Lab 2: Infect the Target System using a Virus

Lab Scenario

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

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

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

Lab Objectives

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

Overview of Viruses and Worms

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

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

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

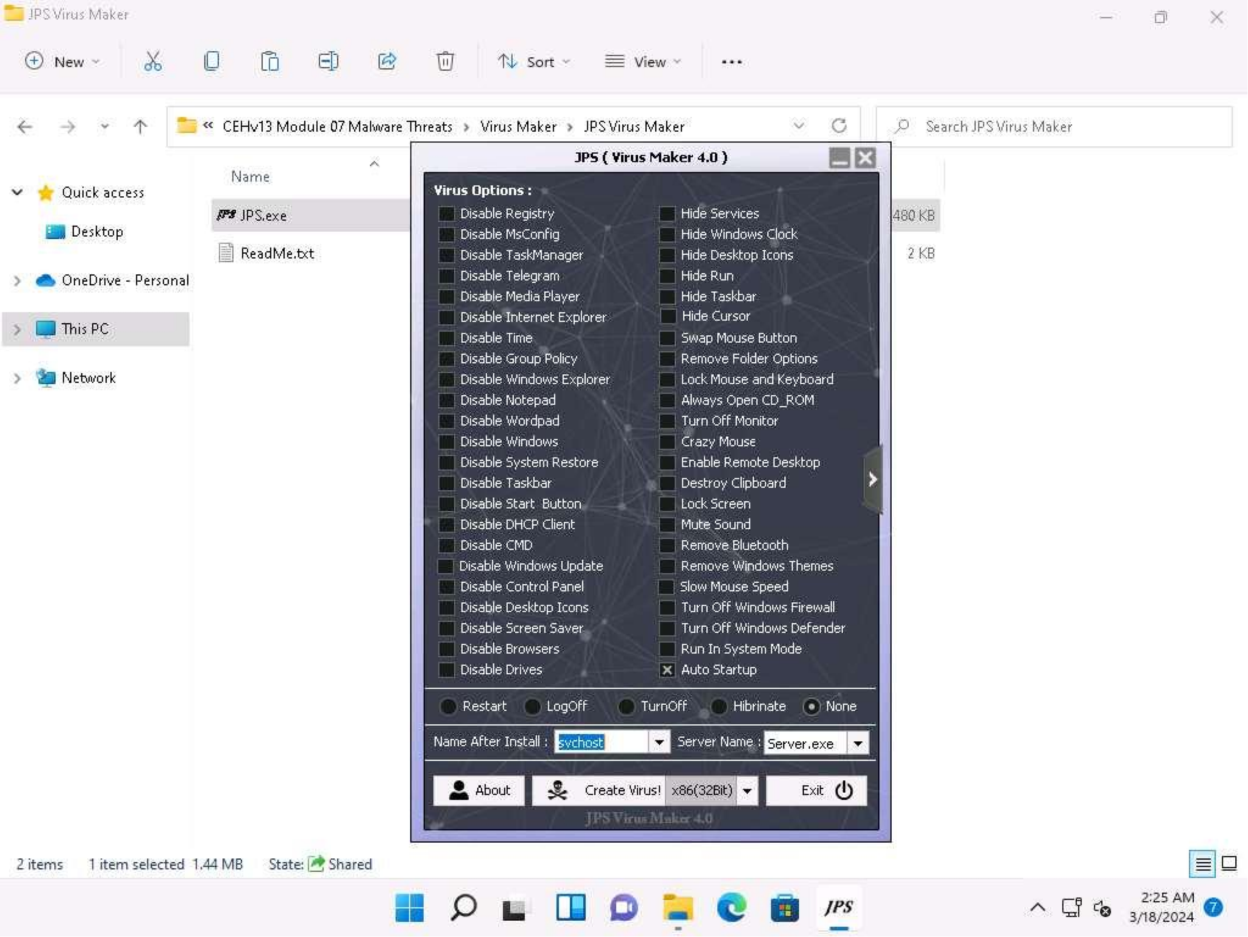
The JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool's features are auto-start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows. An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

After performing this task, we will end and re-launch the lab instance, as **Windows Server 2019** machine will be infected by the virus.

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

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

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



JPS (Virus Maker 4.0)

Virus Options :

□ Disable Registry
□ Disable MsConfig
□ Disable TaskManager
□ Disable Telegram
□ Disable Media Player
□ Disable Internet Explorer
□ Disable Time
□ Disable Group Policy
□ Disable Windows Explorer
□ Disable Notepad
□ Disable Wordpad
□ Disable Windows
□ Disable System Restore
□ Disable Taskbar
□ Disable Start Button
□ Disable DHCP Client
□ Disable CMD
□ Disable Windows Update
□ Disable Control Panel
□ Disable Desktop Icons
□ Disable Screen Saver
□ Disable Browsers
□ Disable Drives
□ Hide Services
□ Hide Windows Clock
□ Hide Desktop Icons
□ Hide Run
□ Hide Taskbar
□ Hide Cursor
□ Swap Mouse Button
□ Remove Folder Options
□ Lock Mouse and Keyboard
□ Always Open CD_ROM
□ Turn Off Monitor
□ Crazy Mouse
□ Enable Remote Desktop
□ Destroy Clipboard
□ Lock Screen
□ Mute Sound
□ Remove Bluetooth
□ Remove Windows Themes
□ Slow Mouse Speed
□ Turn Off Windows Firewall
□ Turn Off Windows Defender
□ Run In System Mode
☒ Auto Startup

