EC-Council

codered
FROM EC-COUNCIL

CHAPTER 1

INFORMATION SECURITY THREATS AND VULNERABILITIES

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Chapter 1:
Information Security Threats and Vulnerabilities

SCENARIO

The recent trends in cyber security breaches illustrate that no system or network is immune to attacks. All organizations that store, transmit, and handle data must enforce strong security mechanisms to continuously monitor their IT environment to identify the vulnerabilities and resolve them before exploitation. It is important to understand the difference between a security threat and a vulnerability. Security threats are incidents that have a negative impact on the organization's IT infrastructure. Whereas vulnerabilities are security gaps or flaws in a system or network that enable attacks, tempting hackers to exploit them.
Hence, security professionals must have the required knowledge of information security threats and vulnerabilities to safeguard the organization's sensitive data against unauthorized access or theft.

OBJECTIVE

The objective of this lab is to provide expert knowledge about the information security threats and vulnerabilities. This includes knowledge of the following tasks:

- Creating a trojan, virus, and worm to gain access to the target machine

- Monitoring user activities on a remote machine

- Finding vulnerabilities using exploit sites

OVERVIEW INTERRUPTED SESSIONS

A threat is the potential occurrence of an undesirable event that can eventually damage and disrupt the operational and functional activities of an organization. A threat can be any type of entity or action performed on physical or intangible assets that can disrupt security. The existence of threats may be accidental, intentional, or due to the impact of another action.
A vulnerability refers to a weakness in the design or implementation of a system that can be exploited to compromise the security of the system. It is frequently a security loophole that enables an attacker to enter the system by bypassing user authentication.

LAB TASKS

The recommended labs to assist you in learning various information security threats and vulnerabilities include the following:

01 Create a Trojan to Gain Access to the Target System

02 Create a Virus to Infect the Target System

03 Create a Worm using the Internet Worm Maker Thing

04 User System Monitoring and Surveillance using Spytech SpyAgent

05 Find Vulnerabilities on Exploit Sites

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.

EXERCISE 1: **CREATE A TROJAN TO GAIN ACCESS TO THE TARGET SYSTEM**

A computer Trojan is a program in which malicious or harmful code is packed inside an apparently harmless program or data.

LAB SCENARIO

A Trojan is wrapped within or attached to a legitimate program, implying that the program may have functionality that is not apparent to the user. Furthermore, attackers use victims as unwitting intermediaries to attack others. They can use a victim's computer to commit illegal Denial-of-service (DoS) attacks.

A compromised system can affect other systems on the network. Systems that transmit authentication credentials such as passwords over shared networks in clear text or a trivially encrypted form are particularly vulnerable. If an intruder compromises a system on such a network, they may be able to record usernames and passwords or other sensitive information. Additionally, a Trojan, depending on the actions it performs, may falsely implicate a remote system as the source of an attack by spoofing, causing a liability to the remote system. Trojans enter a system by means such as email attachments, downloads, and instant messages.

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

OBJECTIVE

This lab demonstrates how to do create a Trojan Server using Theef RAT Trojan.

OVERVIEW OF TROJAN

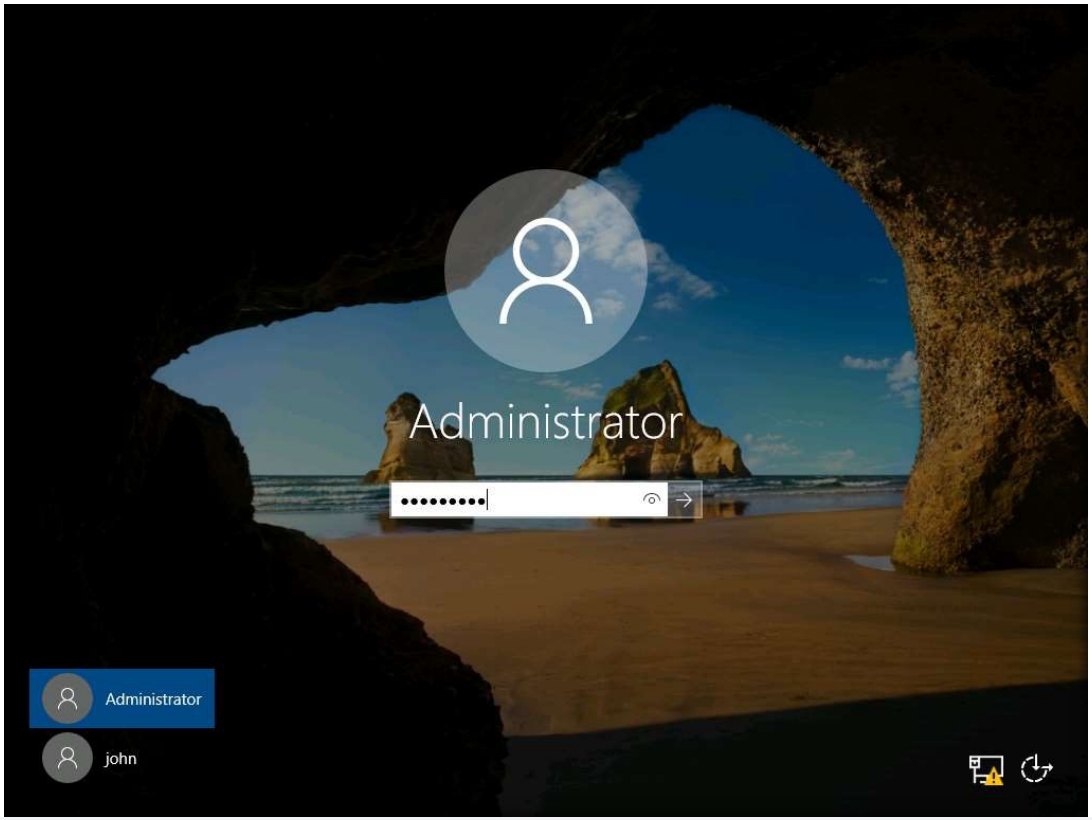
Attackers use Remote Access Trojans (RATs) to infect the target machine to gain administrative access. RATs help an attacker remotely access the complete Graphical User Interface (GUI) of the victim's computer and control without his/her awareness. They can perform screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and other tasks. The Trojan 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.

Theef is a RAT 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 Trojan that can be installed on a target computer, and the Theef client is then used to control the Trojan. Security professional can use the Theef Tool as a proof of concept to audit perimeter security controls in an organization.

Note: The versions of the created client or host, as well as 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.
Note: Ensure that PfSense Firewall virtual machine is running.

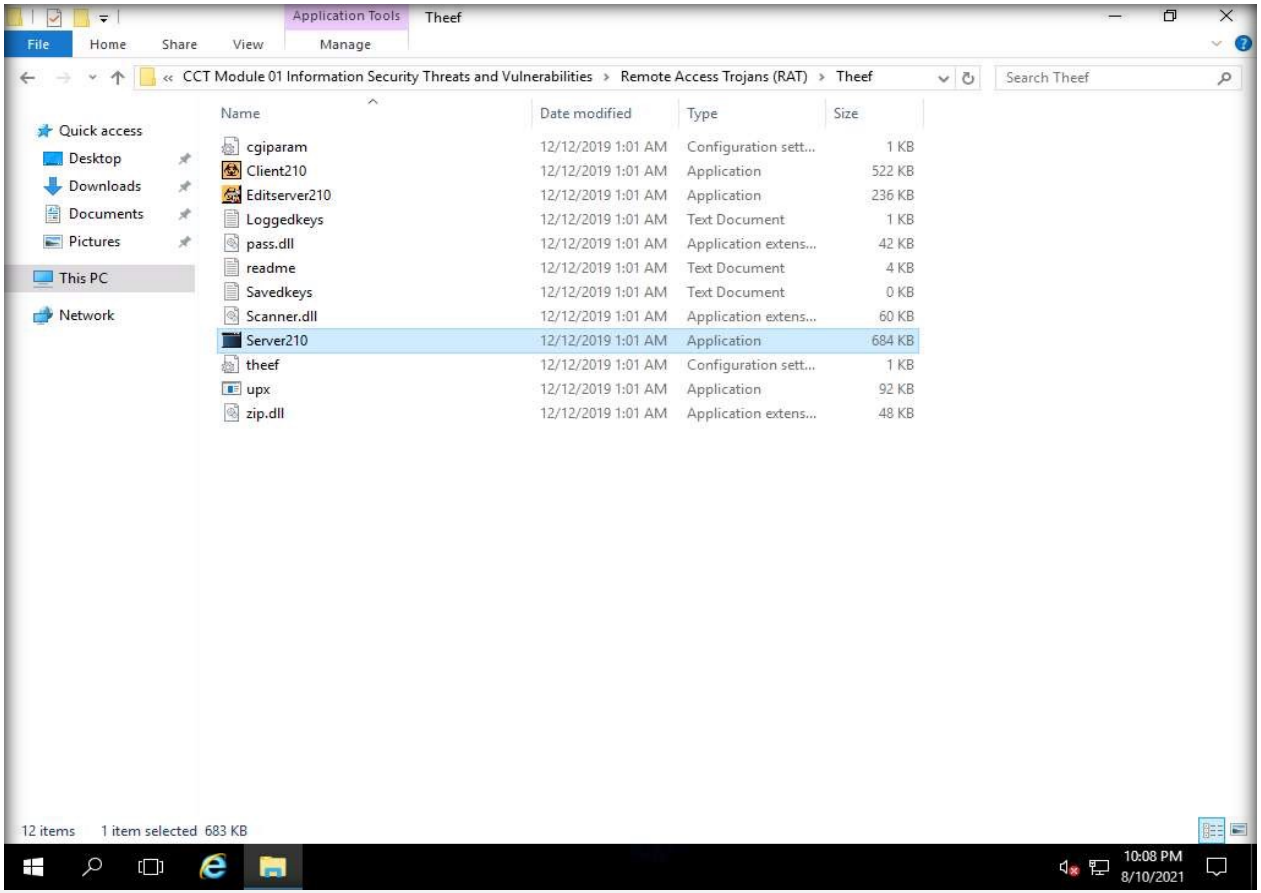
1. Generally, an attacker might send a server executable to the victim machine and entice the victim into running it. In this lab, for demonstration purposes, we are directly executing the file on the victim machine, Web Server virtual machine.
2. Turn on Admin Machine-1 and Web Server virtual machines.
3. Switch to the Web Server virtual machine.
4. In the Web Server virtual machine, log in with the credentials Administrator and admin@123.

EXERCISE 1: CREATE A TROJAN TO GAIN ACCESS TO THE TARGET SYSTEM



5. Navigate to Z:\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Theef and double-click Server210.exe to run the Trojan on the victim machine.
Note: If an Open File - Security Warning pop-up appears, click Run.

EXERCISE 1: CREATE A TROJAN TO GAIN ACCESS TO THE TARGET SYSTEM

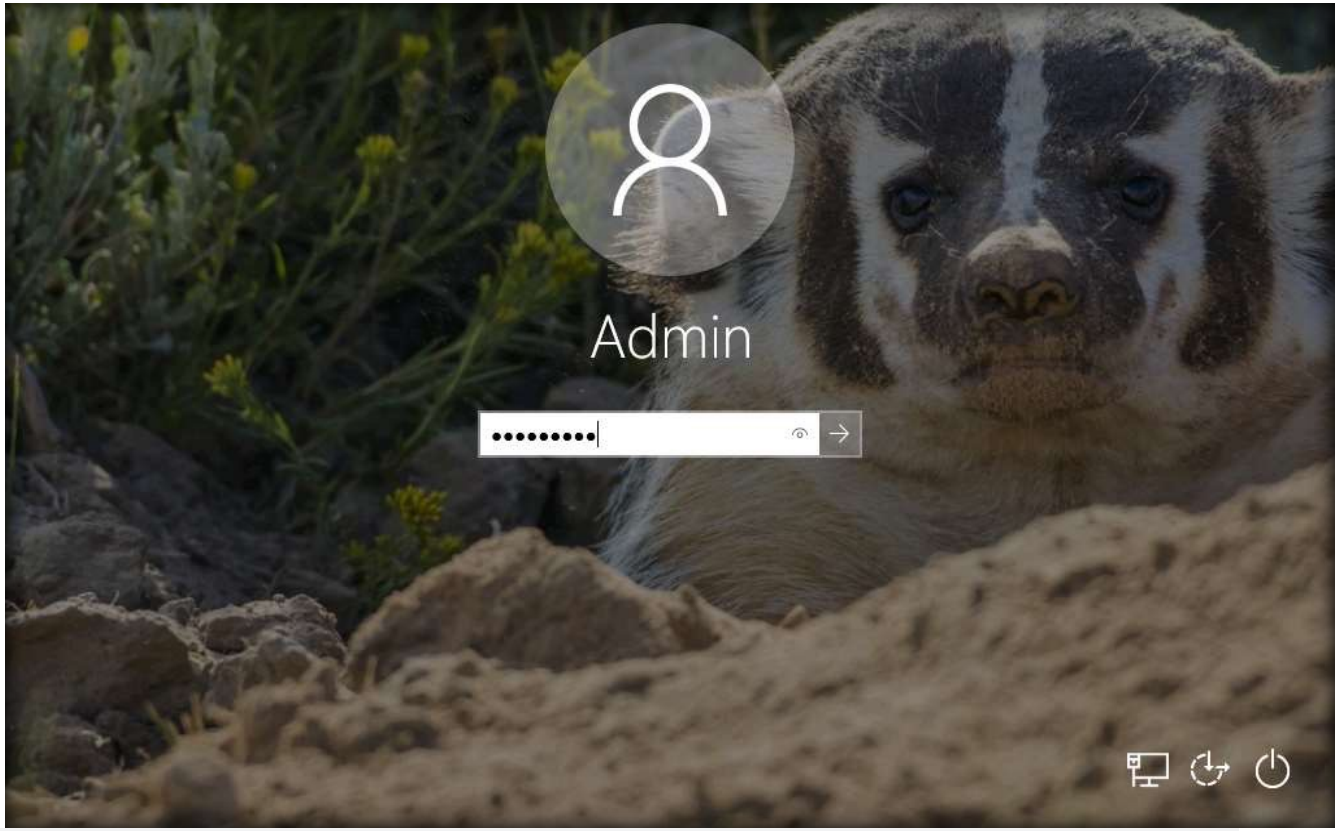


6. Now, switch to the Admin Machine-1 virtual machine and log in with the credentials Username: Admin and Password: Pa$$w0rd (as an attacker).

Note: If the Welcome to Windows wizard appears, click Continue and in the Sign in with Microsoft wizard, click Cancel.

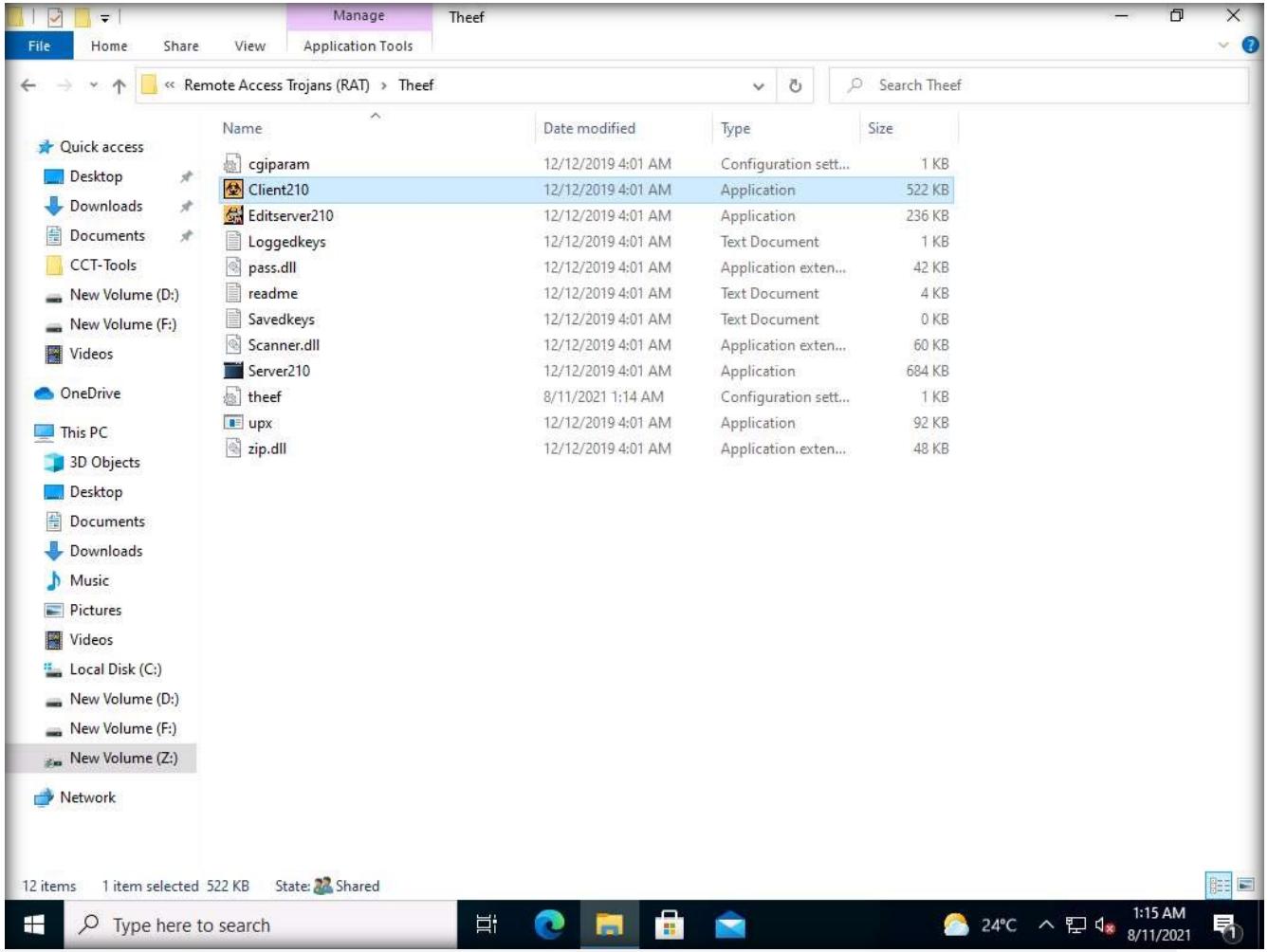
A Networks screen appears. Click Yes to allow the PC to be discoverable by other PCs and devices on the network.

EXERCISE 1: CREATE A TROJAN TO GAIN ACCESS TO THE TARGET SYSTEM



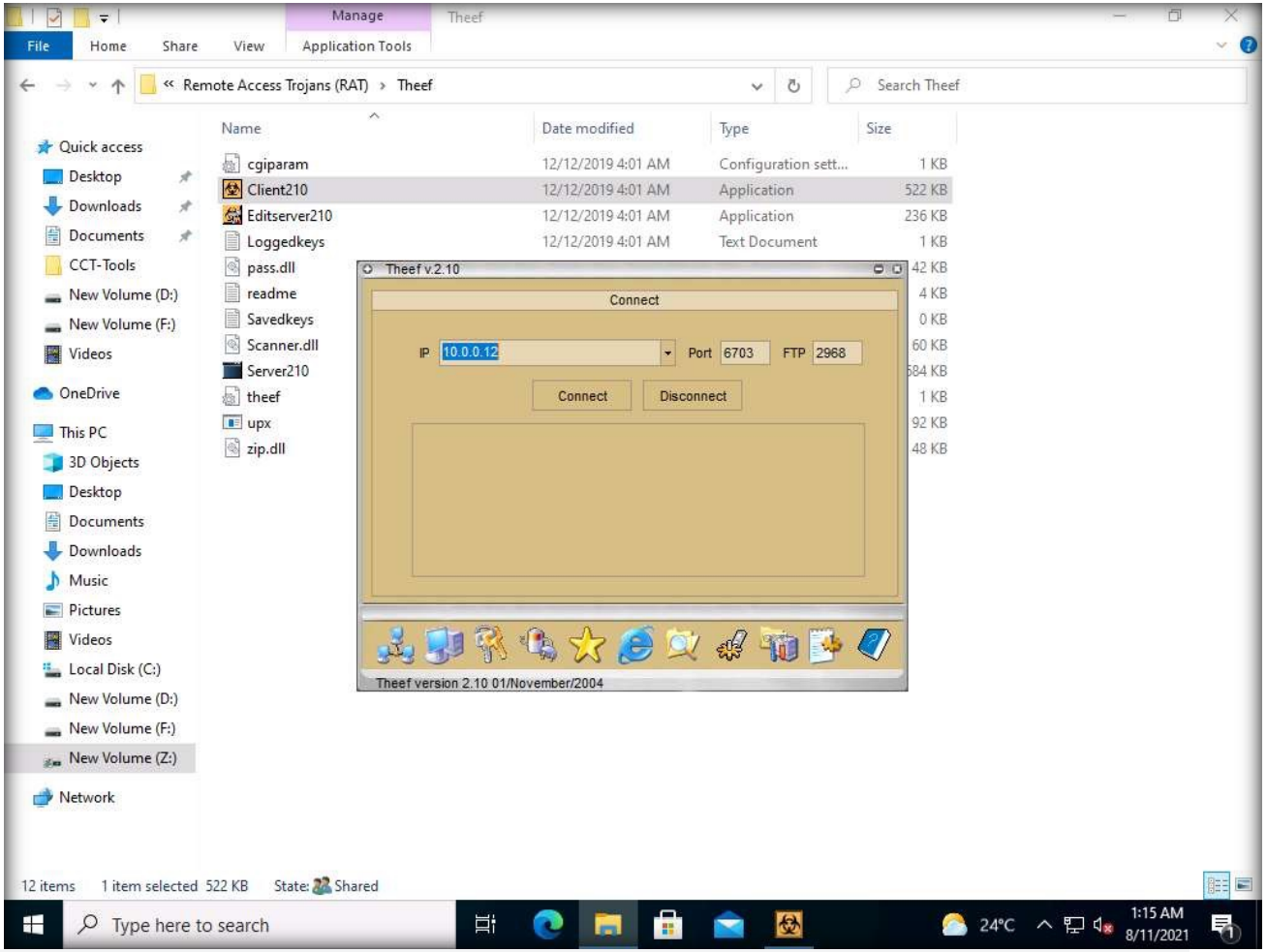
7. Navigate to Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Remote Access Trojans (RAT)\Theef and double-click Client210.exe to access the victim machine remotely.

EXERCISE 1:
CREATE A TROJAN
TO GAIN ACCESS
TO THE TARGET
SYSTEM



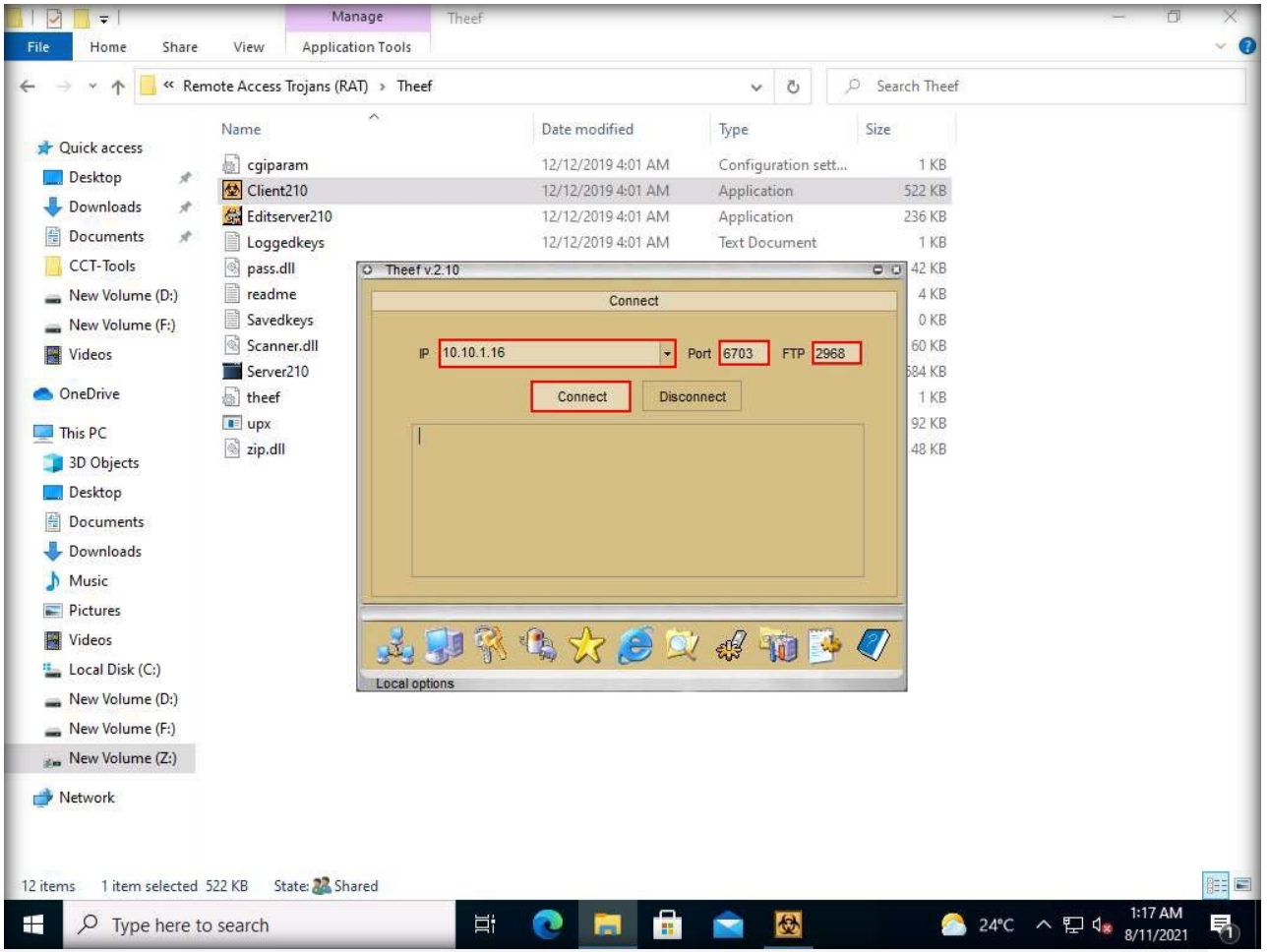
8. The Theef main window appears, as shown in the screenshot below.

EXERCISE 1:
CREATE A TROJAN
TO GAIN ACCESS
TO THE TARGET
SYSTEM



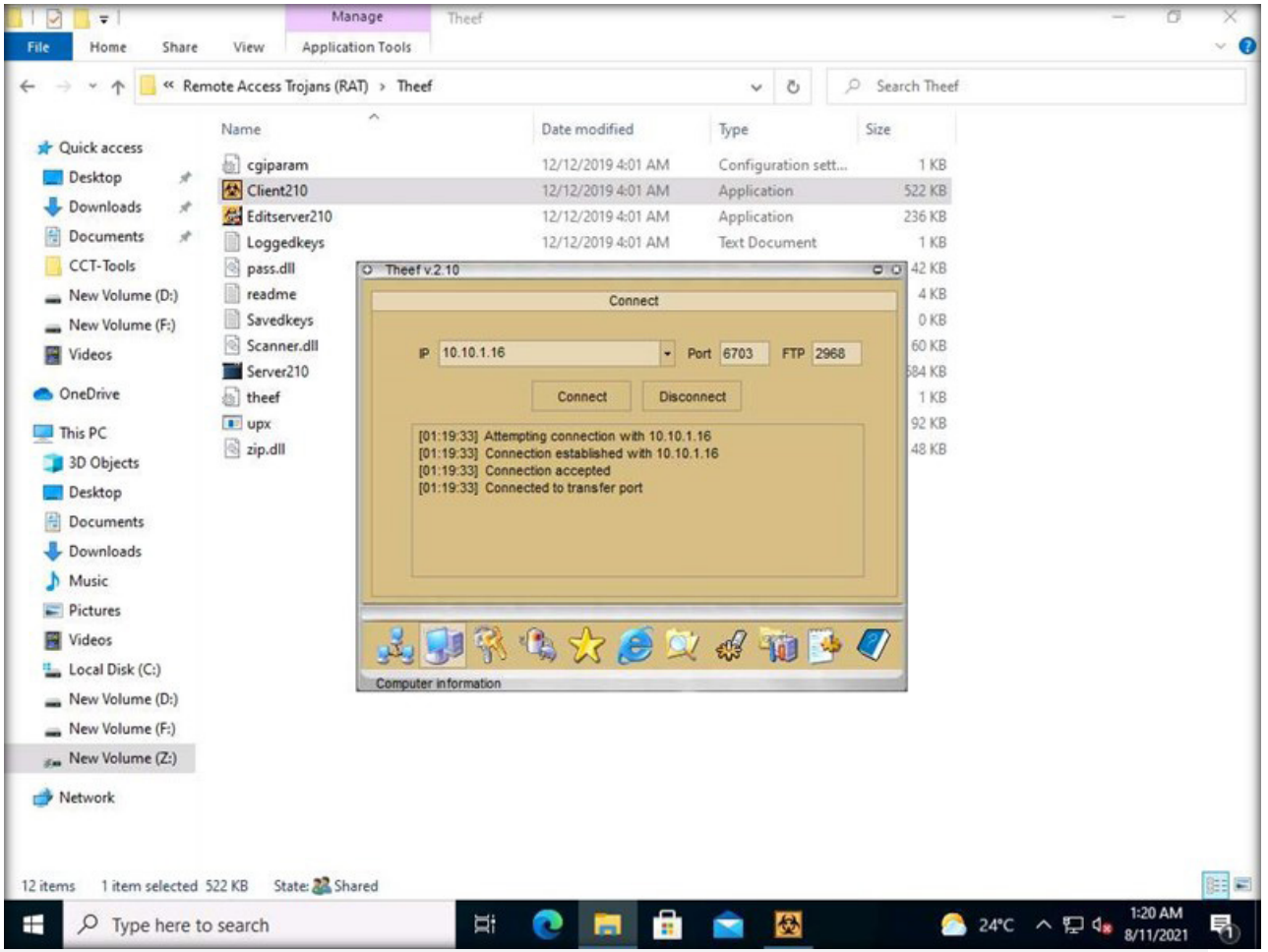
9. Enter the IP address of the target machine (here, Web Server) in the IP field (10.10.1.16) and leave the Port and FTP fields set to default. Click Connect.

EXERCISE 1:
CREATE A TROJAN
TO GAIN ACCESS
TO THE TARGET
SYSTEM



10. Now, from the Admin Machine-1 virtual machine, a remote connection with the Web Server machine has been successfully established.
11. To view the computer's information, click the Computer Information icon from the lower part of the window.

