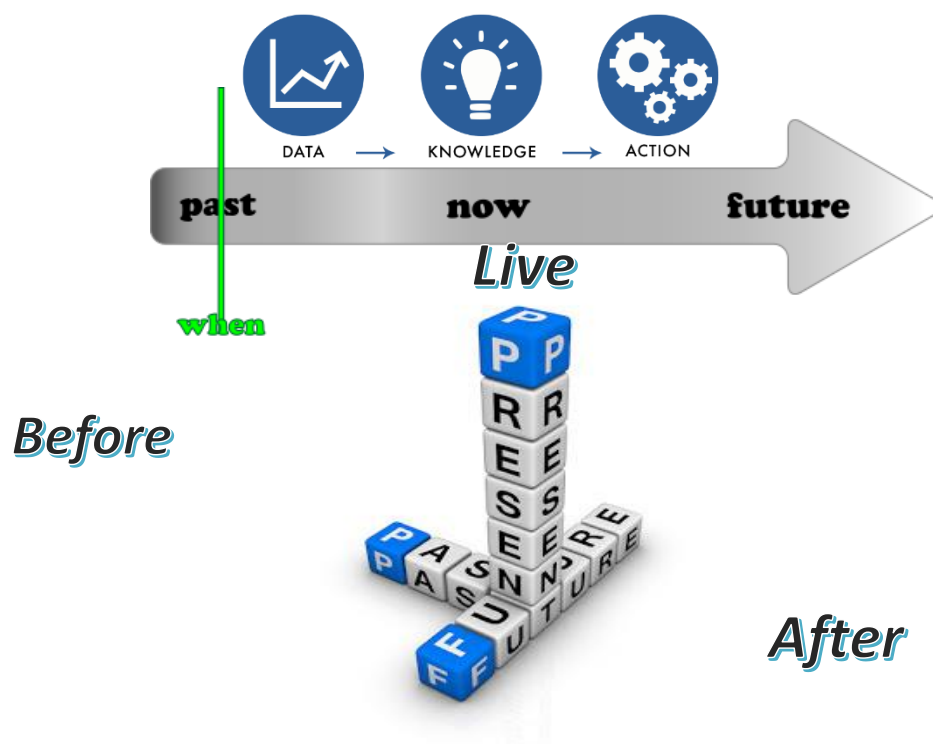




Ethical Hacking (ACCA7033)

Malware Analysis



Lab Activities are based on **EC Council – CEH Curriculum**

Objectives

In continuation to our earlier lectures, this tutorial helps in providing you insights to create malware, trojan, virus to exploit, infect the target machine. Continue further to analyse the malware to determine its origin, functionality and potential impact of the available malware.

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should contact me prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

* This LAB is adopted from EC Council's Malware Analysis Lab

Task 1: Gain access to the Target System using Trojans
Task 2: Hide a Trojan using SwayzCryptor and make it undetectable to various anti-virus programs
Task 3: Detect Trojan and Backdoor Attacks
Task 4: Creating a Virus

ICONS Used in this document:



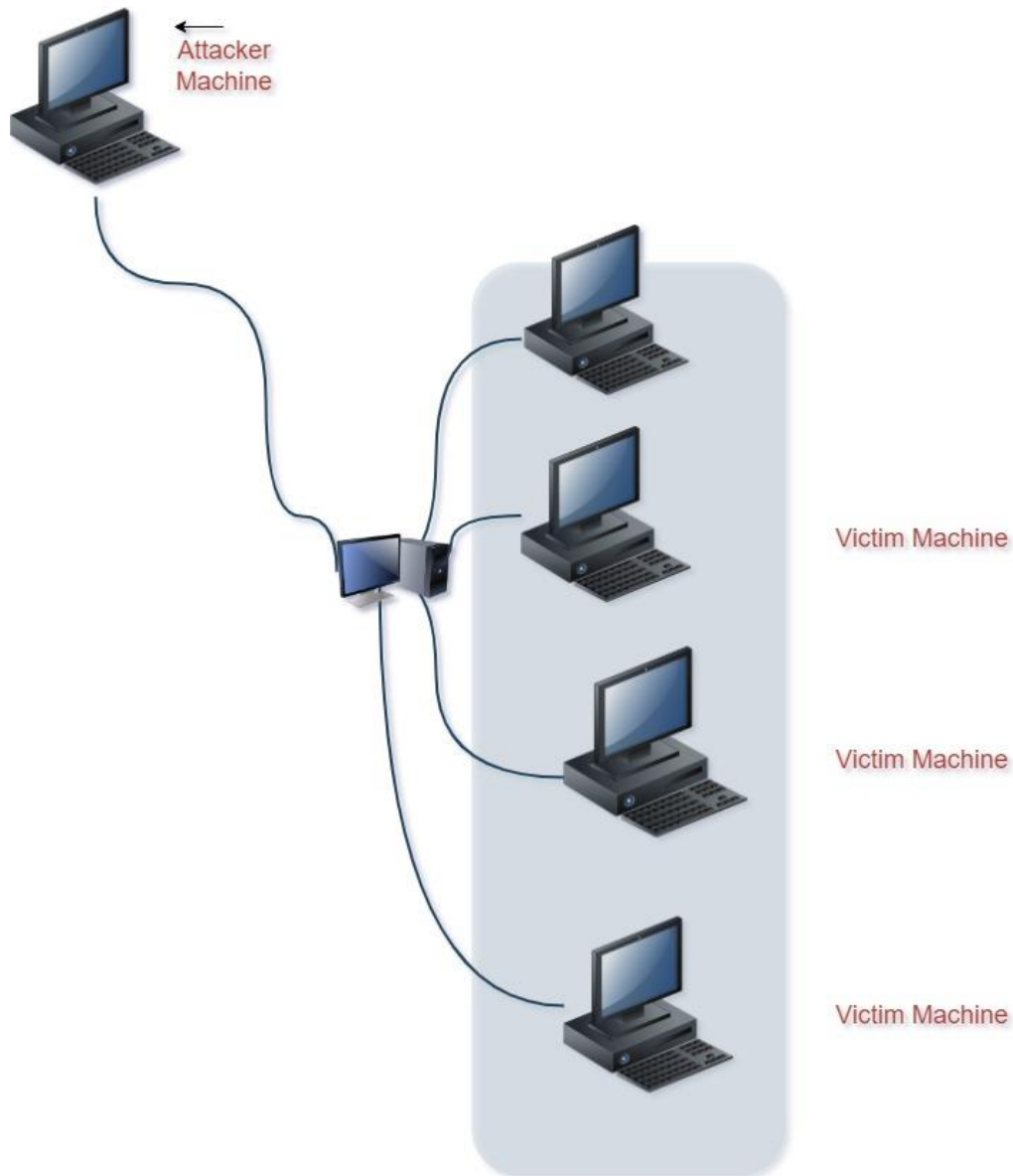
Find out the outcome/ Answers/ Solution/ Discussion via Forum



Do research and complete the task. Need referencing/ in-text citations. Shall be included as a part of your coursework.

Lab Topology

Guide to Setup
your Lab



- **Attacker Machines:** *Kali Linux, Parrot, Ubuntu (It's your Choice)*
- **Victim Machines:** *Combination of Win 10, 11, Win Server 2019, 22, Linux (CentOS, Debian), bee-box v1.6*
- **Web Servers:** DVWA, Good Shopping etc

Scenario

Attackers use digital Trojan horses to trick the victim into performing a predefined action on a computer. Trojans are activated upon users' specific predefined actions, like unintentionally installing a piece of malicious software or clicking on a malicious link, and upon activation, it can grant attackers unrestricted access to all data stored on compromised information systems and cause potentially immense damage. For example, users could download a file that appears to be a movie, but, when opened, it unleashes a dangerous program that erases the hard drive or sends credit card numbers and passwords to the attacker. Trojan horses work on the same level of privileges as victims. For example, if a victim has the privileges to delete files, transmit information, modify existing files, and install other programs (such as programs that provide unauthorized network access and execute privilege elevation attacks), once the Trojan infects that system, it will possess the same privileges. Furthermore, it can attempt to exploit vulnerabilities to increase its level of access, even beyond the user running it. If successful, the Trojan could use the increased privileges to install other malicious code on the victim's machine. An expert security auditor or ethical hacker needs to ensure that the organization's network is secure from Trojan attacks by finding machines vulnerable to these attacks and making sure that anti-virus tools are properly configured to detect such attacks. The lab tasks in this exercise demonstrate how easily hackers can gain access to the target systems in the organization and create a covert communication channel for transferring sensitive data between the victim computer and the attacker.

Use Windows 10/ 11, Server 2022 with Admin Privileges

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.

Note: This lab is configured with Windows 11 (10.10.1.11) machine as the attacker machine and the Windows Server 2022 (10.10.1.22) machine as the victim machine.

