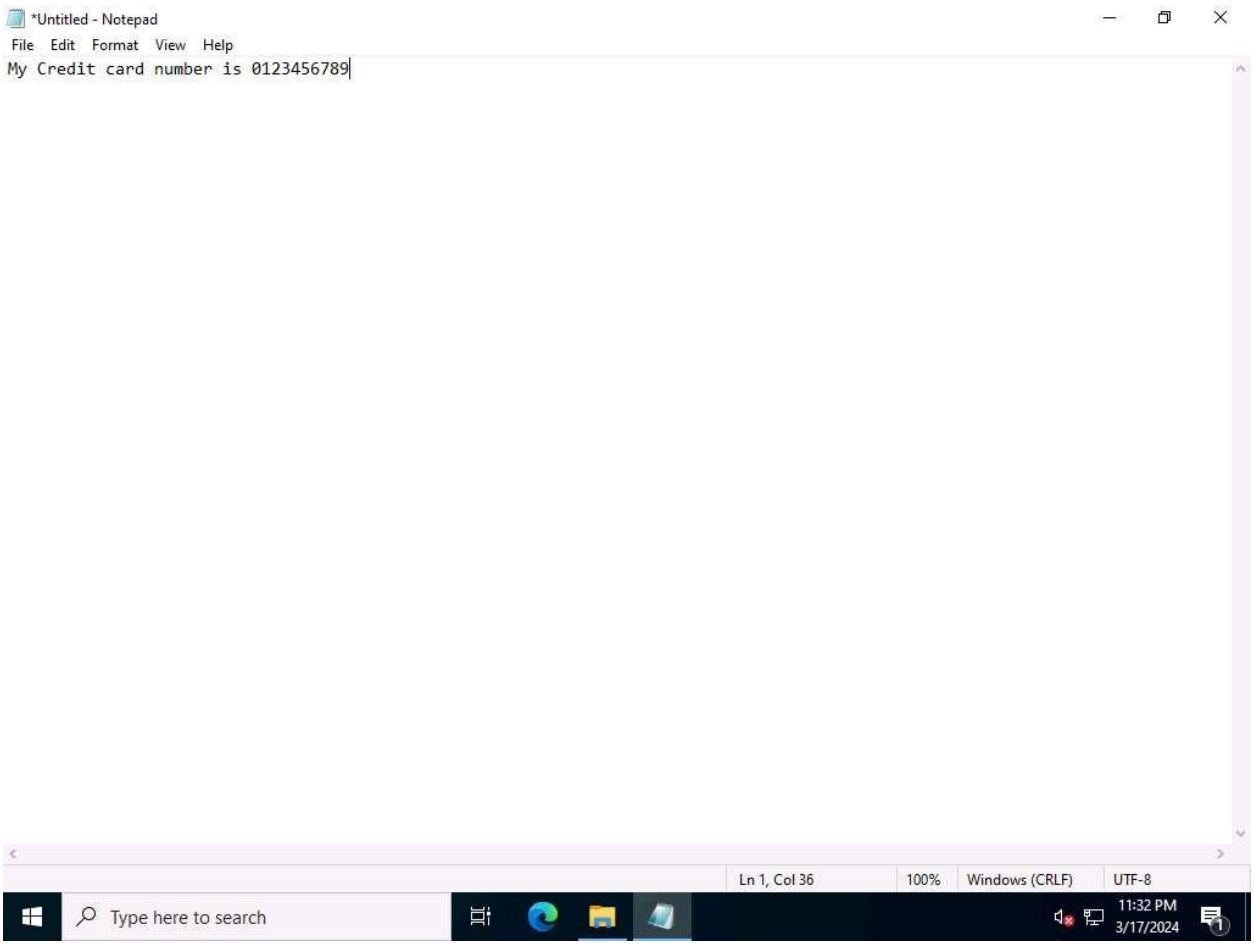
33. Now, you will be able to remotely spy the activities performed on the victim machine.
34. On completing the task, close the **Remote Desktop** window.

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.