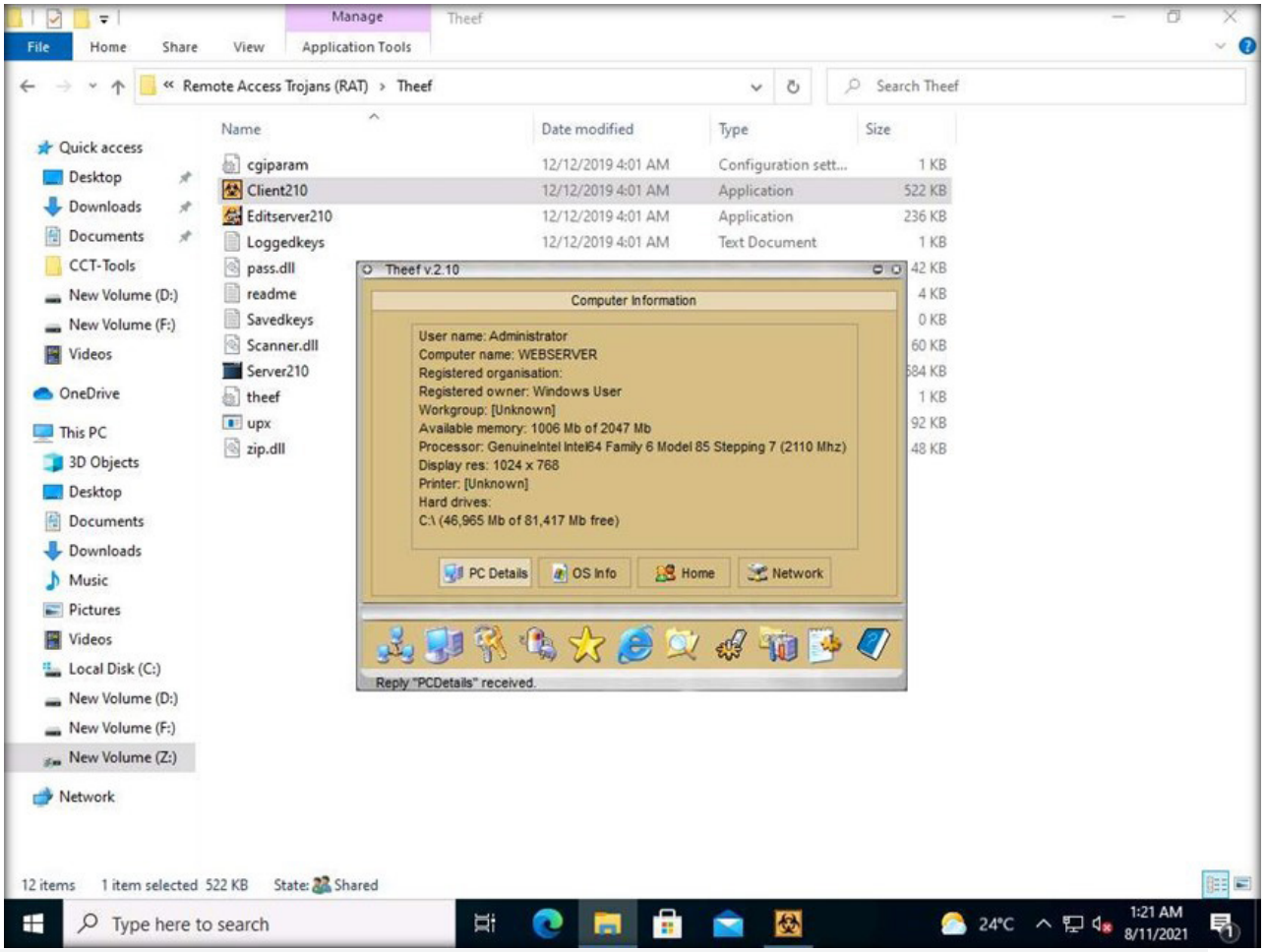
EXERCISE 1: CREATE A TROJAN TO GAIN ACCESS TO THE TARGET SYSTEM



12. In Computer Information, PC Details, OS Info, Home, and Network can be viewed by clicking their respective buttons.
13. Here, for example, selecting PC Details reveals computer-related information.

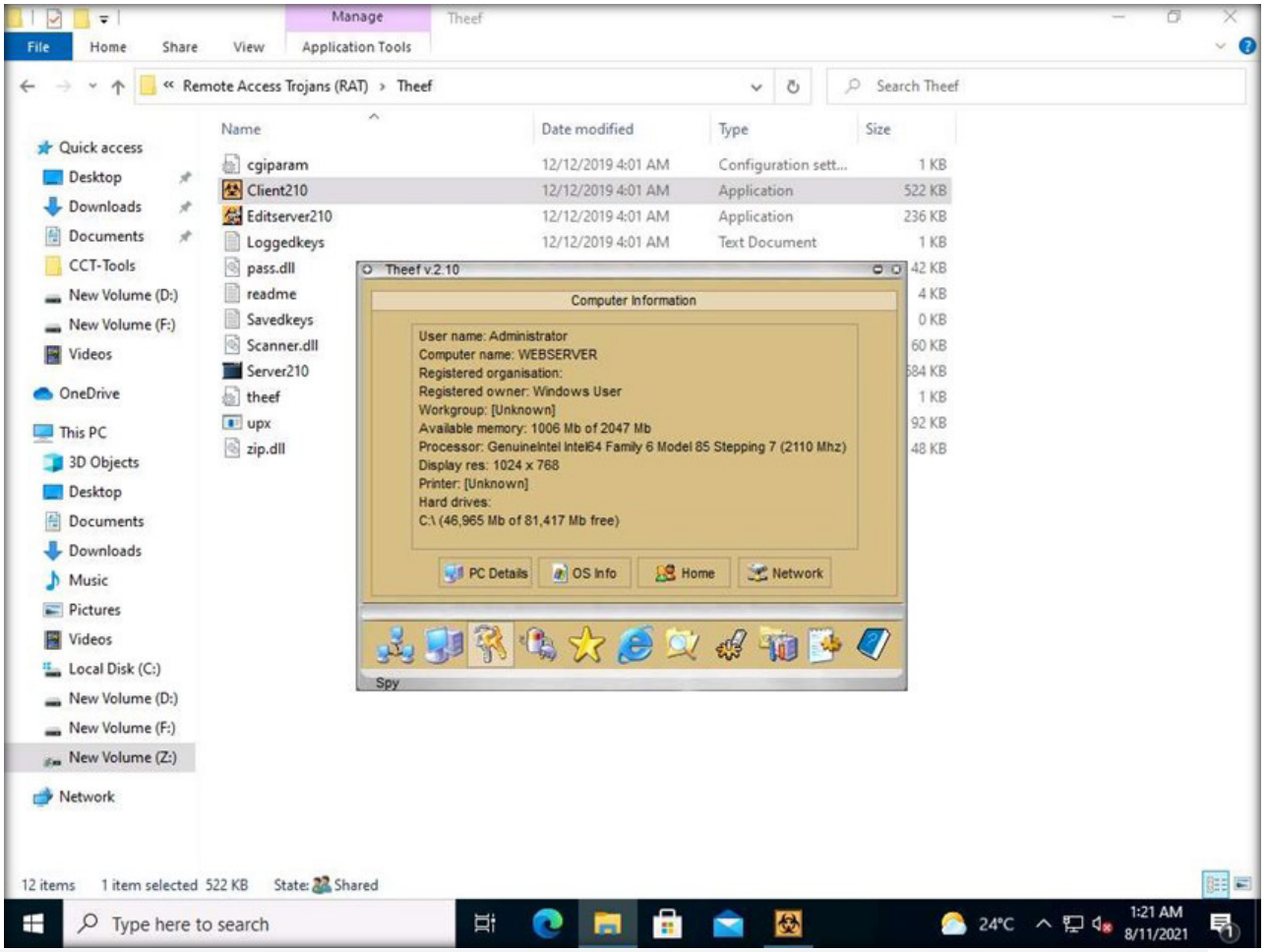
Note: The Computer Information might differ when you perform the lab.

EXERCISE 1:
CREATE A TROJAN
TO GAIN ACCESS
TO THE TARGET
SYSTEM



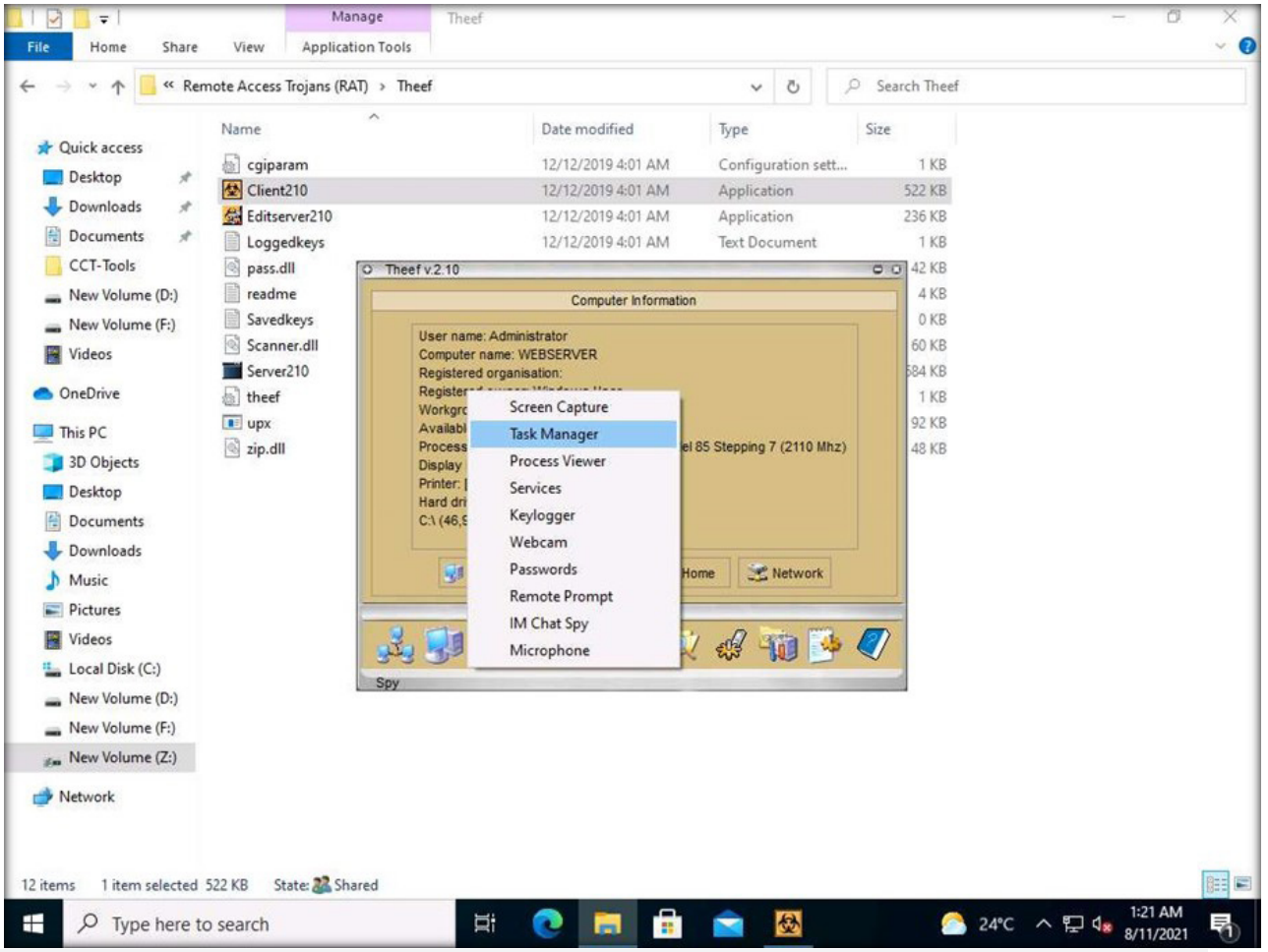
14. Click the Spy icon to perform various operations on the target machine.

EXERCISE 1:
CREATE A TROJAN
TO GAIN ACCESS
TO THE TARGET
SYSTEM



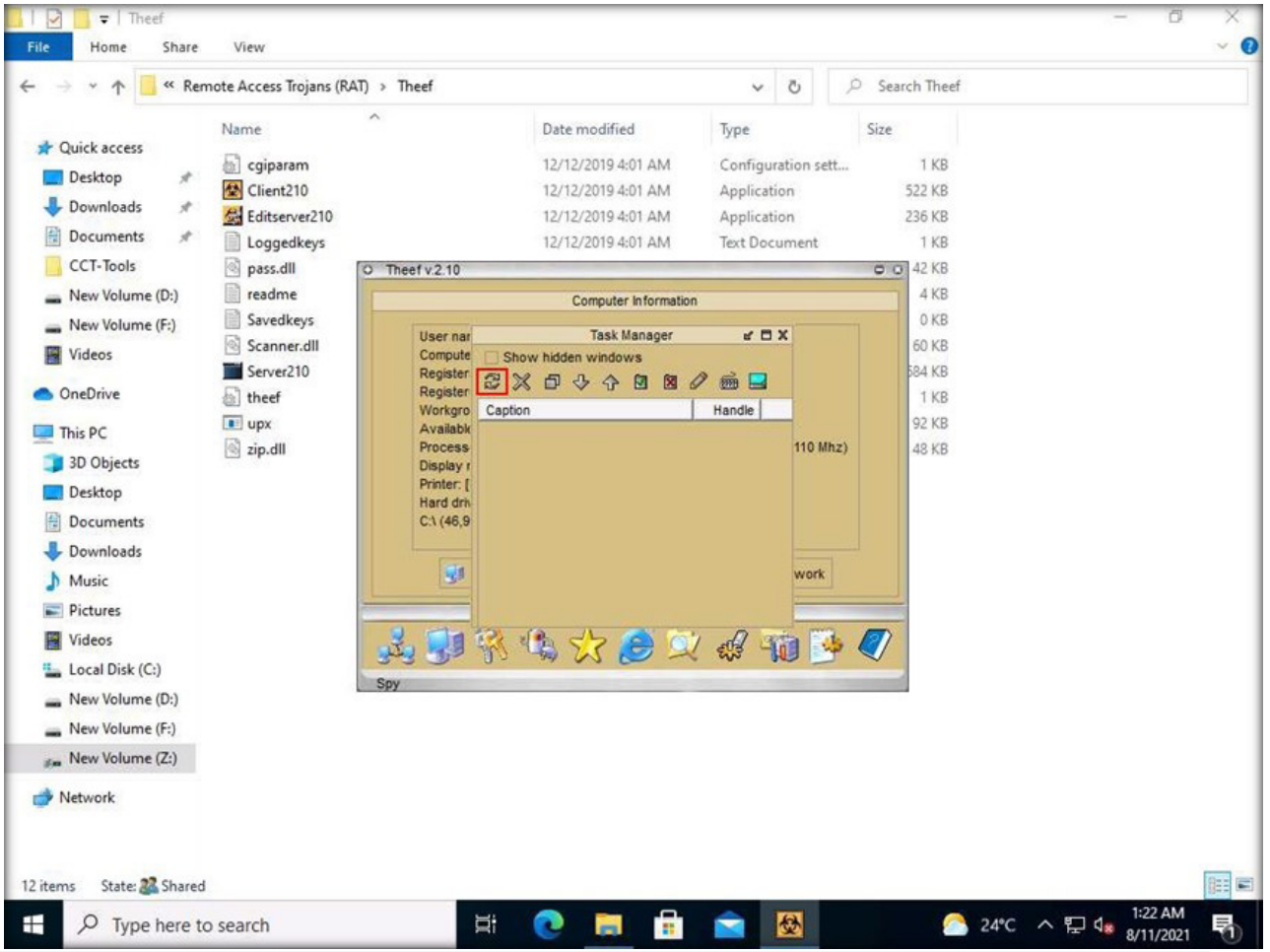
15. You can perform various operations such as capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the victim machine by selecting their respective options.
16. Here, for instance, selecting Task Manager displays the tasks running on the target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

EXERCISE 1: CREATE A TROJAN TO GAIN ACCESS TO THE TARGET SYSTEM



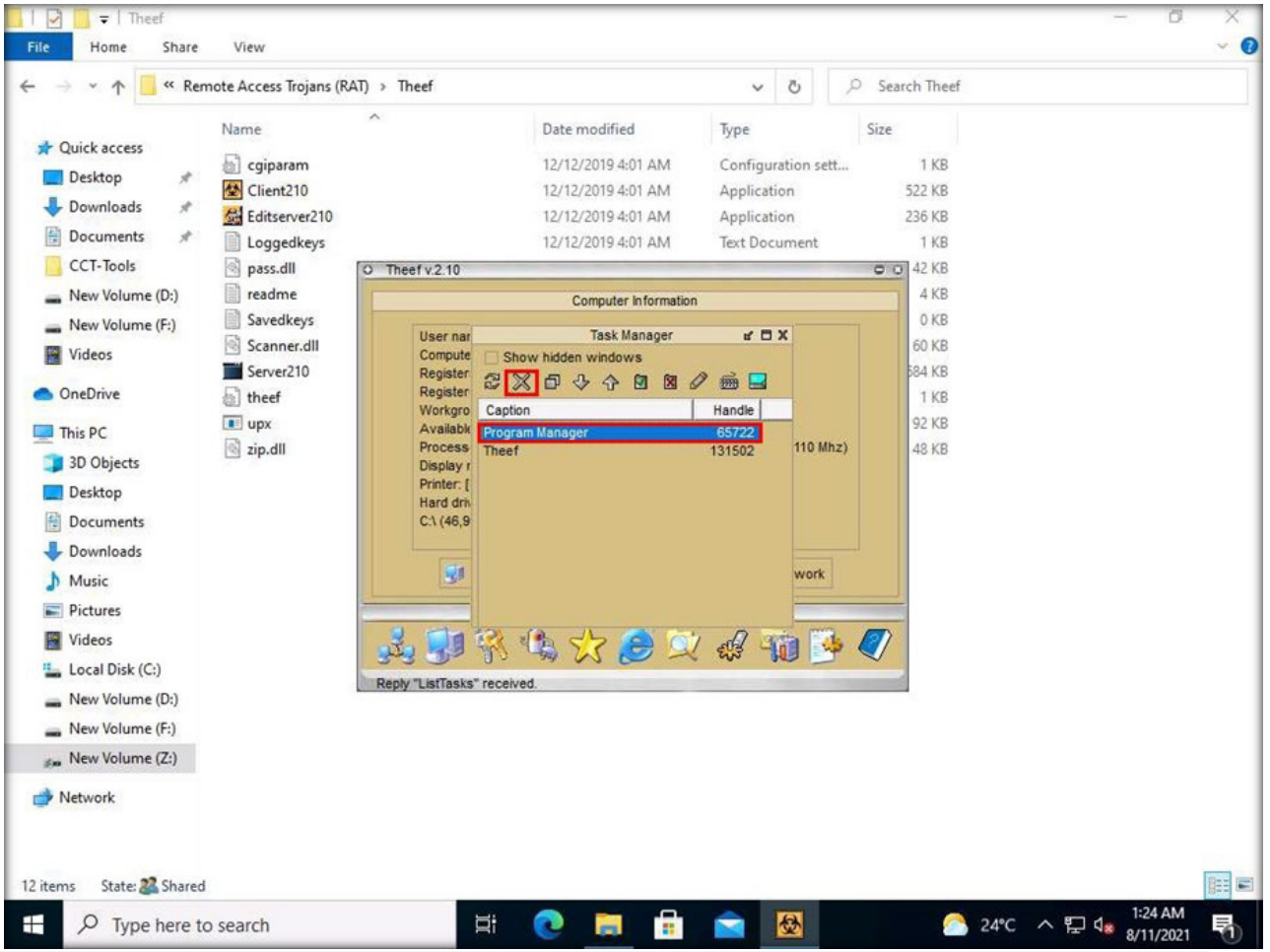
17. In the Task Manager window, click the Refresh icon to obtain the list of running processes.

EXERCISE 1:
CREATE A TROJAN
TO GAIN ACCESS
TO THE TARGET
SYSTEM



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

EXERCISE 1:
CREATE A TROJAN
TO GAIN ACCESS
TO THE TARGET
SYSTEM

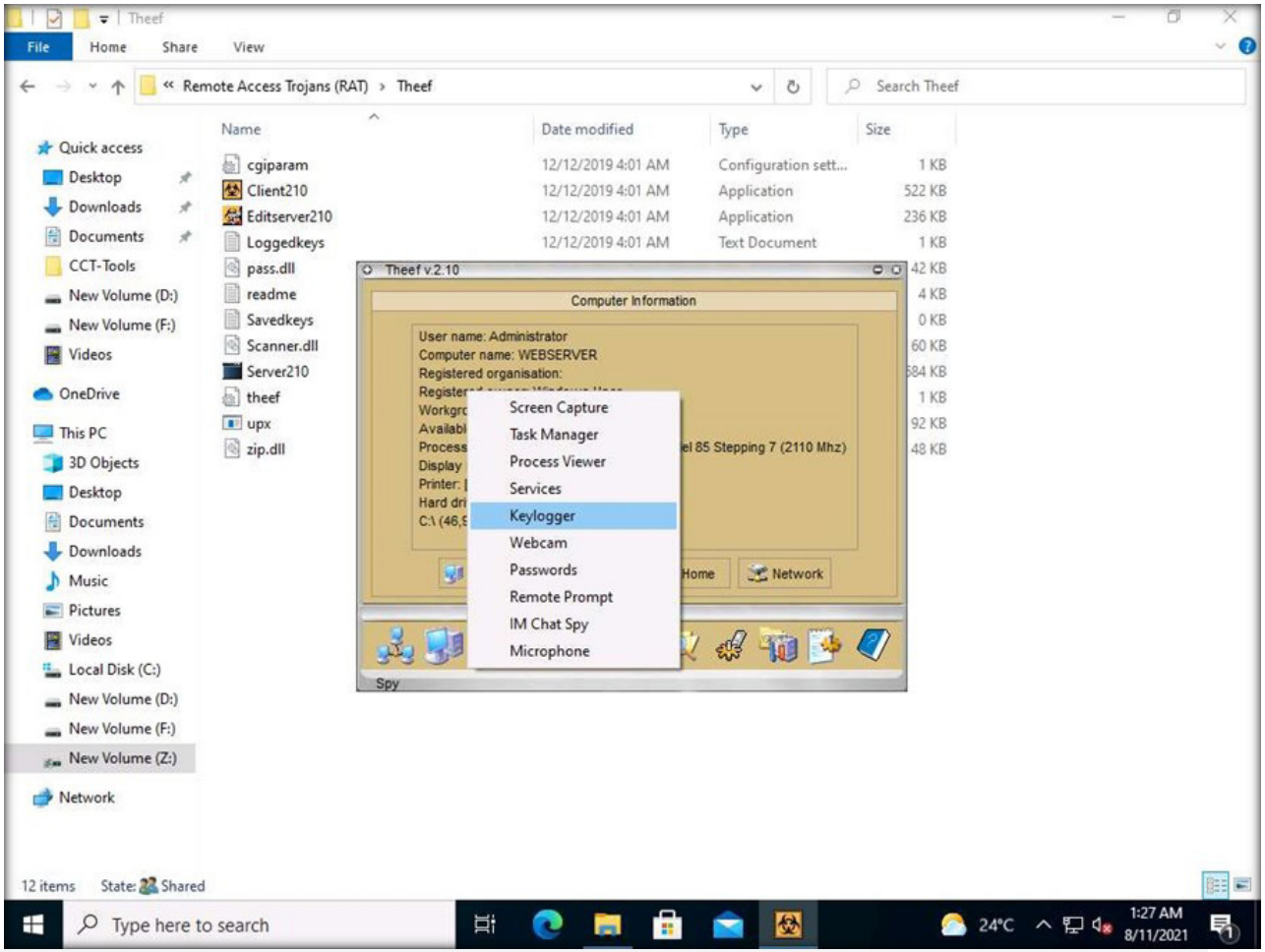


19. Close the Task Manager window.

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

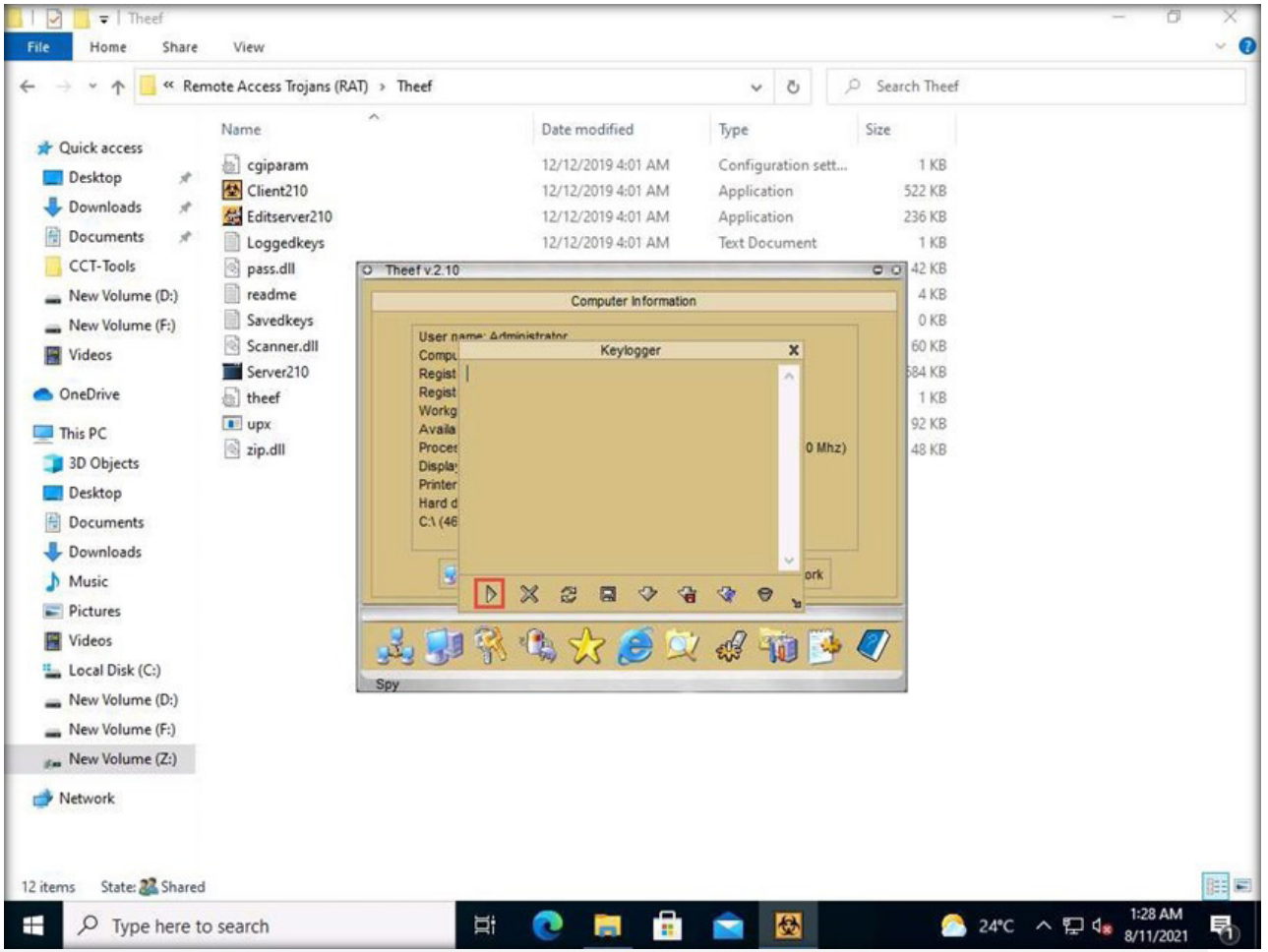
20. From the Spy menu, click Keylogger to record the keystrokes made on the victim machine.

EXERCISE 1: CREATE A TROJAN TO GAIN ACCESS TO THE TARGET SYSTEM



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

EXERCISE 1:
CREATE A TROJAN
TO GAIN ACCESS
TO THE TARGET
SYSTEM



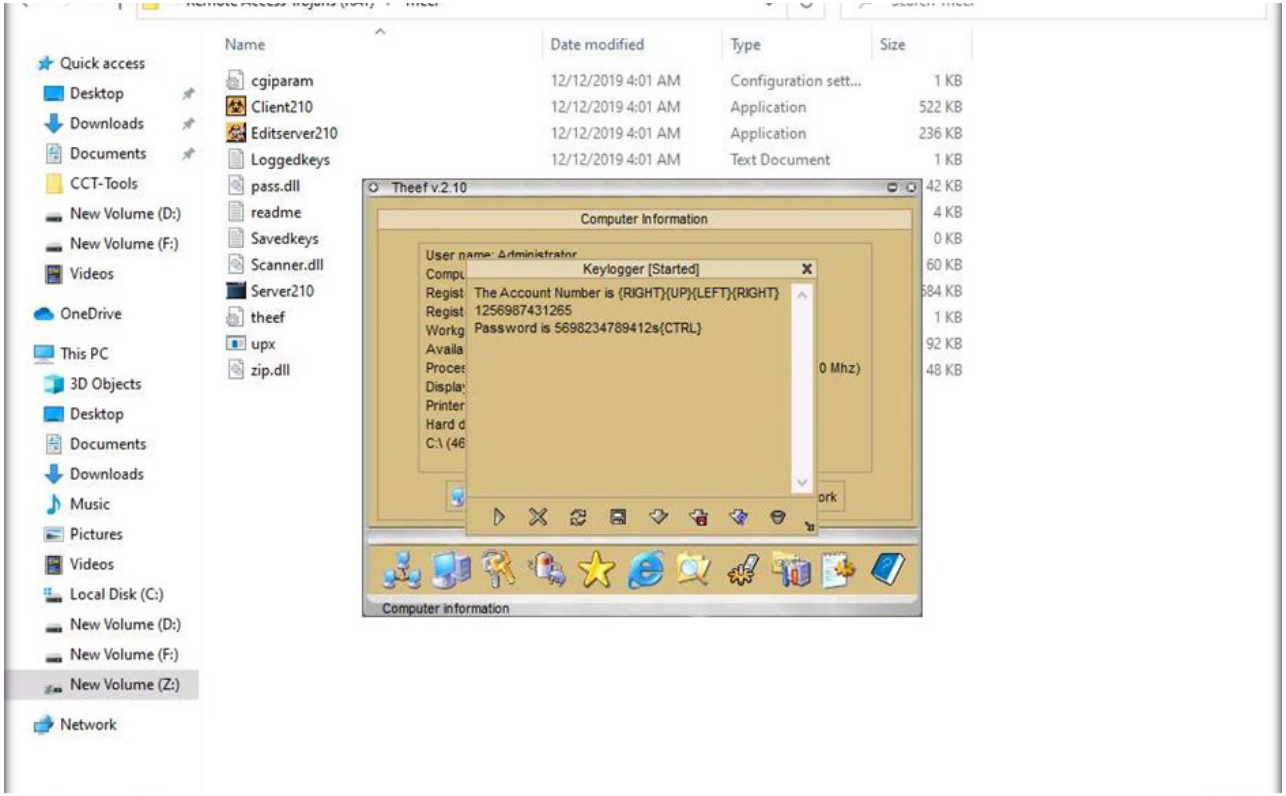
Note: If you are already logged into the Web Server machine, then skip to Step#23.

