Lab 4: Perform Dynamic Malware Analysis

Lab Scenario

Dynamic Malware Analysis, also known as behavioral analysis, involves executing malware code to learn how it interacts with the host system and its impact after infecting the system.

Dynamic analysis involves the execution of malware to examine its conduct and operations and identify technical signatures that confirm the malicious intent. It reveals information such as domain names, file path locations, created registry keys, IP addresses, additional files, installation files, and DLL and linked files located on the system or network.

This type of analysis requires a safe environment such as machines and sandboxes to deter the spreading of malware. The environment design should include tools that can capture every movement of the malware in detail and give feedback. Typically, systems act as a base for conducting such experiments.

An ethical hacker and pen tester must perform dynamic malware analysis to find out about the applications and processes running on a computer and remove unwanted or malicious programs that can breach privacy or affect the system's health.

Lab Objectives

- Perform port monitoring using TCPView and CurrPorts
- Perform process monitoring using Process Monitor

Overview of Dynamic Malware Analysis

Dynamic analysis is performed to gather valuable information about malware activity, including the files and folders created, ports and URLs accessed, called functions and libraries, applications and tools accessed, information transferred, settings modified processes, and services the malware started, and other items. You should design and set up the environment for performing the dynamic analysis in such a way that the malware cannot propagate to the production network, and ensure that the testing system can recover to an earlier set timeframe (prior to launching the malware) in case anything goes wrong during the test.

To achieve this, you need to perform the following:

- **System Baselining** Baselining refers to the process of capturing a system's state (taking snapshot of the system) at the time the malware analysis begins. This can be used to compare the system's state after executing the malware file, which will help understand the changes that the malware has made across the system. A system baseline involves recording details of the file system, registry, open ports, network activity, and other items.
- **Host Integrity Monitoring** Host integrity monitoring is the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents. It involves using the same tools to take a snapshot of the system before and after the incident or actions and analyzing the changes to evaluate the malware's impact on the system and its properties. In malware analysis, host integrity monitoring helps to understand the runtime behavior of a

malware file as well as its activities, propagation techniques, URLs accessed, downloads initiated, and other characteristics.

Host integrity monitoring includes:

- Port monitoring
- Process monitoring
- Registry monitoring
- Windows services monitoring
- Startup program monitoring
- Event logs monitoring and analysis
- Installation monitoring
- Files and folder monitoring
- Device driver monitoring
- Network traffic monitoring and analysis
- DNS monitoring and resolution
- API calls monitoring

Task 1: Perform Port Monitoring using TCPView and CurrPorts

We know that the Internet uses a software protocol named TCP/IP to format and transfer data. Malware programs corrupt the system and open system input and output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks. These open ports can also act as backdoors or communication channels for other types of harmful malware and programs. They open unused ports on the victim's machine to connect back to the malware handlers.

You can identify the malware trying to access a particular port by installing port monitoring tools such as TCPView and CurrPorts.

TCPView TCPView is a Windows program that shows the detailed listings of all the TCP and UDP endpoints on the system, including the local and remote addresses, and the state of the TCP connections. It provides a subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.