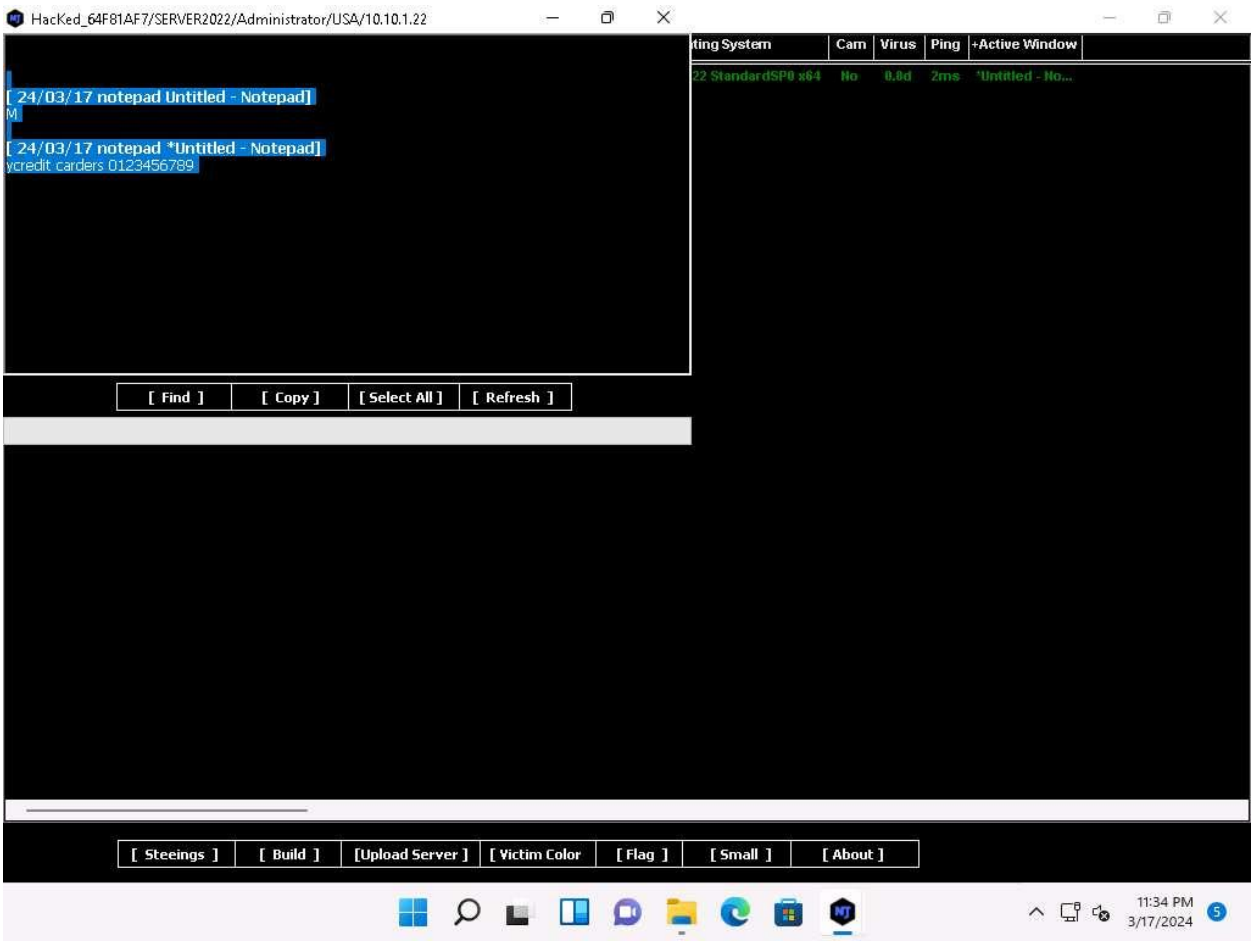


36. Click Windows Server 2022 to switch to the **Windows Server 2022** machine. Assume that you are a legitimate user and perform a few activities such as logging into any website or typing some text in text documents.