1. Turn on the Windows 11 and Windows Server 2022 virtual machines.
2. Switch to the Windows 11 virtual machine, click Ctrl+Alt+Del.
3. Navigate to our lecture resources to download njRAT.exe
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 task, 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 11 (attacker machine) machine in the Host field, check the option Registry StartUp, leave the other settings to default, and click Build.
Note: In this task, the IP address of the Windows 11 machine is 10.10.1.11.
8. The Save As window appears; specify a location to store the server, rename it, and click Save.
9. In this lab, the destination location chosen is Desktop, and the file is named Test.exe.
10. Once the server is created, the DONE! pop-up appears; click OK.
11. Now, use any technique to send this server to the intended target through email or any other source (in real-time, attackers send this server to the victim).
12. Switch to the Windows Server 2022 virtual machine, assuming, that the file test.exe is sent to the Server 2022
13. Double-click the server (Test.exe) to run this malicious executable.
14. Switch back to the Windows 11 virtual machine.
15. Maximize njRAT GUI window. As soon as the Test.exe is executed, the executable starts running and the njRAT client (njRAT GUI) running in Windows 11 establishes a persistent connection with the victim machine
16. Unless the attacker working on the Windows 11 machine disconnects the server on their own, the victim machine remains under their control.
17. The GUI displays the machine's basic details such as the IP address, User name, and Type of Operating system.
18. Right-click on the detected victim name and click Manager.
19. The manager window appears with File Manager selected by default.

20. 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.
21. 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.
22. 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.
23. Click on Registry, choose a registry directory from the left pane, and right-click on its associated registry files.
24. A few options appear for the files; you can use these to manipulate them.
25. Click Remote Shell. This launches a remote command prompt for the victim machine (Windows Server 2022).
26. In the text field present in the lower section of the window, type the command `ipconfig/all` and press Enter. This displays all interfaces related to the victim machine, as shown in the screenshot.
27. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine.
28. 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.
29. Close the Manager window.
30. Right-click on the victim name, and then select Remote Desktop.
31. This launches a remote desktop connection without the victim's awareness.
32. A Remote Desktop window appears; hover the mouse cursor to the top-center area of the window. A down arrow appears; click it. Note: It might take a while for the screen to appear.
33. A remote desktop control panel appears; check the Mouse option.
34. Now, you will be able to remotely interact with the victim machine using the mouse.
Note: If you want to create any files or write any scripts on the victim machine, you need to check the Keyboard option.
35. In the same way, right-click on the victim name, and select Remote Cam and Microphone to spy on them and track voice conversations.
36. Switch to the Windows Server 2022 virtual machine. Assume that you are a legitimate user and perform a few activities such as logging into any website or typing some text in text documents.
37. Switch back to the Windows 11 virtual machine, right-click on the victim name, and click Keylogger.
38. The Keylogger window appears; wait for the window to load.
39. The window displays all the keystrokes performed by the victim on the Windows Server 2022 machine.

40. Right-click on the victim name, and click Open Chat. A Chat pop-up appears; enter a nickname and click OK. A chat box appears; type a message, and then click Send.
41. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (Windows Server 2022)
42. Switch to the Windows Server 2022 virtual machine, you can observe the message from the hacker appears on the screen.
43. Try to close the chat from the victim machine. Irrespective of what you do, the chatbox remains for open as long as the attacker uses it.
44. Try to break the connection by restarting the machine.
45. As soon as this happens, njRAT loses its connection with Windows Server 2022, as the machine is shut down in the process of restarting.
46. Switch back to the attacker machine (Windows 11); you can see that the connection with the victim machine is lost. However, as soon as the victim logs in to their machine, the njRAT client automatically establishes a connection with the victim.
47. This concludes the demonstration of how to create a Trojan using njRAT Trojan to gain control over a victim machine. Close all open windows in all machines.

