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

Note: The versions of the created client or host and appearance of the website may differ from what it is in this lab. However, the actual process of creating the server and the client is the same, as shown in this lab.

Note: In this lab task, we will use the Windows 10 (10.10.10.10) virtual machine as the attacker machine and the Windows Server 2016 (10.10.10.16) virtual machine as the victim machine.

1. Turn on the Windows 10 and Windows Server 2016 victim machines.

2. In the Windows 10 virtual machine, log in with the credentials Admin and Pa$$word.

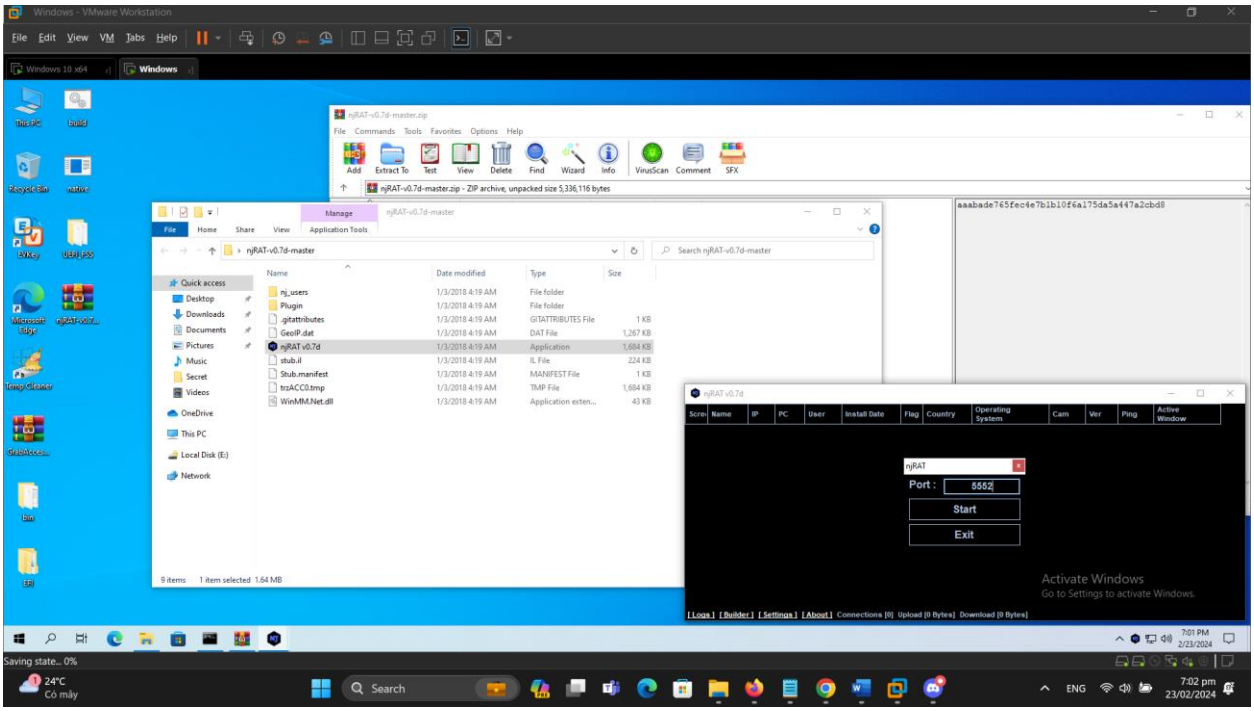
3. Navigate to E:\CEH-Tools CEHv11 Module 07 Malware Threats Trojans Types Remote Access Trojans (RAT)\njRAT and double-click njRAT v0.7d.exe.

Note: If a User Account Control window appears, click Yes.

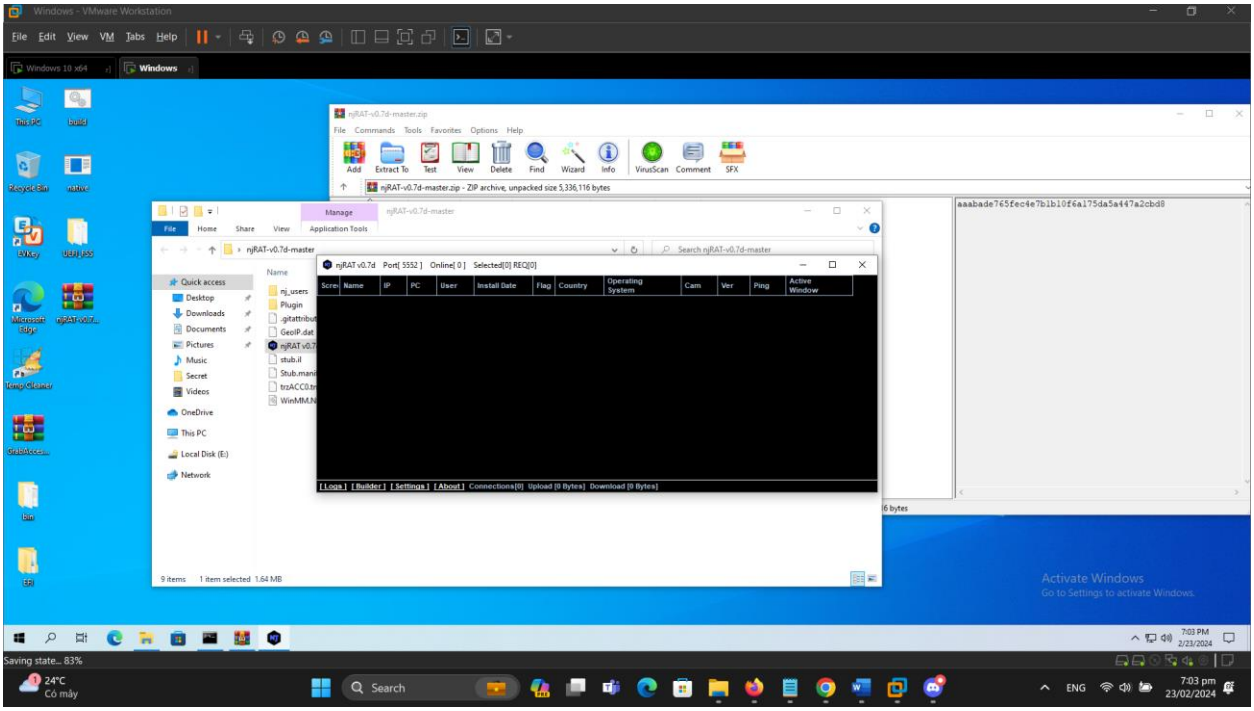
Note: If an Open File - Security Warning pop-up appears, click Run.

4. The njRAT GUI appears along with an njRAT pop-up, where you need to specify the port you want to use to interact with the victim machine. Enter the port number and click Start.

5. In this lab, the default port number 5552 has been chosen.

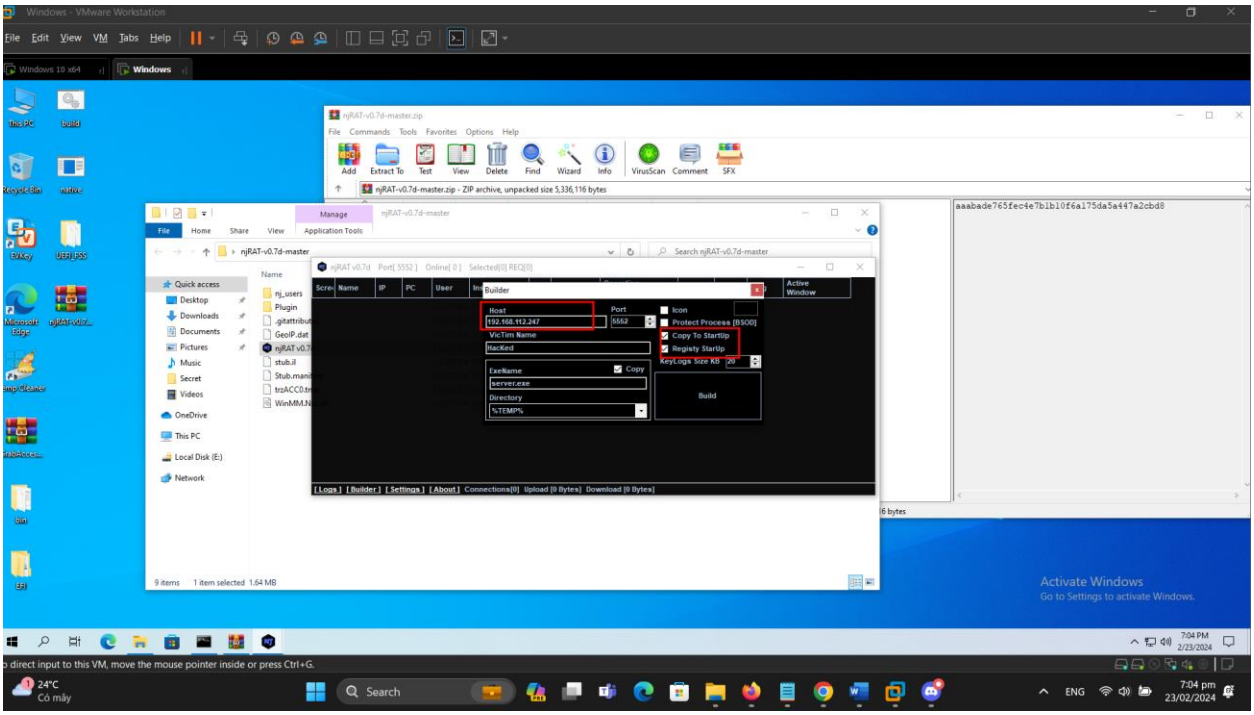



The njRAT GUI appears; click the Builder link located in the lower-left corner of the GUI to configure the exploit details.



7. The Builder dialog-box appears; enter the IP address of the Windows 10 (attacker machine) virtual machine in the Host field, check the options Copy To StartUp and Registy StarUp, leave the other settings to default, and click Build.

Note: In this lab, the IP address of the Windows 10 virtual machine is 10.10.10.10. This IP address might vary in your lab environment.