○ Restart ○ LogOff ○ TurnOff ○ Hibrinate ● None

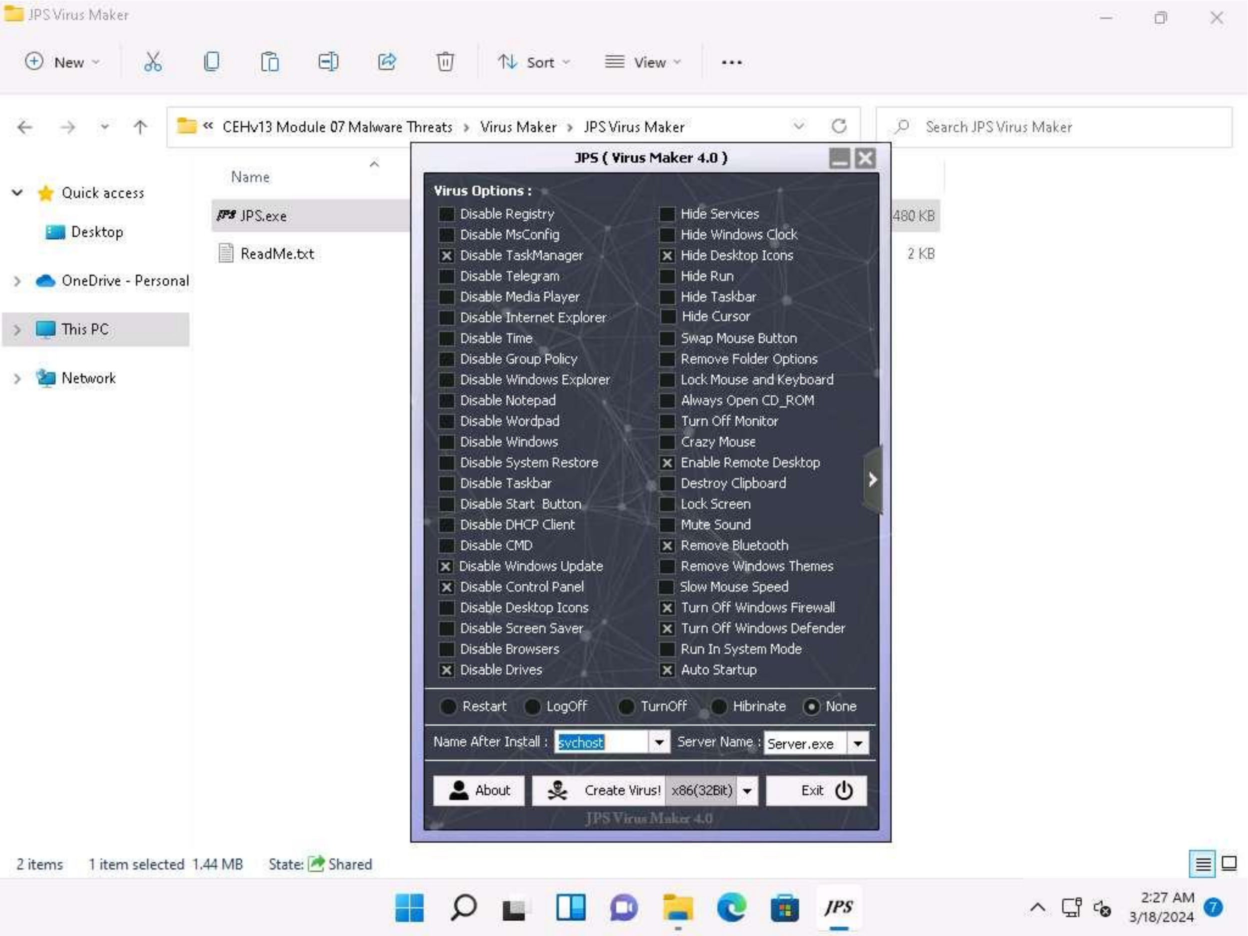
Name After Install : svchost   Server Name : Server.exe

x86(32Bit)

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

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

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



JPS (Virus Maker 4.0)

Virus Options :

☐ Disable Registry
☐ Disable MsConfig
☒ Disable TaskManager
☐ Disable Telegram
☐ Disable Media Player
☐ Disable Internet Explorer
☐ Disable Time
☐ Disable Group Policy
☐ Disable Windows Explorer
☐ Disable Notepad
☐ Disable Wordpad
☐ Disable Windows
☐ Disable System Restore
☐ Disable Taskbar
☐ Disable Start Button
☐ Disable DHCP Client
☐ Disable CMD
☒ Disable Windows Update
☒ Disable Control Panel
☐ Disable Desktop Icons
☐ Disable Screen Saver
☐ Disable Browsers
☒ Disable Drives