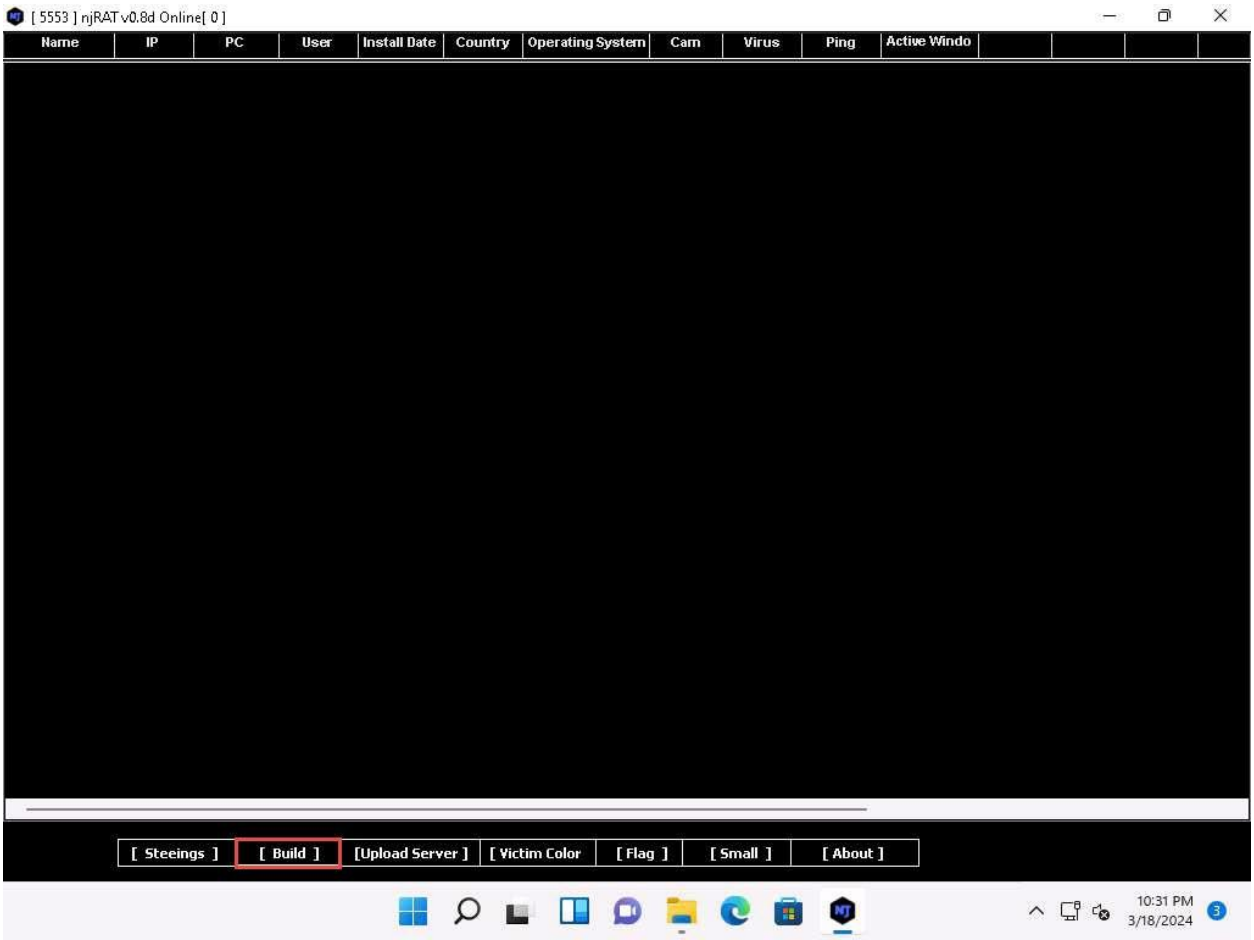
CurrPorts CurrPorts is a piece of network monitoring software that displays a list of all the currently open TCP/IP and UDP ports on a local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, etc.), the time that the process was created, and the user that created it.

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP port information to an HTML file, XML file, or to tab-delimited text file.

CurrPorts also automatically marks suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons) in pink.

