Module 07: 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 1: Gain Access to the Target System using Trojans

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.

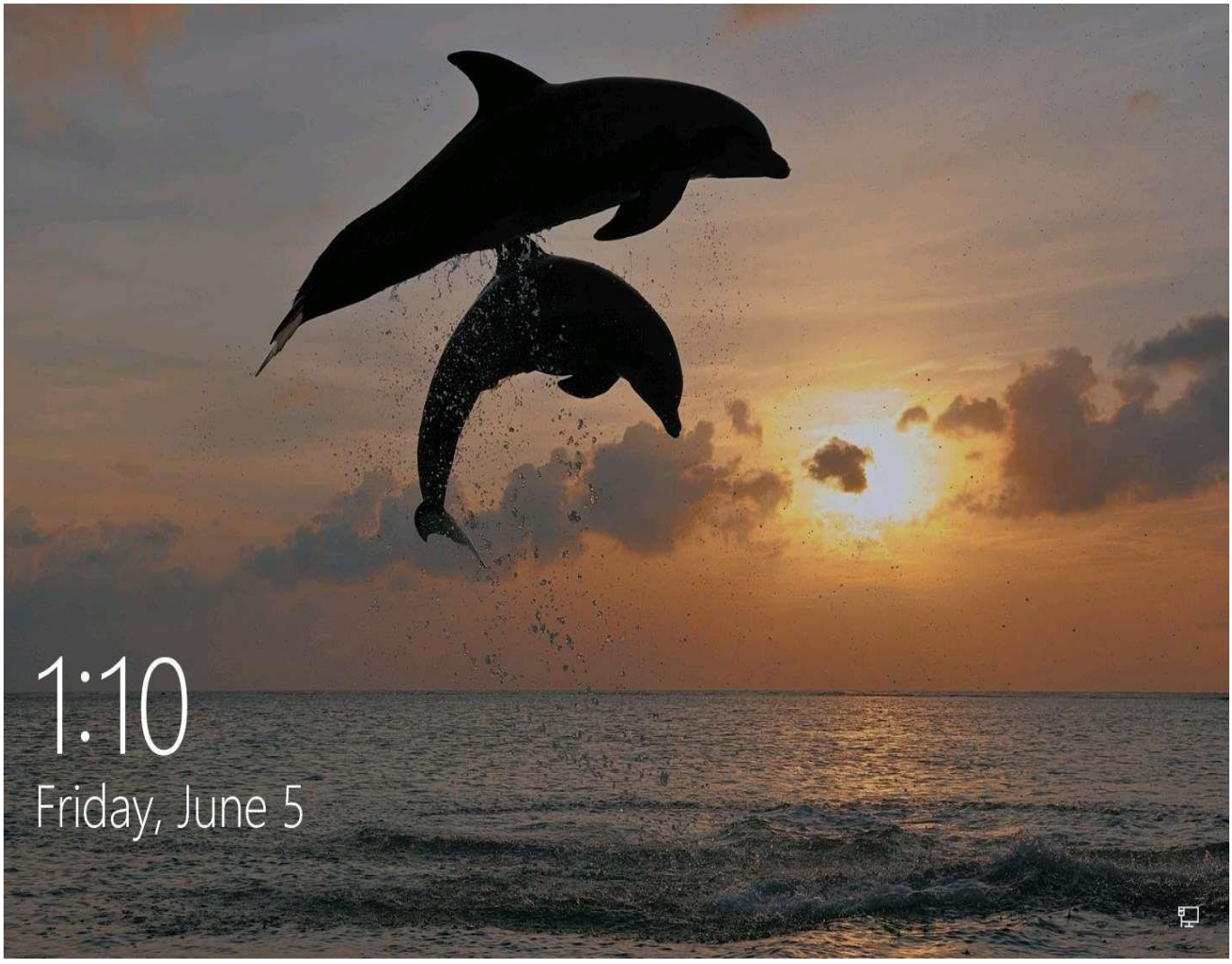
This RAT can be used to control Botnets (networks of computers), allowing the attacker to update, uninstall, disconnect, restart, and close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the Command and Control 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 lab. However, the actual process of creating the server and the client is the same, as shown in this lab.
In this lab task, we will use the **Windows 10** (**10.10.10.10**) machine as the attacker machine and the **Windows Server 2016** (**10.10.10.16**) machine as the victim machine.

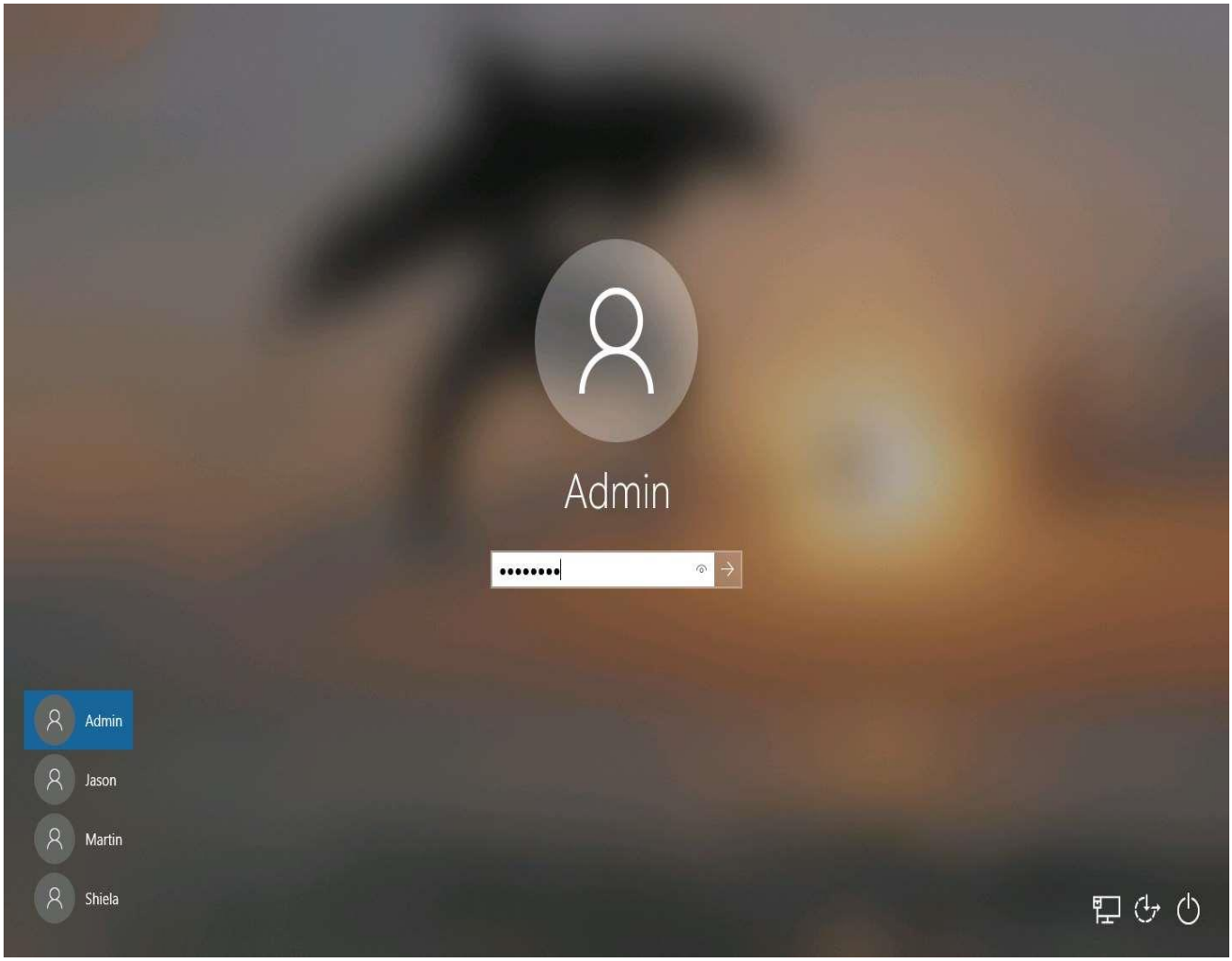
1. By default, **Windows 10** machine selected, click Ctrl+Alt+Delete.

Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.



2. By default, **Admin** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

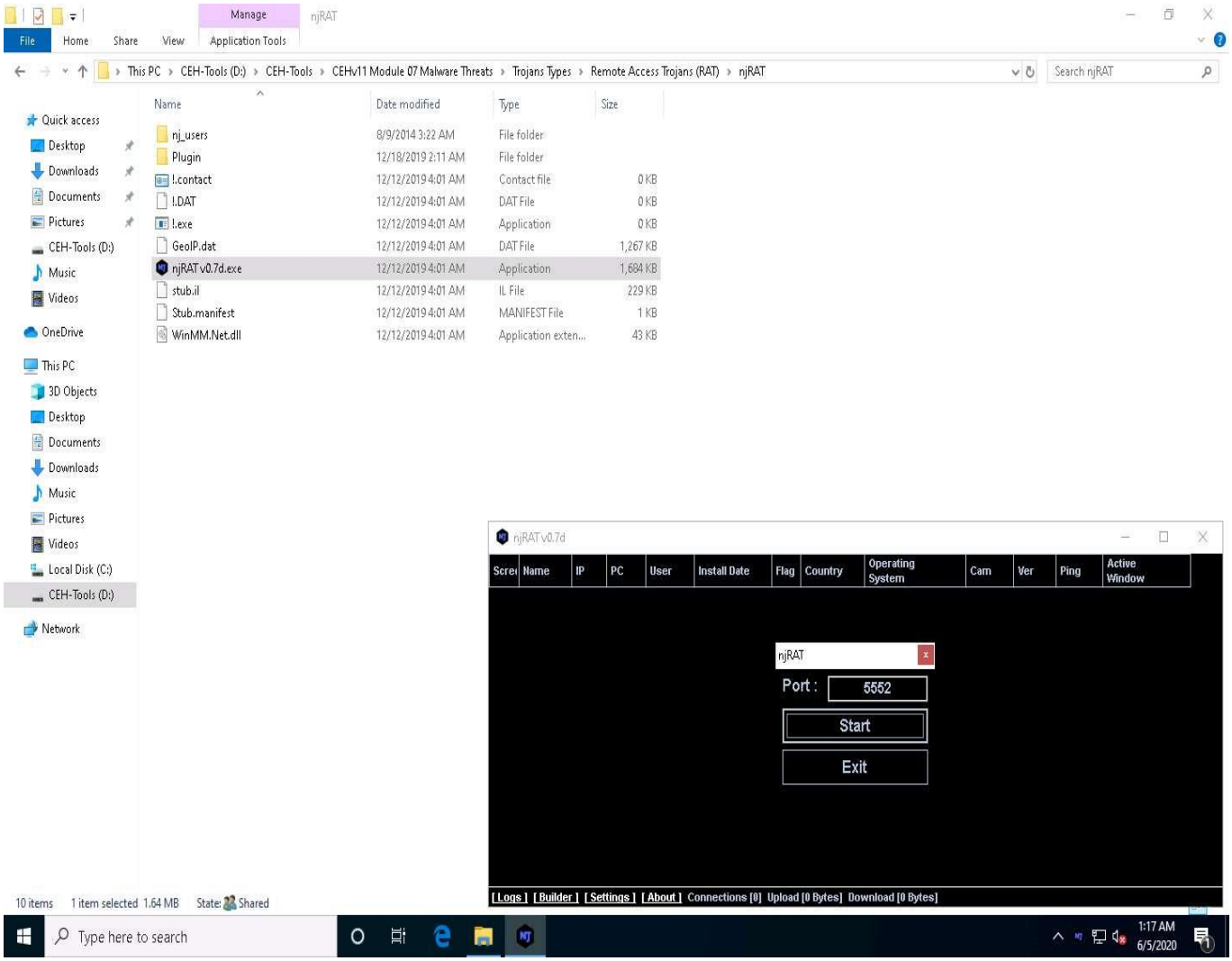
Alternatively, you can also click **Pa$$w0rd** under **Windows 10 **machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.
Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



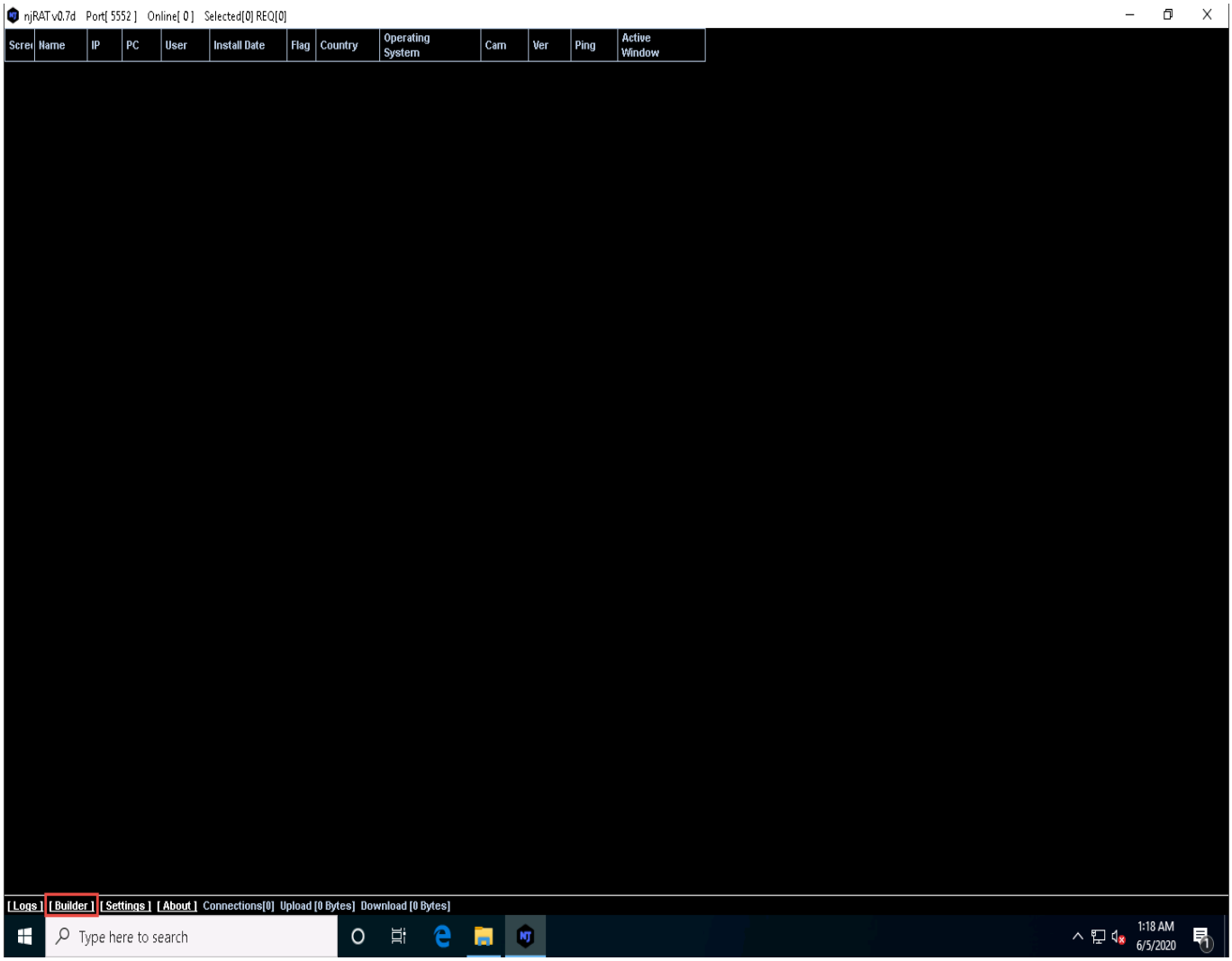
3. ☐ Navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe**.

If a **User Account Control** window appears, click **Yes**.
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.

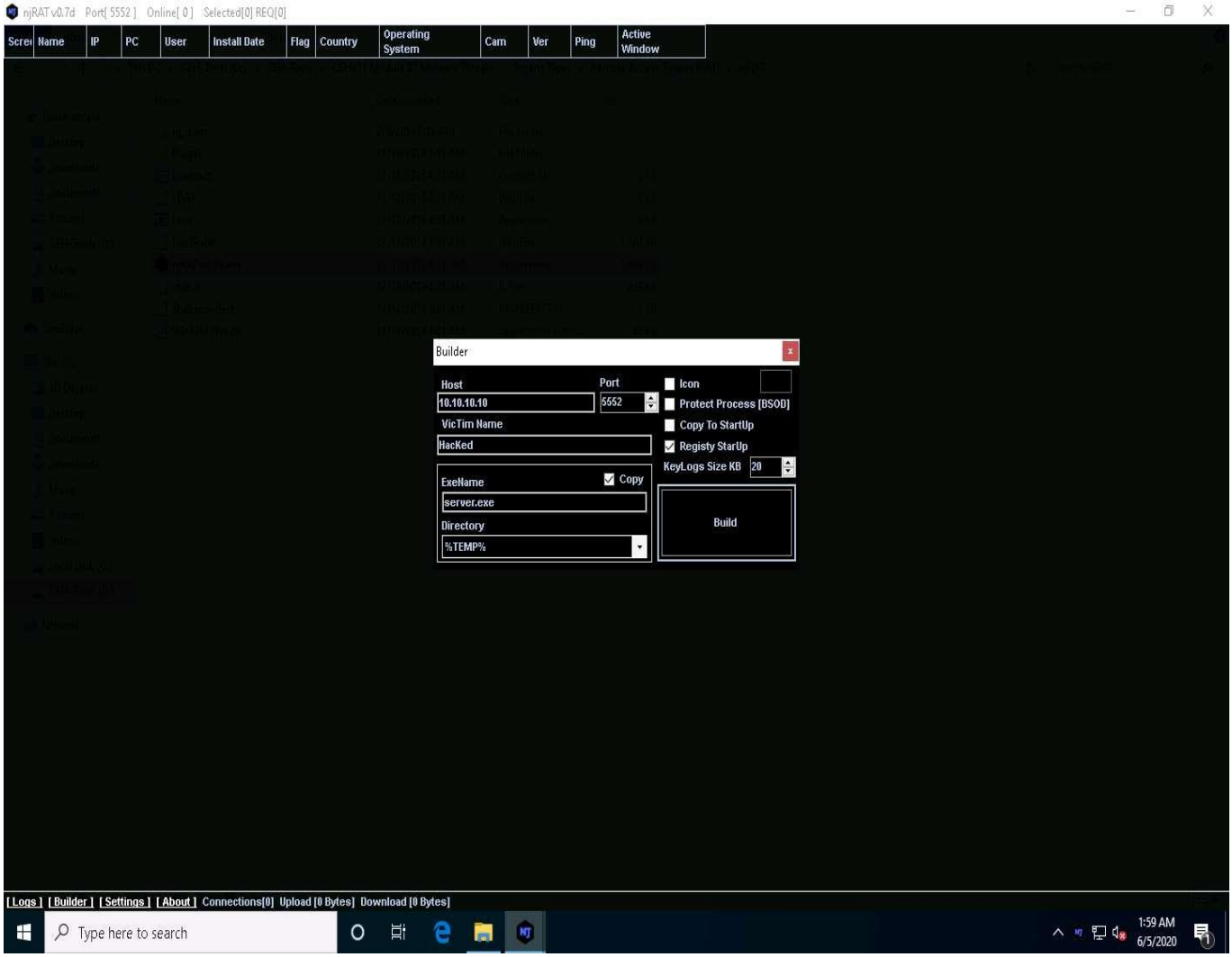


6. The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.

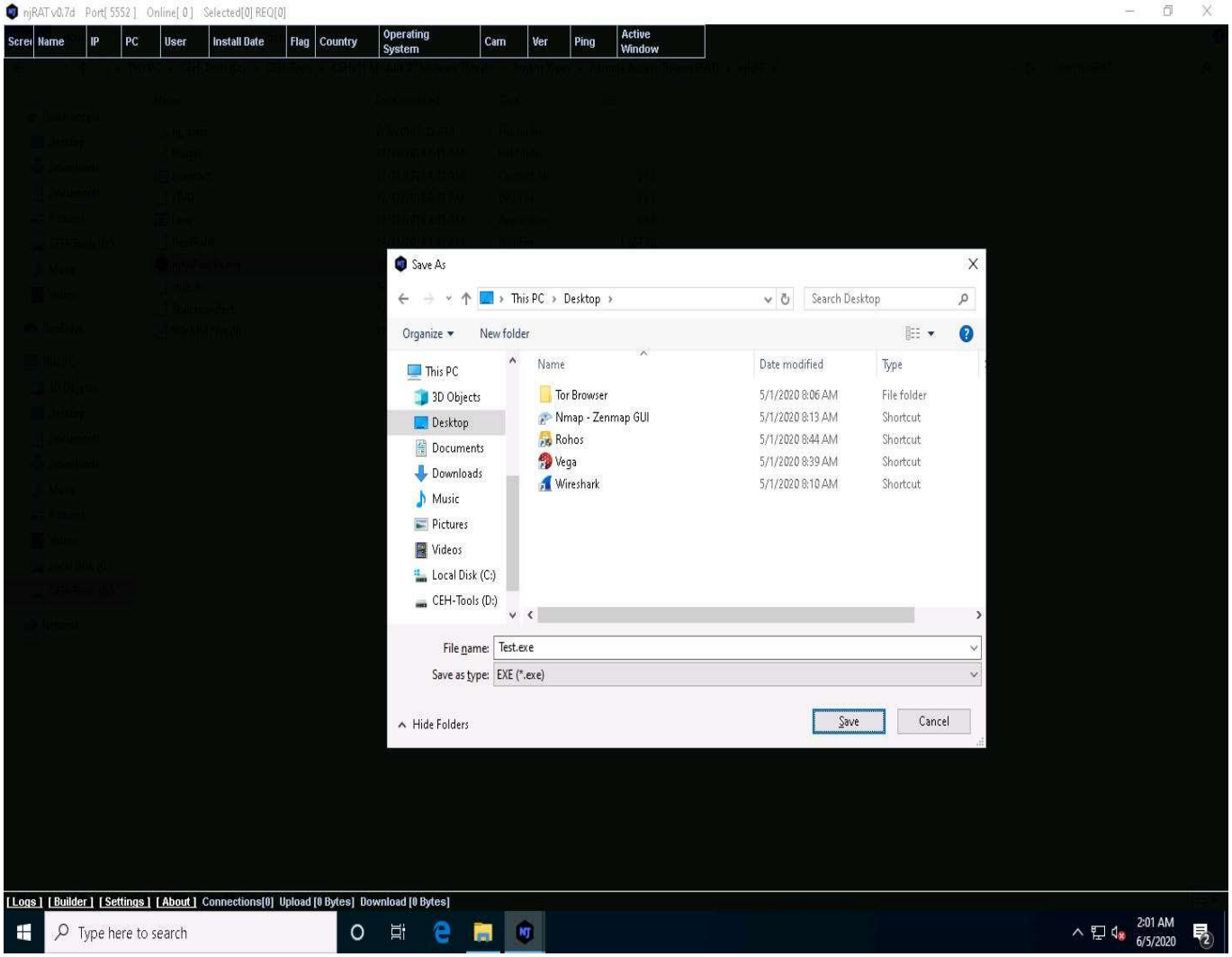


7. The **Builder** dialog-box appears; enter the IP address of the **Windows 10** (attacker machine) machine in the **Host** field, check the option **Registy StarUp**, leave the other settings to default, and click **Build**.

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



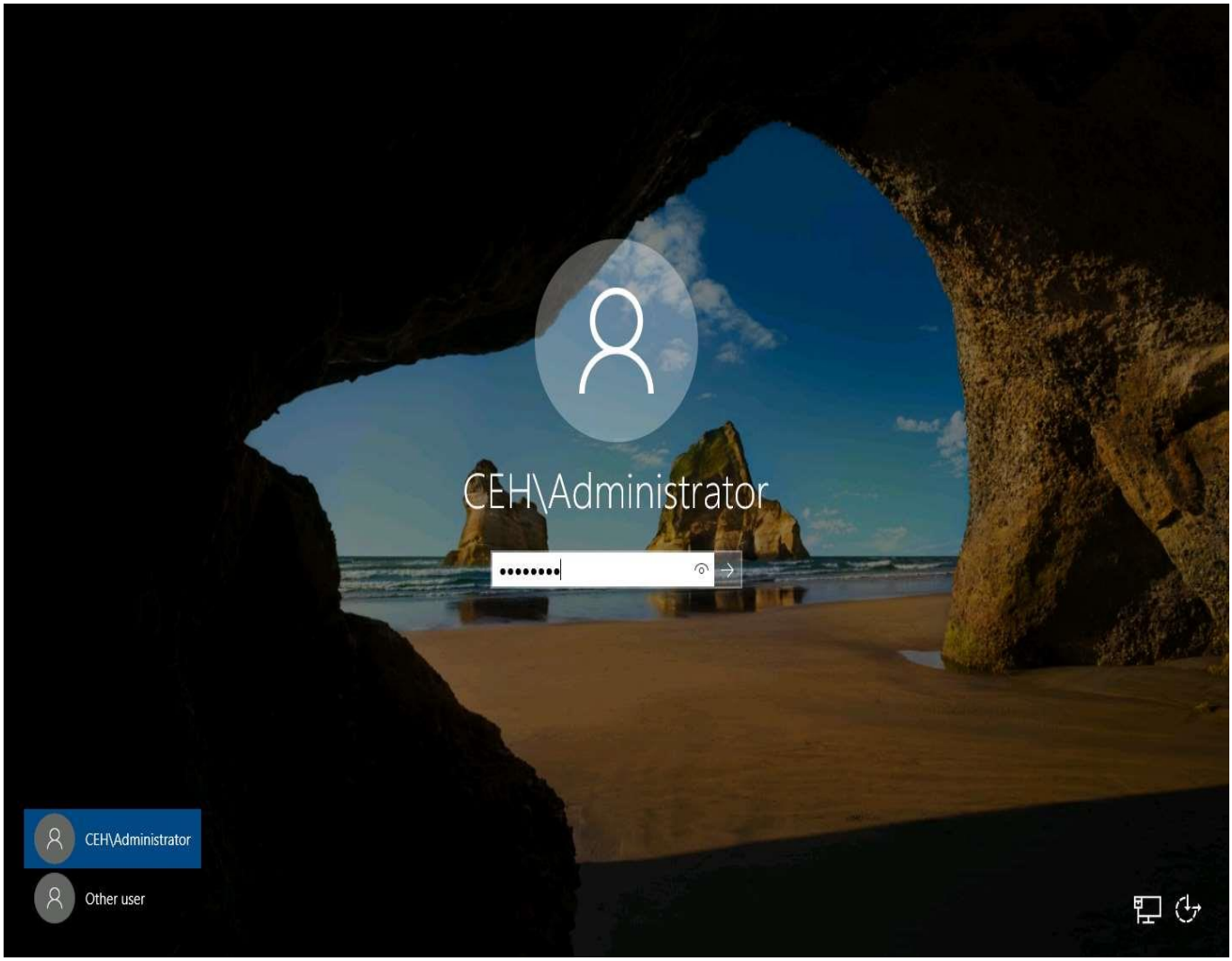
8. ☐ The **Save As** window appears; specify a location to store the server, rename it, and click **Save**.
9. ☐ In this lab, the destination location chosen is **Desktop**, and the file is named **Test.exe**.



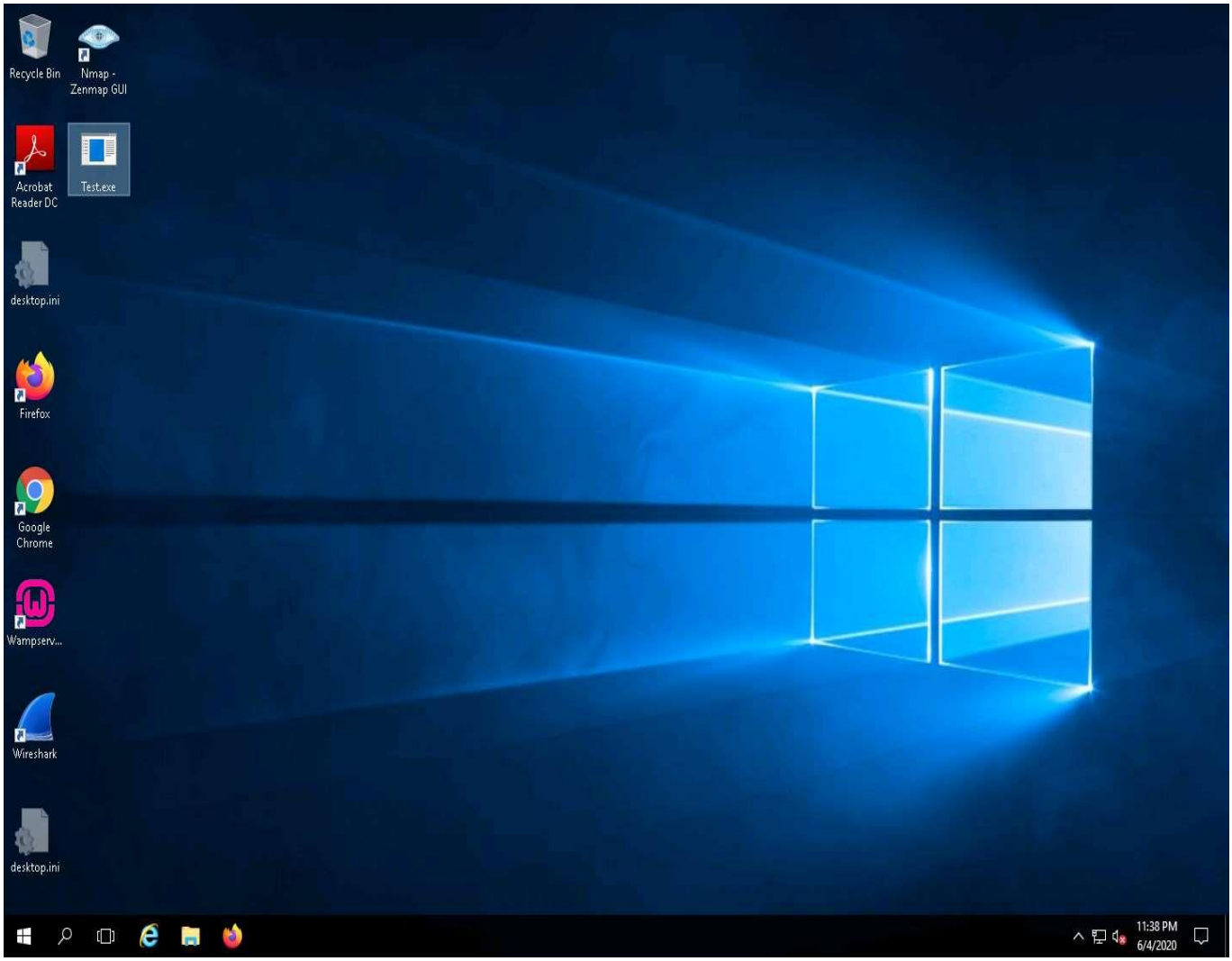
10. ☐ Once the server is created, the **DONE!** pop-up appears; click **OK**.
11. ☐ Now, use any technique to send this server to the intended target through email or any other source (in real-time, attackers send this server to the victim).

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

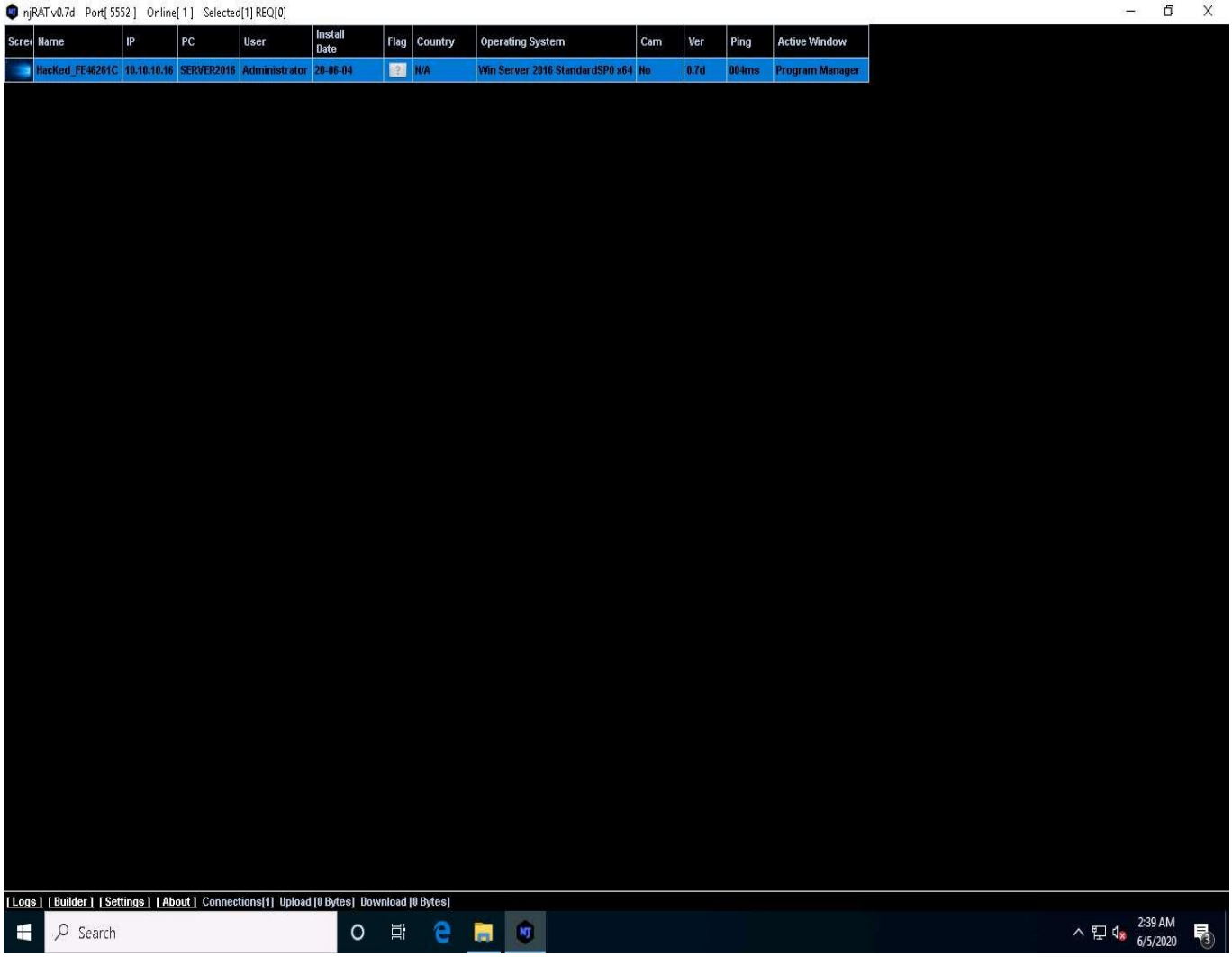
12. ☐ Click Windows Server 2016 to switch to the **Windows Server 2016** machine. Click Ctrl+Alt+Delete to activate the machine, by default, **CEH\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.



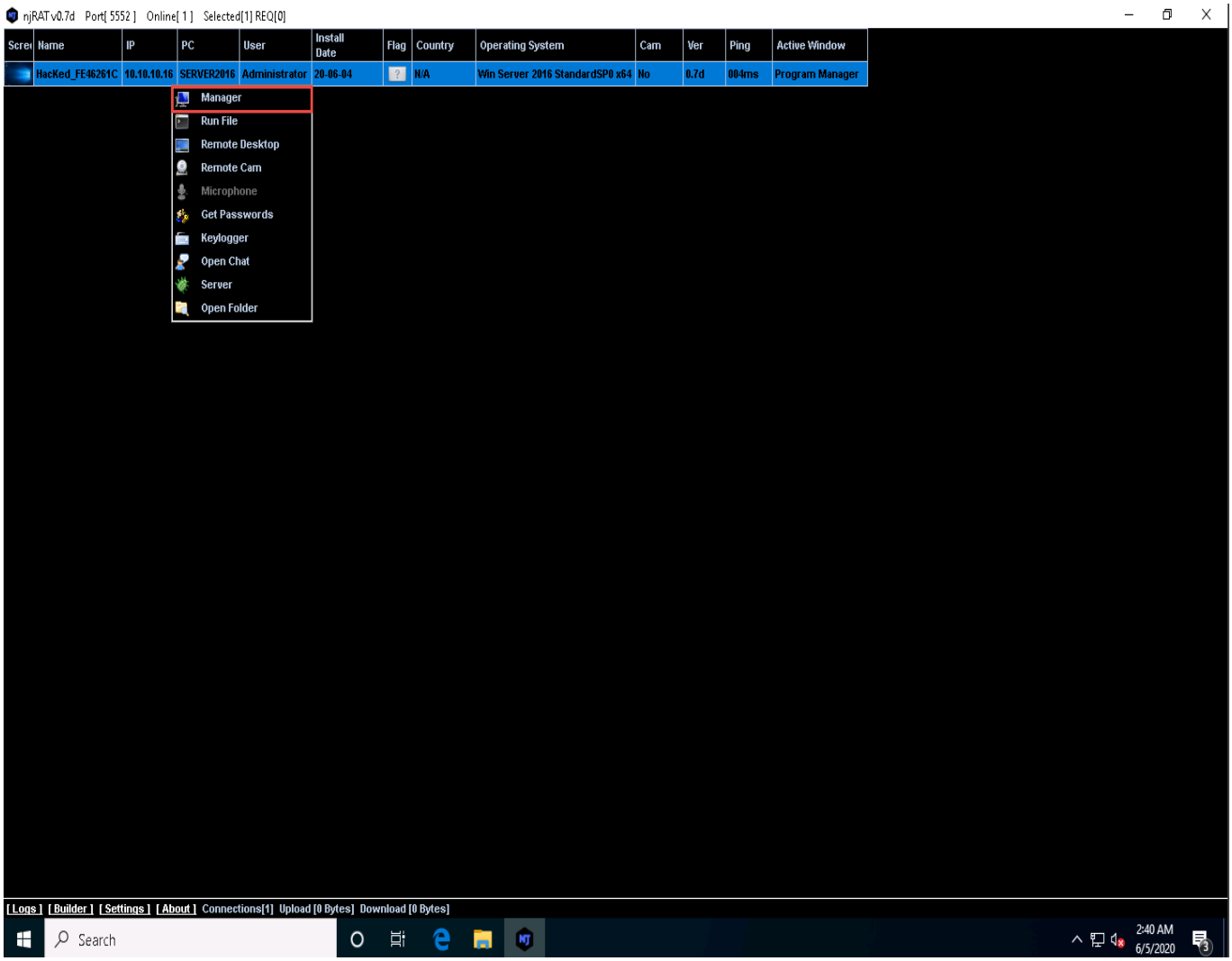
13. ☐ Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**Test.exe**) onto the **Desktop** of **Windows Server 2016**.
14. ☐ Here, you are acting both as an **attacker** who logs into the **Windows 10** machine to create a malicious server, and as a **victim** who logs into the **Windows Server 2016** machine and downloads the server.
15. ☐ Double-click the server (**Test.exe**) to run this malicious executable.



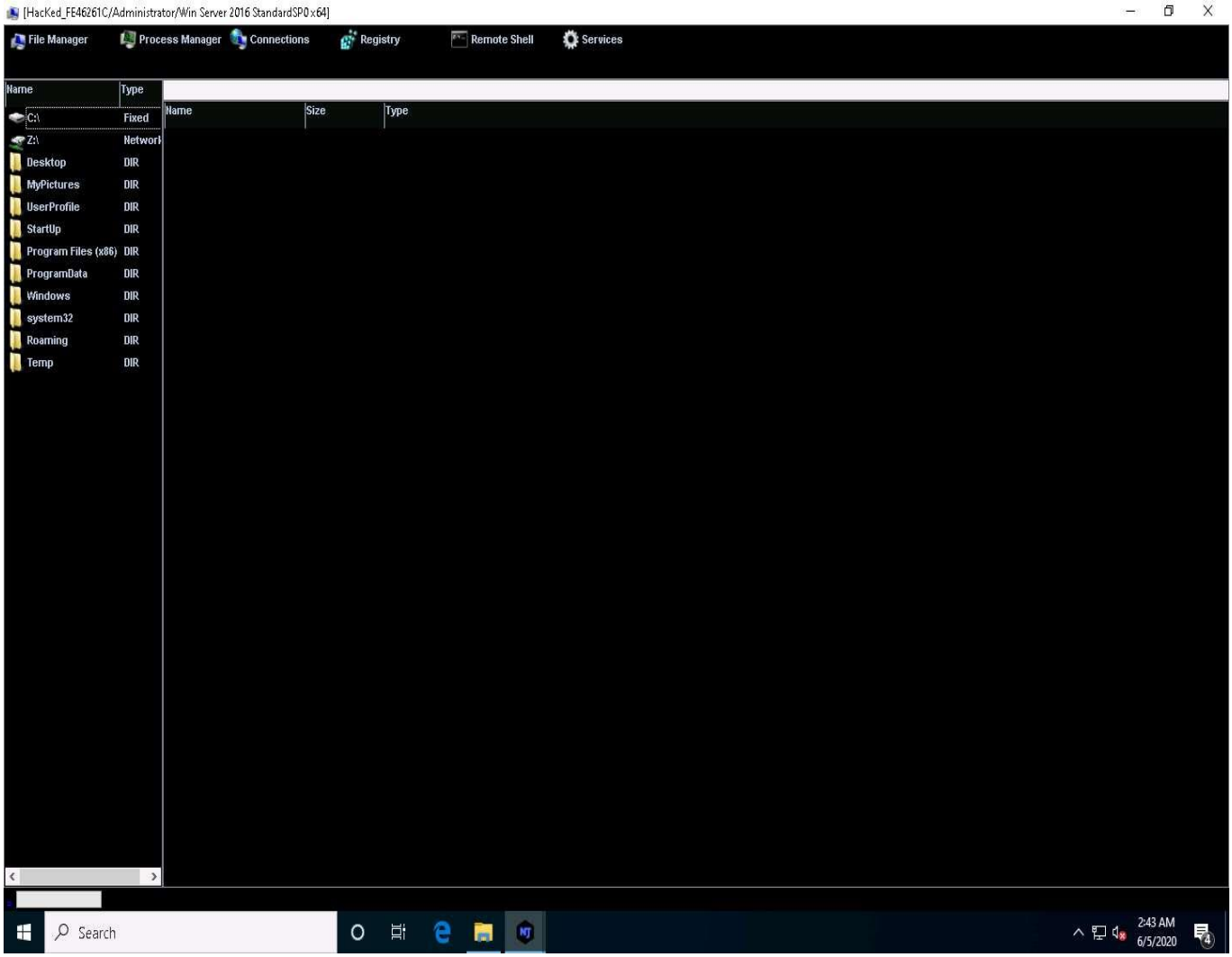
16. Click Windows 10 to switch back to the **Windows 10** machine. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in **Windows 10** establishes a persistent connection with the victim machine, as shown in the screenshot.