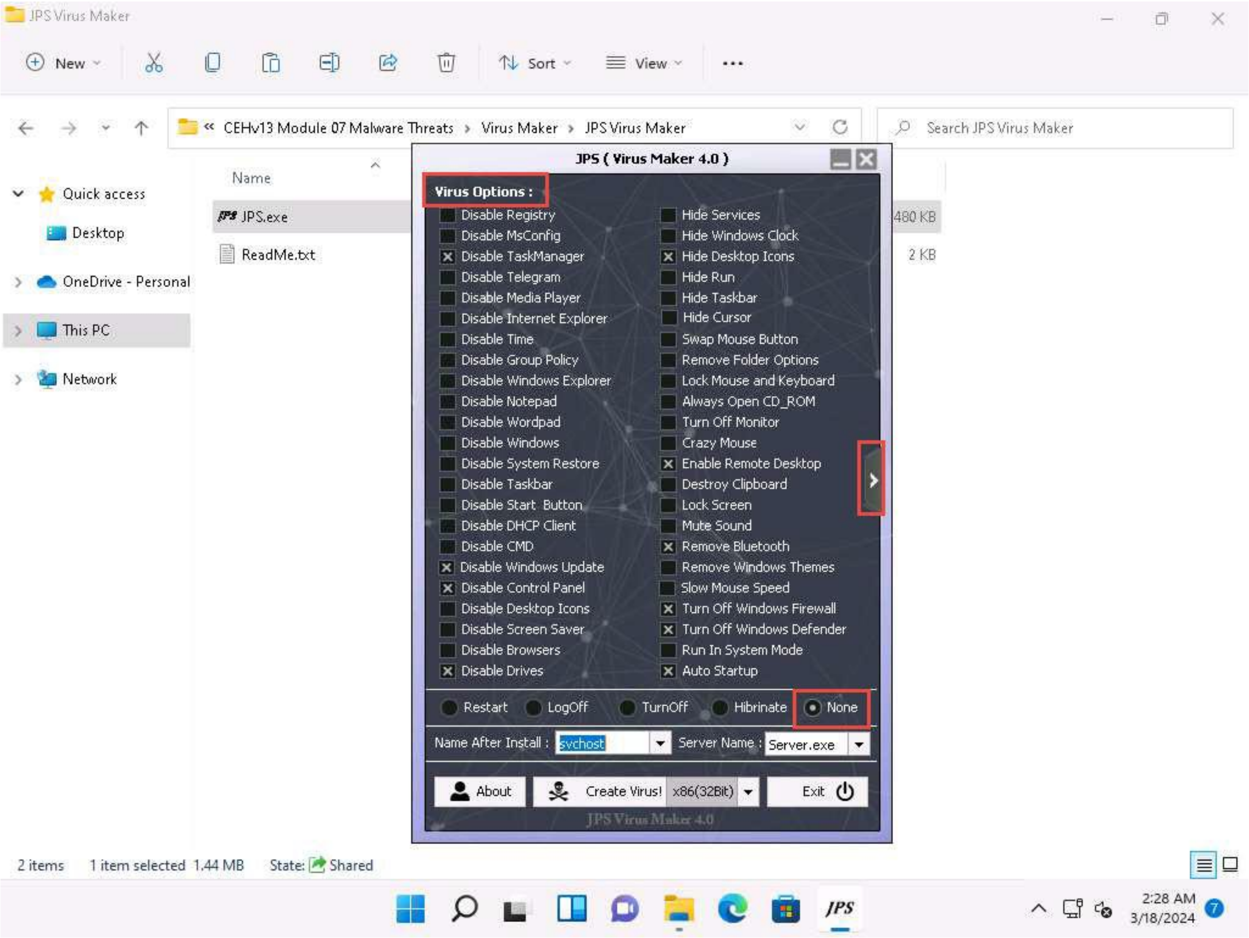
☐ Hide Services
☐ Hide Windows Clock
☒ Hide Desktop Icons
☐ Hide Run
☐ Hide Taskbar
☐ Hide Cursor
☐ Swap Mouse Button
☐ Remove Folder Options
☐ Lock Mouse and Keyboard
☐ Always Open CD_ROM
☐ Turn Off Monitor
☐ Crazy Mouse
☒ Enable Remote Desktop
☐ Destroy Clipboard
☐ Lock Screen
☐ Mute Sound
☒ Remove Bluetooth
☐ Remove Windows Themes
☐ Slow Mouse Speed
☒ Turn Off Windows Firewall
☒ Turn Off Windows Defender
☐ Run In System Mode
☒ Auto Startup

○ Restart ○ LogOff ○ TurnOff ○ Hibrinate ● None

Name After Install : svchost Server Name : Server.exe

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

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



JPS (Virus Maker 4.0)

Virus Options :

□ Disable Registry
□ Disable MsConfig
☒ Disable TaskManager
□ Disable Telegram
□ Disable Media Player
□ Disable Internet Explorer
□ Disable Time
□ Disable Group Policy
□ Disable Windows Explorer
□ Disable Notepad
□ Disable Wordpad
□ Disable Windows
□ Disable System Restore
□ Disable Taskbar
□ Disable Start Button
□ Disable DHCP Client
□ Disable CMD
☒ Disable Windows Update
☒ Disable Control Panel
□ Disable Desktop Icons
□ Disable Screen Saver
□ Disable Browsers
☒ Disable Drives

□ Hide Services
□ Hide Windows Clock
☒ Hide Desktop Icons
□ Hide Run
□ Hide Taskbar
□ Hide Cursor
□ Swap Mouse Button
□ Remove Folder Options
□ Lock Mouse and Keyboard
□ Always Open CD_ROM
□ Turn Off Monitor
□ Crazy Mouse
☒ Enable Remote Desktop
□ Destroy Clipboard
□ Lock Screen
□ Mute Sound
☒ Remove Bluetooth
□ Remove Windows Themes
□ Slow Mouse Speed
☒ Turn Off Windows Firewall
☒ Turn Off Windows Defender
□ Run In System Mode
☒ Auto Startup