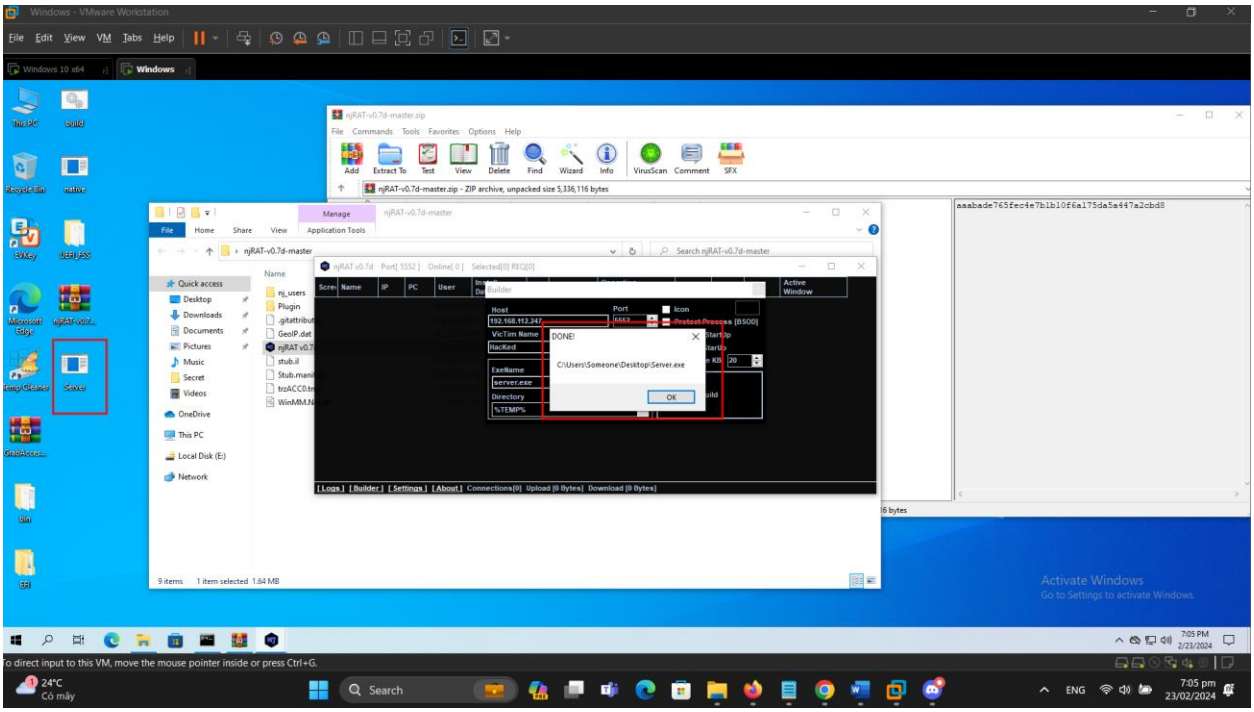


8. The Save As window appears; specify a location to store the server, rename it, and click Save.

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

10. Once the server is created, the DONE! pop-up appears, click OK.

11. 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)

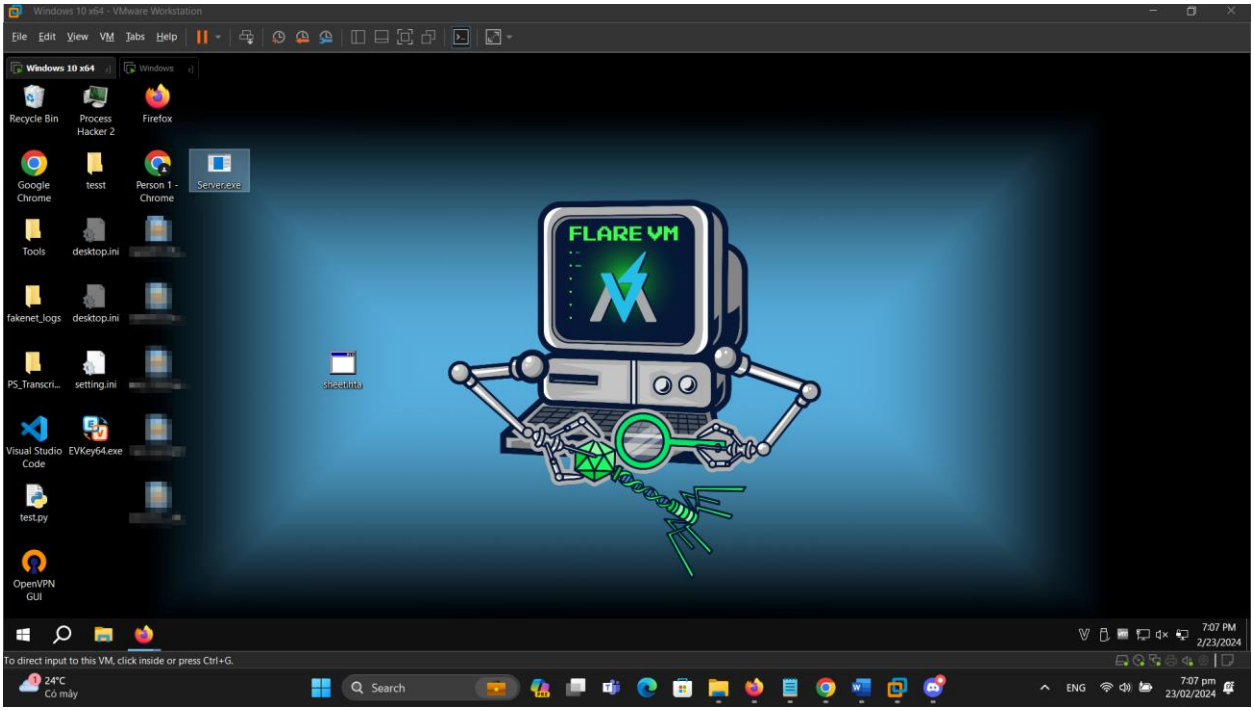



12. Log in to the Windows Server 2016 virtual machine as a legitimate user using the credentials Administrator and Password.

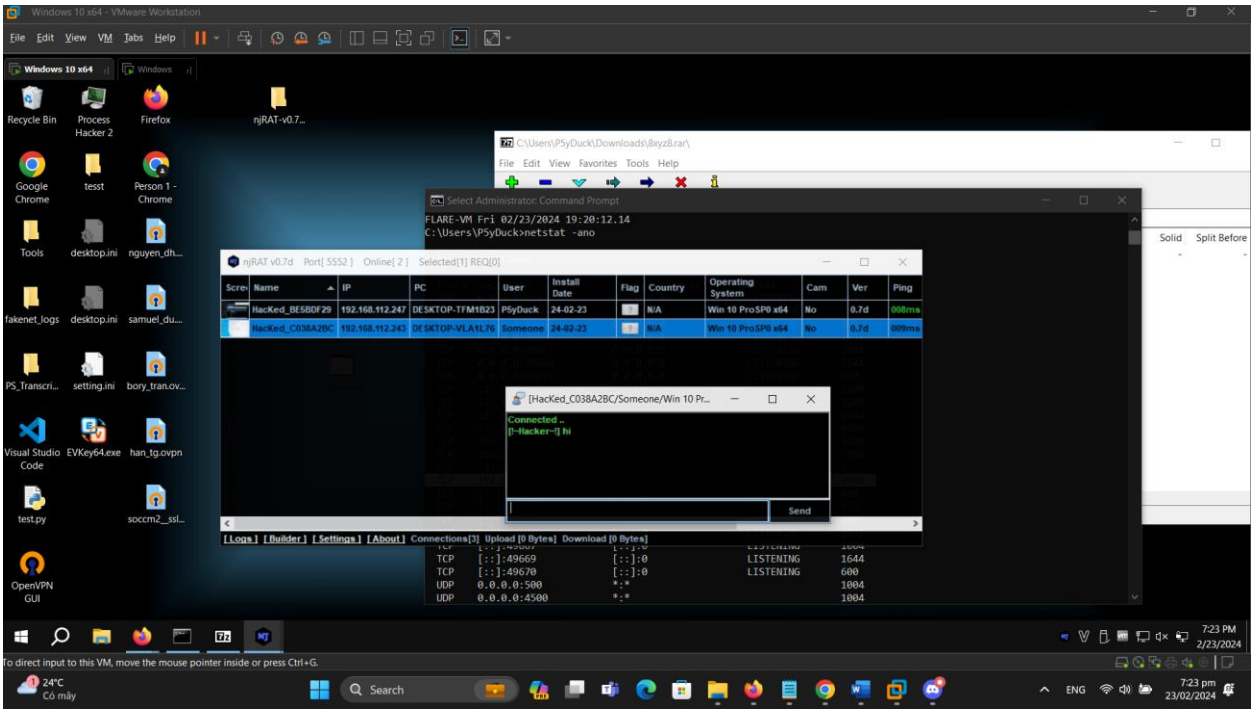
13. Navigate to the shared network location (CEH-Tools), and then Copy and Paste the executable file (Test.exe) onto the Desktop of Windows Server 2016.

14. Here, you are acting both as an attacker who logs into the Windows 10 machine to create a malicious server, and as a victim who logs into the Windows Server 2016 virtual machine and downloads the server.

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




16. Switch back to the Windows 10 virtual machine. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in Windows 10 establishes a persistent connection with the victim machine, as shown in the screenshot.



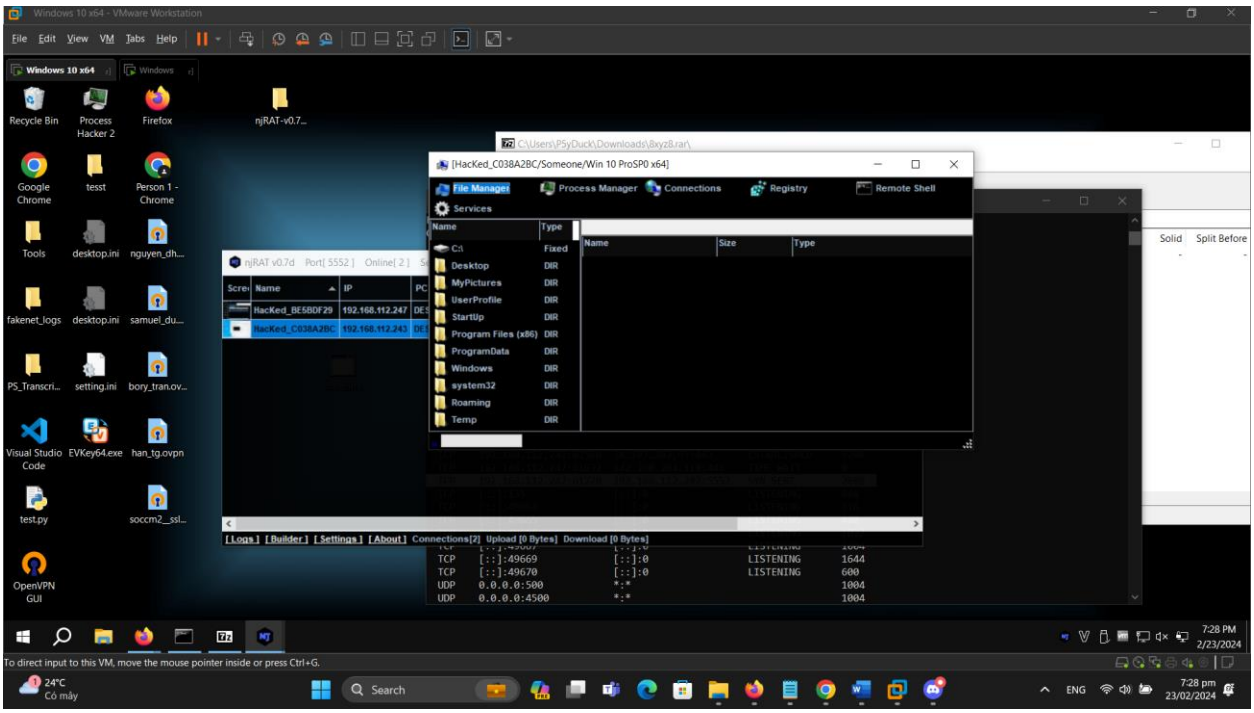

17. Unless the attacker working on the Windows 10 machine disconnects the server on their own, the victim machine remains under their control.