22. Switch to the Web Server virtual machine and log in with the credentials Administrator and admin@123.

Note: If a Shut Down Windows window appears click on Cancel.

23. Open a text document and enter some sensitive information.
24. Switch back to the attacker machine (Admin Machine-1) to view the recorded keystrokes of the victim machine in the Theef Keylogger window.

EXERCISE 1: CREATE A TROJAN TO GAIN ACCESS TO THE TARGET SYSTEM



25. Close the Theef Keylogger window.
26. Similarly, other details of the victim machine can be accessed by clicking on the various icons.
27. Close all open windows on both the Admin Machine-1 and Web Server virtual machines.
28. Turn off Web Server virtual machine.

EXERCISE 1: CREATE A TROJAN TO GAIN ACCESS TO THE TARGET SYSTEM

EXERCISE 2: **CREATE A VIRUS TO INFECT THE TARGET SYSTEM**

A computer virus is a self-replicating program that reproduces its code by attaching copies of itself to other executable code and operates without the knowledge or consent of the user.

LAB SCENARIO

Viruses are the scourge of modern computing. Computer viruses have the potential to wreak havoc on both businesses and personal computers. The lifetime of a virus depends on its ability to reproduce. Therefore, attackers design virus code in such a manner that the virus replicates itself n times, where n is a number specified by the attacker.
A security professional must have the required knowledge to create a virus and infect a machine in the local network to test the security infrastructure.

OBJECTIVE

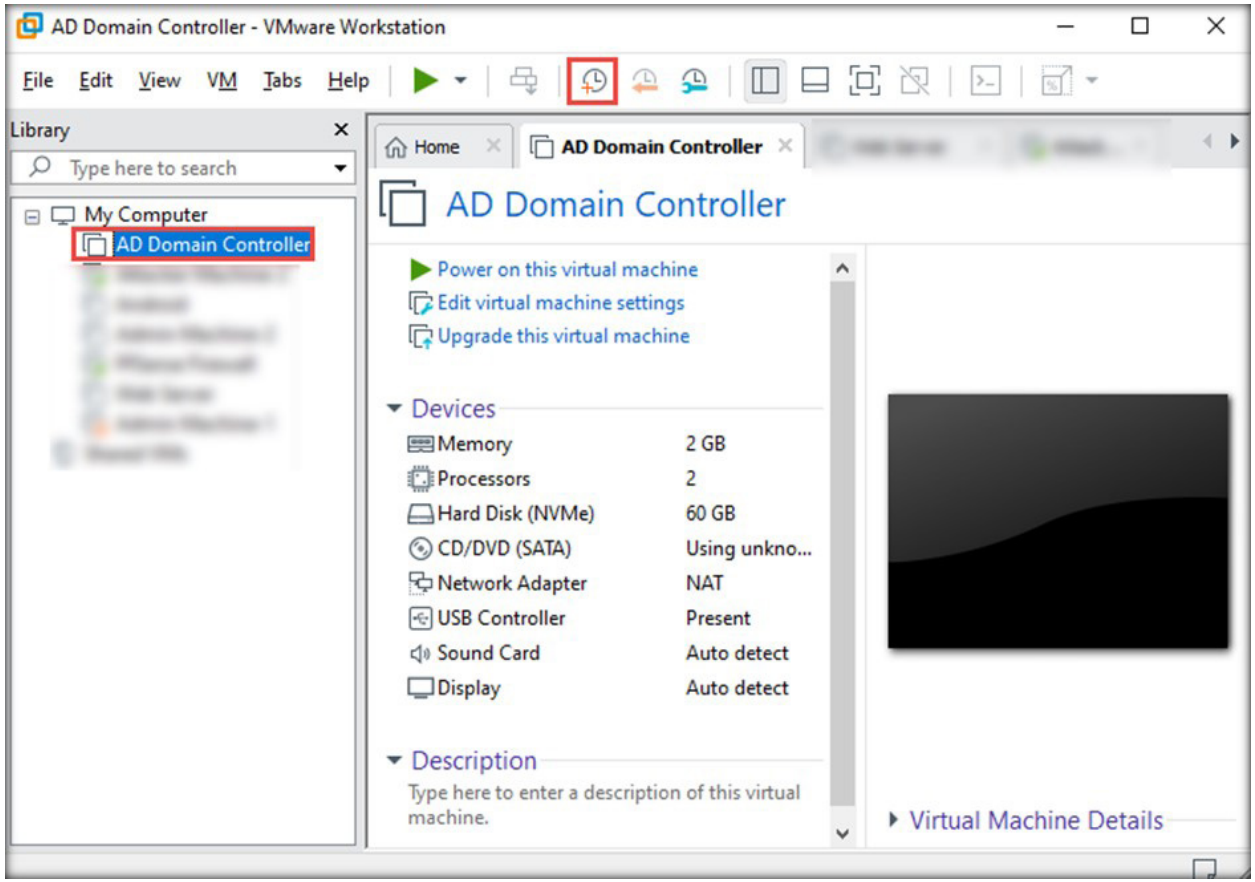
This lab demonstrates how to create a virus using the JPS Virus Maker Tool and Infect the Target System.

OVERVIEW OF TROJAN

Virus reproduces its own code while enclosing other executables, and spreads throughout the computer. Viruses can spread the infection by damaging files in a file system. Some viruses reside in the memory and may infect programs through the boot sector. A virus can also be in an encrypted form.
The JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool's features are auto-start, shutdown, disable security centre, lock mouse and keyboard, destroy protected storage, and terminate windows. Security professional can use the JPS Virus Maker Tool as a proof of concept to audit perimeter security controls in an organization.

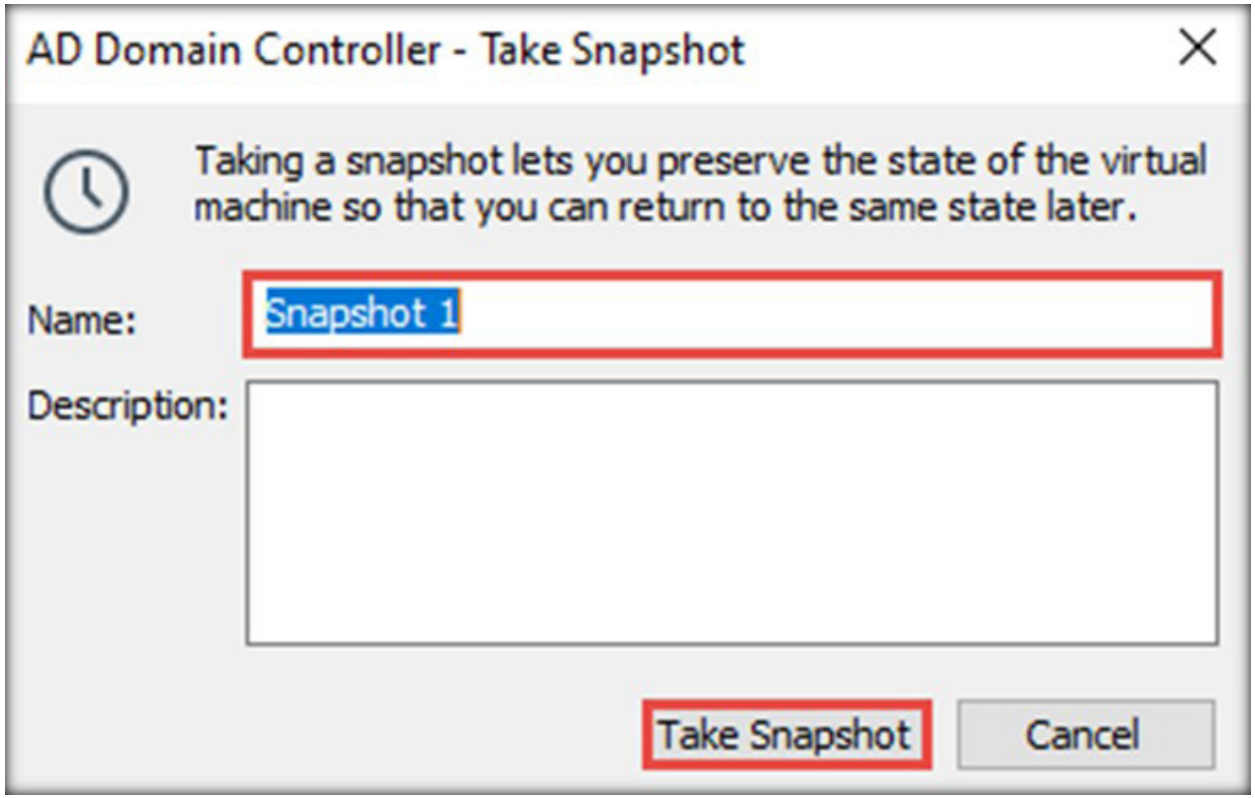
EXERCISE 2:
CREATE A VIRUS TO
INFECT THE TARGET
SYSTEM

Note: Before performing this task, take a snapshot of the AD Domain Controller virtual machine as the trojan will infect the machine.
a. In the VMware Workstation window, click AD Domain Controller in the left pane and click the Take a snapshot of this virtual machine ( ) icon, as shown in the screenshot.



b. The AD Domain Controller - Take Snapshot pop-up appears; type a name for the snapshot in the Name field, leave the description field set to default, and click Take Snapshot.

EXERCISE 2:
CREATE A VIRUS TO
INFECT THE TARGET
SYSTEM



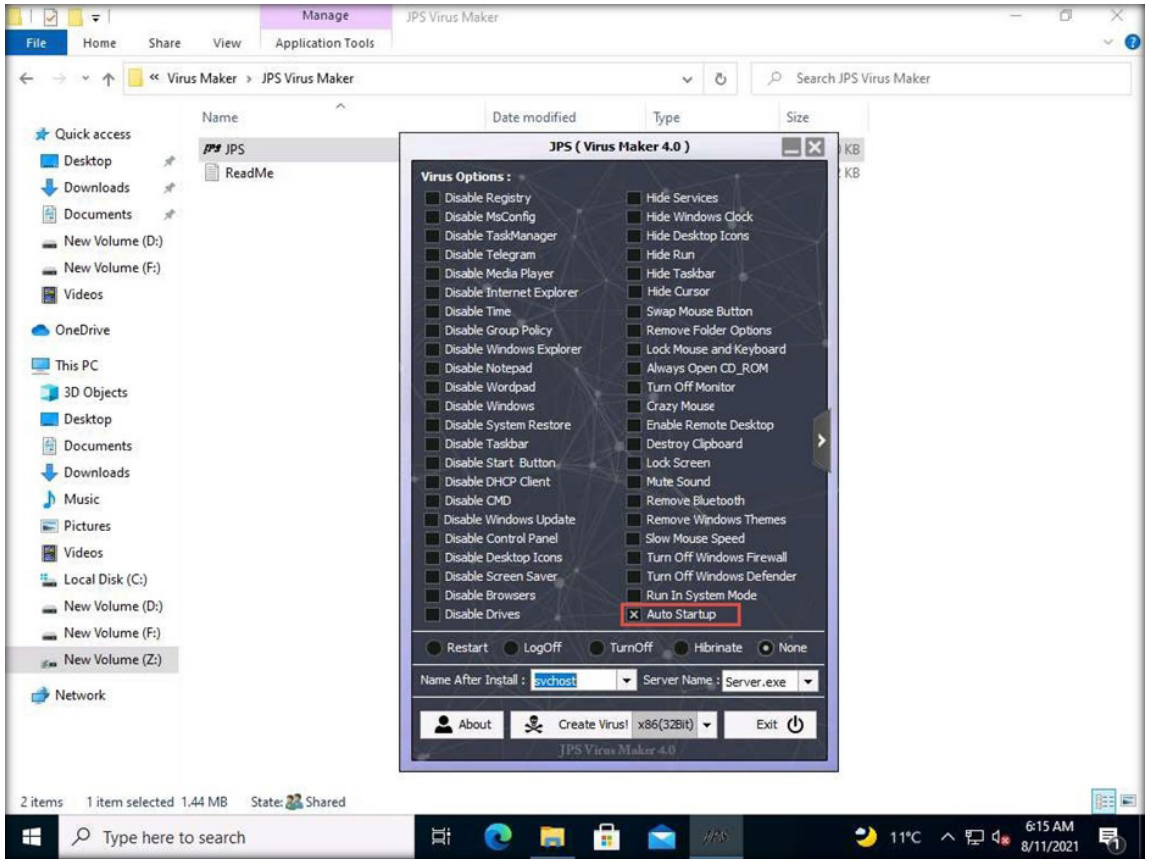
EXERCISE 2: CREATE A VIRUS TO INFECT THE TARGET SYSTEM

Note: Ensure that PfSense Firewall and Admin Machine-1 virtual machines are running.

1. Turn on the AD Domain Controller virtual machine.
2. Switch to the Admin Machine-1 virtual machine. Navigate to Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Virus Maker\JPS Virus Maker and double-click JPS.exe.

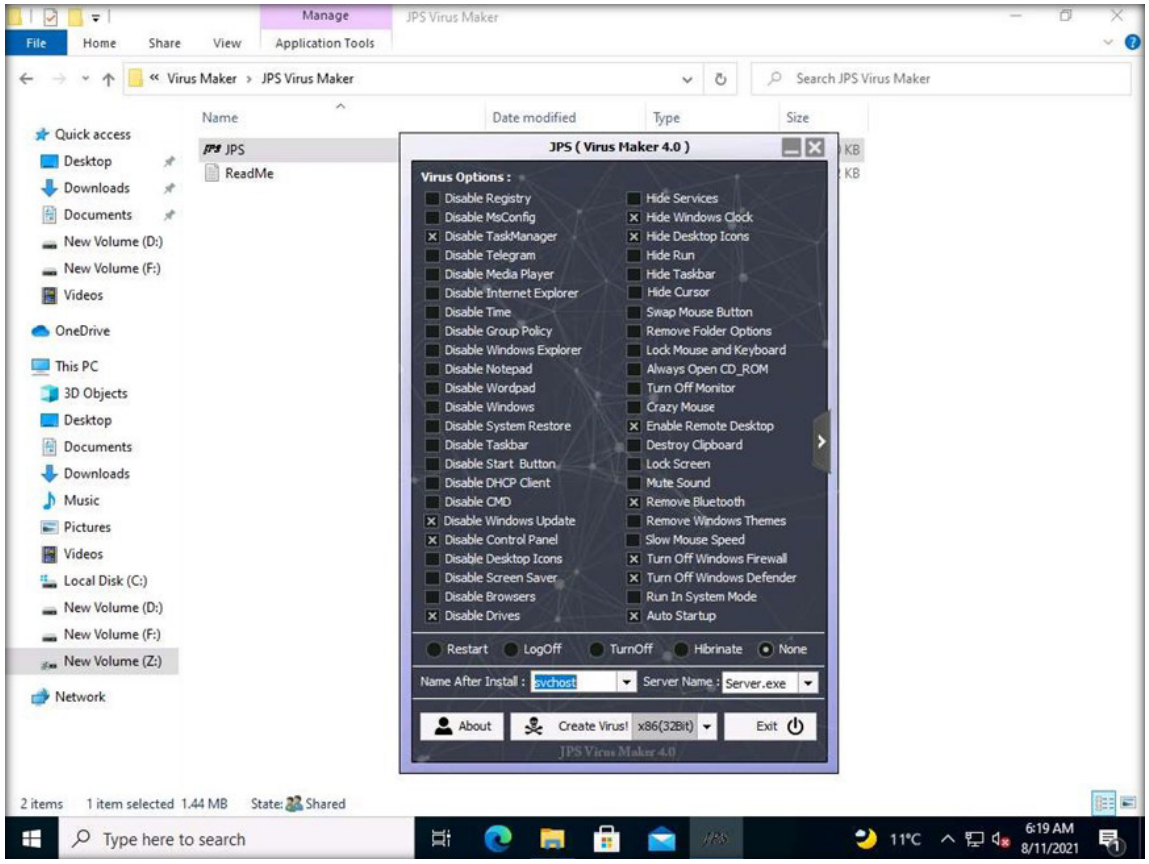
Note: If an Open File - Security Warning pop-up appears, click Run.

3. The JPS (Virus Maker 4.0) window appears; check the Auto Startup checkbox.



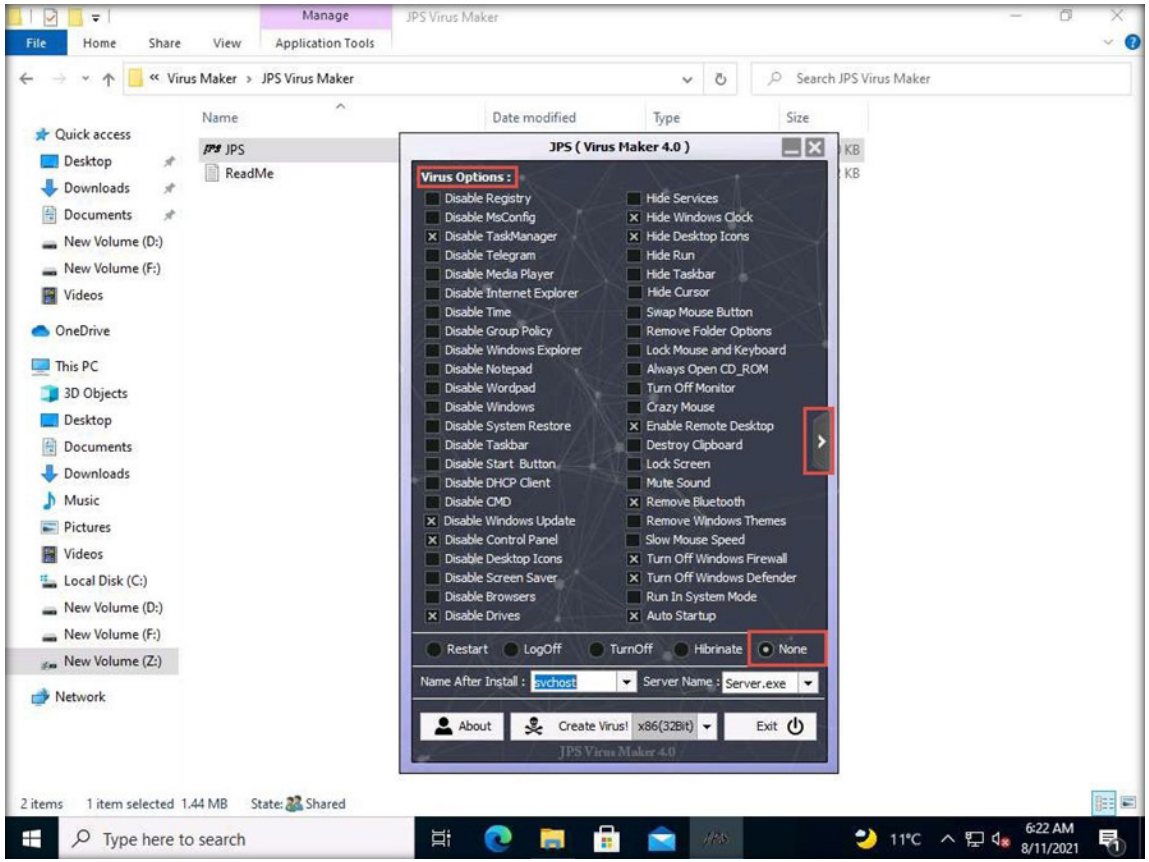
4. The window displays various features and options that can be chosen while creating a virus file.
5. From Virus Options, check the options to embed in a new virus file.
6. In this lab, the options to embed in the virus file are Disable TaskManager, Disable Windows Update, Disable Control Panel, Disable Drives, Hide Windows Clock, Hide Desktop Icons, Enable Remote Desktop, Remove Bluetooth, Turn Off Windows Firewall, Turn Off Windows Defender, and Auto Startup.

EXERCISE 2: CREATE A VIRUS TO INFECT THE TARGET SYSTEM



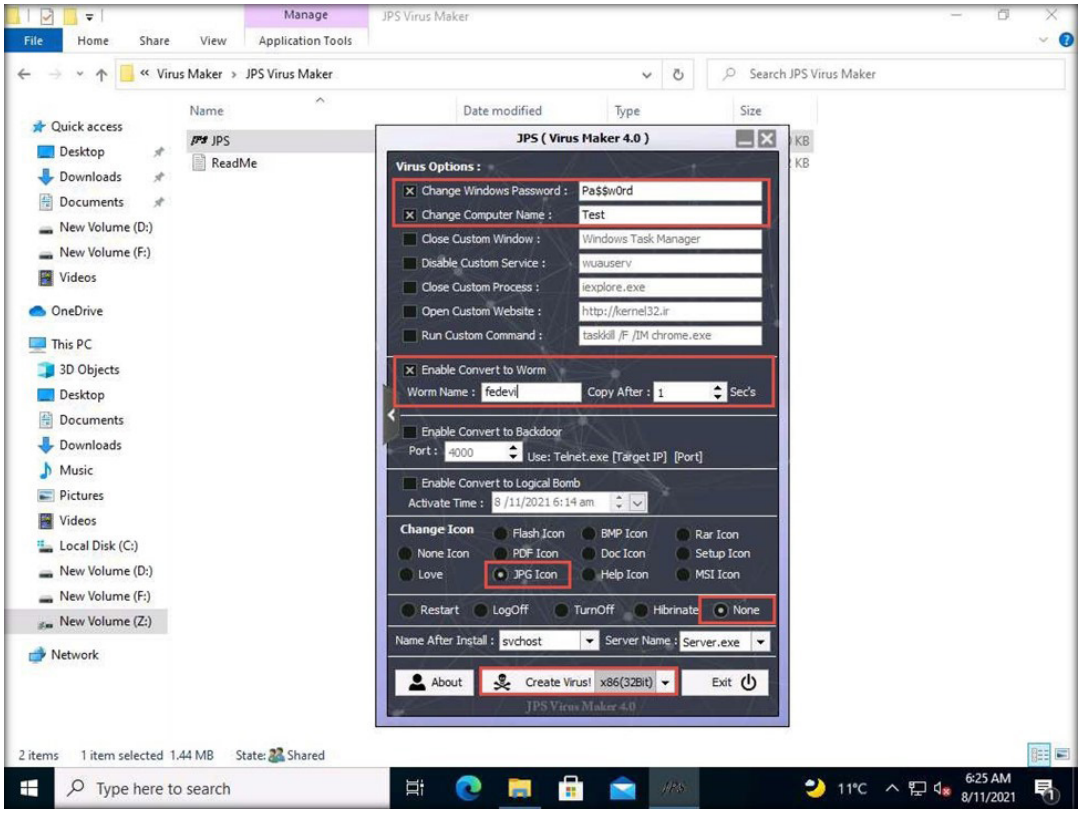
7. Ensure that the None radio button is selected to specify the trigger event for the virus to start attacking the system after its creation.
8. Before clicking on Create Virus!, click the right arrow icon from the right-hand pane of the window to configure the virus options.

EXERCISE 2: CREATE A VIRUS TO INFECT THE TARGET SYSTEM



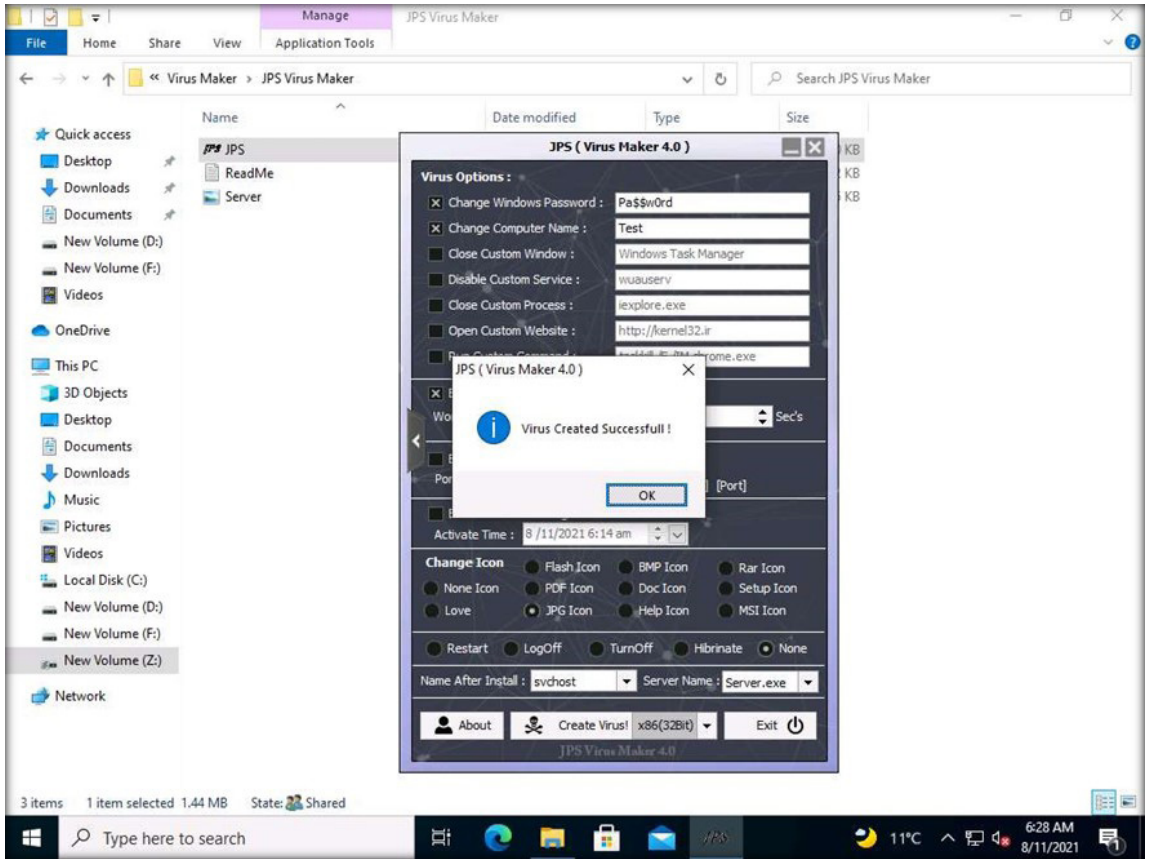
9. A Virus Options window appears, as shown in the screenshot below.
10. Check the Change Windows Password option, and enter a password (here, Pa$$w0rd) in the text field. Check the Change Computer Name option, and type Test in the text field.
11. You can even configure the virus to convert to a worm. To do this, check the Enable Convert to Worm checkbox, and provide a Worm Name (here, fedevi). For the worm to self-replicate after a particular time, specify the time in seconds (here, 1 s) in the Copy After field.
12. Ensure that the JPG Icon radio button is selected under the Change Icon section. Ensure that the None radio button is selected in the lower part of the window.
13. After completing the selection of options, click the drop-down icon next to the Create Virus! button and select x86(32Bit). Click Create Virus!

EXERCISE 2: CREATE A VIRUS TO INFECT THE TARGET SYSTEM



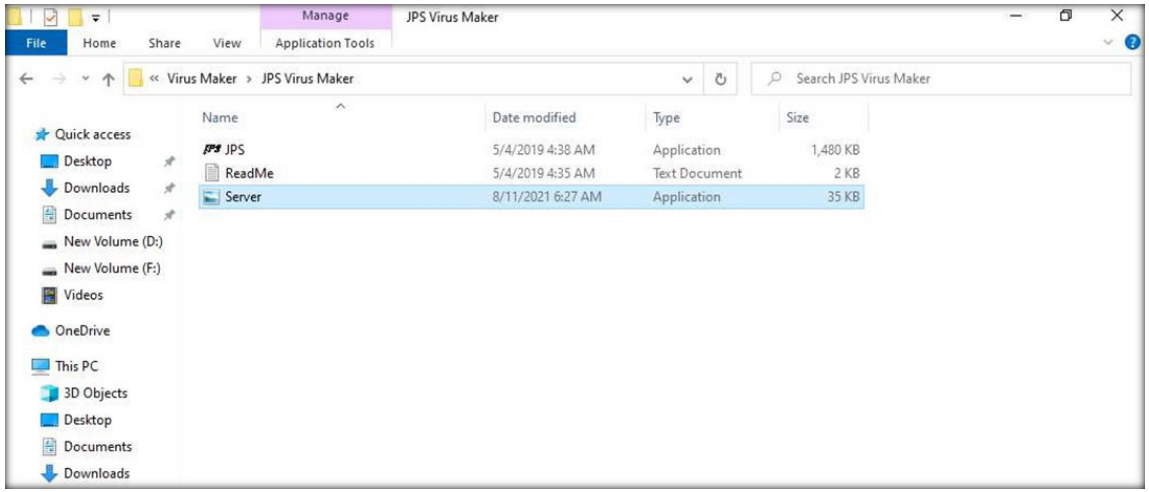
14. A Virus Created Successful! pop-up appears; click OK.

EXERCISE 2:
CREATE A VIRUS TO
INFECT THE TARGET
SYSTEM



15. The newly created virus (server) is placed automatically in the folder where jps.exe is located, but with the name Server.exe. Navigate to Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Virus Maker\JPS Virus Maker and observe that the newly created virus with the name Server.exe is available at the specified location.