○ Restart ○ LogOff ○ TurnOff ○ Hibrinate ● None

Name After Install : svchost Server Name : Server.exe

About | Create Virus! x86(32Bit) | Exit

JPS Virus Maker 4.0

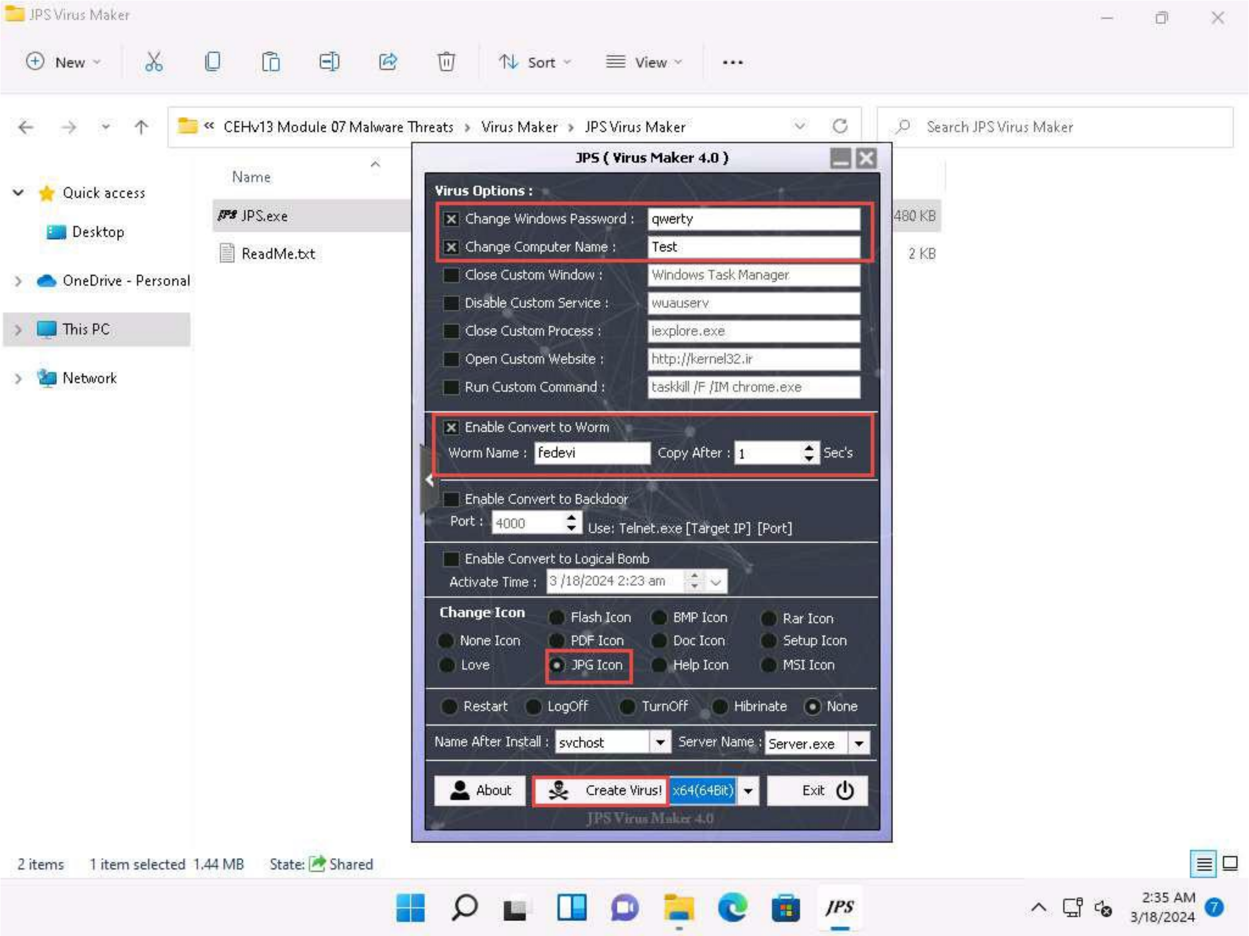
8. A **Virus Options** window appears.

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

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

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

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



JPS (Virus Maker 4.0)

Virus Options :

☒ Change Windows Password : qwerty
☒ Change Computer Name : Test
□ Close Custom Window : Windows Task Manager
□ Disable Custom Service : wuauserv
□ Close Custom Process : iexplore.exe
□ Open Custom Website : http://kernel32.ir
□ Run Custom Command : taskkill /F /IM chrome.exe

☒ Enable Convert to Worm
Worm Name : fedevi Copy After : 1 Sec's

□ Enable Convert to Backdoor
Port : 4000 Use: Telnet.exe [Target IP] [Port]