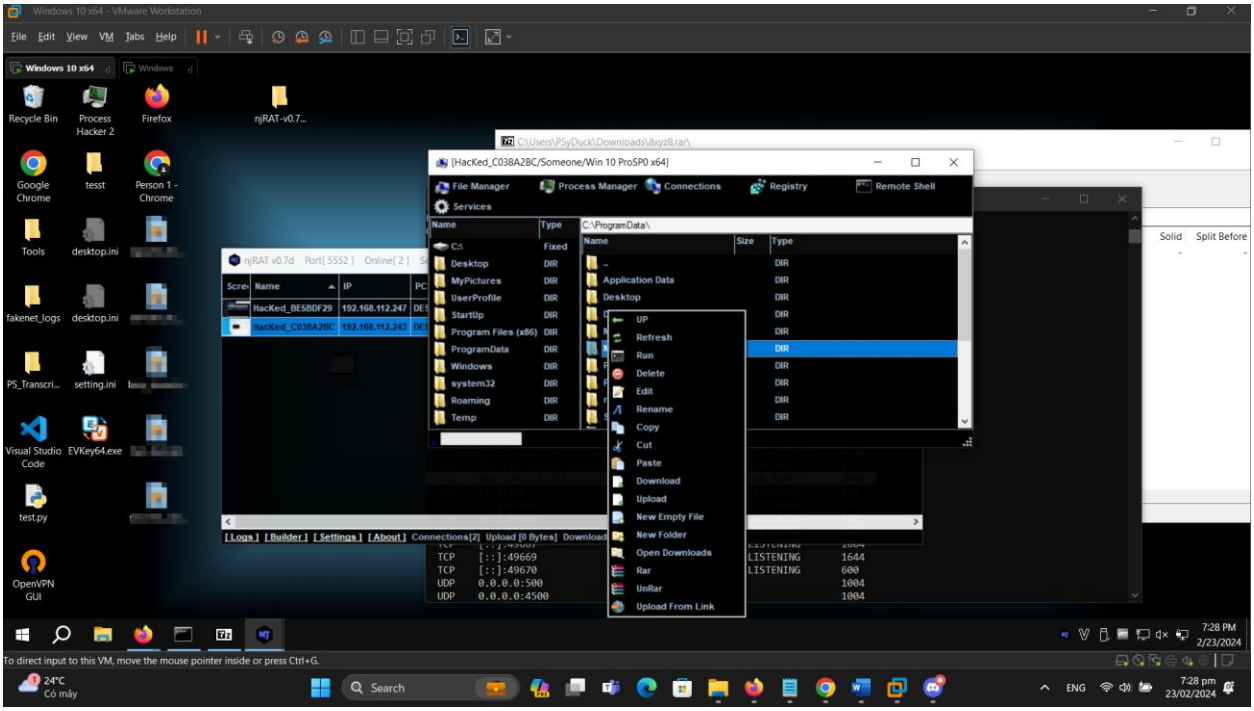
18. The GUI displays the machine's basic details such as the IP address, User name, and Type of Operating system.

19. Right-click on the detected victim name and click Manager

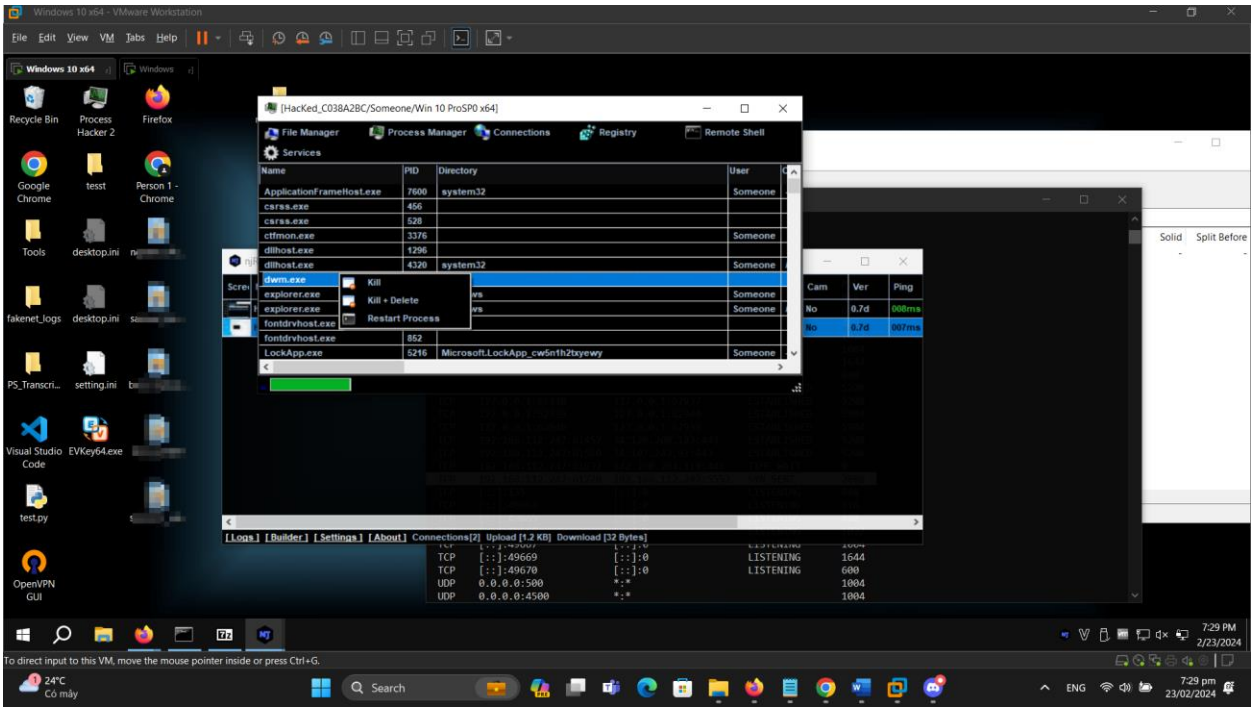
20. The manager window appears with File Manager selected by default.

21. 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

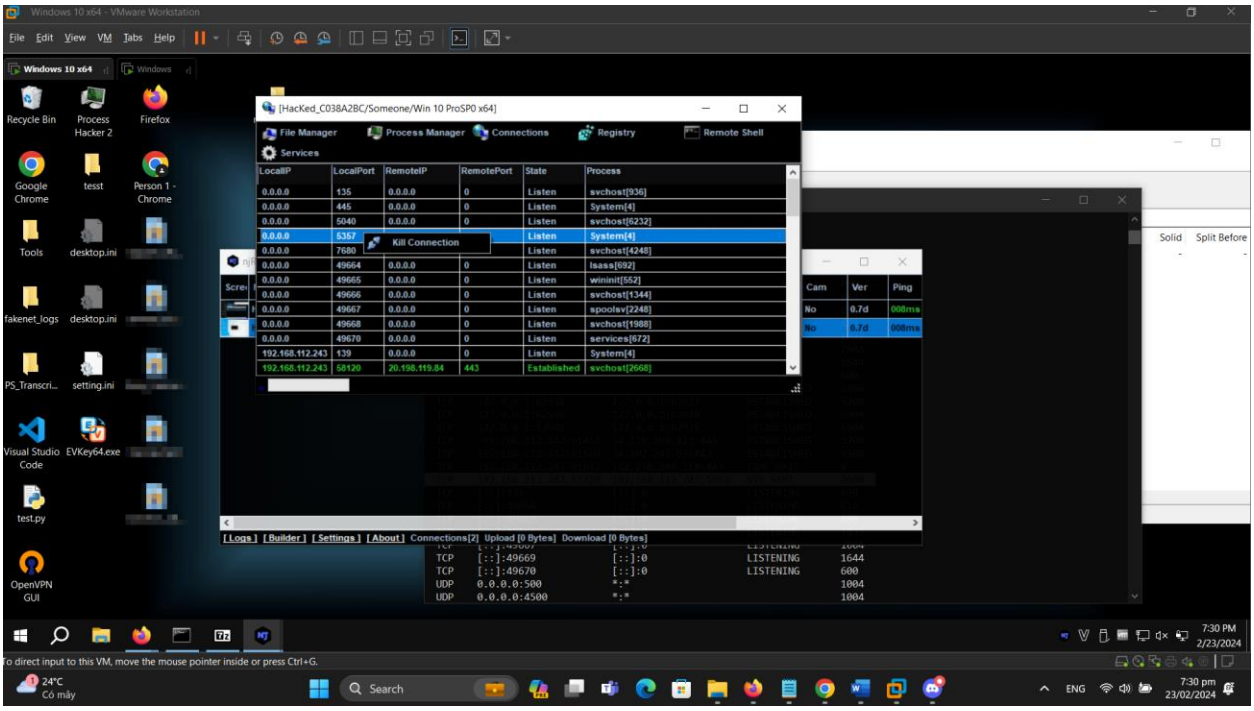





22. Click on Process Manager. You will be redirected to the Process Manager, where you can right-click on a selected process and perform actions such as Kill, Delete, and Restart

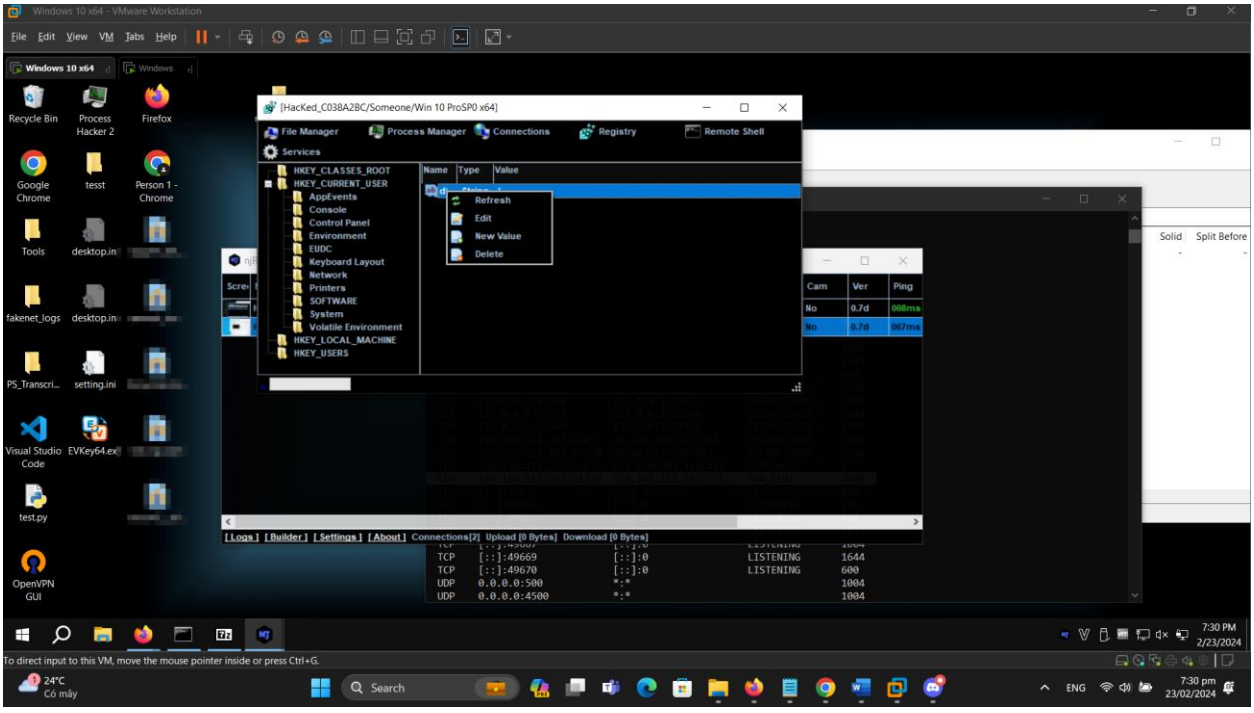



23. Click on Connections, select a specific connection, right-click on it, and click Kill Connection. This kills the connection between two machines communicating through a particular port




24. Click on Registry, choose a registry directory from the left pane, and right- click on its associated registry files.

