

Lab 2: Infect the Target System using a Virus

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

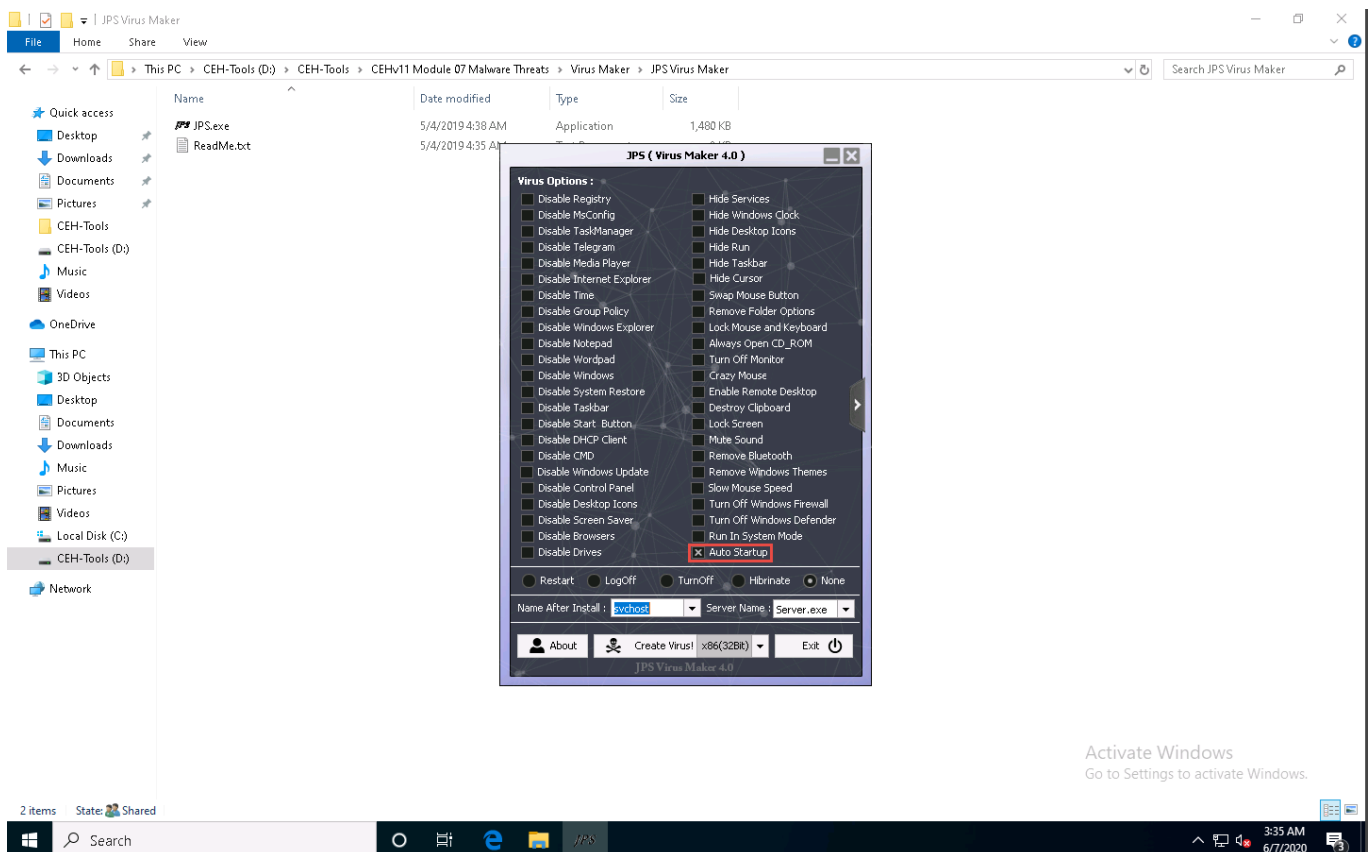
The JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool's features are auto-start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows. An 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 as **Windows Server 2019** machine will be infected by the virus.

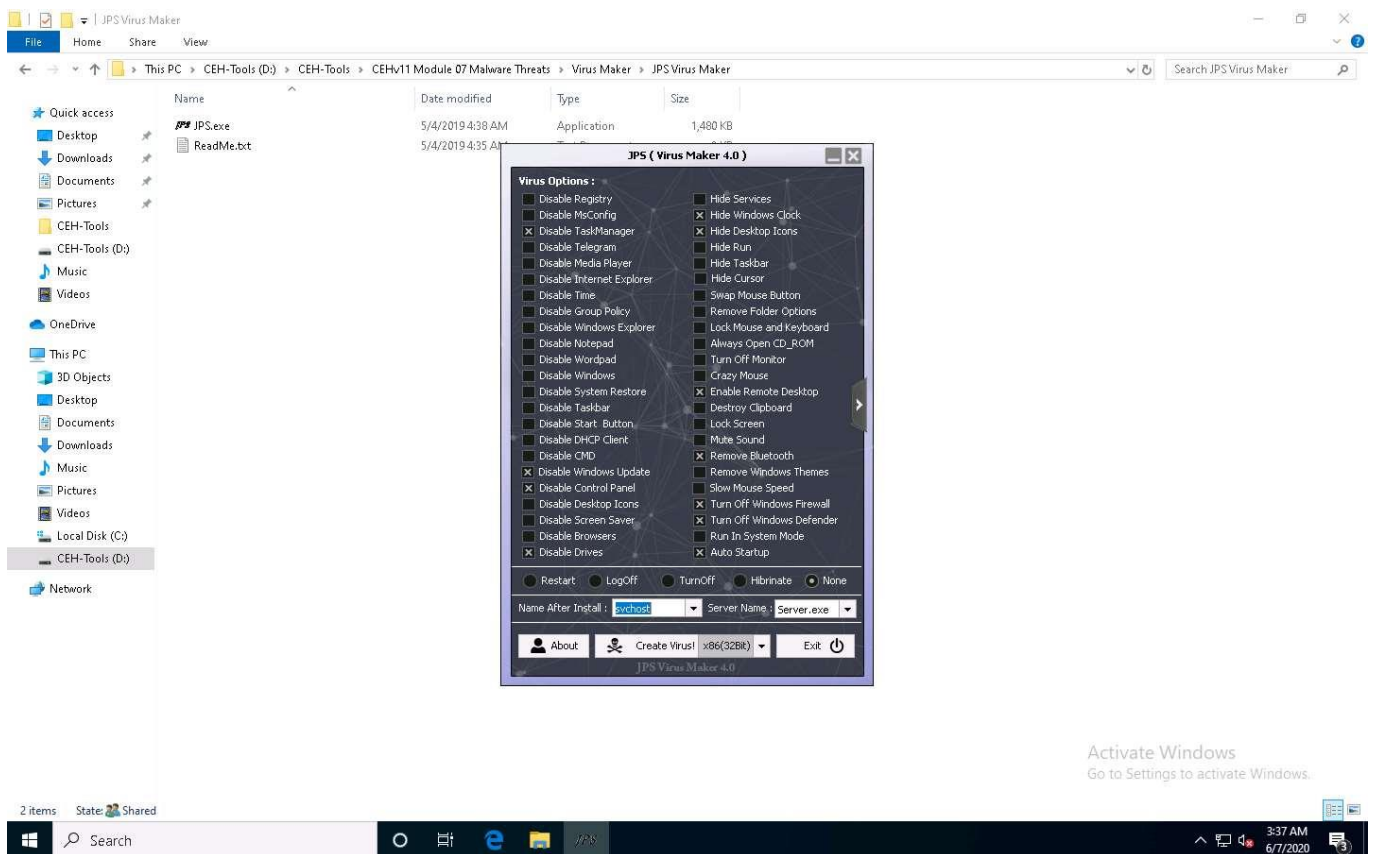
1. ☐ In the **Windows 10** machine, navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **jps.exe**.