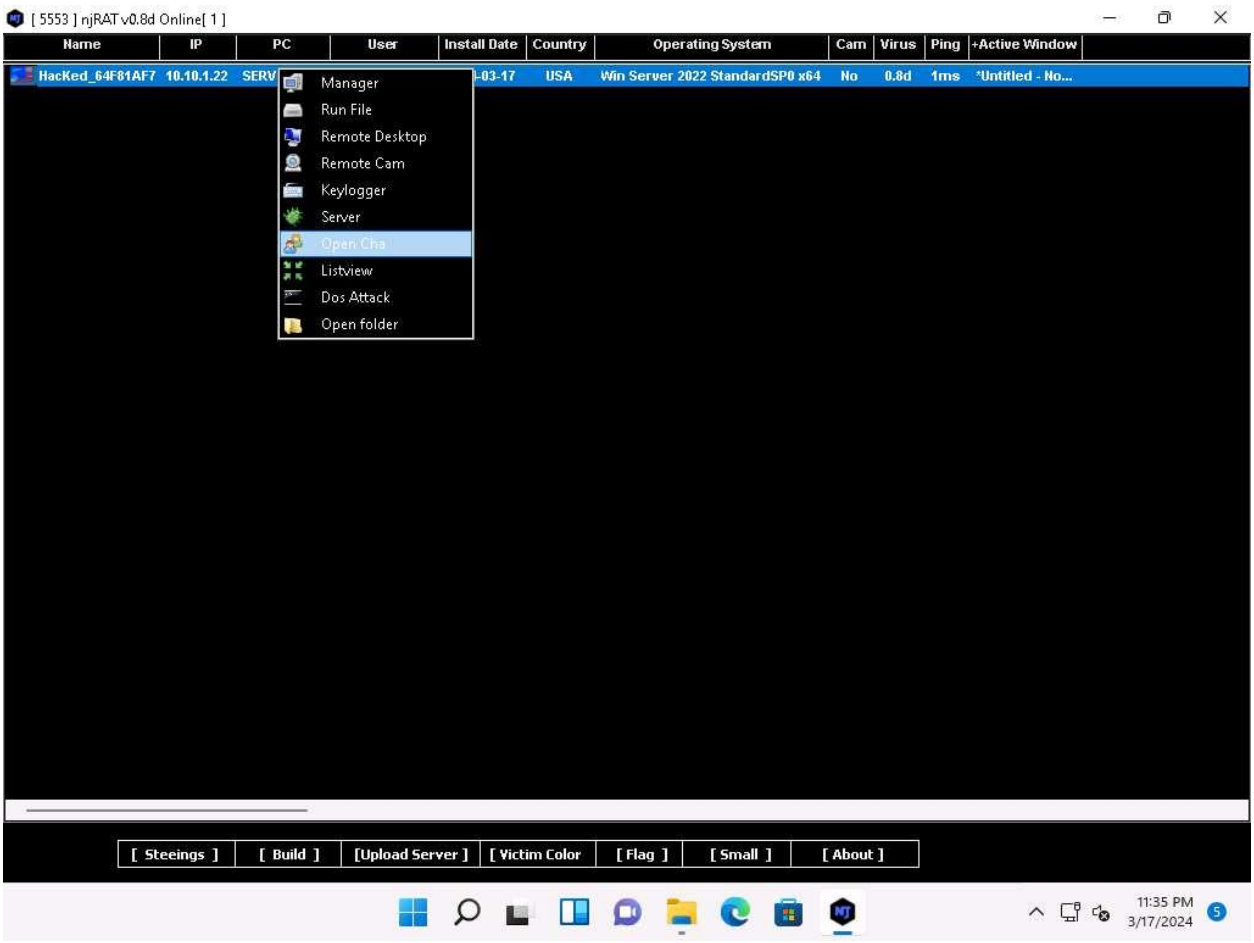


37. Click Windows 11 to switch back to the **Windows 11** machine, right-click on the victim name, and click **Keylogger**.
38. The Keylogger window appears; wait for the window to load.
39. The window displays all the keystrokes performed by the victim on the **Windows Server 2022** machine, as shown in the screenshot.

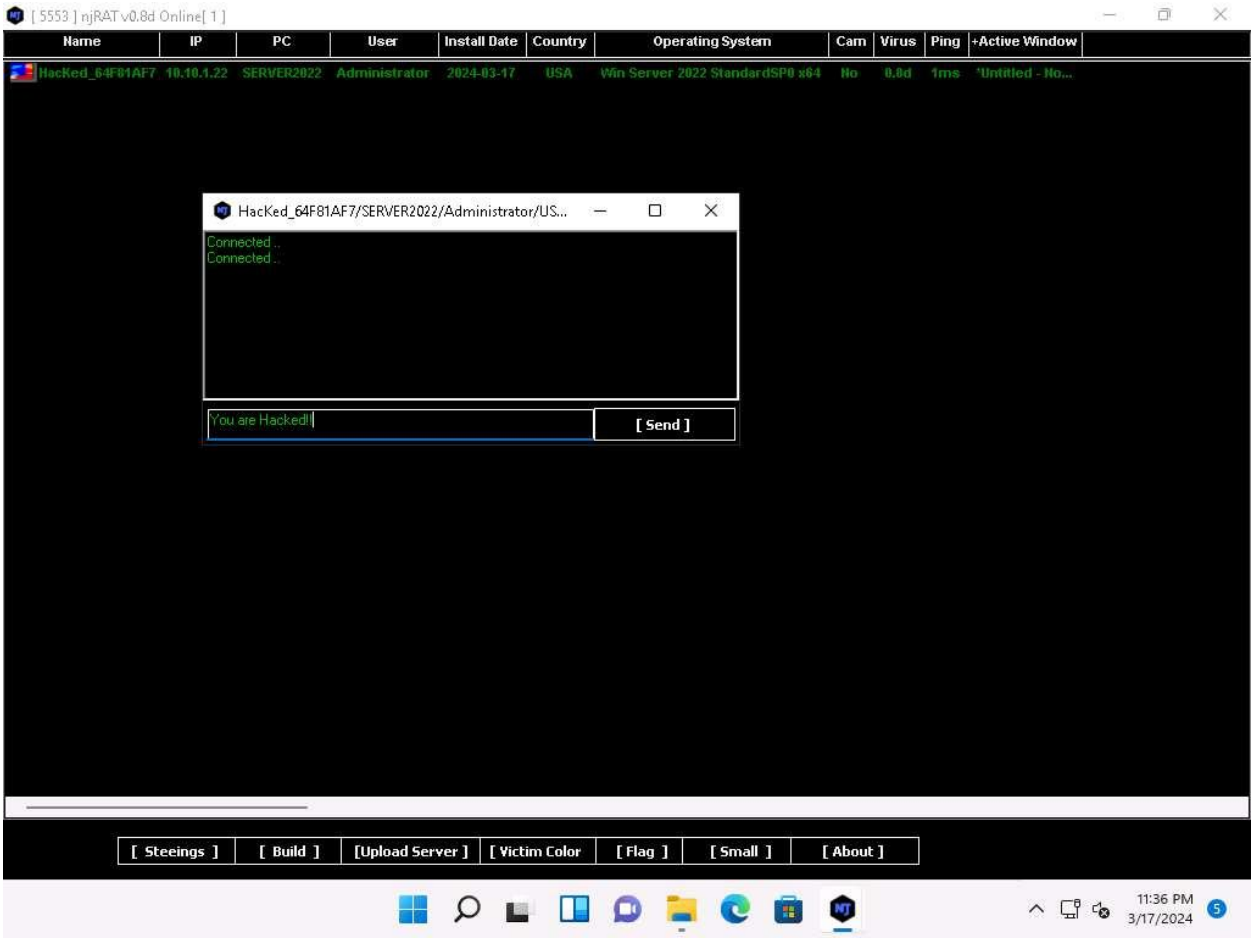
Select the text manually to view the keystrokes that were, typed.