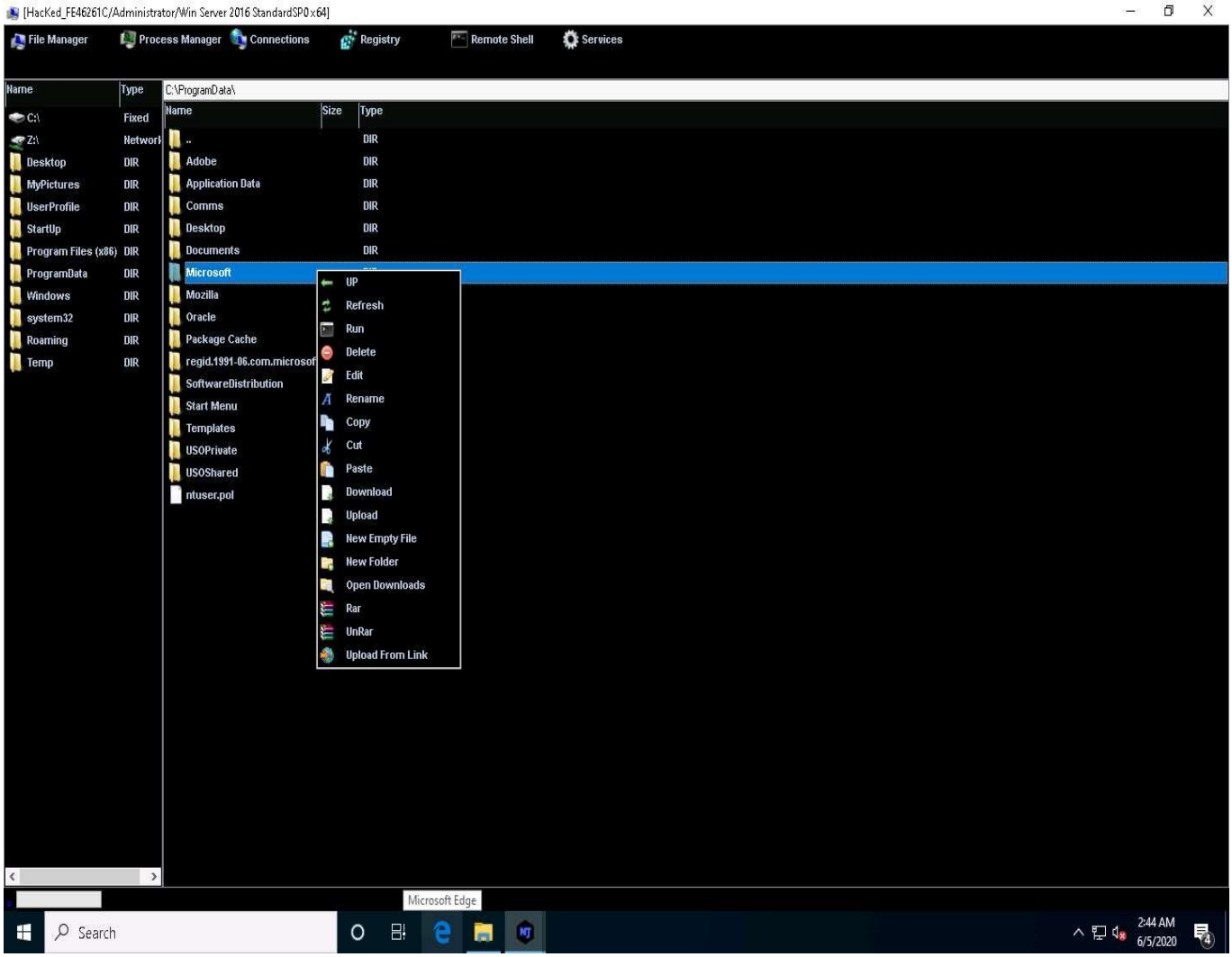
17. ☐ Unless the attacker working on the **Windows 10** machine disconnects the server on their own, the victim machine remains under their control.
18. ☐ The GUI displays the machine's basic details such as the IP address, User name, and Type of Operating system.
19. ☐ Right-click on the detected victim name and click **Manager**.



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

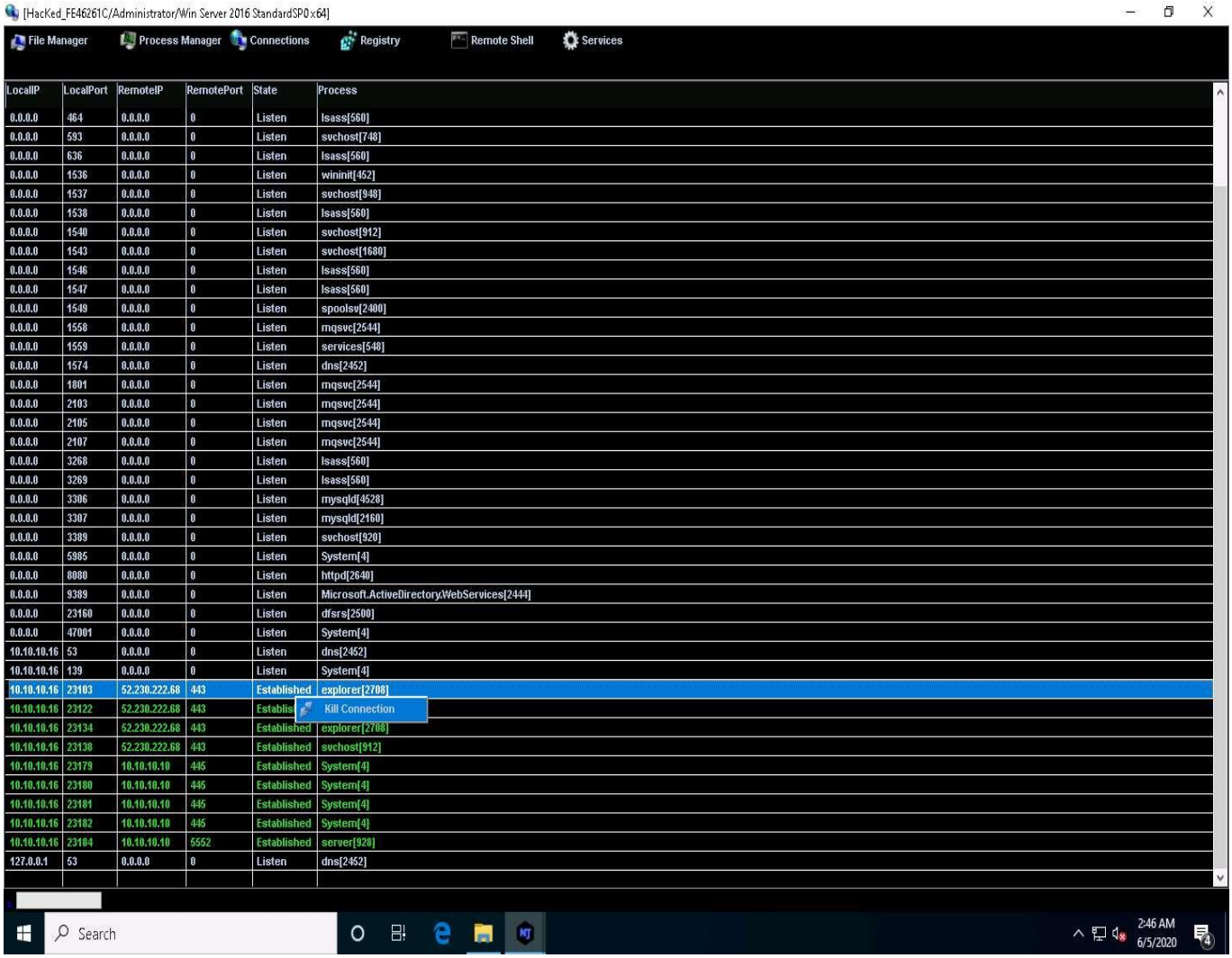


21. Double-click any directory in the left pane (here, **ProgramData**); all its associated files and directories are displayed in the right pane. You can right-click a selected directory and manipulate it using the contextual options.

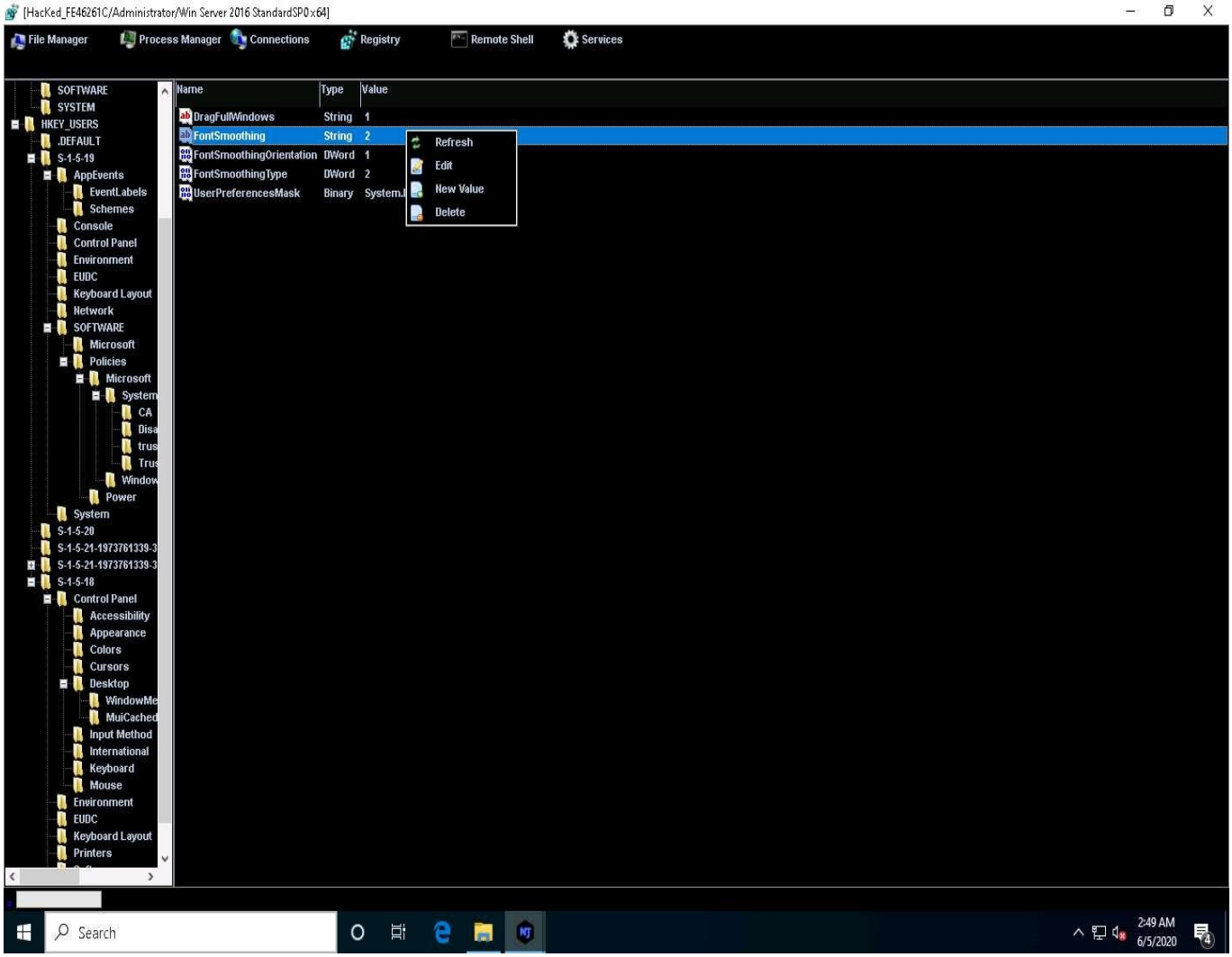


22. Click on **Process Manager**. You will be redirected to the Process Manager, where you can right-click on a selected process and perform actions such as **Kill**, **Delete**, and **Restart**.

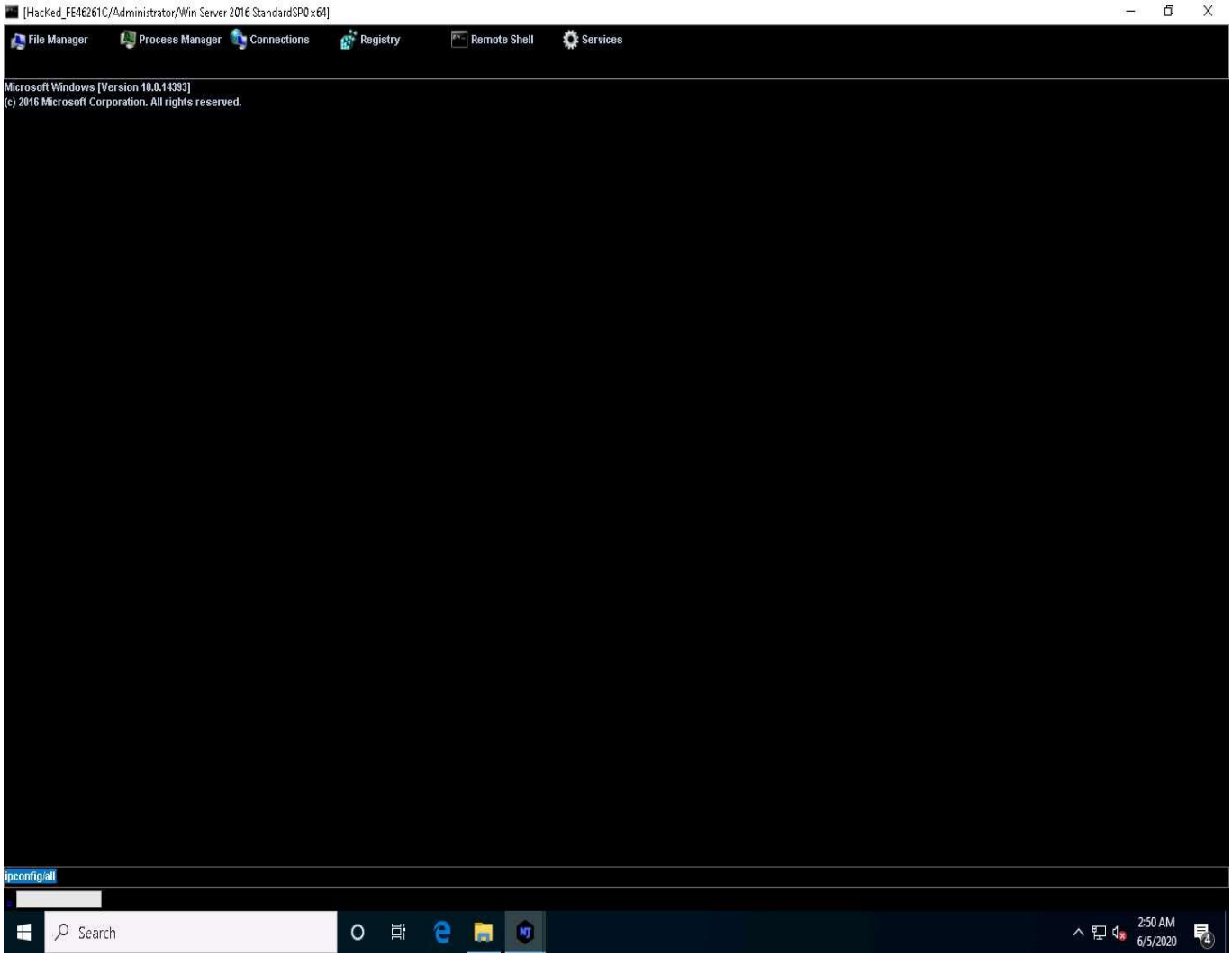
23. Click on **Connections**, select a specific connection, right-click on it, and click **Kill Connection**. This kills the connection between two machines communicating through a particular port.



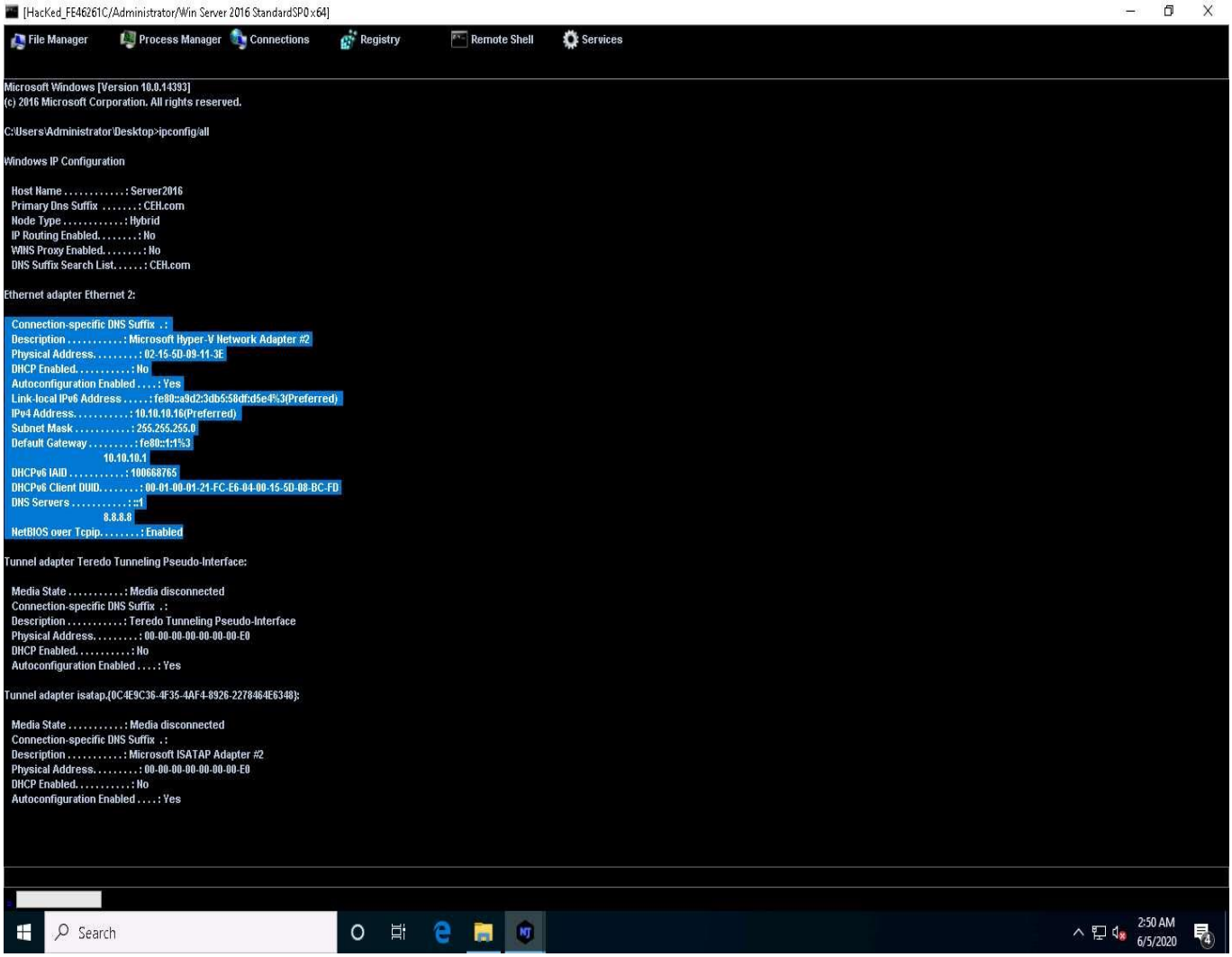
24. ☐ Click on **Registry**, choose a registry directory from the left pane, and right-click on its associated registry files.
25. ☐ A few options appear for the files; you can use these to manipulate them.



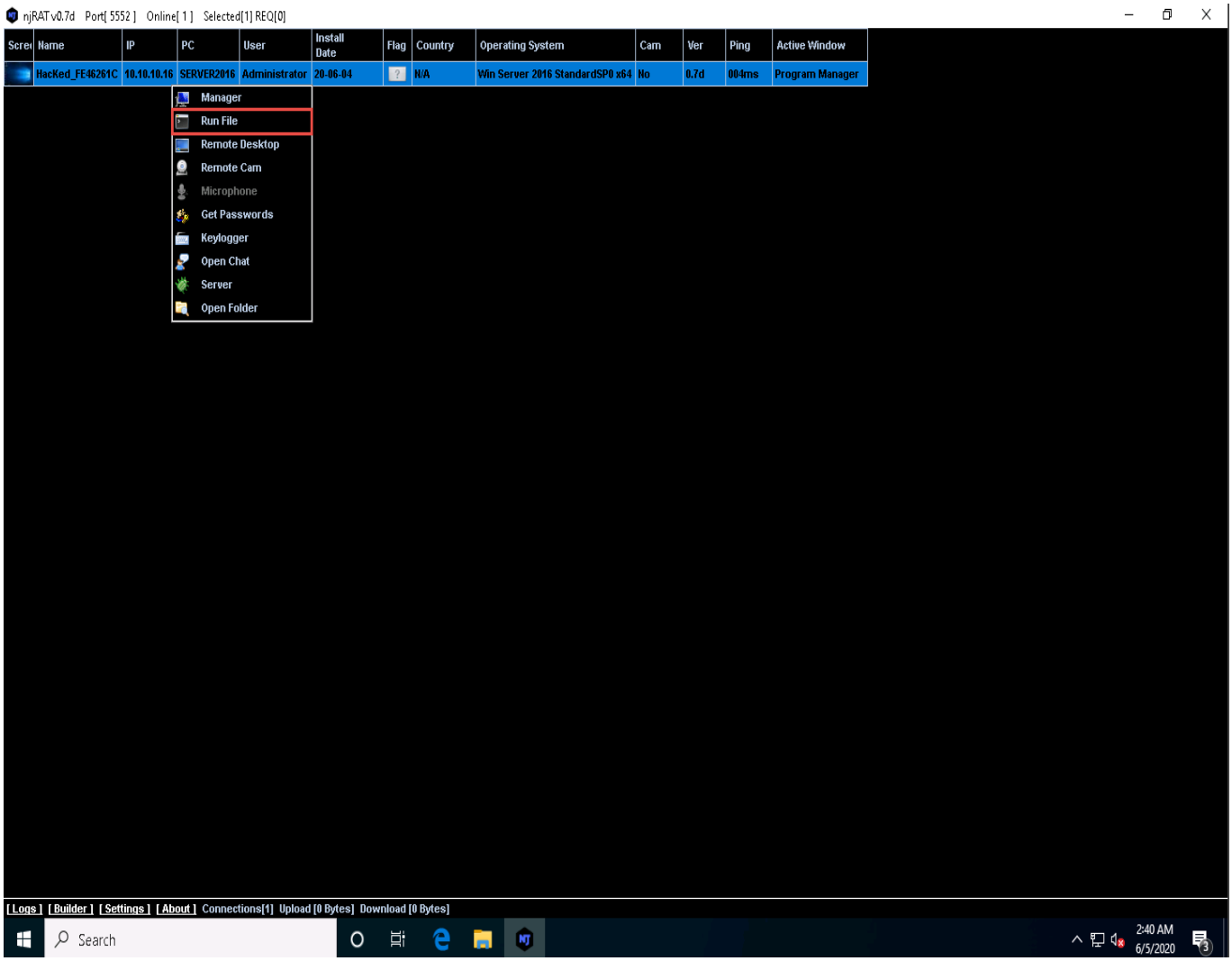
26. ☐ Click **Remote Shell**. This launches a remote command prompt for the victim machine (**Windows Server 2016**).
27. ☐ Type the command **ipconfig/all** and press **Enter**.



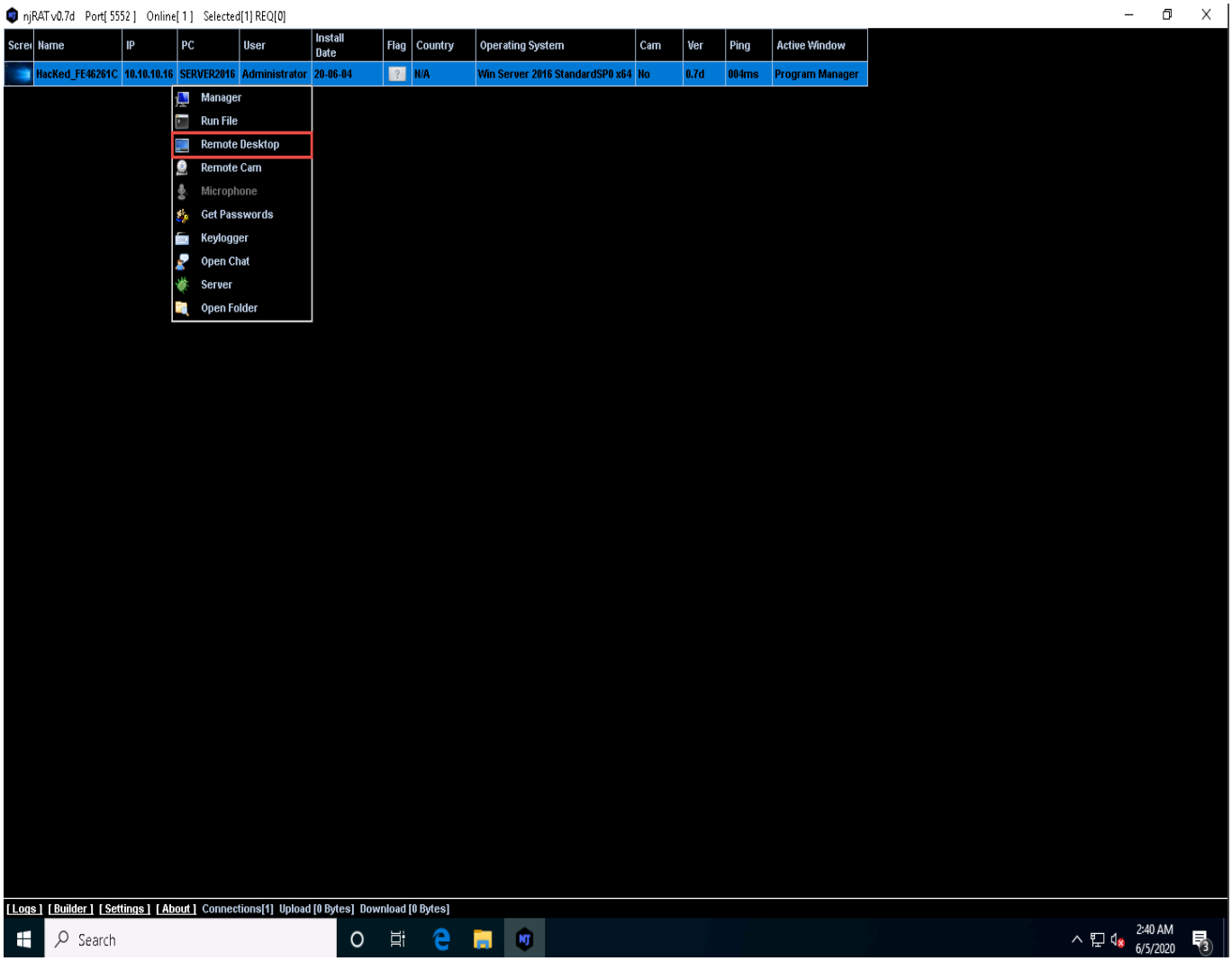
28. This displays all interfaces related to the victim machine, as shown in the screenshot.



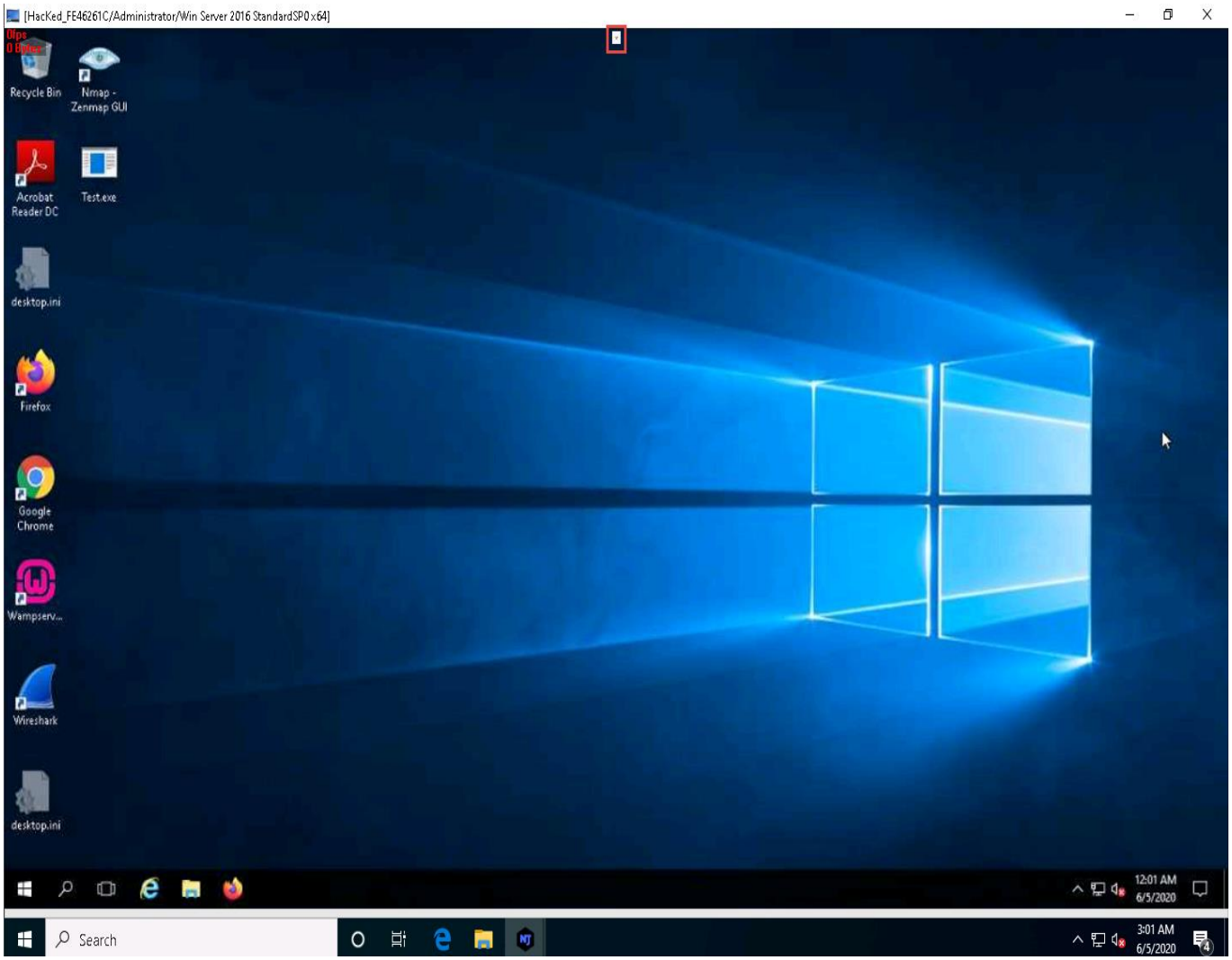
29. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine.
30. In the same way, click **Services**. You will be able to view all services running on the victim machine. In this section, you can use options to **start**, **pause**, or **stop** a service.
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.



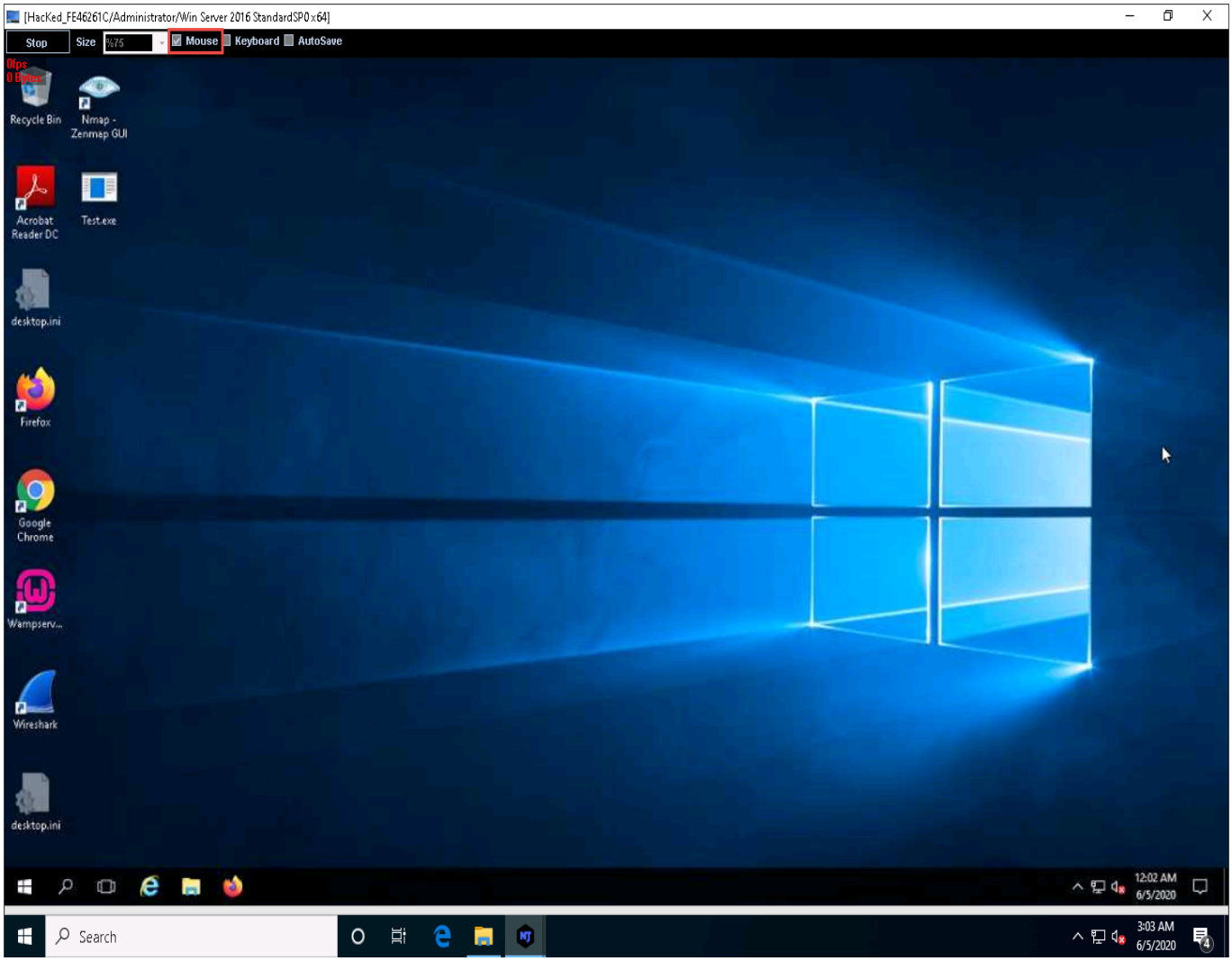
33. Right-click on the victim name, and then select **Remote Desktop**.



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.



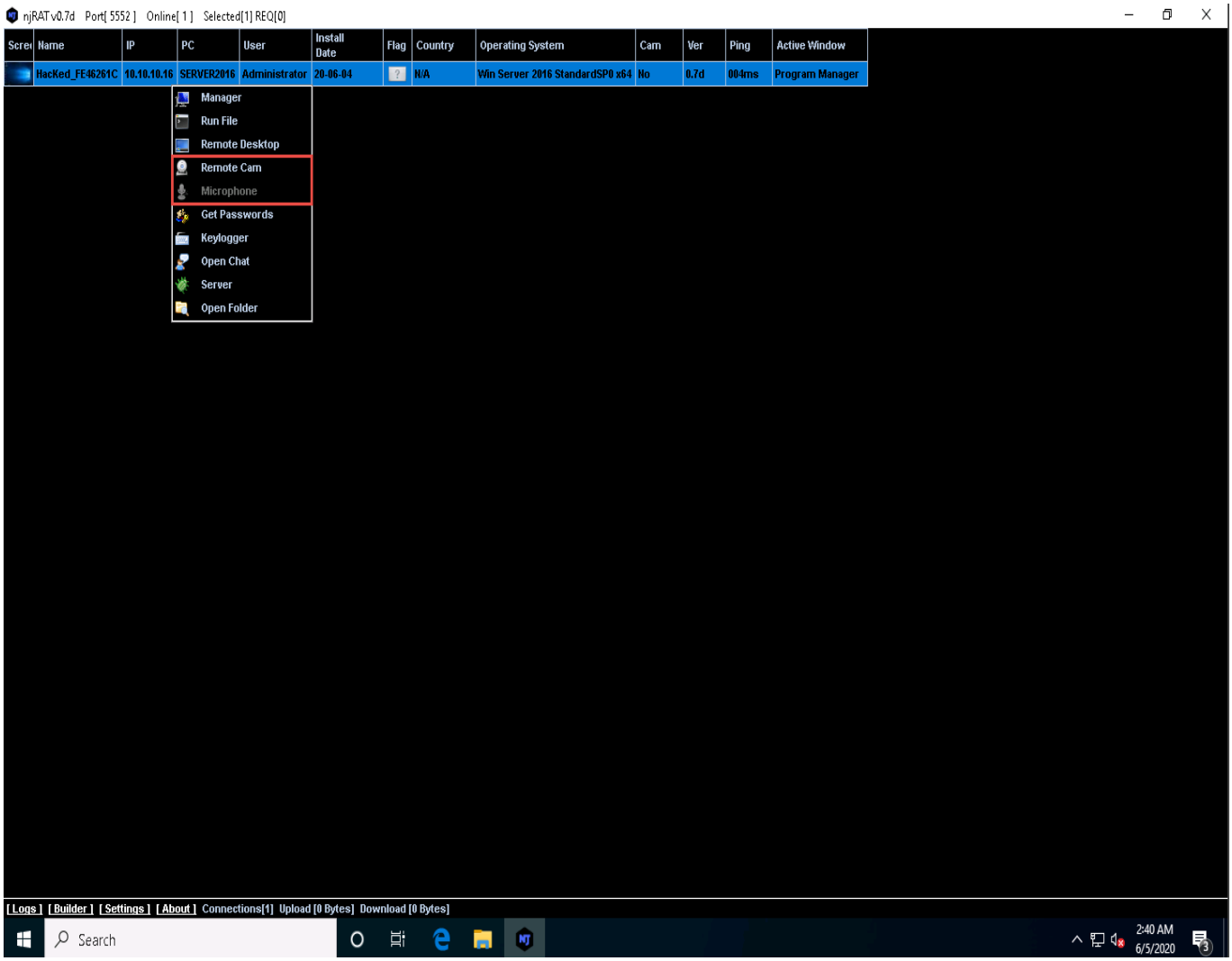
36. ☐ A remote desktop control panel appears; check the **Mouse** option.



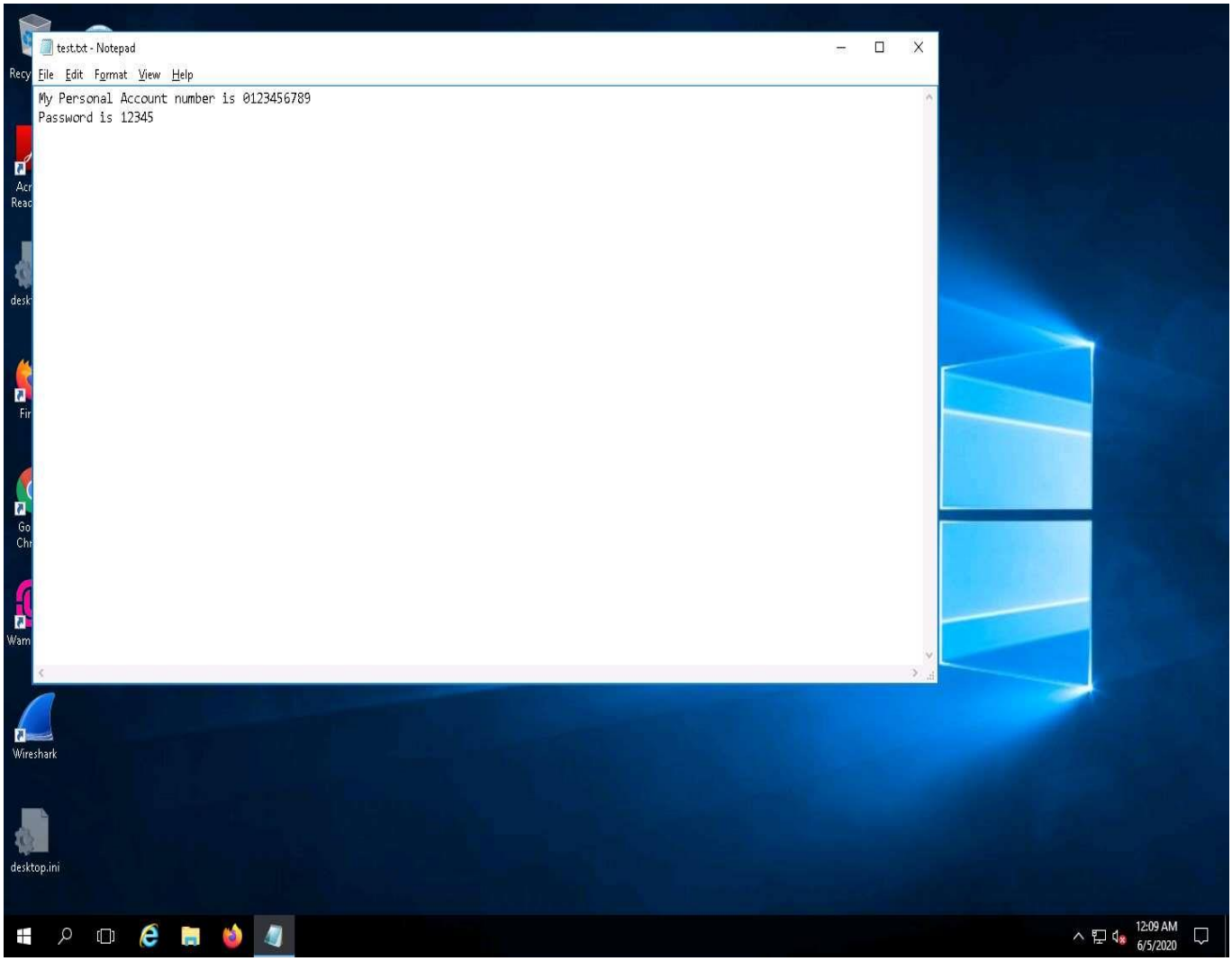
37. ☐ Now, you will be able to remotely interact with the victim machine using the mouse.

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

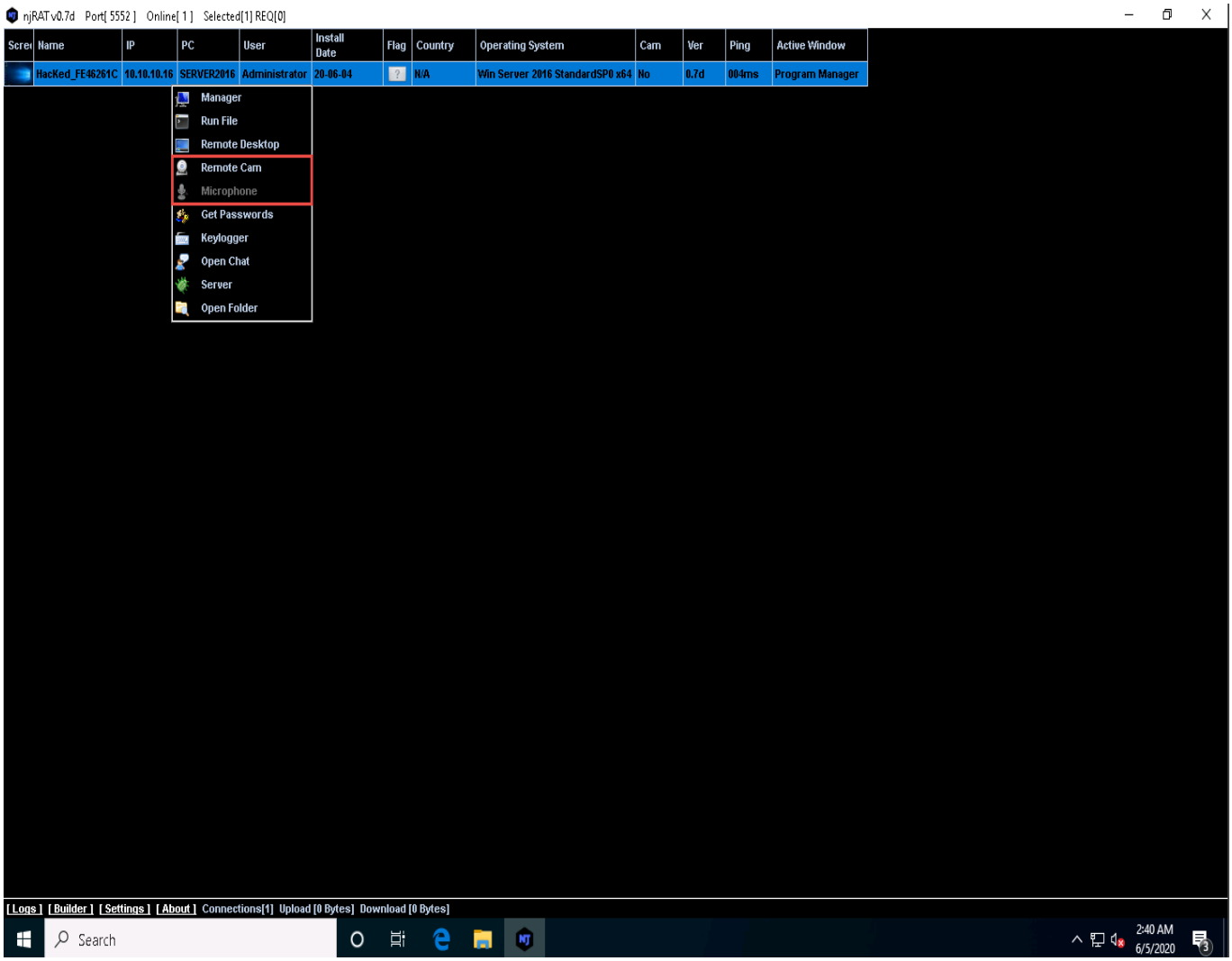
38. ☐ On completing the task, close the **Remote Desktop** window.
39. ☐ In the same way, right-click on the victim name, and select **Remote Cam** and **Microphone** to spy on them and track voice conversations.