EXERCISE 2:
CREATE A VIRUS TO
INFECT THE TARGET
SYSTEM

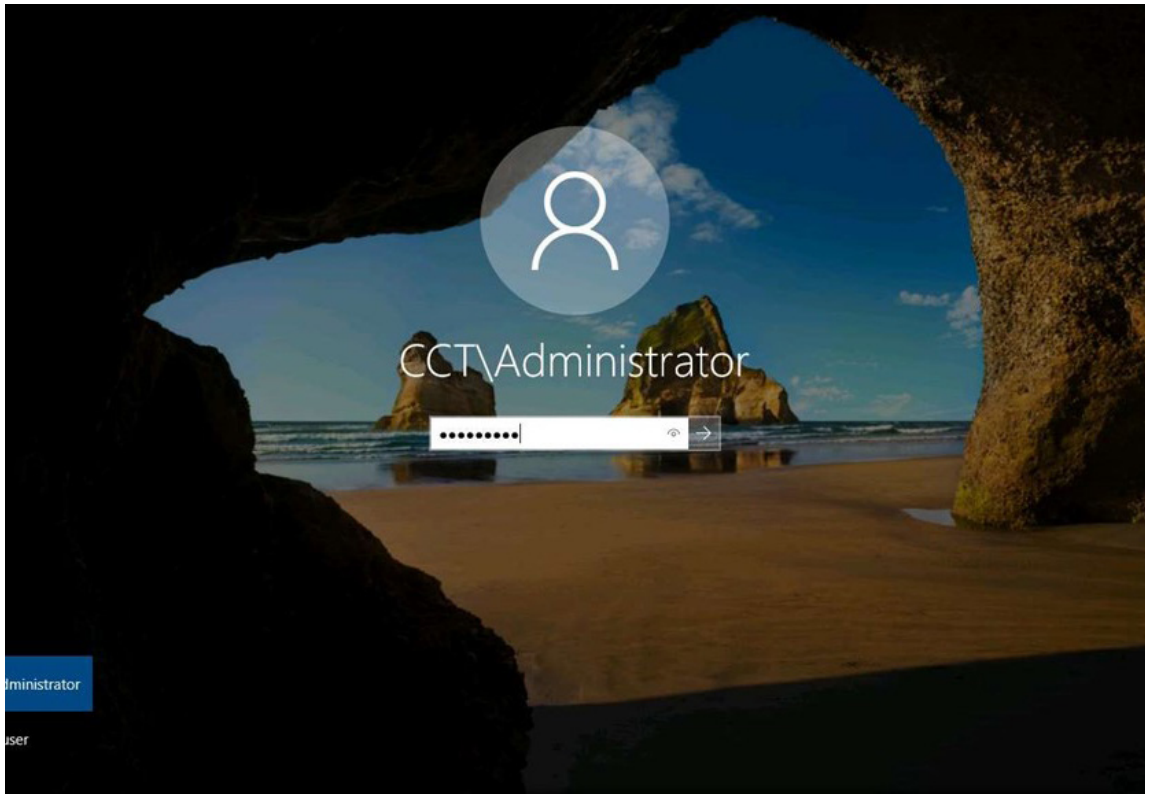


16. Now, pack this virus with a binder or virus packager and send it to the victim machine through email, chat, a mapped network drive, or other method.
17. In this task, we are using a mapped network drive to share the virus file to the victim machine. Assume that you are a victim and that you have received this file.
18. Switch to the AD Domain Controller to virtual machine, log in with credentials CCT\Administrator and admin@123.

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

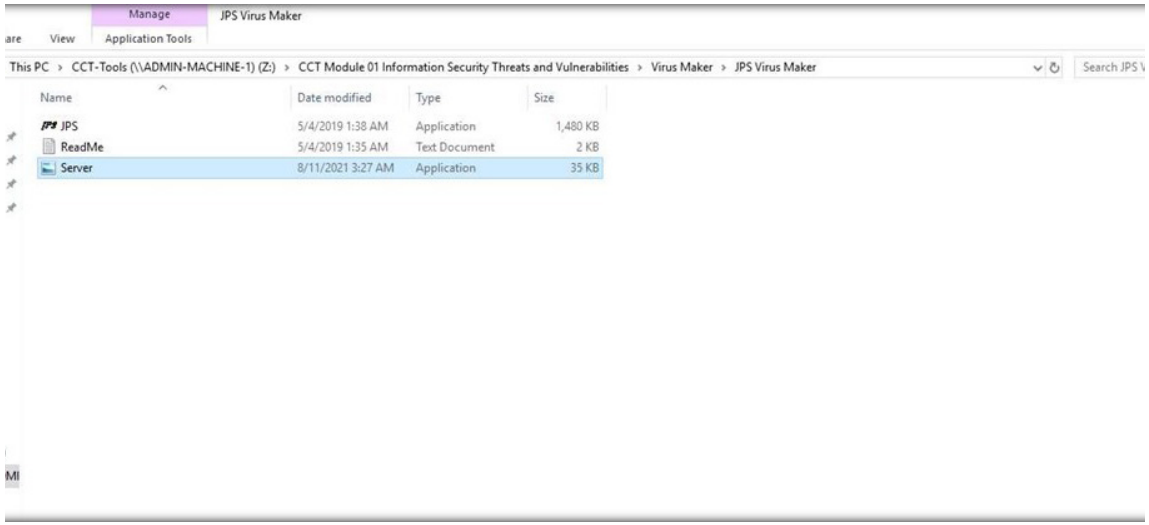
Networks screen appears, click Yes to allow your PC to be discoverable by other PCs and devices on the network.

EXERCISE 2: CREATE A VIRUS TO INFECT THE TARGET SYSTEM



19. Navigate to Z:\CCT-Tools\CCT Module 01 Information Security Threats and Vulnerabilities\Virus Maker\JPS Virus Maker and double-click the Server.exe file to execute the virus.

EXERCISE 2:
CREATE A VIRUS TO
INFECT THE TARGET
SYSTEM

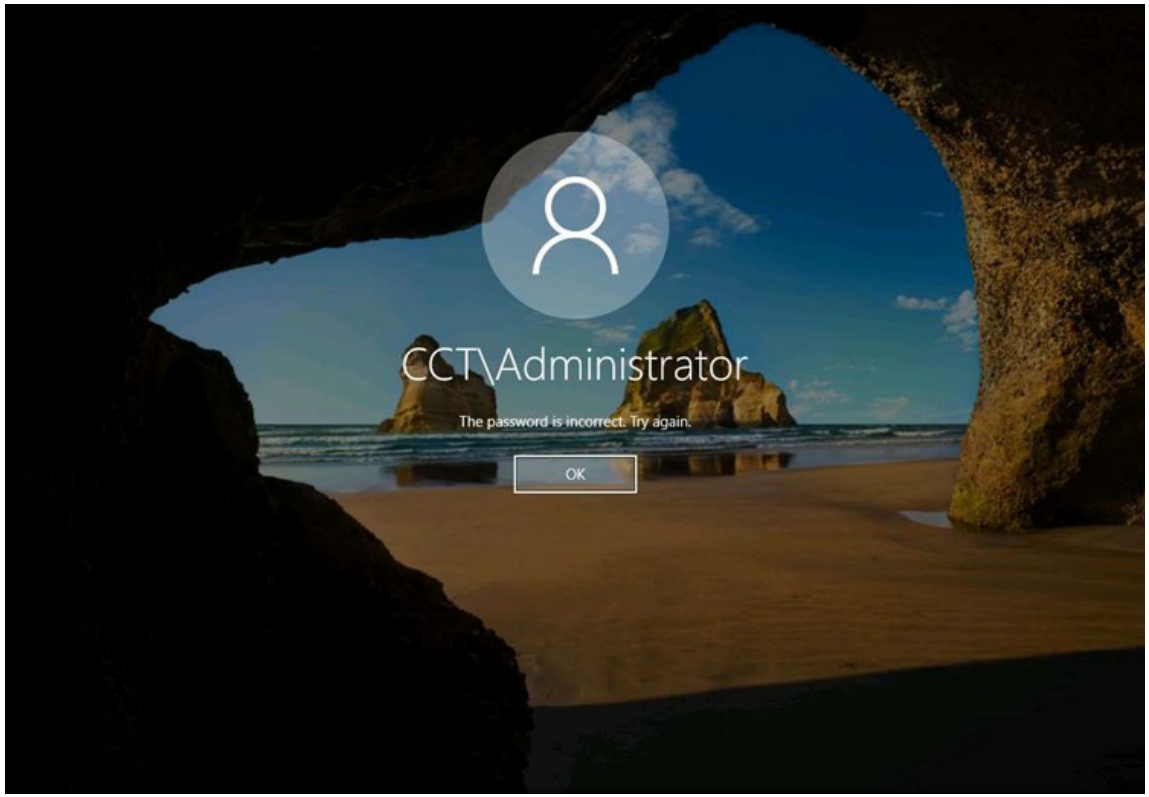


20. Once you have executed the virus, the Desktop screen becomes blank, indicating that the virus has infected the system, as shown in the screenshot below.

EXERCISE 2: CREATE A VIRUS TO INFECT THE TARGET SYSTEM

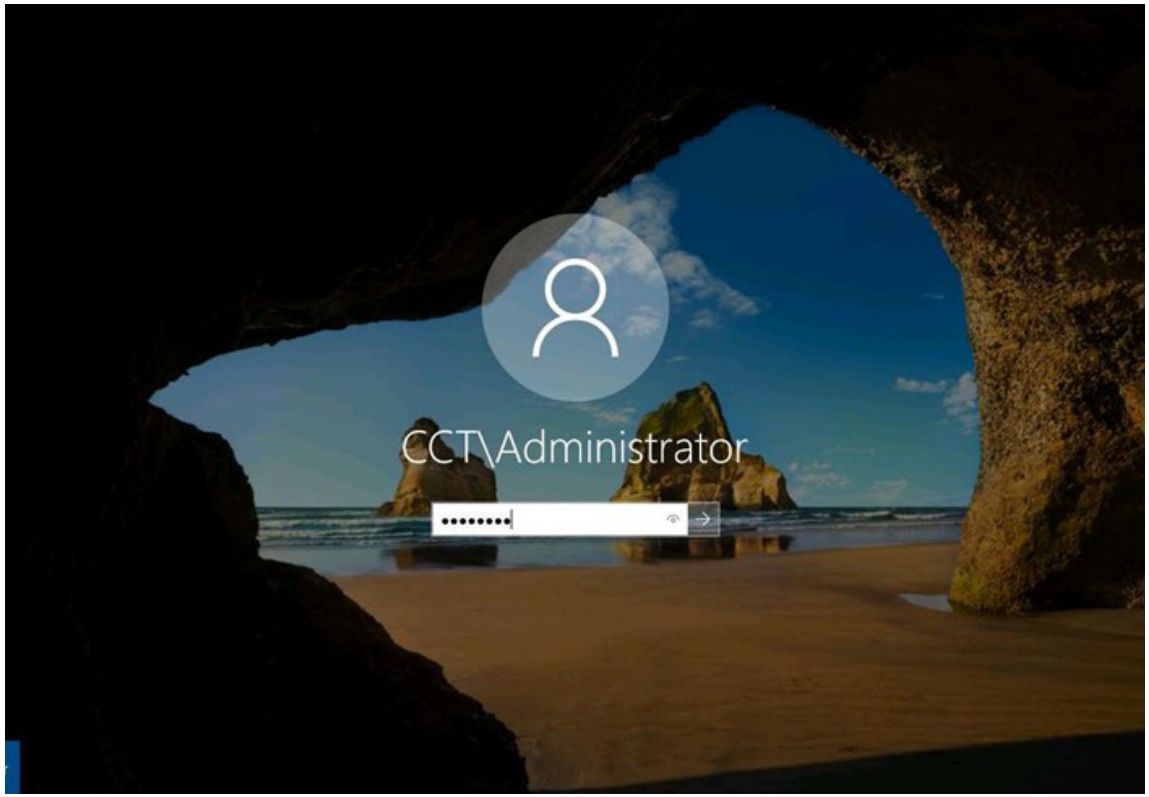
21. Surprised by the system behaviour, the victim (you) attempts to fix the machine by restarting it. Once the machine has rebooted, attempt to log in to the machine with the provided Username and Password. You should receive the following error message, “The password is incorrect. Try again.”
22. Log in with the credentials CCT\Administrator and admin@123.

EXERCISE 2:
CREATE A VIRUS TO
INFECT THE TARGET
SYSTEM



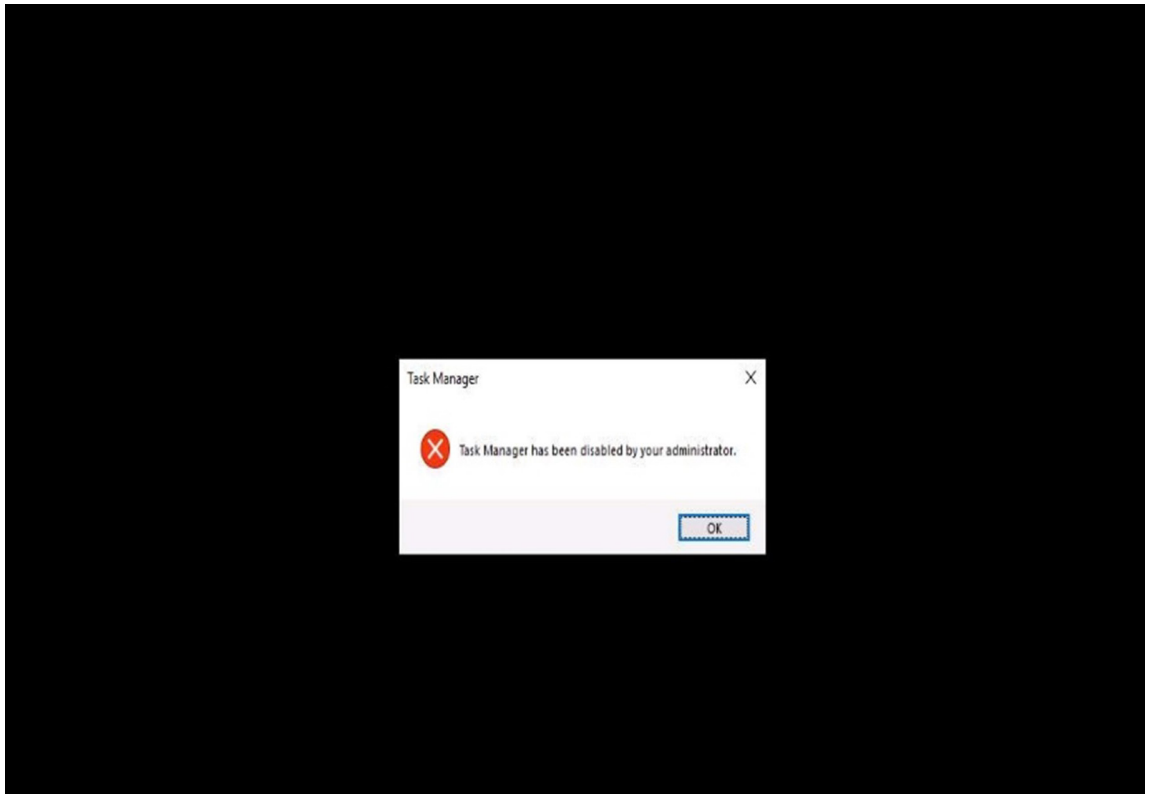
23. Now, login with the password that was provided at the time of virus creation (i.e., Pa$$w0rd). You should be able to log in to the machine with the new password.

EXERCISE 2:
CREATE A VIRUS TO
INFECT THE TARGET
SYSTEM



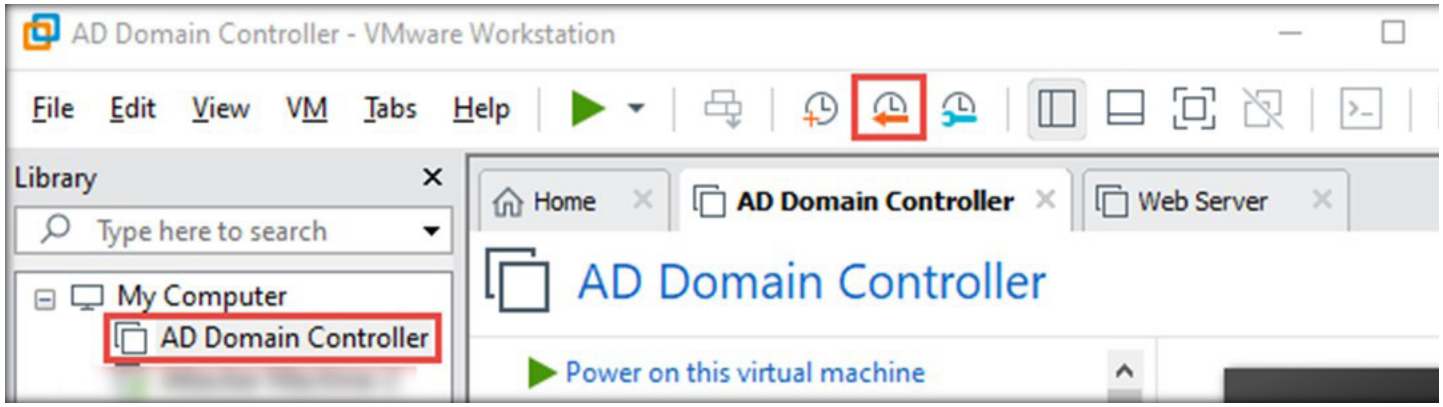
24. Now, attempt to open Task Manager. Observe that an error pop-up appears. Click OK.
Note: To open Task Manager, type task manager in Type here to search field and select Task Manager application.

EXERCISE 2:
CREATE A VIRUS TO
INFECT THE TARGET
SYSTEM



25. A similar error is displayed for all the applications that are disabled by the virus.
26. Turn off Admin Machine-1 and AD Domain Controller virtual machines.
27. Now, before going to the next task, click the Revert this virtual machine to snapshot: (Saved snapshot) icon to revert the machine to its initial state (before running trojan).

EXERCISE 2: CREATE A VIRUS TO INFECT THE TARGET SYSTEM



28. The VMware Workstation pop-up appears, stating that, By restoring this snapshot, the current state will be lost; click Yes.

EXERCISE 2:
CREATE A VIRUS TO
INFECT THE TARGET
SYSTEM

EXERCISE 3: **CREATE A WORM USING THE INTERNET WORM MAKER THING**

Computer worms are standalone malicious programs that replicate, execute, and spread across network connections independently without human intervention.

LAB SCENARIO

Worms are a subtype of viruses. A worm does not require a host to replicate; however, in some cases, the worm's host machine is also infected. Initially, black hat professionals treated worms as a mainframe problem. Later, with the introduction of the Internet, they mainly focused on and targeted Windows OS using the same worms by sharing them in via e-mail, IRC, and other network functions. Attackers use worm payloads to install backdoors on infected computers, which turns them into zombies and creates a botnet.
This lab demonstrates how easily an attacker can create a worm. A security professional can use Internet Worm Maker Thing as a proof of concept to audit perimeter security controls in the organization.

OBJECTIVE

This lab demonstrates how to create a worm using Internet Worm Maker Thing.

OVERVIEW OF WORM MAKERS

Worm makers are tools that are used to create and customize computer worms to perform malicious tasks. These worms, once created, spread independently over networks and poison entire networks. With the help of pre-defined options in the worm makers, a worm can be designed according to the task it is intended to execute.

Internet Worm Maker Thing is an open-source tool used to create worms that can infect a victim's drives and files, show messages, disable antivirus software, etc. This tool comes with a compiler that can easily convert your batch virus into an executable to evade antivirus software or for any other purpose.

Note: Ensure that PfSense Firewall virtual machine is running.

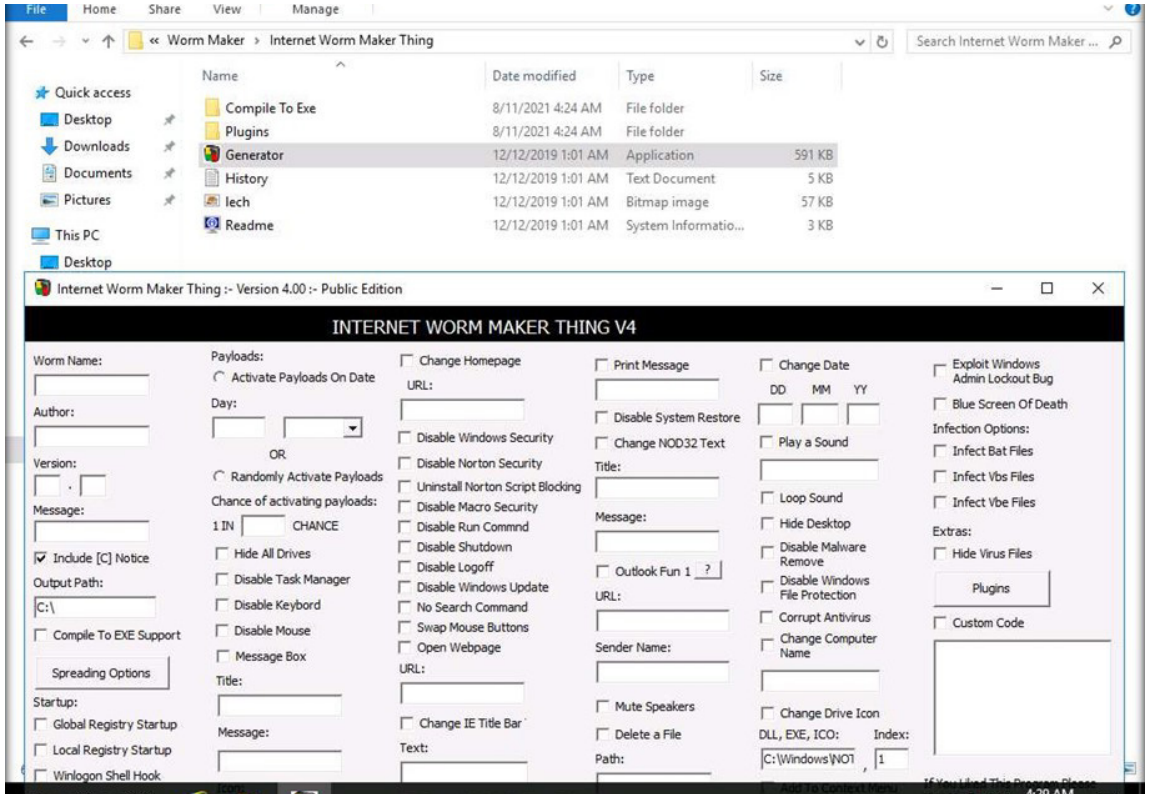
1. Turn on the Web Server virtual machine and log in with the credentials Administrator and admin@123.

Note: The Networks screen appears. Click Yes to allow the PC to be discoverable by other PCs and devices on the network.

2. To launch Internet Worm Maker Thing, navigate to Z:\CCT Module 01 Information Security Threats and Vulnerabilities\Worm Maker\Internet Worm Maker Thing, and double-click the Generator.exe file. The main window of Internet Worm Maker Thing appears, as shown in the screenshot below.

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

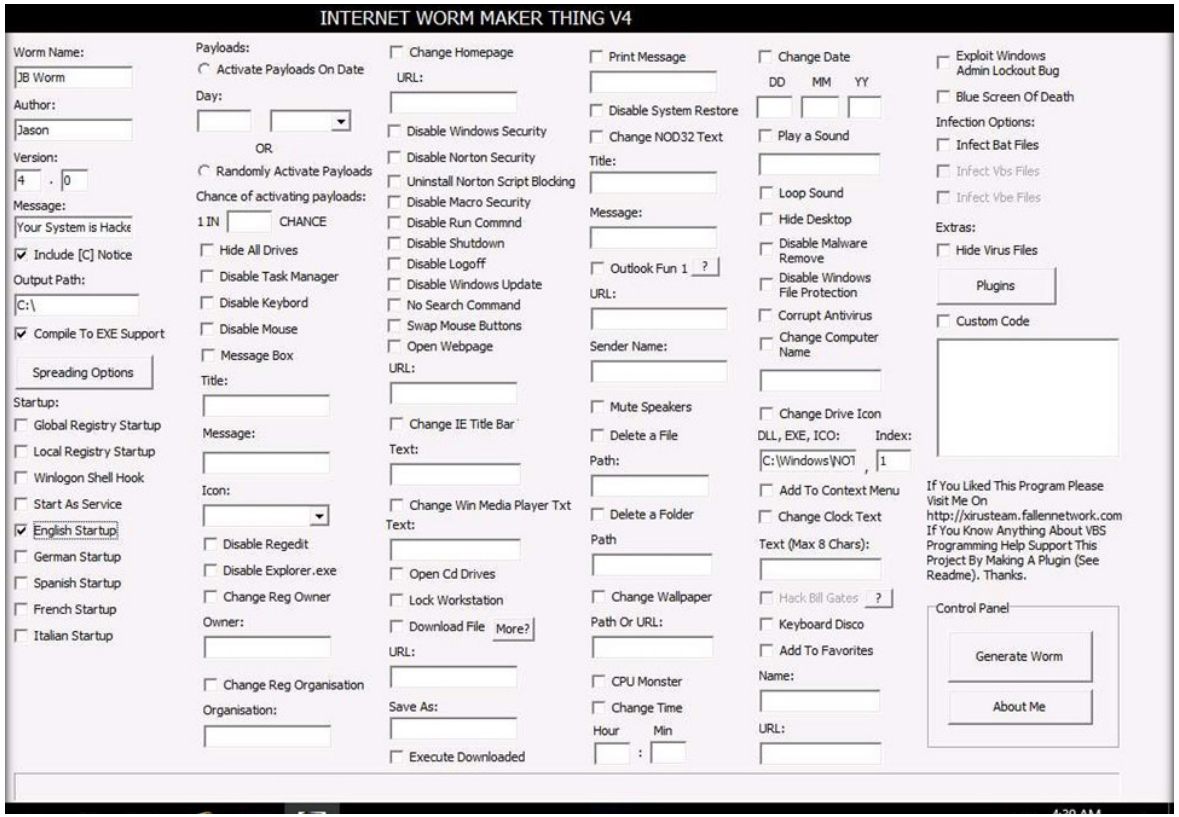
EXERCISE 3: CREATE A WORM USING THE INTERNET WORM MAKER THING



3. Enter a Worm name, author, version, message and output path for the created worm. Click the Compile To EXE Support checkbox, under the Worm Name section and English Startup under Startup section.

Note: We have entered JB Worm in the Worm Name field, and Jason in the Author field, 4.0 in the Version field, Your System is Hacked in the Message field and C:\\ in the Output Path.

EXERCISE 3: CREATE A WORM USING THE INTERNET WORM MAKER THING



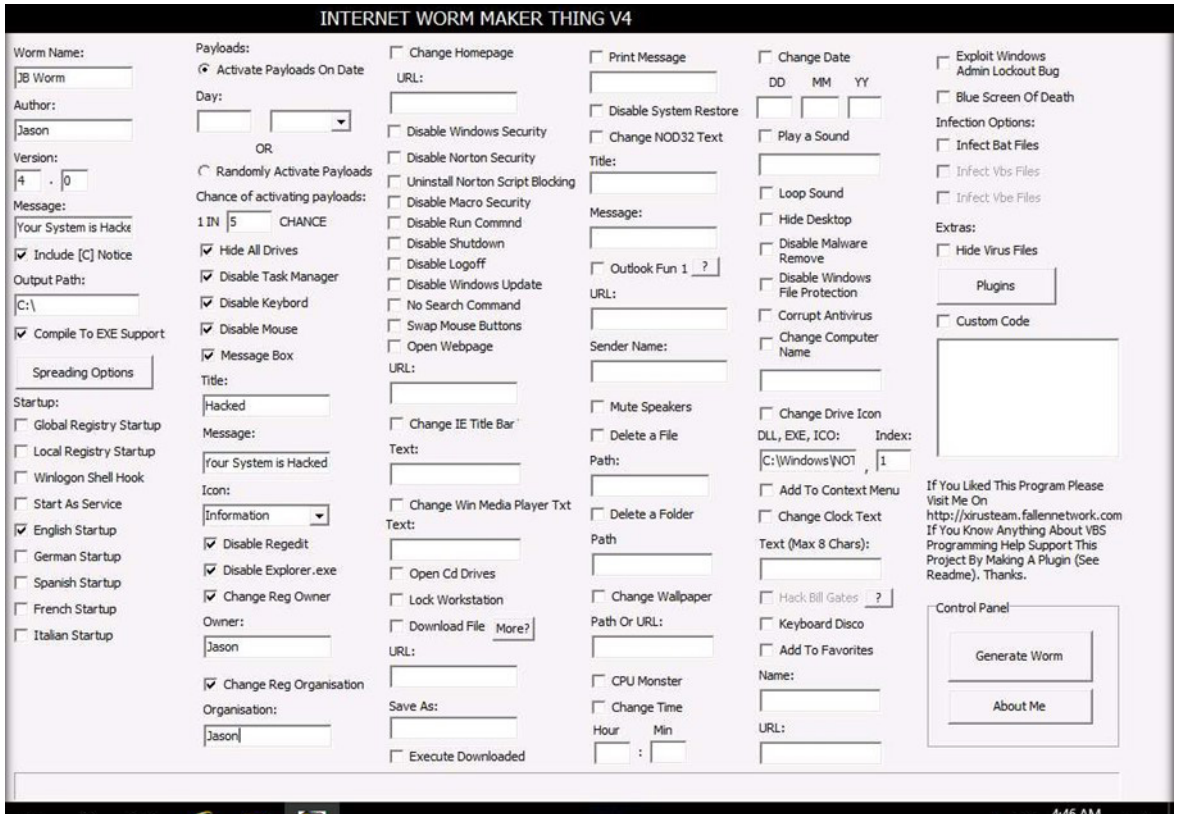
4. Select the Activate Payloads On Date radio button, under Payloads; and enter the Chance of activating payloads value of 5. Select the Hide All Drives, Disable Task Manager, Disable Keyboard, Disable Mouse, and Message Box checkboxes.

Enter a Title and a Message, and select Information from the Icon drop-down list. Select the Disable Regedit, Disable Explorer.exe and Change Reg Owner checkboxes.

Type the name in the Owner field here Jason, check Change Reg Organisation and type Jason in the Organisation field.