25. A few options appear for the files; you can use these to manipulate them



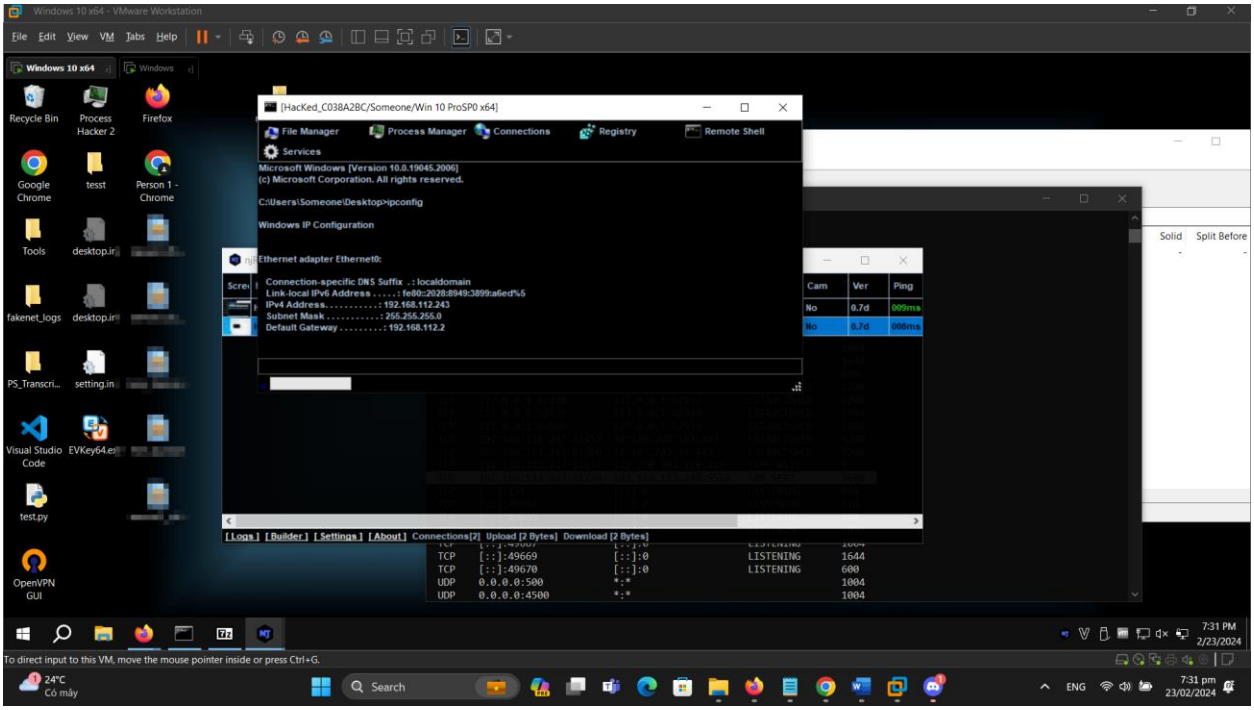

.

26. Click Remote Shell. This launches a remote command prompt for the victim machine (Windows Server 2016).

Launch a Remote Shell

27. Type the command ipconfig/all and press Enter.

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

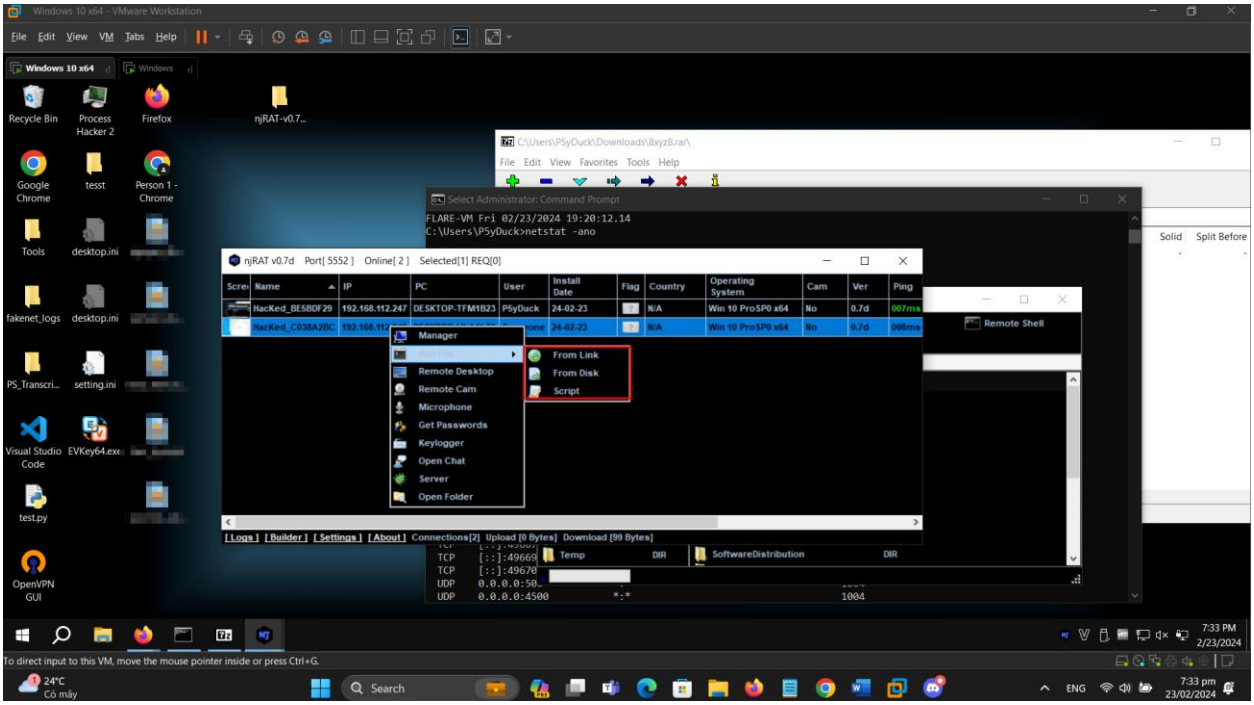



29. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine.

30. In the same way, click Services. You will be able to view all services running on the victim machine. In this section, you can use options to start, pause, or stop a service.

31. Close the Manager window.

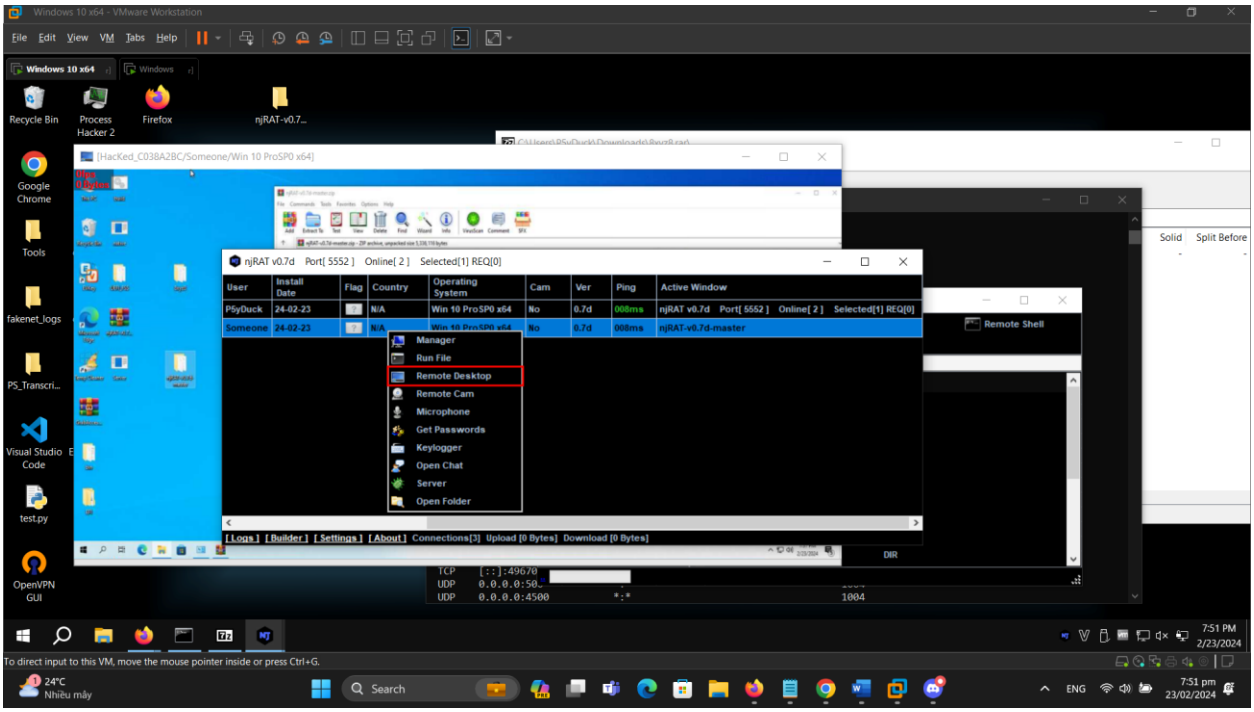
32. Now, right-click on the victim name, click Run File, and choose an option. from the drop-down list to execute scripts or files remotely from the attacker machine.