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

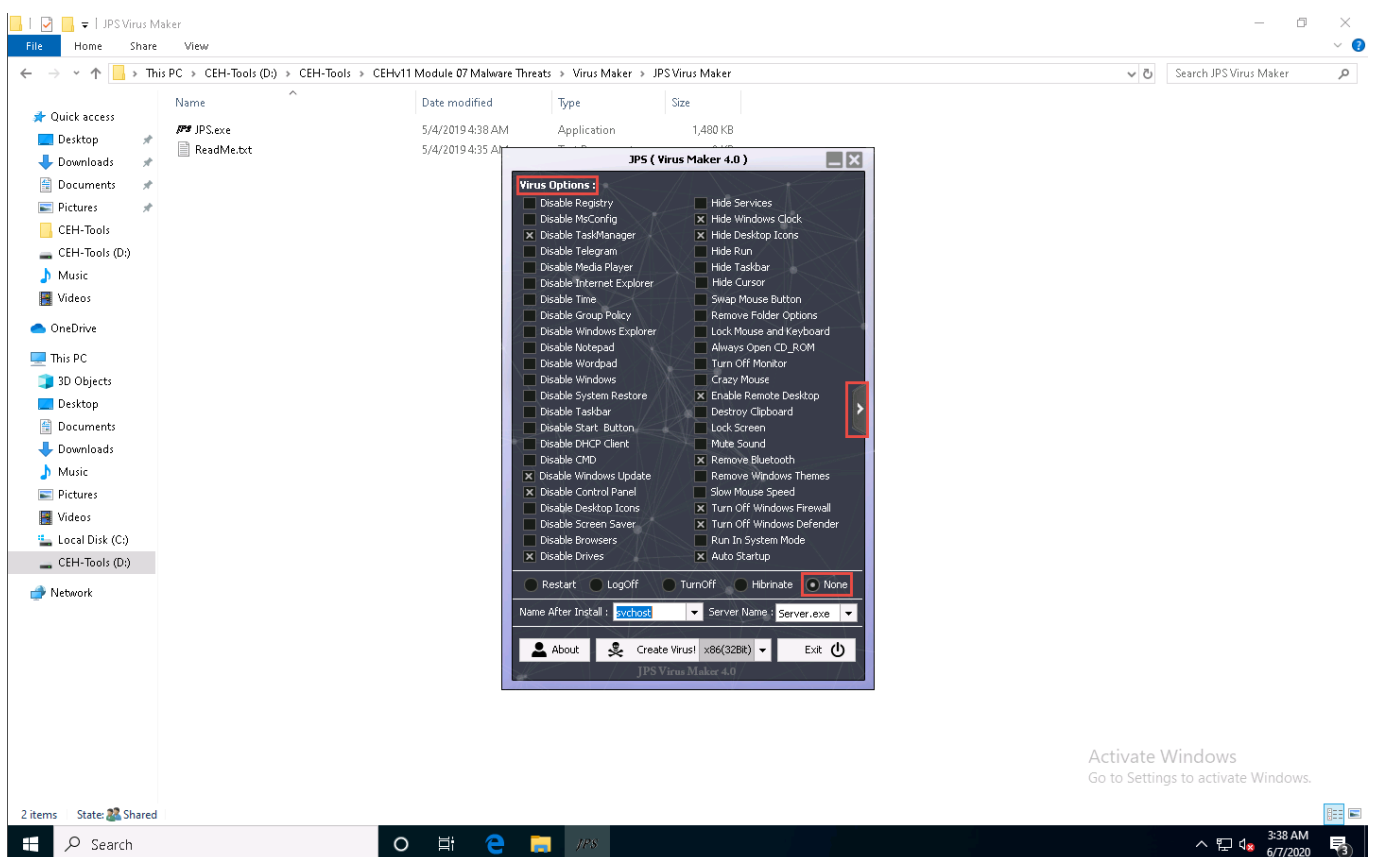
2. ☐ The **JPS (Virus Maker 4.0)** window appears; tick the **Auto Startup** checkbox.



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 lab, the options embedded 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**.