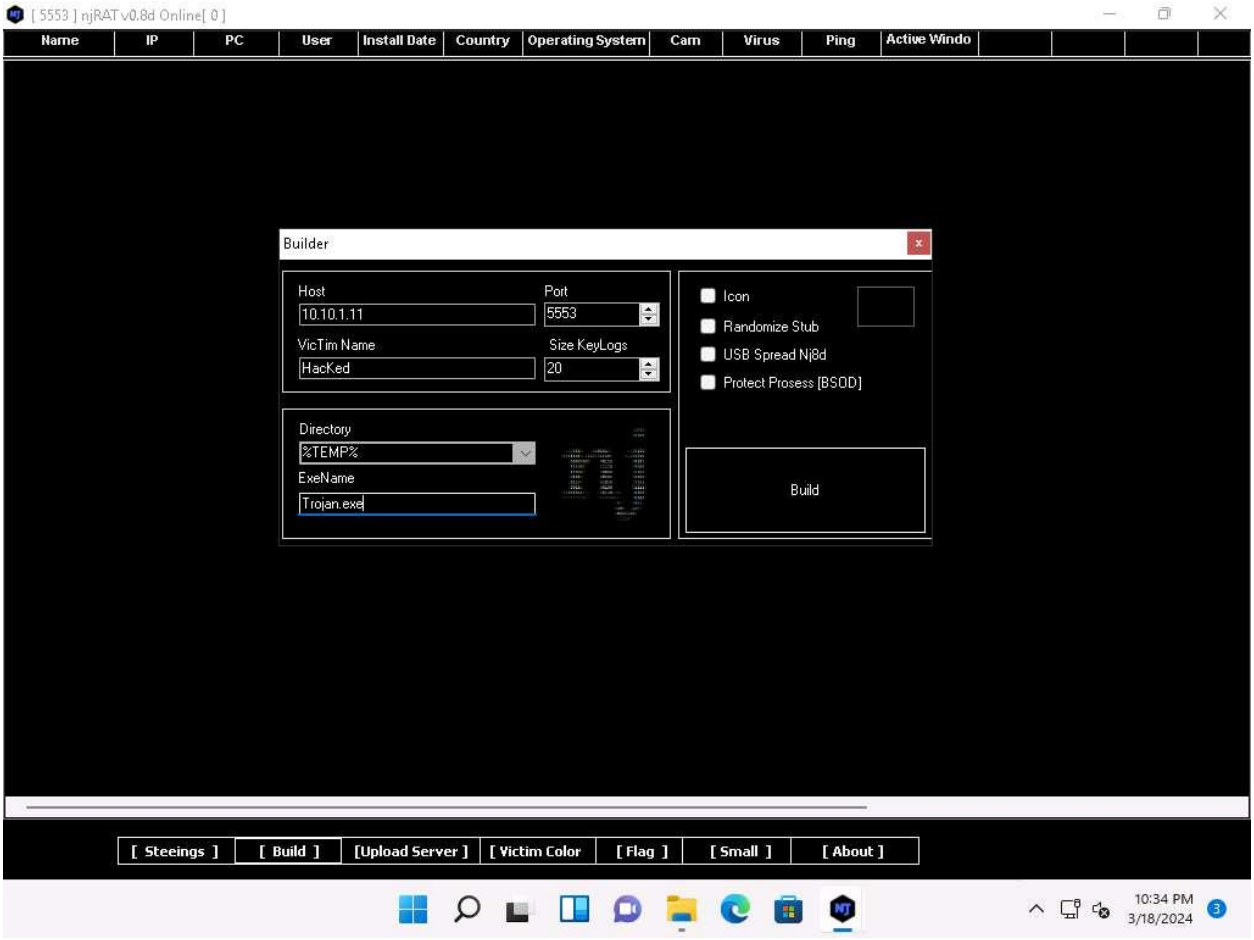
This lab activity demonstrates how to analyze malicious processes running on a machine using TCPView and CurrPorts. Here, you will first create a server using njRAT, and then execute this server from the second machine. Later, you will run the TCPView and CurrPorts applications on the second machine and find that the process associated with the server is running on it.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.8d.exe** to launch **njRAT**.
2. A **[Port Now]** pop-up appears, leave the port number to default and click on **OK**.
3. The njRAT GUI appears; click the **Build** link located in the lower-left corner of the GUI to configure the exploit details.