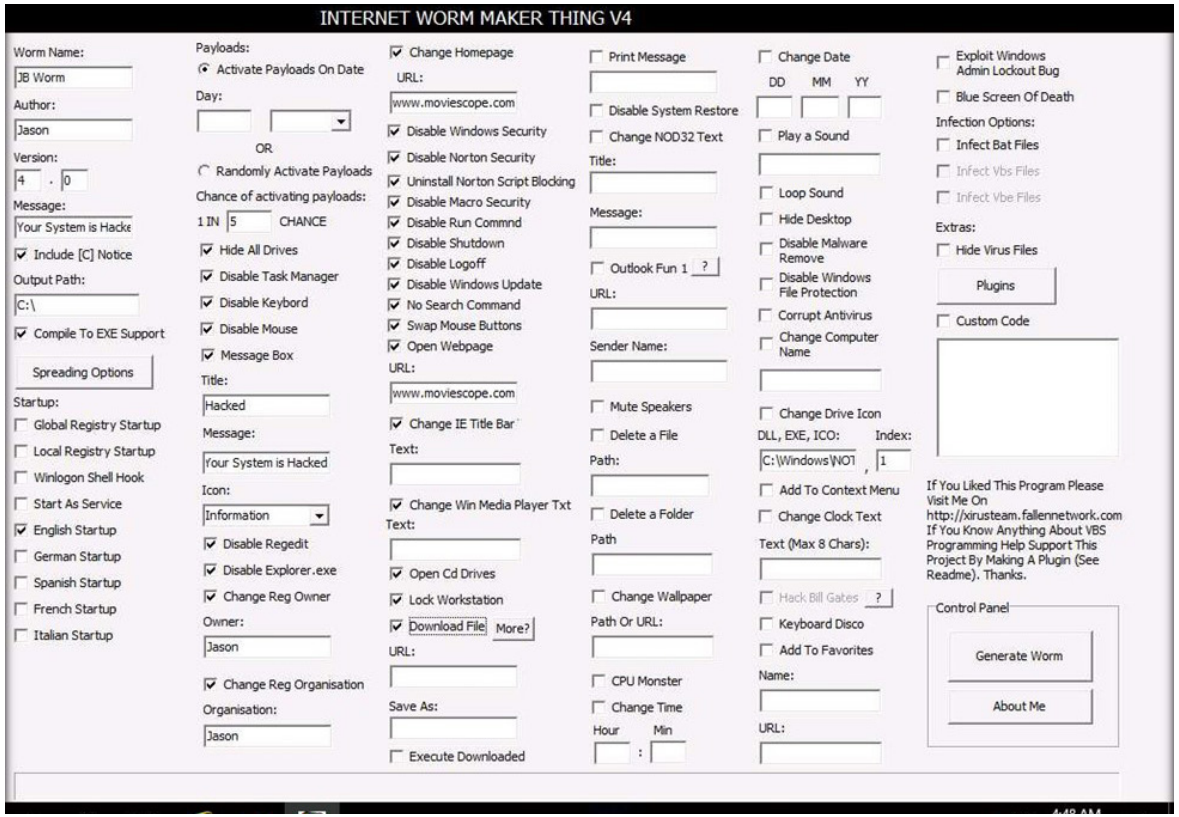
Note: In this lab we have entered Hacked in the Title field, and Your System is Hacked in the Message field

EXERCISE 3: CREATE A WORM USING THE INTERNET WORM MAKER THING



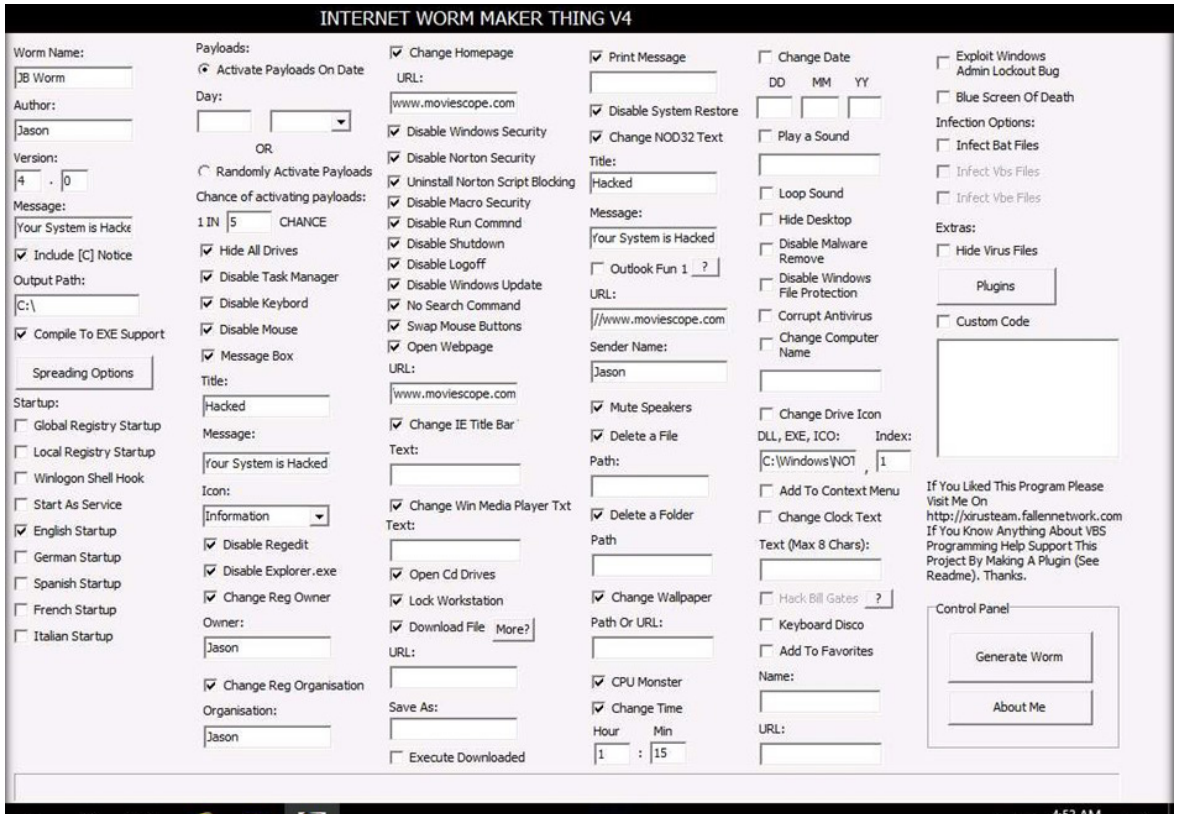
5. Select the Change Homepage checkbox, and type http://www.moviescope.com in both URL fields. Select the Disable Windows Security, Disable Norton Security, Uninstall Norton Script Blocking, Disable Macro Security, Disable Run Command, Disable Shutdown, Disable Logoff, Disable Windows Update, No Search Command, Swap Mouse Buttons, and Open Webpage checkboxes.
Select the Change IE Title Bar, Change Win Media Player Txt, Open Cd Drives, Lock Workstation and Download File checkboxes.

EXERCISE 3: CREATE A WORM USING THE INTERNET WORM MAKER THING



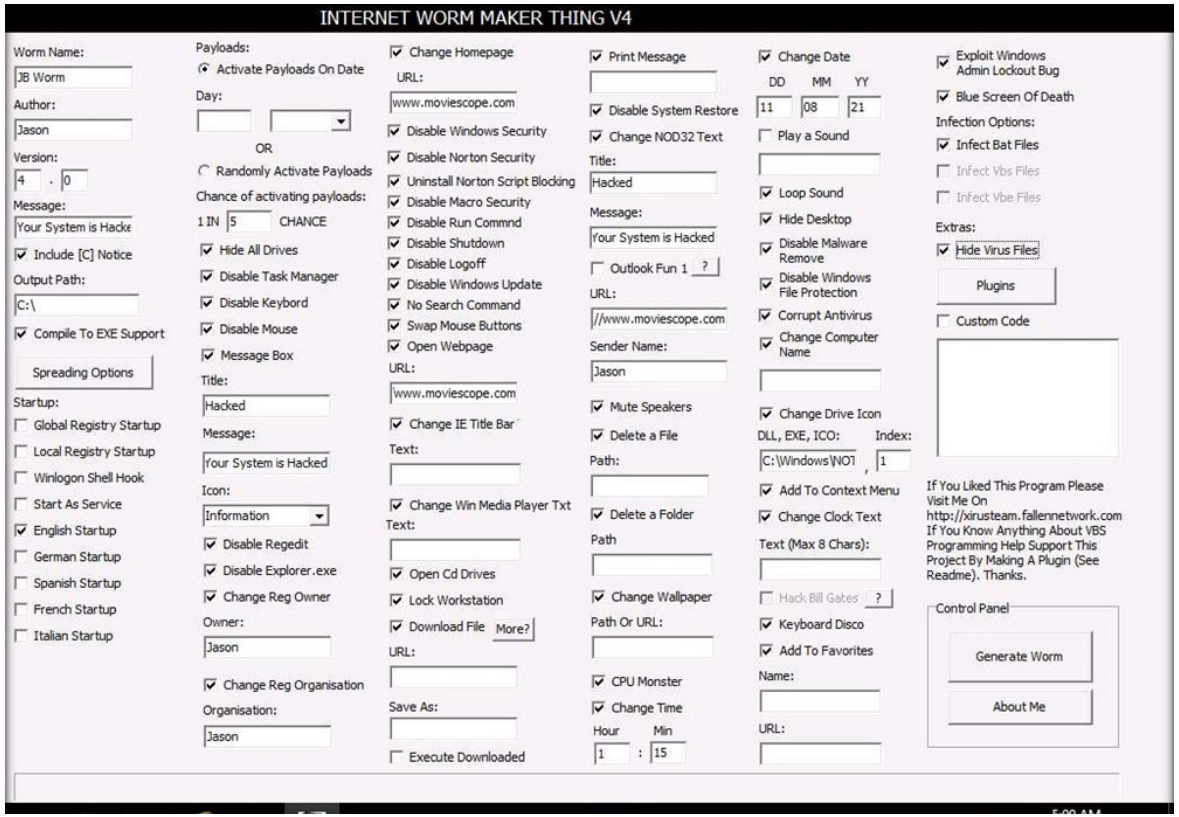
6. Select the Print Message, Disable System Restore, and Change NOD32 Text checkboxes. Enter a Title and a Message in their respective fields. Enter the URL as http://www.moviescope.com and Sender Name as Jason. Select the Mute Speakers, Delete a File, Delete a Folder, Change Wallpaper, and CPU Monster checkboxes. Select the Change Time checkbox, and enter a time in the Hour and Min fields.

EXERCISE 3: CREATE A WORM USING THE INTERNET WORM MAKER THING



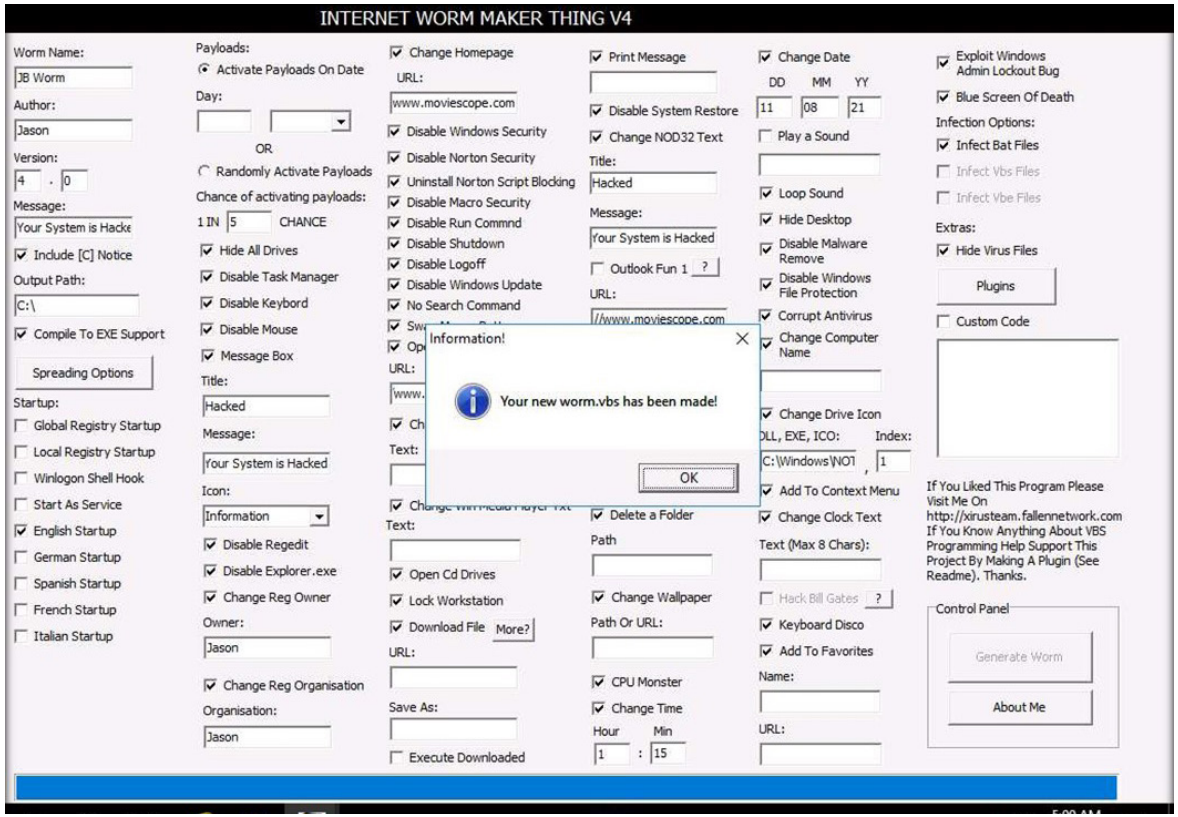
7. Select the Change Date checkbox, and enter a date in the DD, MM, and YY fields. Select the Loop Sound, Hide Desktop, Disable Malware Remove, Disable Windows File Protection, Corrupt Antivirus, and Change Computer Name checkboxes. Select the Change Drive Icon, Add To Context Menu, Change Clock Text, Keyboard Disco, and Add To Favorites checkboxes.
Select the Exploit Windows Admin Lockout Bug and Blue Screen of Death checkboxes. Select the Infect Bat Files checkbox, under Infection Options. Select the Hide Virus Files checkbox, under Extras. Click Generate Worm, under Control Panel.

EXERCISE 3:
CREATE A WORM
USING THE
INTERNET WORM
MAKER THING



8. Once the worm is successfully created, an Information! dialog box appears. Click OK to close the pop-up.

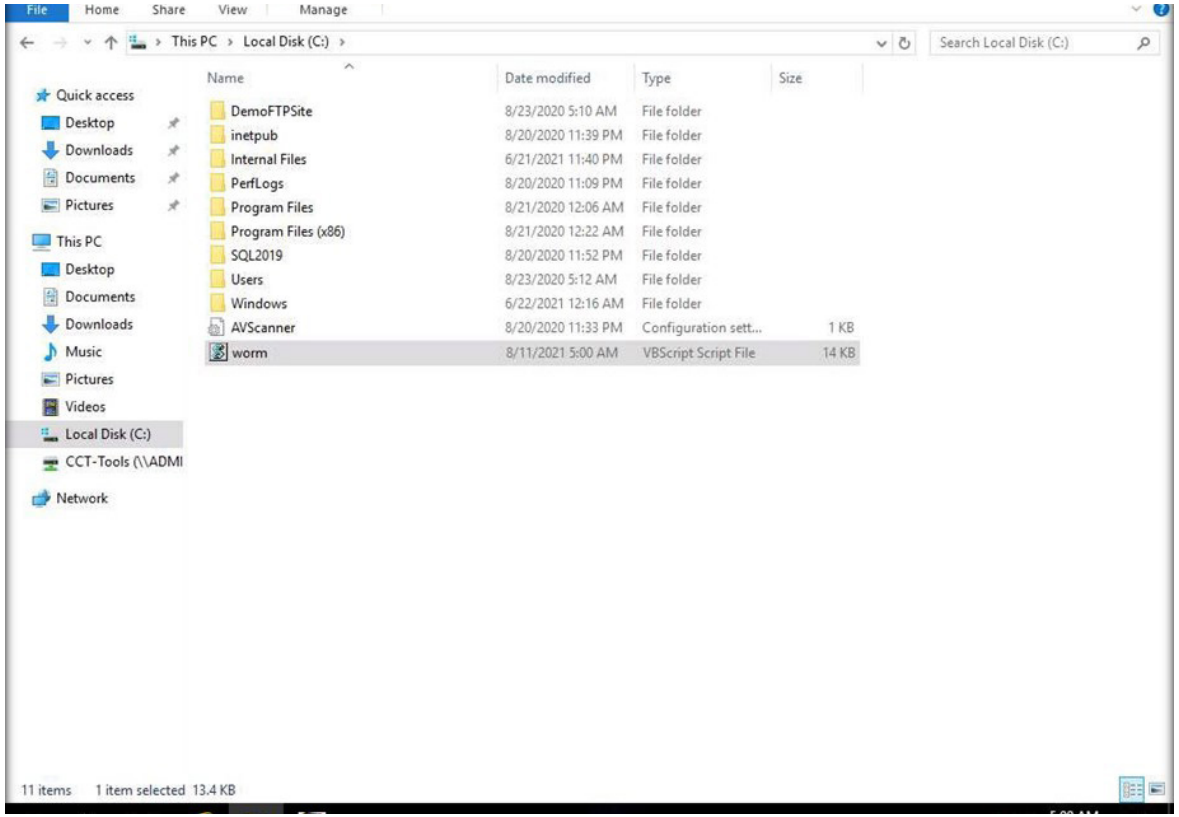
EXERCISE 3:
CREATE A WORM
USING THE
INTERNET WORM
MAKER THING



9. The created worm.vbs file is saved to the output path provided, while configuring Internet Worm Maker Thing. In this lab, the worm is saved to the location C:\.

Note: In this manner, attackers might craft worms using any of the above options and send them to their targets. When the victim runs the worm, the options configured in the worm start acting upon the victim's machine and might also affect its performance.

EXERCISE 3: CREATE A WORM USING THE INTERNET WORM MAKER THING



10. On completion of the lab, close all the windows.
11. Turn off the Web Server virtual machine.

EXERCISE 3: CREATE A WORM USING THE INTERNET WORM MAKER THING

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

Spytech SpyAgent is a powerful computer spy software that allows monitoring all user activity on a computer—in complete stealth mode.

LAB SCENARIO

Spyware is stealthy computer monitoring software that allows you to secretly record all the user activities on a target computer. It automatically delivers logs to the remote attacker using the Internet (via email, FTP, command and control through encrypted traffic, HTTP, DNS, etc.). The delivery logs include information about all areas of the system, such as emails sent, websites visited, every keystroke (including logins/passwords for Gmail, Facebook, Twitter, LinkedIn, etc.), file operations, and online chat conversations. It also takes screenshots at set intervals, just like a surveillance camera aimed at the computer monitor.

OBJECTIVE

This lab demonstrates how to perform user system monitoring and surveillance using Spytech SpyAgent.

OVERVIEW OF SPYTECH SPYAGENT

SpyAgent provides a large array of essential computer monitoring features as well as website, application, and chat-client blocking, lockdown scheduling, and the remote delivery of logs via email or File Transfer Protocol (FTP).

Note: Here, we will use AD Domain Controller as the host machine and Web Server as the target machine. We will first establish a remote connection with the target machine and later install the keylogger spyware (Here, Spyware SpyAgent) to capture keystrokes and monitor the other activities of the user.

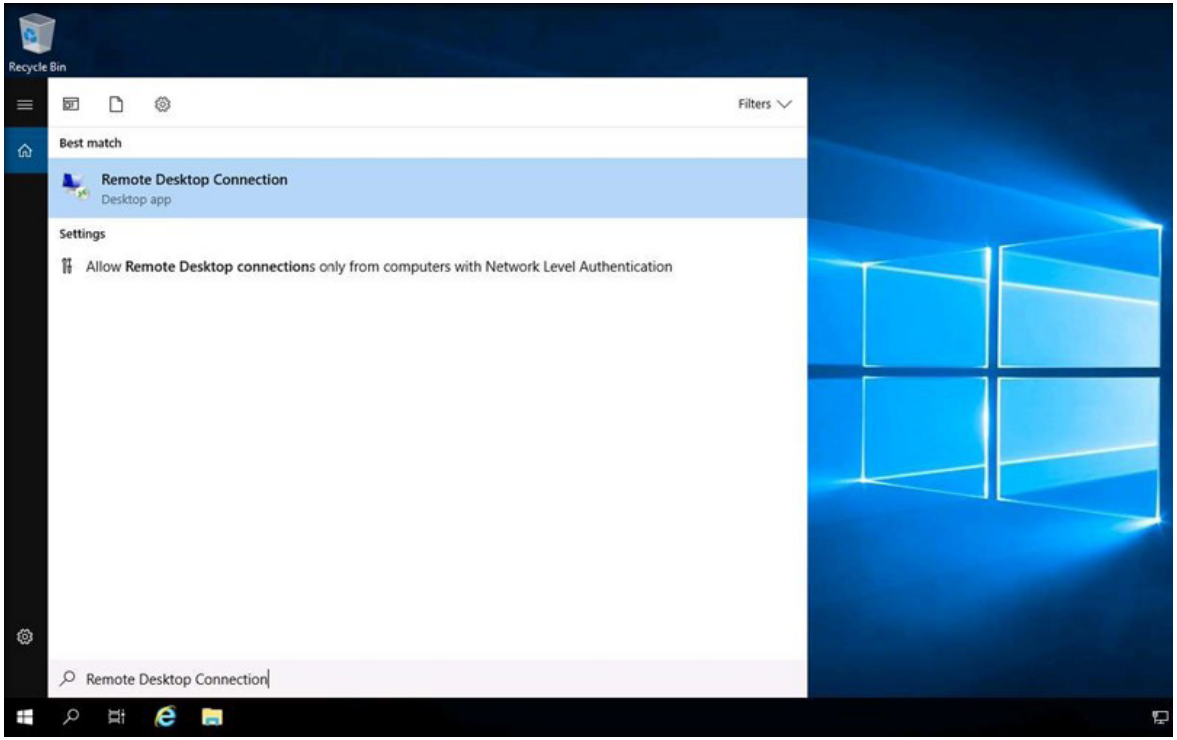
Note: Ensure that PfSense Firewall virtual machine is running.

1. Turn on the AD Domain Controller and Web Server virtual machines.
2. In the AD Domain Controller virtual machine, log in with the credentials CCT\Administrator and admin@123.

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

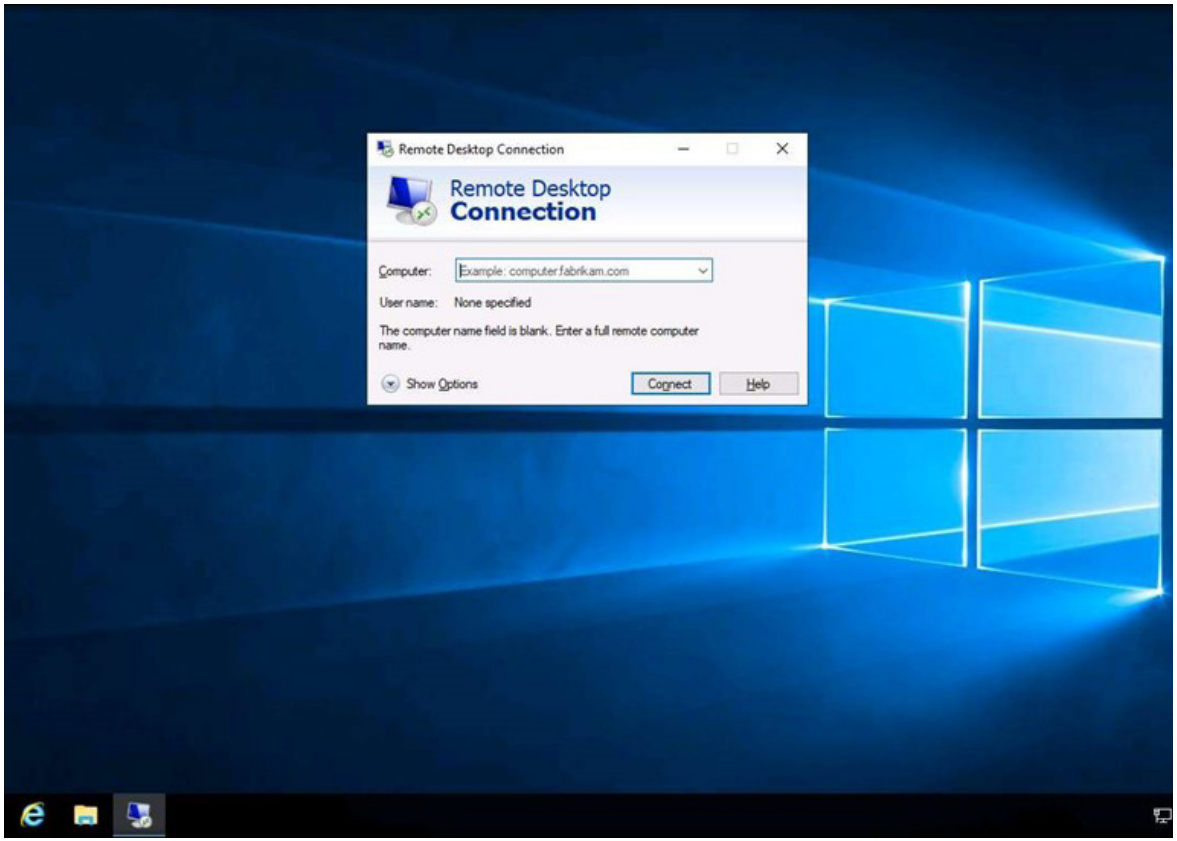
3. Click the Type here to search icon at the bottom of the Desktop and type Remote Desktop Connection. Click Remote Desktop Connection from the results.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



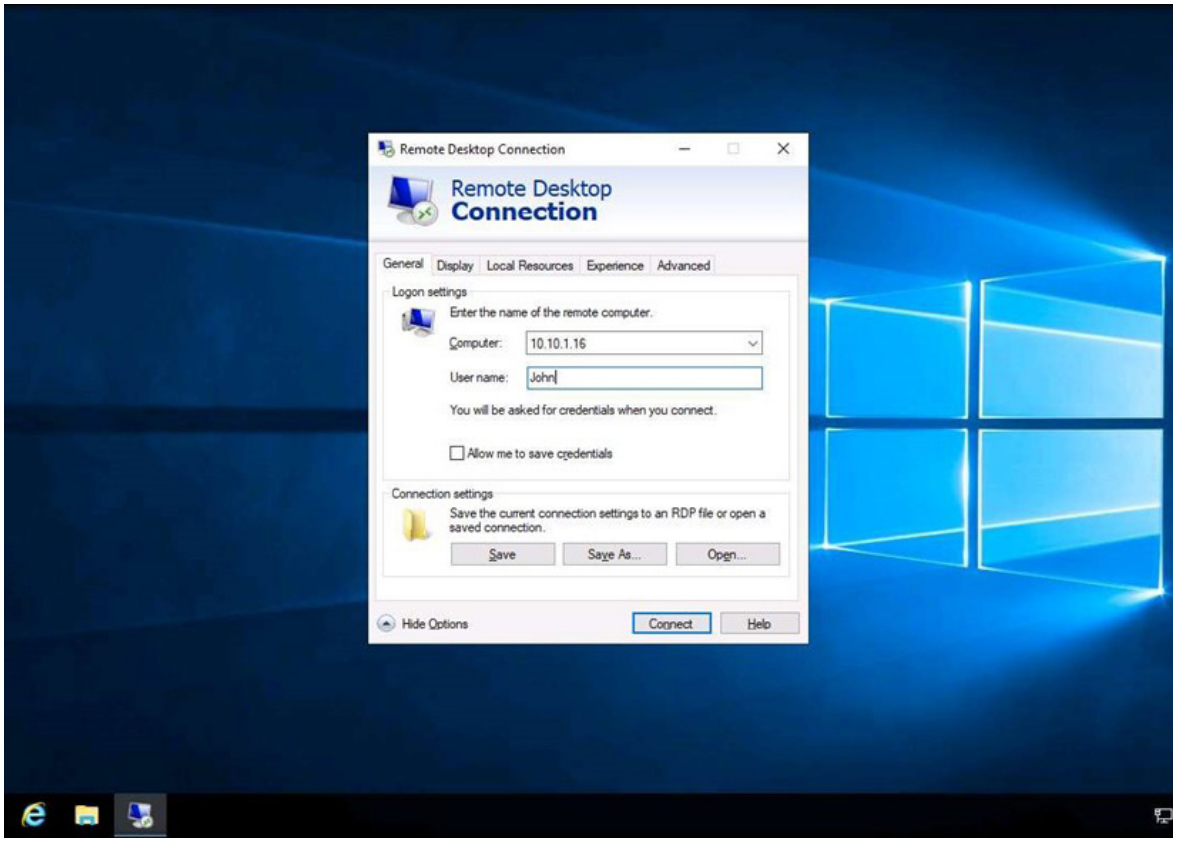
4. The Remote Desktop Connection window appears. Click on Show Options.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



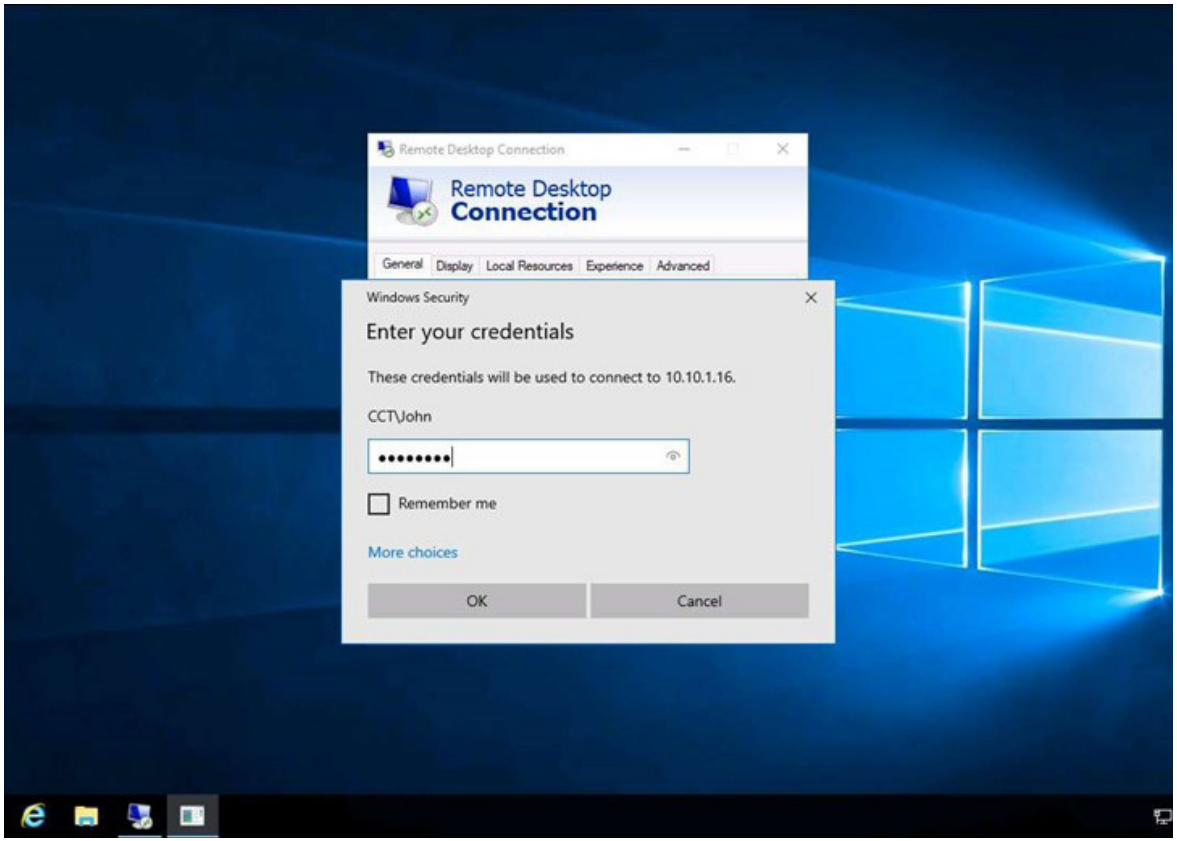
5. In the next window under the Computer field, type the target system's IP address (here, 10.10.1.16 [IP address of Web Server]) and in the User name field enter John and click Connect.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



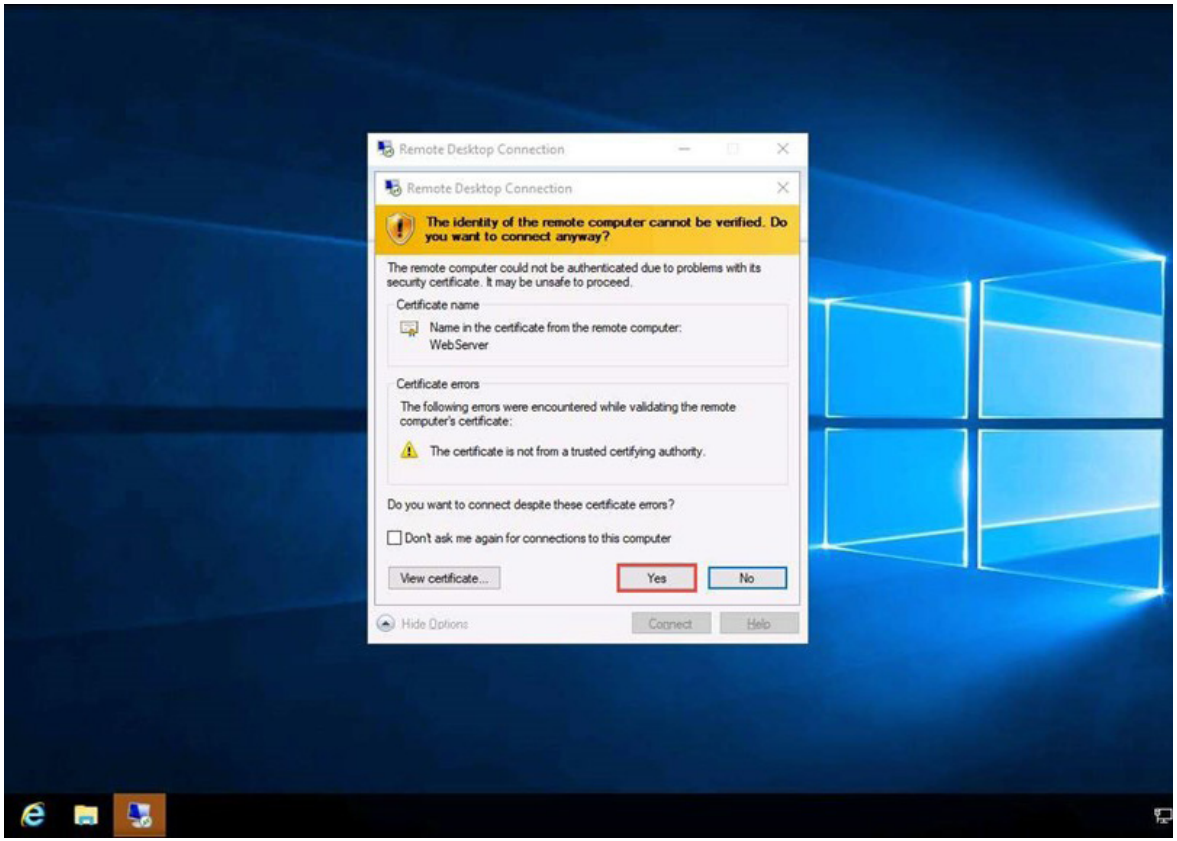
6. The Windows Security pop-up appears. Enter user@123 as the Password and click OK.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



7. A Remote Desktop Connection window appears. Click Yes.

EXERCISE 4:
USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



Note: The target machine cannot be accessed remotely if it is off. Access is possible only when the machine is turned on.