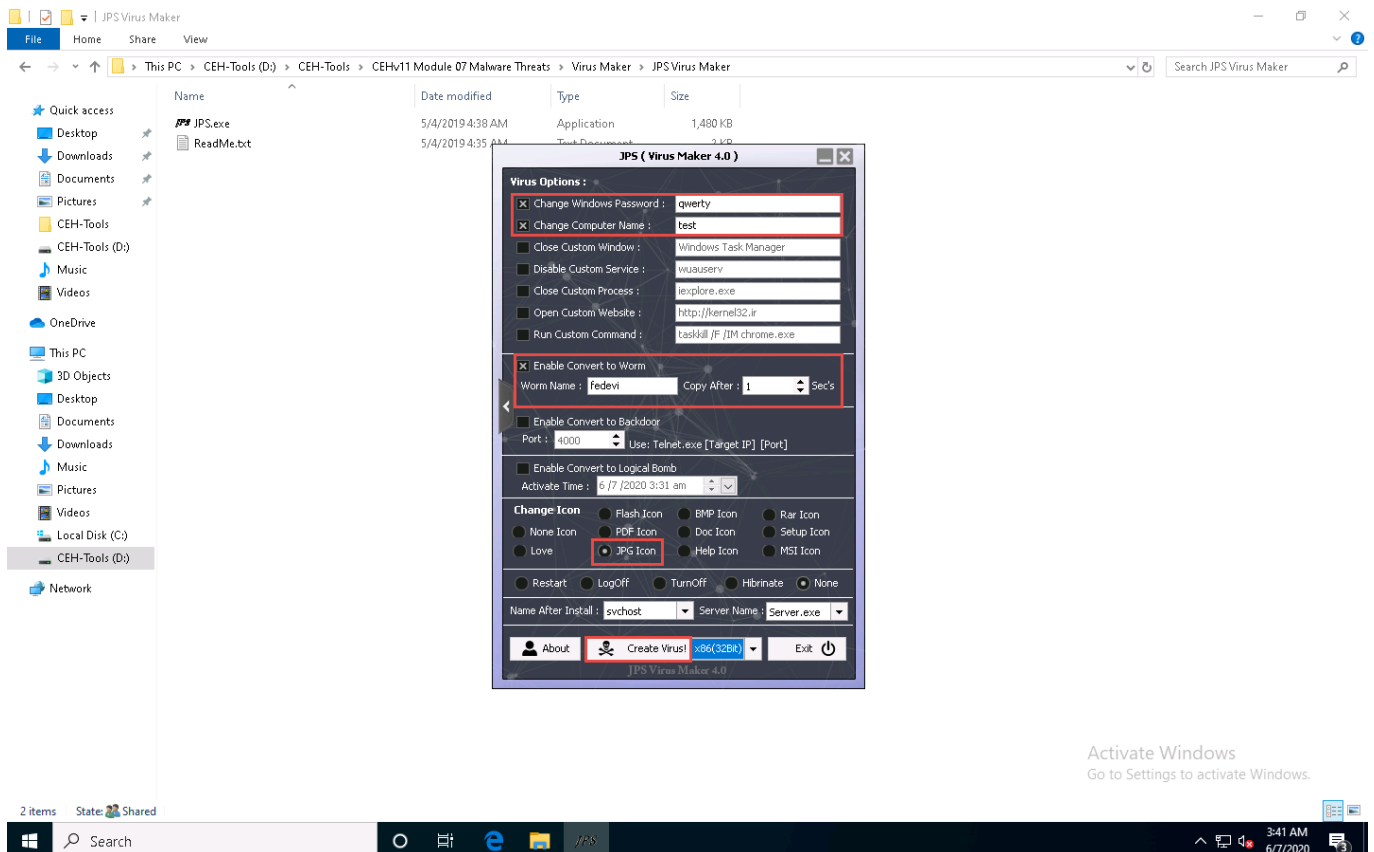


6. ☐ Ensure that the **None** radio button is selected to specify the trigger event when the virus should start attacking the system after its creation.
7. ☐ Now, before clicking on **Create Virus!**, click the right arrow icon from the right-hand pane of the window to configure the virus options.