40. Close the **Keylogger** window.
41. Right-click on the victim name, and click **Open Cha**.

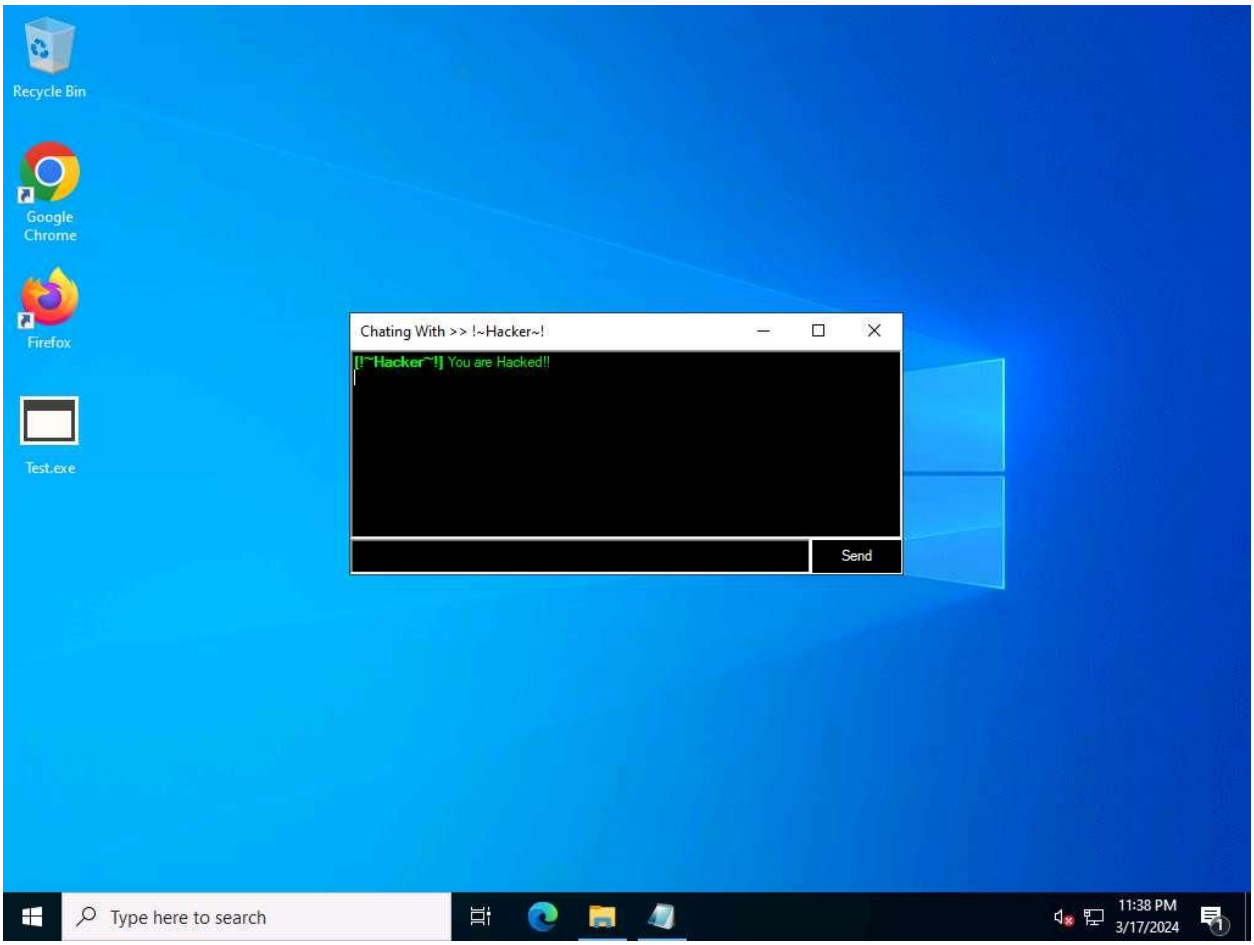


42. A **Chat** pop-up appears; enter a nickname (here, **Hacker**) and click **OK**.
43. A chat box appears; type a message, and then click **Send**.