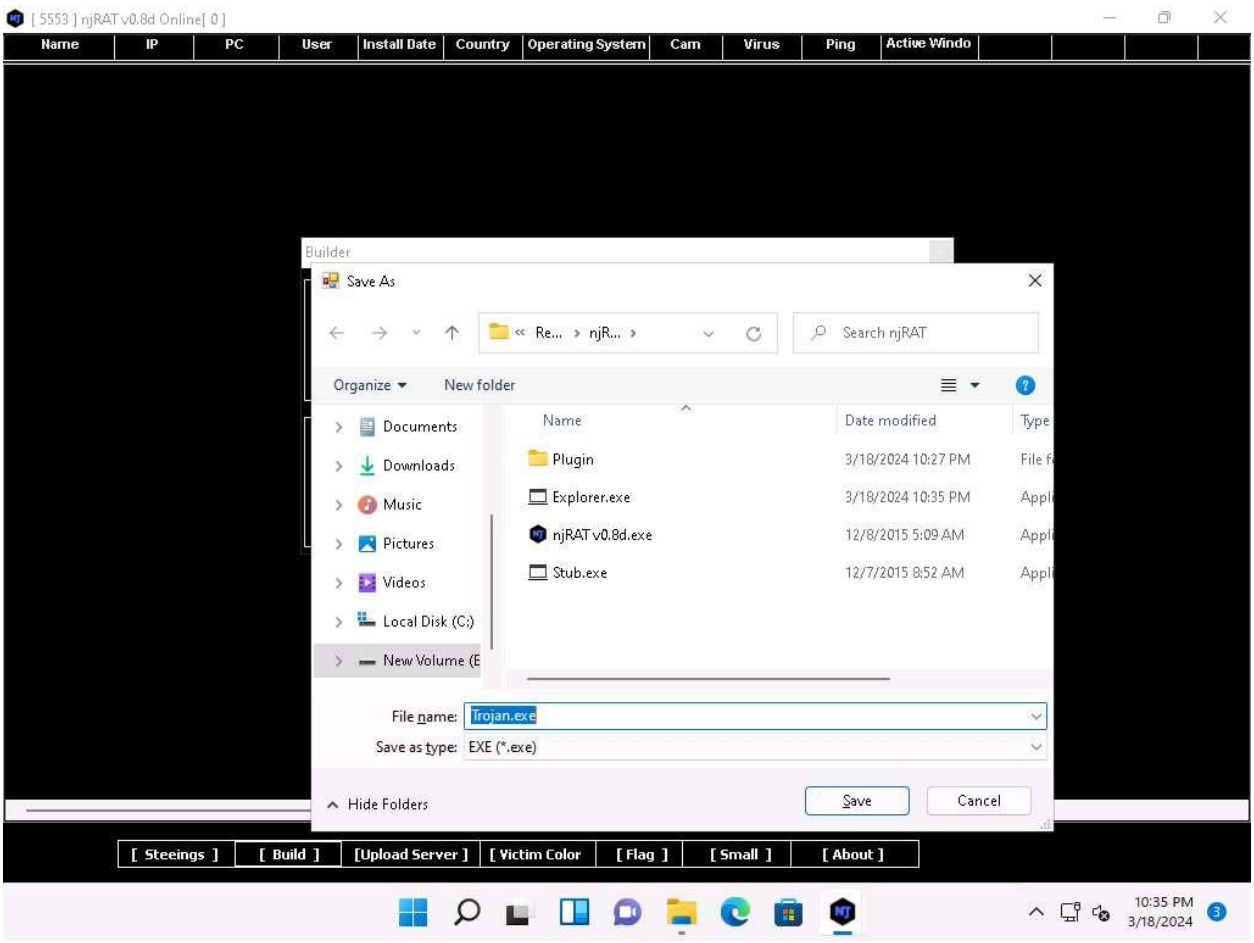


4. The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, rename **ExeName** as **Trojan.exe**. Leave the other settings to default, and click **Build**.