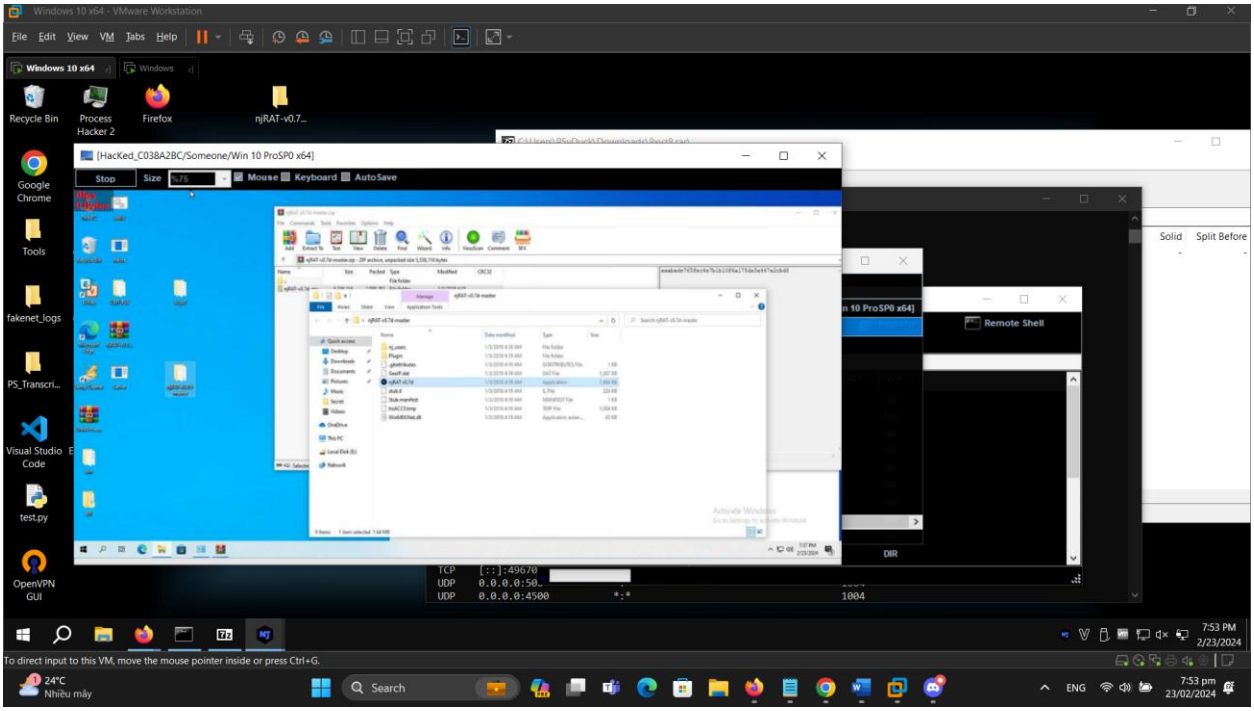



33. Right-click on the victim name, and then select Remote Desktop.

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

35. A Remote Desktop window appears; hover the mouse cursor to the top- center area of the window. A down arrow appears; click it.



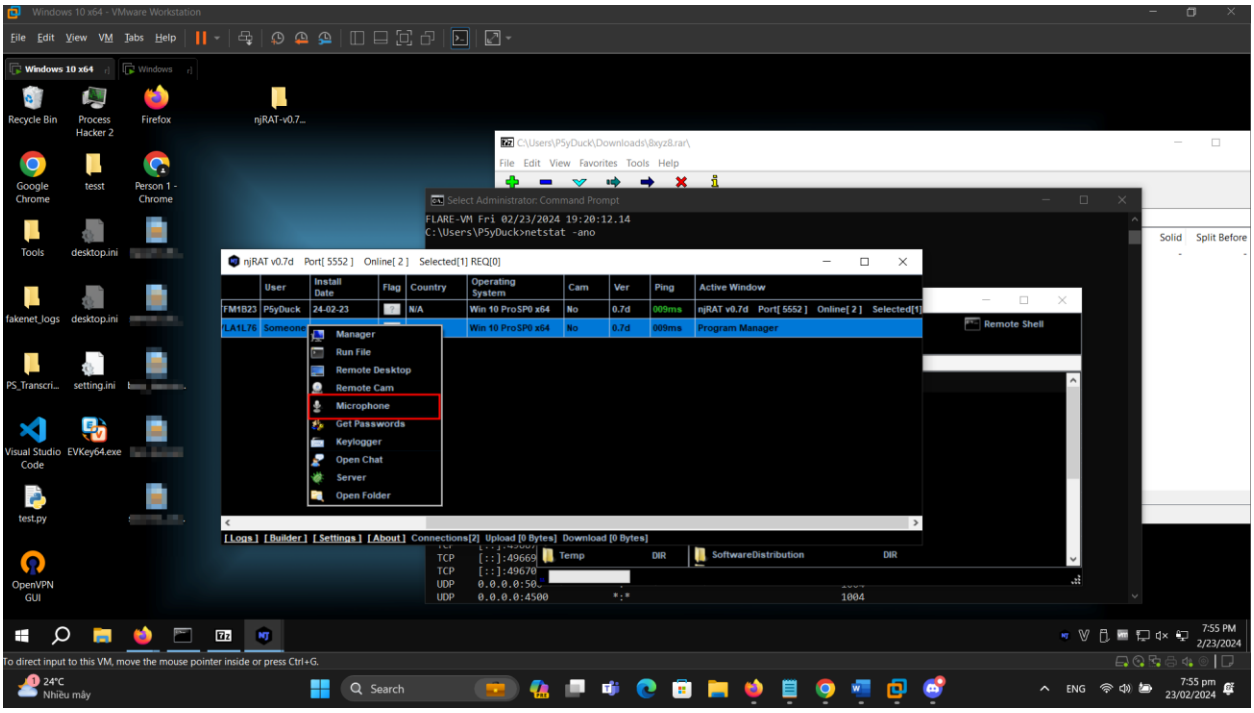



37. Now, you will be able to remotely interact with the victim machine using the mouse.

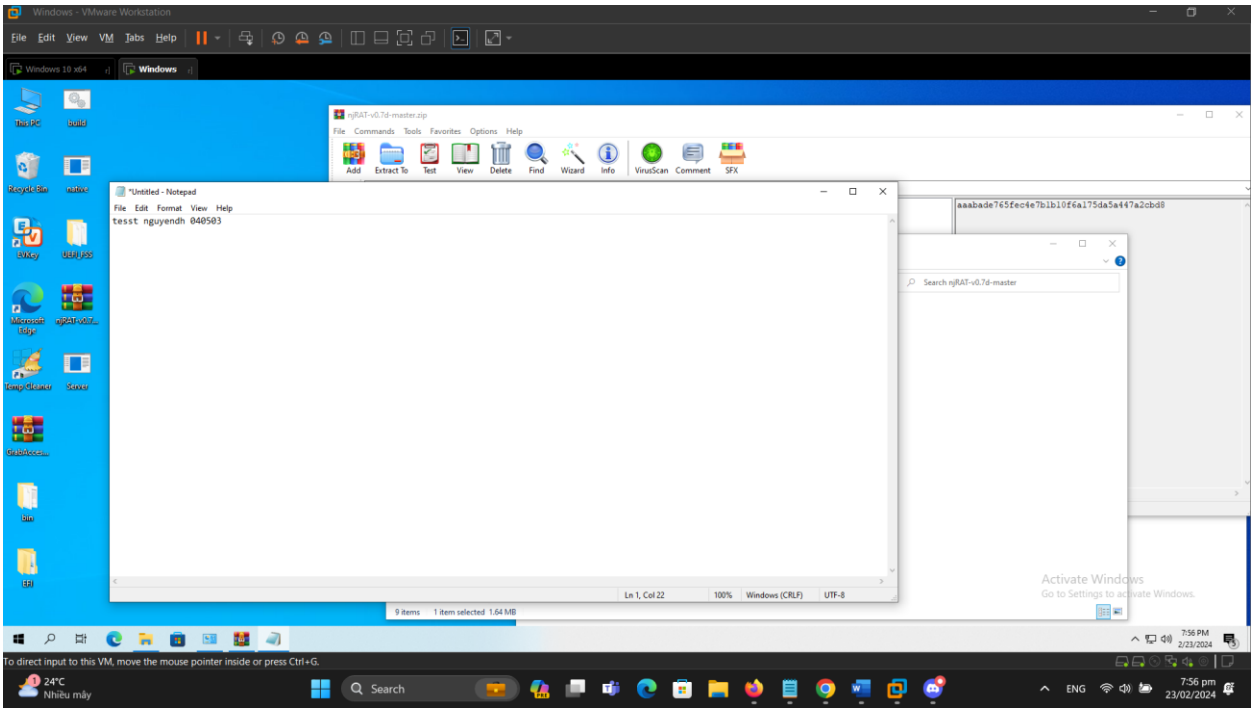
Note: If you want to create any files or write any scripts on the victim machine, you need to check the Keyboard option.

38. On completing the task, close the Remote Desktop window.

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



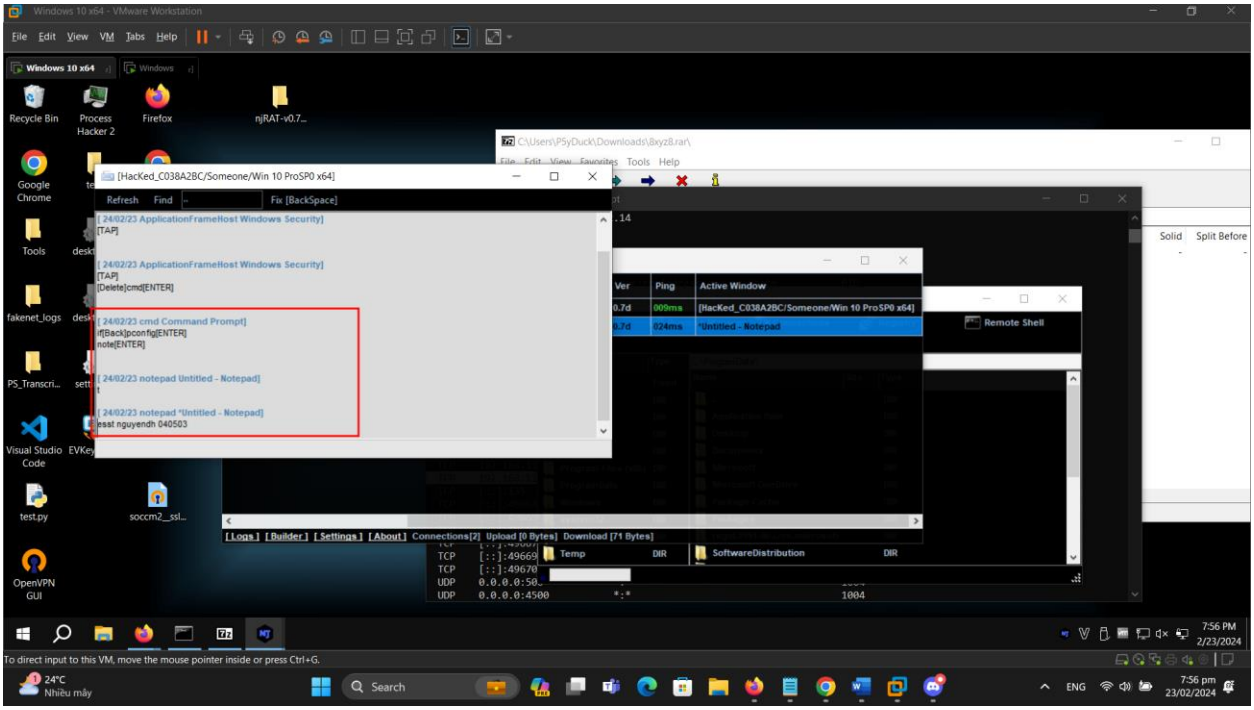

40. Switch to the Windows Server 2016 virtual machine. Assume that you are a legitimate user and perform a few activities such as logging into any website or typing some text in text documents.




41. Switch back to the Windows 10 virtual machine, right-click on the victim name, and click Keylogger

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

43. The window displays all the keystrokes performed by the victim on the Windows Server 2016 virtual machine, as shown in the screenshot.