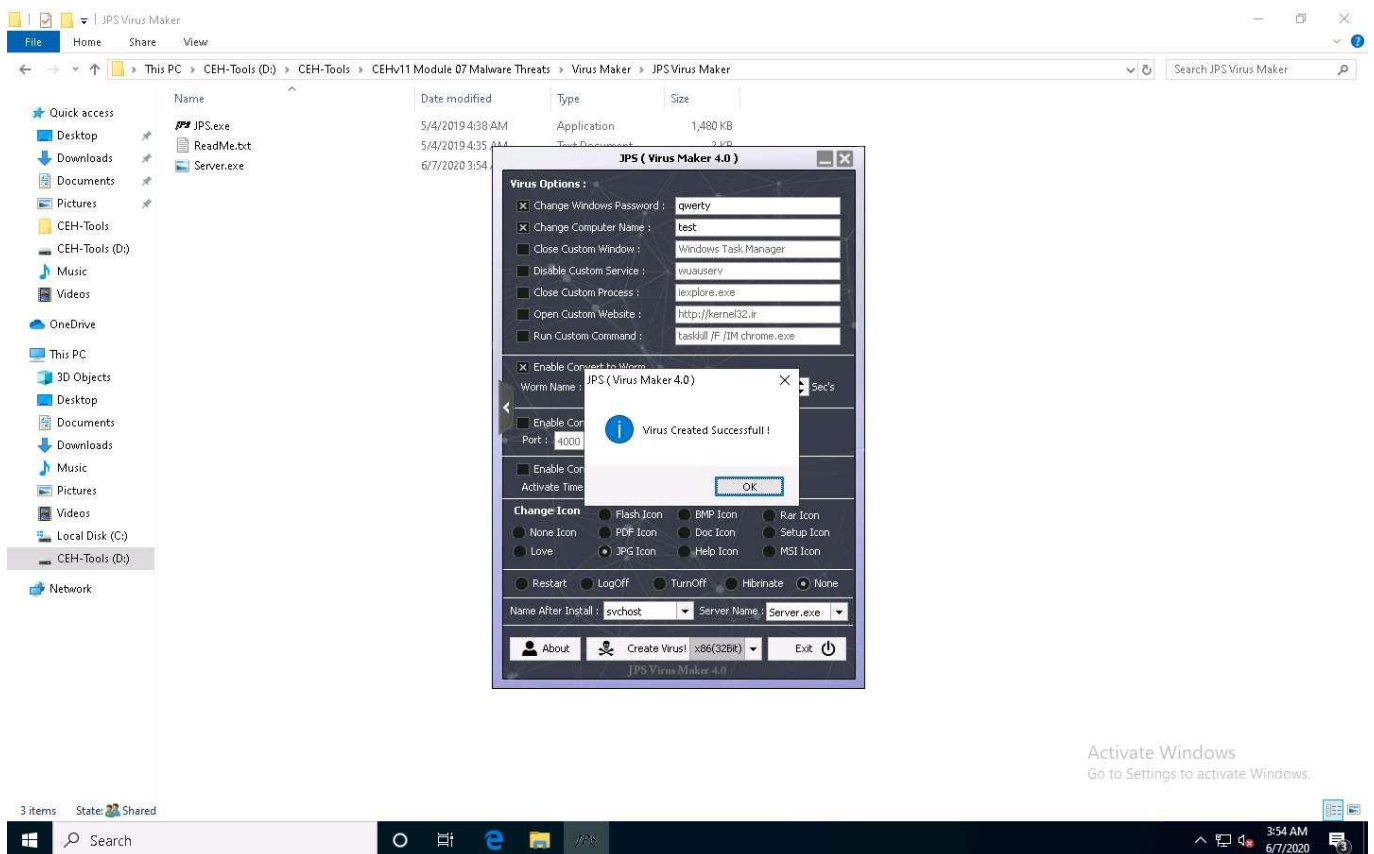


8. ☐ A **Virus Options** window appears, as shown in the screenshot.

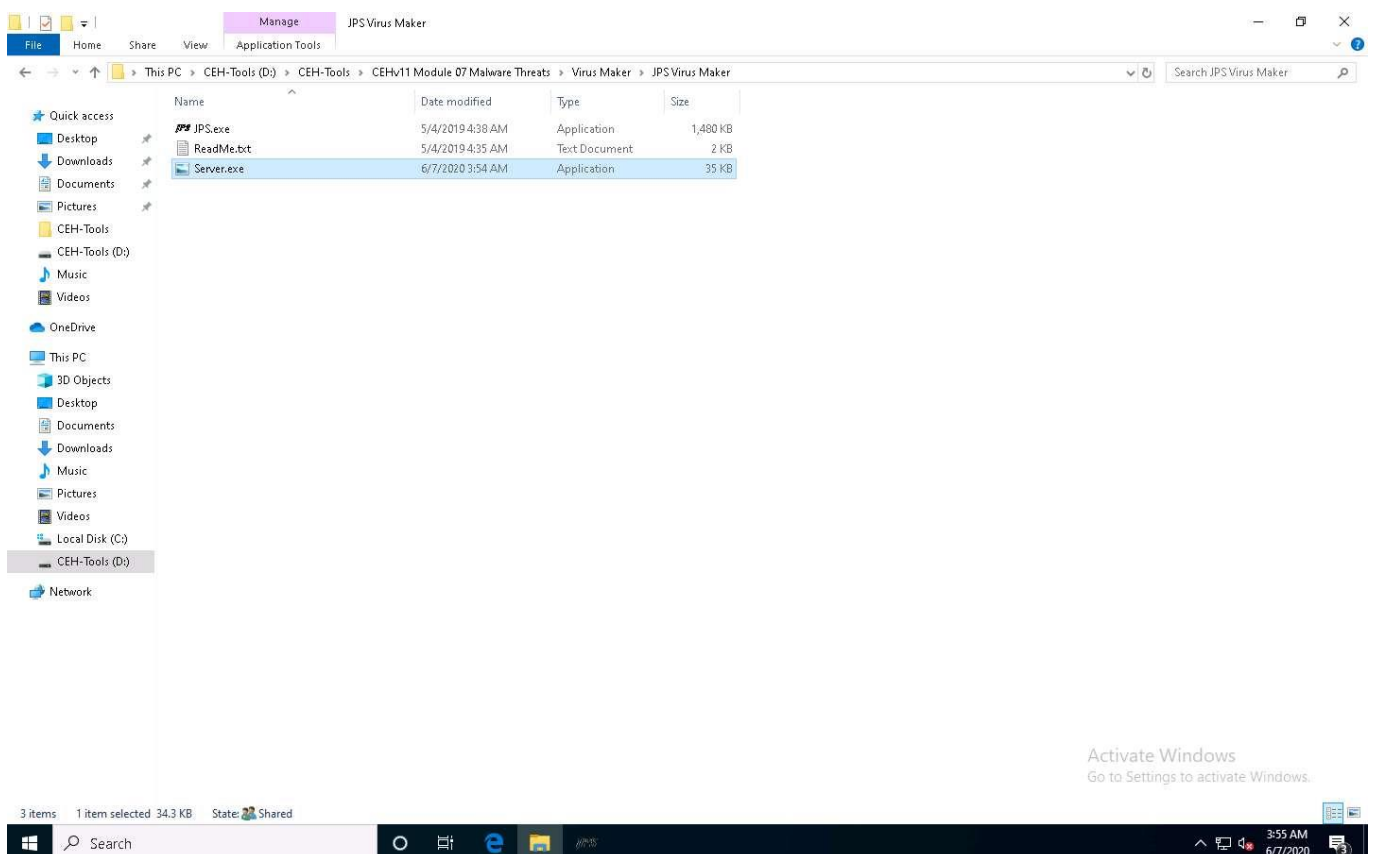
9. ☐ Check the **Change Windows Password** option, and enter a password (here, **qwerty**) in the text field. Check the **Change Computer Name** option, and type **Test** in the text field.
10. ☐ You can even configure the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox, 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 **x86(32Bit)**; click **Create Virus!**
13. ☐ A **Virus Created Successful!** pop-up appears; click **OK**.