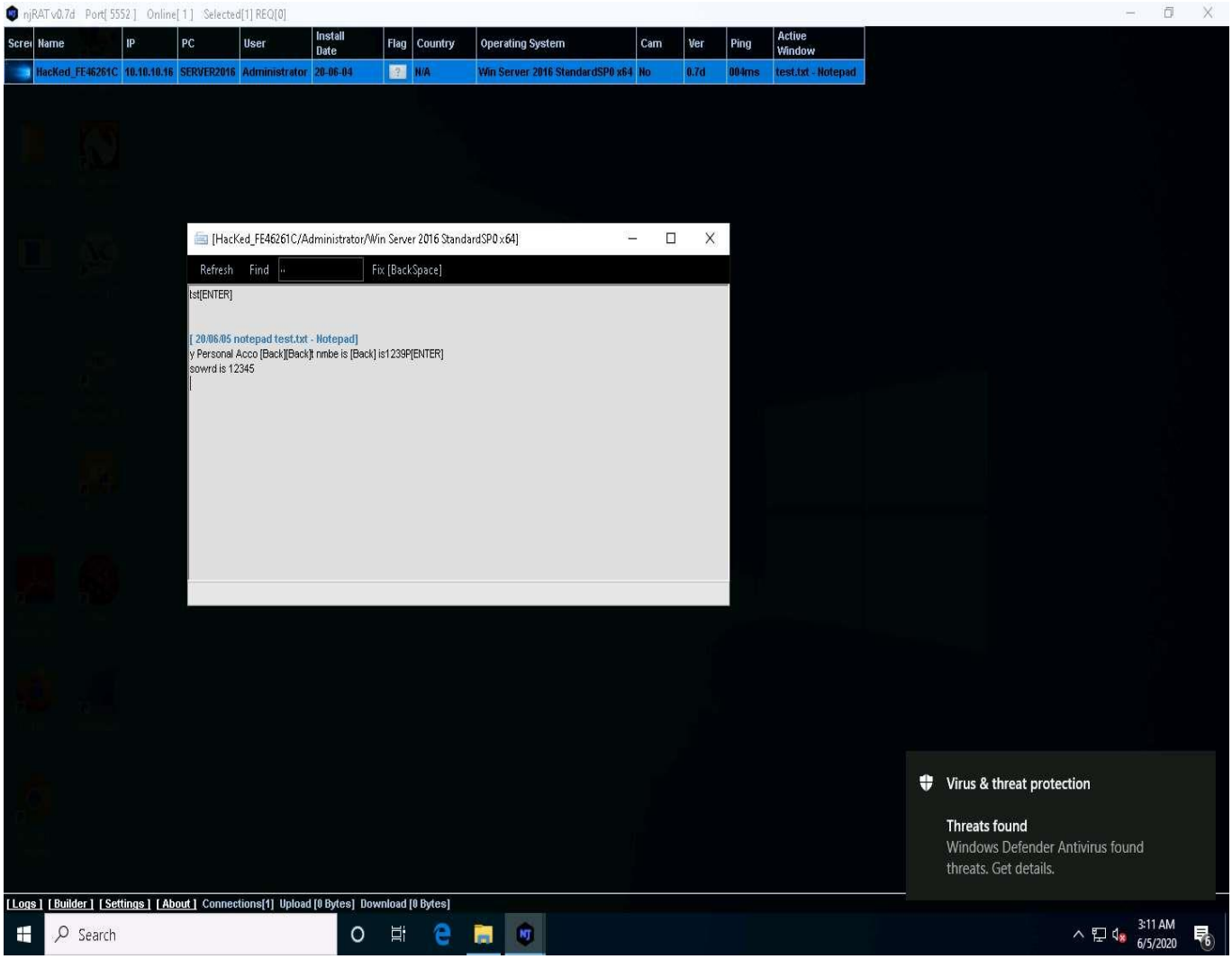
40. Click Windows Server 2016 to switch to the **Windows Server 2016** machine. Assume that you are a legitimate user and perform a few activities such as logging into any website or typing some text in text documents.



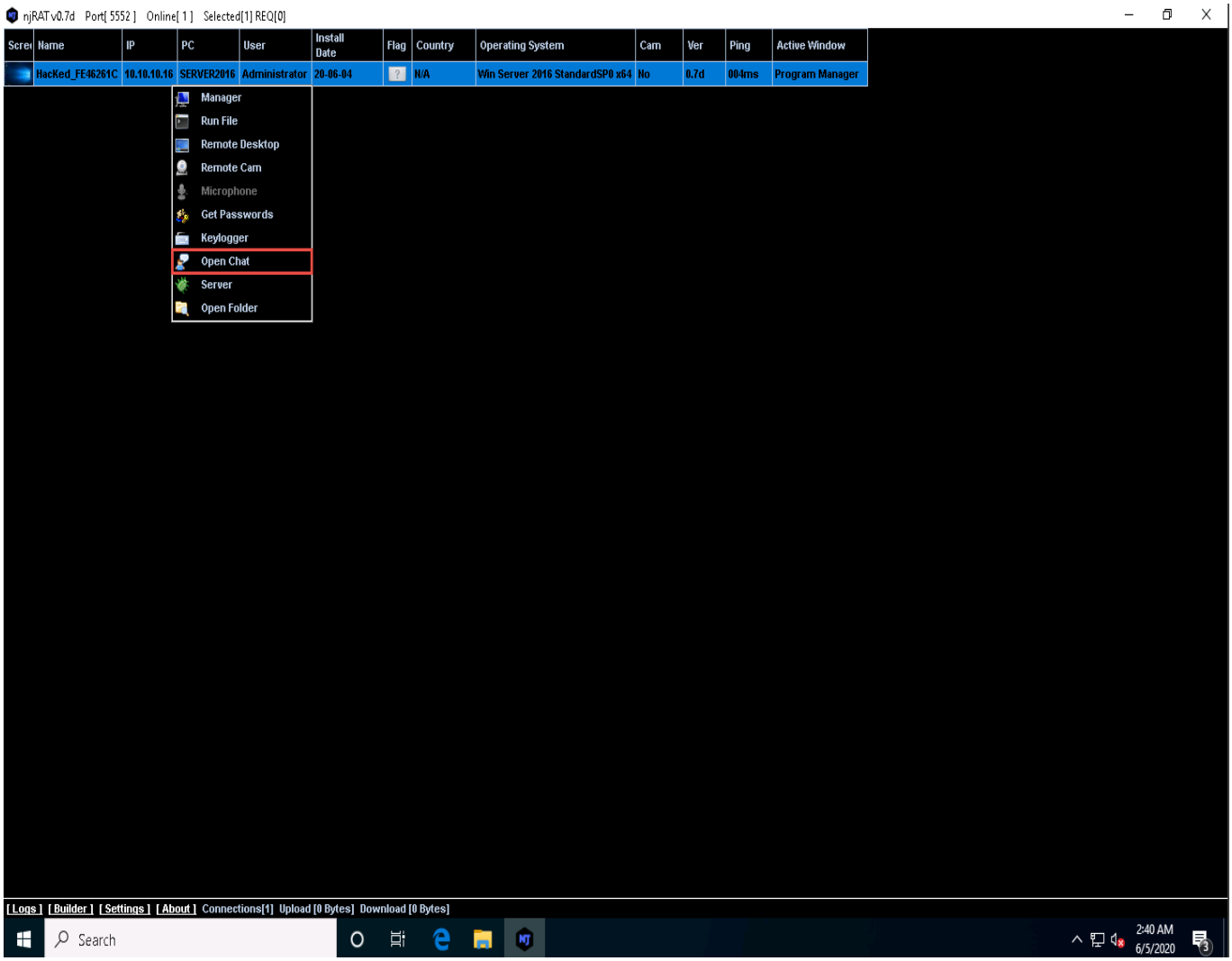
41. ☐ Click Windows 10 to switch back to the **Windows 10** machine, right-click on the victim name, and click **Keylogger**.



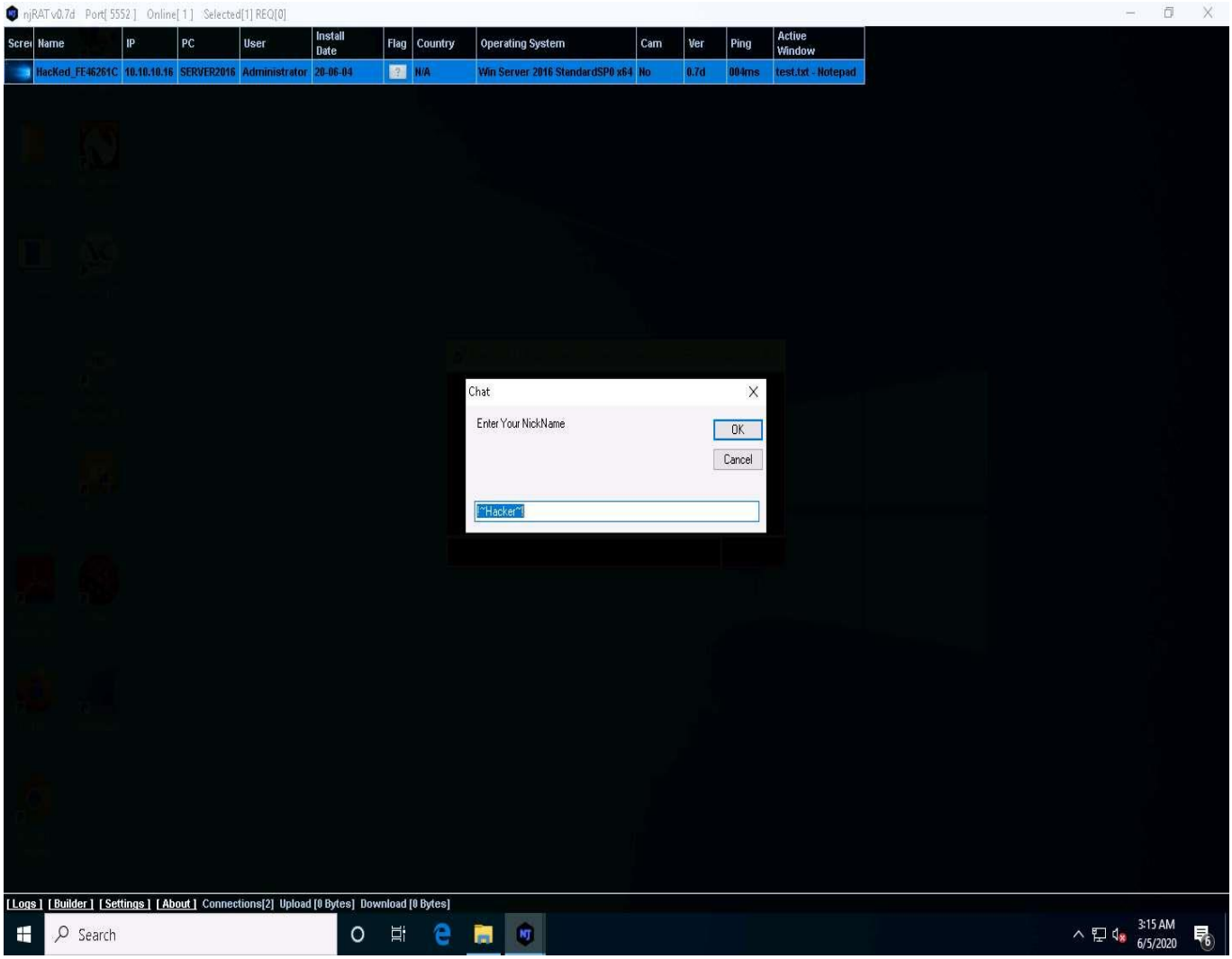
42. ☐ The Keylogger window appears; wait for the window to load.
43. ☐ The window displays all the keystrokes performed by the victim on the **Windows Server 2016** machine, as shown in the screenshot.



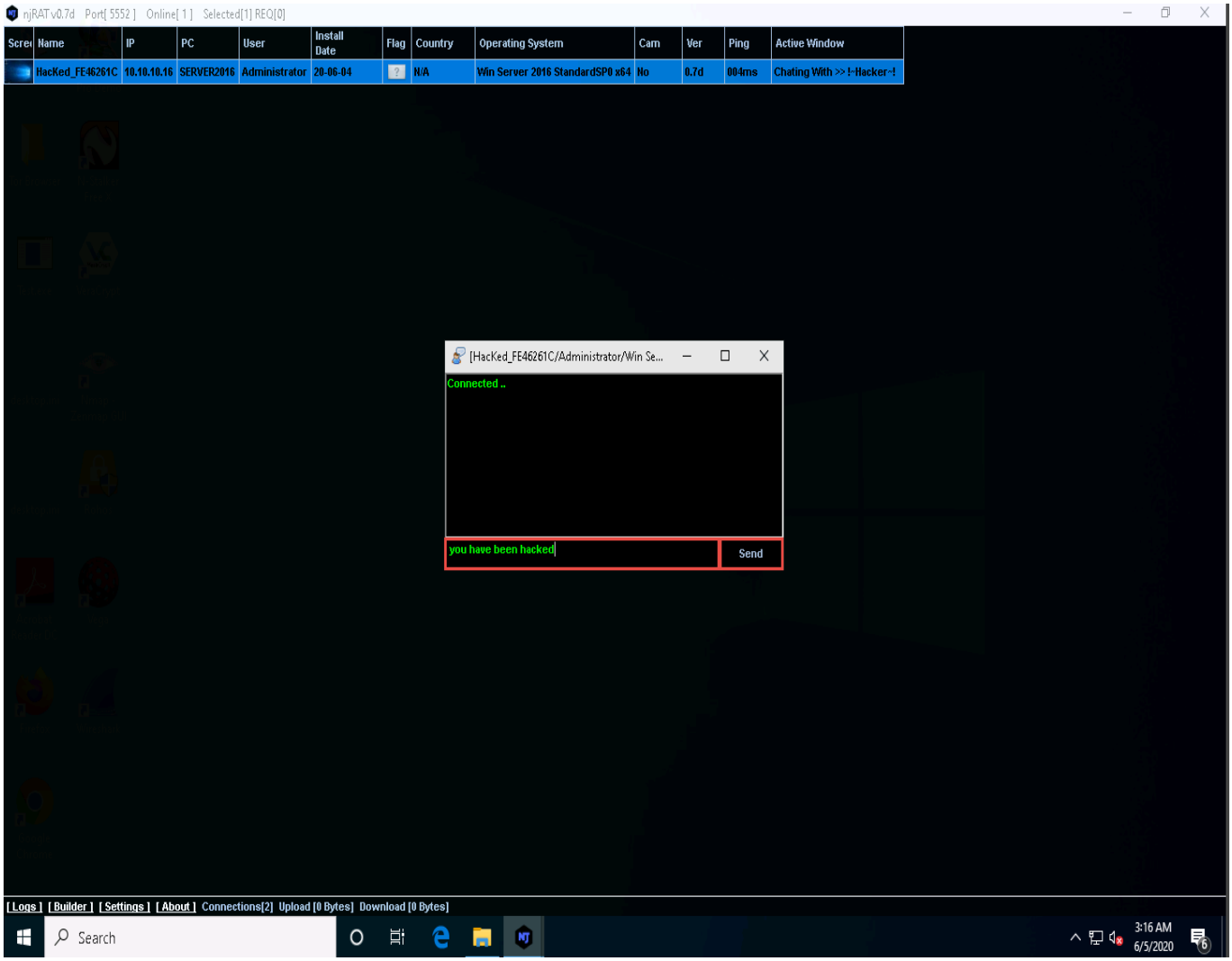
44. ☐ Close the **Keylogger** window.
45. ☐ Right-click on the victim name, and click **Open Chat**.



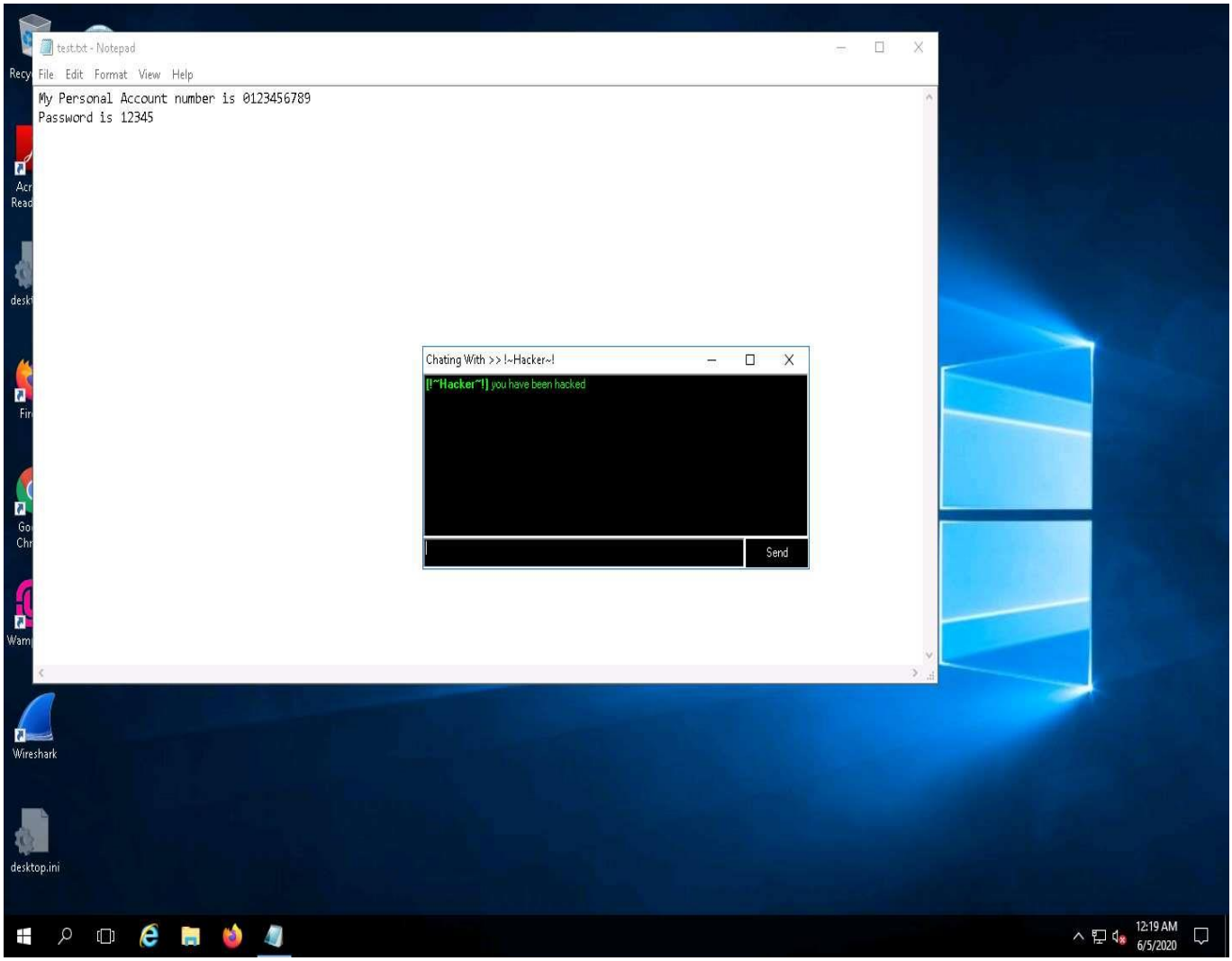
46. A **Chat** pop-up appears; enter a nickname (here, **Hacker**) and click **OK**.



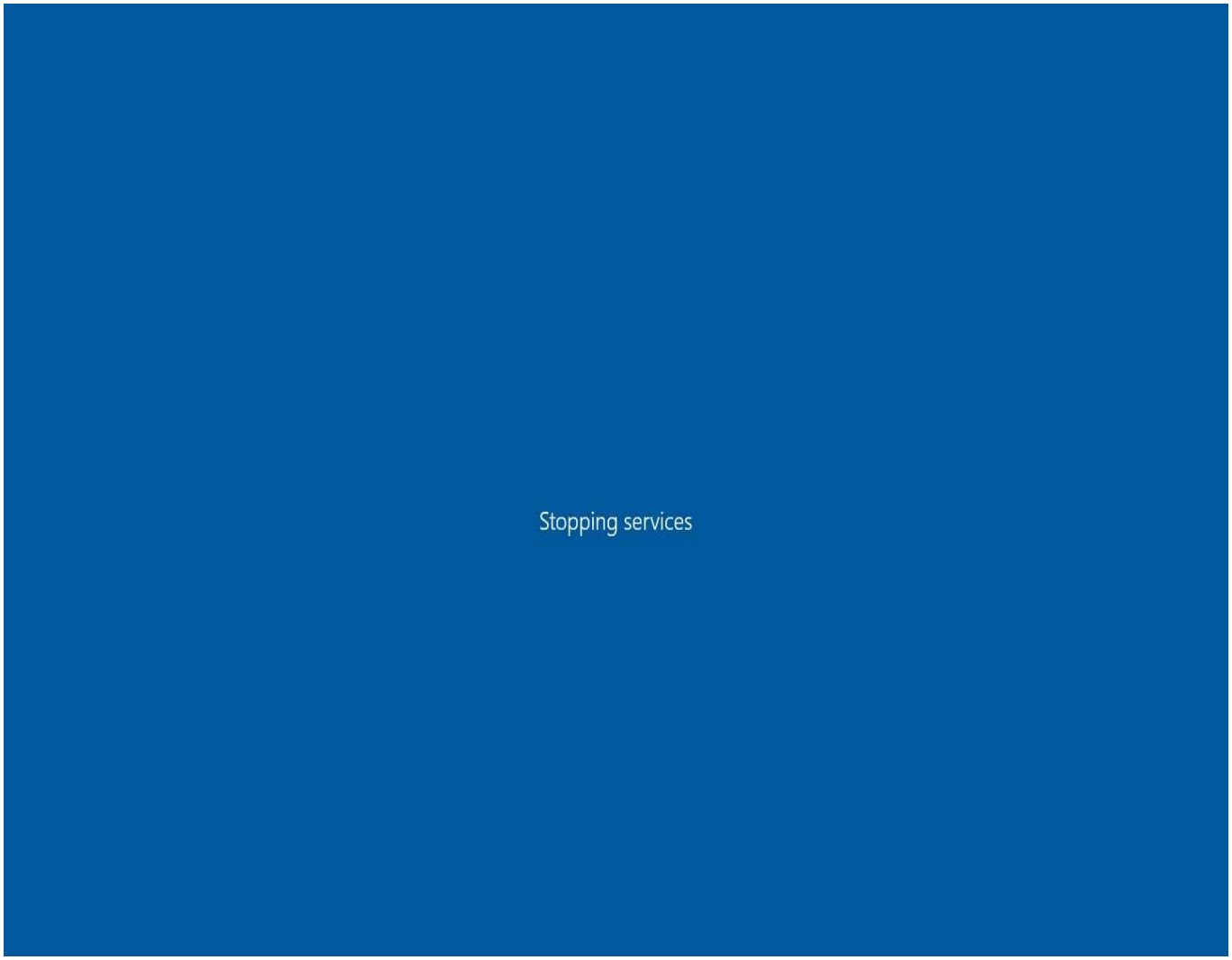
47. A chat box appears; type a message, and then click **Send**.



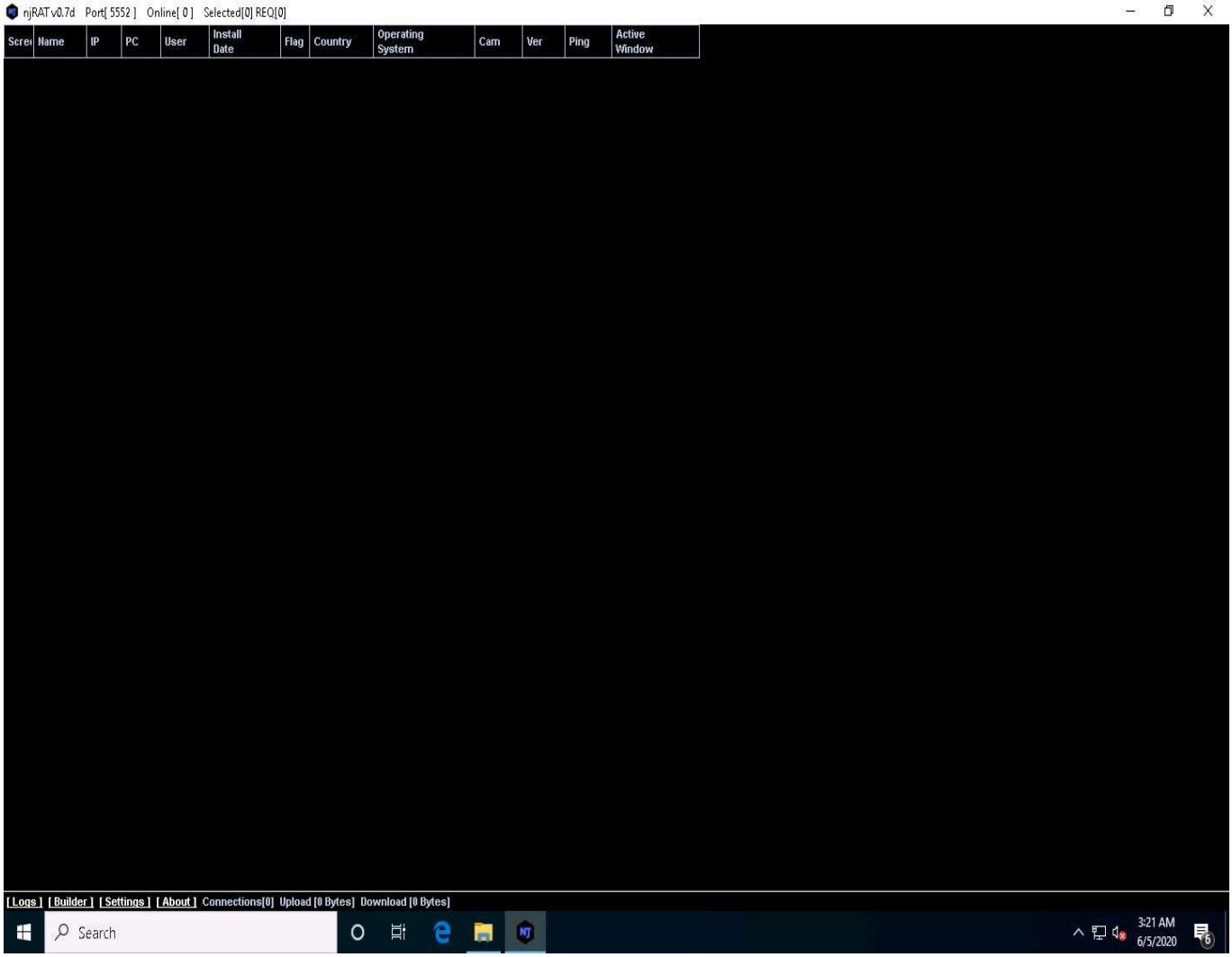
48. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows Server 2016**), as demonstrated in the screenshot.
49. Click Windows Server 2016 to switch to the **Windows Server 2016** machine, you can observe the message from the hacker appears on the screen.



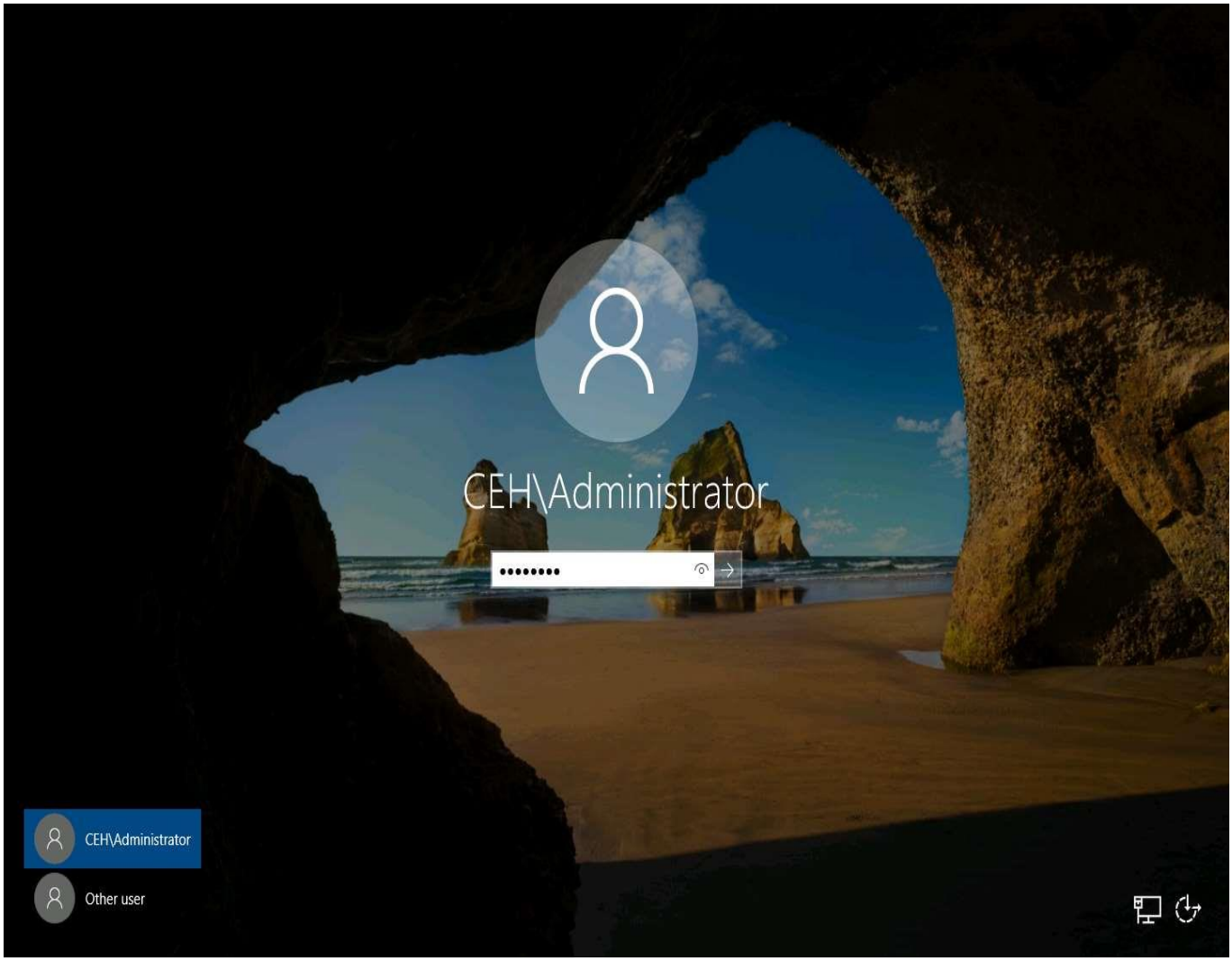
50. ☐ Seeing this, the victim becomes alert and attempts to close the chatbox. Irrespective of what the victim does, the chatbox remains for open as long as the attacker uses it.
51. ☐ Surprised by the behavior, the victim (you) attempts to break the connection by restarting the machine. As soon as this happens, njRAT loses its connection with **Windows Server 2016**, as the machine is shut down in the process of restarting.



52. Click Windows 10 to switch back to the attacker machine (**Windows 10**); you can see that the connection with the victim machine is lost.

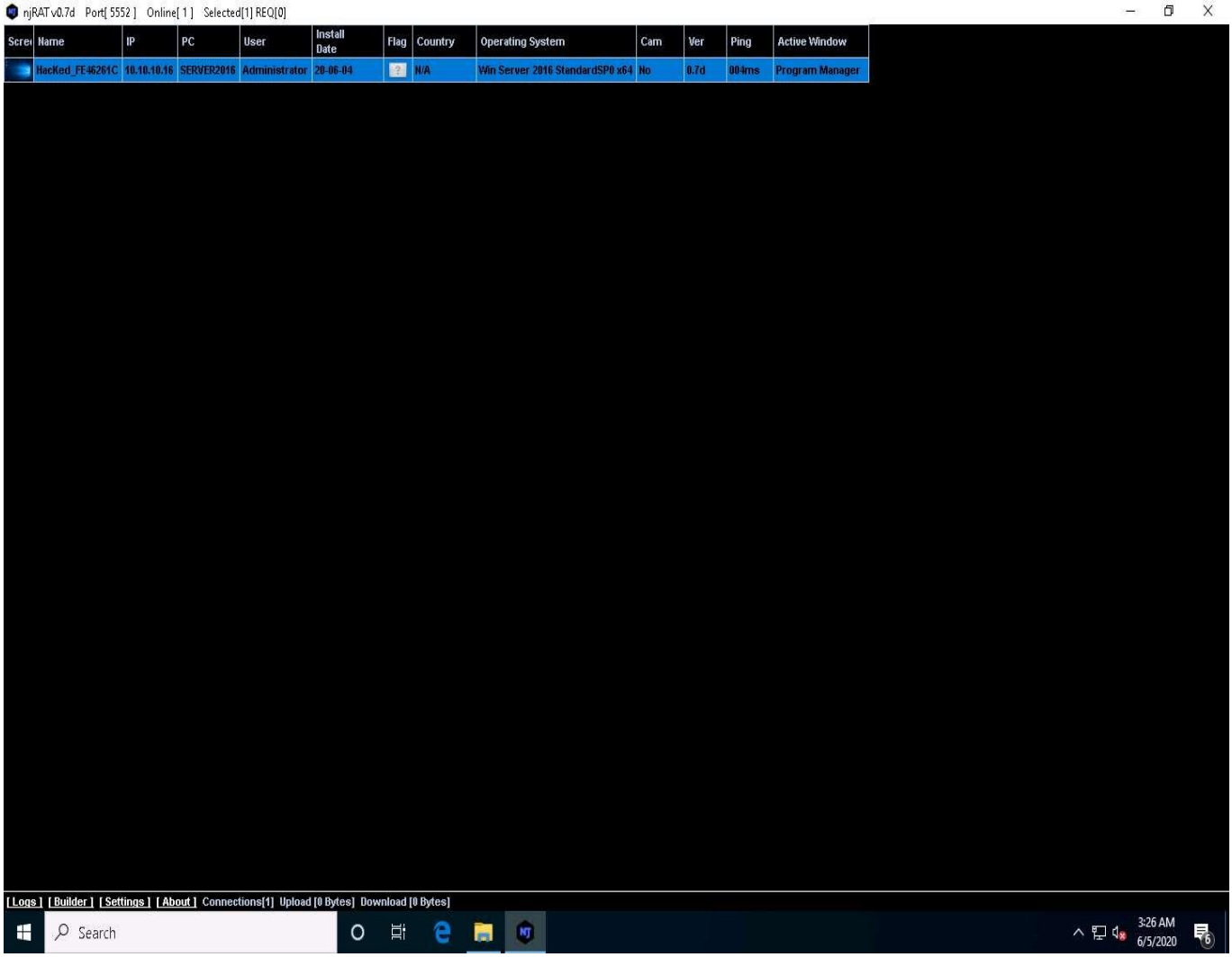


53. ☐ However, as soon as the victim logs in to their machine, the njRAT client automatically establishes a connection with the victim, as shown in the screenshot.
54. ☐ Click Windows Server 2016 to switch to the victim machine (**Windows Server 2016**). Click Ctrl+Alt+Delete to activate the machine, by default, **CEH\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.

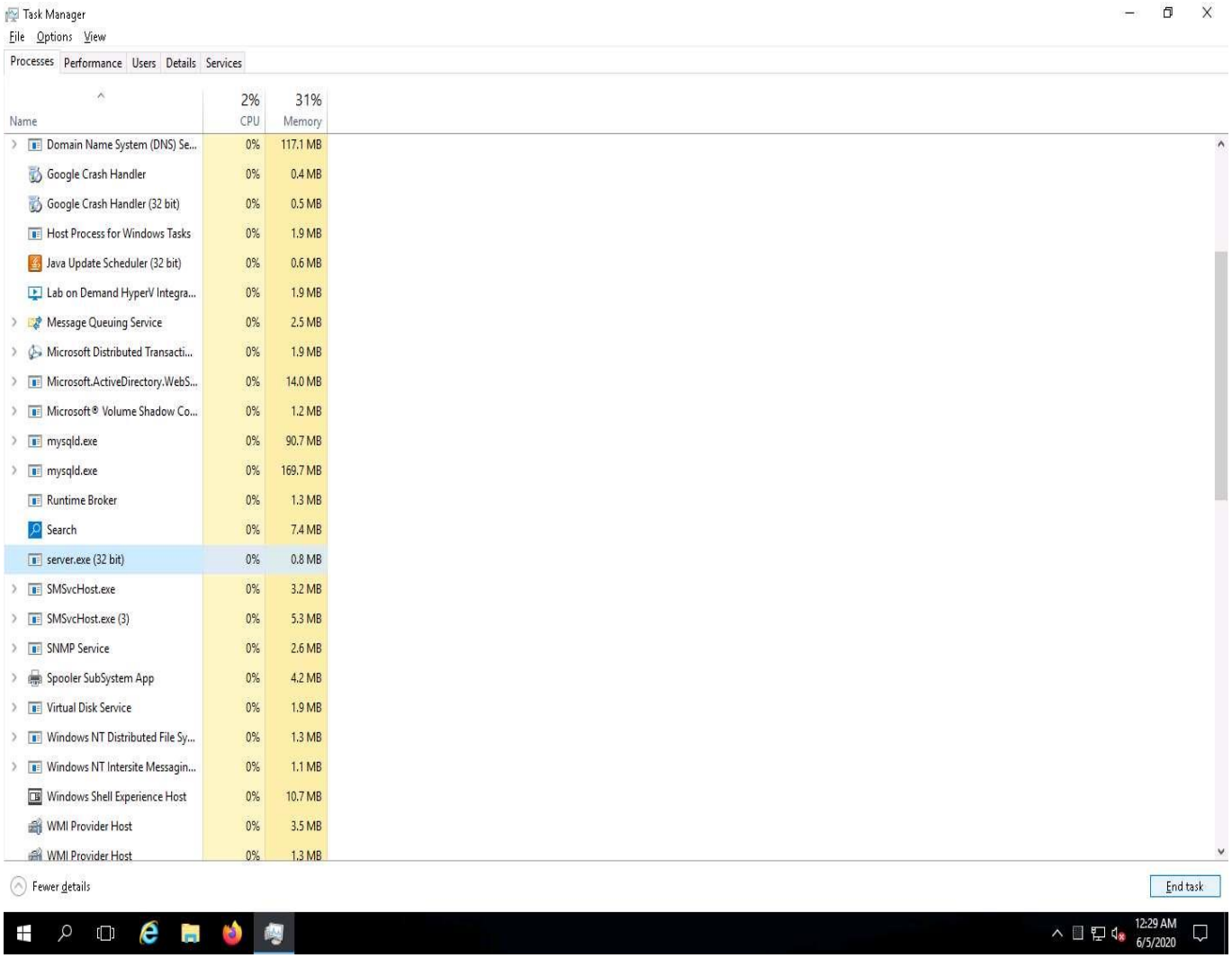


55. Click Windows 10 to switch back to the attacker machine (**Windows 10**); you can see that the connection has been re-established with the victim machine.

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



56. ☐ The attacker, as usual, makes use of the connection to access the victim machine remotely and perform malicious activity.
57. ☐ On completion of this lab, click Windows Server 2016 to switch to the **Windows Server 2016** machine, launch **Task Manager**, look for the **server.exe (32 bit)** process, and click **End task**.



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

Task 2: Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs

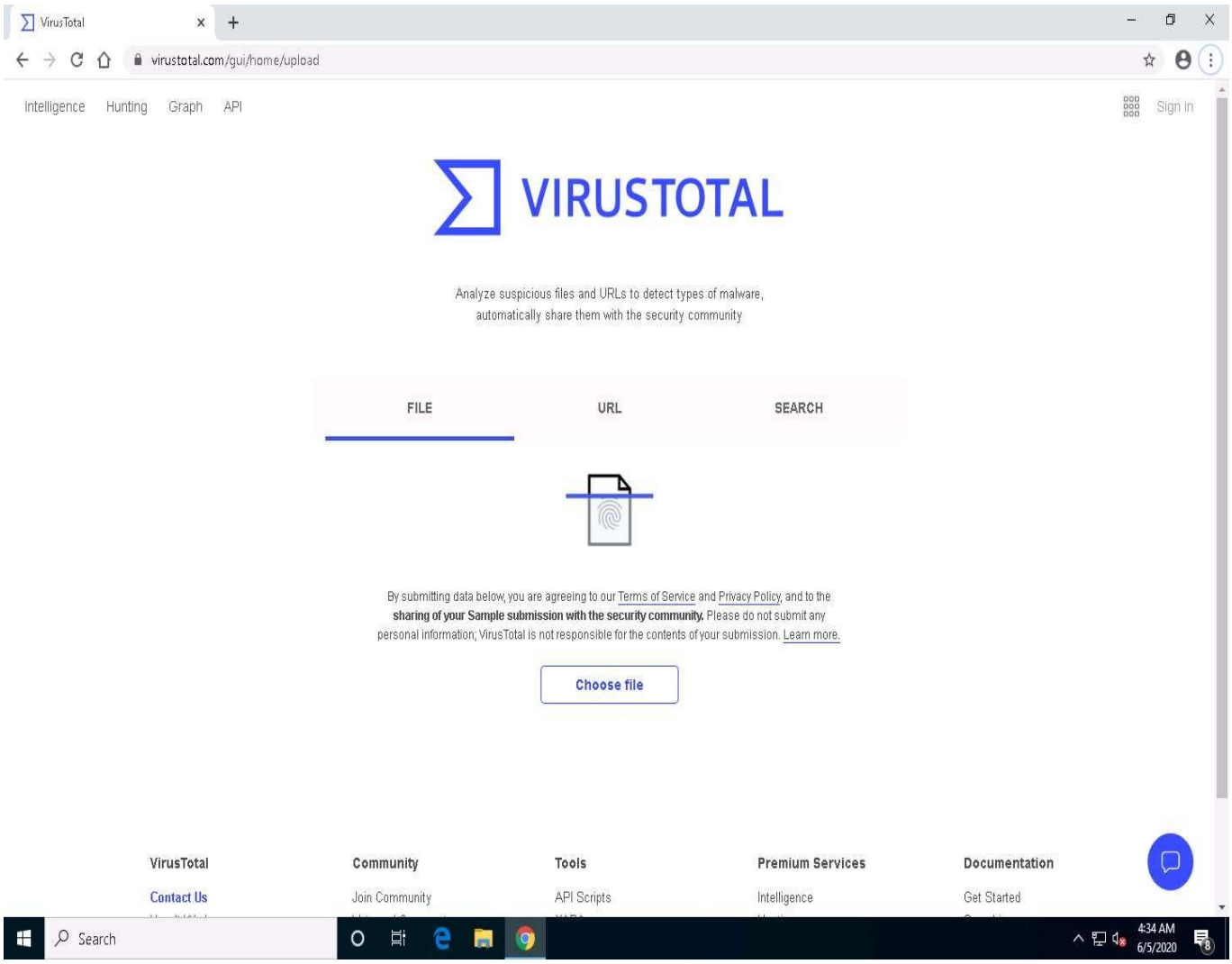
At present, numerous anti-virus software programs have been configured to detect malware such as Trojans, viruses, and worms. Although security specialists keep updating the virus definitions, hackers continually try to evade or bypass them. One method that attackers use to bypass AVs is to "crypt" (an abbreviation of "encrypt") the malicious files using fully undetectable crypters (FUDs). Crypting these files allows them to achieve their objectives, and thereby take complete control over the victim's machine.