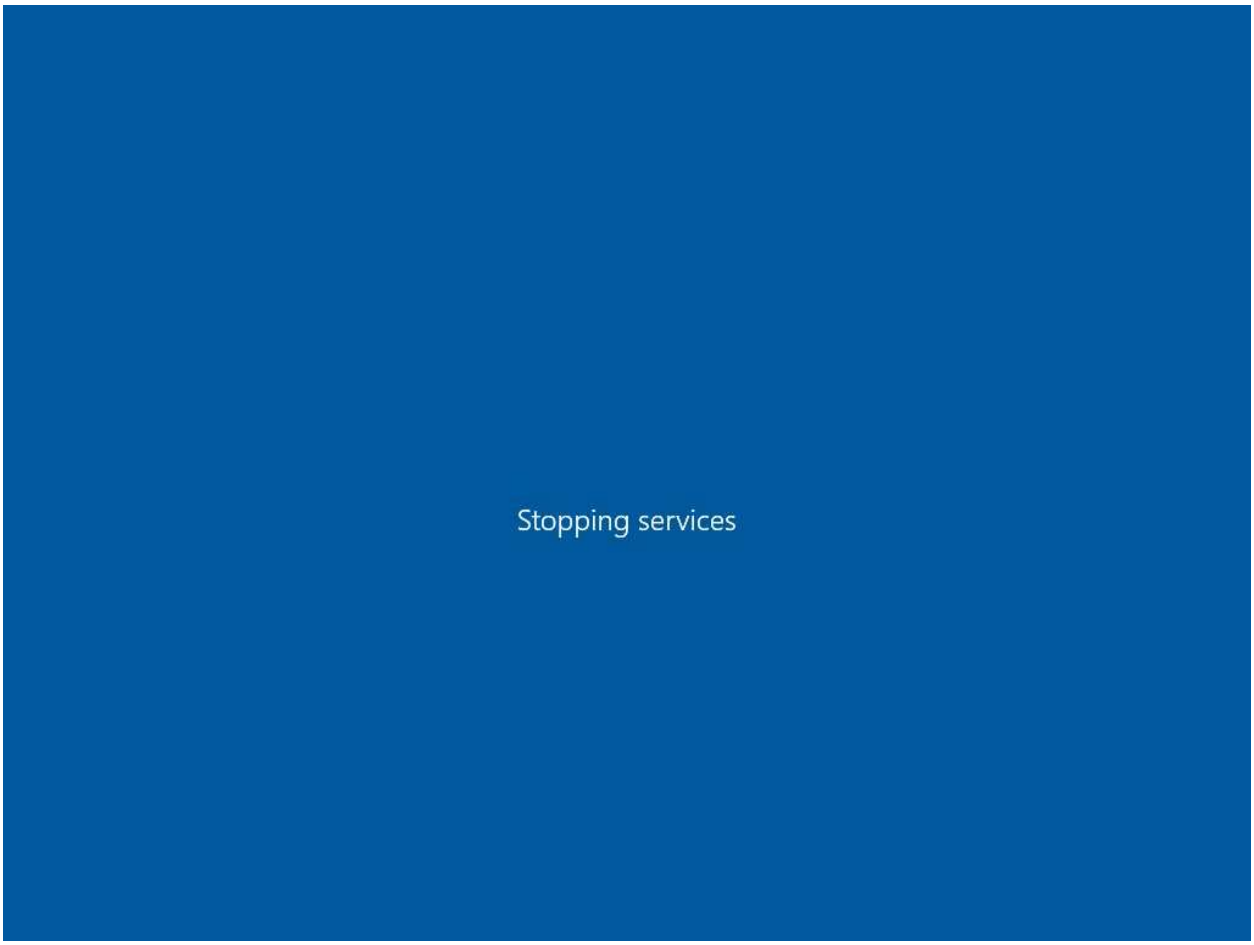
44. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows Server 2022**), as demonstrated in the screenshot.

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.