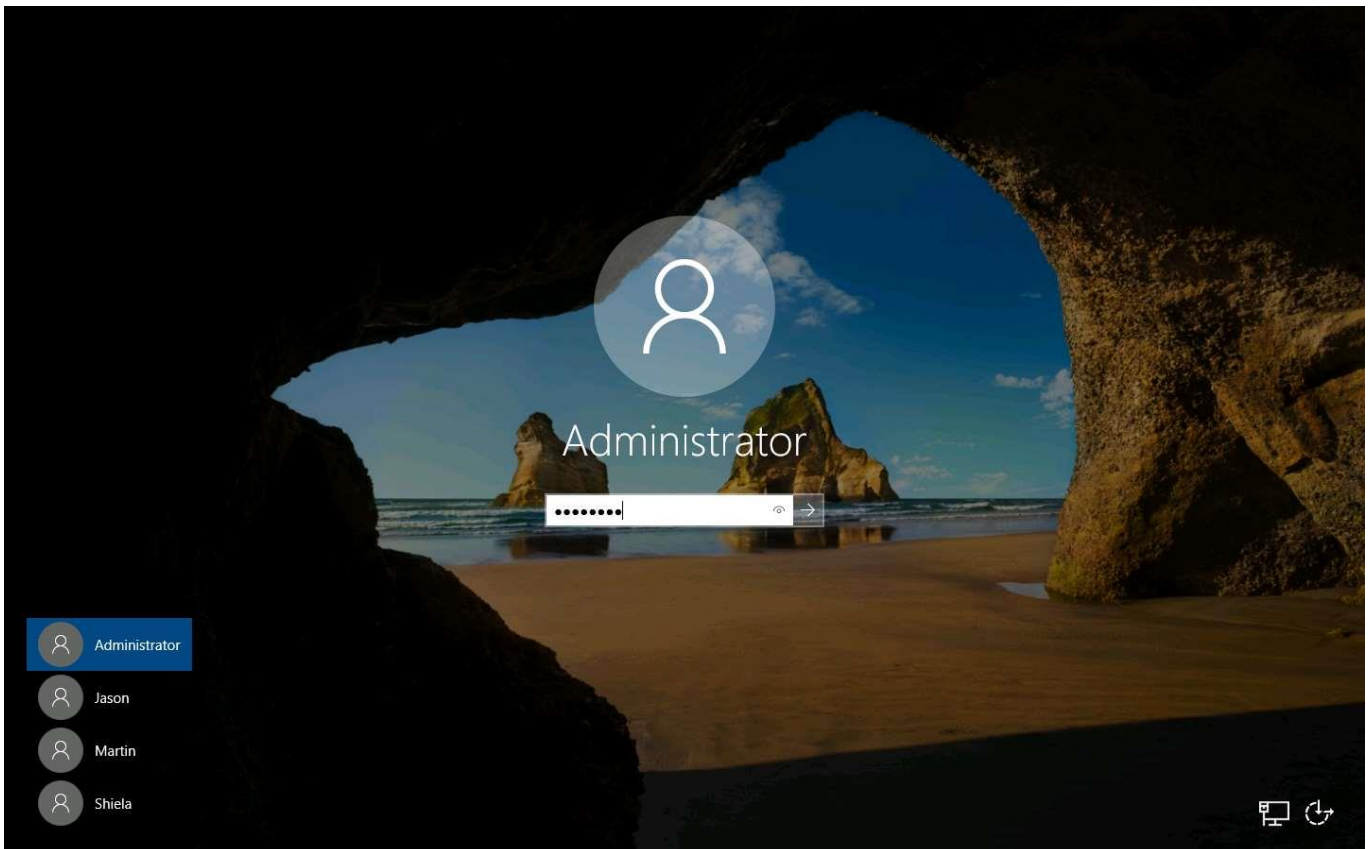


14. The newly created virus (server) is placed automatically in the **folder** where jps.exe is located, but with the name **Server.exe**. Navigate to **D:\CEH-Tools\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and observe that the newly created virus with the name **Server.exe** is available at the specified location.