Crypter is a software that encrypts the original binary code of the .exe file to hide viruses, spyware, keyloggers, and RATs, among others, in any kind of file to make them undetectable by anti-viruses. SwayzCryptor is an encrypter (or "crypter") that allows users to encrypt their program's source code.

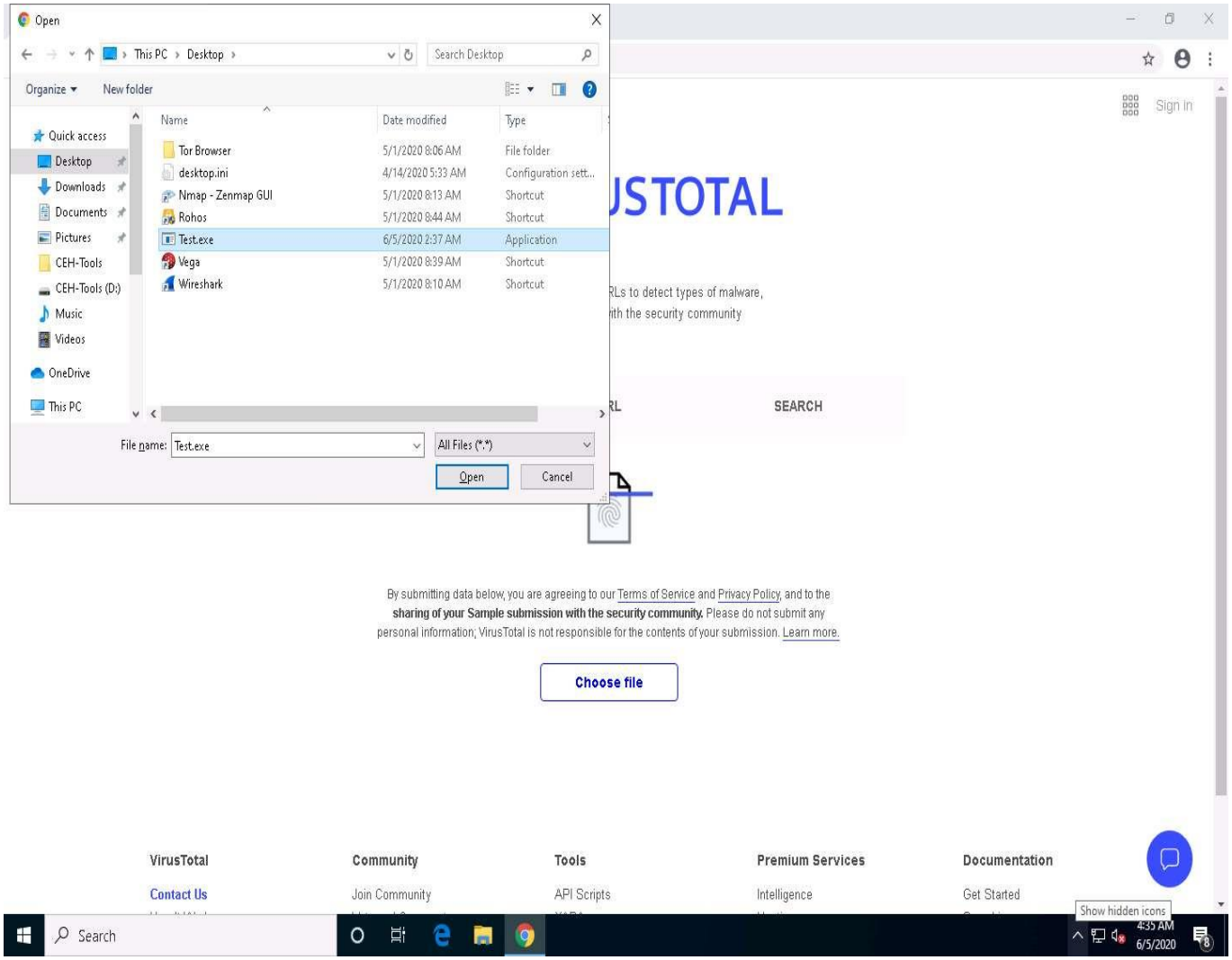
Here, we will use the SwayzCryptor to hide a Trojan and make it undetectable by anti-virus software.

1. ☐ Click Windows 10 to switch to the **Windows 10** machine, open any web browser (here, **Google Chrome**).In the address bar of the browser place your mouse cursor and click https://www.virustotal.com and press **Enter**.

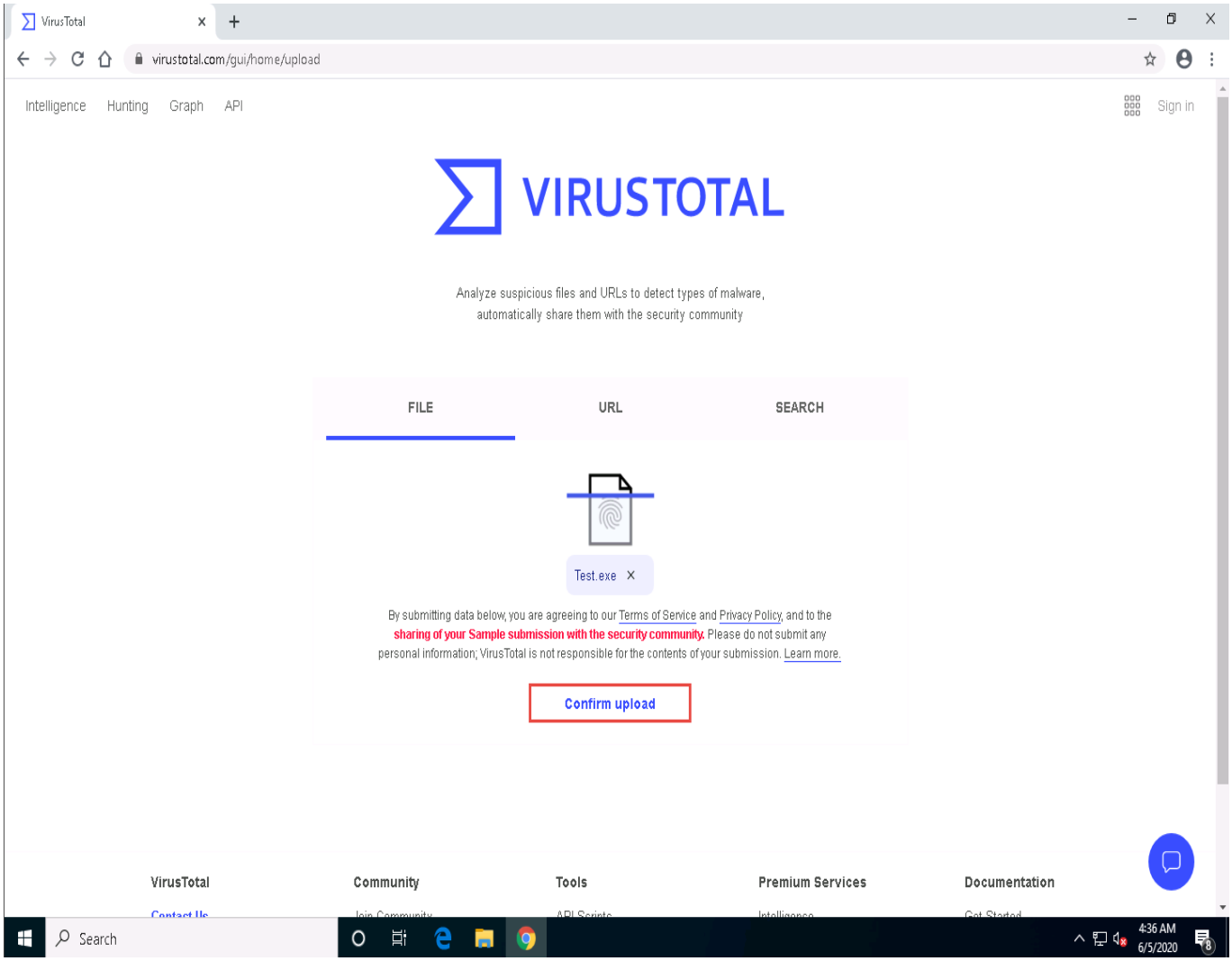
2. The **VirusTotal** main analysis site appears; click **Choose file** to upload a virus file.



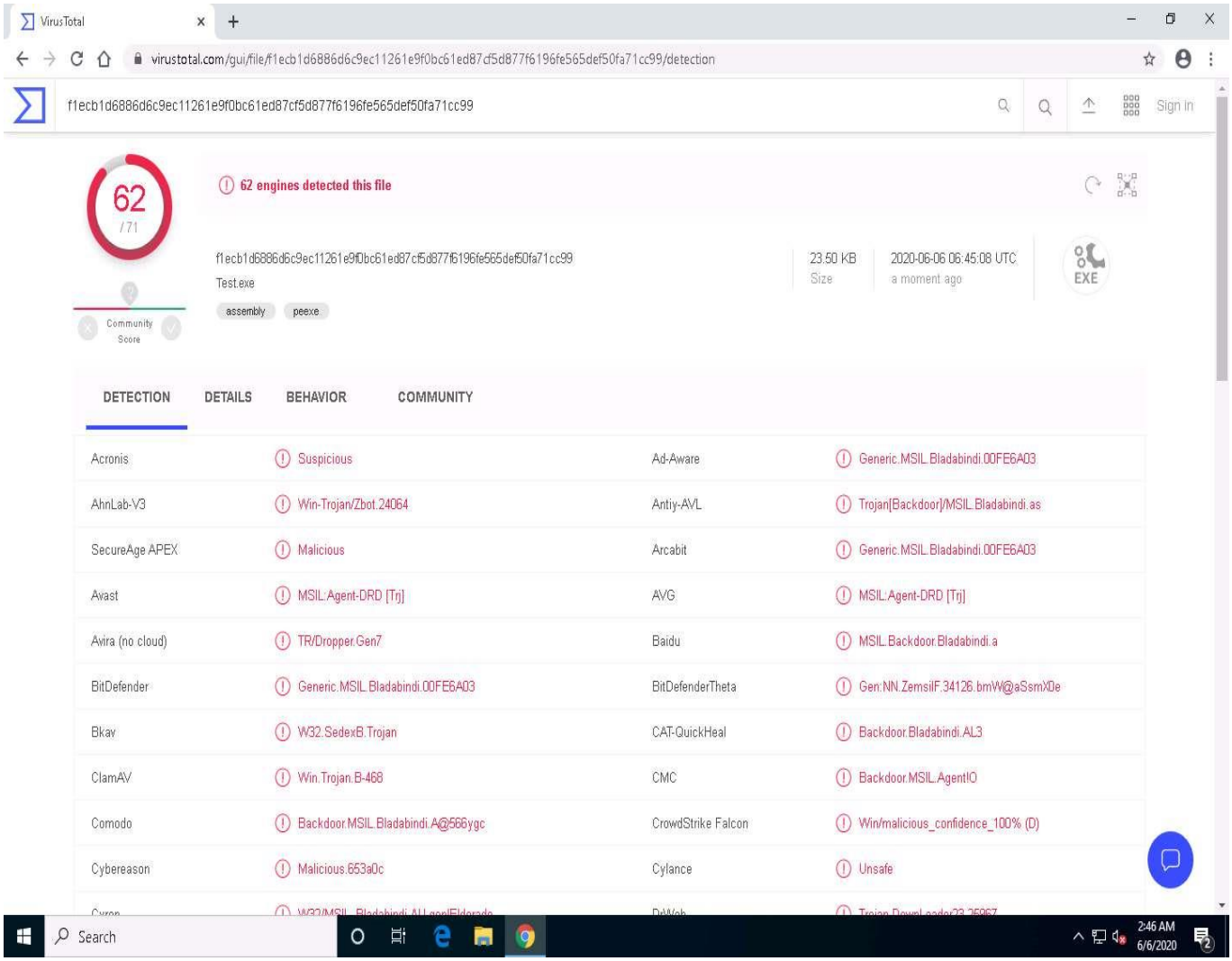
3. An **Open** dialog box appears; navigate to the location where you saved the malware file **Test.exe** in the previous lab (**Desktop**), select it, and click **Open**.



4. ☐ Click **Confirm upload** on the **VirusTotal** page.



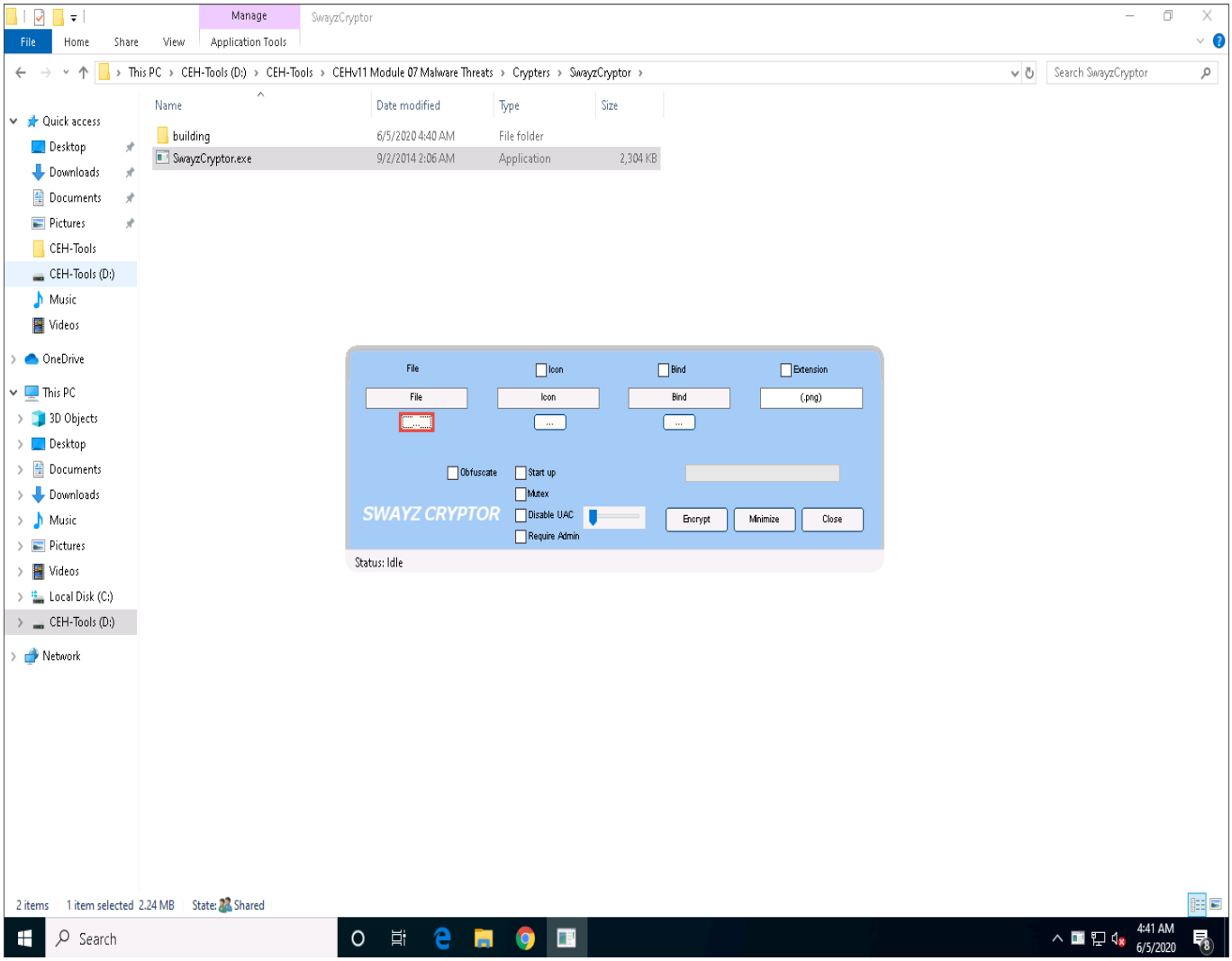
5. The **VirusTotal** uploads the file, scans it with the various anti-virus programs in its database, and displays the scan result, as shown in the screenshot.



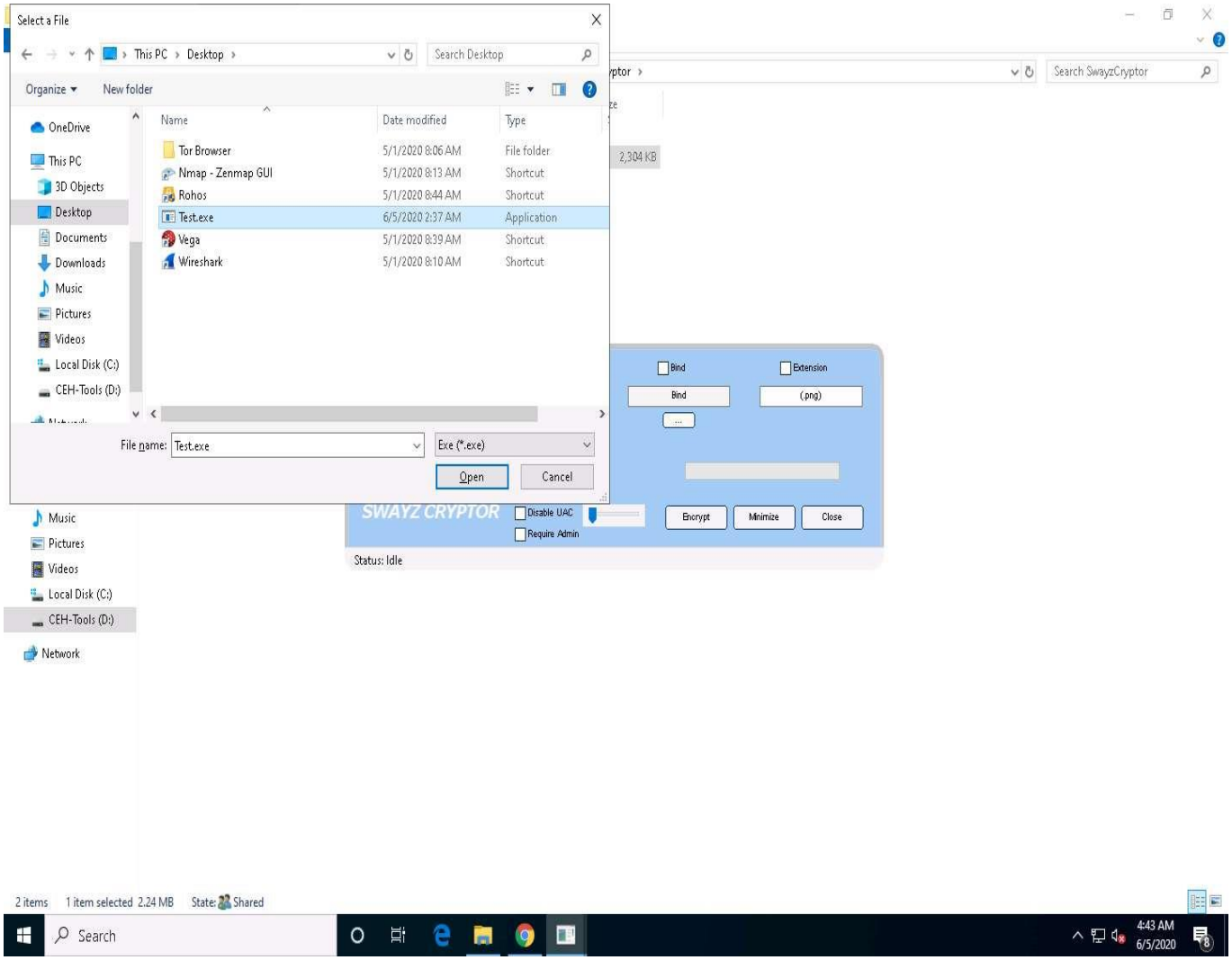
6. ☐ You can see that **62** out of **71** anti-virus programs have detected **Test.exe** as a malicious file. Minimize the web browser window.

The detection ratio might vary in your lab environment.

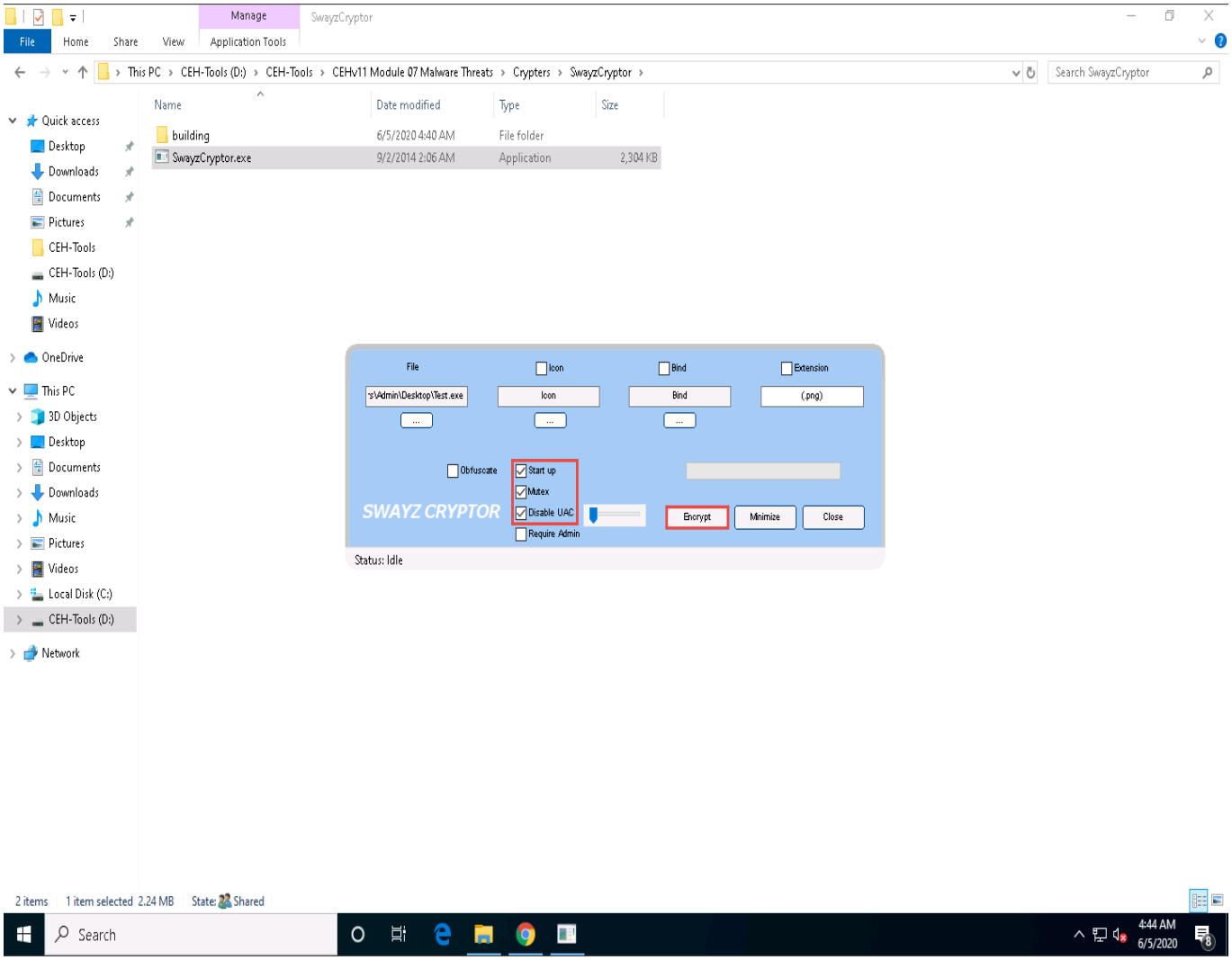
7. ☐ Go to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Crypters\SwayzCryptor** and double-click **SwayzCryptor.exe**.
8. ☐ The **SwayzCryptor GUI** appears; click ellipses icon below **File** to select the Trojan file.



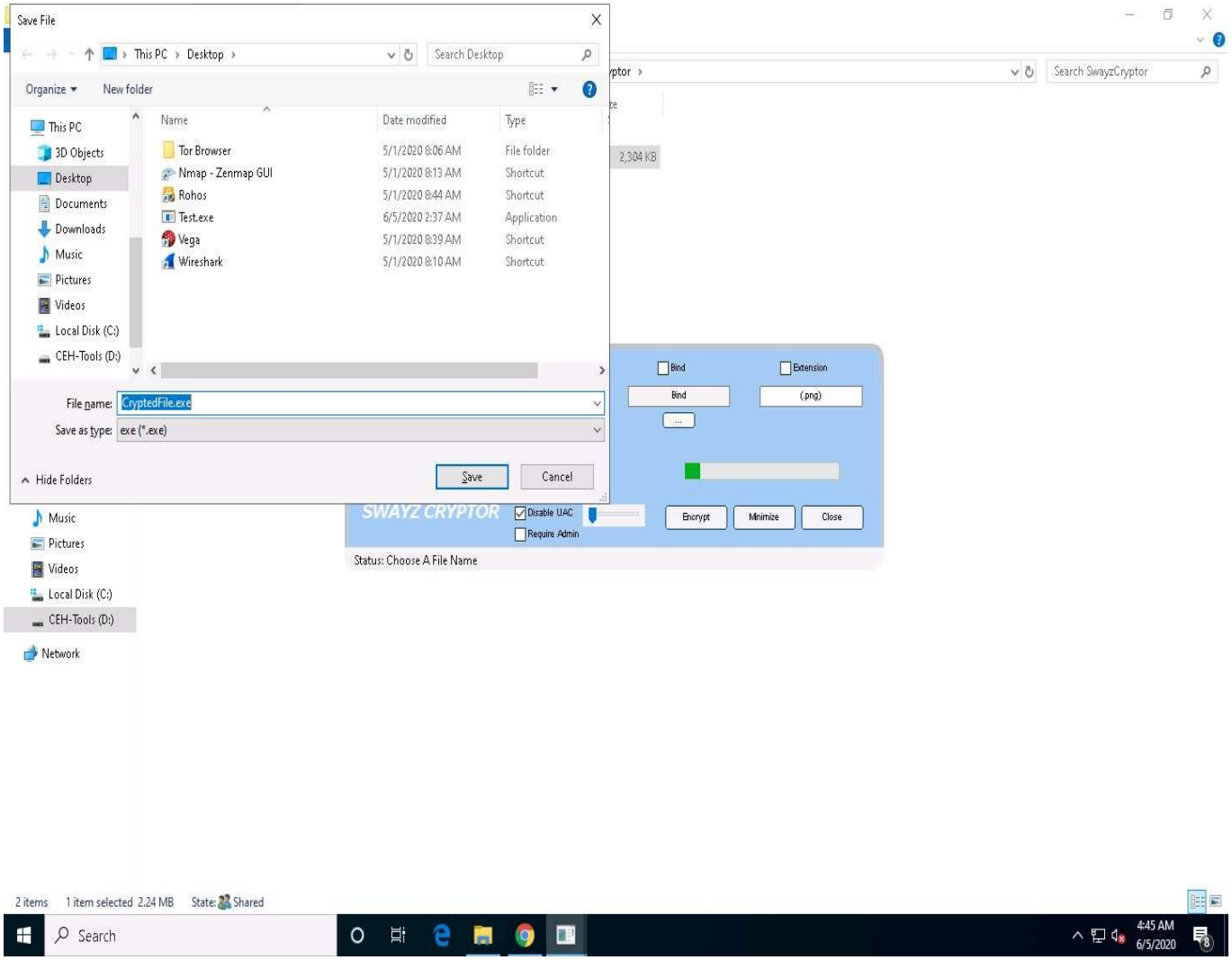
9. ☐ The **Select a File** dialog-box appears; navigate to the location of **Test.exe** (**Desktop**), select it, and click **Open**.



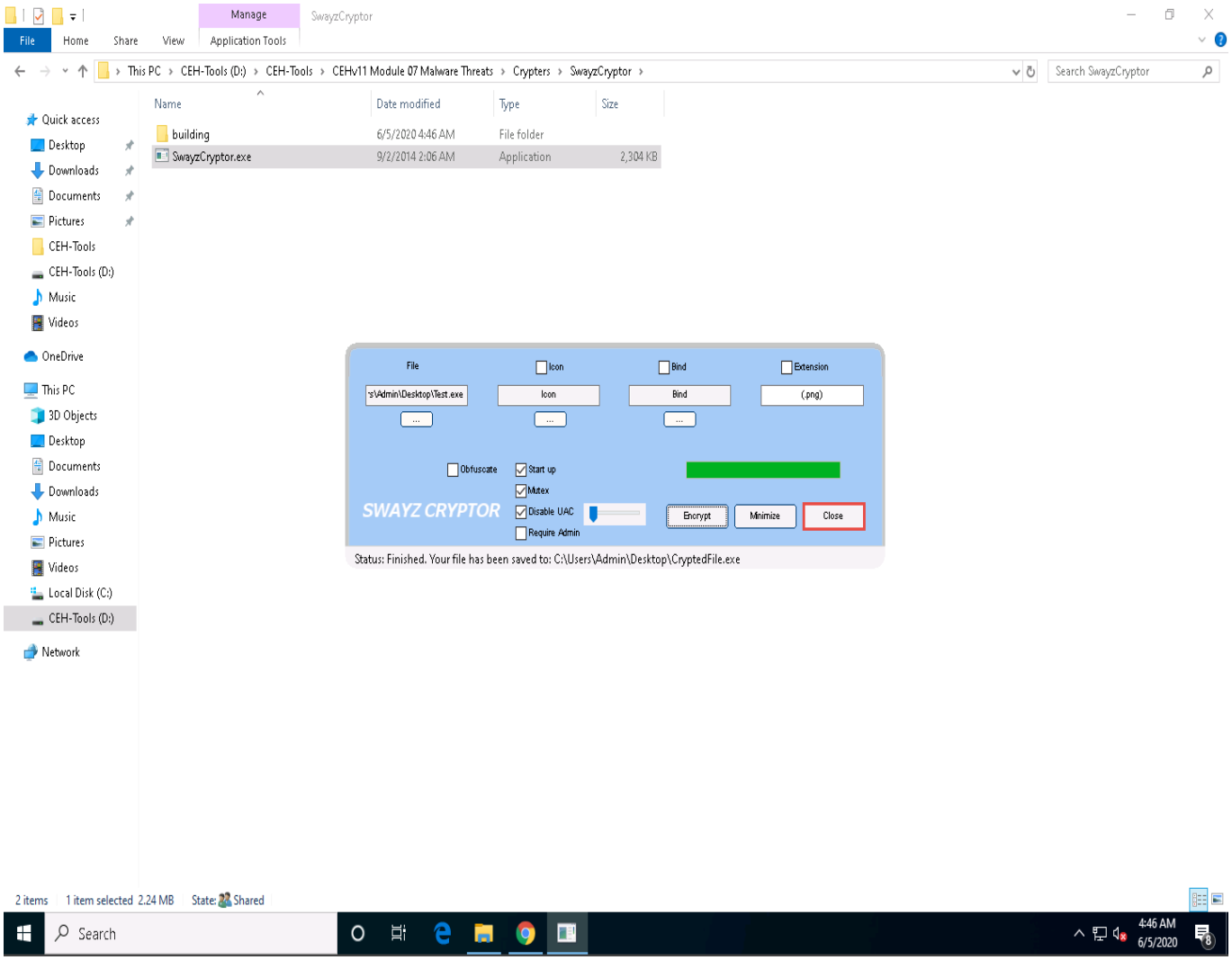
10. ☐ Once the file is selected, check the options **Start up**, **Mutex**, and **Disable UAC**, and then click **Encrypt**.



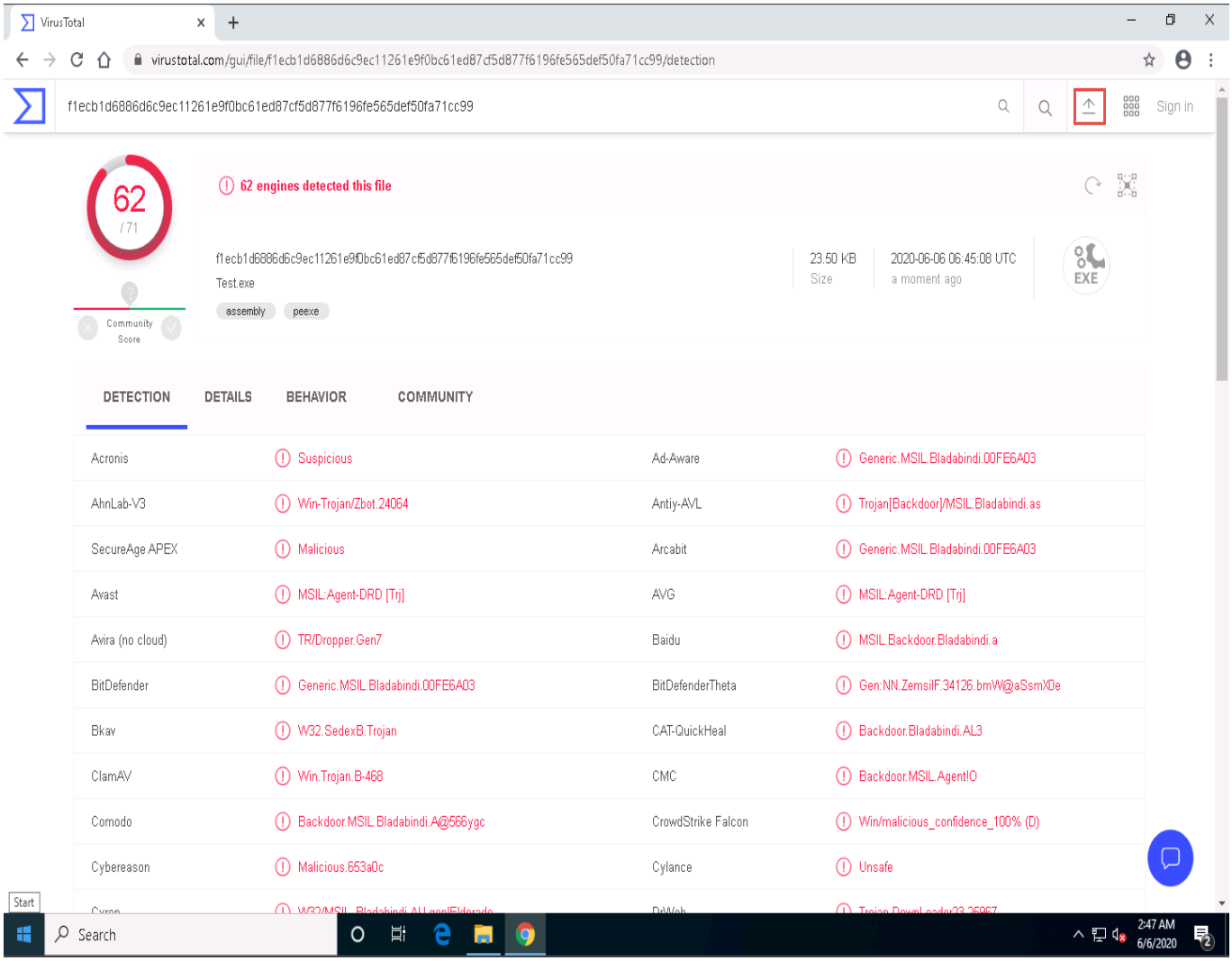
11. The **Save File** dialog-box appears; select the location where you want to store the crypted file (here, **Desktop**), leave the file name set to its default (**CryptedFile**), and click **Save**.



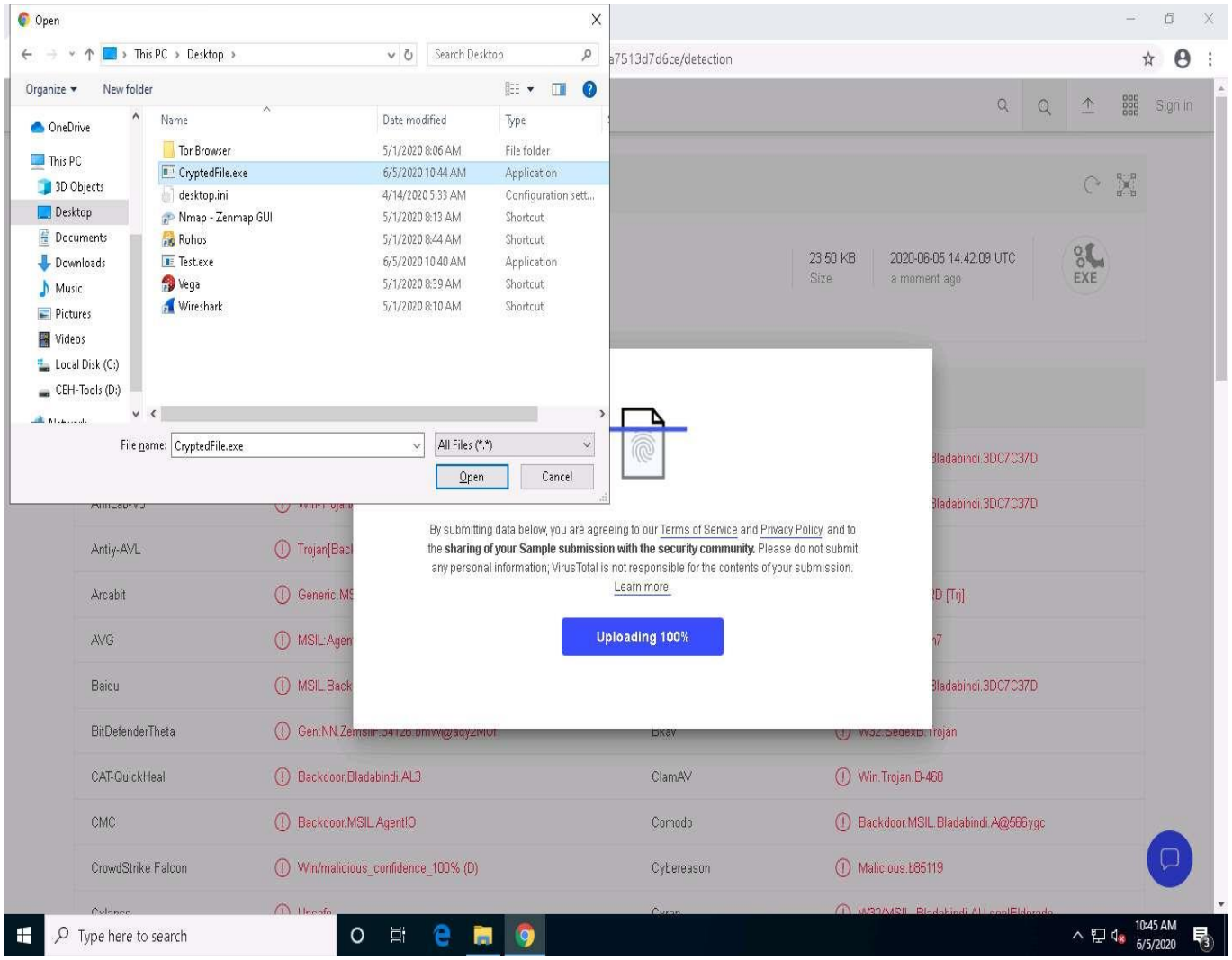
12. ☐ Once the encryption is finished, click **Close**.



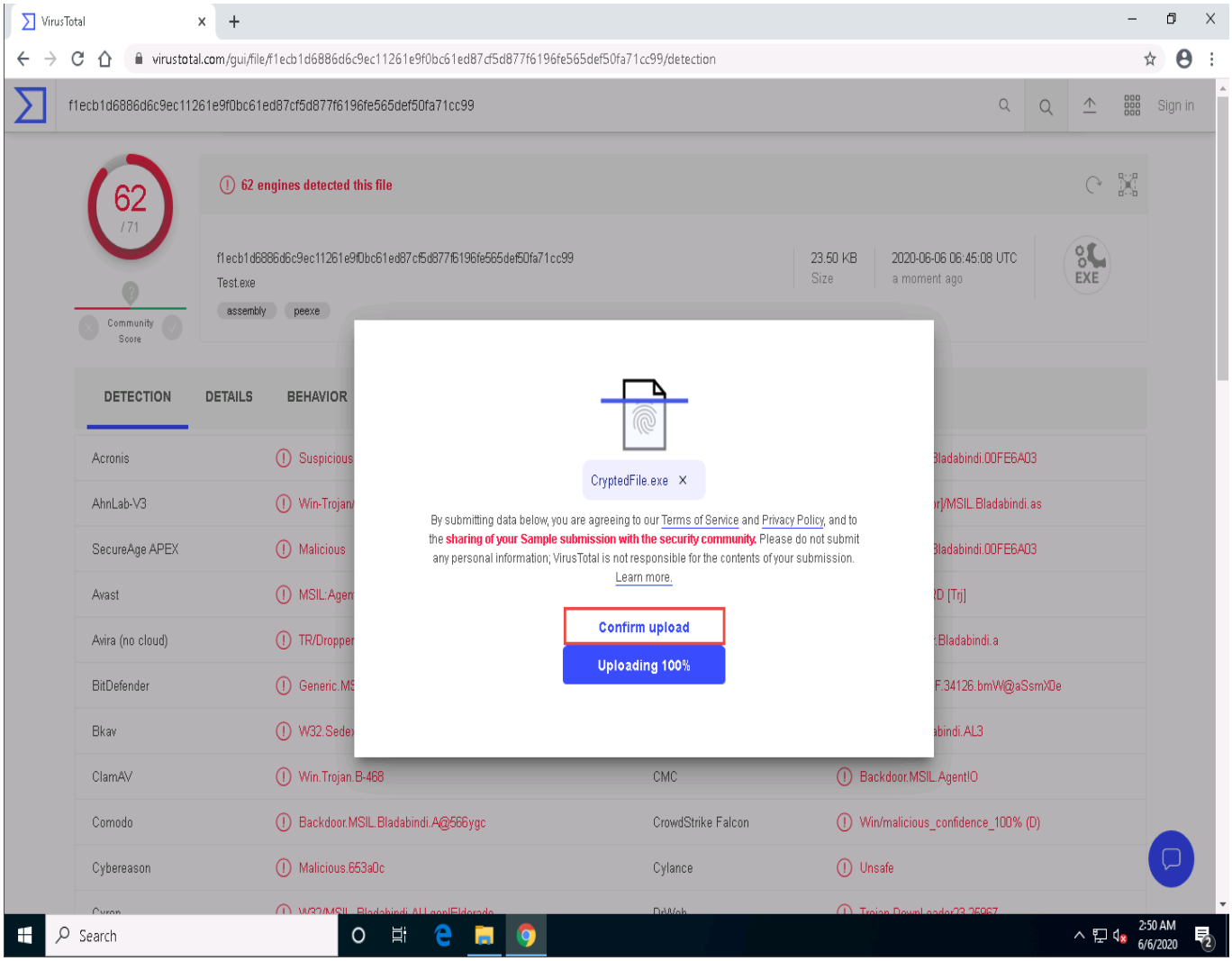
13. Maximize the web browser (here, **Google Chrome**). In the VirusTotal analysis page, click the **Upload file** icon in the top-right corner of the page.