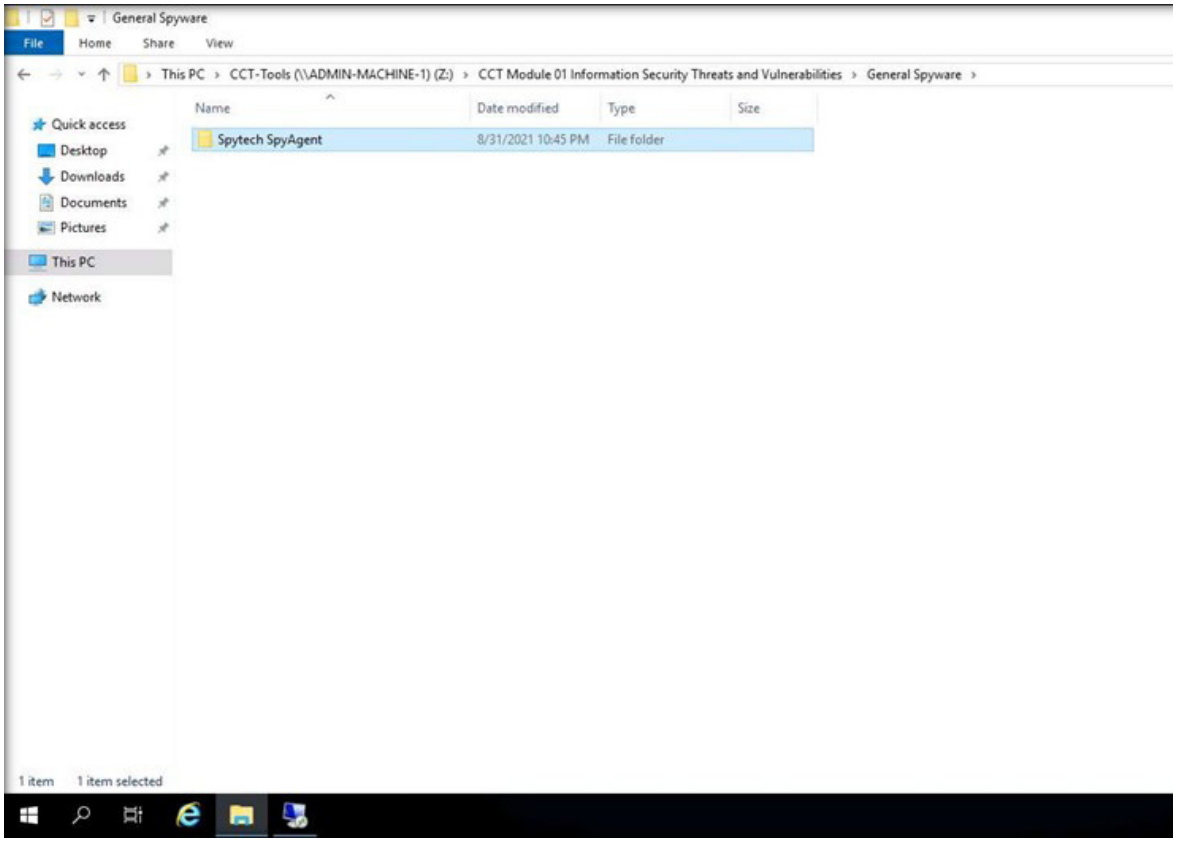
8. A Remote Desktop Connection is successfully established.

Note: If a Server Manager window appears, close it.

9. Minimize Remote Desktop Connection.

10. Navigate to Z:\CCT Module 01 Information Security Threats and Vulnerabilities\General Spyware and copy the Spytech SpyAgent folder.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



11. Switch to the Remote Desktop Connection window and paste the Spytech SpyAgent folder on target system's Desktop, as shown in the screenshot below.

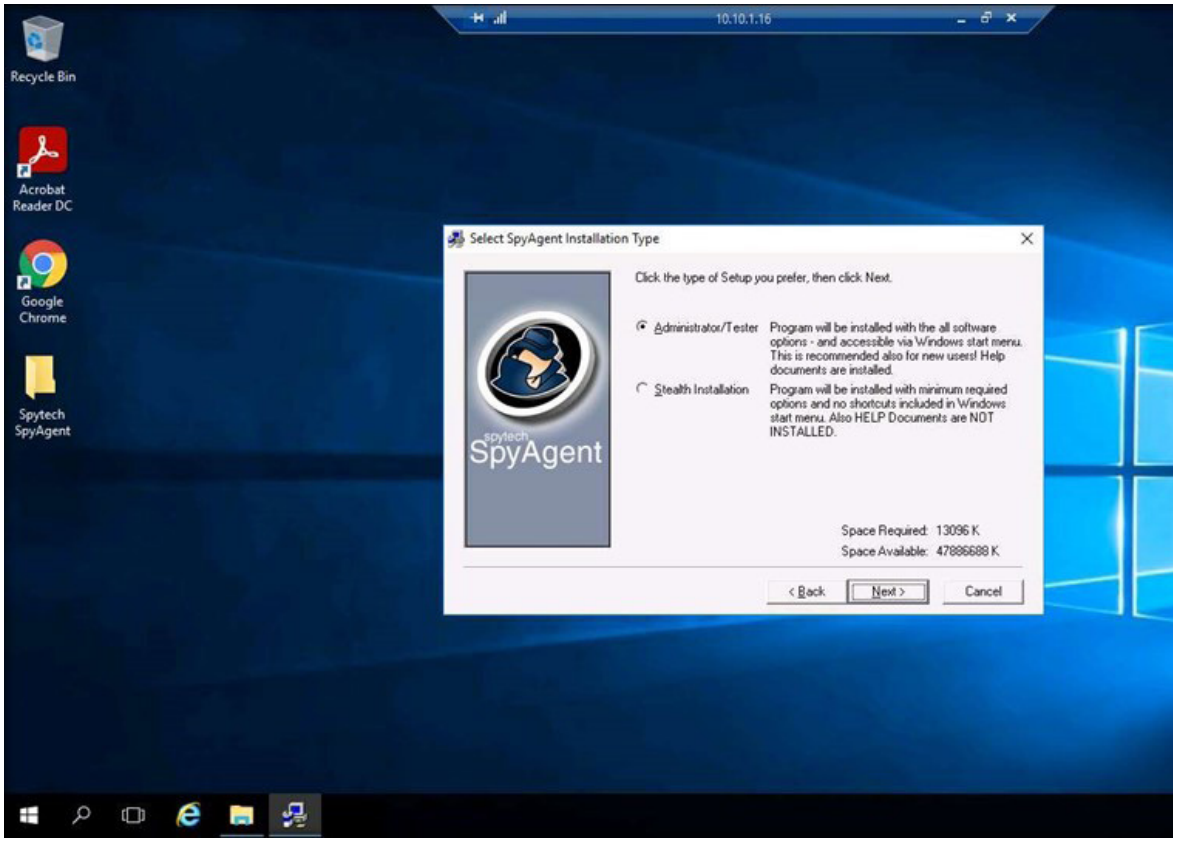
EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

12. Open the Spytech SpyAgent folder and double-click the Setup (password=spytech) application.
Note: If a User Account Control pop-up appears, enter the password for Administrator (admin@123).
13. The Spytech SpyAgent Setup window appears; click Next. Follow the installation wizard and install Spytech SpyAgent using the default settings.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

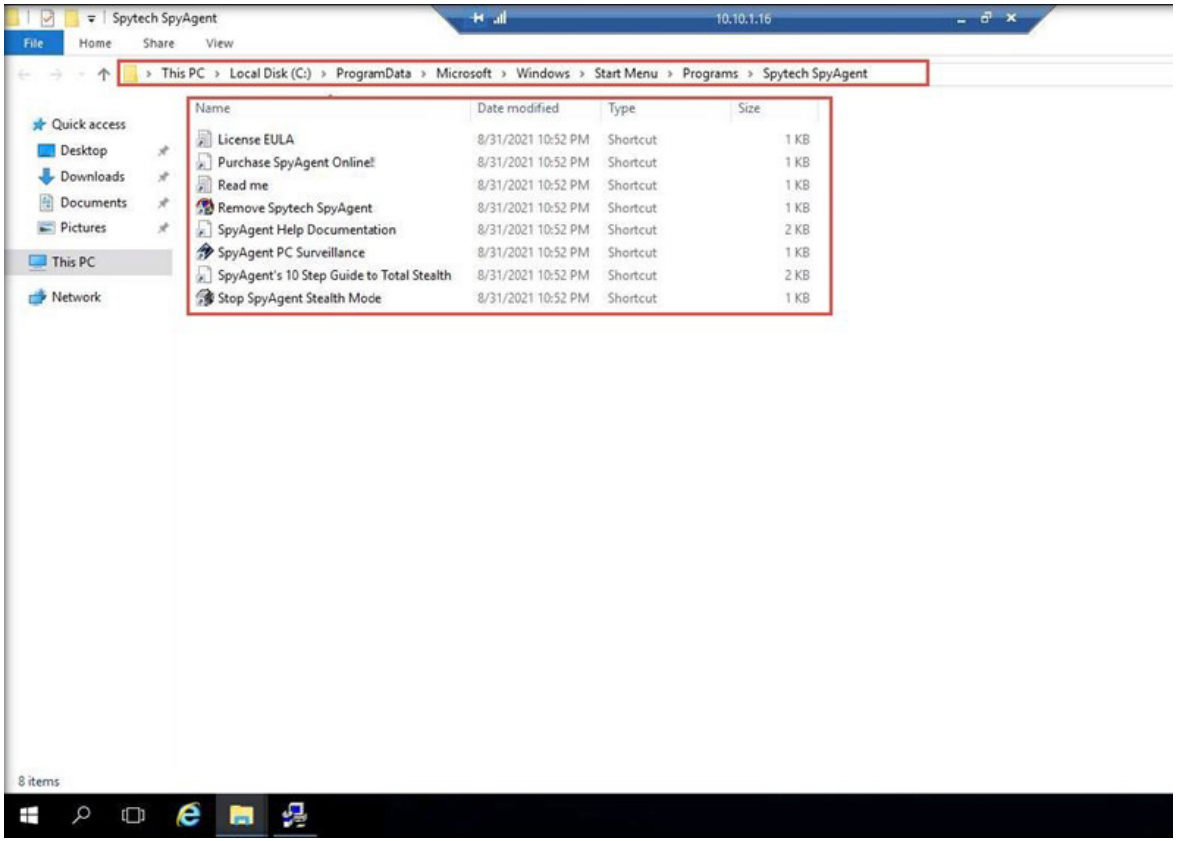
14. In the Select SpyAgent Installation Type window, ensure that the Administrator/Tester radio button is selected. Click Next.

EXERCISE 4:
USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



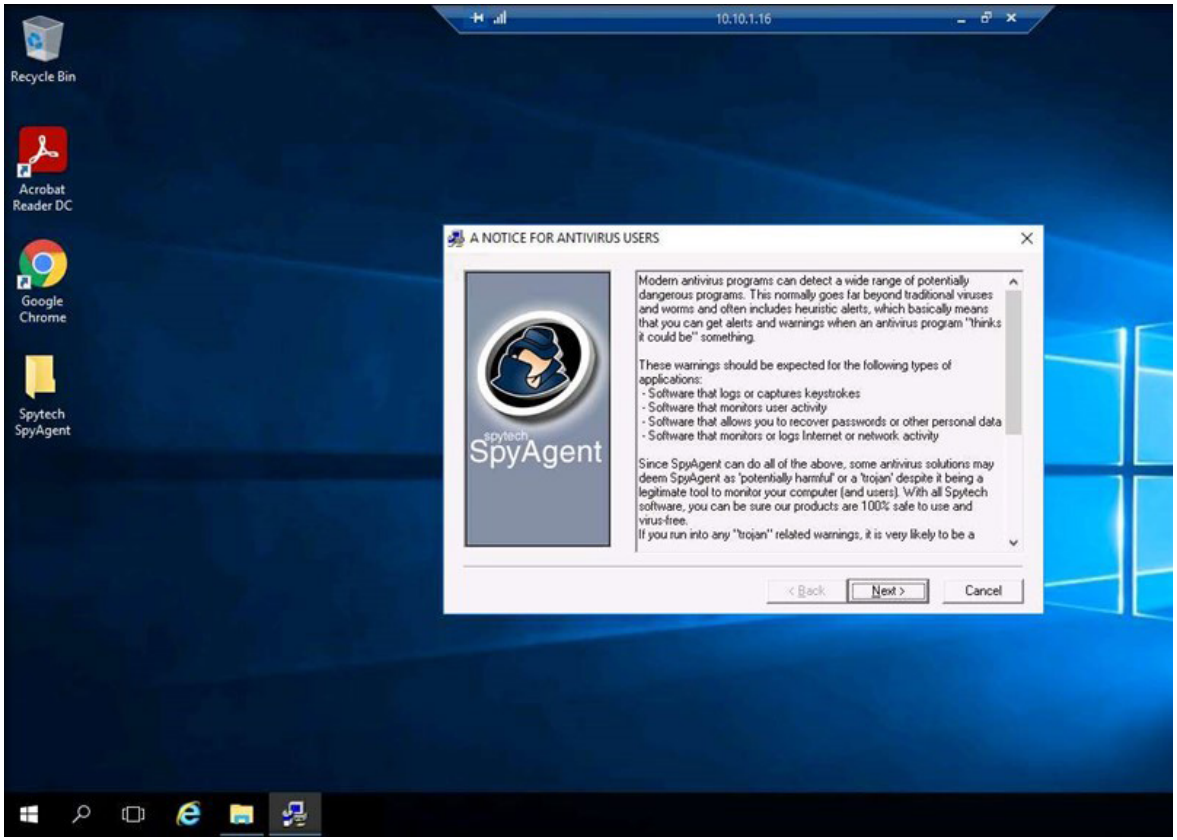
15. In the Ready To Install window, click Next.
16. The Spytech SpyAgent Setup pop-up appears, asking Would you like to include an uninstaller?. Click Yes.
17. A File Explorer windows appears, showing the Spytech SpyAgent folder location. Close the window.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



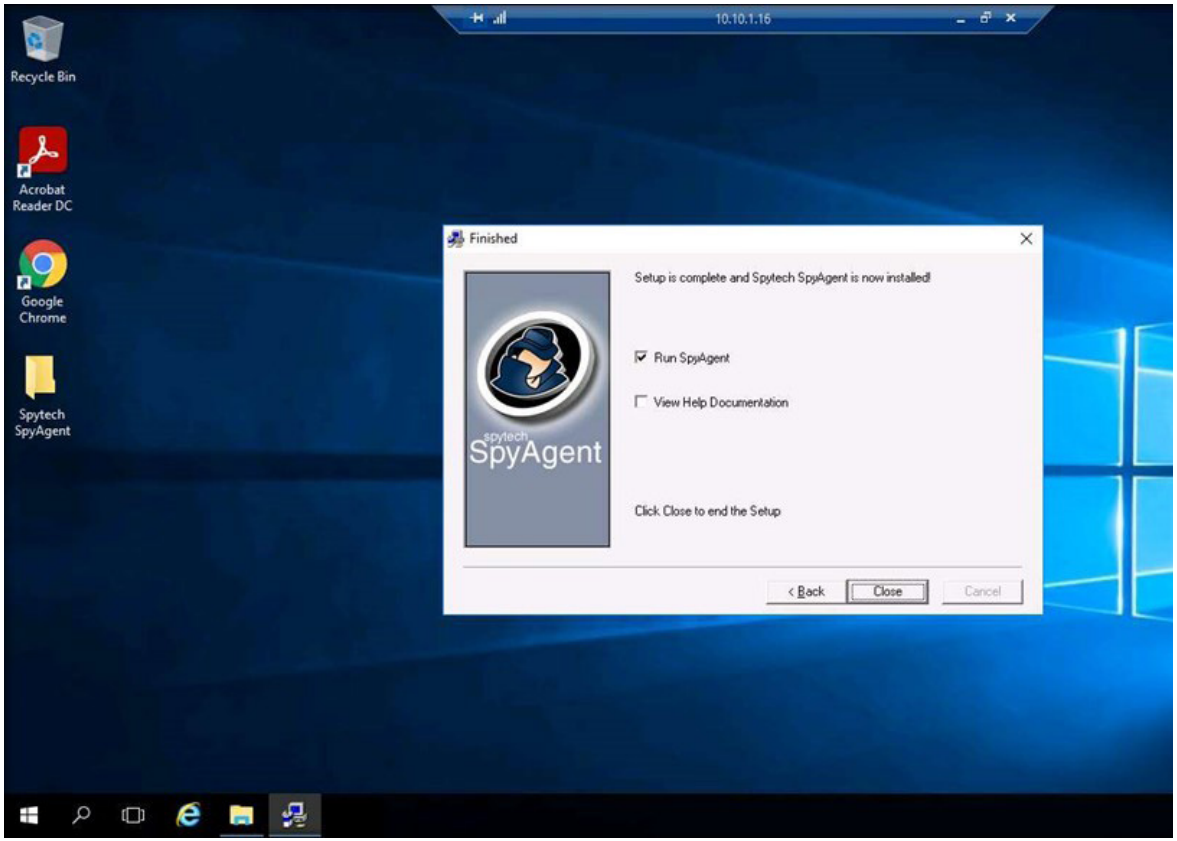
18. In the A NOTICE FOR ANTIVIRUS USERS window; read the notice and click Next.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



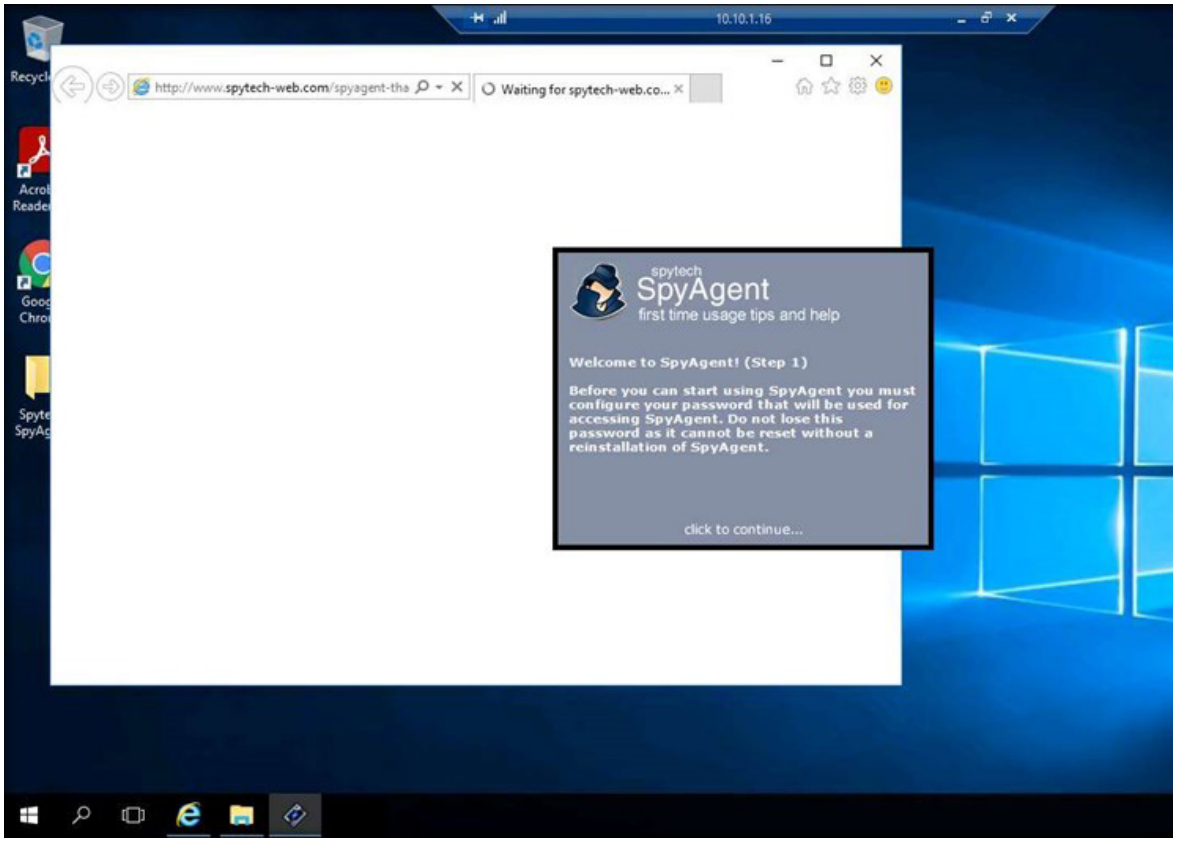
19. The Finished window appears. Ensure that the Run SpyAgent checkbox is selected and click Close.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



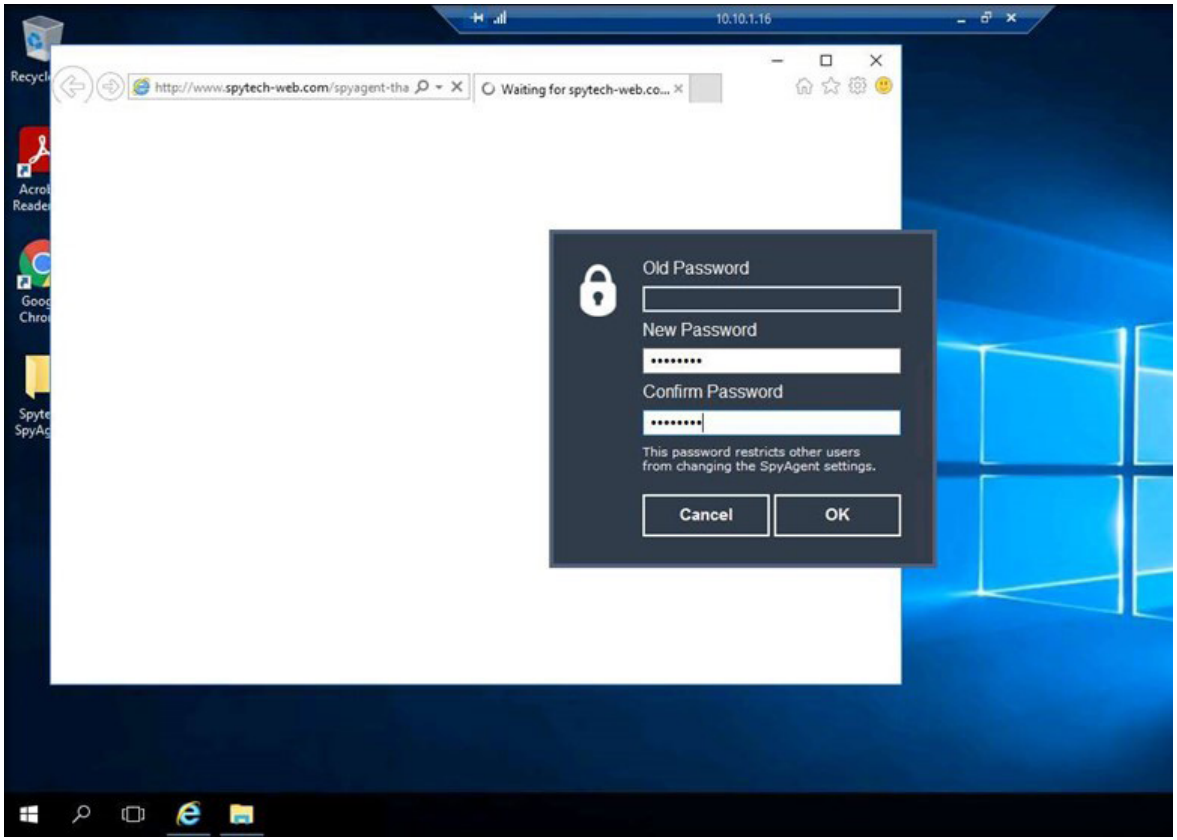
20. The Spytech SpyAgent dialog box appears. Click Continue....
21. The Welcome to SpyAgent! (Step 1) wizard appears. Click click to continue....

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



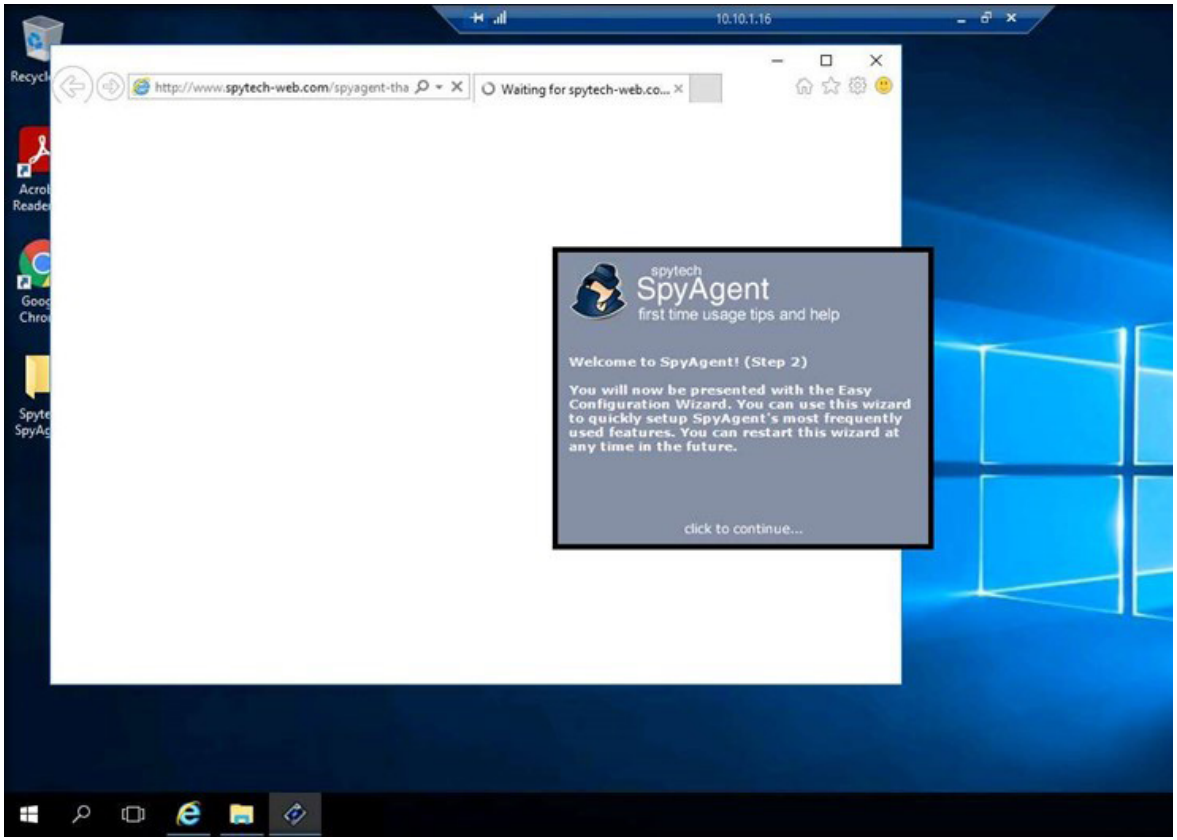
22. Enter the password test@123 in the New Password and Confirm Password fields; click OK.
Note: You can set the password of your choice.