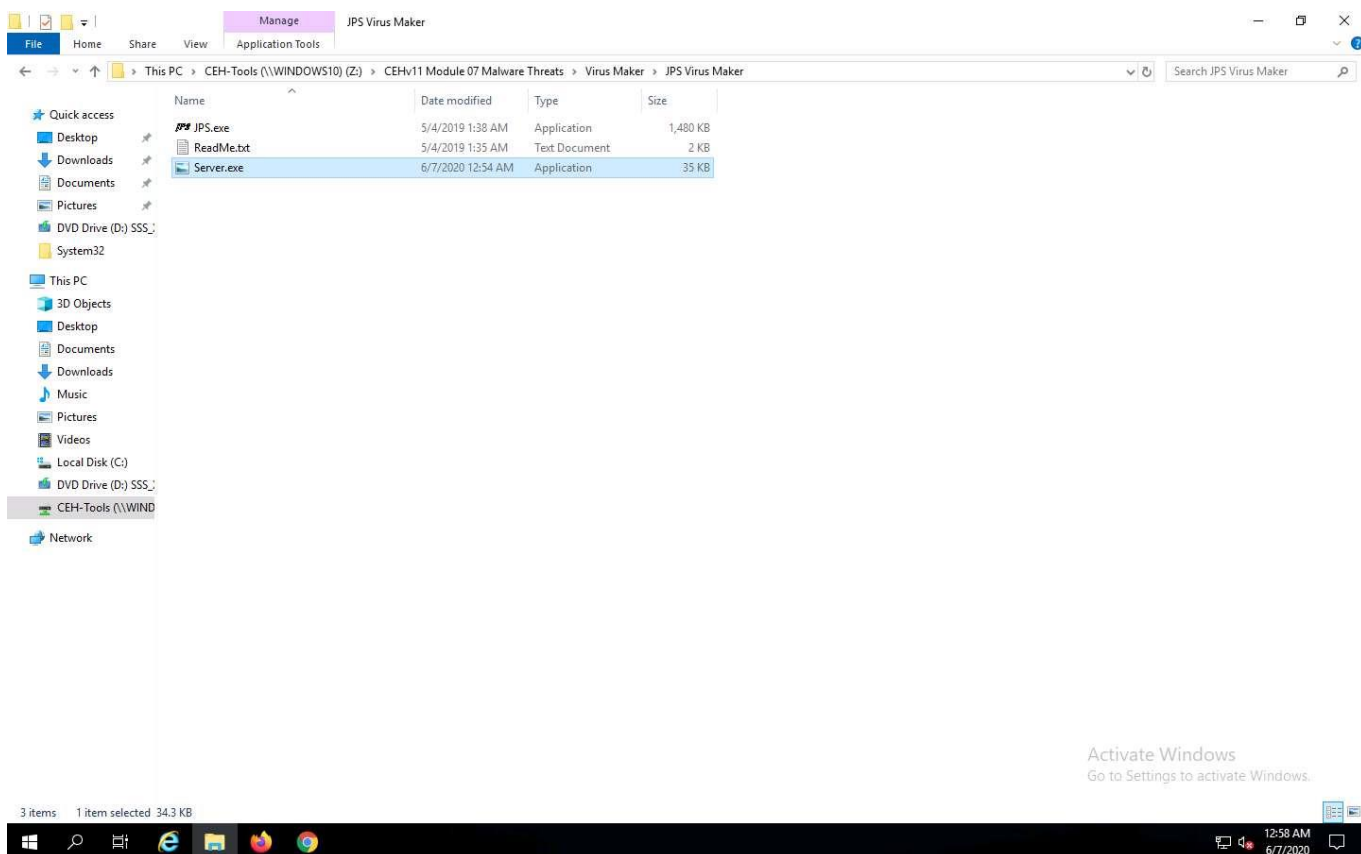


15. ☐ Now, pack this virus with a binder or virus packager and send it to the victim machine through email, chat, a mapped network drive, or other method.
16. ☐ In this task, we are using a mapped network drive to share the virus file to the victim machine. Assume that you are a victim and that you have received this file.
17. ☐ Click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine. Click [Ctrl+Alt+Delete](#) to activate the machine, by default, **Administrator** account is selected, click **Pa\$\$w0rd** to enter the password and press **Enter**.

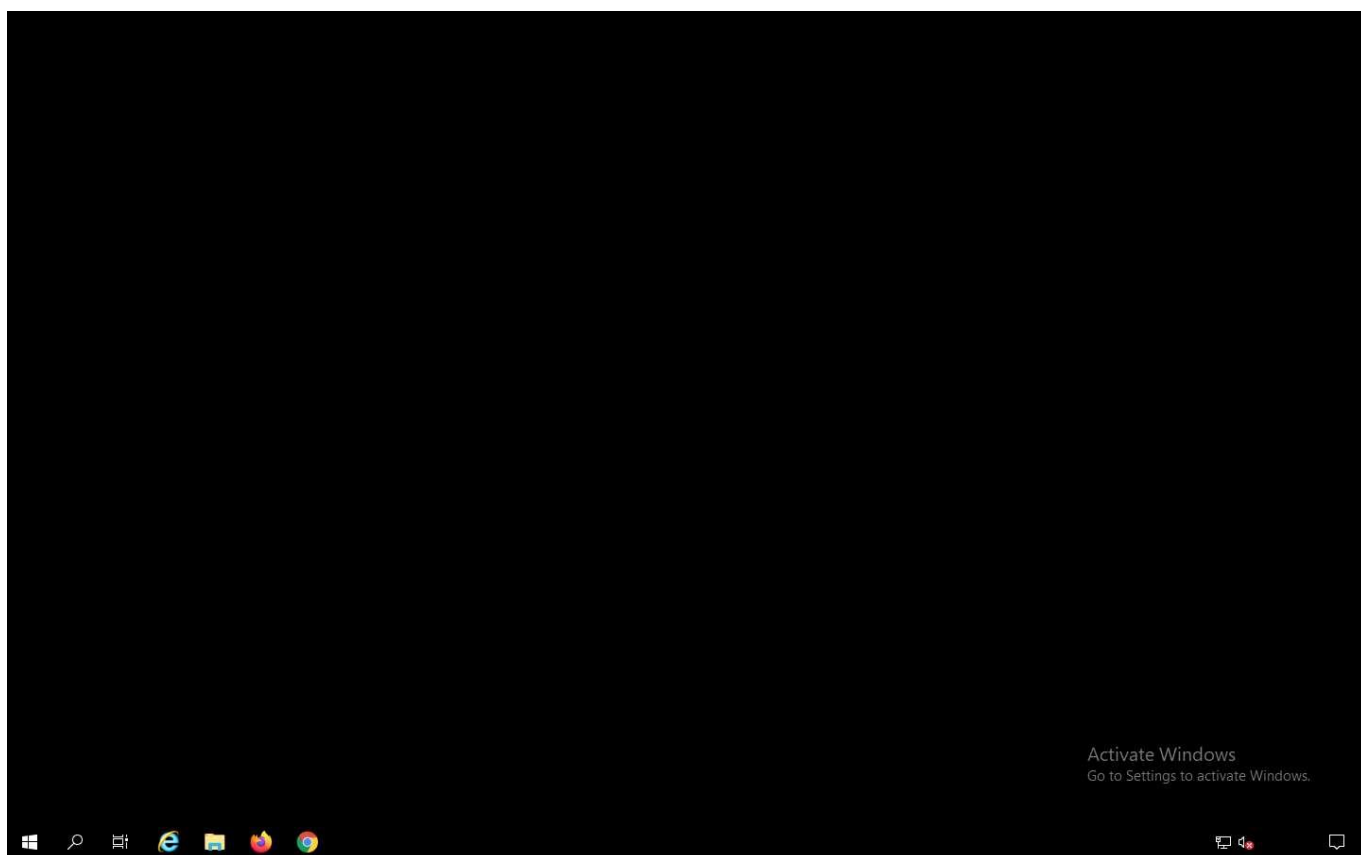
Here, we are logging into the machine as a victim.



18. ☐ Navigate to **Z:\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **Server.exe** file to execute the virus.