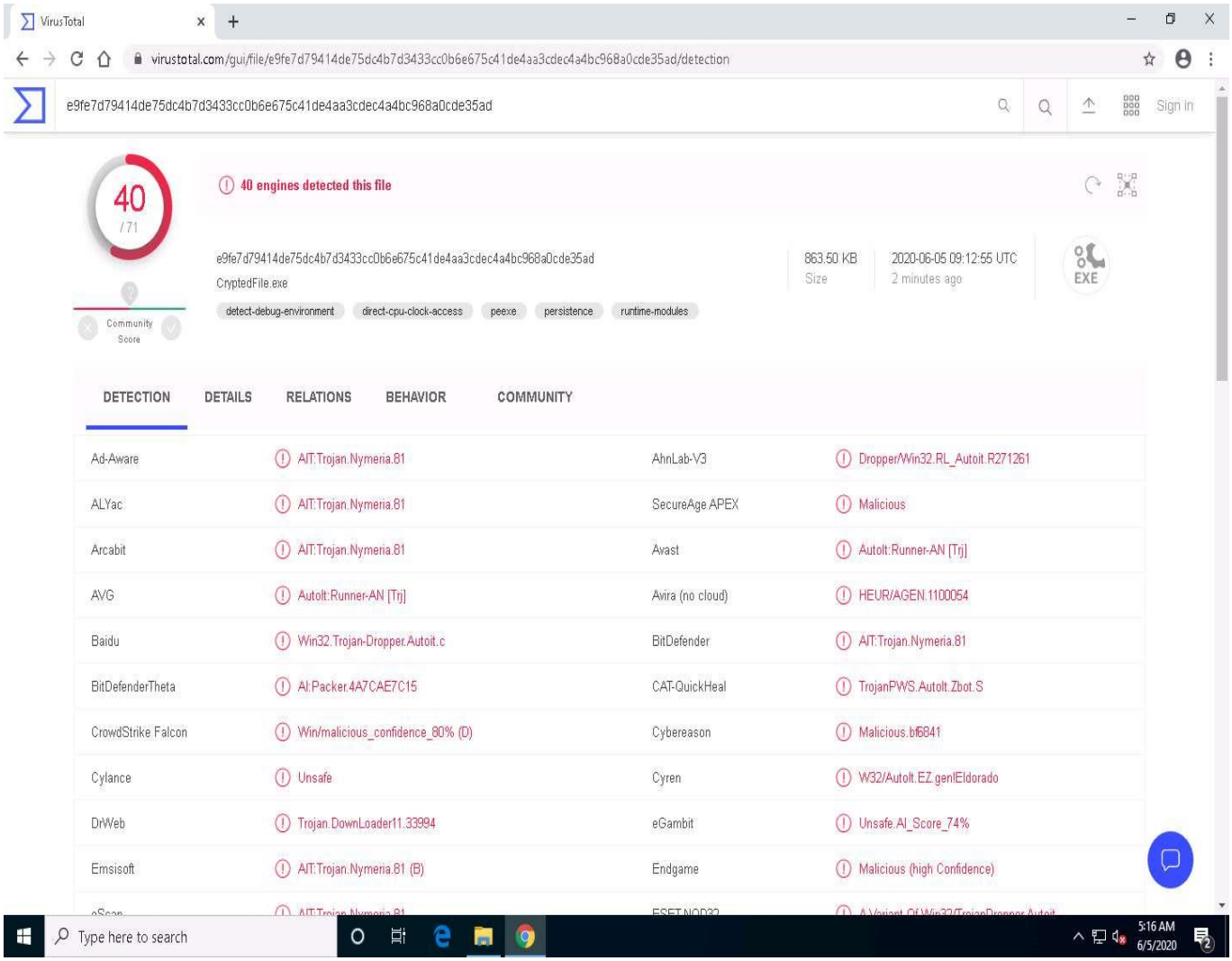
14. An **Open** dialog-box appears; navigate to the location where you saved the encrypted file **CryptedFile.exe** (**Desktop**), select the file, and click **Open**.

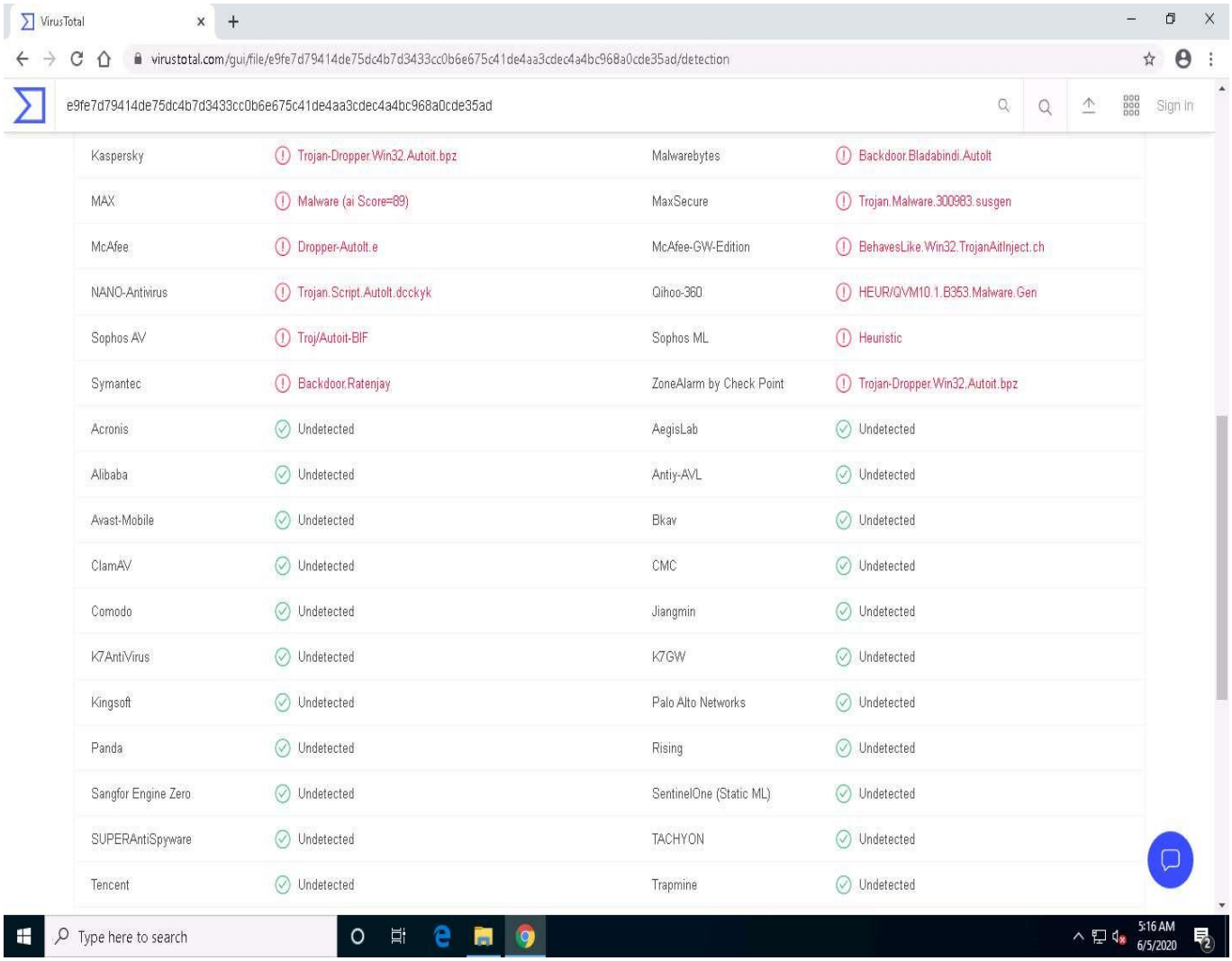


15. ☐ Click **Confirm upload**.

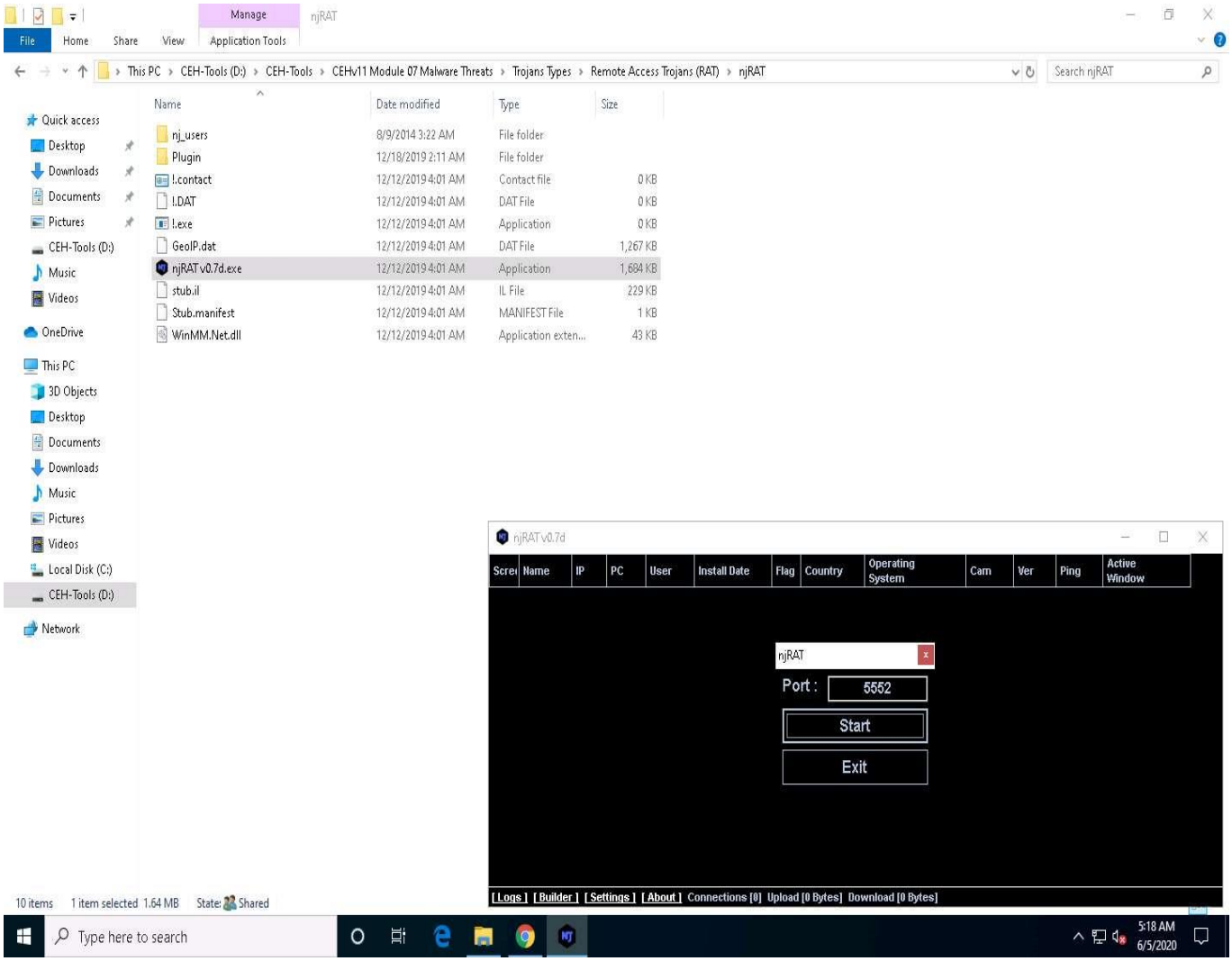


16. VirusTotal uploads the file and begins to scan it with the various anti-virus programs in its database. It displays the scan result, as shown in the screenshot.


VirusTotal
virustotal.com/gui/file/e9fe7d79414de75dc4b7d3433cc0b6e675c41de4aa3cdec4a4bc968a0cde35ad/detection
e9fe7d79414de75dc4b7d3433cc0b6e675c41de4aa3cdec4a4bc968a0cde35ad
Sign in
40
/ 71
40 engines detected this file
e9fe7d79414de75dc4b7d3433cc0b6e675c41de4aa3cdec4a4bc968a0cde35ad
CryptedFile.exe
detect-debug-environment
direct-cpu-clock-access
peexe
persistence
runtime-modules
863.50 KB
Size
2020-06-05 09:12:55 UTC
2 minutes ago
EXE
Community Score
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Ad-Aware
AIT:Trojan.Nymeria.81
AhnLab-V3
Dropper/Win32.RL_Autoit.R271261
ALYac
AIT:Trojan.Nymeria.81
SecureAge APEX
Malicious
Arcabit
AIT:Trojan.Nymeria.81
Avast
AutoIt:Runner-AN [Trj]
AVG
AutoIt:Runner-AN [Trj]
Avira (no cloud)
HEUR/AGEN.1100054
Baidu
Win32.Trojan-Dropper.Autoit.c
BitDefender
AIT:Trojan.Nymeria.81
BitDefenderTheta
AI:Packer.4A7CAE7C15
CAT-QuickHeal
TrojanPWS.AutoIt.Zbot.S
CrowdStrike Falcon
Win/malicious_confidence_80% (D)
Cybereason
Malicious.bf6841
Cylance
Unsafe
Cyren
W32/AutoIt.EZ.gen!Eldorado
DrWeb
Trojan.DownLoader11.33994
eGambit
Unsafe.AI_Score_74%
Emsisoft
AIT:Trojan.Nymeria.81 (B)
Endgame
Malicious (high Confidence)
Type here to search
5:16 AM
6/5/2020



17. ☐ Only a few anti-virus programs have detected **CryptedFile.exe** as a malicious file. Minimize or close the browser window.
18. ☐ Now, we will test the functioning of a Crypted file (**CryptedFile.exe**).
19. ☐ Go to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**, double-click the **njRAT v0.7d.exe** file and launch **njRAT** by choosing the default port number **5552**, and then click **Start**.
20. ☐ In this exercise, we have already created a crypted file (**CryptedFile.exe**), built using njRAT.

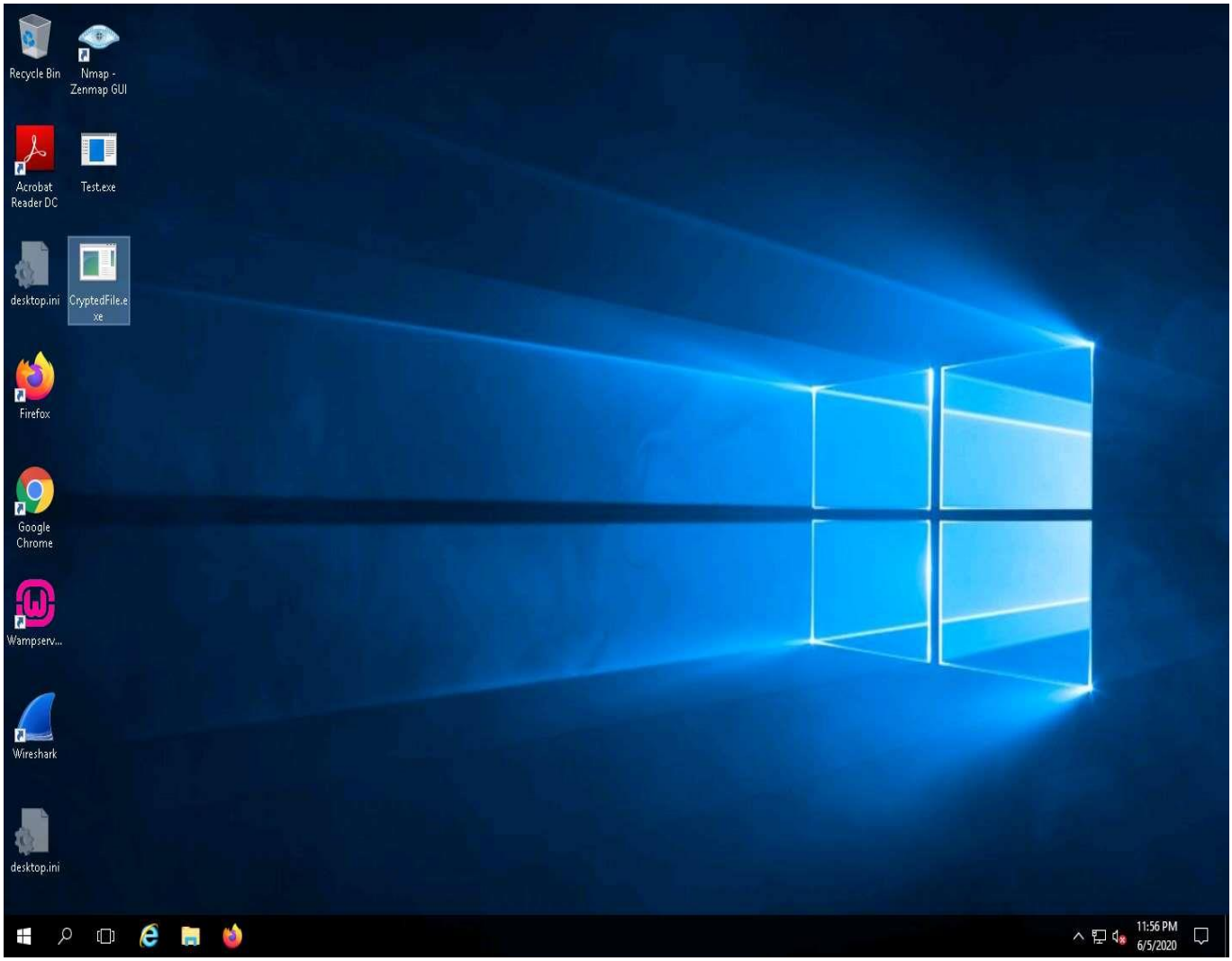


21. ☐ Use any technique to send **CryptedFile.exe** to the intended target—through email or any other source (In real-time, attackers send this server to the victim).

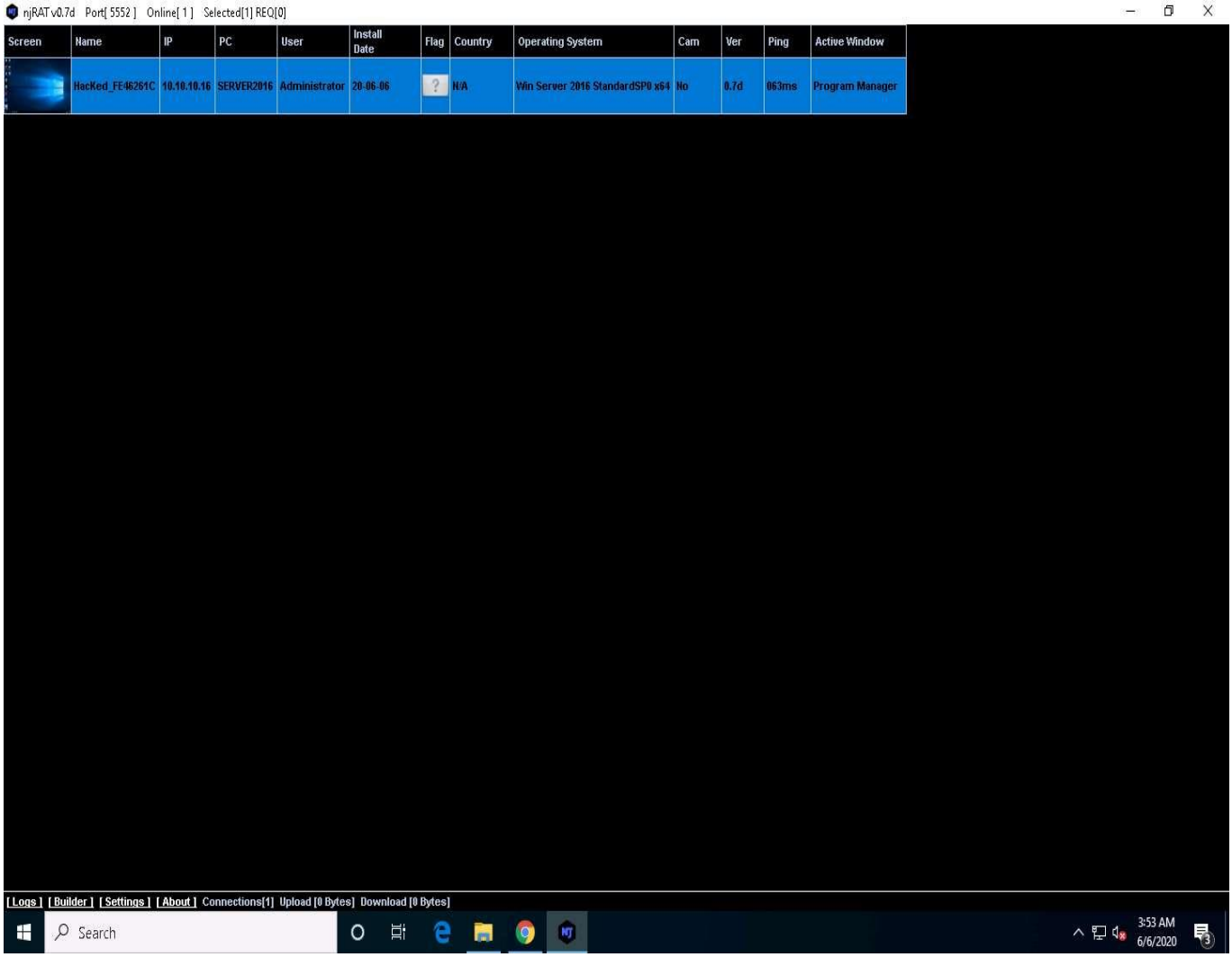
In this lab, we copied the **CryptedFile.exe** file to the shared network location (**CEH-Tools**) to share the file.

22. ☐ Click Windows Server 2016 to switch to the **Windows Server 2016** machine.
23. ☐ 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**.
24. ☐ 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** machine and downloads the server.
25. ☐ Double-click **CryptedFile.exe** to run this malicious executable.

If **You must restart your computer to turn off User Account Control** pop-up appears in the right-bottom corner of the window, then **Restart** the **Windows Server 2016** machine and click Ctrl+Alt+Delete to activate the machine, by default, **CEH\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.



26. ☐ 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** machine establishes a persistent connection with the victim machine.
27. ☐ Click Windows 10 to switch to the **Windows 10** machine and in the njRAT window you can observe that the connection has been established with the victim machine.



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, click Windows Server 2016 to switch to the **Windows Server 2016** machine, 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.

Task 3: Create a Server using the ProRat Tool

Attackers use malware to steal personal information, financial data, and business information from target systems. ProRat is a “remote administration tool” created by the PRO Group. ProRat was written in the C programming language and is capable of working with all Windows OSes. ProRat was designed to allow users to control their own computers remotely from other computers. However, attackers have co-opted it for their own nefarious purposes. Some hackers take control of remote computer systems to conduct a Denial-of-Service (DoS) attack, which renders the target system unavailable for normal personal or business use. These targeted systems include high-profile web servers such as banks and credit card gateways.

As with other Trojan horses, ProRat uses a client and server. It opens a port on the computer that allows the client to perform numerous operations on the server (the victim machine).

Some of ProRat's malicious actions on the victim's machine include:

- Logging keystrokes
- Stealing passwords
- Taking full control over files
- Drive formatting
- Opening and closing the DVD tray
- Hiding the taskbar, desktop, and start button
- Viewing system information

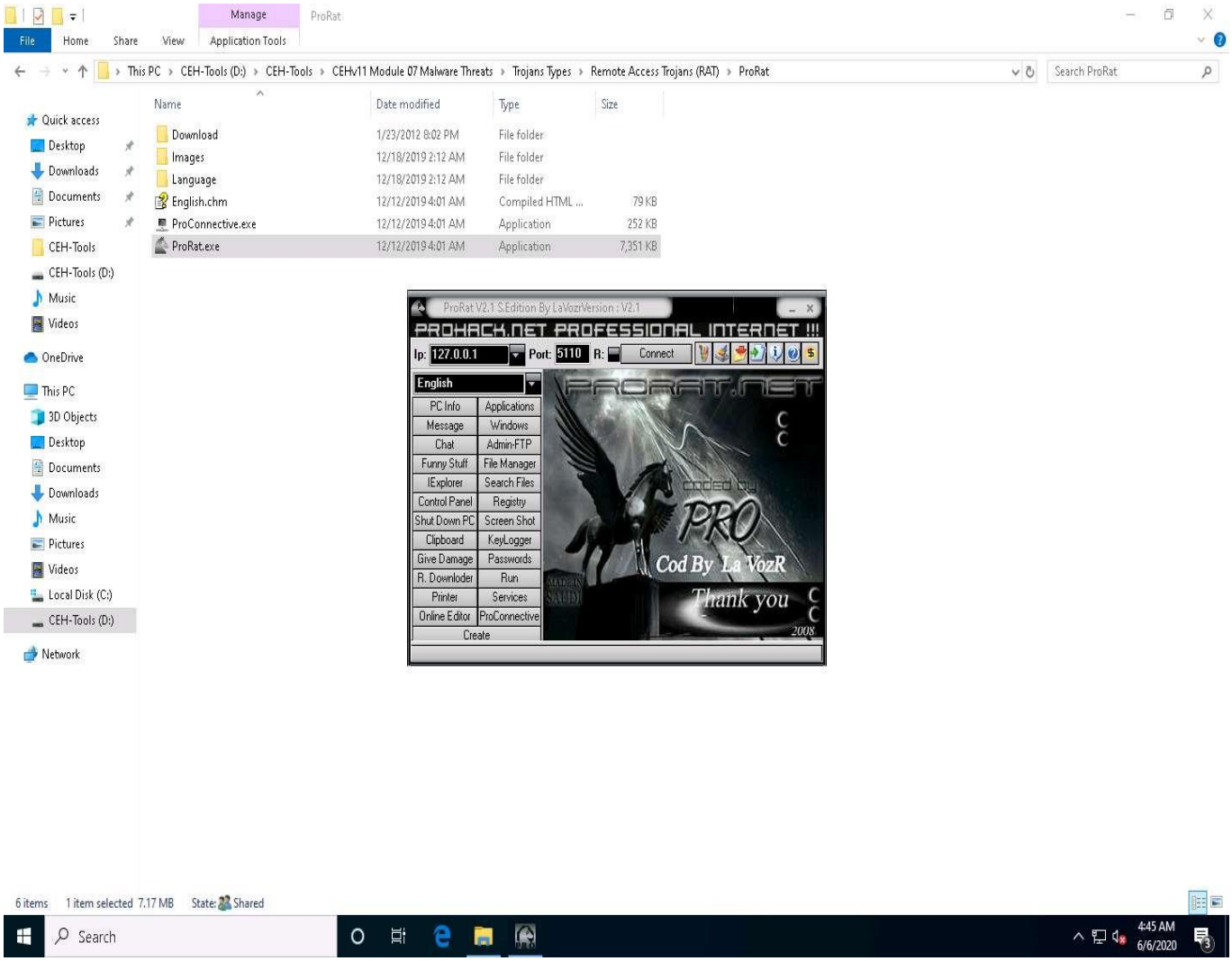
An ethical hacker or pen tester can use ProRat to audit their own network against remote access Trojans.

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

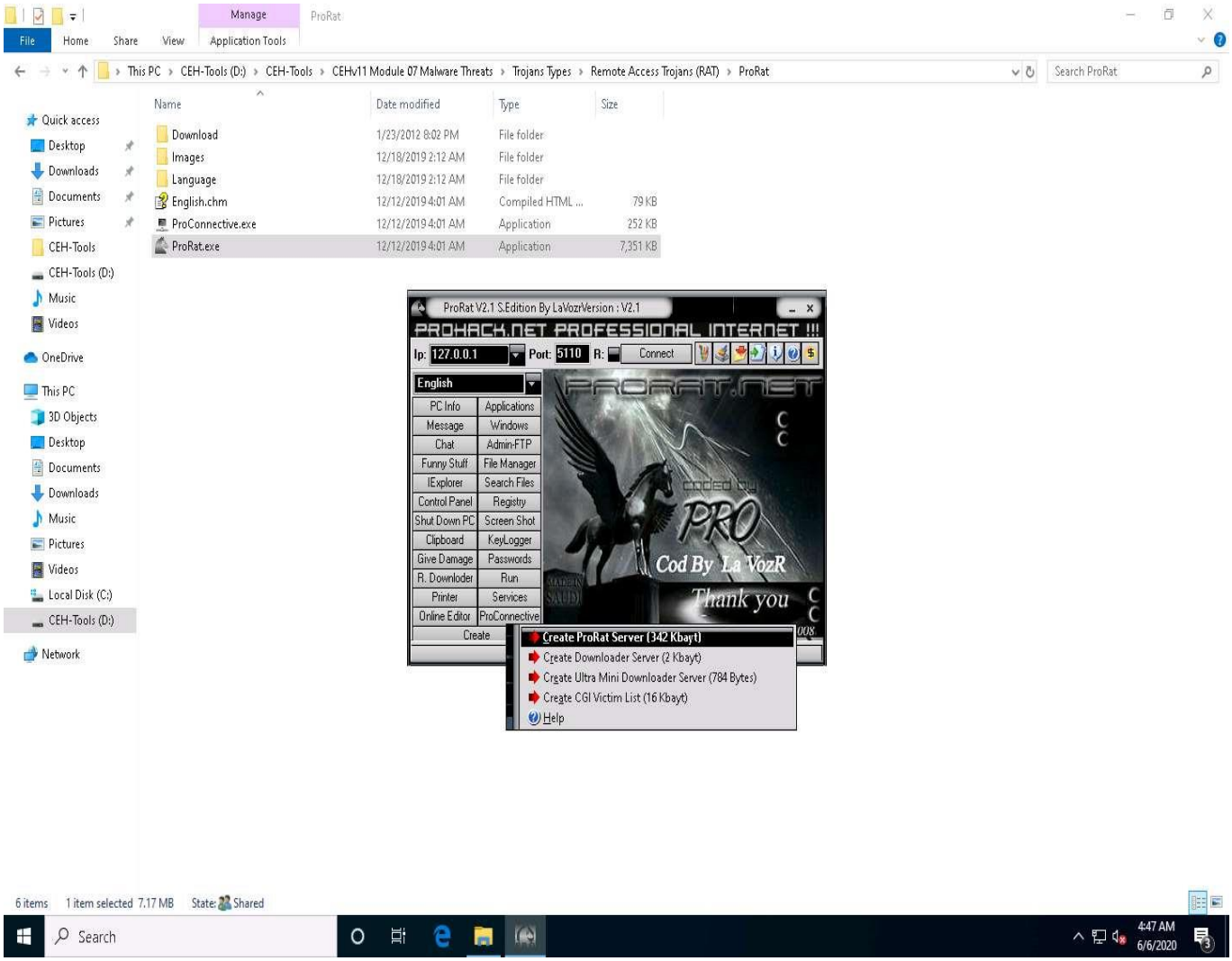
1. Click Windows 10 to switch to the **Windows 10** machine.
2. Navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat** and double-click the **ProRat.exe** file.

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

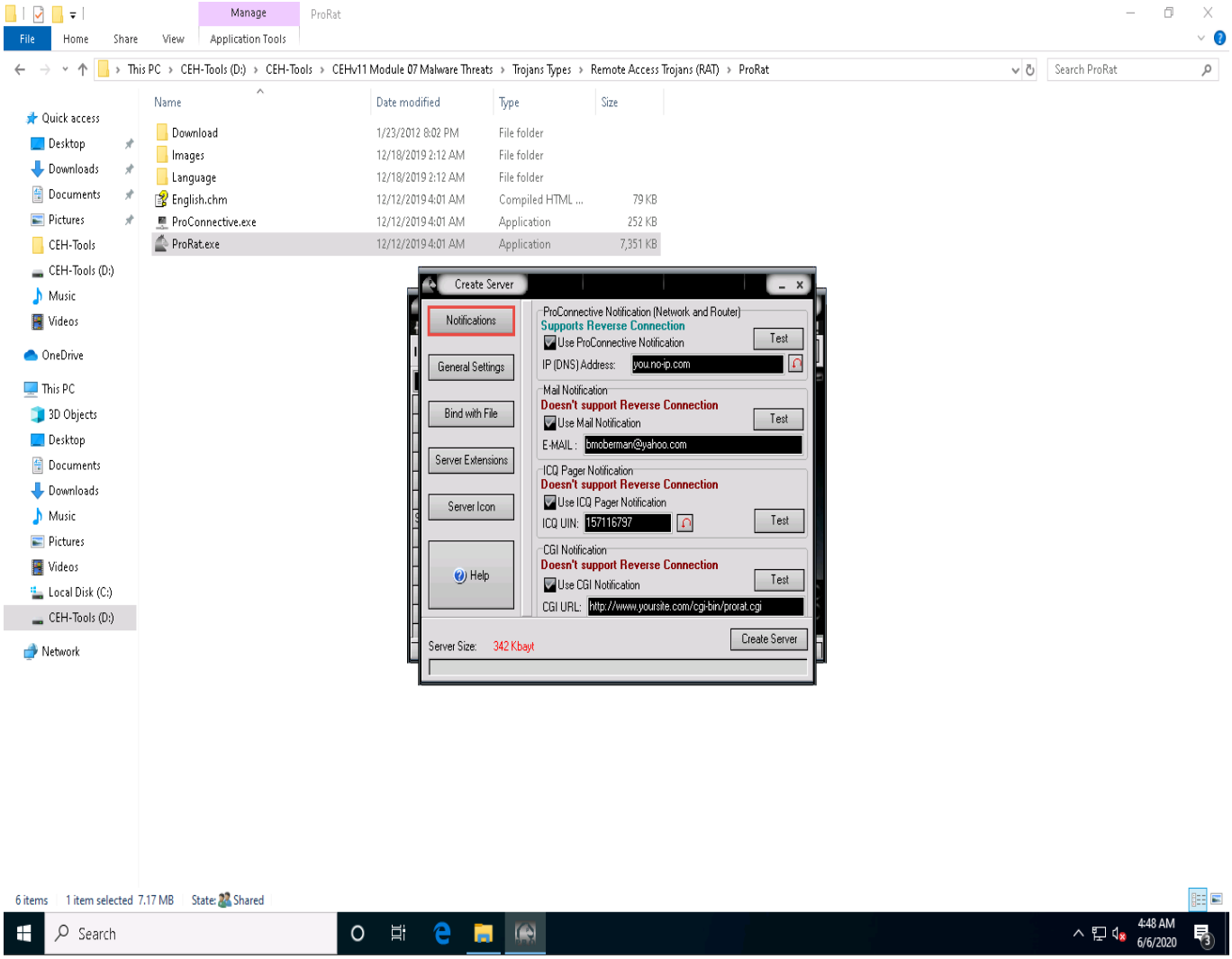
3. The **ProRat** main window appears, as shown in the screenshot.



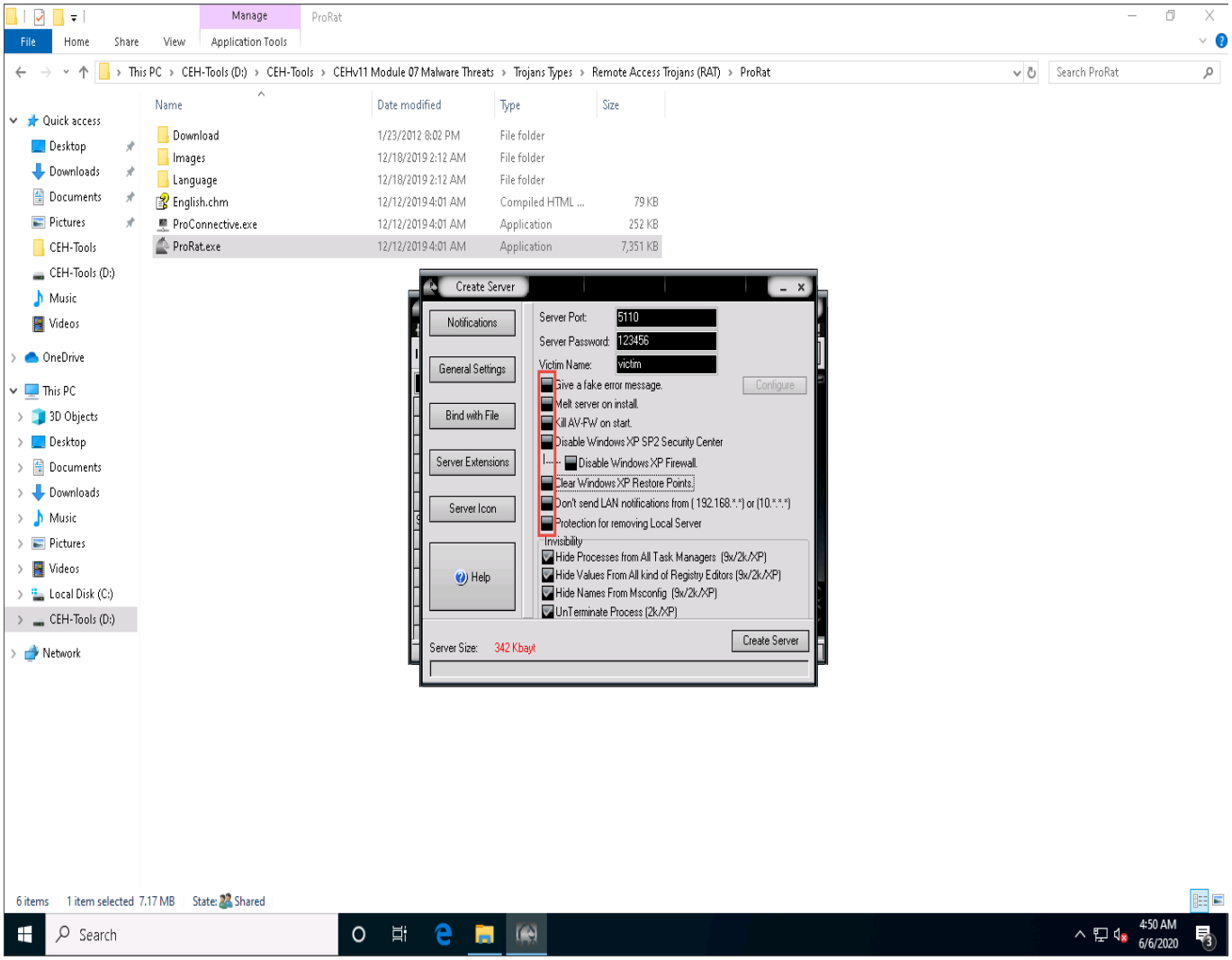
4. ☐ Click **Create**, and then click the **Create ProRat Server (342 Kbayt)** option to create a ProRat server.



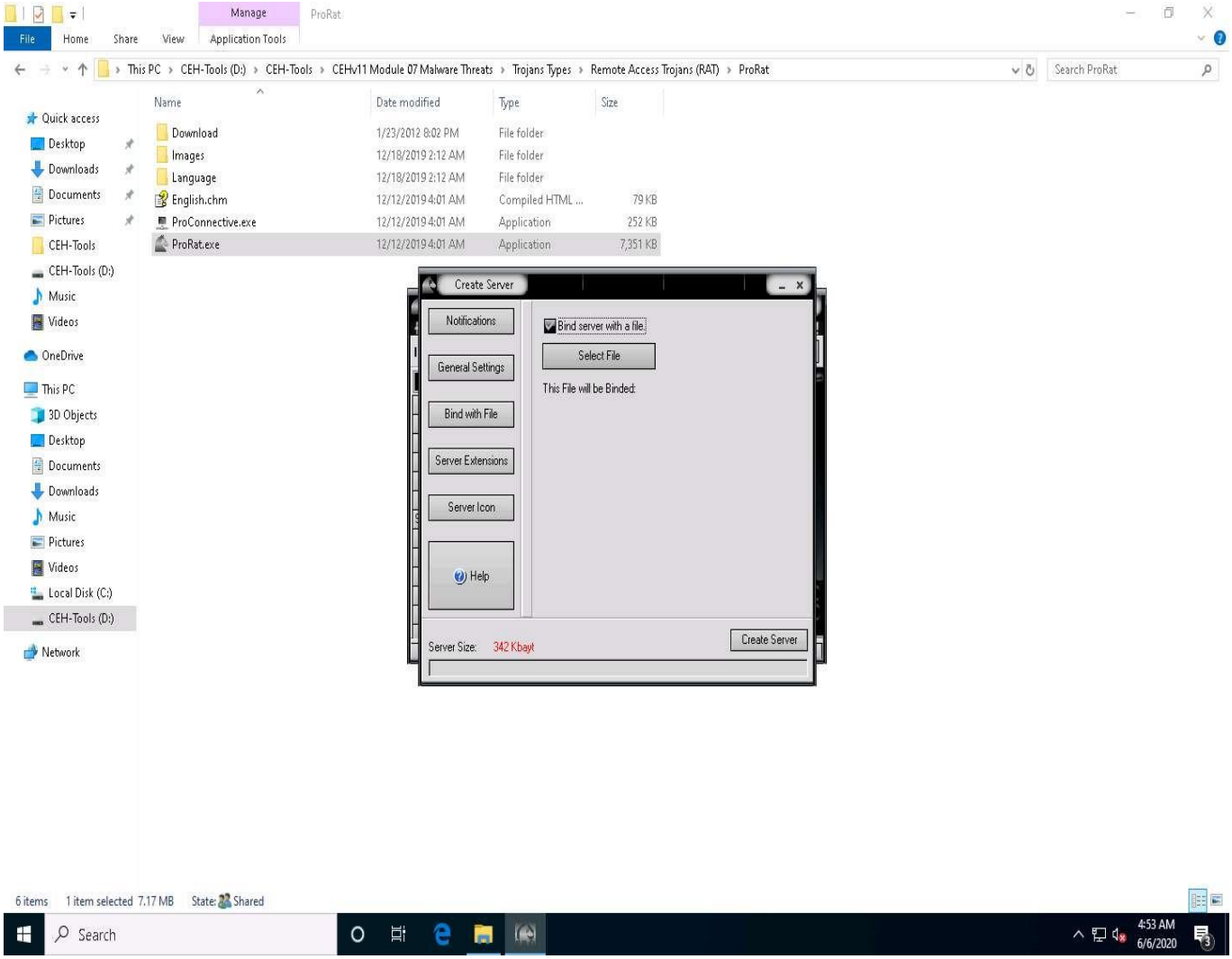
5. ☐ The **Create Server** window appears. In **Notifications**, leave the settings to default.