□ Enable Convert to Logical Bomb
Activate Time : 3 /18/2024 2:23 am

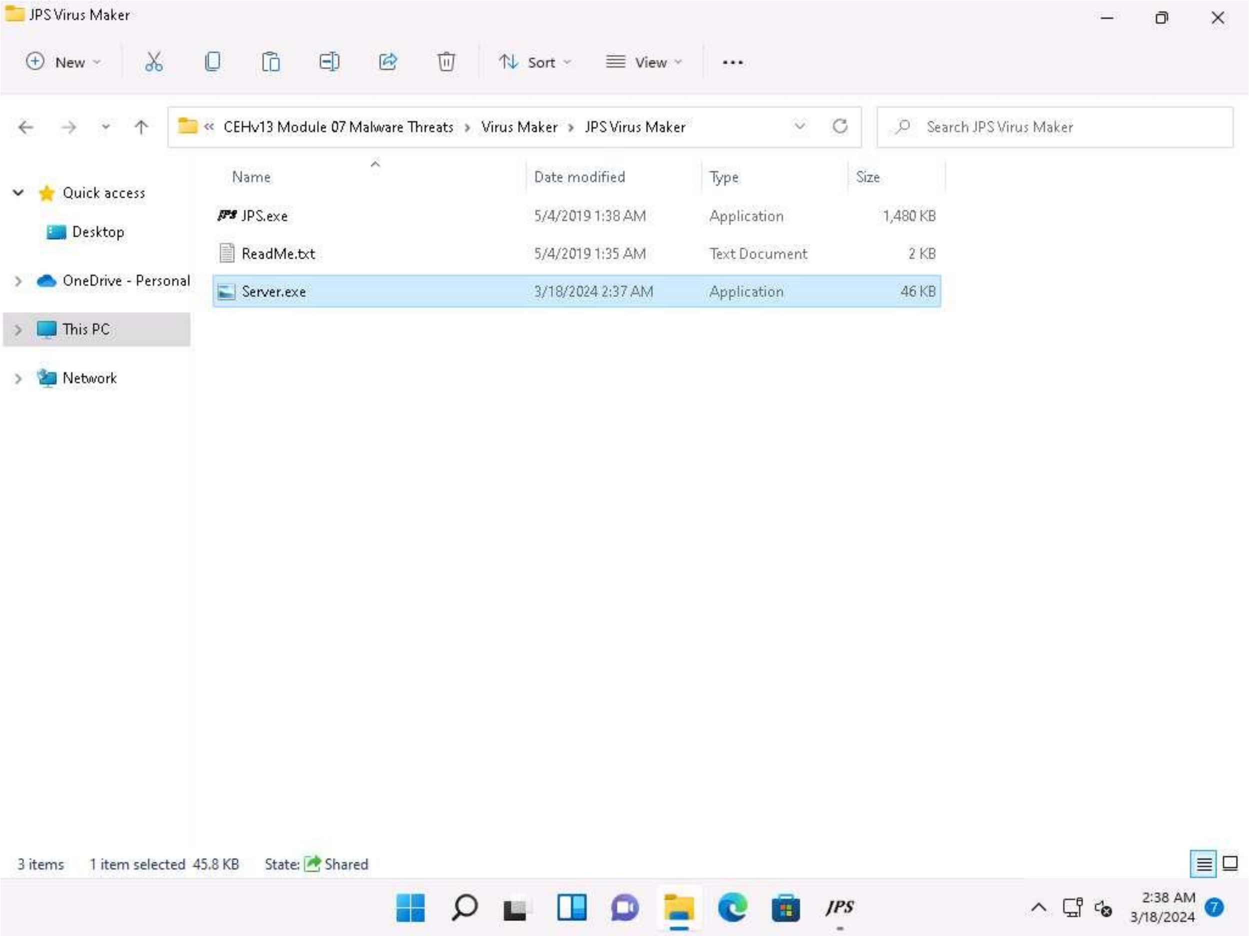
Change Icon
○ Flash Icon ○ BMP Icon ○ Rar Icon
○ None Icon ○ PDF Icon ○ Doc Icon ○ Setup Icon
○ Love ● JPG Icon ○ Help Icon ○ MSI Icon

○ Restart ○ LogOff ○ TurnOff ○ Hibrinate ● None

Name After Install : svchost Server Name : Server.exe

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

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



Name	Date modified	Type	Size
JPS.exe	5/4/2019 1:38 AM	Application	1,480 KB
ReadMe.txt	5/4/2019 1:35 AM	Text Document	2 KB
Server.exe	3/18/2024 2:37 AM	Application	46 KB

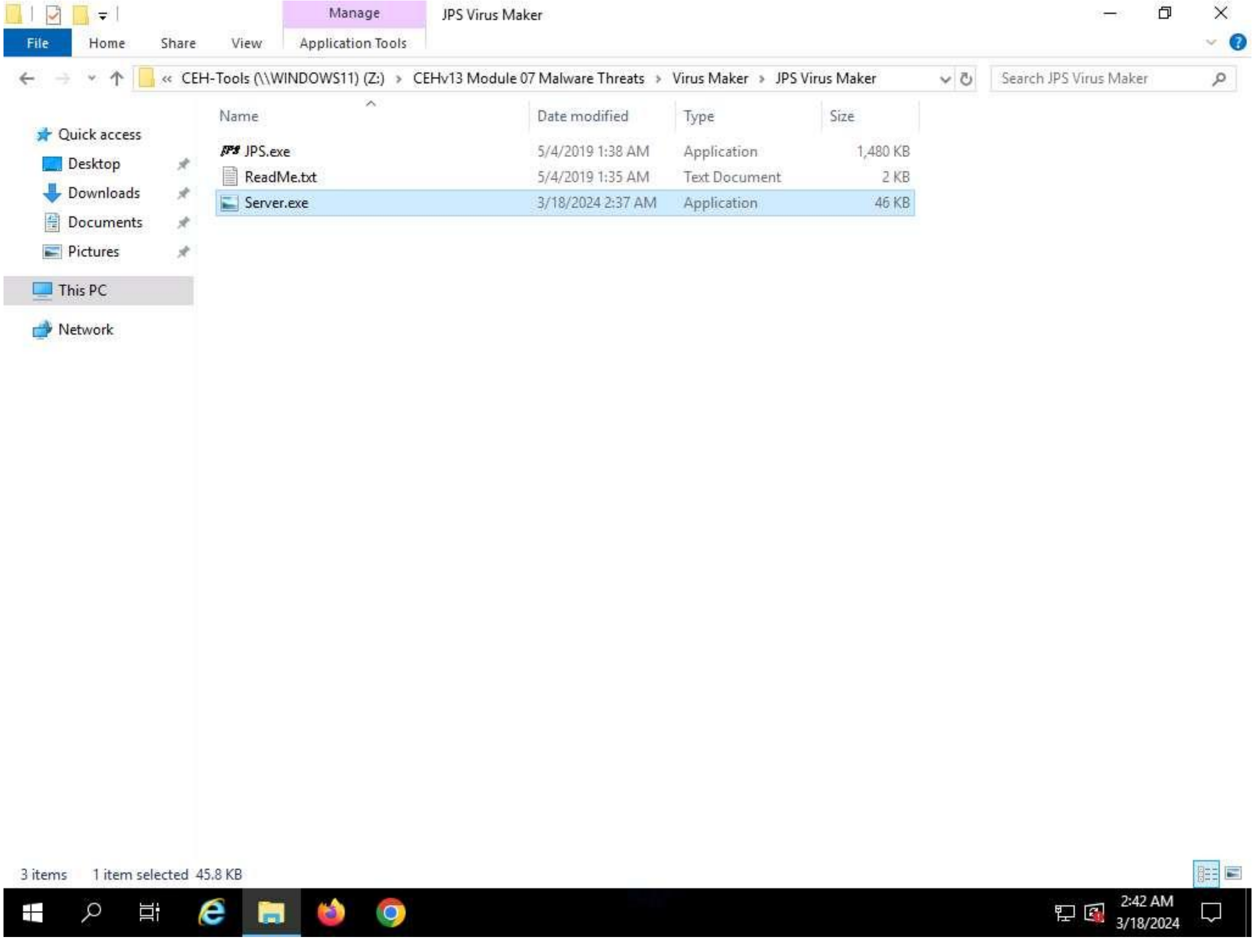
15. Now, pack this virus with a binder or virus packager and send it to the victim machine through email, chat, a mapped network drive, or other method.