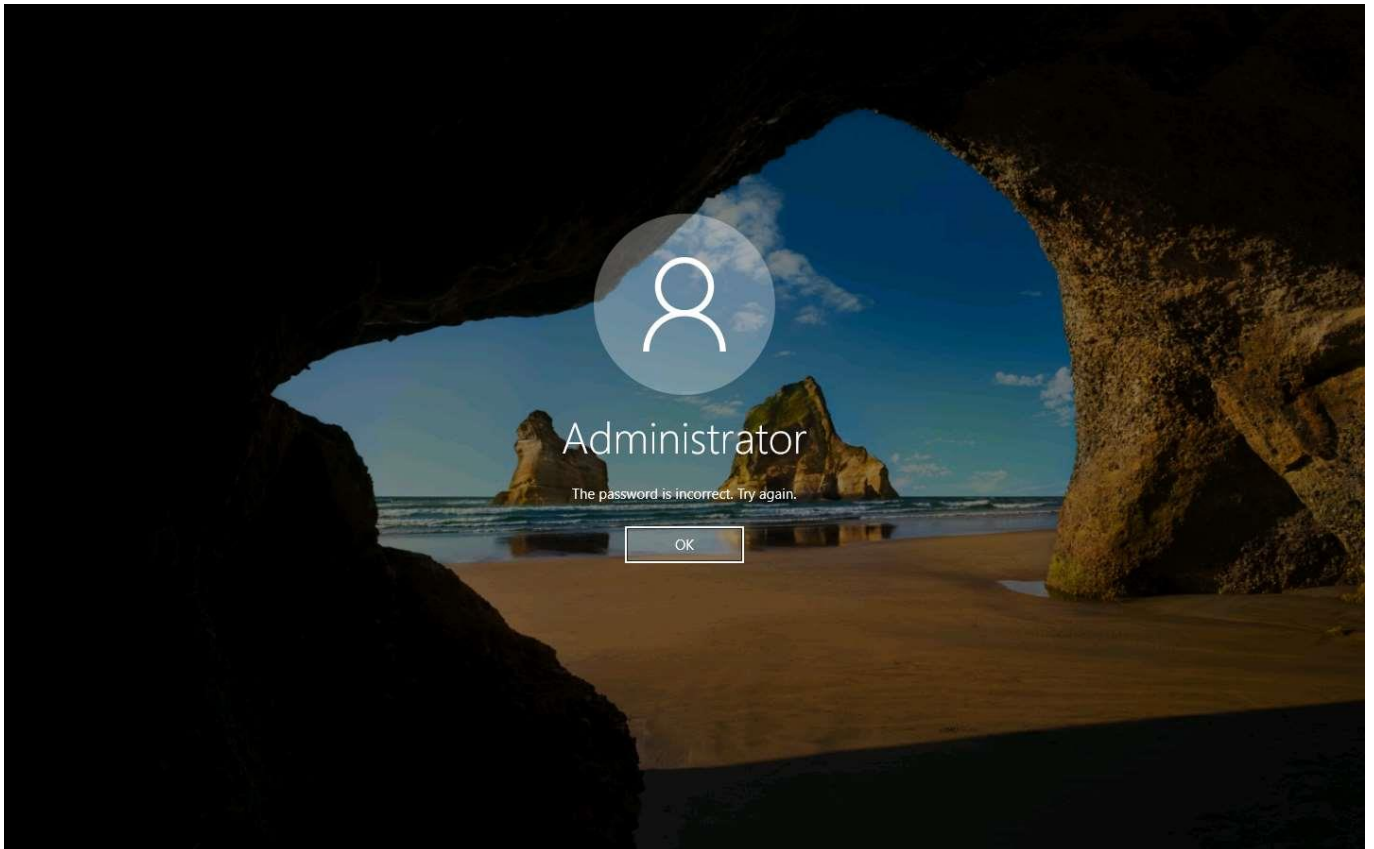


19. ☐ Once you have executed the virus, the **Desktop** screen goes blank, indicating that the virus has infected the system, as shown in the screenshot.