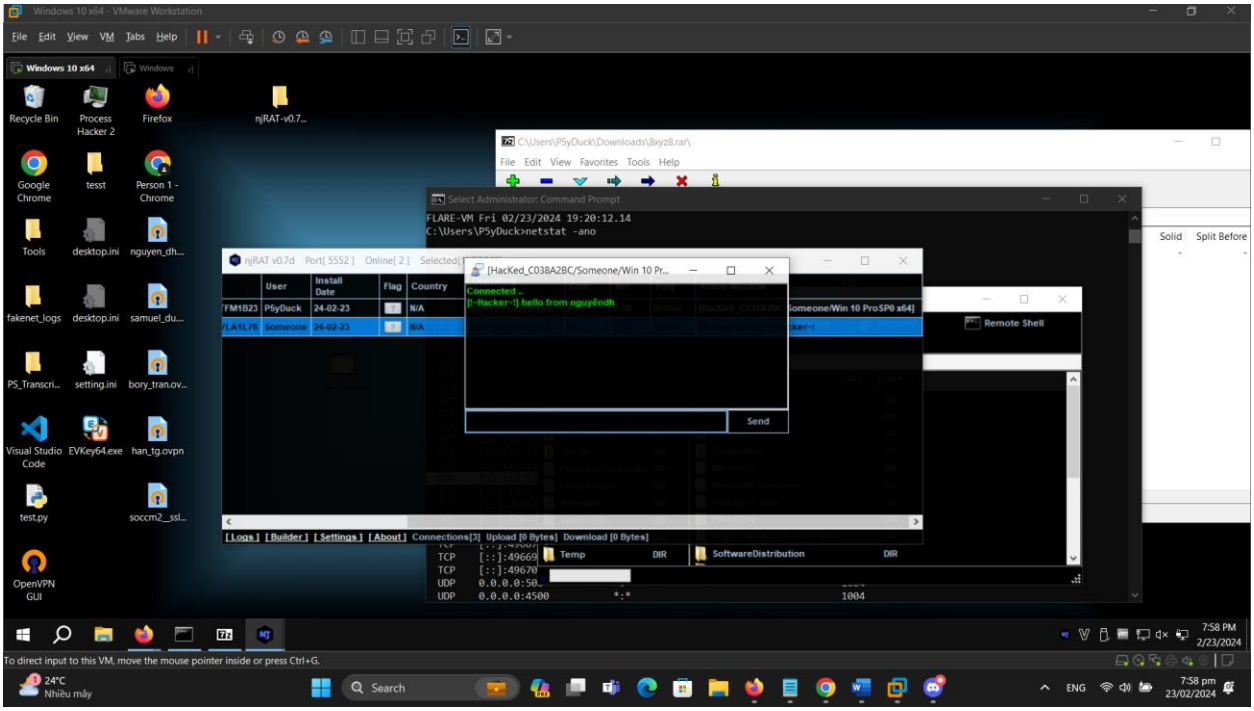

44. Close the Keylogger window.

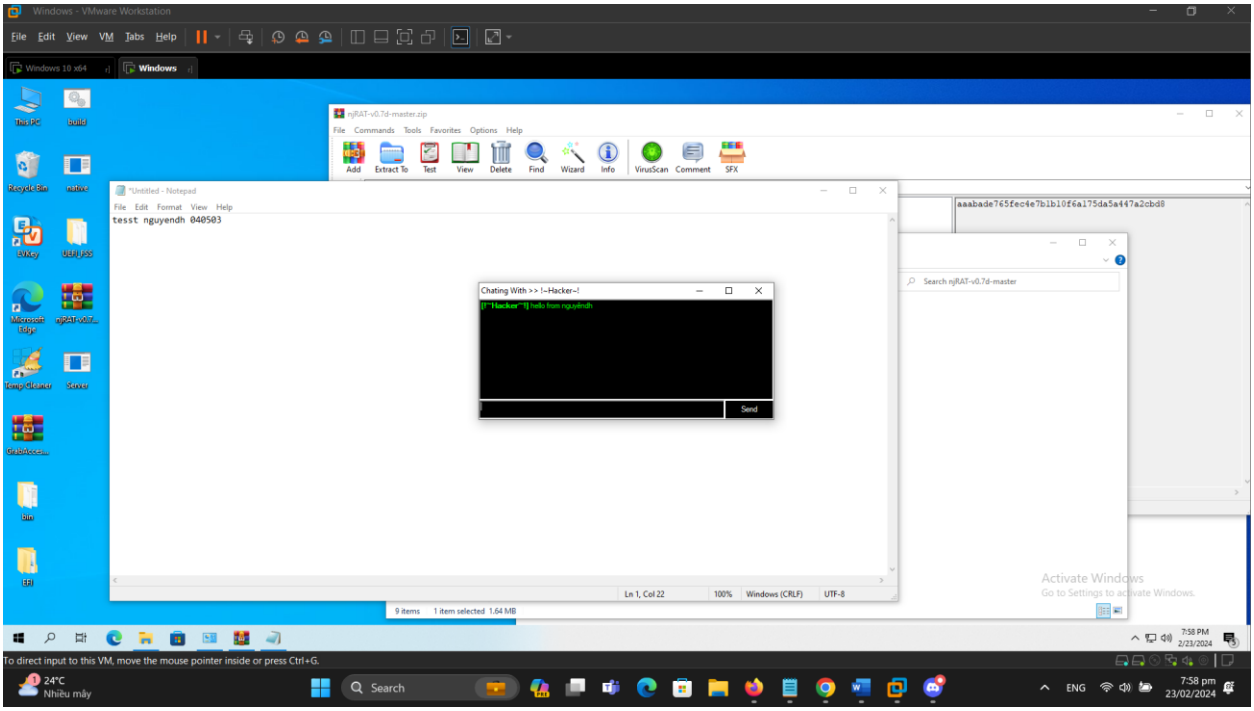
45. Right-click on the victim name, and click Open Chat.

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

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

48. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (Windows Server 2016), as demonstrated in the screenshot

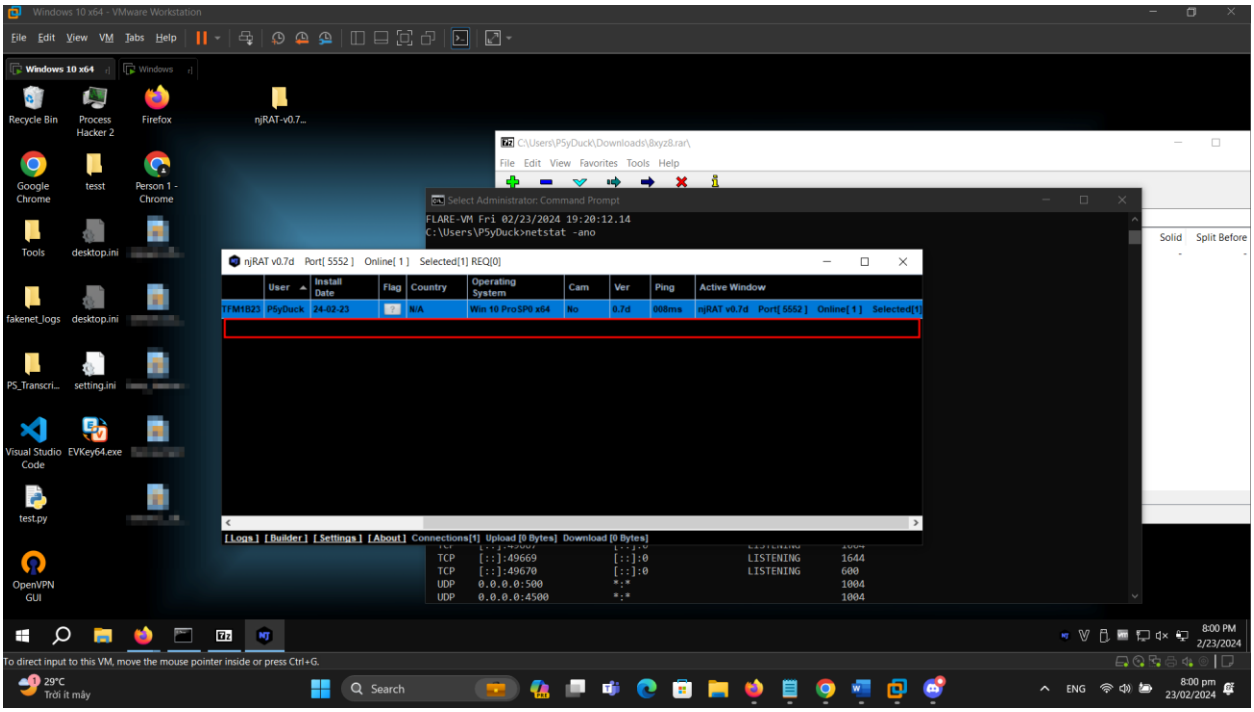




49. Seeing this, the victim becomes alert and attempts to close the chatbox. Irrespective of what the victim does, the chatbox remains for open as long as the attacker uses it.

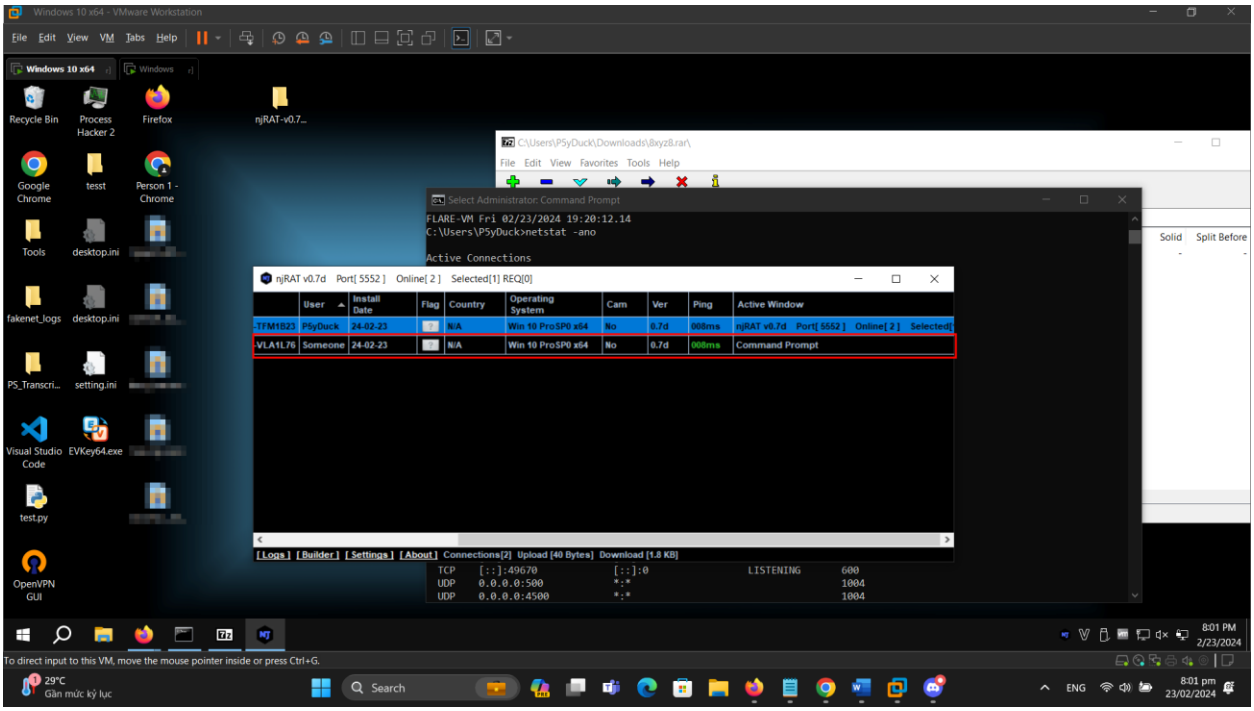
50. Surprised by the behavior, the victim (you) attempts to break the connection by restarting the machine. As soon as this happens, njRAT loses its connection with Windows Server 2016, as the machine is shut down in the process of restarting,

51. Switch back to the attacker machine (Windows 10); you can see that the connection with the victim machine is lost.




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

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



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

54. On completion of this lab, launch Task Manager, look for the server.exe (32 bit) process, and click End task on the Windows Server 2016 machine.