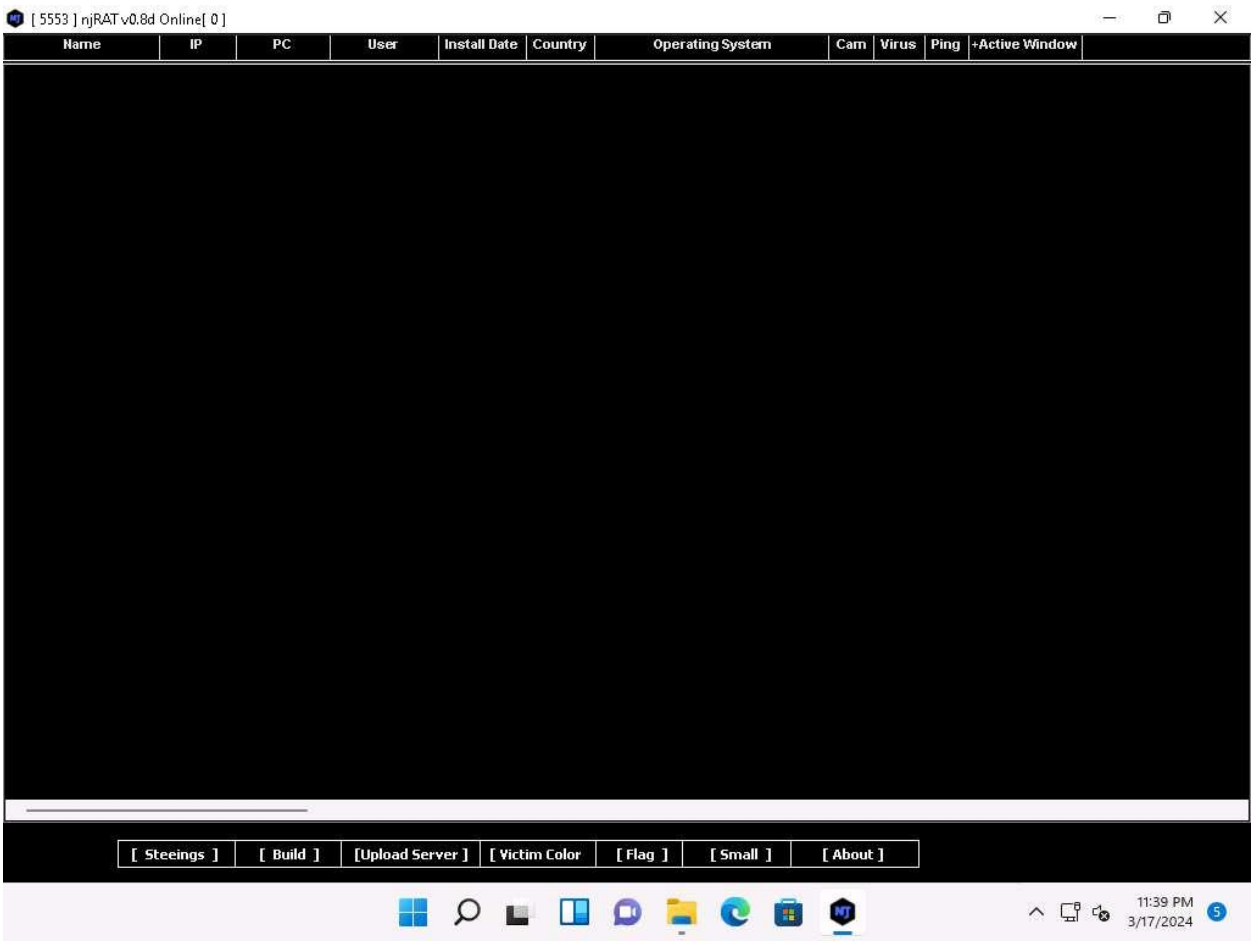


46. Seeing this, the victim becomes alert and attempts to close the chatbox. Irrespective of what the victim does, the chat box remains for open as long as the attacker uses it.

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.