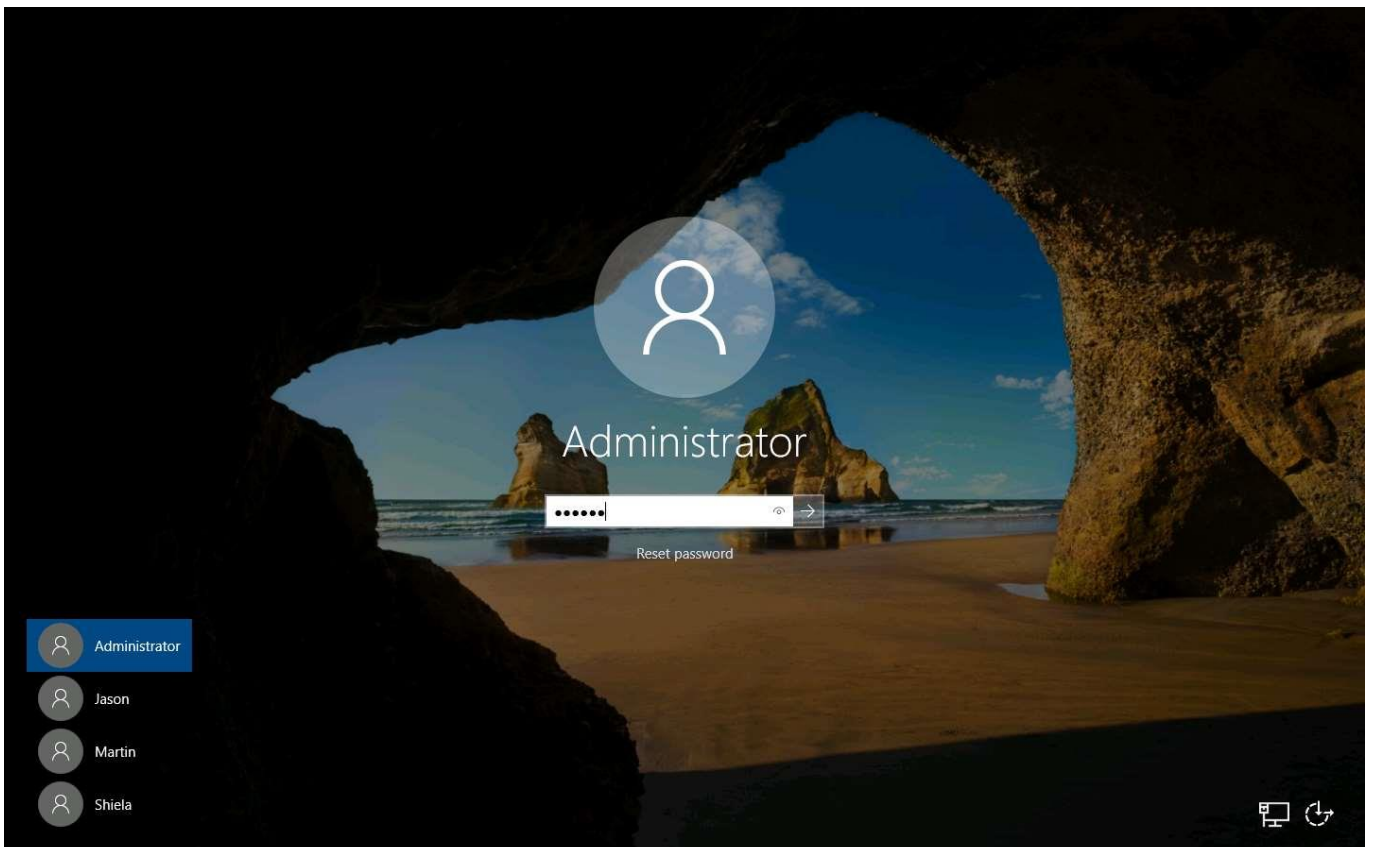


20. ☐ Surprised by the system behavior, the victim (you) attempts to fix the machine by restarting it. Once the machine has rebooted, try to log in to the machine with the provided **Username** and **Password**. You should receive the error message "the password is incorrect. Try again."

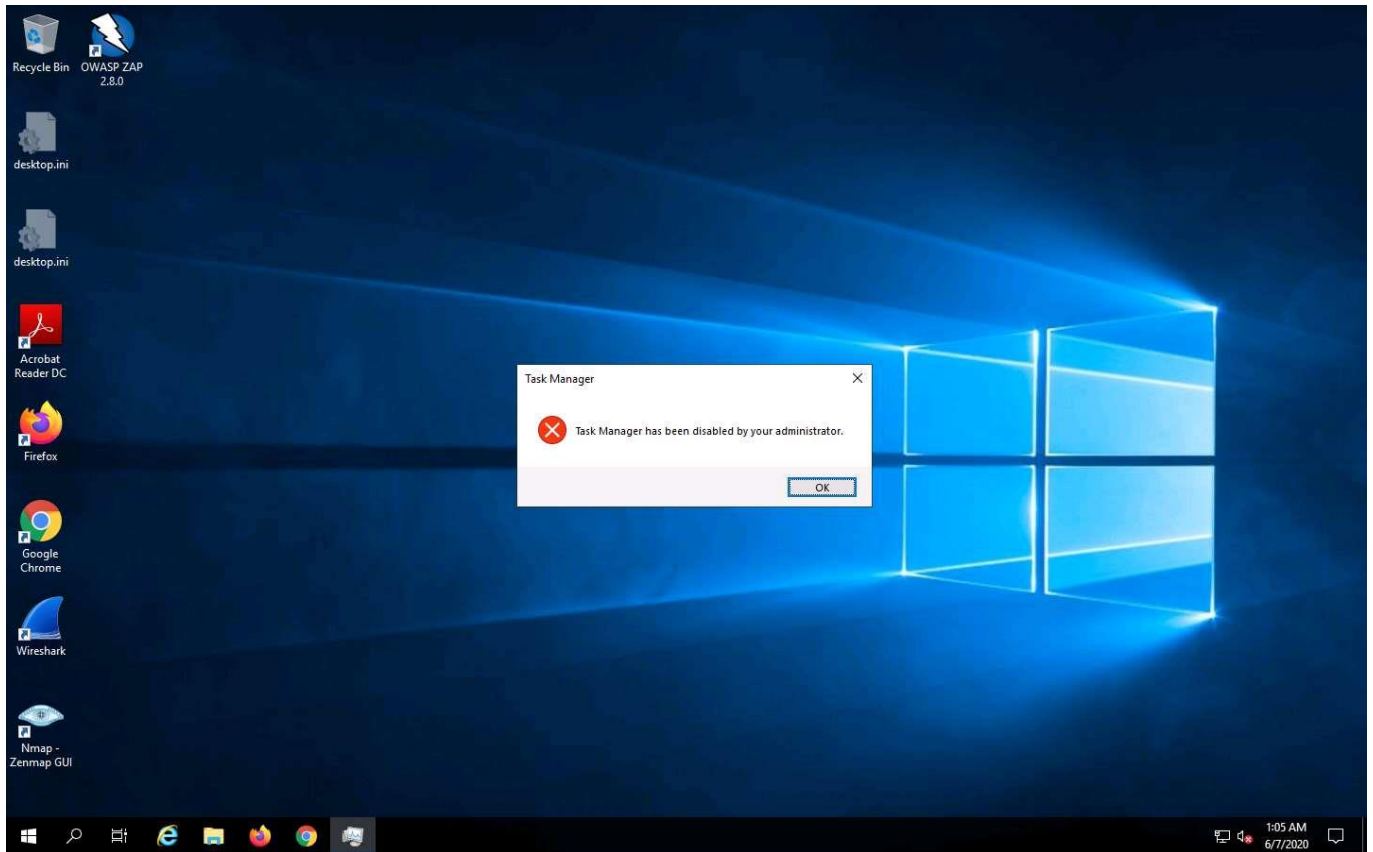
21. ☐ Click [Ctrl+Alt+Delete](#) to activate the machine, by default, **Administrator** account is selected, click **Pa\$\$w0rd** to enter the password and press **Enter**.



22. ☐ Now, 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**.



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.