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

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

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

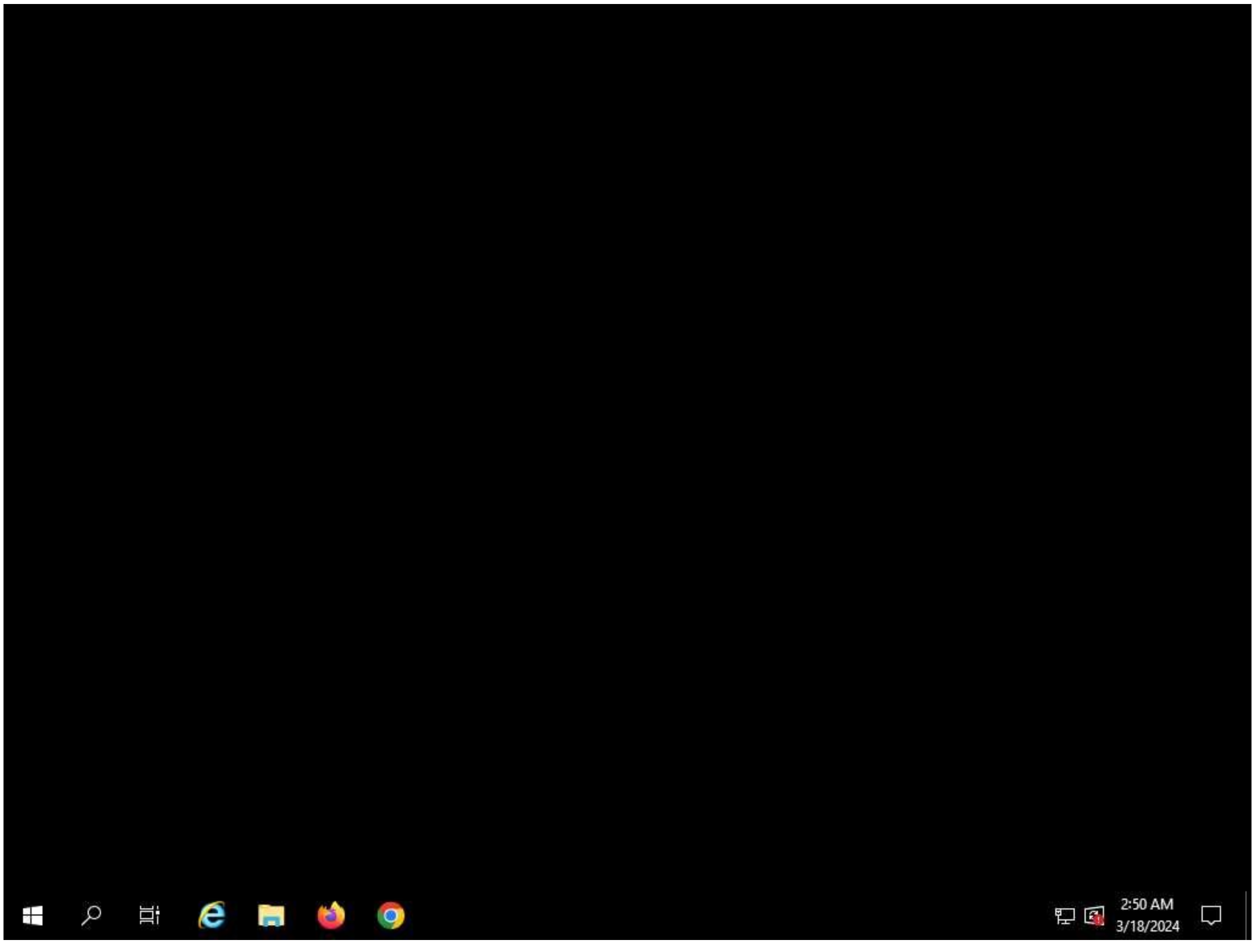
18. Navigate to **Z:\CEHv13 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **Server.exe** file to execute the virus.



Name	Date modified	Type	Size
JPS.exe	5/4/2019 1:38 AM	Application	1,480 KB
ReadMe.txt	5/4/2019 1:35 AM	Text Document	2 KB
Server.exe	3/18/2024 2:37 AM	Application	46 KB