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 on both the Windows 10 and Windows Server 2016 virtual machines.

57. Turn off the Windows Server 2016 virtual machine.

## Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs

Here, we will use the SwayzCryptor to hide a Trojan and make it undetectable by anti-virus software.

Note: Ensure that the Windows 10 virtual machine is running.

1. Turn on the Windows Server 2016 virtual machine

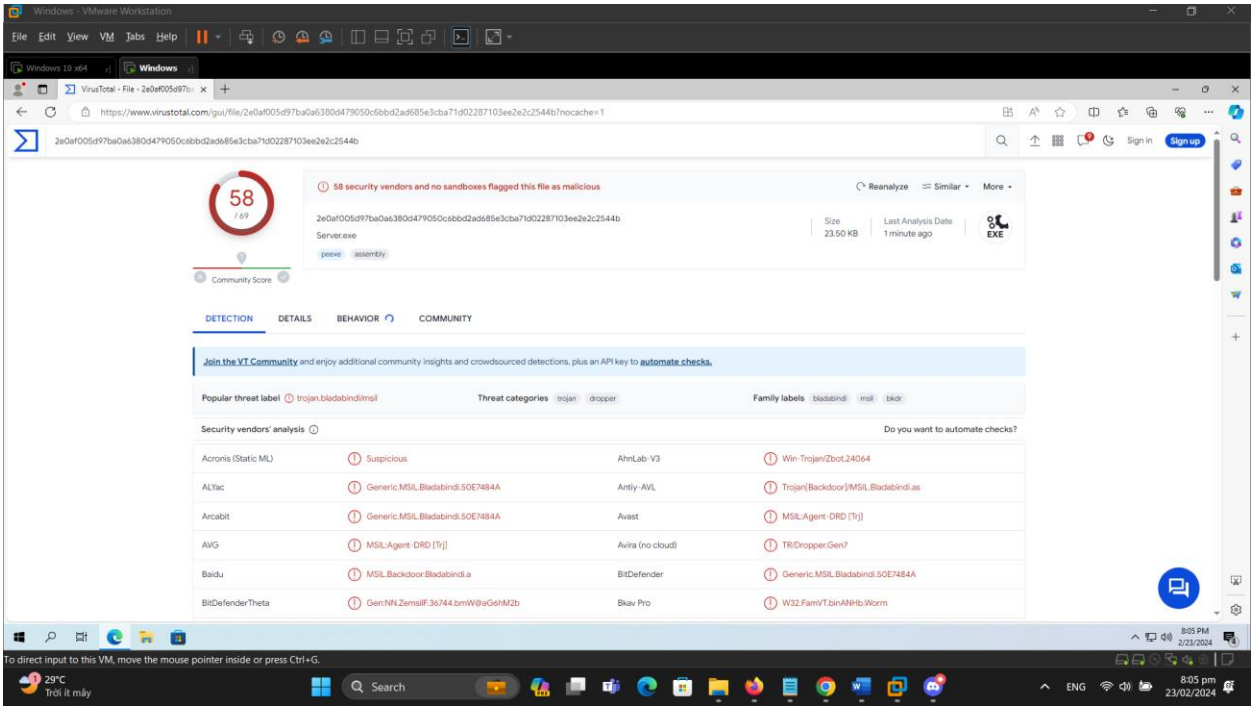
2. In the Windows 10 virtual machine, open any web browser (here, Google Chrome), enter the URL. https://www.virustotal.com in the address bar, and press Enter.

3. The Virus Total main analysis site appears; click Choose file to upload a virus file.

4. An Open dialog box appears; navigate to the location where you saved the malware file Test.exe in the previous lab (Desktop), select it, and click Open.

5. Click Confirm upload on the Virus Total page.

6. The VirusTotal uploads the file, scans it with the various anti-virus programs in its database, and displays the scan result, as shown in the screenshot.



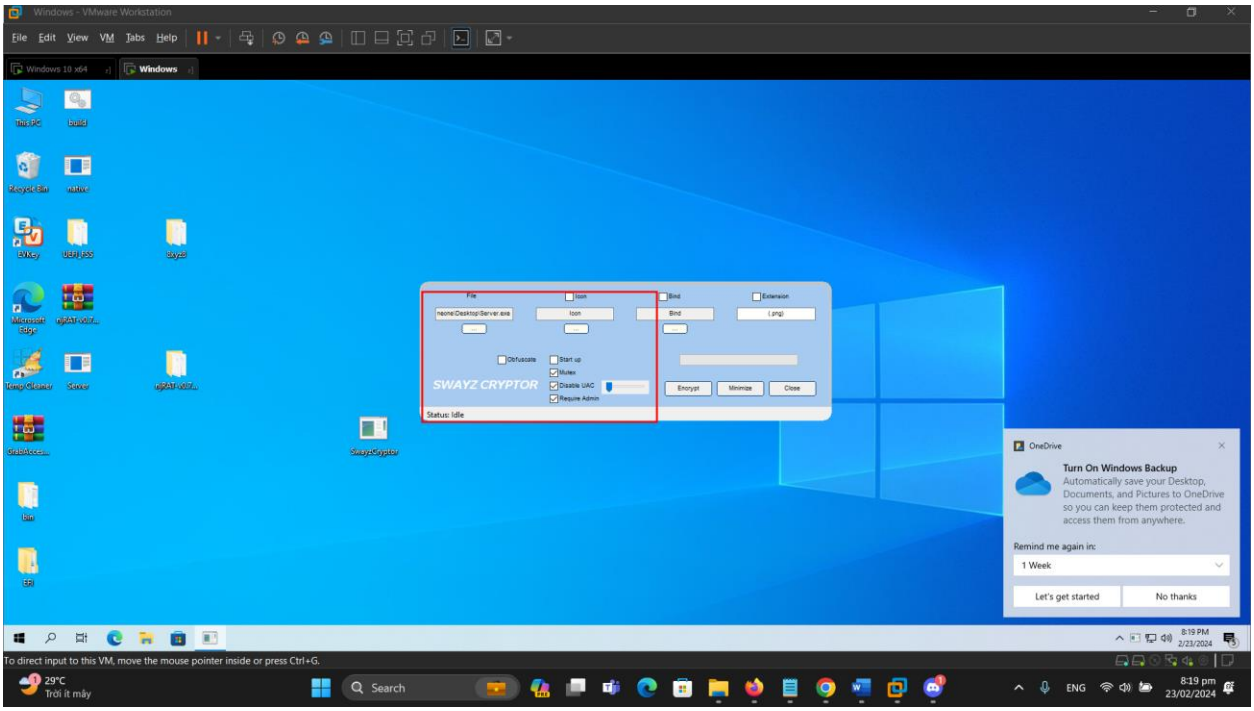

7. You can see that 61 out of 69 anti-virus programs have detected Test.exe as a malicious file. Minimize the web browser window.

Note: The detection ratio might vary in your lab environment.

8. The SwayzCryptor GUI appears; click below File to select the Trojan file.

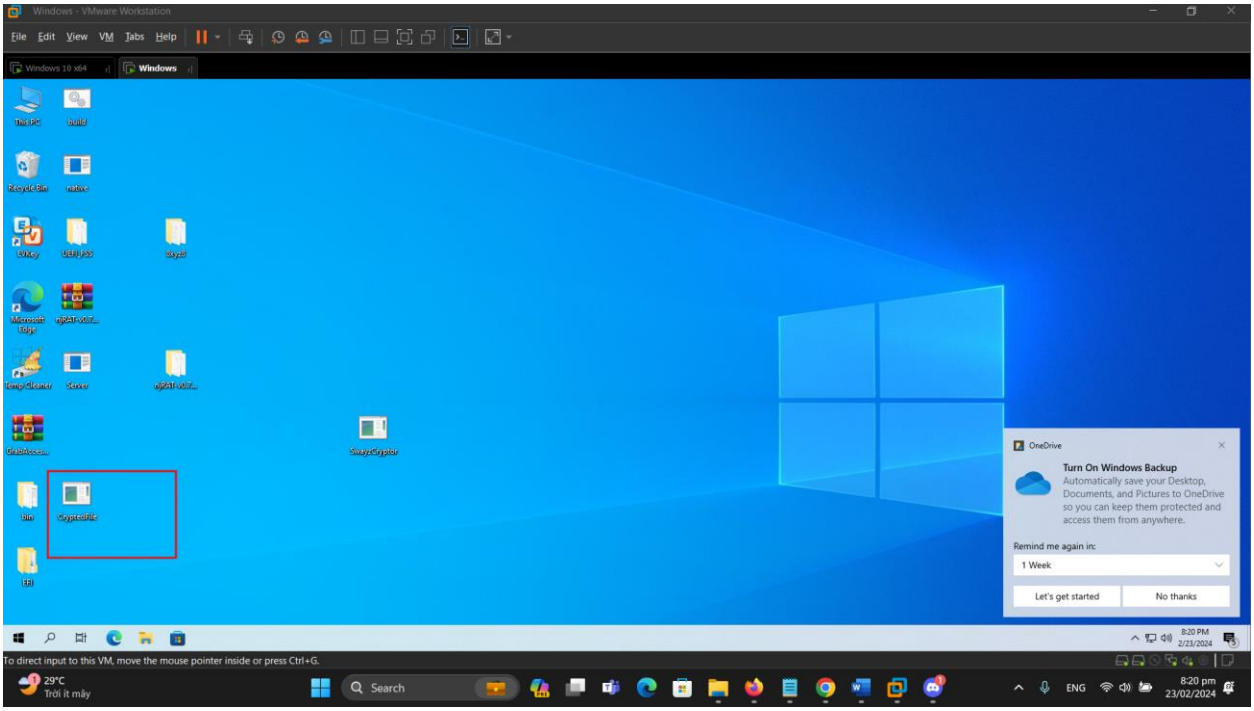
10. The Select a File dialog-box appears; navigate to the location of Test.exe (Desktop), select it, and click Open.

11. Once the file is selected, check the options Start up, Mutex, and Disable UAC, and then click Encrypt.




12. The Save File dialog-box appears; select the location where you want to store the crypted file (here, Desktop), leave the file name set to its default (CryptedFile), and click Save.