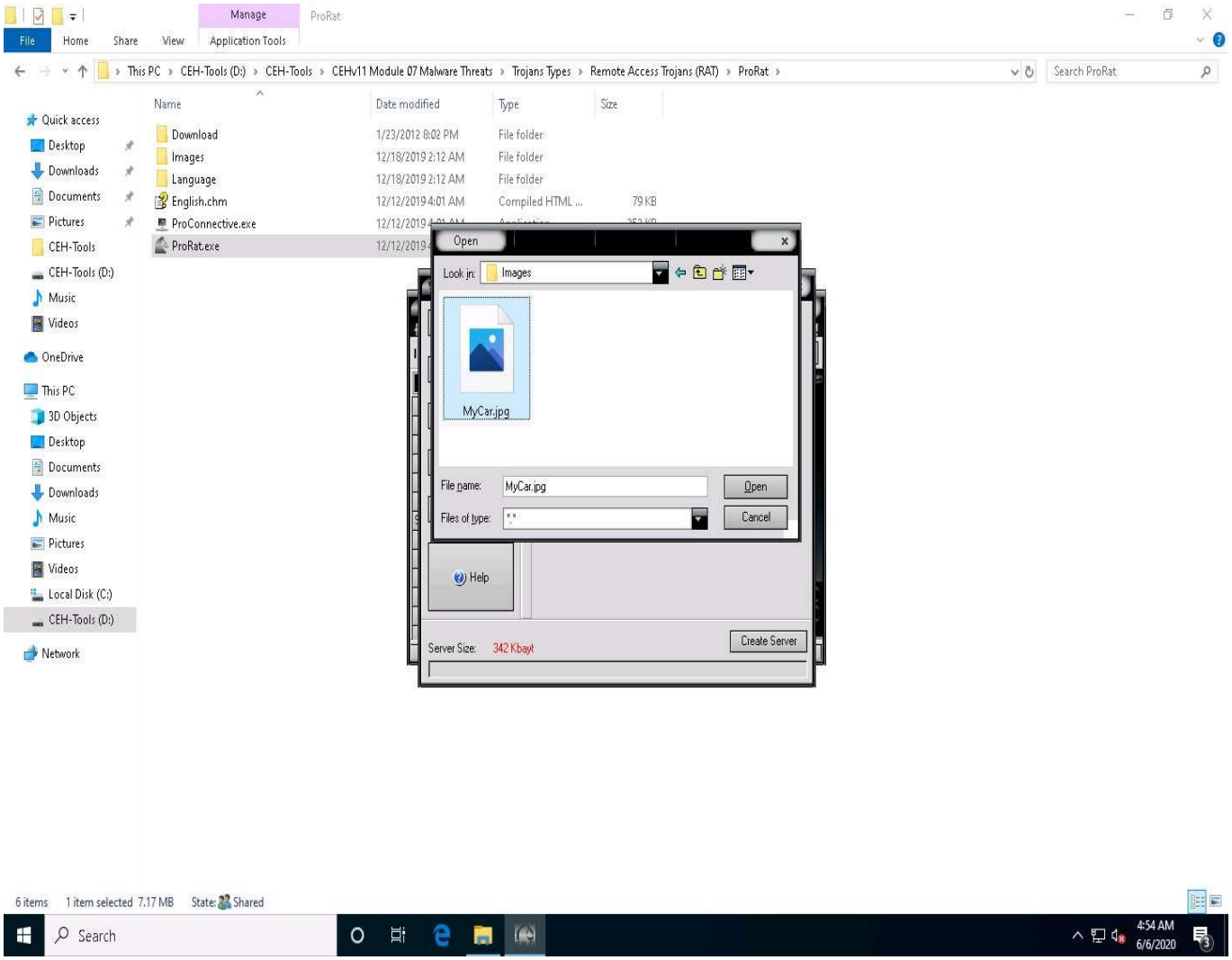
6. Click on the **General Settings** button to configure features such as **Server Port**, **Server Password**, **Victim Name**, and **port number**. In this lab, the default settings are chosen. Note down the **Server password**.
7. Uncheck the highlighted options under the **Victim Name** field, as shown in the screenshot.



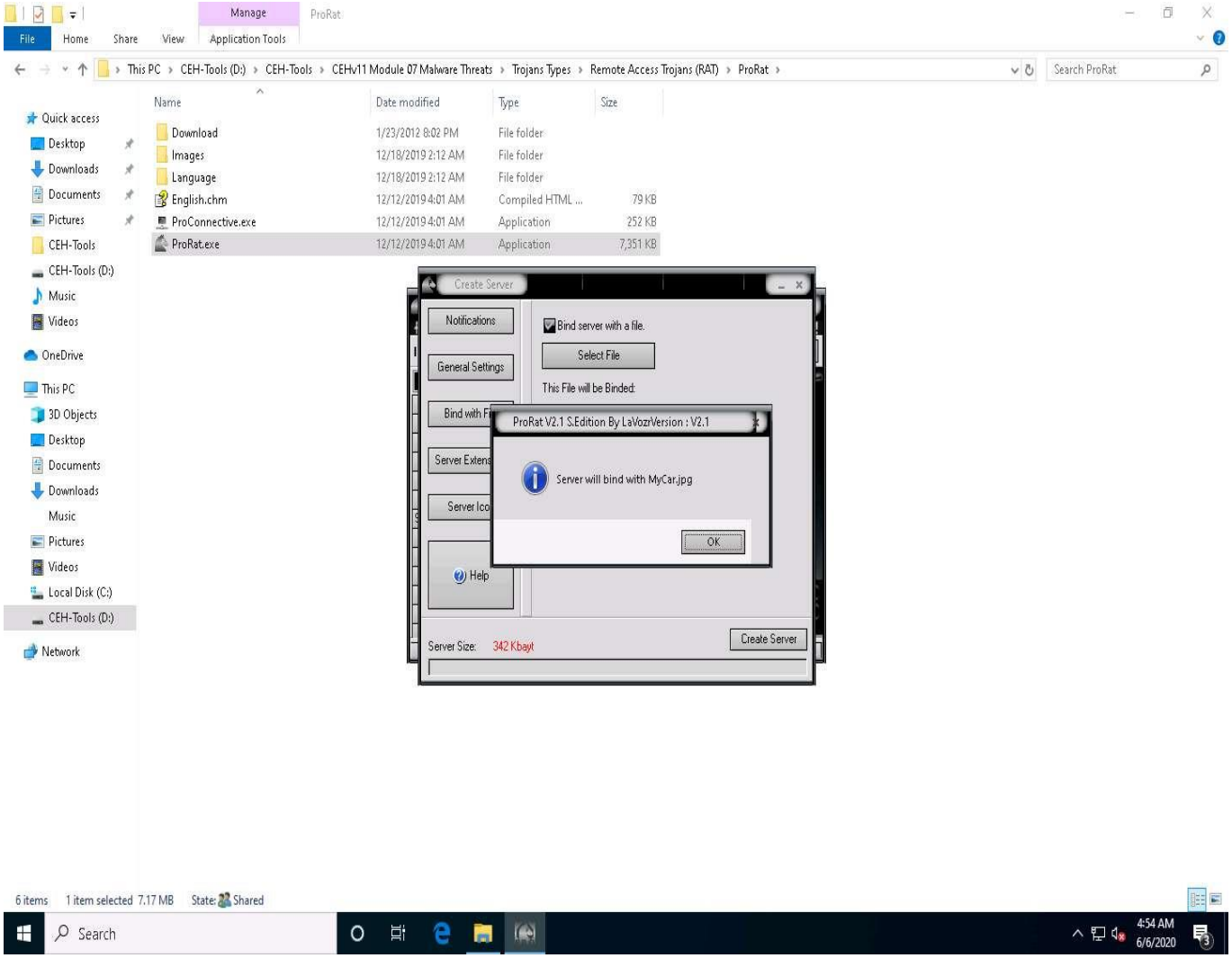
8. ☐ Click on the **Bind with File** button to bind the server with a file. In this lab, we are using a **.jpg** file to bind the server.
9. ☐ Check the **Bind server with a file** option and then click the **Select File** button.



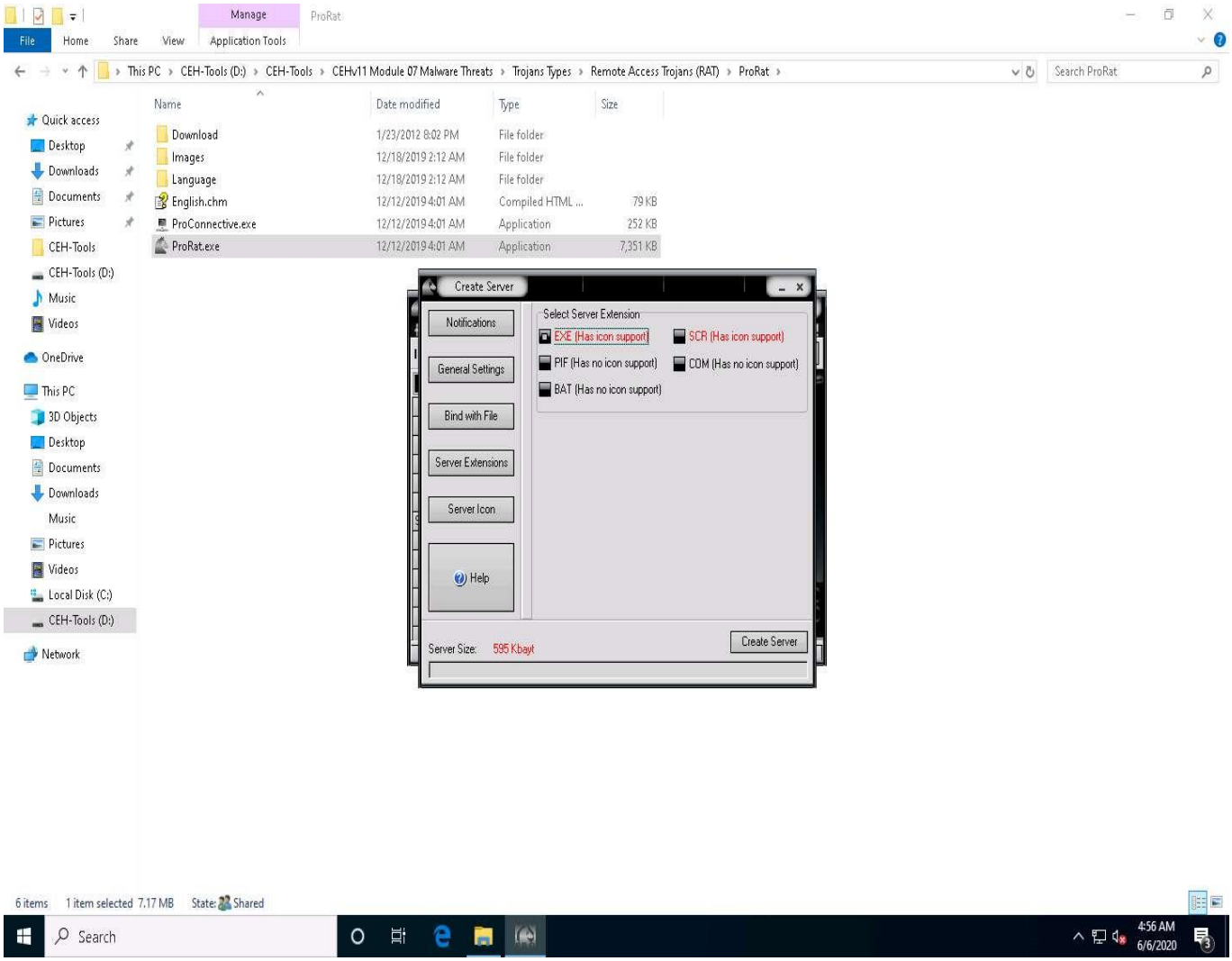
10. An **open** pop-up window appears; navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat\Images** and select **MyCar.jpg** in the browser window. Click **Open** to bind the file.



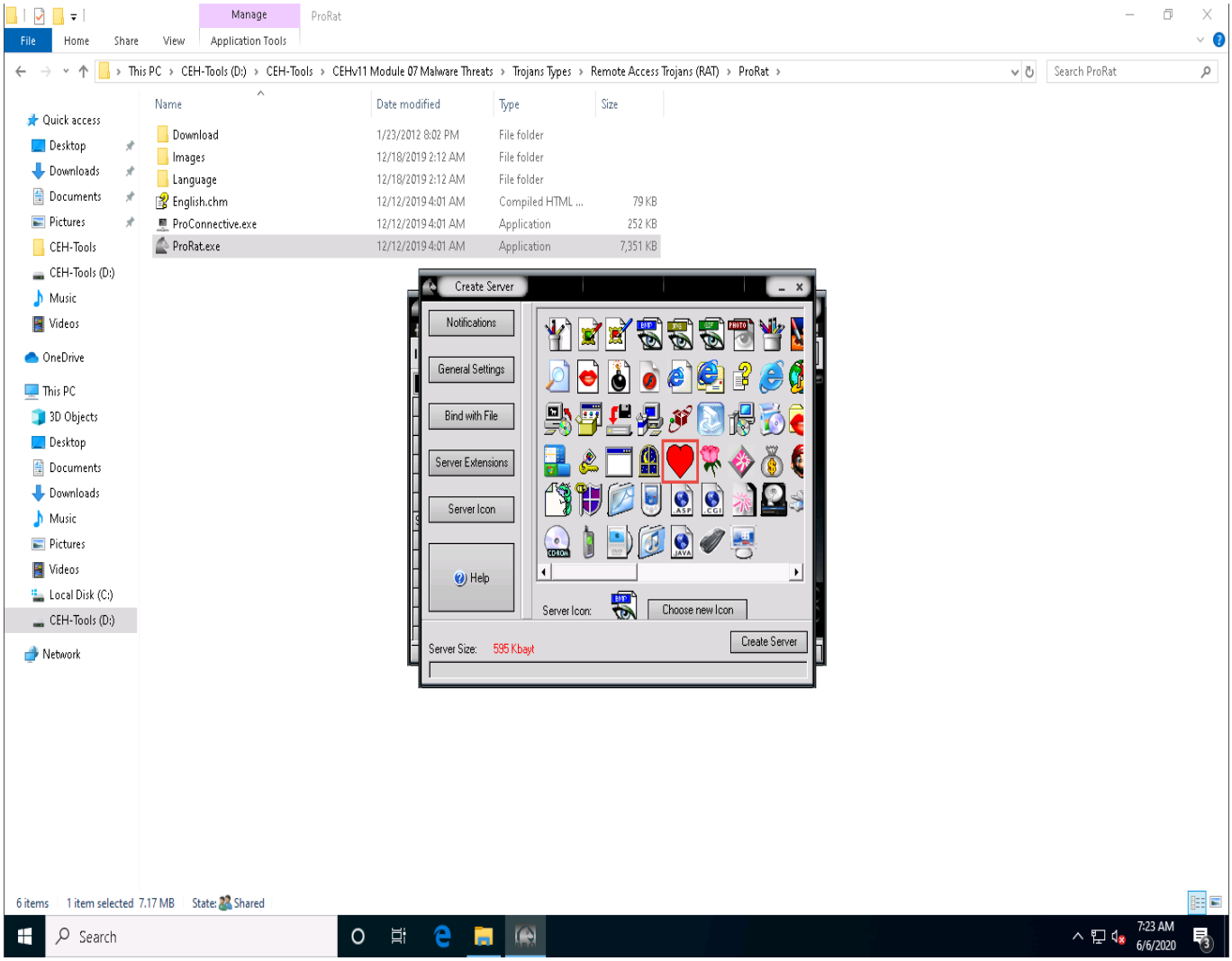
11. A pop-up displays the prompt: **Server will bind with MyCar.jpg**; click **OK**.



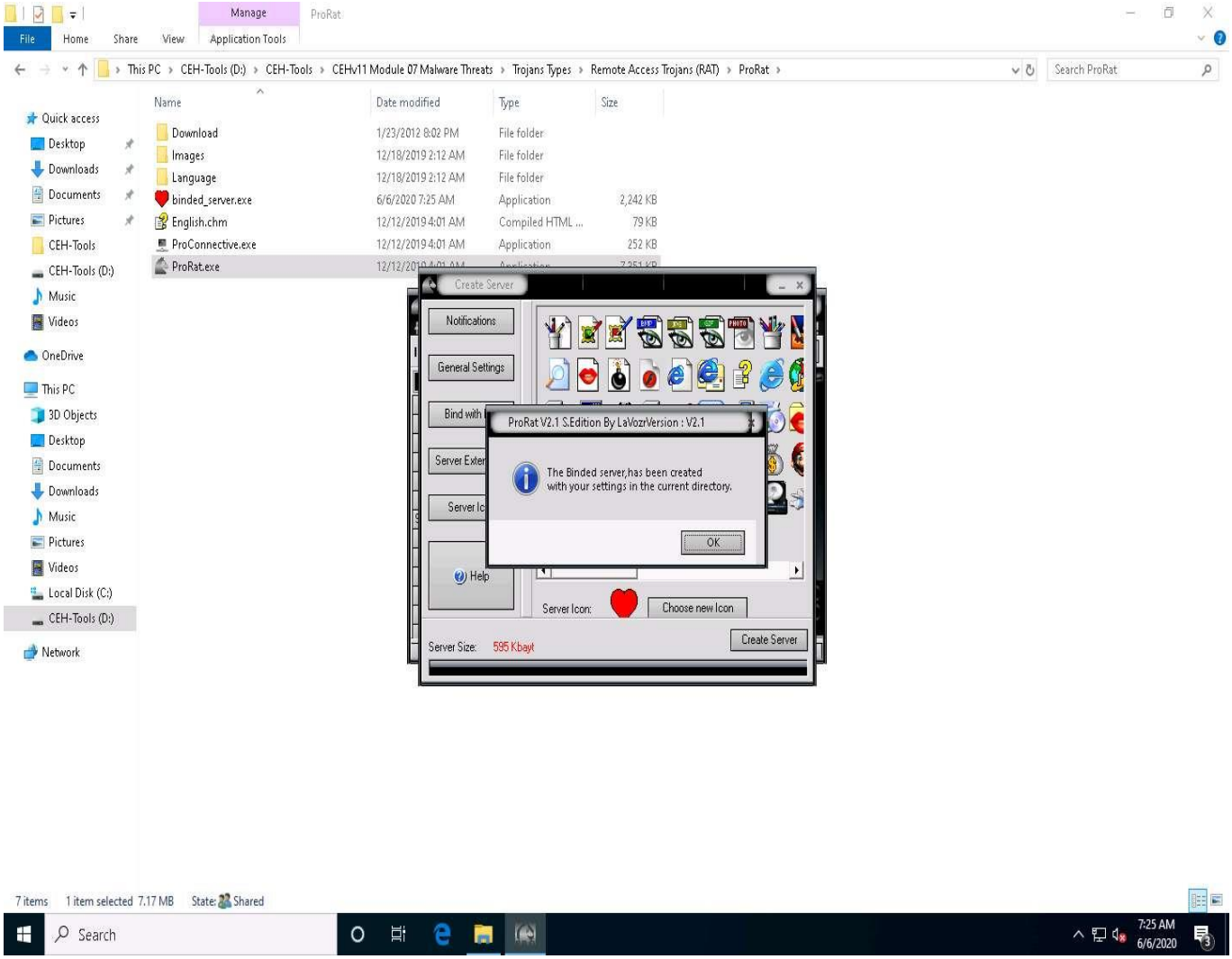
12. ☐ Click the **Server Extensions** button.
13. ☐ Under **Select Server Extension**, ensure that the **EXE (Has icon support)** checkbox is ticked.



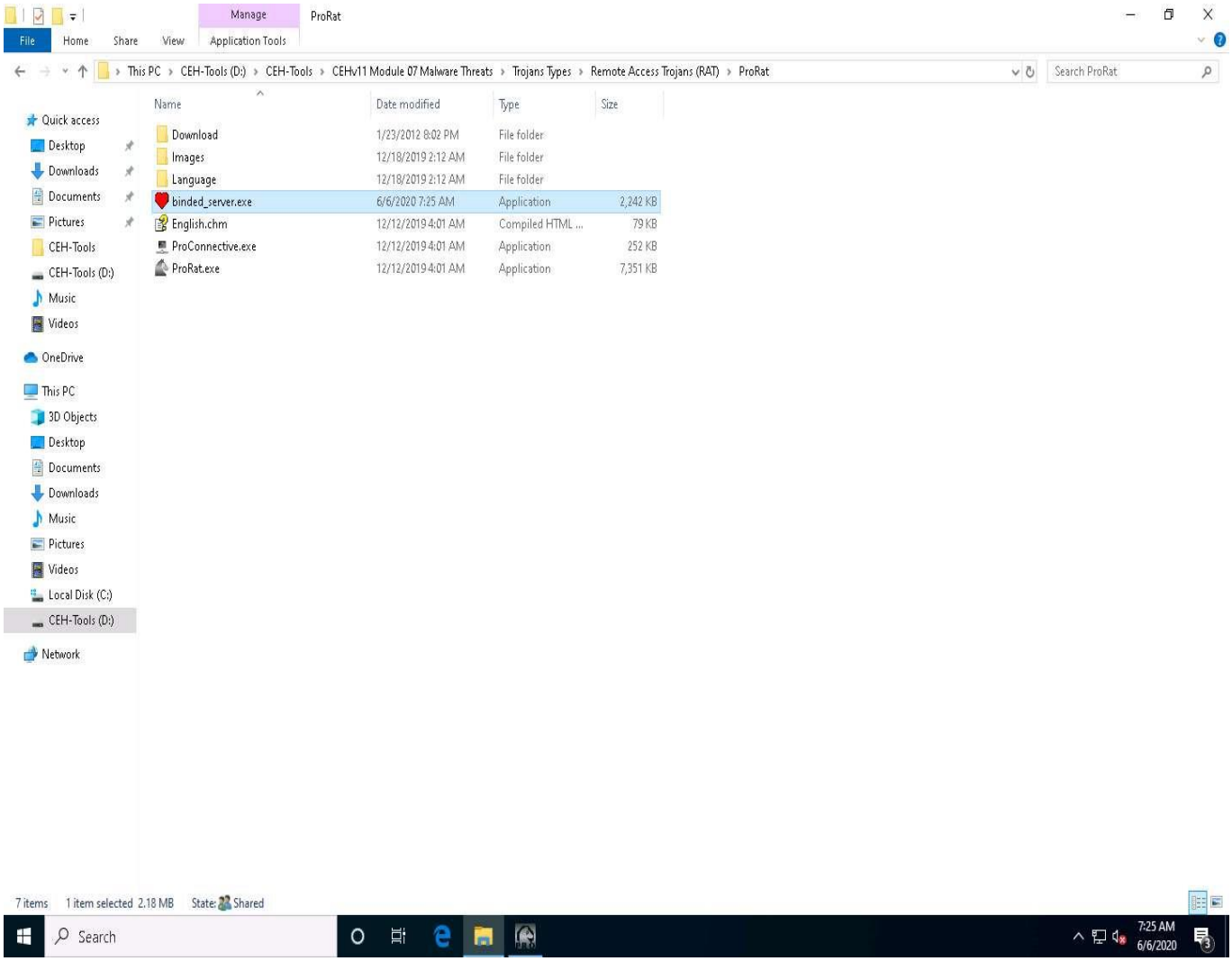
14. ☐ Click the **Server Icon** button. Under **Server Icon**, select any icon, and click **Create Server**.



15. ☐ A pop-up states that the server has been created; click **OK**.



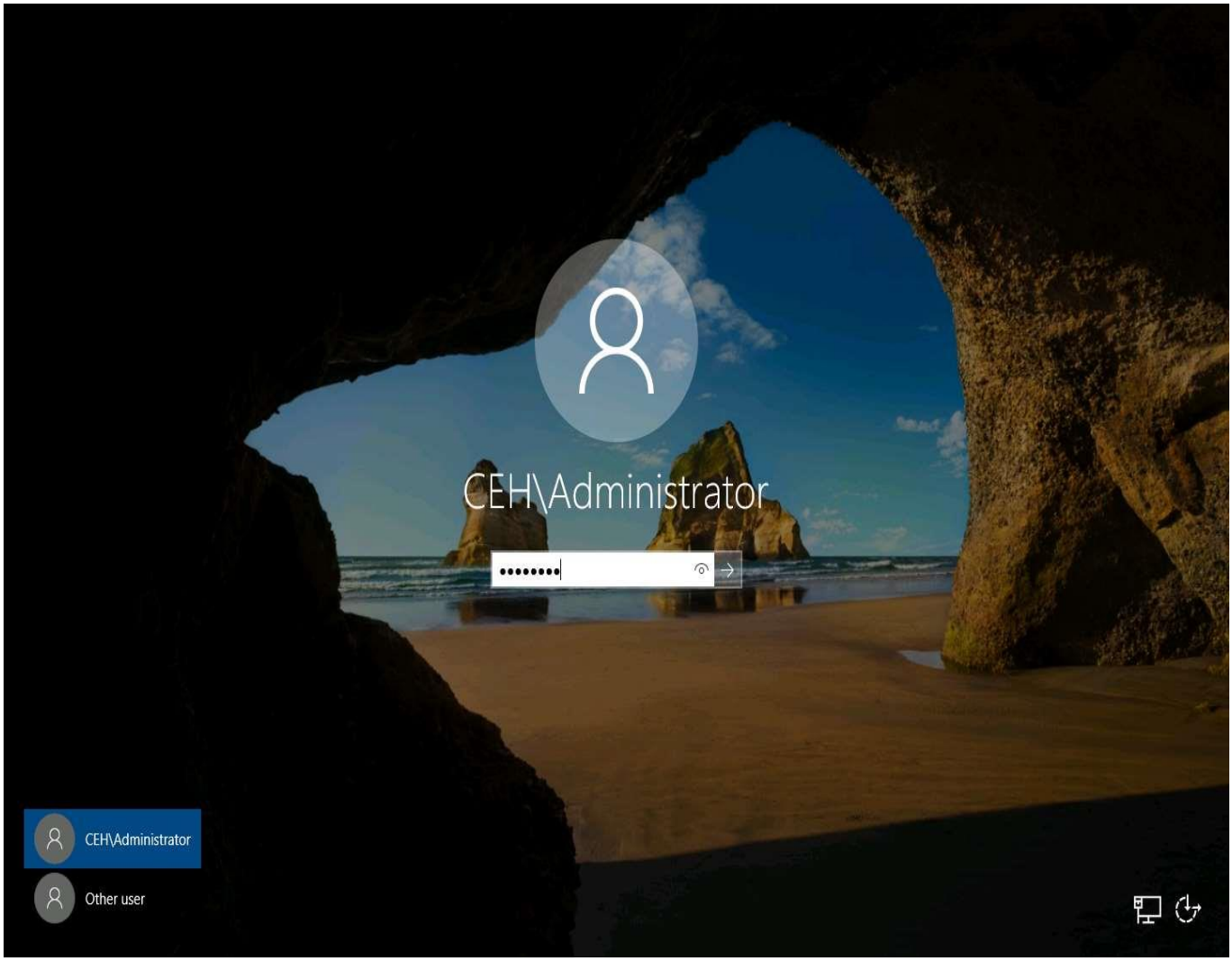
16. ☐ The created server will be saved at **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat**. This server is named **binded_server.exe** by default. Close ProRat's **Create Server** window.



17. ☐ In real-time, hackers may craft such servers and send them by email or other communication media to the victim's machine.

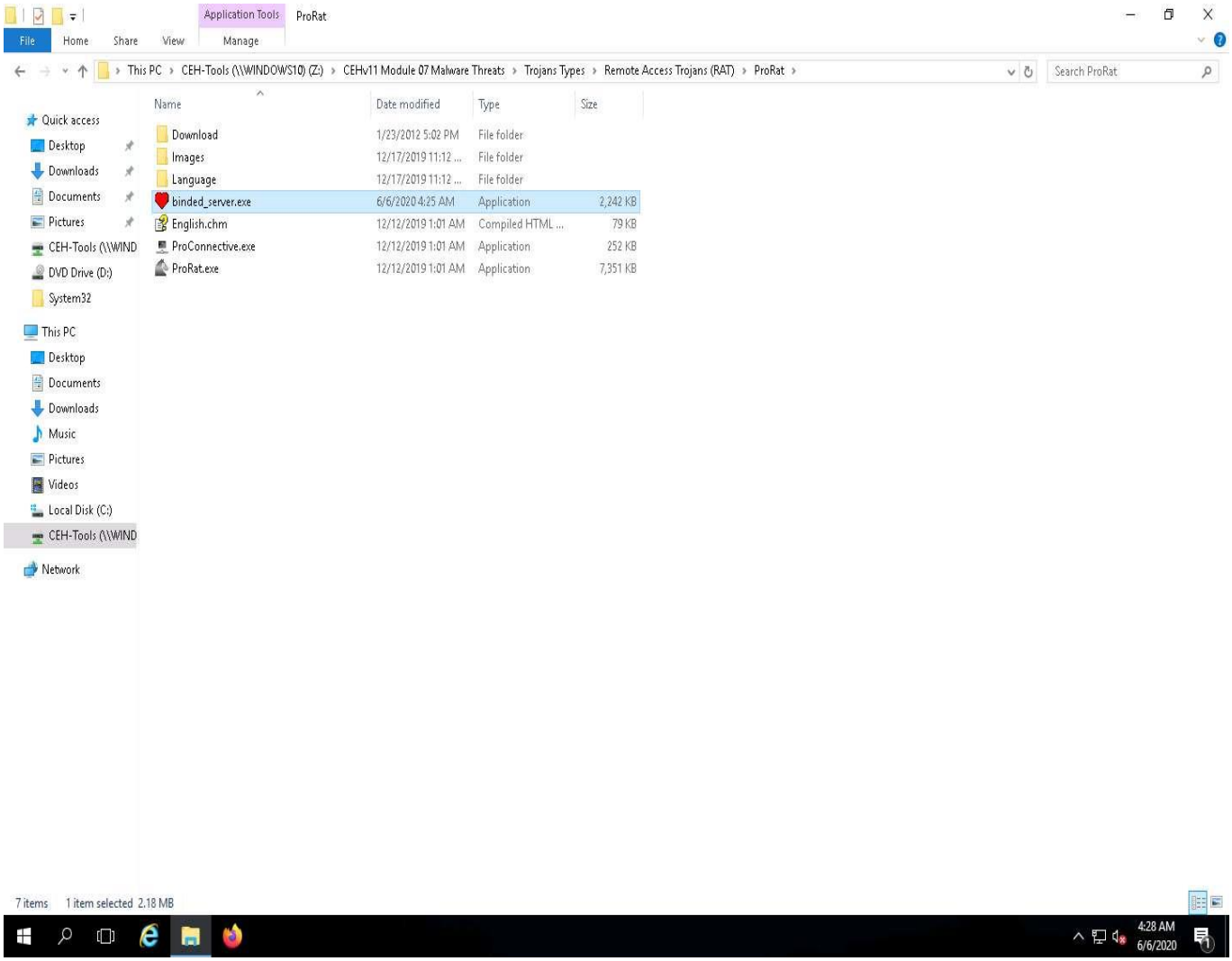
You need to **zip** the file before emailing it, as you cannot attach **.exe** files on some mail servers.

18. ☐ Click Windows Server 2016 to switch to the **Windows Server 2016** machine. Click Ctrl+Alt+Delete to activate the machine, by default, **CEH\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.

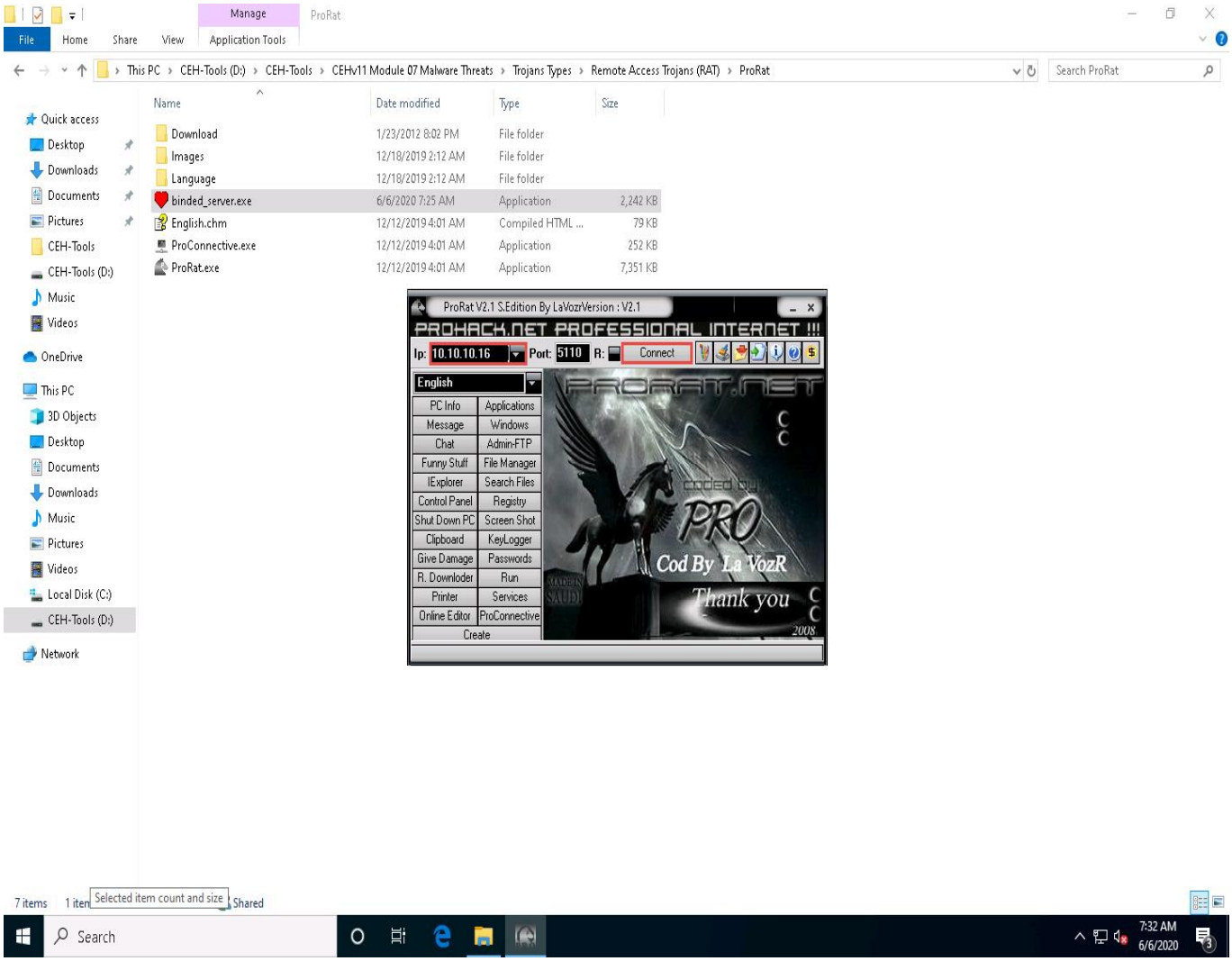


19. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat** and double-click **binder_server.exe**.

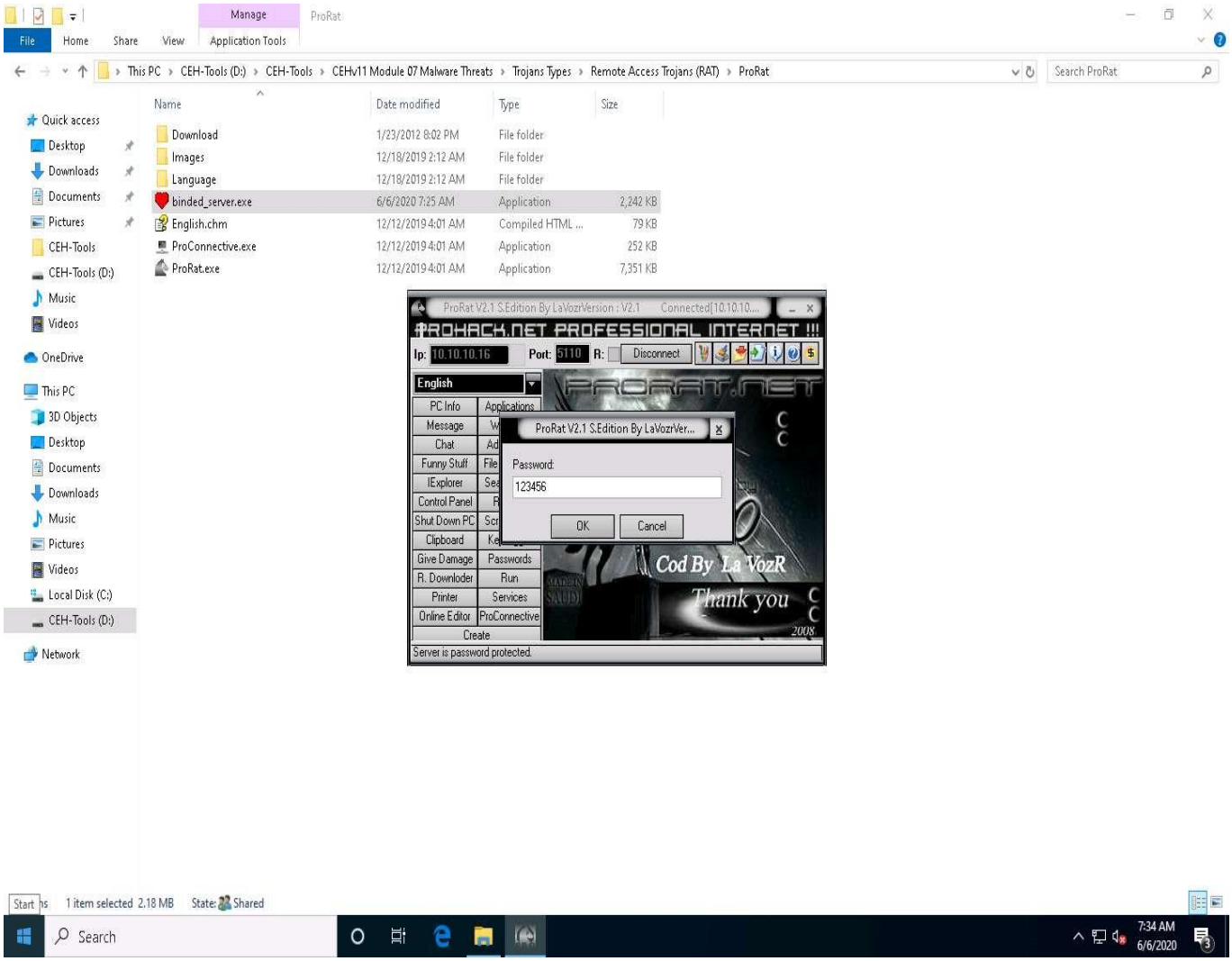
If an **Open File - Security** Warning pop-up appears, click **Run**.



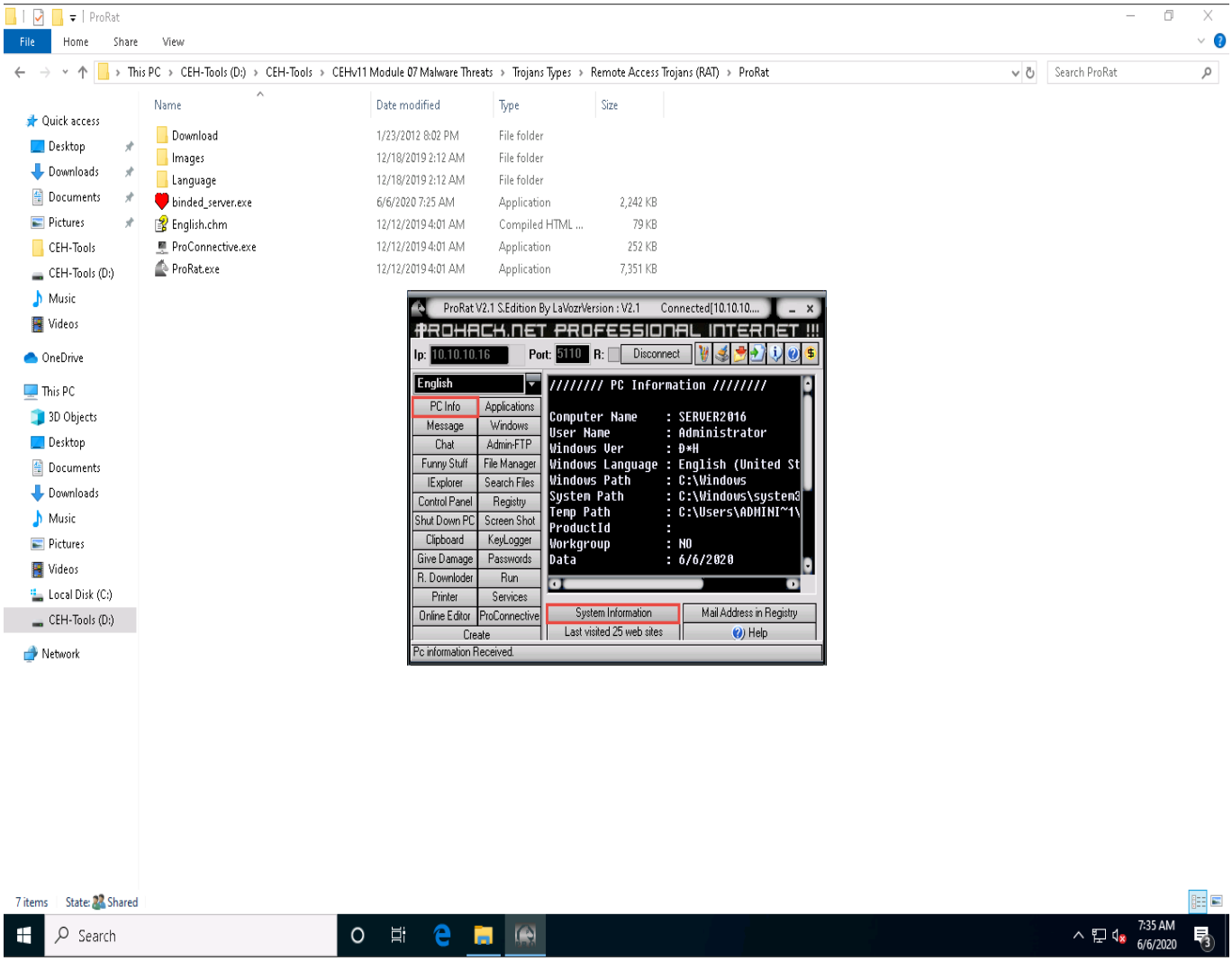
20. ☐ Click Windows 10 to switch back to the **Windows 10** machine, and enter the IP address of **Windows Server 2016** in the **Ip** field; keep the default port number in the ProRat main window, and click **Connect**.
21. ☐ In this lab, the IP address of **Windows Server 2016** is **10.10.10.16**.



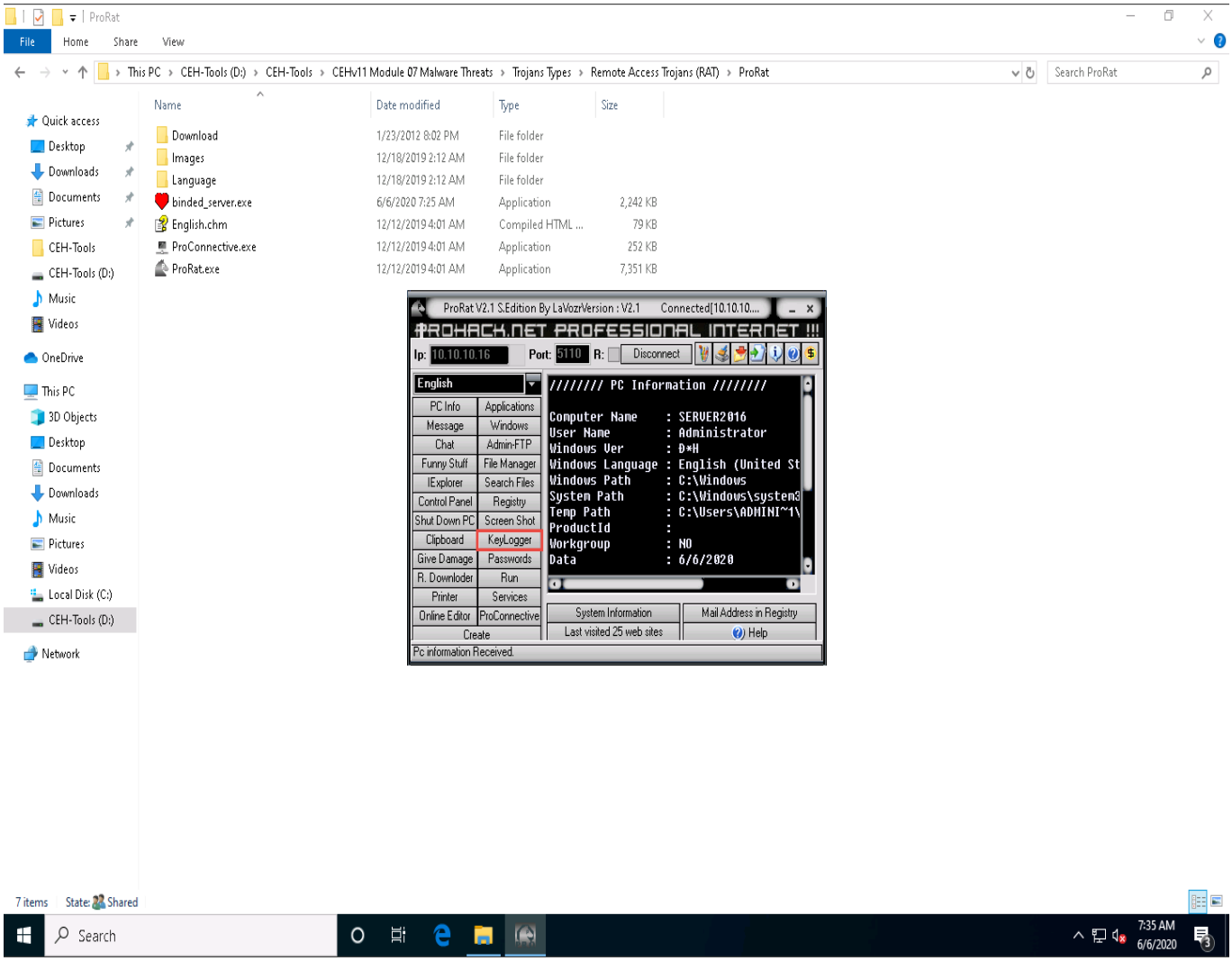
22. ☐ Enter the **password** you noted down when creating the server and click **OK**.