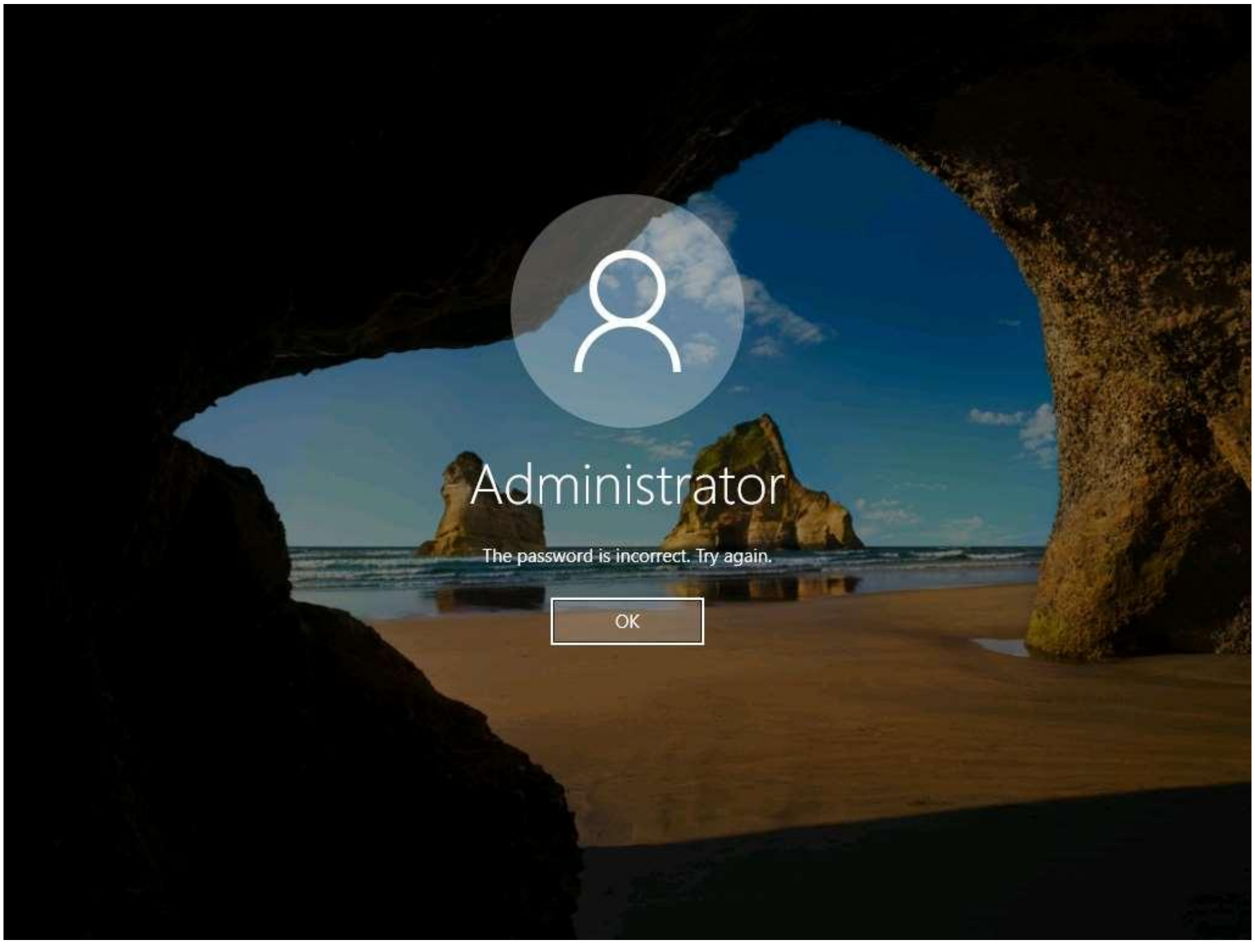
3 items 1 item selected 45.8 KB

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



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

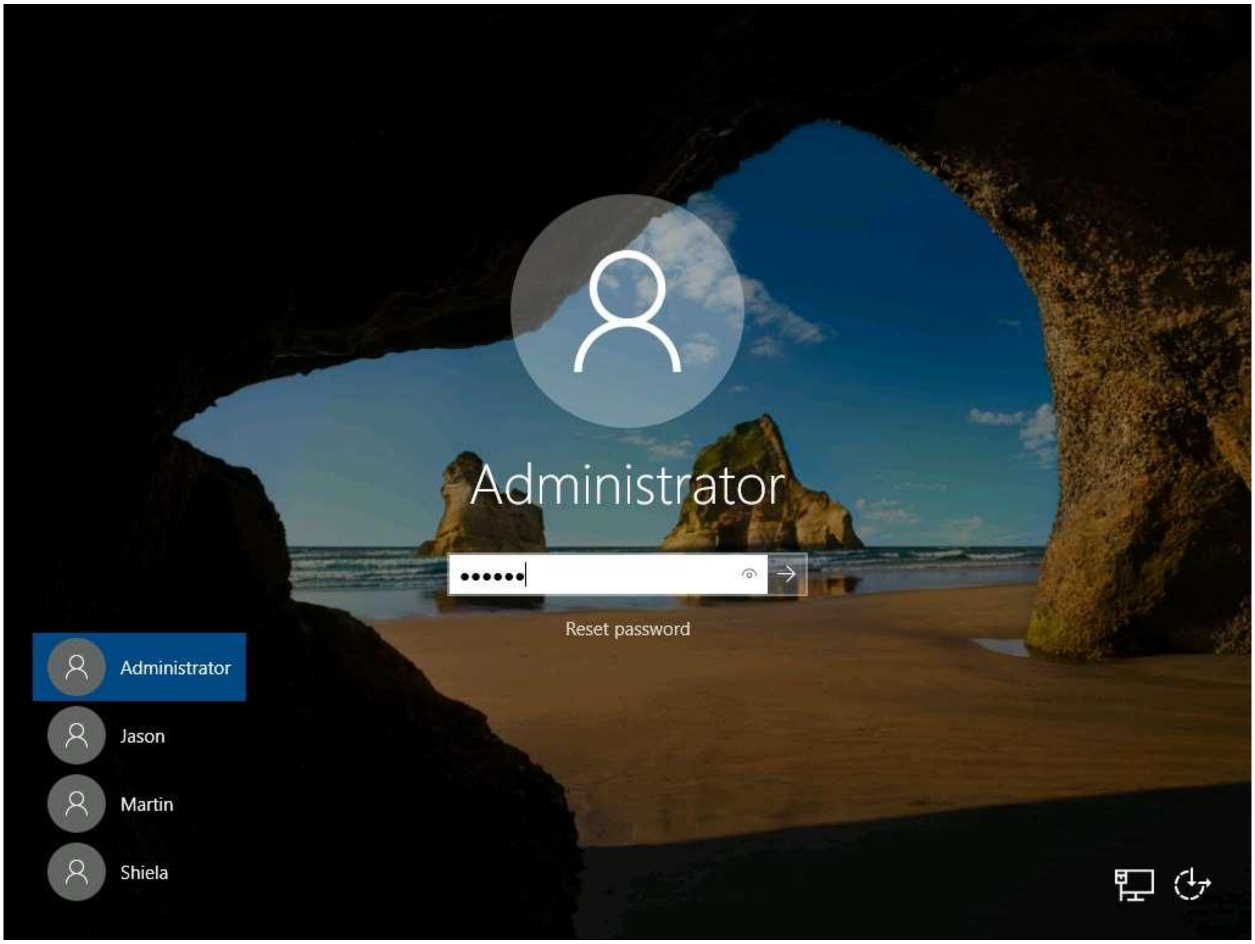
21. Click Ctrl+Alt+Delete to activate the machine, login with **Administrator/Pa$$w0rd**.