EXERCISE 4:
USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



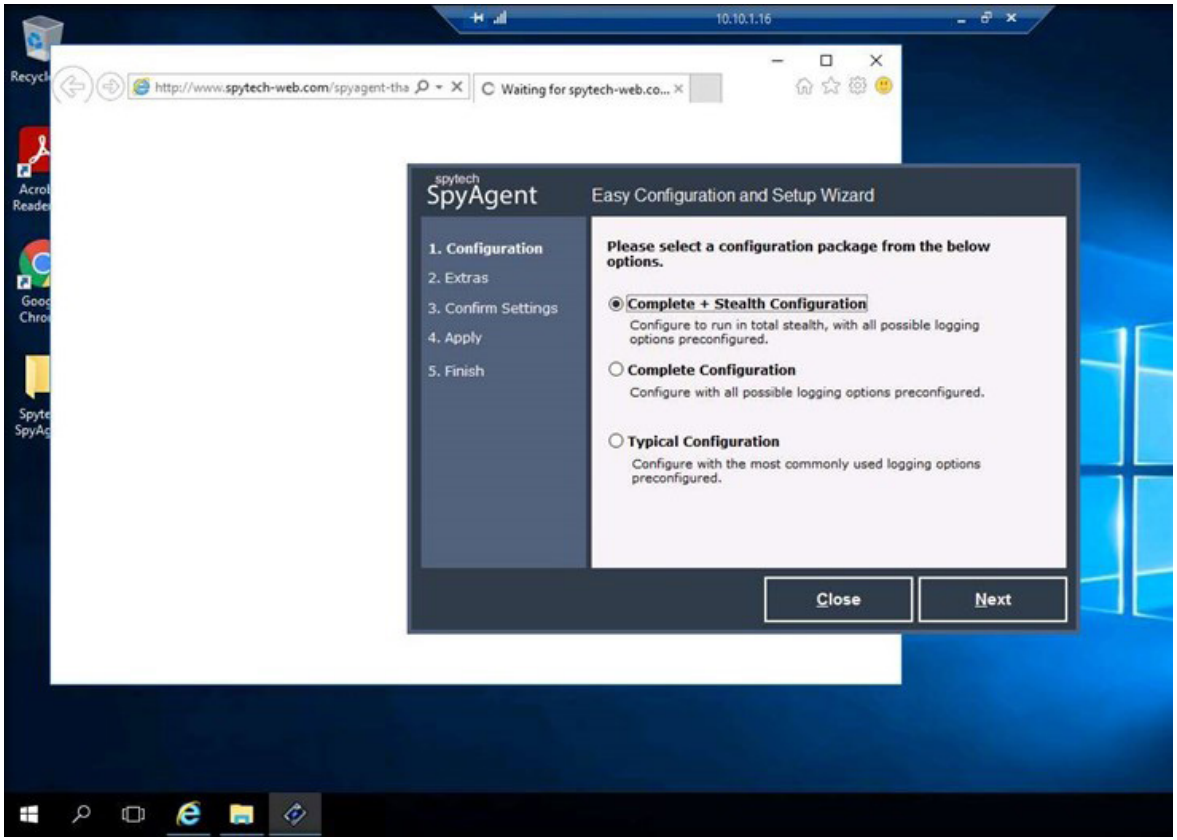
23. The password changed pop-up appears. Click OK.
24. The Welcome to SpyAgent! (Step 2) wizard appears. Click click to continue....

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



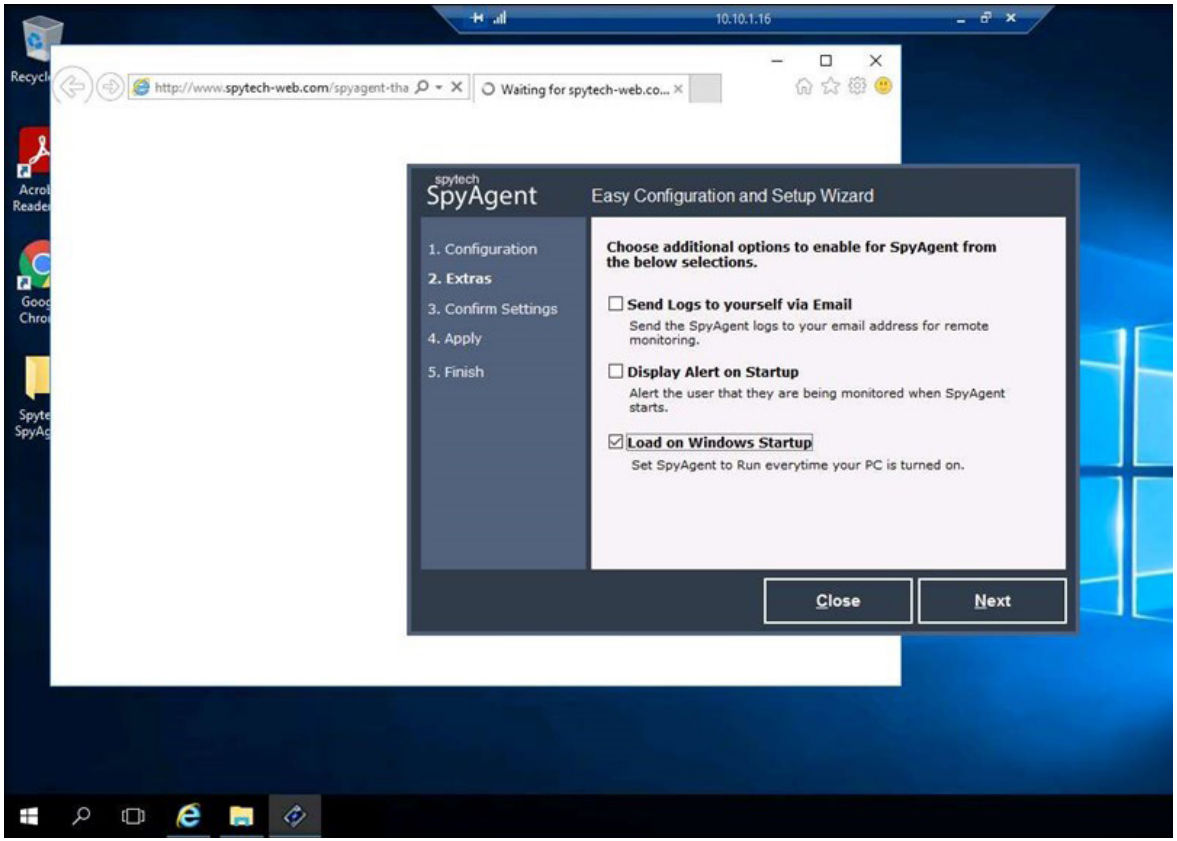
25. The Easy Configuration and Setup Wizard appears. In the Configuration section, ensure that the Complete + Stealth Configuration radio button is selected and click Next.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



26. In the Extras section, select the Load on Windows Startup checkbox and click Next.

EXERCISE 4:
USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



27. In the Confirm Settings section, click Next to continue.

Note: If the Thank you for downloading SpyAgent! webpage appears, close the browser.

28. In the Apply section, click Next. In the Finish section, click Finish.

29. The spytech SpyAgent main window appears, along with the Welcome to SpyAgent! (Step 3) setup wizard. Click click to continue....

30. If a Getting Started dialog box appears, click No.

31. In the spytech SpyAgent main window, click Start Monitoring in the bottom-left corner.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

32. The Enter Access Password pop-up appears. Enter the password you specified in Step 21 and click OK.
Note: Here, the password is test@123.

EXERCISE 4:
USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

33. The Stealth Notice window appears. Read the instructions carefully, and then click OK.

Note: To bring SpyAgent out of stealth mode, press Ctrl+Shift+Alt+M.

EXERCISE 4:
USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

34. The spytech SpyAgent pop-up appears. Select the Do not show this Help Tip again and Do not show Related Help Tips like this again checkboxes and click click to continue....

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

35. Remove the Spytech SpyAgent folder from Desktop.
36. Close Remote Desktop Connection by clicking on the close icon (X).

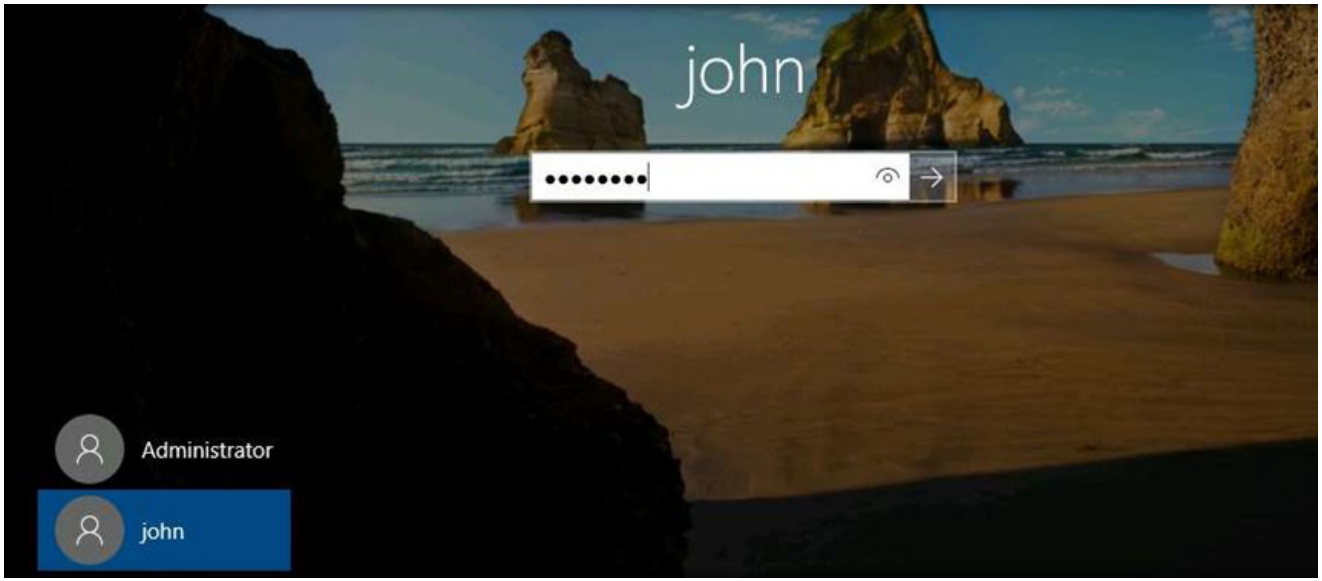
Note: If a Remote Desktop Connection pop-up appears saying Your remote session will be disconnected, click OK.

37. Switch to the Web Server virtual machine. Click John from the left-pane and log in with the password user@123.

Note: Here, we are running the target machine as a legitimate user.

Note: If a Server Manager window appears close it.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

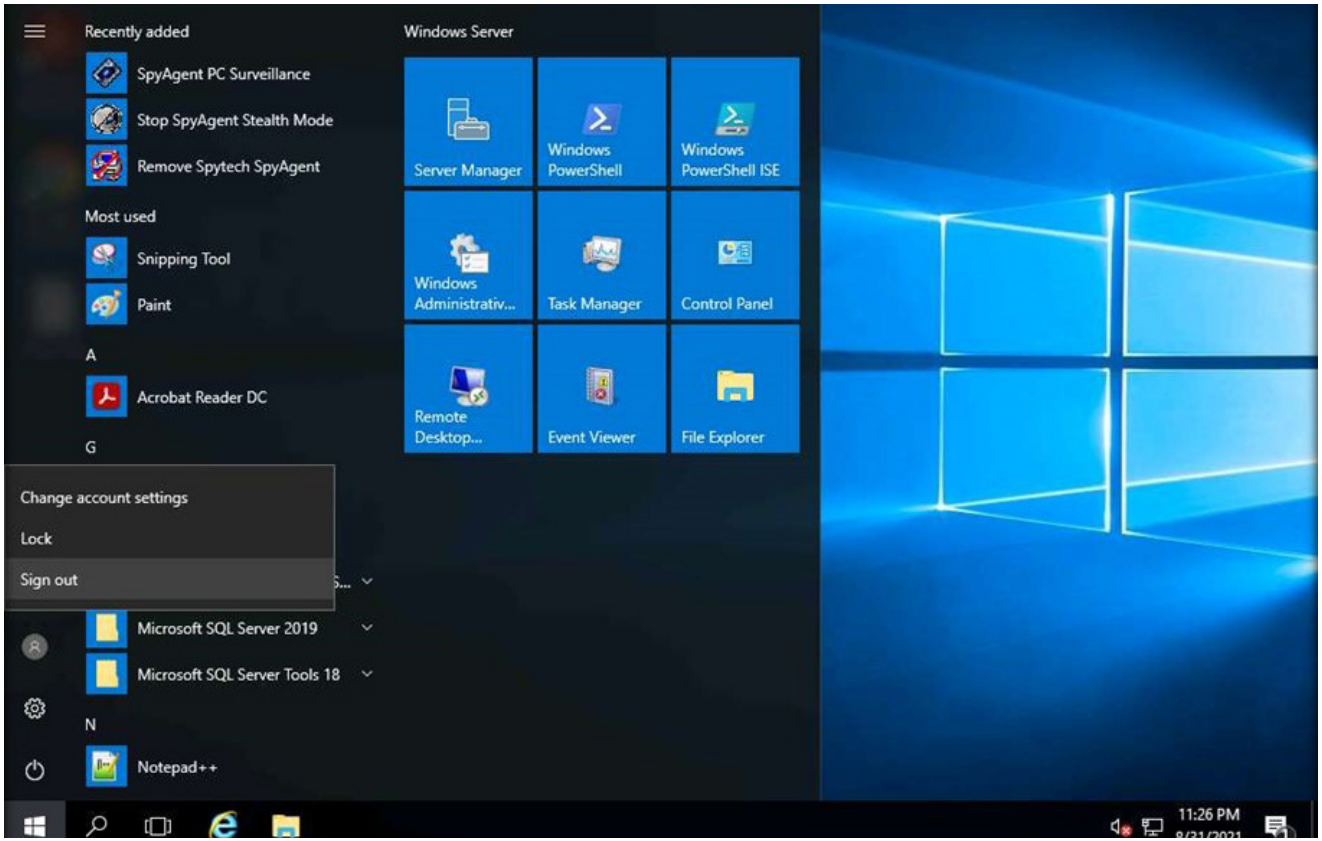


38. Open the Google Chrome web browser and browse any website.

Note: In this lab, we are browsing the Gmail website and creating a Notepad file with sensitive information

39. Once you have performed some user activities, close all windows. Click the Start icon from the bottom left corner of the Desktop, click the user icon, and click Sign out. You will be signed out the account John.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



40. Switch back to the AD Domain Controller. Follow Steps 3 - 6 to launch Remote Desktop Connection.
41. Close the Server Manager window.
Note: If a SpyAgent trial version pop-up appears, click continue....
42. To bring Spytech SpyAgent out of stealth mode, press Ctrl+Shift+Alt+M.
43. The Enter Access Password pop-up appears; enter the password from Step 22 and click OK.
Note: Here, the password is test@123.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

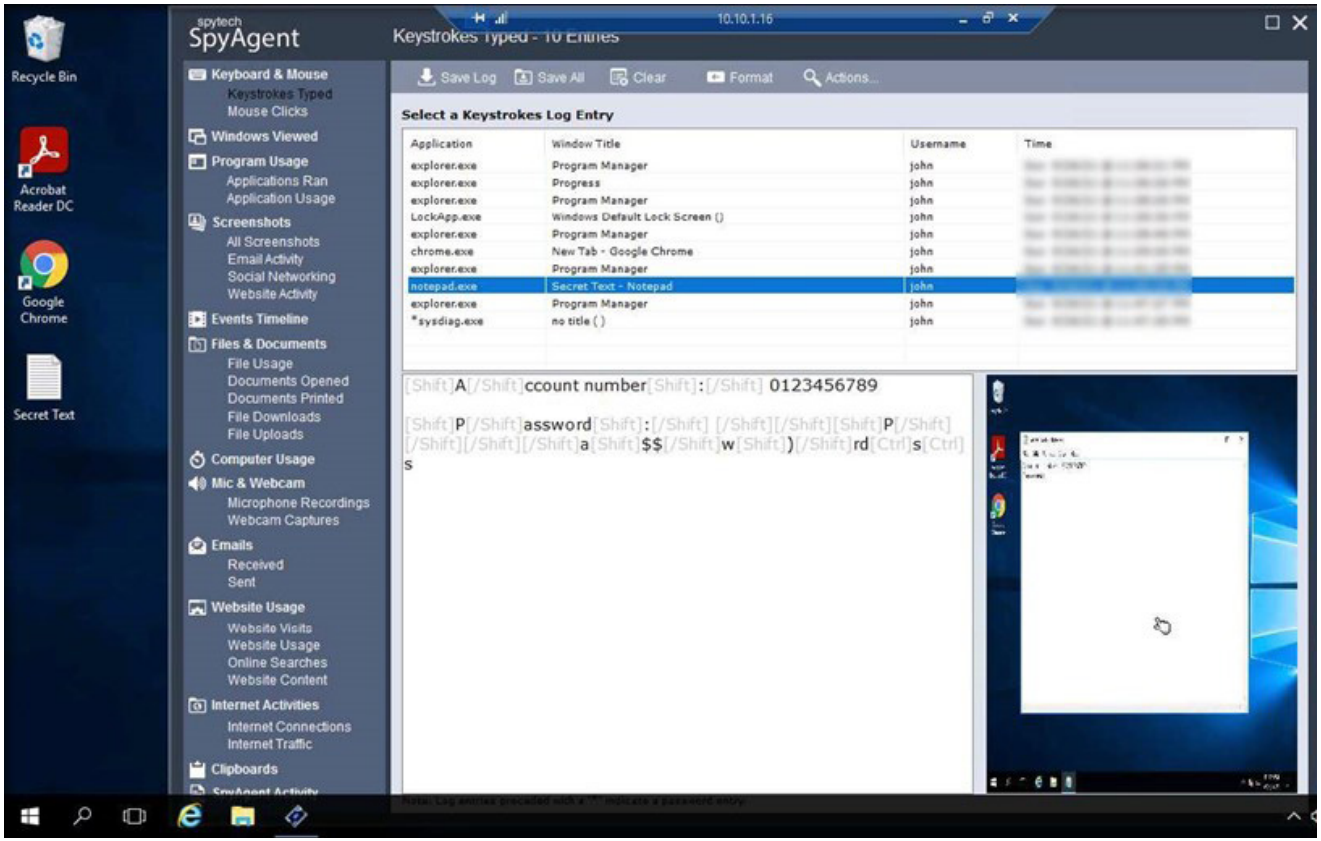
44. The spytech SpyAgent window appears; click KEYBOARD & MOUSE, and then click View Keystrokes Log from the resulting options.

EXERCISE 4:
USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

45. SpyAgent displays all the resultant keystrokes under the Keystrokes Typed section. Click any of the captured keystrokes to view detailed information in the field below.

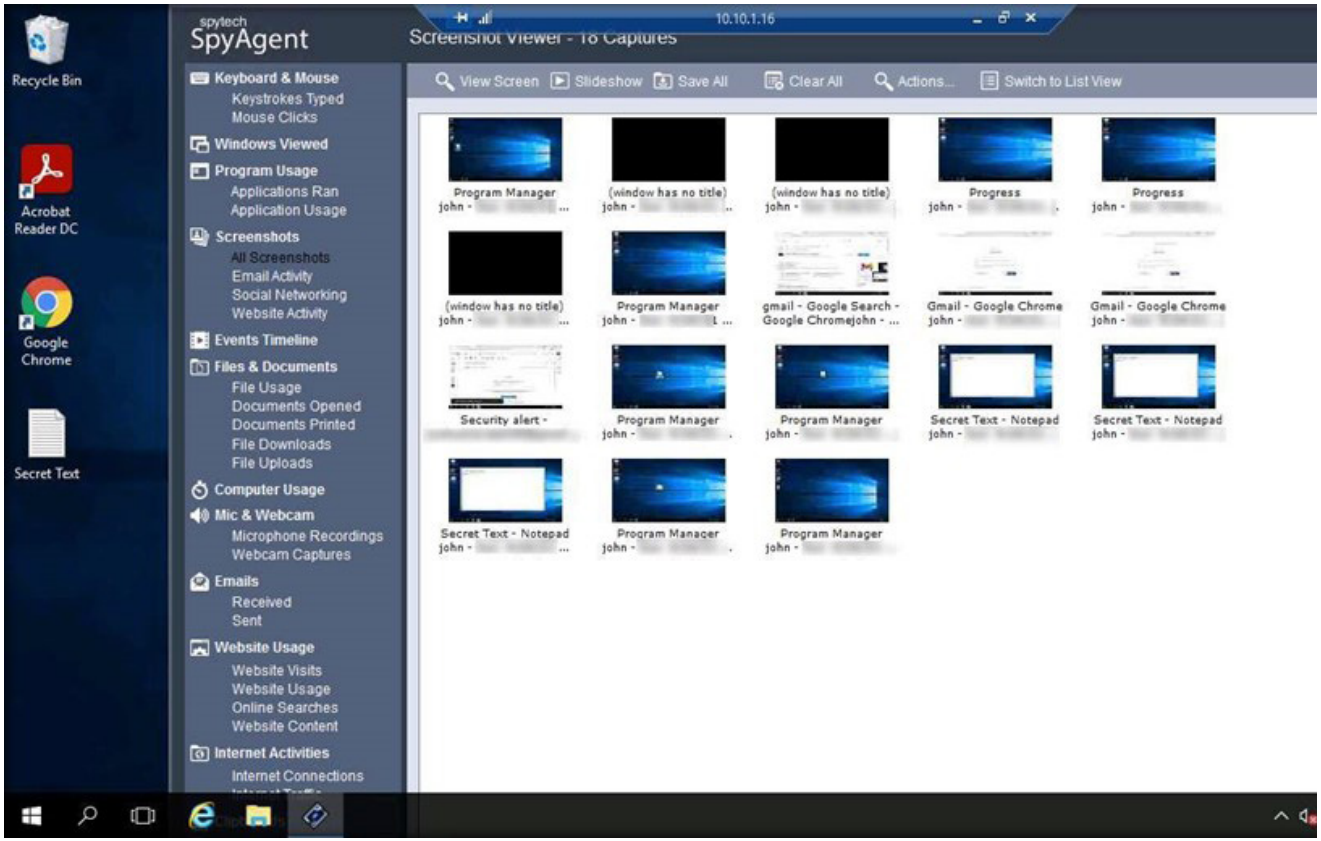
Note: The screenshot here might differ from the image on your screen, depending upon the user activities you performed earlier.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



46. Click the Screenshots option from the left-hand pane to view the captured screenshot of the user activities. Similarly, in Email Activity under the Screenshots options, view the email account accessed by the user on the target system.

EXERCISE 4:
USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

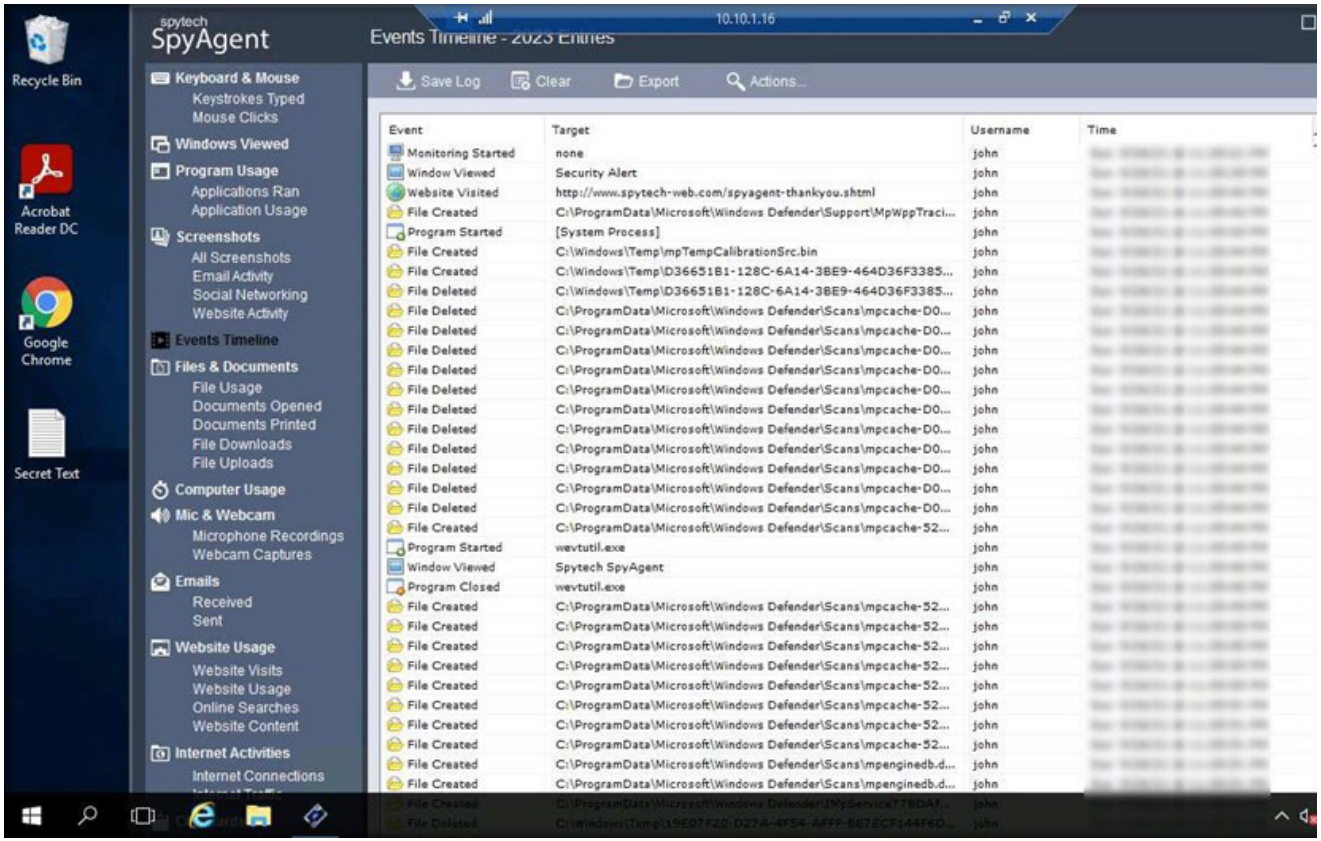


47. Navigate back to the spytech SpyAgent main window. Click Events Timeline.

EXERCISE 4:
USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT

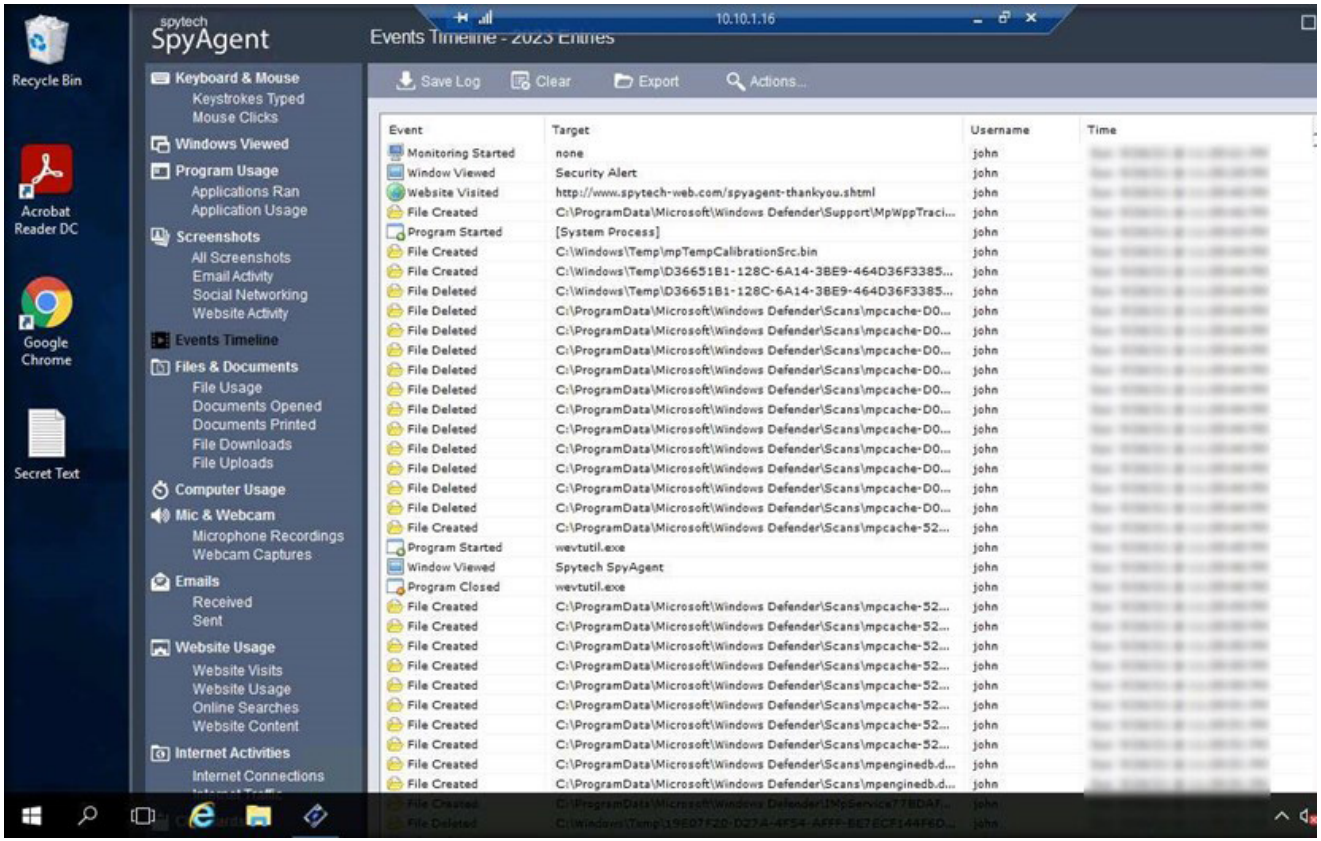
48. SpyAgent displays all the Events as shown in the screenshot below.

EXERCISE 4:
USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



49. Similarly, select each tile and further explore the tool by clicking various options such as Windows Viewed, Program Usage, Website Usage, Files & Documents, Computer Usage, etc.
50. Once you have finished, close all open windows. Close Remote Desktop Connection.
51. This concludes the demonstration of user system monitoring and surveillance using Spytech SpyAgent.
52. Close all open windows and document all the acquired information.
53. Turn off AD Domain Controller and Web Server virtual machines.

EXERCISE 4: USER SYSTEM MONITORING AND SURVEILLANCE USING SPYTECH SPYAGENT



EXERCISE 5: **FIND VULNERABILITIES ON EXPLOIT SITES**

Exploit sites contain details of the latest vulnerabilities of various OSes, devices, and applications.

LAB SCENARIO

Vulnerability research is the process of analyzing protocols, services, and configurations to discover the vulnerabilities and design flaws that will expose an operating system and its applications to exploit, attack, or misuse.
A security professional must have the required knowledge to find vulnerabilities on exploit sites and further mitigate them to enhance the organization's security infrastructure.

OBJECTIVE

This lab demonstrates how to find the vulnerabilities of the target system using various exploit sites such as Exploit DB.

OVERVIEW OF EXPLOIT SITES

Exploit sites can be used to find relevant vulnerabilities about the target system based on the information gathered, the exploits from the database and exploitation tools such as Metasploit can be used, to gain remote access.

Note: Ensure that PfSense Firewall virtual machine is running.