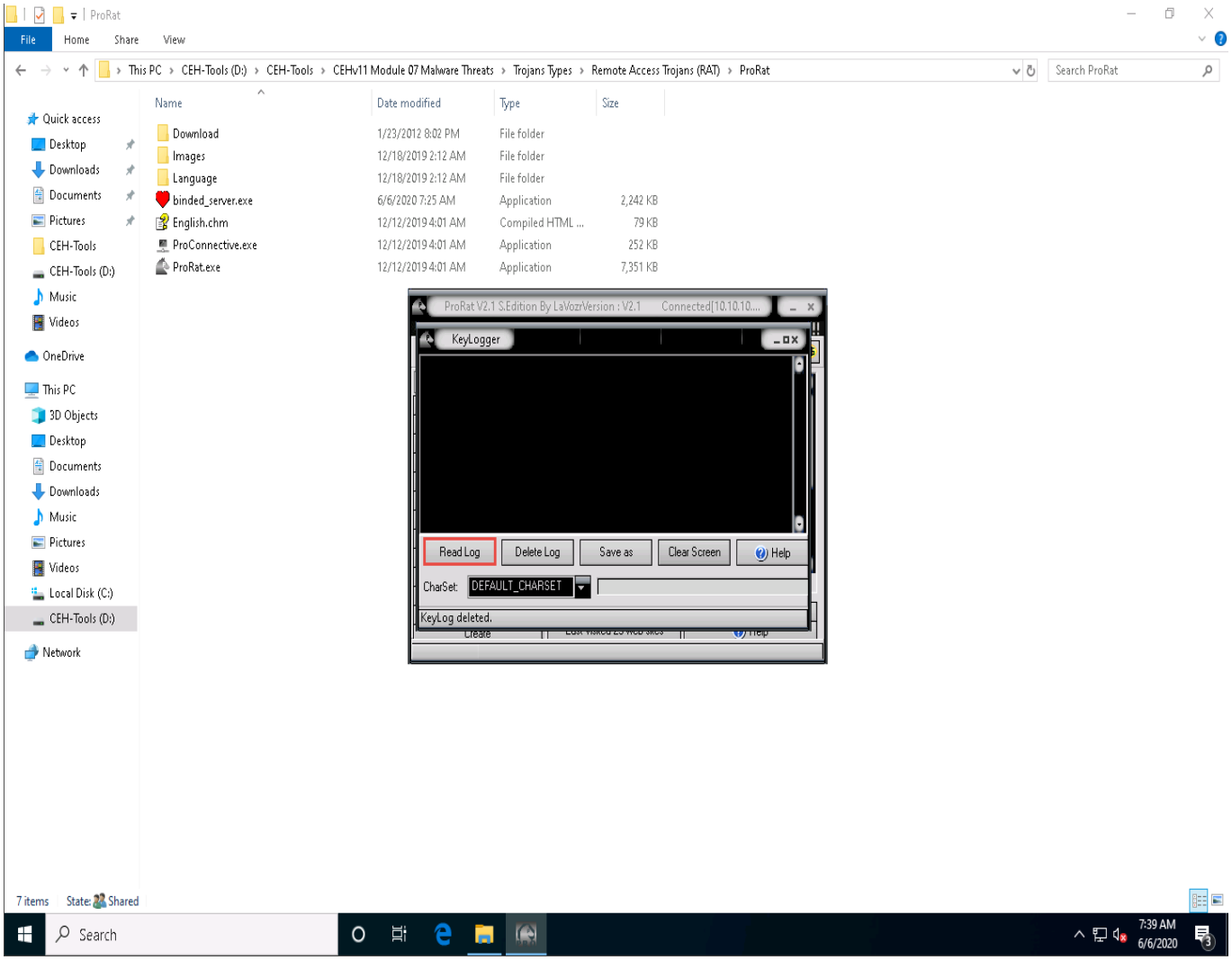
23. ☐ Now, you are **connected** to the victim machine.
24. ☐ ProRat begins to monitor user activities. It records all passwords, keystrokes, and other sensitive data.
25. ☐ To test the connection, click **PC Info**, and choose **System Information**.
26. ☐ ProRat displays the information of the victim machine, as shown in the screenshot.



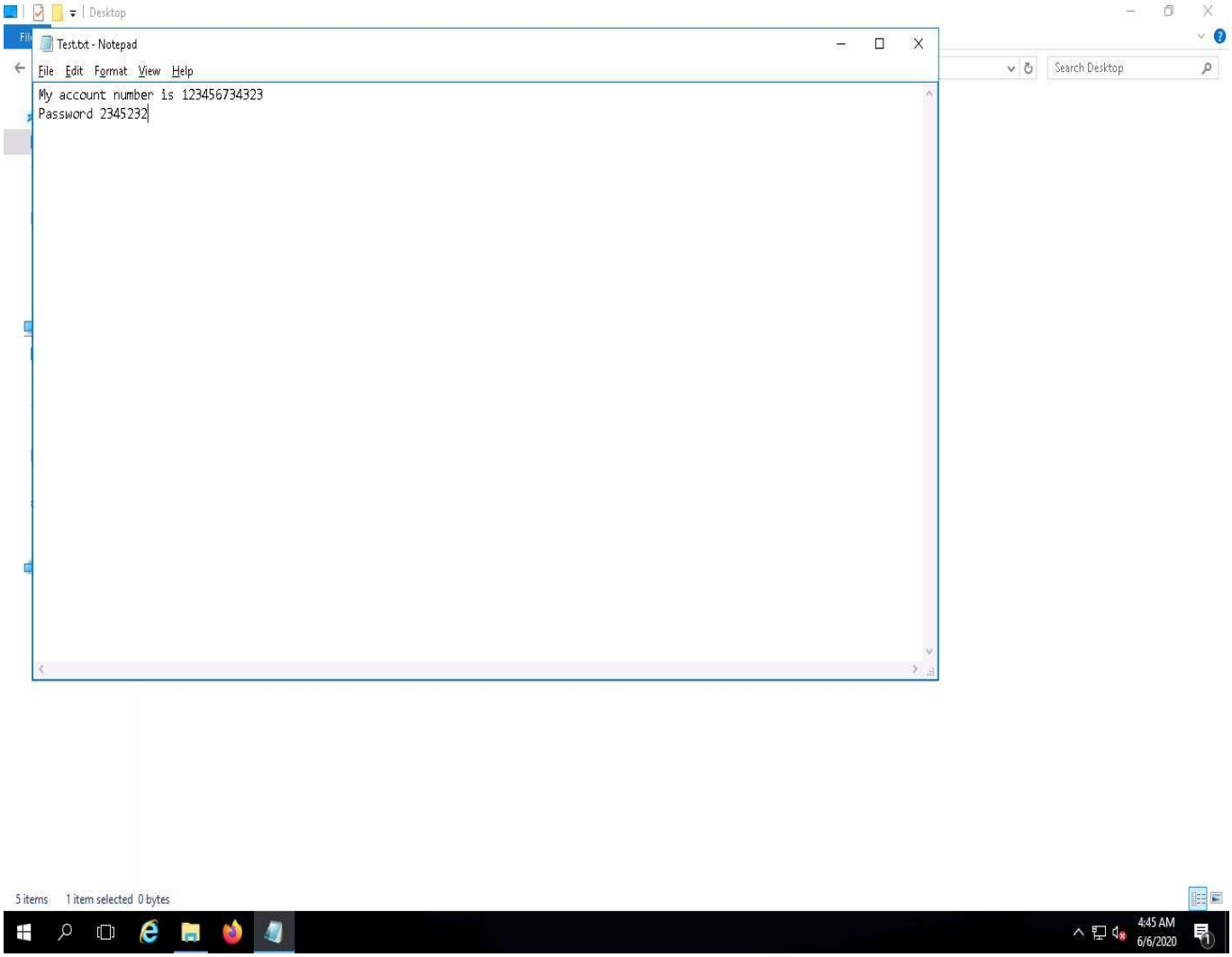
27. Click on **KeyLogger** to steal the user passwords for the online system. This will read the keystrokes performed on the victim machine.



28. The **KeyLogger** window appears; click **Read Log** to view the key logs created by the target user on the victim machine.

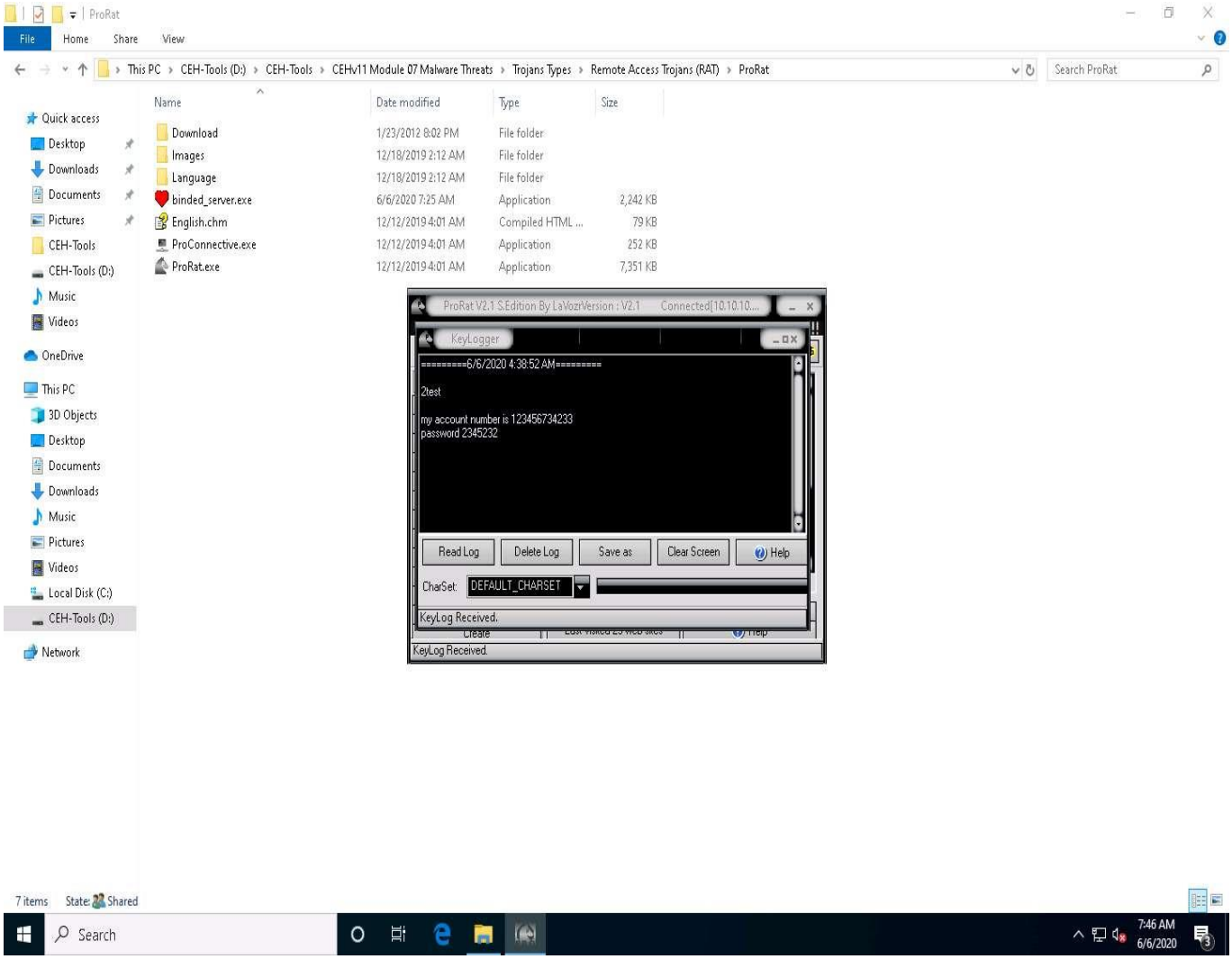


29. Click Windows Server 2016 to switch to the **Windows Server 2016** machine. Click Ctrl+Alt+Delete to activate the machine, by default, **CEH\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**. Navigate to the **Desktop** and open **Notepad** or a browser window, and type any text.

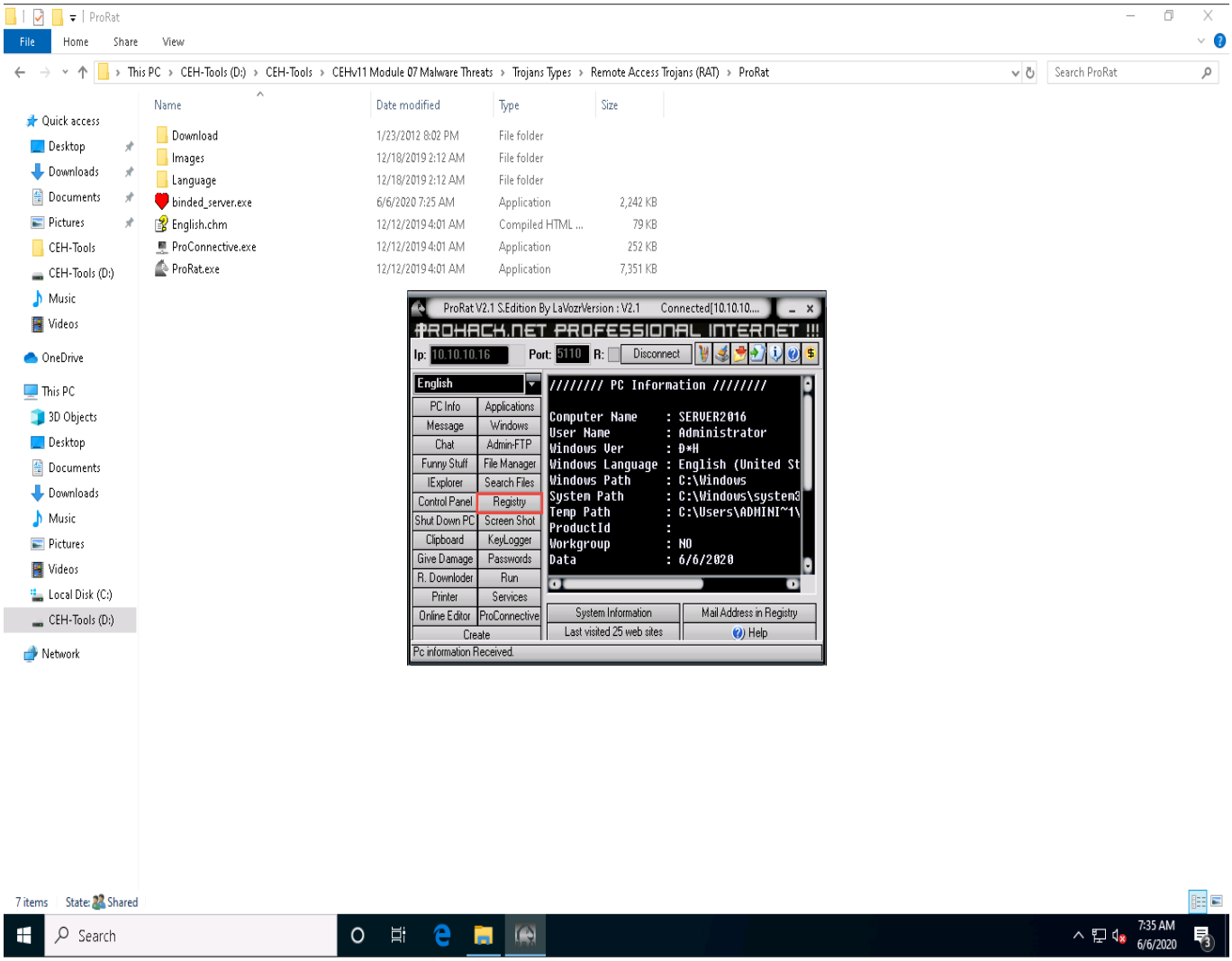


30. ☐ While the victim is writing a message or entering a username and password, you can capture the log entity.
31. ☐ Now, click Windows 10 to switch to the Windows 10 machine, and periodically click **Read Log** to check for keystrokes logged from the victim machine. Close the KeyLogger window.

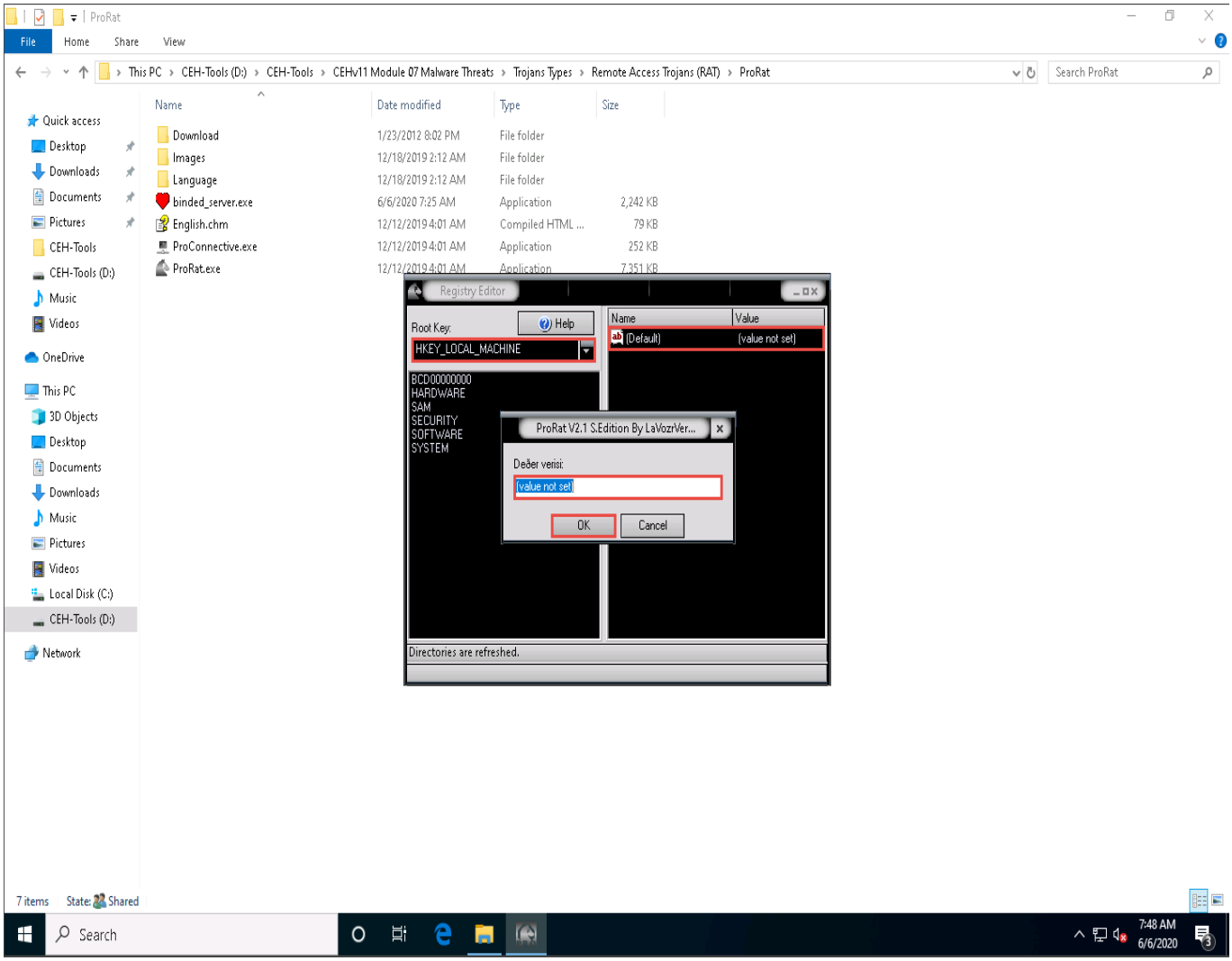
ProRat Keylogger will not read special characters.



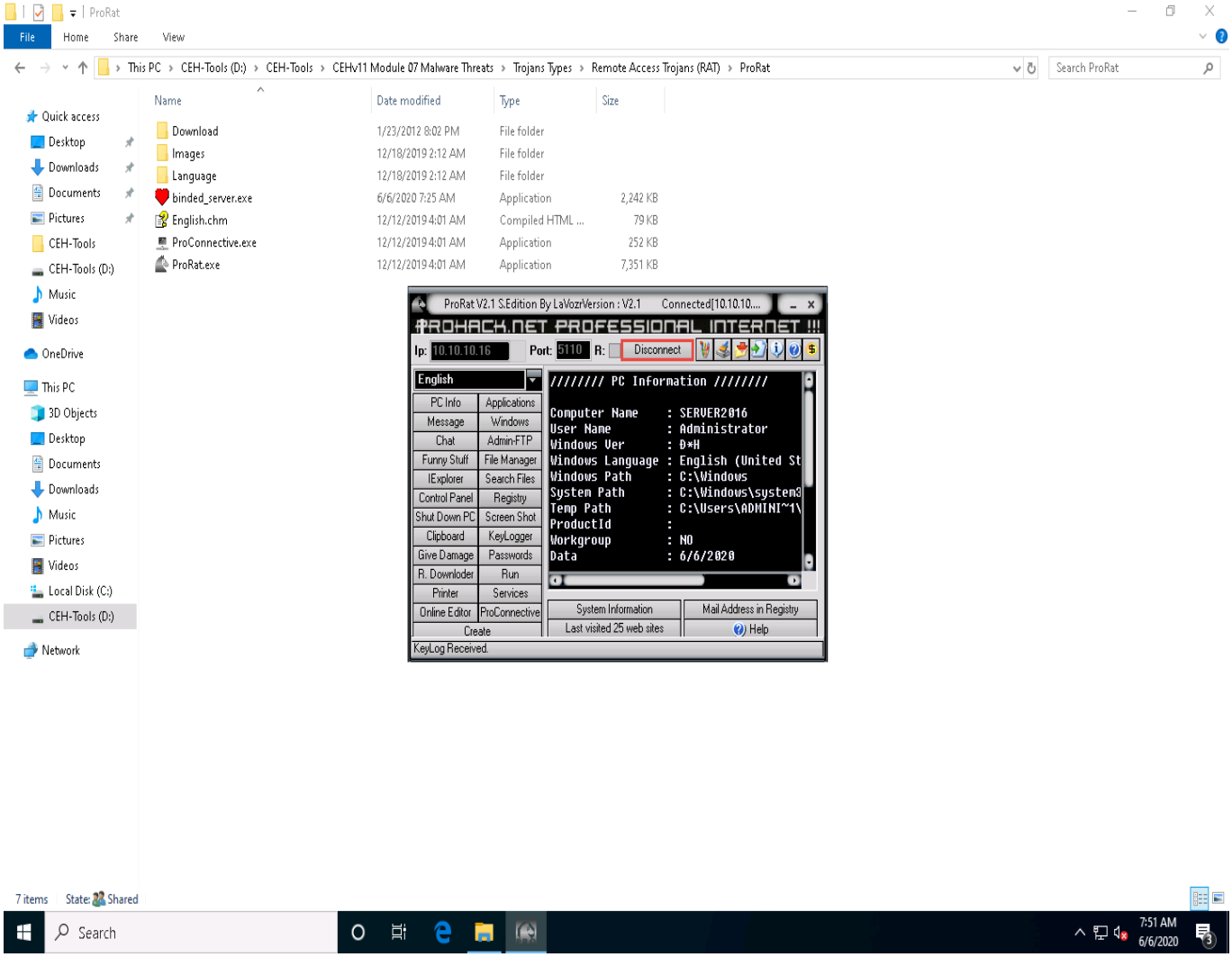
32. ☐ Now, click the **Registry** button to view the registry editor of the **Windows Server 2016** machine.



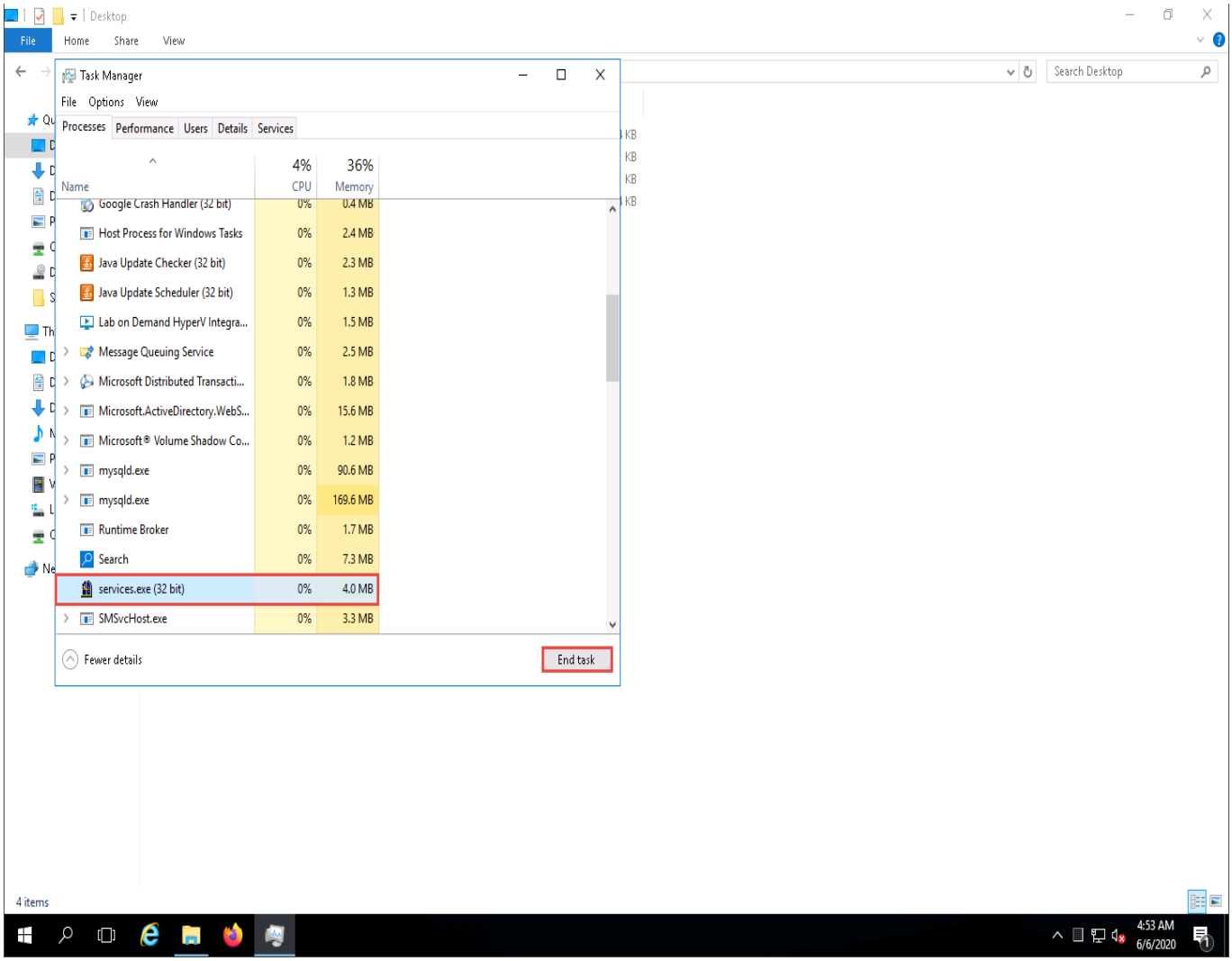
33. The **Registry Editor** window appears, where you can choose the Registry Editor from the **Root Key** drop-down list. You can see and also modify the registry of the victim's machine, as shown in the screenshot.



34. ☐ Close the **Registry** related windows and switch back to the ProRat main window.
35. ☐ In the same way, you can make use of the other options that allow you to explore and control the victim machine.
36. ☐ On the **Windows 10** machine, click **Disconnect** in the ProRat window.



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

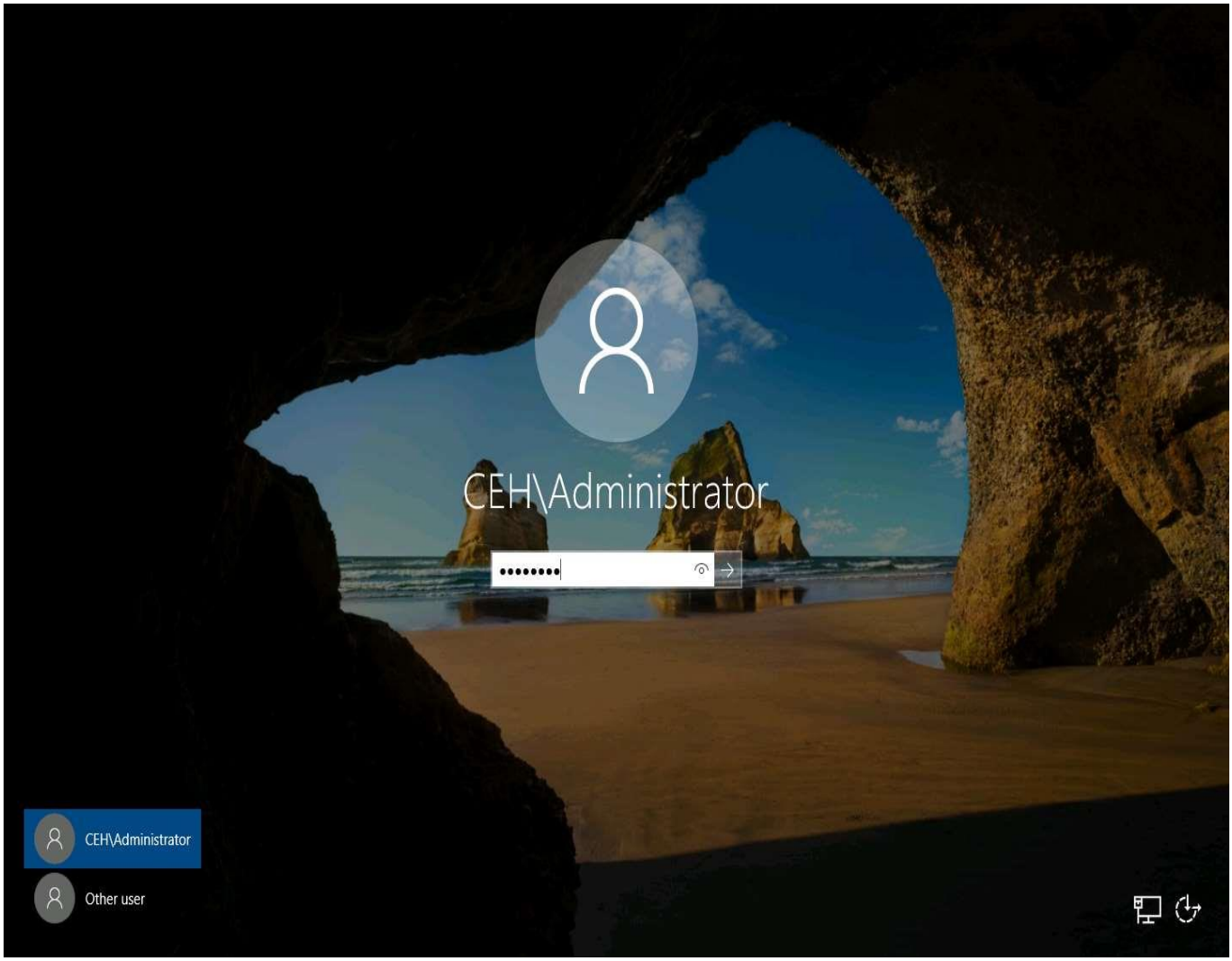


Task 4: Create a Trojan Server using Theef RAT Trojan

Theef is a Remote Access Trojan written in Delphi. It allows remote attackers access to the system via port 9871. Theef is a Windows-based application for both client and server. The Theef server is a virus that you install on a target computer, and the Theef client is what you then use to control the virus.

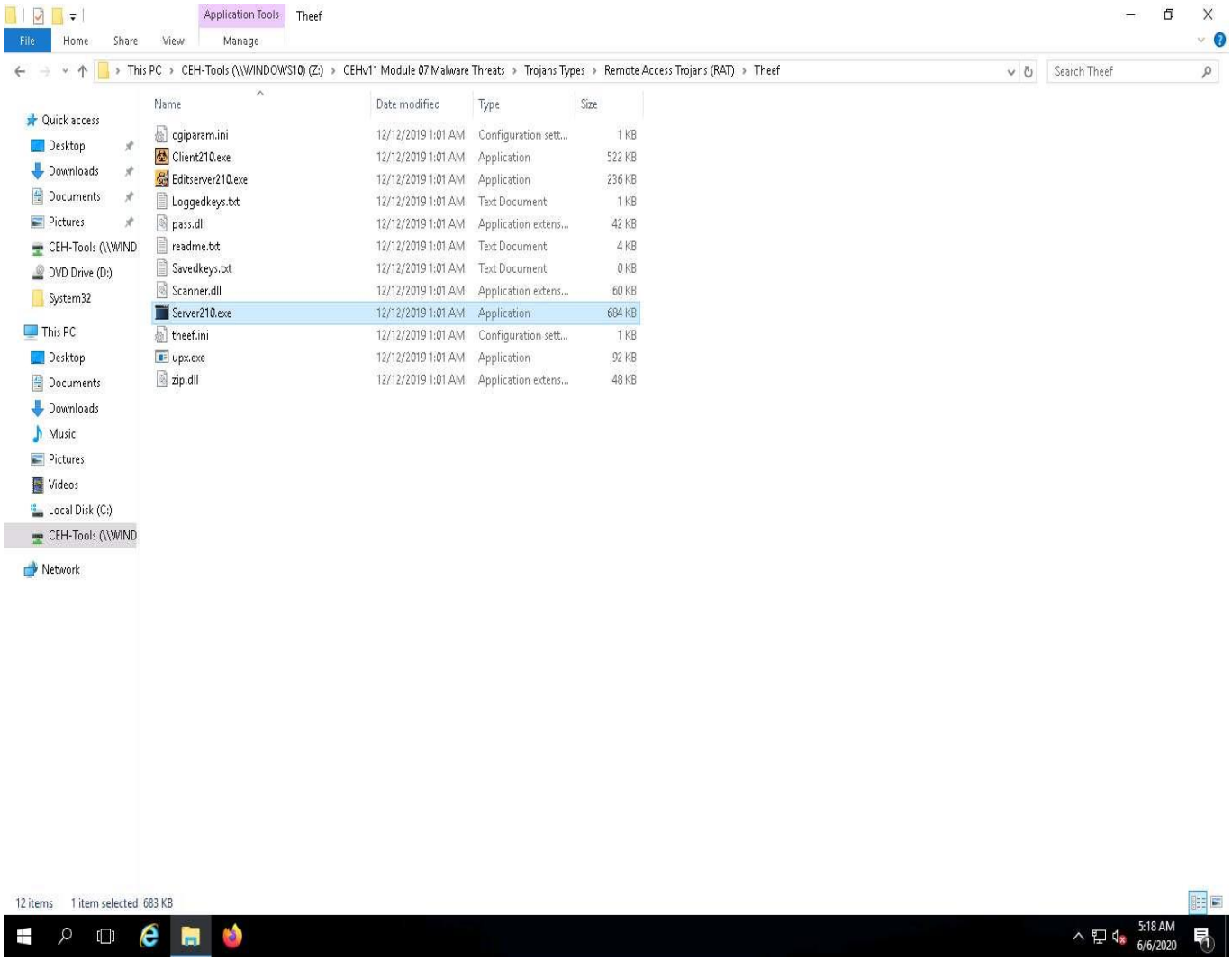
The versions of the created client or host, and the appearance of its website, may differ from that of this lab. However, the actual process of creating the server and the client is the same.

1. Generally, an attacker might send a server executable to the victim machine and entice the victim into running it. In this lab, for demonstration purposes, we are directly executing the file on the victim machine, **Windows Server 2016**.
2. Click Windows Server 2016 to switch to the **Windows Server 2016** machine. Click Ctrl+Alt+Delete to activate the machine, by default, **CEH\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.

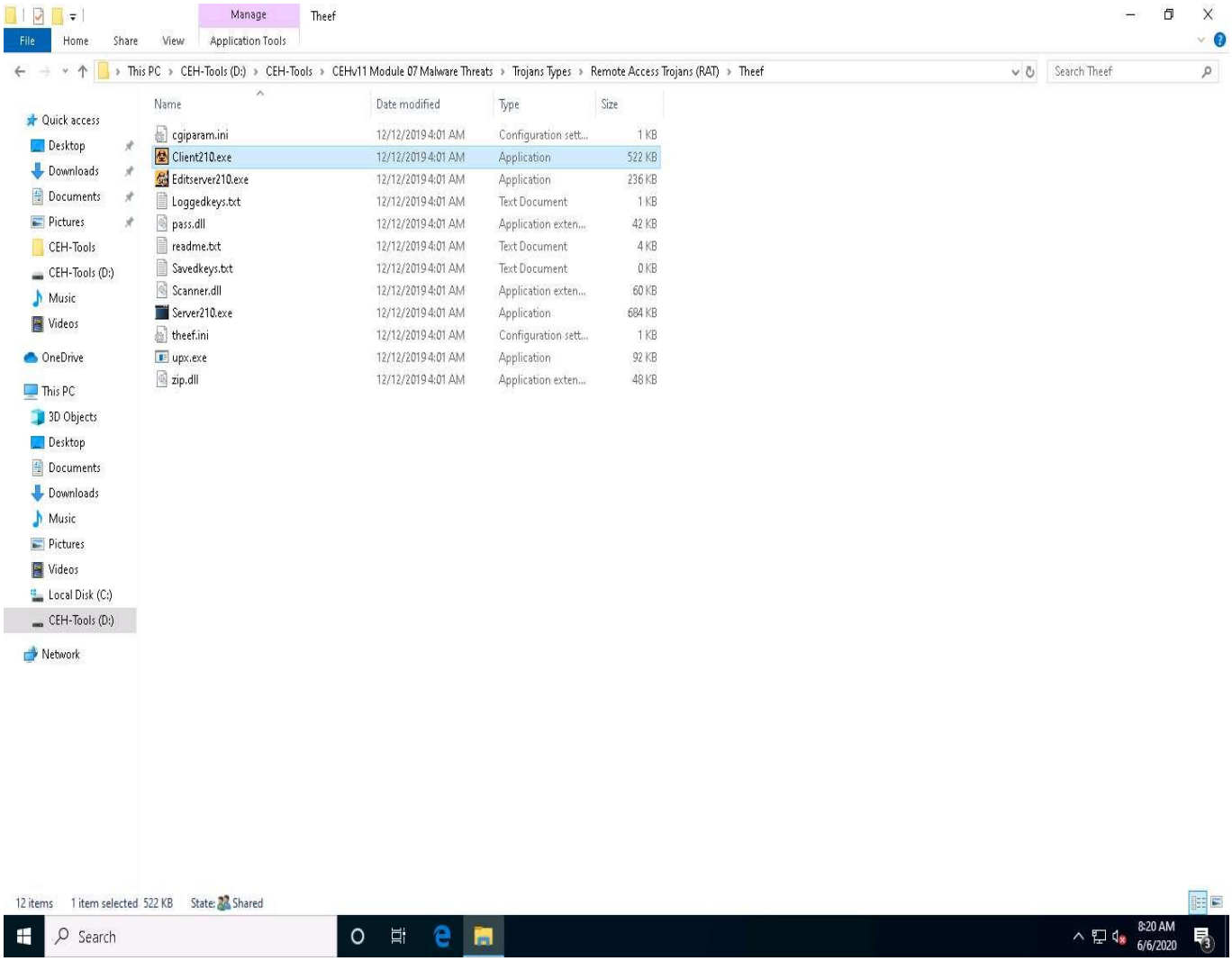


3. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Server210.exe** to run the Trojan on the victim machine.

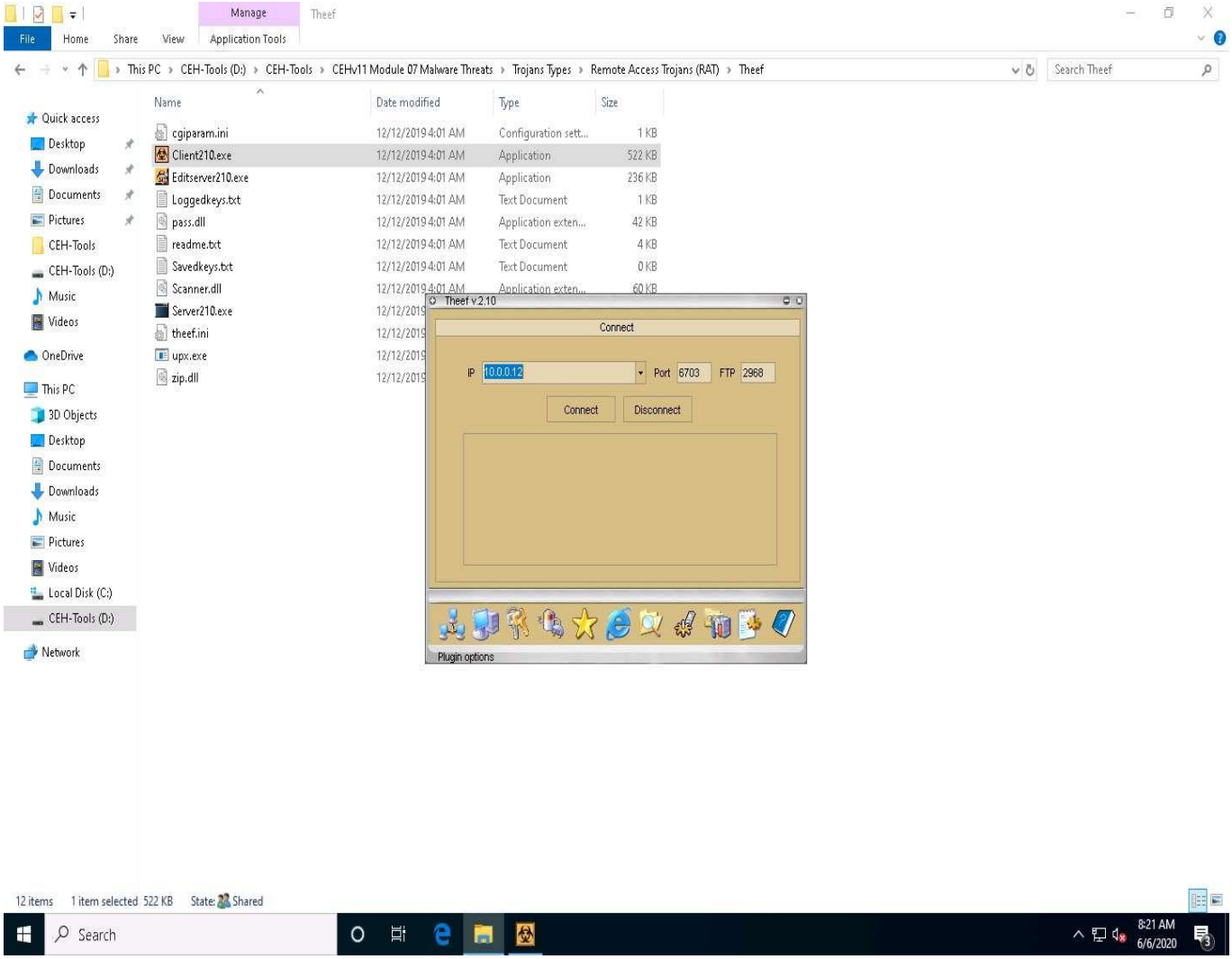
If an **Open File - Security** Warning pop-up appears, click **Run**.