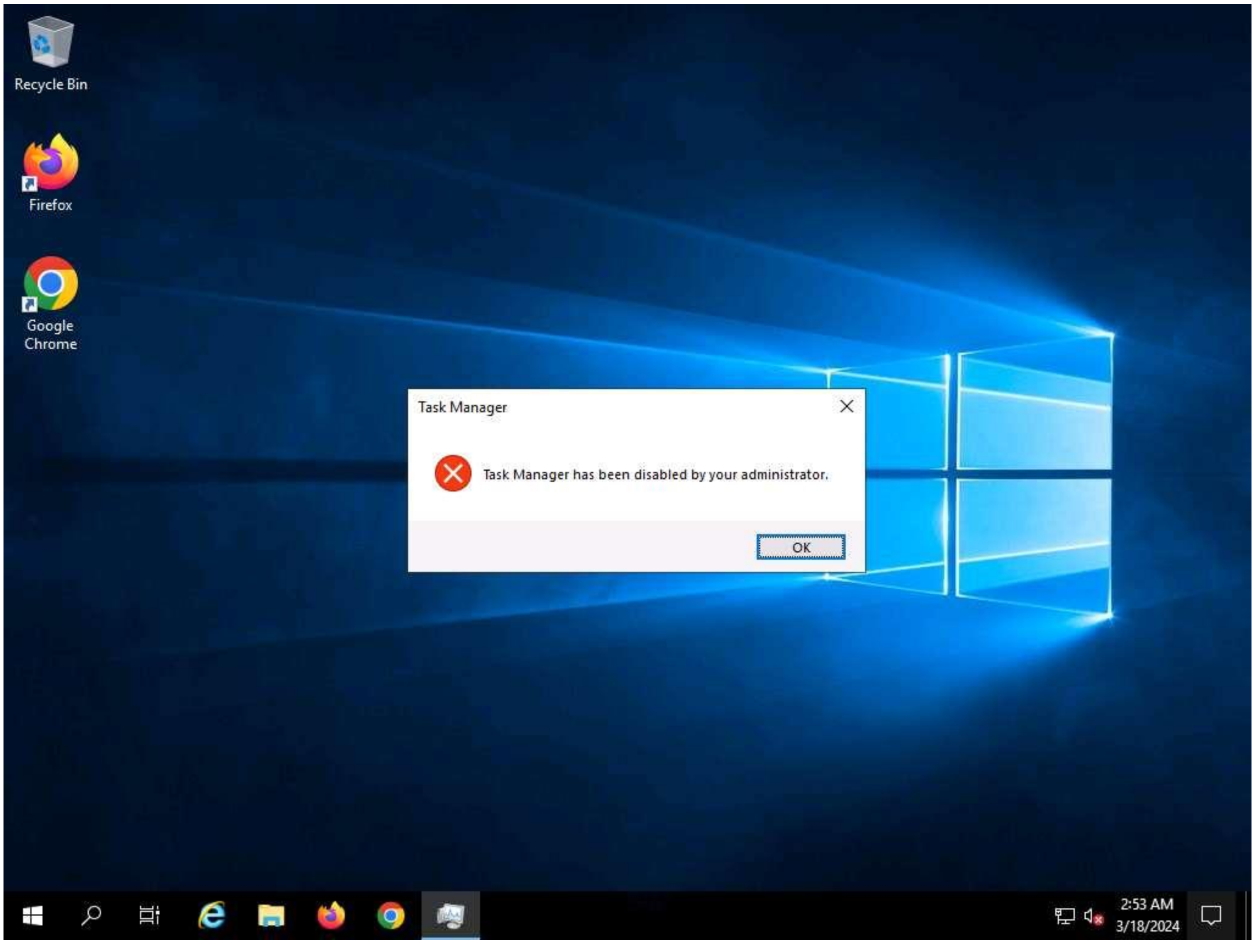
Administrator

The password is incorrect. Try again.

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



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



Task Manager

Task Manager has been disabled by your administrator.

24. You will get a similar error for all the applications that are disabled by the virus.
25. This is how attackers infect a system with viruses. Now, before going to the next task, **End** the lab and re-launch it to reset the machines. To do so, click the **Exit Lab** icon from the top right and click **End Lab** from the drop-down options.

Question 7.2.1.1

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