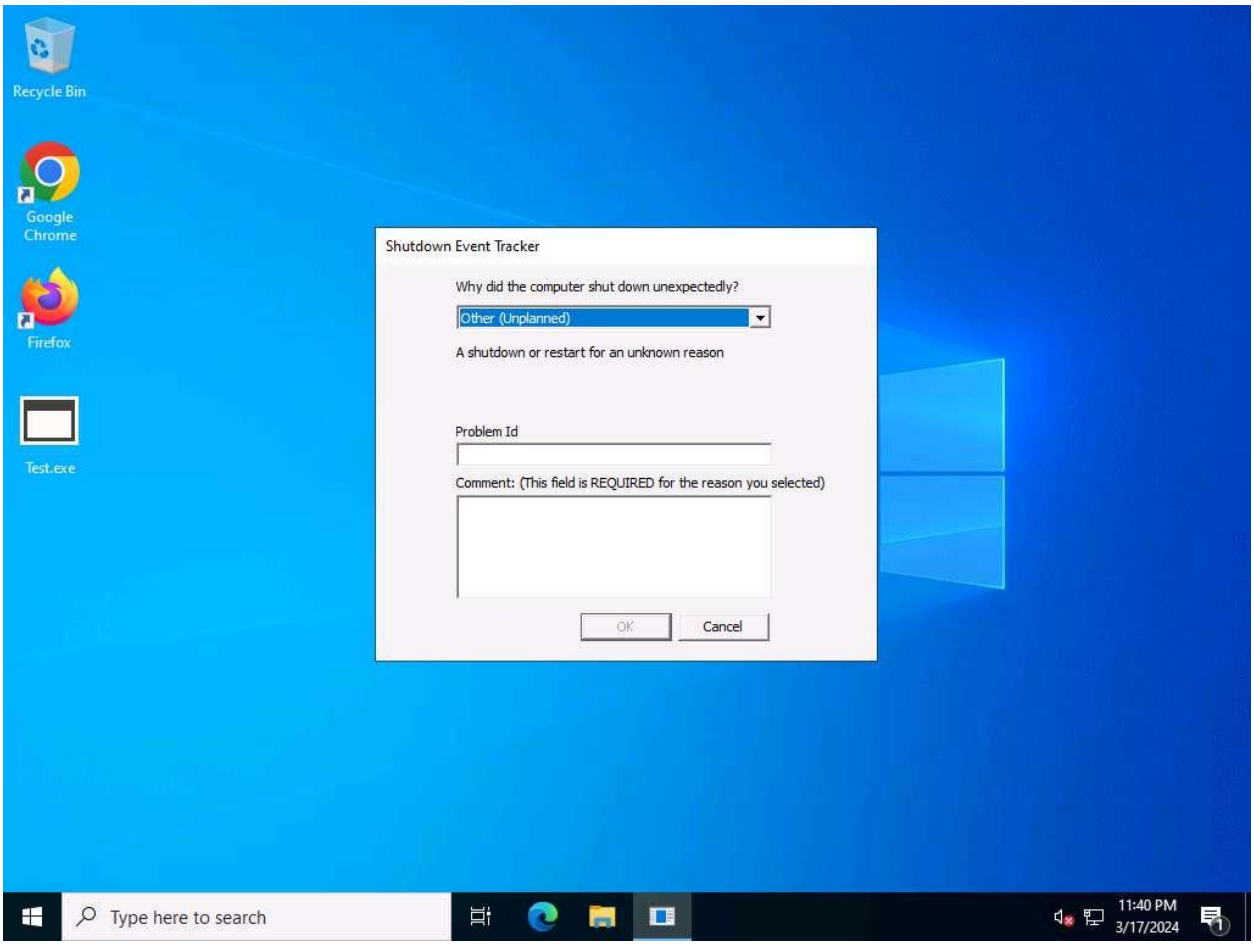


48. Click Windows 11 to switch back to the attacker machine (**Windows 11**); you can see that the connection with the victim machine is lost.



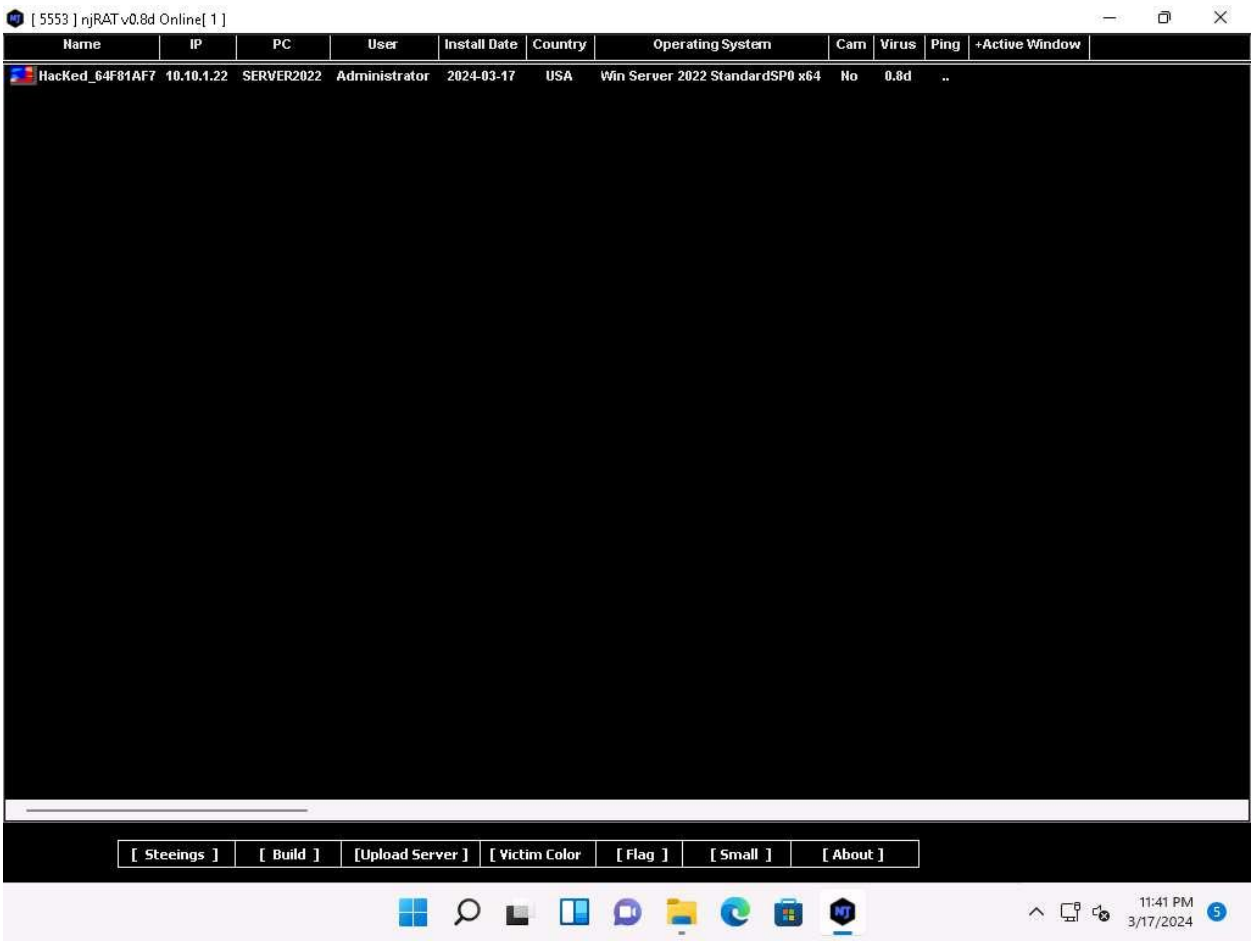
49. However, as soon as the victim logs in to their machine, the njRAT client automatically establishes a connection with the victim.