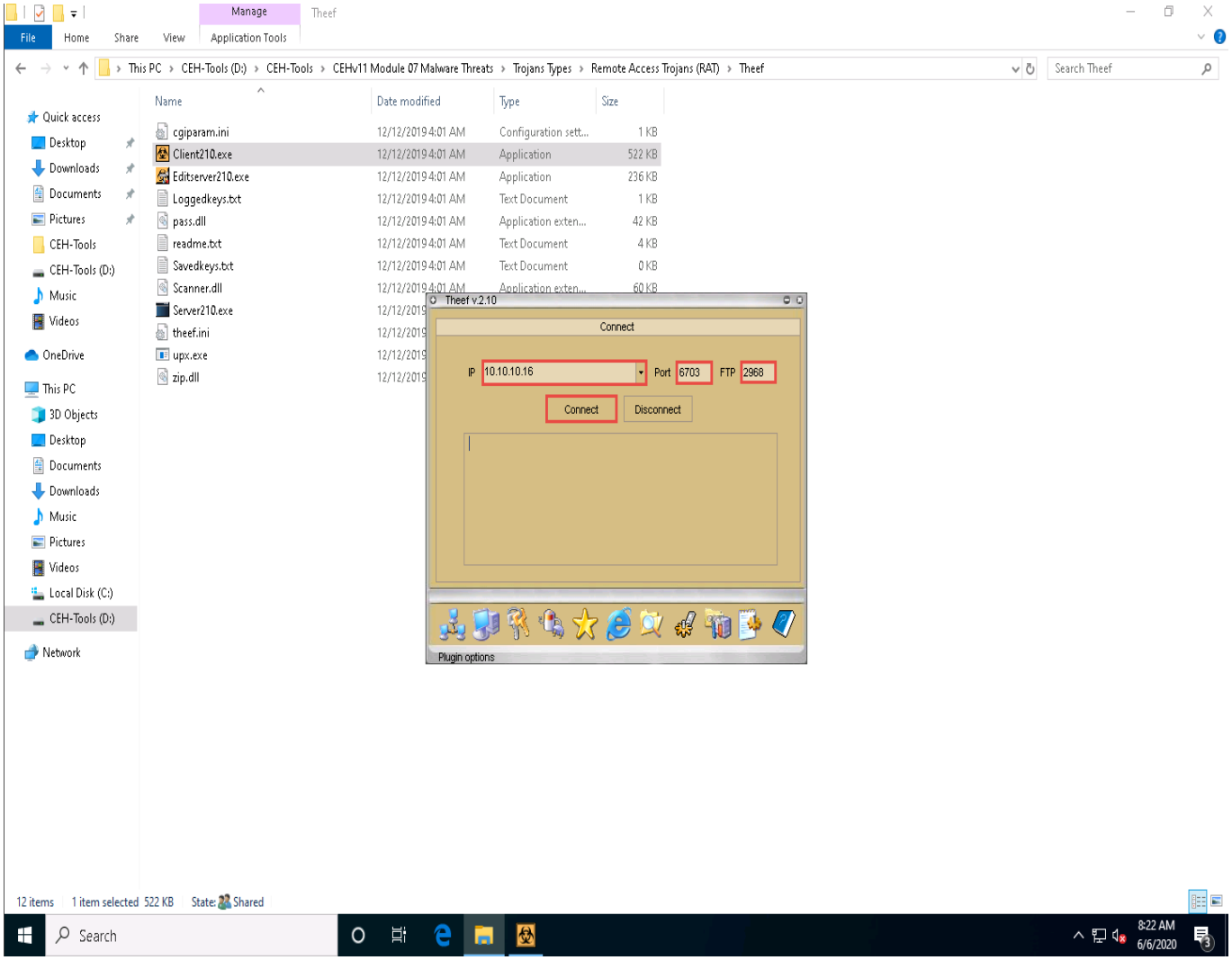
4. Now, click Windows 10 to switch to the **Windows 10** machine (as an attacker).
5. Navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Client210.exe** to access the victim machine remotely.



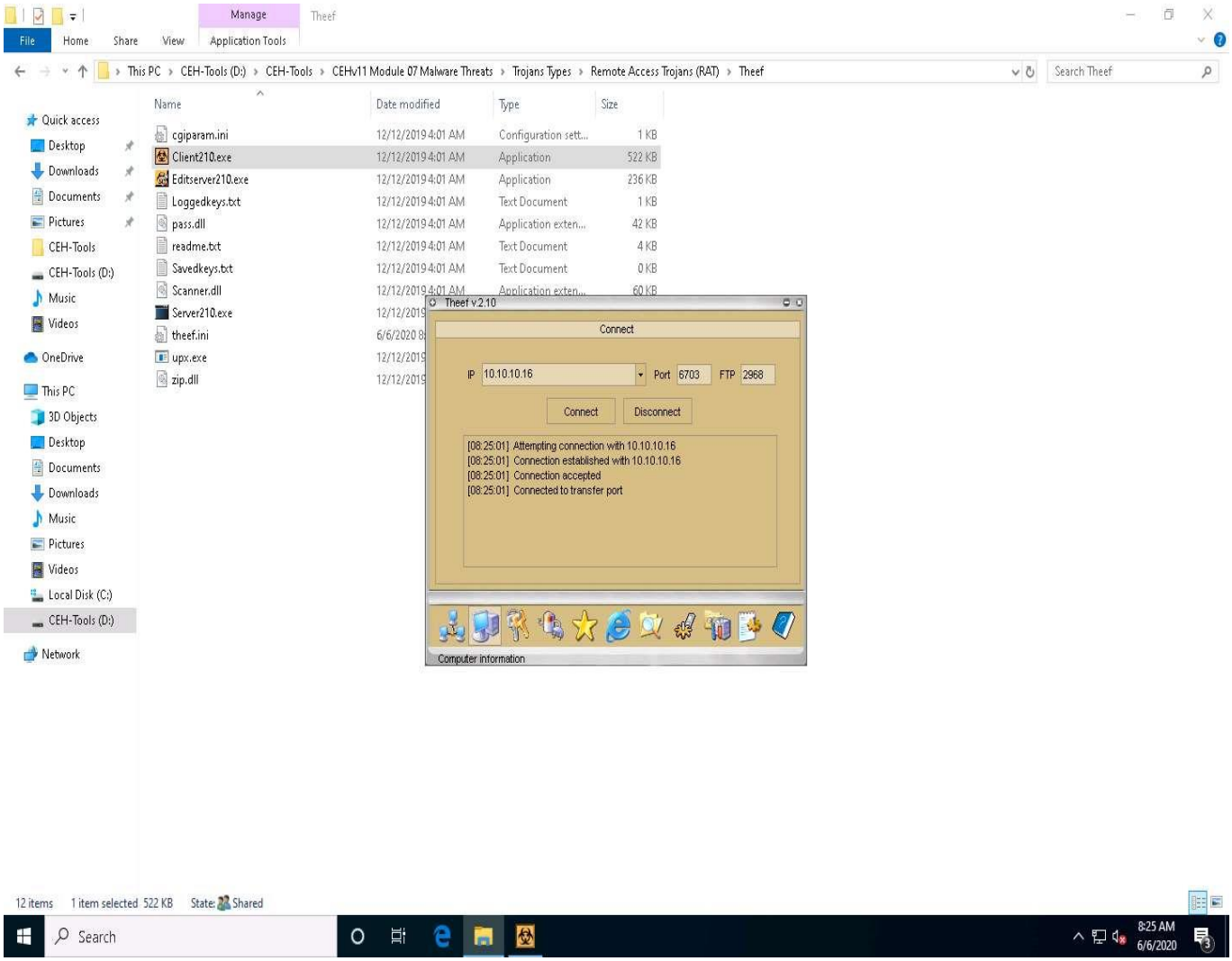
6. ☐ The **Theef** main window appears, as shown in the screenshot.



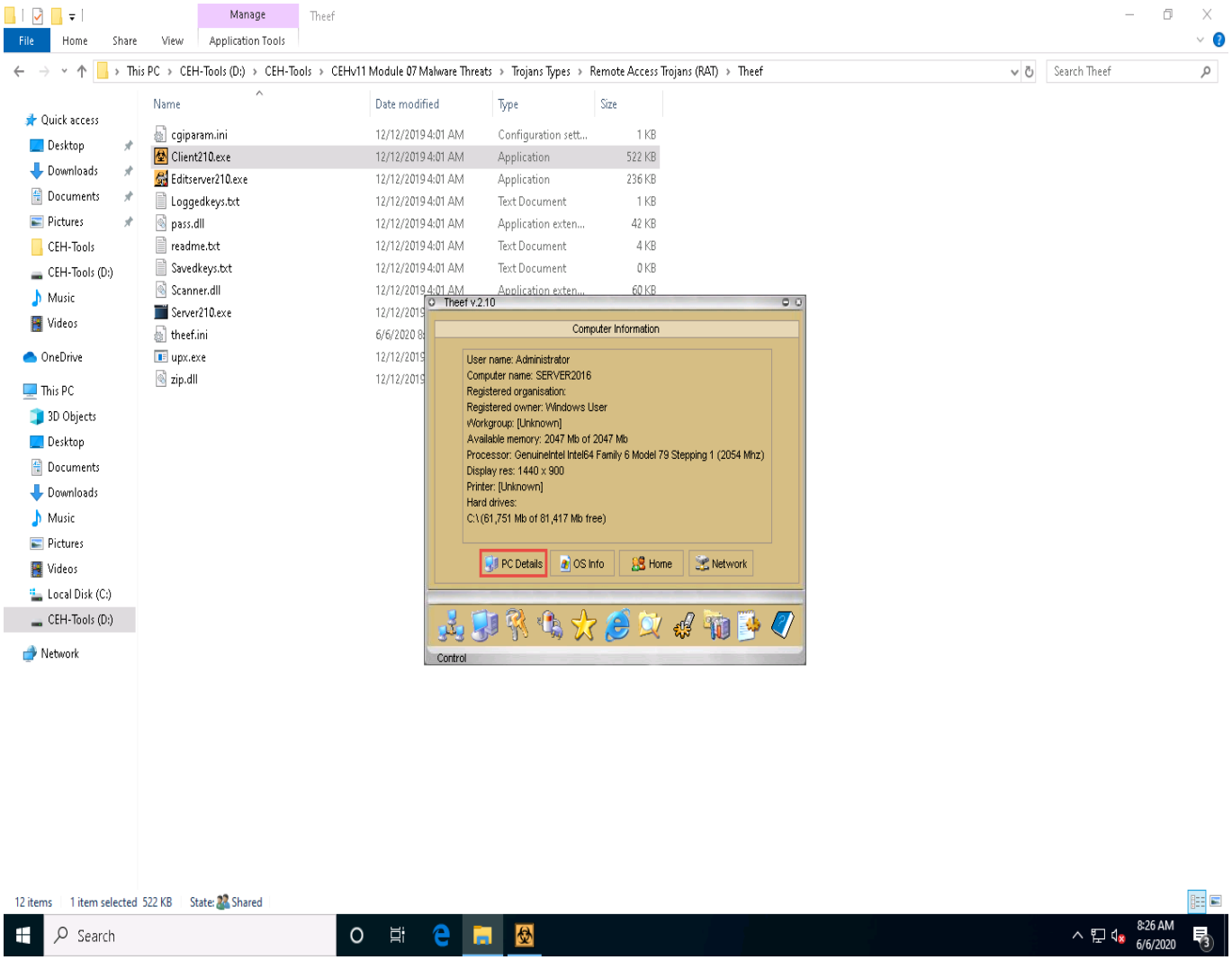
7. Enter the IP address of the target machine (here, **Windows Server 2016**) in the **IP** field (**10.10.10.16**), and leave the **Port** and **FTP** fields set to default; click **Connect**.



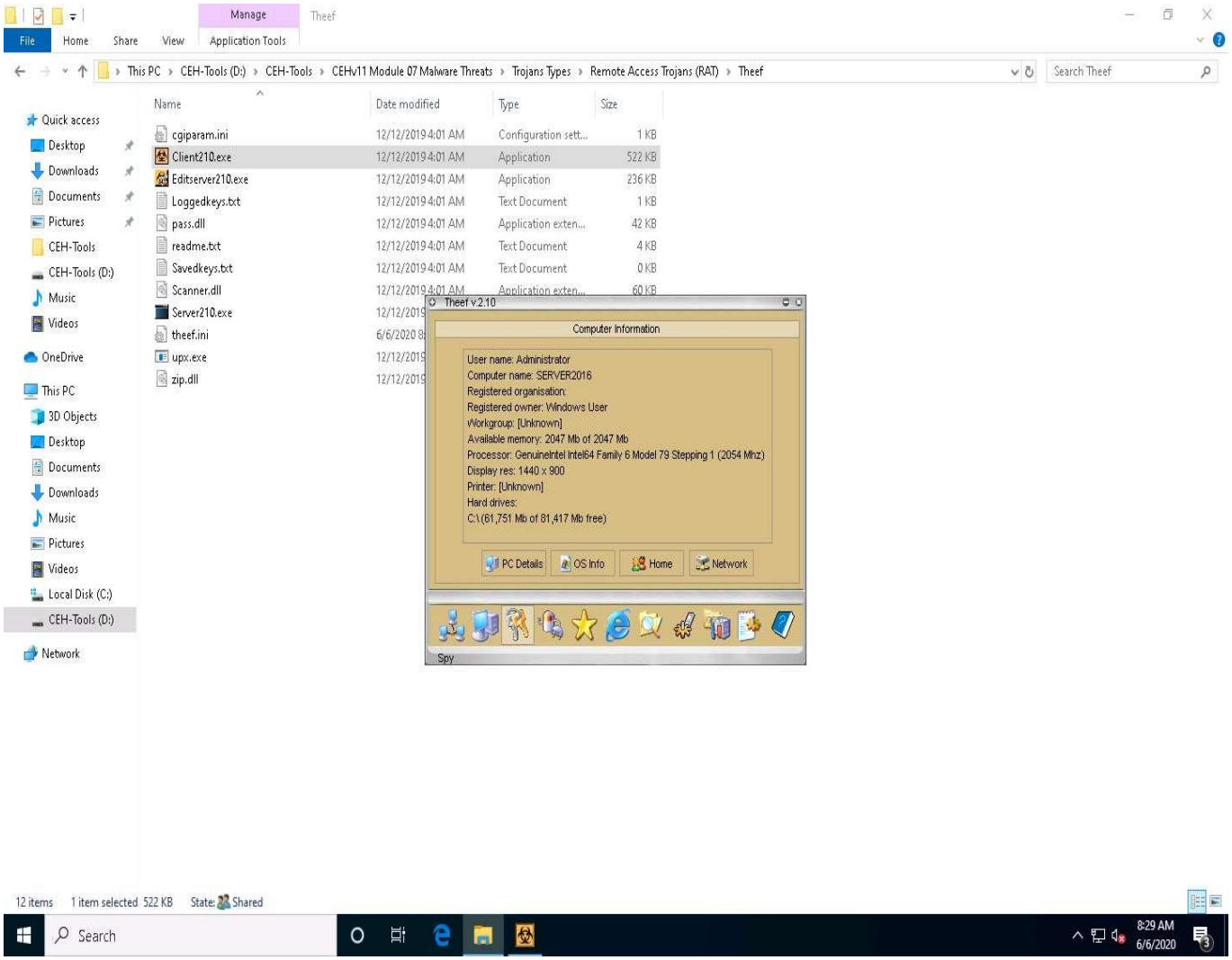
8. ☐ Now, from **Windows 10**, you have successfully established a remote connection with the **Windows Server 2016** machine.
9. ☐ To view the computer's information, click the **Computer Information** icon from the lower part of the window.



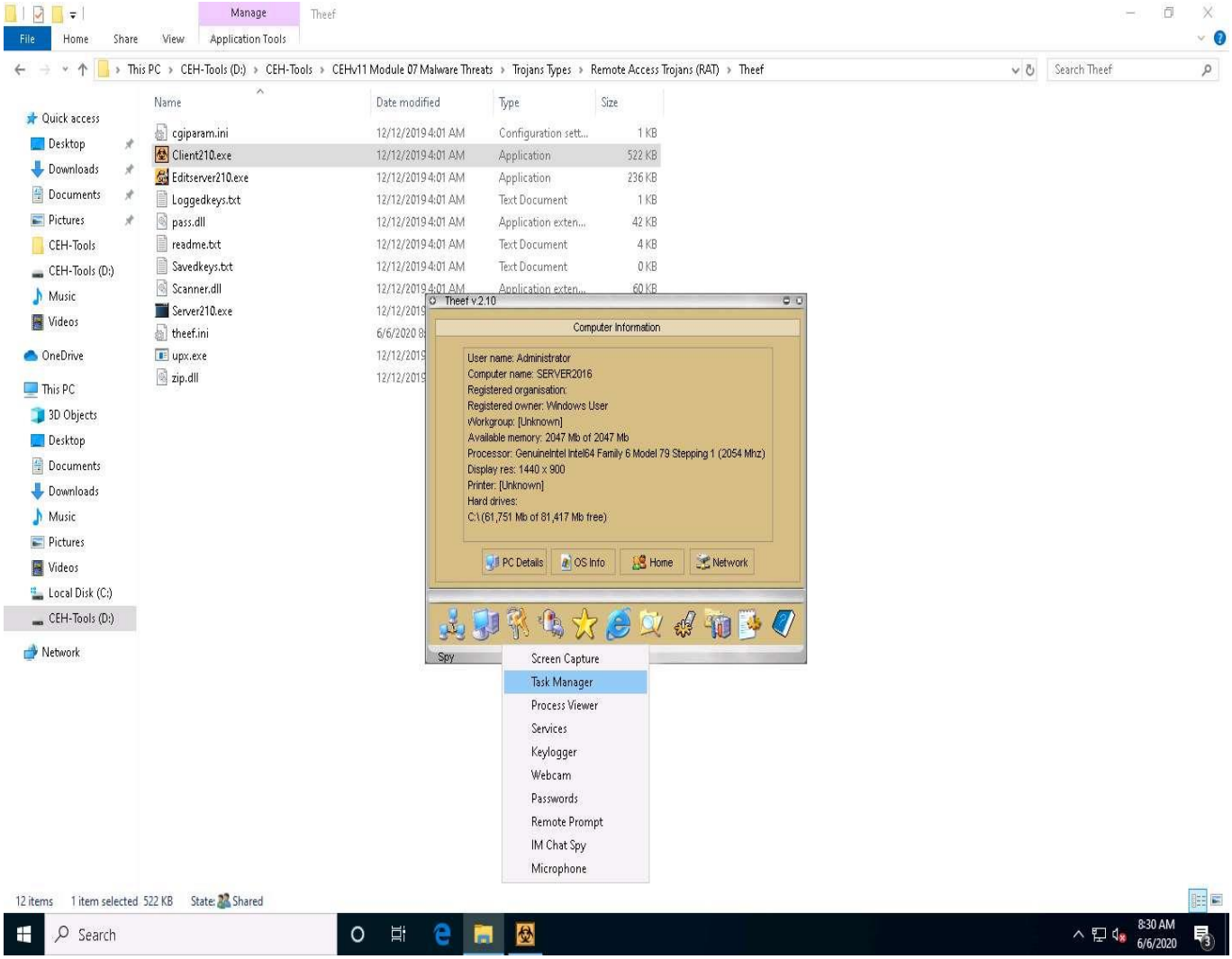
10. ☐ In **Computer Information**, you can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.
11. ☐ Here, for example, selecting **PC Details** reveals computer-related information.



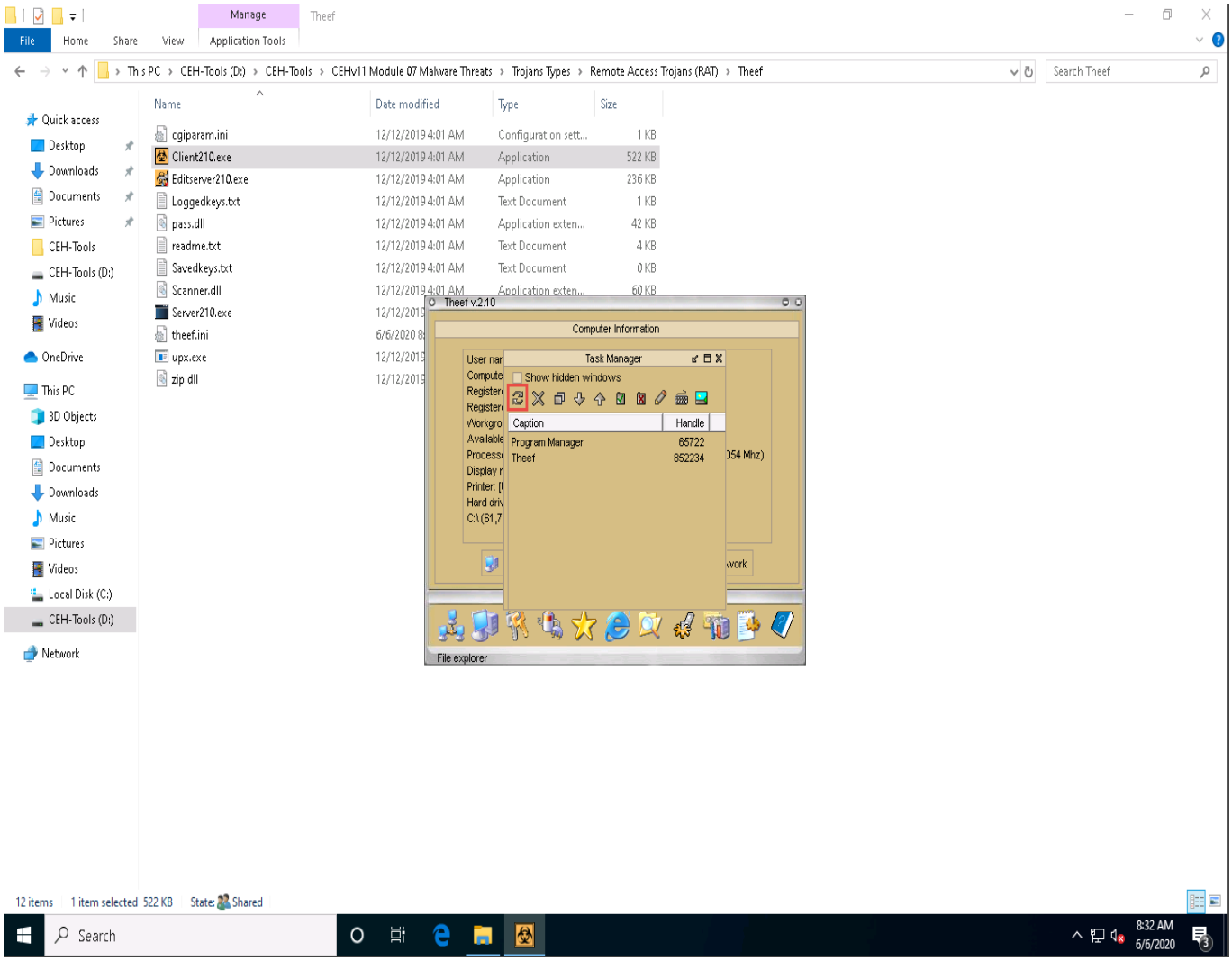
12. Click the **Spy** icon to perform various operations on the target machine.



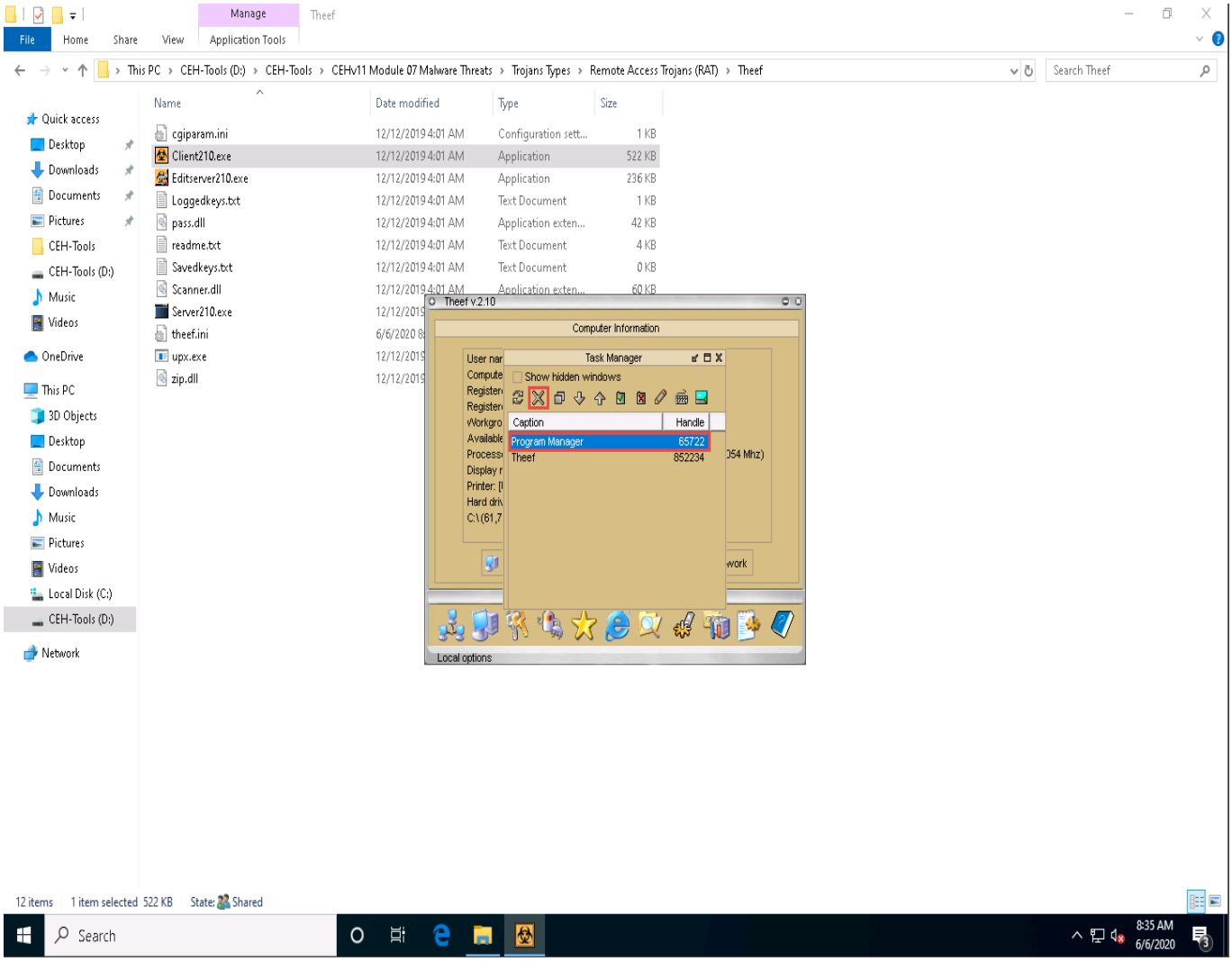
13. You can perform various operations such as capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the victim machine by selecting their respective options.
14. Here, for instance, selecting **Task Manager** views the tasks running on the target machine.



15. ☐ In the **Task Manager** window, click **Refresh** icon to obtain the list of running processes.



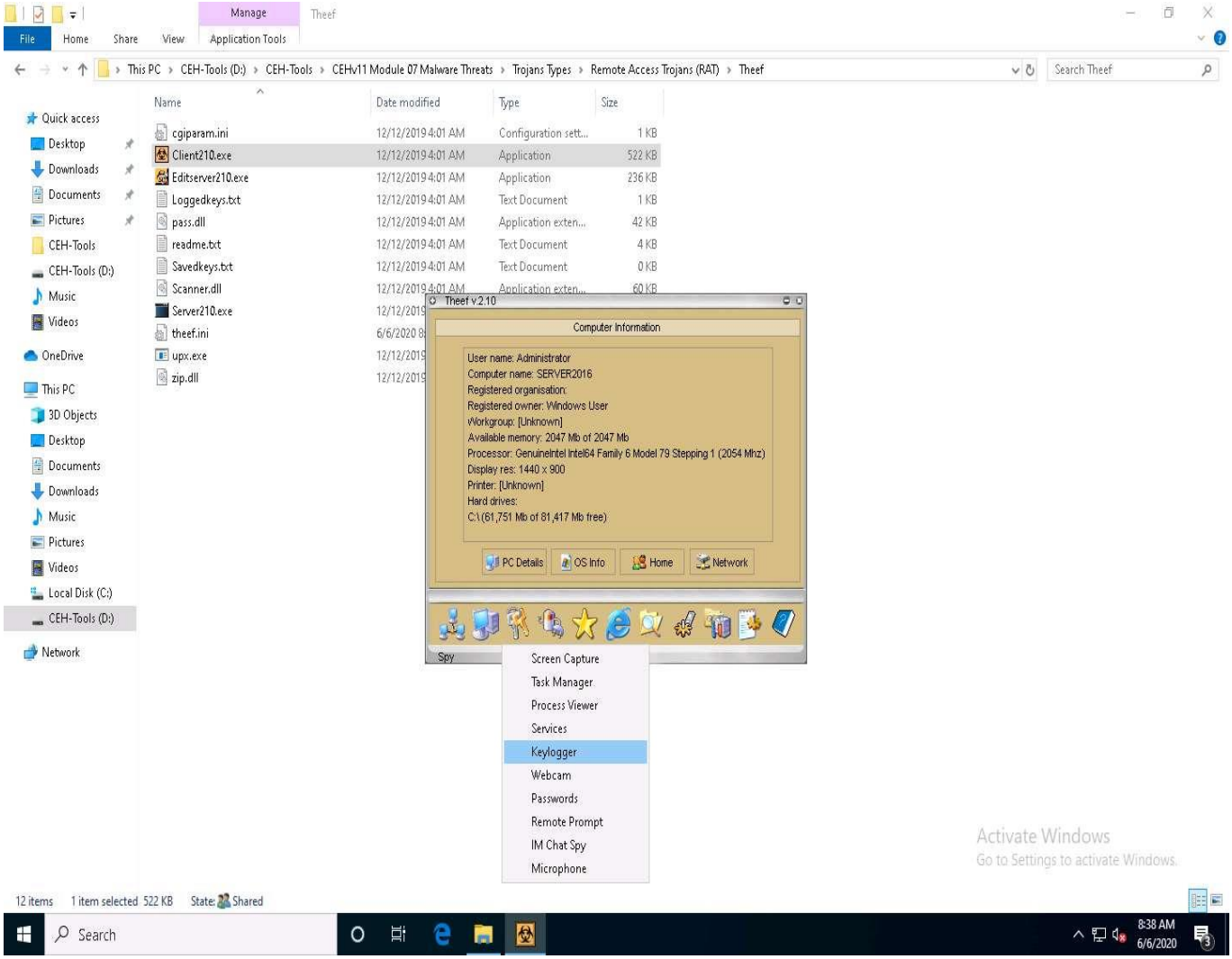
16. Select a process (task); click the **Close window** icon to end the task on the target machine.



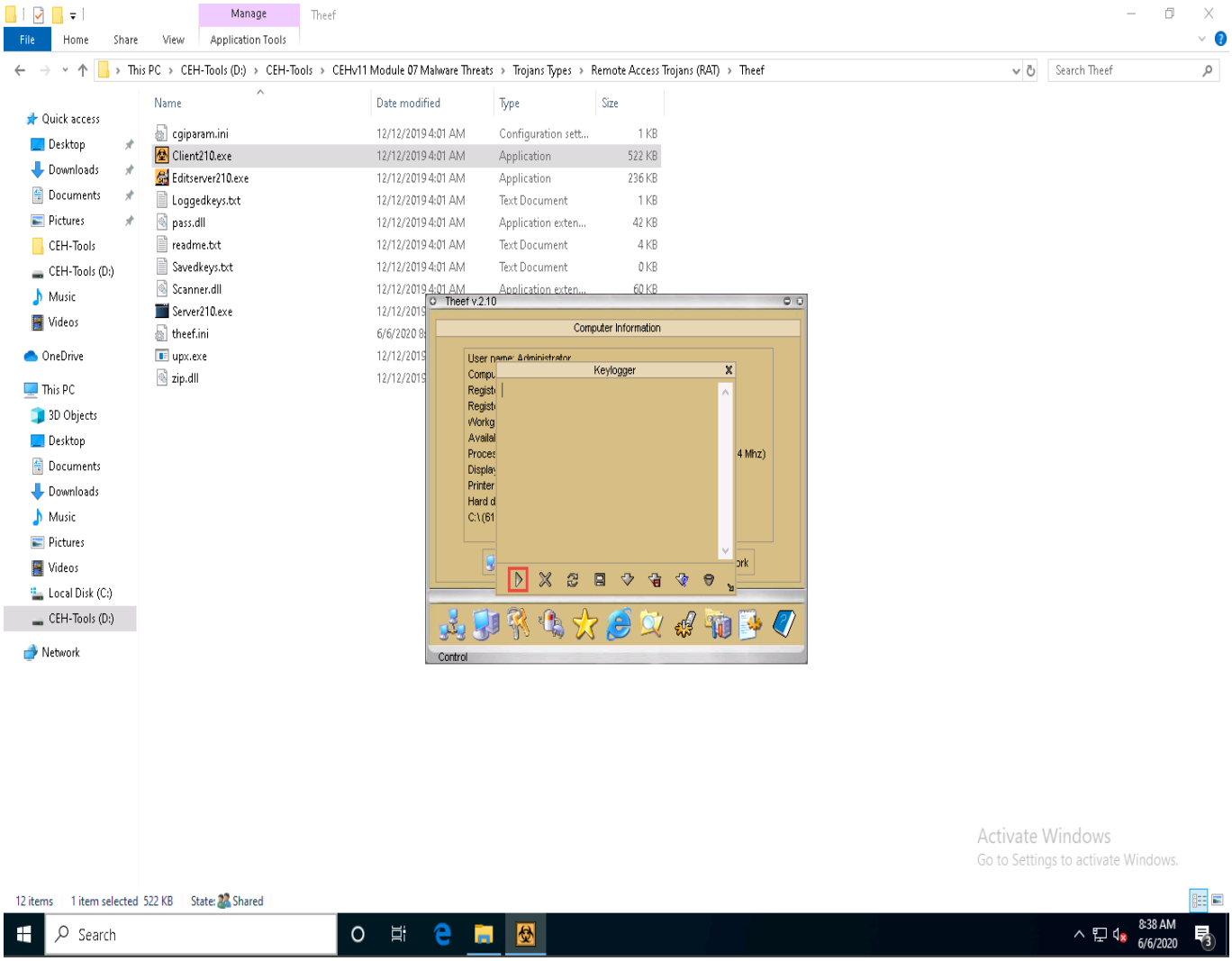
17. ☐ Close the **Task Manager** window.

The tasks running in the task manager may vary in your lab environment.

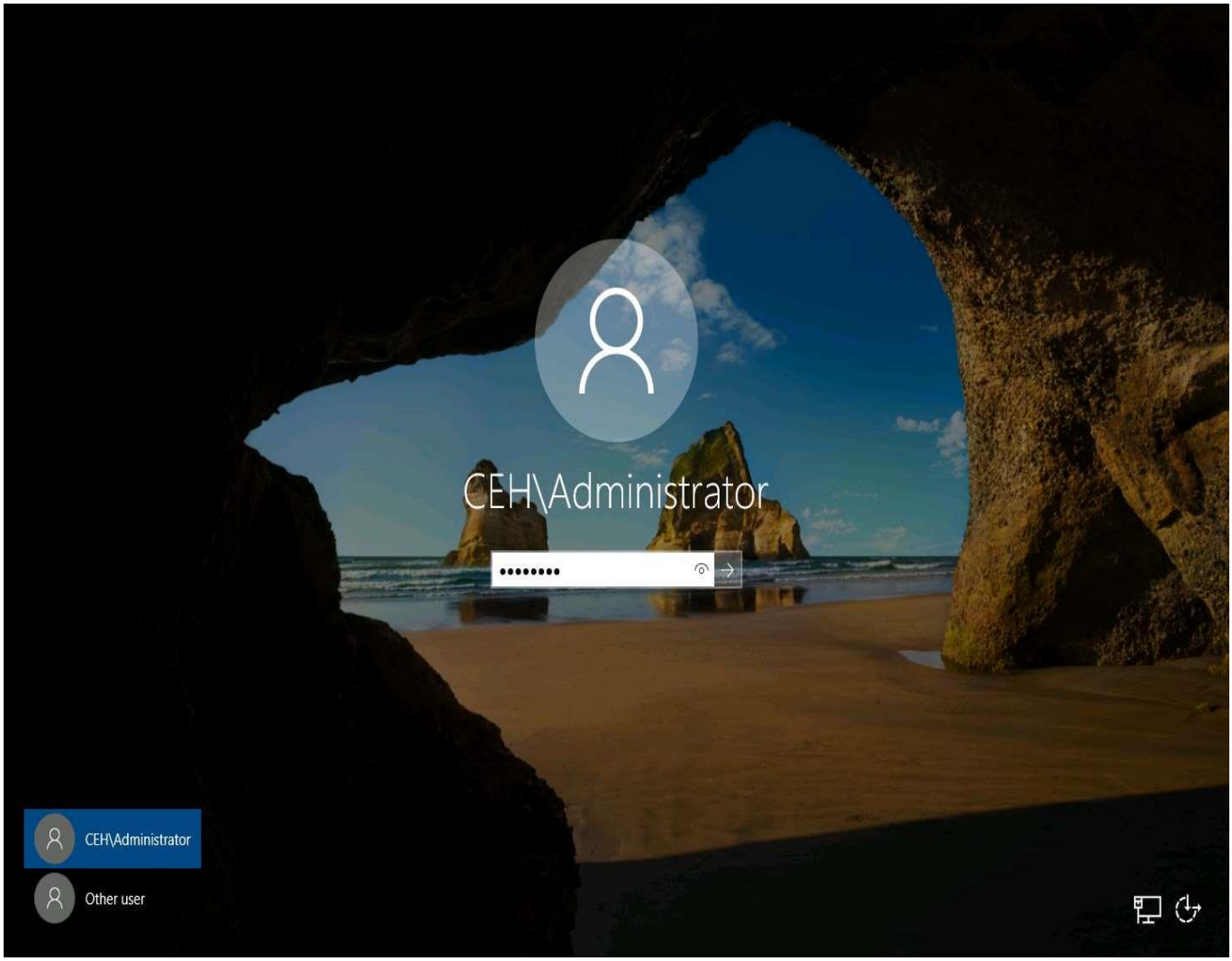
18. ☐ From the **Spy** menu, click **Keylogger** to record the keystrokes made on the victim machine.



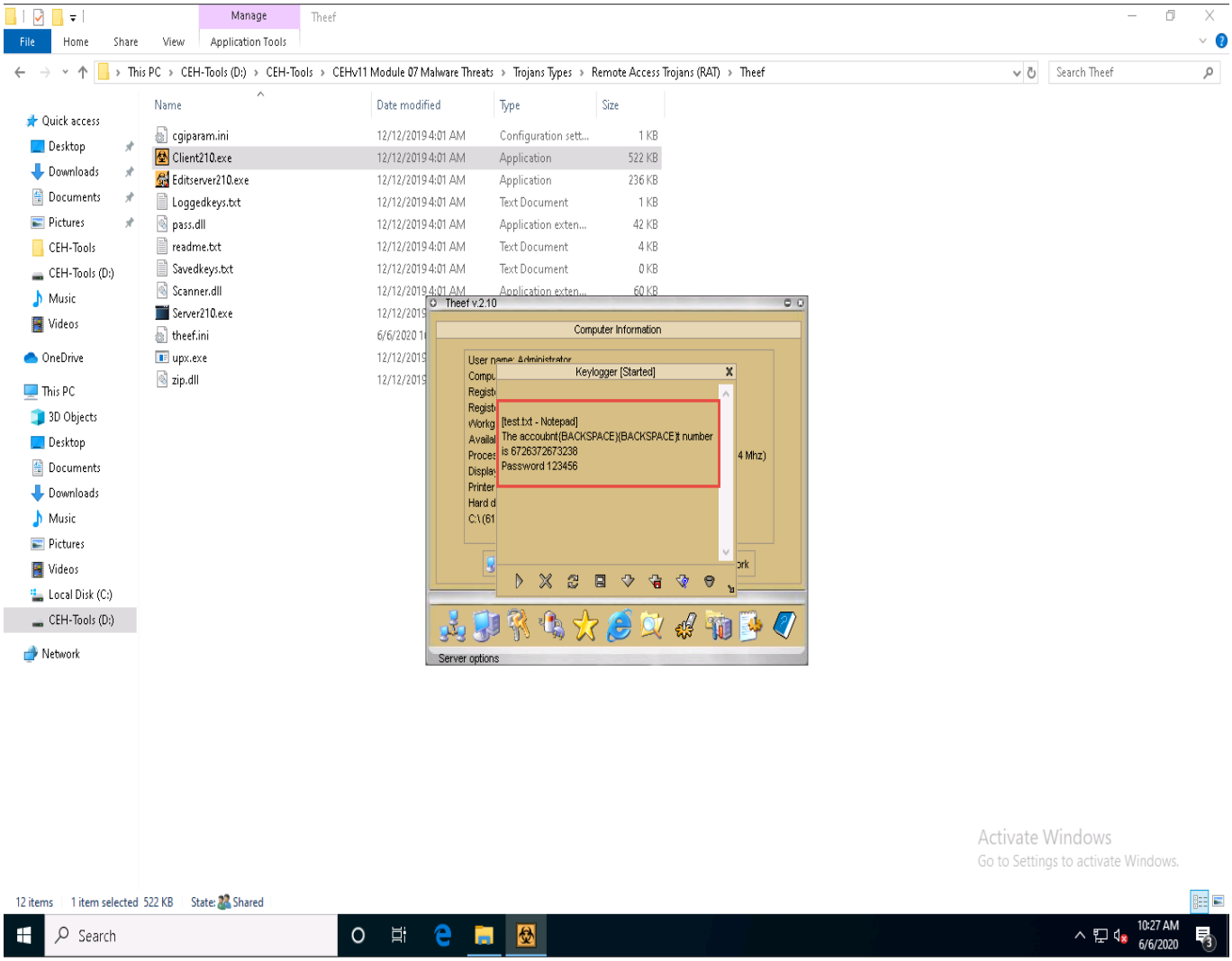
19. ☐ The **Keylogger** pop-up appears; click the **Start** icon to read the keystrokes of the victim machine.



20. Click Windows Server 2016 to switch to the **Windows Server 2016** machine. Click Ctrl+Alt+Delete to activate the machine, by default, **CEH\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.



21. ☐ Open a browser window and browse some websites or open a text document and type some sensitive information.
22. ☐ Click Windows 10 to switch back to the attacker machine (**Windows 10**) to view the recorded keystrokes of the victim machine in the **Theef** Keylogger window.



23. ☐ Close the Theef **Keylogger** window.
24. ☐ Similarly, you can access the details of the victim machine by clicking on the various icons.
25. ☐ Close all open windows on both the **Windows 10** and **Windows Server 2016** machines.