13. Once the encryption is finished, click Close.

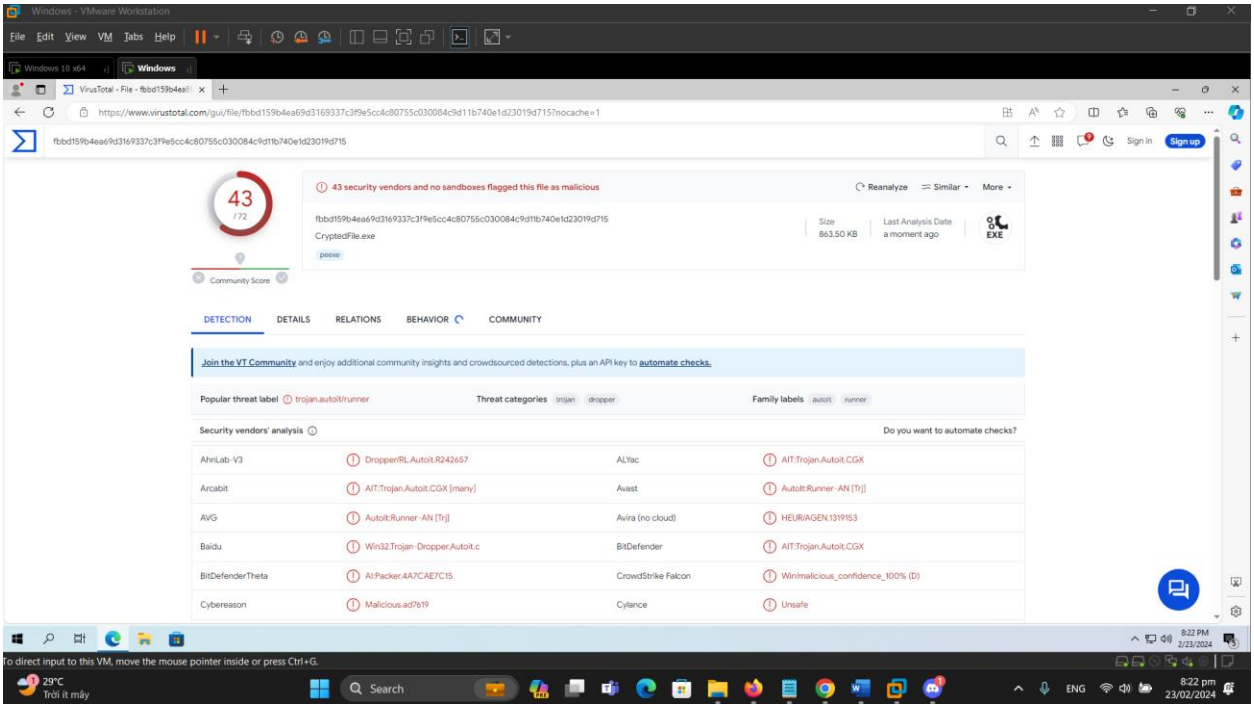



14. Maximize the web browser (here, Google Chrome). In the Virus Total analysis page, click the Upload file icon in the top-right corner of the page

15. An Open dialog-box appears; navigate to the location where you saved the encrypted file CryptedFile.exe (Desktop), select the file, and click Open.

16. Click Confirm upload.

17. VirusTotal uploads the file and begins to sean it with the various anti-virus programs in its database. It displays the scan result, as shown in the screenshot.




18. Only a few anti-virus programs have detected CryptedFile.exe as a malicious file. Minimize or close the browser window.

Note: The specific scan result might vary in your lab environment.

19. Now, we will test the functioning of a Crypted file (CryptedFile.exe).

20. Go to ECEH-Tools CEHv11 Module 07 Malware Threats Trojans Types Remote Access Trojans (RAT)injRAT, double-click the njRAT v0.7d.exe file and launch njRAT by choosing the default port number 5552, and then click Start

21. In this exercise, we have already created a crypted file (CryptedFile.exe), built using njRAT.

22. Use any technique to send CryptedFile.exe to the intended target-through email or any other source (In real-time, attackers send this server to the victim).

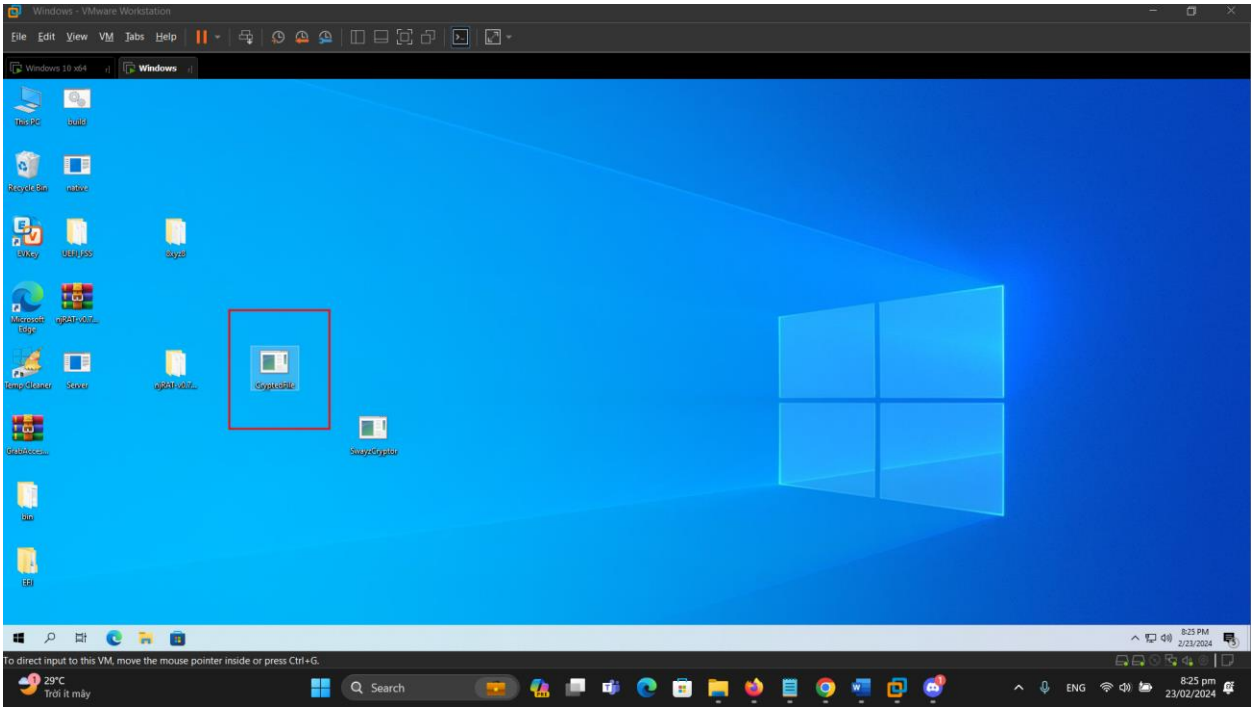
Note: In this lab, we copied the CryptedFile.exe file to the shared network location (CEH-Tools) to share the file.

23. Log in to the Windows Server 2016 virtual machine as a legitimate user using the credentials Administrator and Password.

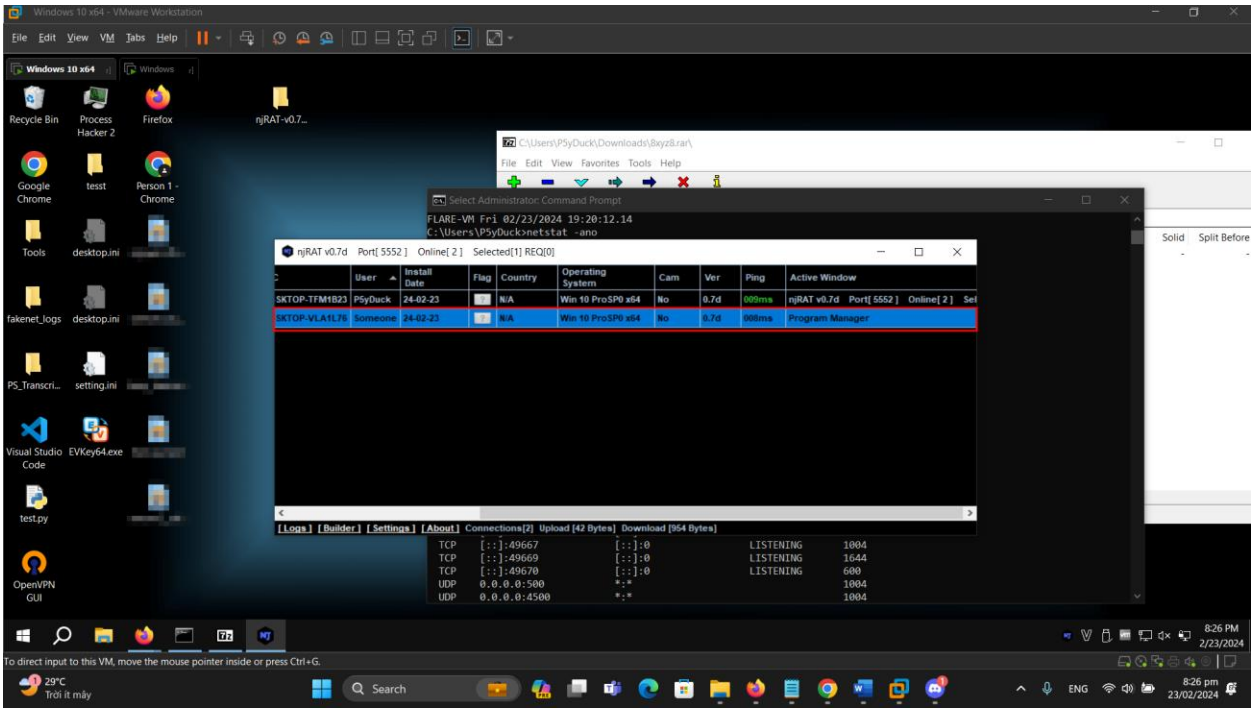
24. Navigate to the shared network location (CEH-Tools), and then Copy and Paste the executable file (CryptedFile.exe), in which the attacker (here, you) sent the server executable, to the Desktop of Windows Server 2016.

25. Here, you are acting both as the attacker who logs into the Windows 10 machine to create a malicious server and as the victim who logs into the Windows Server 2016 virtual machine and downloads the server.

26. Double-click CryptedFile.exe to run this malicious executable.



27. As soon as the victim (here, you) double-clicks the server, the executable starts running, and the njRAT client (njRAT GUI) running on the Windows 10 virtual machine establishes a persistent connection with the victim machine, as shown in the screenshot



28. Unless the attacker working on the Windows 10 machine disconnects the server on their own, the victim machine remains under their control.

29. Thus, you have created an undetectable Trojan that can bypass the anti-virus and firewall programs, as well as be used to maintain a persistent connection with the victim.

30. On completion of this lab, launch Task Manager, look for the server.exe (32 bit) process, and click End task on the Windows Server 2016 machine.

31. This concludes the demonstration of how to hide a Trojan using SwayzCryptor to make it undetectable to various anti-virus programs.

32. Close all open windows on both the Windows 10 and Windows Server 2016 virtual machines.

33. Turn off the Windows Server 2016 virtual machine.