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. Switch to the Windows 11 virtual machine, open any web browser and open <https://www.virustotal.com>.
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 task (Desktop), select it, and click Open.
4. The VirusTotal uploads the file, scans it with the various anti-virus programs in its database. After the completion of the scan, the scan result appears.
5. Do you see any detection?
6. Go to appropriate website and download SwayzCryptor tool.T
7. Click ellipses icon below File to select the Trojan file. The Select a File dialog-box appears; navigate to the location of Test.exe (Desktop), select it, and click Open.
8. Once the file is selected, check the options Start up, Mutex, and Disable UAC, and then click Encrypt.
9. The Save File dialog-box appears; select the location where you want to store the crypted file, leave the file name set to its default (CryptedFile), and click Save.
10. Once the encryption is finished, click Close.
11. Maximize the web browser. In the VirusTotal analysis page, click the Upload file icon in the top-right corner of the page.
12. An Open dialog-box appears; navigate to the location where you saved the encrypted file CryptedFile.exe (Desktop), select the file, and click Open.
13. VirusTotal uploads the file and begins to scan it with the various anti-virus programs in its database. After the completion of the scan, the scan result appears.
14. What is the outcome now? Is there any difference between the previous scan and this scan?
15. Get the njRAT v0.7d.exe file from Lecturer resources and launch njRAT by choosing the default port number 5552, and then click Start.
16. In this exercise, we have already created a crypted file (CryptedFile.exe), built using njRAT.
17. 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).
18. Switch to the Windows Server 2022 virtual machine.
19. Double-click CryptedFile.exe to run this malicious executable.
20. As soon as you double-clicks the server, the executable starts running, and the njRAT client (njRAT GUI) running on the Windows 11 machine establishes a persistent connection with the victim machine.
21. Switch to the Windows 11 virtual machine and in the njRAT window you can observe that the connection has been established with the victim machine.
22. Unless the attacker working on the Windows 11 machine disconnects the server on their own, the victim machine remains under their control.
23. 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.

24. On completion of this lab, switch to the Windows Server 2022 virtual machine, launch Task Manager, click on More details and look for the server.exe (32 bit) process, and click End task on the Windows Server 2022 machine.
25. This concludes how to hide a Trojan using SwayzCryptor to make it undetectable to various anti-virus programs.

Task 3: Detect Trojan and Backdoor Attacks

ProRat is a Remote Administration Tool written in C programming language and capable of working with all Windows operating systems.

Machines Required: Windows 10 and Windows Server 2019

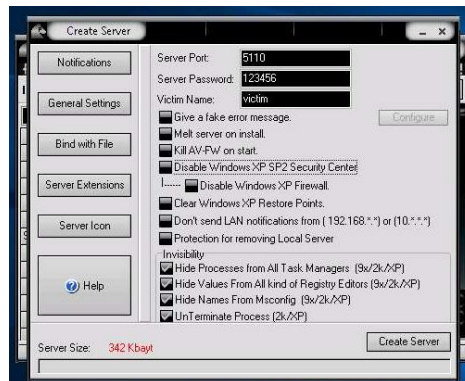
Tools Required: ProRat Server

1. Login to Windows 10
2. To launch ProRAT, download Prorat.exe for appropriate website or from the Lecture's resource folder.
3. If an Open File - Security Warning pop-up appears, click Run.
4. ProRat main window appears, click Create. Click Create ProRat Server (342 Kbayt) to create a ProRat server.



5. Create Server window appears. In Notifications leave the settings to default.
6. Click on General Settings button to configure features such as Server Port, Server Password, Victim Name, and the port number. In this lab, default settings are chosen. Note down the Server password.

7. Uncheck the options, as shown in the screenshot.



8.

9. Click Bind with file button to bind sever with a file. In this lab, we are using .jpg file to bind the server. Check Bind server with a file option, click Select File button, and Select any image of your choice, and click Open to bind the file.
10. A pop-up displays the prompt: ProRat server will bind with MyCar.jpg. Click OK.
11. Click Server Extensions. Under Select Server Extension, check EXE (Has icon support).
12. Click Server Icon. Under Server Icon, select any icon, and click Create Server.
13. A pop-up states that the server has been created. Click OK.
14. Check the file where the created server is saved in. This server is named binded_server by default. Close the Create Server window of the ProRat.
- (In real time, hackers may craft such servers and send them by mail or any communication media to the victim's machine.)*
15. You need to zip the file before mailing it, as you cannot attach .exe files on some mail servers.
16. Click Windows Server 2019.
17. To execute the Trojan, use your own method to place the file (.exe) in the Server.
18. If the Open File - Security Warning pop-up appears, click Run. Leave the Windows Server 2019 machine running.
19. Click Windows 10, and enter the IP address of Windows Server 2019; keep the default port number in the ProRat main window, and click Connect.
20. In this lab IP address of the Windows Server 2019 is 10.10.10.12.
21. Enter the password you noted down at the time of creating Server and click OK.
22. Now you are connected to the victim machine. ProRat begins to monitor the user activities. It records all passwords, keystrokes, and so on.
23. To test the connection, click PC Info, and choose System Information. ProRat displays the information of the victim machine, as shown in the screenshot.
24. Click on Keylogger to steal user passwords for the online system. KeyLogger window appears, leave the Keylogger window running.
25. Click Windows Server 2019, or Notepad, and type any text

26. Click Windows 10 machine, click Read Log button in the Keylogger window. To record the keystrokes of the victim machine. Close the keylogger window.
27. Now click the Registry button to view registry editor of the Windows Server 2012 machine.
28. Registry Editor window appears, where you can choose the Registry Editor from the Root Key: drop-down list and you can see and also modify the registry of the victim's machine as shown in the screenshot.
29. Close the Registry related windows, and switch back to the main window of the ProRat. In the same way, you can make use of the other options that allow you to explore and control the victim machine.