1. Turn on the Admin Machine-1 virtual machine.
2. Log in with the credentials Admin and admin@123.

Note: If the Welcome to Windows wizard appears, click Continue. In the Sign in with Microsoft wizard, click Cancel.

Note: The Networks screen appears. Click Yes to allow the PC to be discoverable by other PCs and devices on the network.

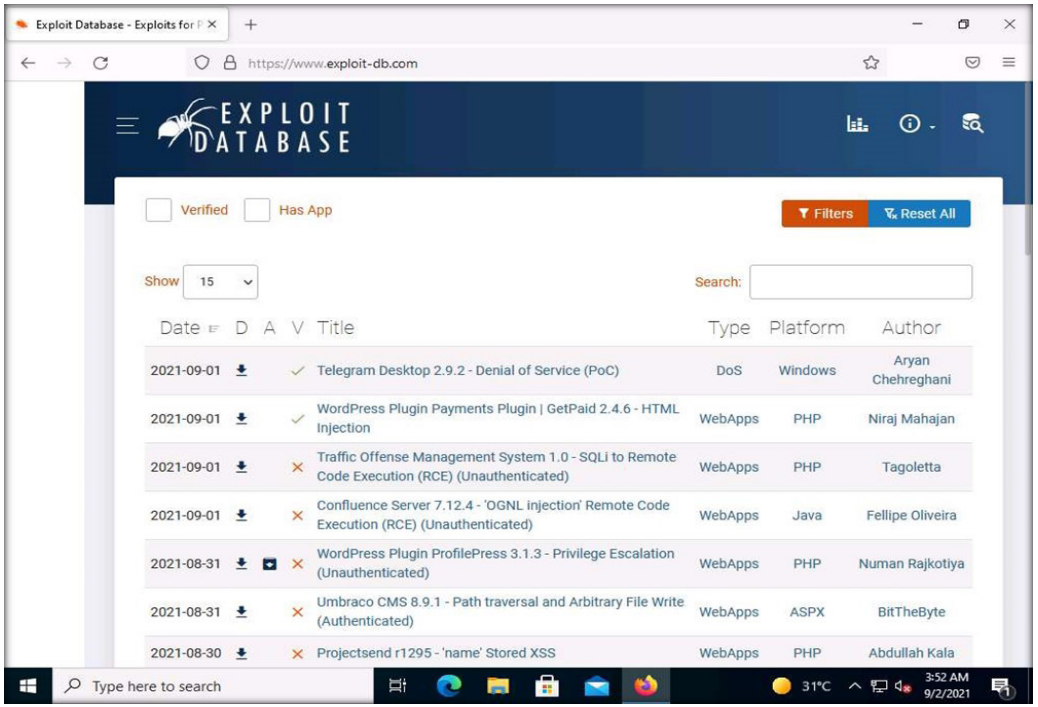
3. Open any web browser (here, Mozilla Firefox). Place your mouse cursor in the address bar of the browser, type https://www.exploit-db.com/ and press Enter.

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

4. The Exploit Database website appears. Click any of the latest vulnerabilities to view detailed information, or search for a specific vulnerability by entering its name in the Search field.

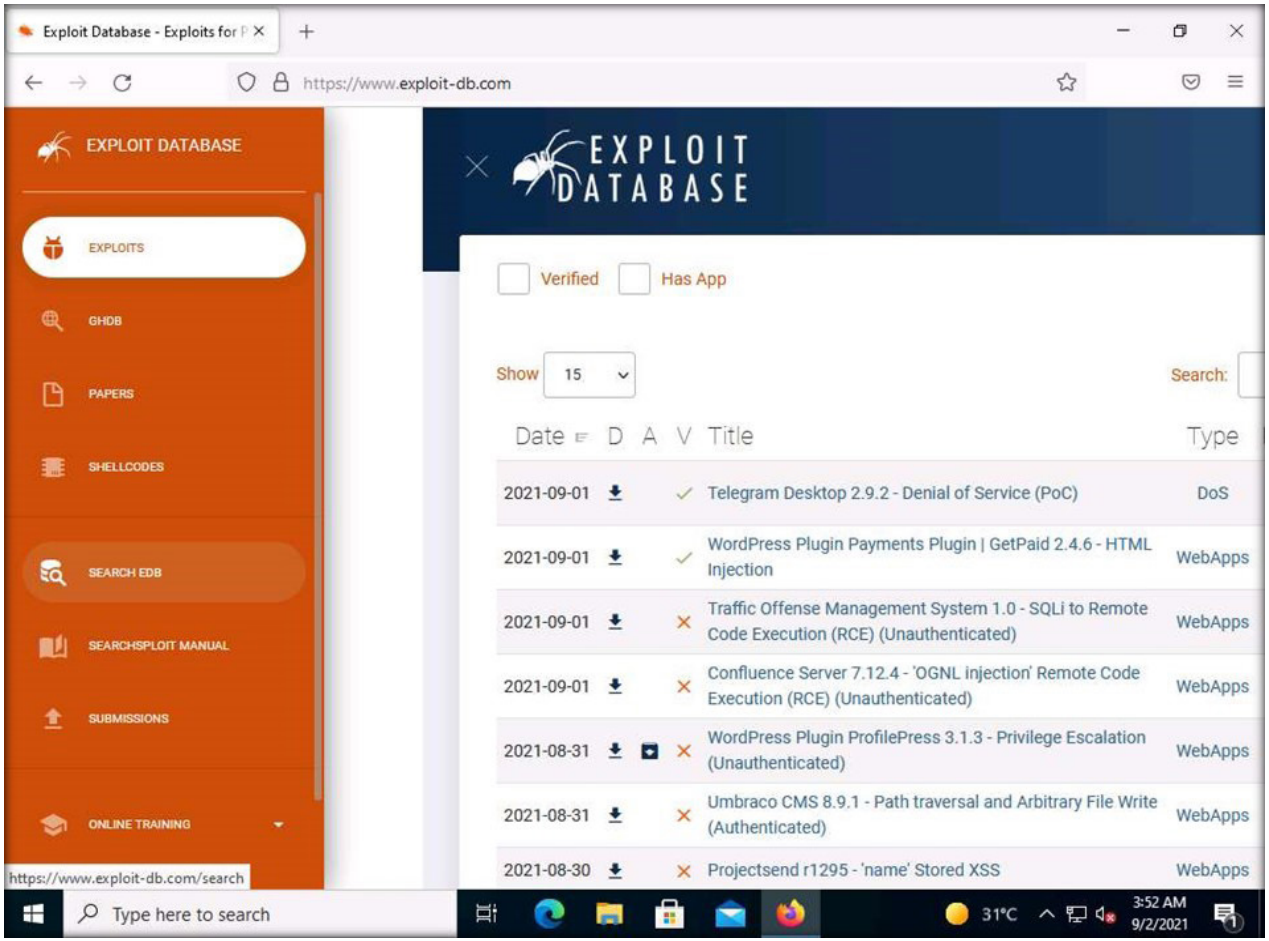
Note: If a This website uses cookie pop-up appears at the bottom, click Allow all cookies.

EXERCISE 5: FIND VULNERABILITIES ON EXPLOIT SITES



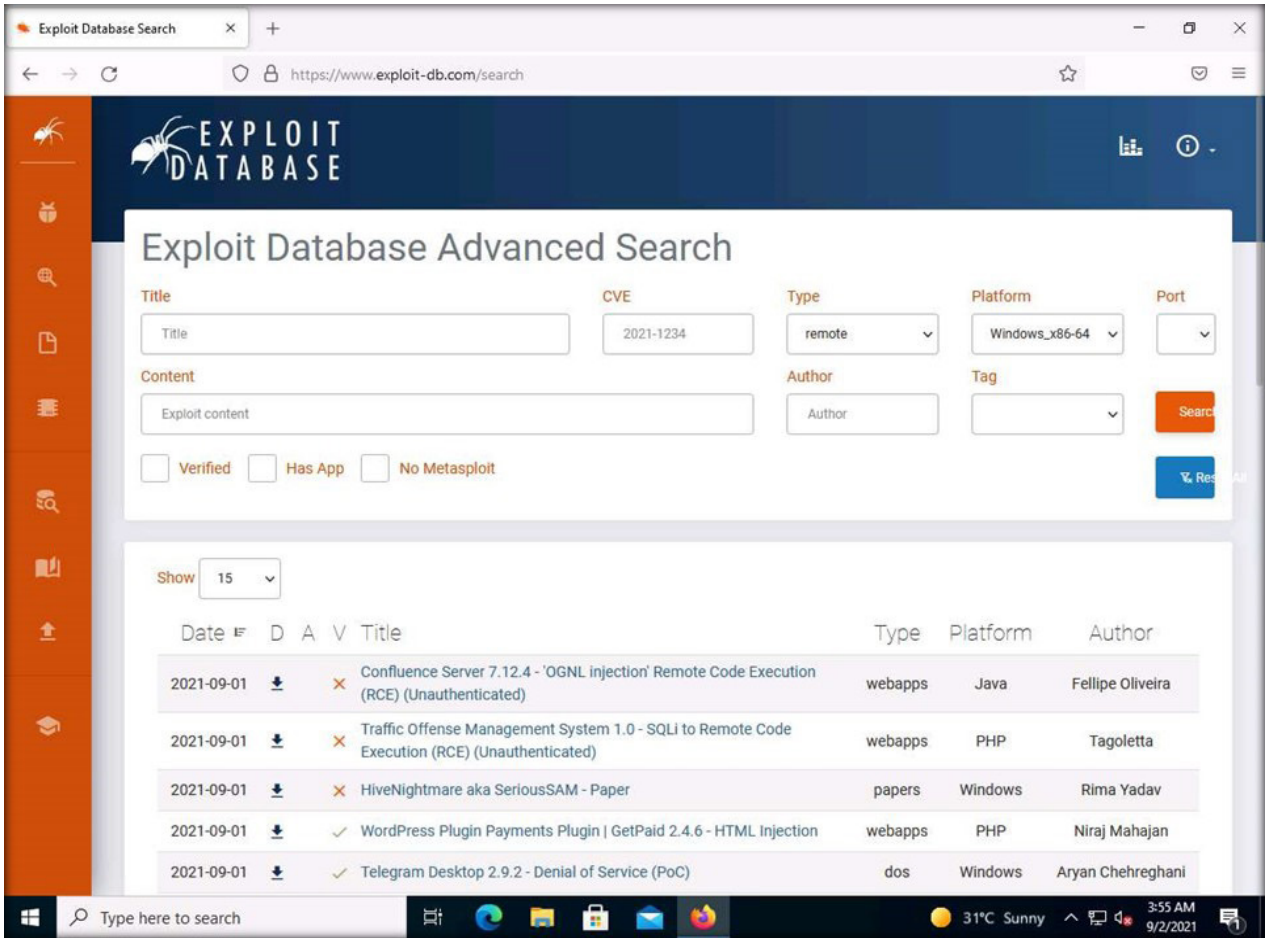
5. Move the mouse cursor to the left-pane of the website and select the SEARCH EDB option from the list to perform an advanced search.

EXERCISE 5:
FIND VULNERABILITIES ON EXPLOIT SITES



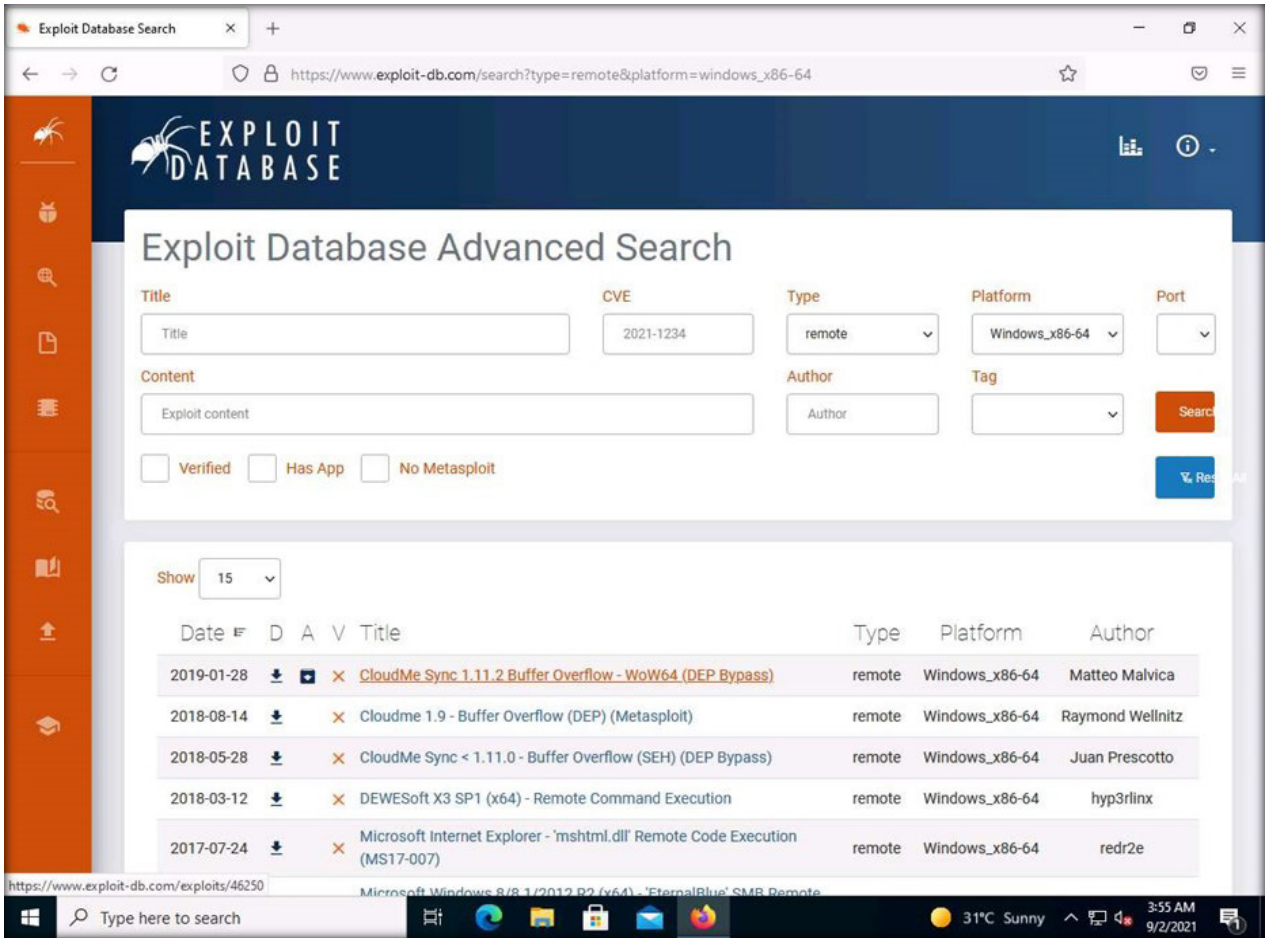
6. The Exploit Database Advanced Search page appears. In the Type field, select any type from the drop-down list (here, remote). Similarly, in the Platform field, select any OS (here, Windows_x86-64). Click Search.
Note: Here, you can perform an advanced search by selecting various search filters to find a specific vulnerability.

EXERCISE 5:
FIND VULNERABILITIES ON EXPLOIT SITES



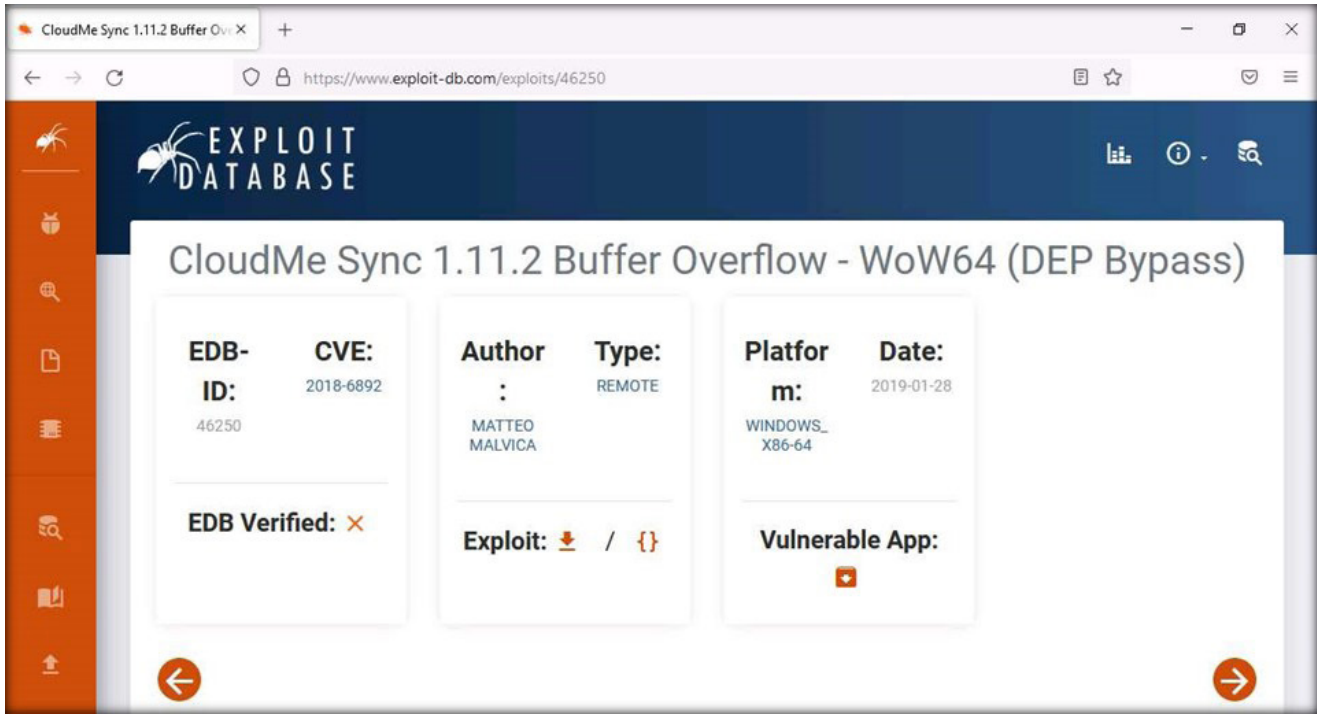
7. Scroll down to view the result, which displays a list of vulnerabilities, as shown in the screenshot.
8. You can click on any vulnerability to view its detailed information (here, CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass).

EXERCISE 5: FIND VULNERABILITIES ON EXPLOIT SITES



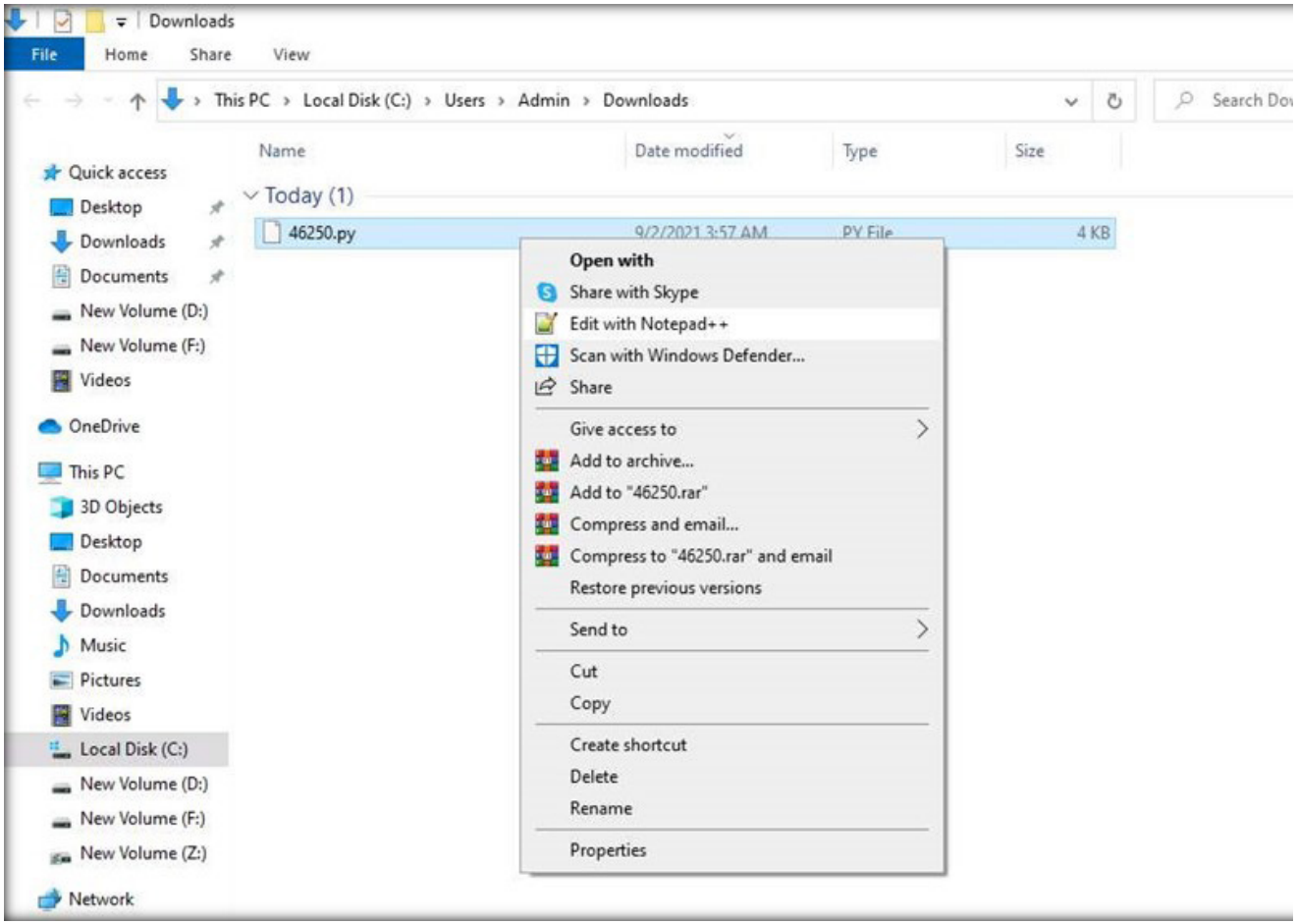
9. Detailed information is displayed regarding the selected vulnerability such as EDB-ID, CVE, author, type, platform, and published date, as shown in the screenshot below.
10. Click on the download icon ( ) in the Exploit section to download the exploit code.

EXERCISE 5: FIND VULNERABILITIES ON EXPLOIT SITES



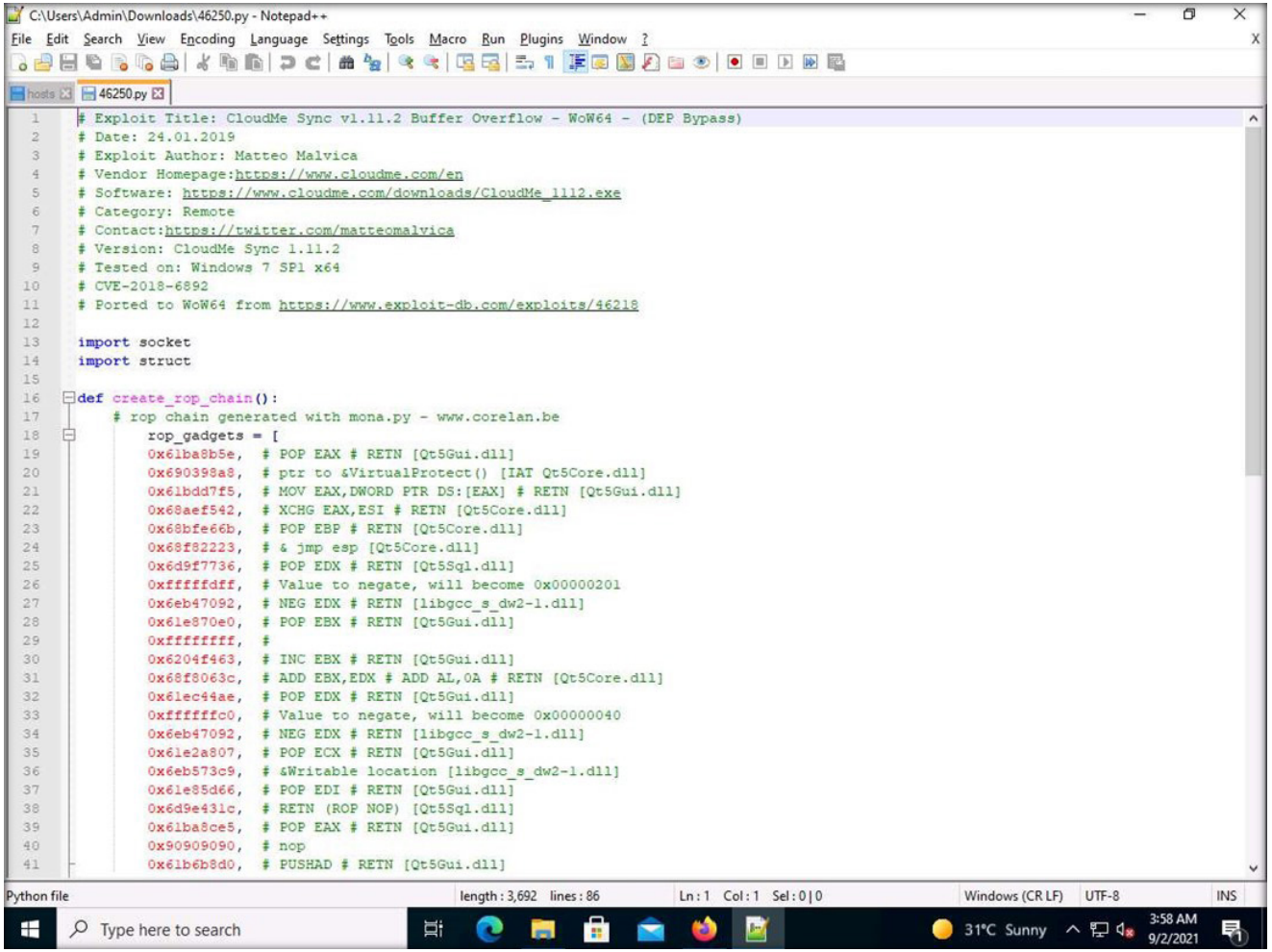
11. The Opening file pop-up appears. Select the Save File radio button and click OK to download the exploit file.
12. Navigate to the downloaded location (here, Downloads), right-click the saved file, and select Edit with Notepad++.

EXERCISE 5:
FIND VULNERABILITIES
ON EXPLOIT SITES



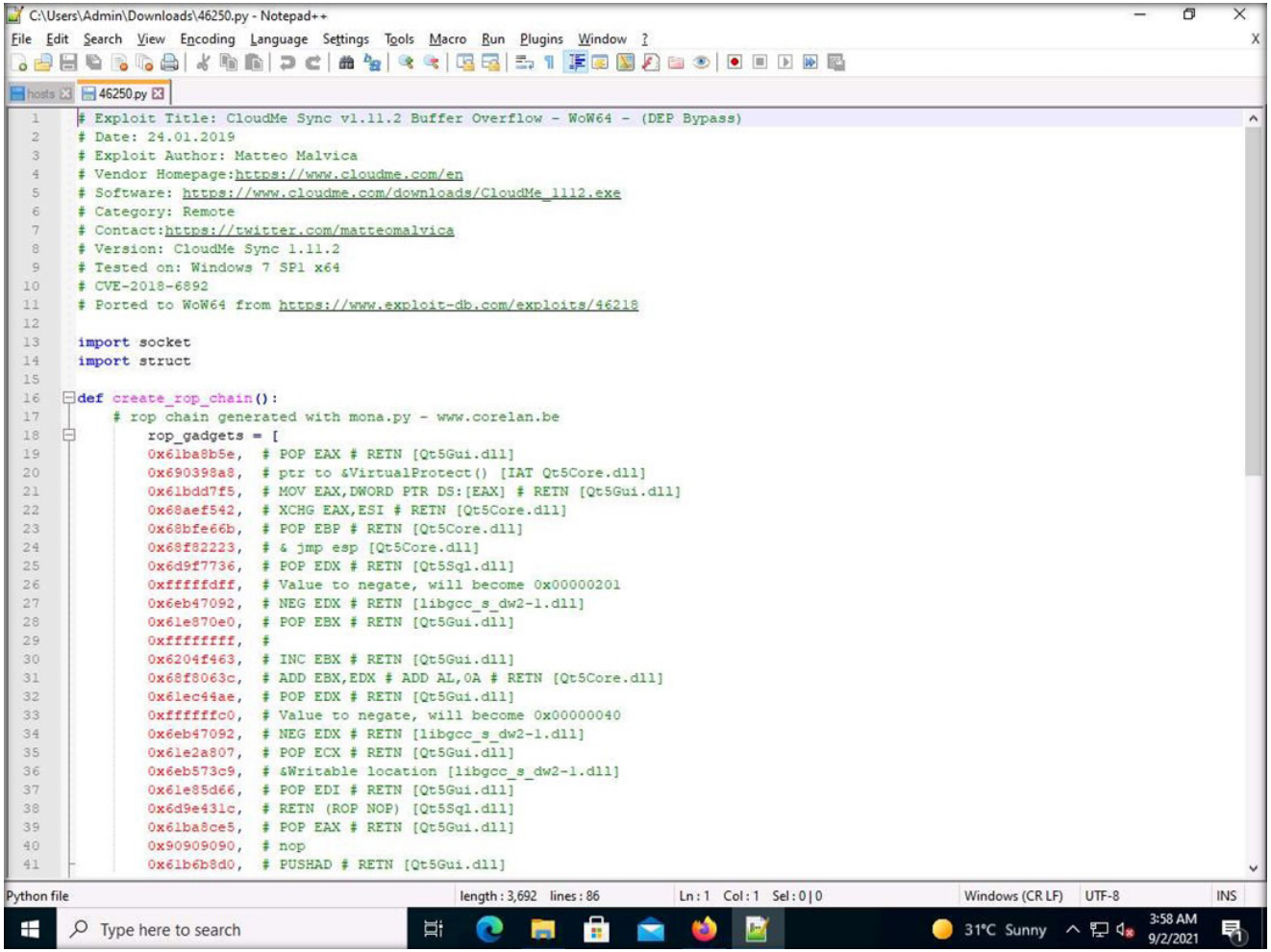
13. A Notepad++ windows appears, displaying the exploit code, as shown in the screenshot below.
Note: If a Notepad++ update pop-up appears, click No.

EXERCISE 5:
FIND VULNERABILITIES
ON EXPLOIT SITES



14. This exploit code can further be used to exploit vulnerabilities in the target system.
15. This concludes the demonstration of finding vulnerabilities on exploit sites such as Exploit Database.
16. Close all open windows and document all the acquired information.
17. Turn off Admin Machine-1 and PfSense Firewall virtual machines.

EXERCISE 5: FIND VULNERABILITIES ON EXPLOIT SITES




EC-Council