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**.



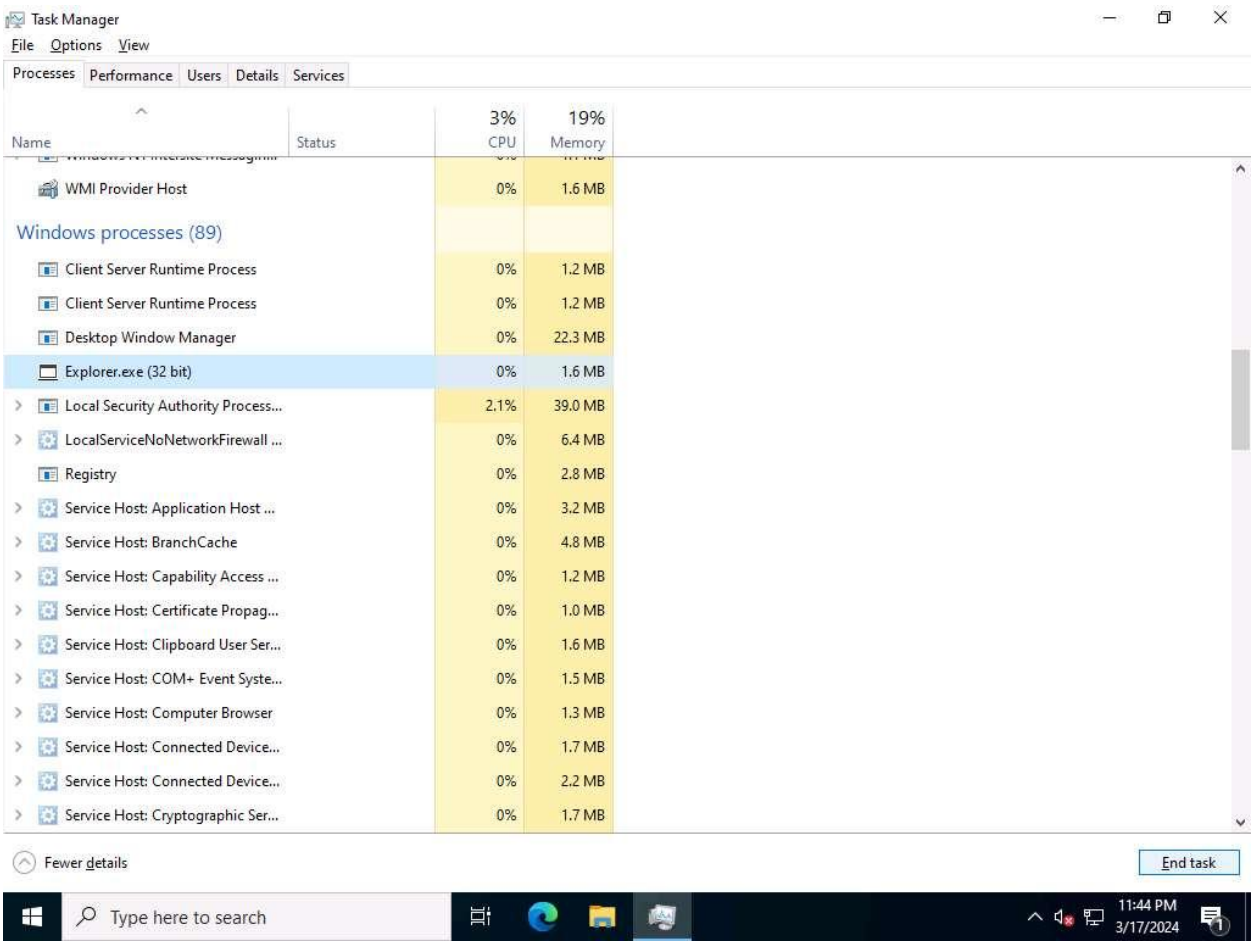
51. Click Windows 11 to switch back to the attacker machine (**Windows 11**); you can see that the connection has been re-established with the victim machine.

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.