In this lab you have learnt how to

Creating a server and testing the network for attack
Attacking a network using sample Trojans and
documenting all vulnerabilities and flaws detected

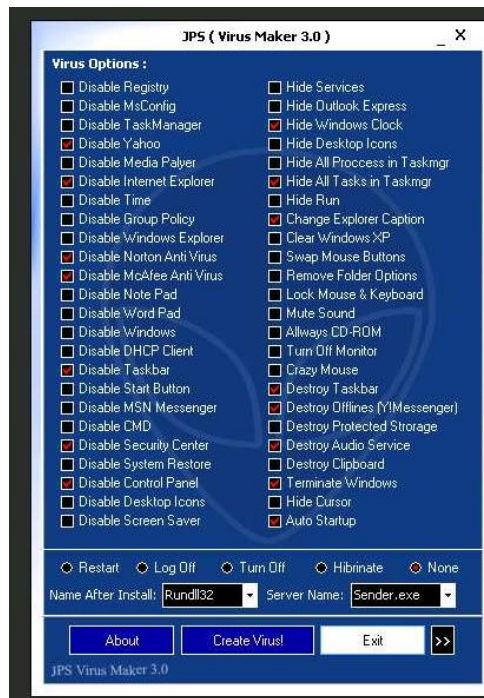
Task 4: Creating a Virus

Machines Required: Windows 10 and Windows Server 2019

Tools Required: JPS Virus Maker Tool

JPS Virus Maker tool is used to create the own customized virus. There are many options in build in this tool which can be used to create the virus. Some of the features of this tool are auto start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows.

1. Click Windows Server 2019
2. To launch JPS (Virus Maker), use appropriate web resource to download the Virus Maker.
3. If an Open File - Security Warning pop-up appears, click Run.
4. The JPS (Virus Maker 3.0) virus maker main window appears. The window displays various features/options that can be chosen while creating a virus file.
5. JPS lists the Virus Options; check the options that you want to embed in a new virus file.
6. In this lab, the options embedded in the virus file are Disable Yahoo, Disable Internet Explorer, Disable Norton Anti Virus, Disable McAfee Anti Virus, Disable Taskbar, Disable Security Center, Disable Control Panel, Hide Windows Clock, Hide All Tasks in Taskmgr, Change Explorer Caption, Destroy Taskbar, Destroy Offlines (Y!Messenger), Destroy Audio Service, Terminate Windows and Auto Startup.



7. Click a radio button to specify when the virus should start attacking the system after its creation.
8. From the Name after Install drop-down list, choose the name of the service you want the virus to mimic.
9. Choose a server name for the virus from the Server Name drop-down list. Now, before clicking on Create Virus!, click >> icon to configure the virus options.
10. A Virus options window appears. Check the Change XP Password option, and enter a password in the text field. Check Change Computer Name option, and type Test in the text field. Check Change IE Home Page option, and type www.moviescope.com 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.
12. For the worm to self-replicate after a particular time period, specify the time (in seconds; here, 1 second) in the Copy after field.
13. Select JPG Icon radio button in the Change Icon section, and click Restart radio button, in the lower part of the window.
14. After completing your selection of options, click on Create Virus!.
15. A pop-up window states: Server Created Successfully.... Click OK. The newly created virus (server) is placed automatically in the folder where jps.exe is located, but with the name Svchost.exe.
16. Now, pack this virus with a binder or virus packager, and send it to the victim machine through emails, chats, mapped network drives, and so on.
17. Try to install this in the victim machine (Note: This needs to be practised only within the Simulated – Virtual Environment)
18. Observe the behavior of the virus.

- 19. As an Ethical Hacker, what are your proposed mitigation strategies to overcome this kind of malware attacks?**
- 20. Present your mitigation strategies with adequate demonstration. Record a video demonstrating the attack and its mitigation and share the link.**

Record your Reflection:



1. Understanding on all the activities
2. Understanding about various tools used
3. New/ Similar tools you identified and used
4. Compare and Contrast the tutorial tools with your identified tools
5. Any other Troubleshooting Steps, you need to share?
6. Rate yourself: How confident are you to analyse any malware in your network?
What measures do you take to overcome/ mitigate such attacks

-----End of Activity 4 -----