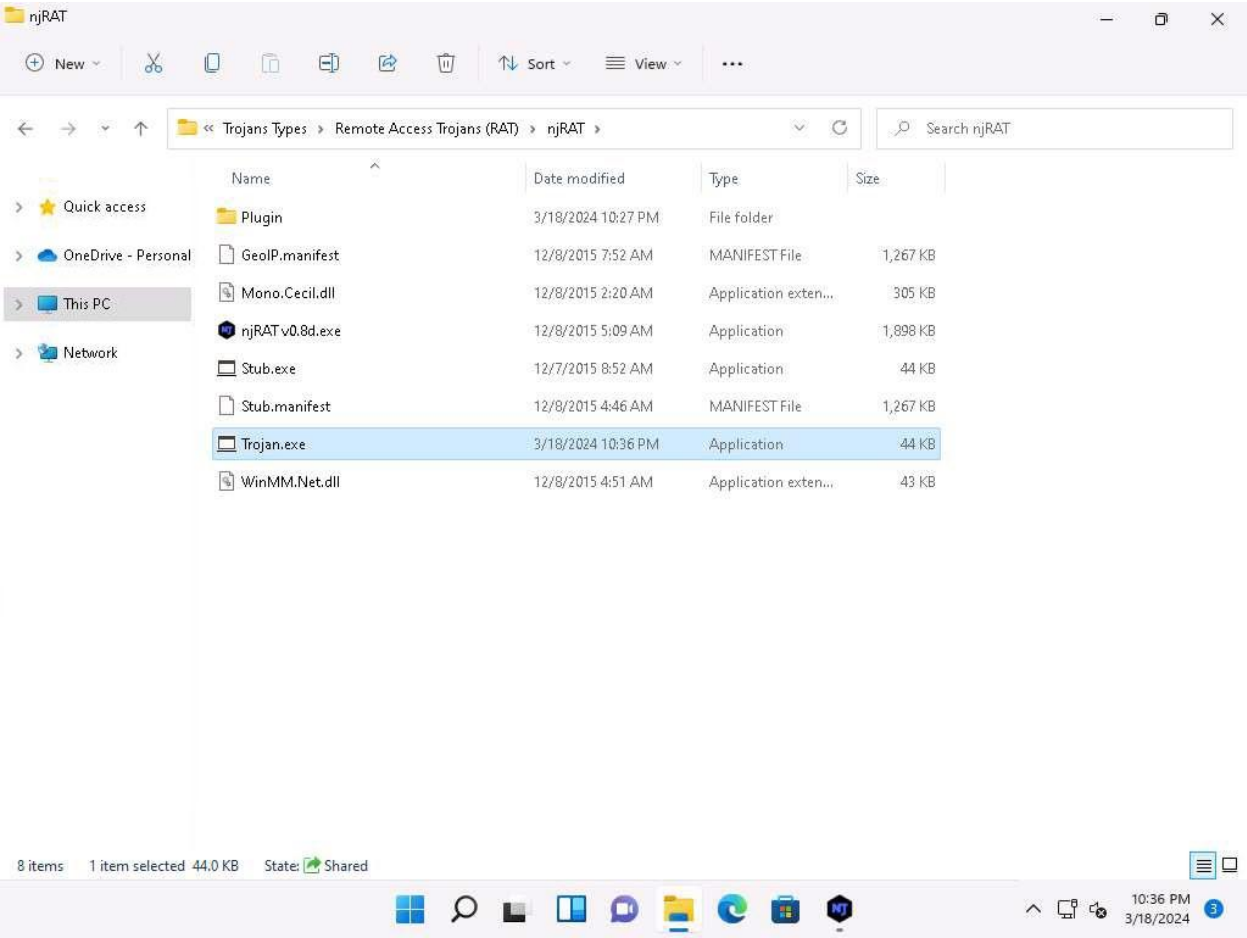
In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.



5. **Save As** window appears, **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**. In the **File name**, enter **Trojan.exe** and click **Save**. **Done!** pop-up appears, click **OK**.



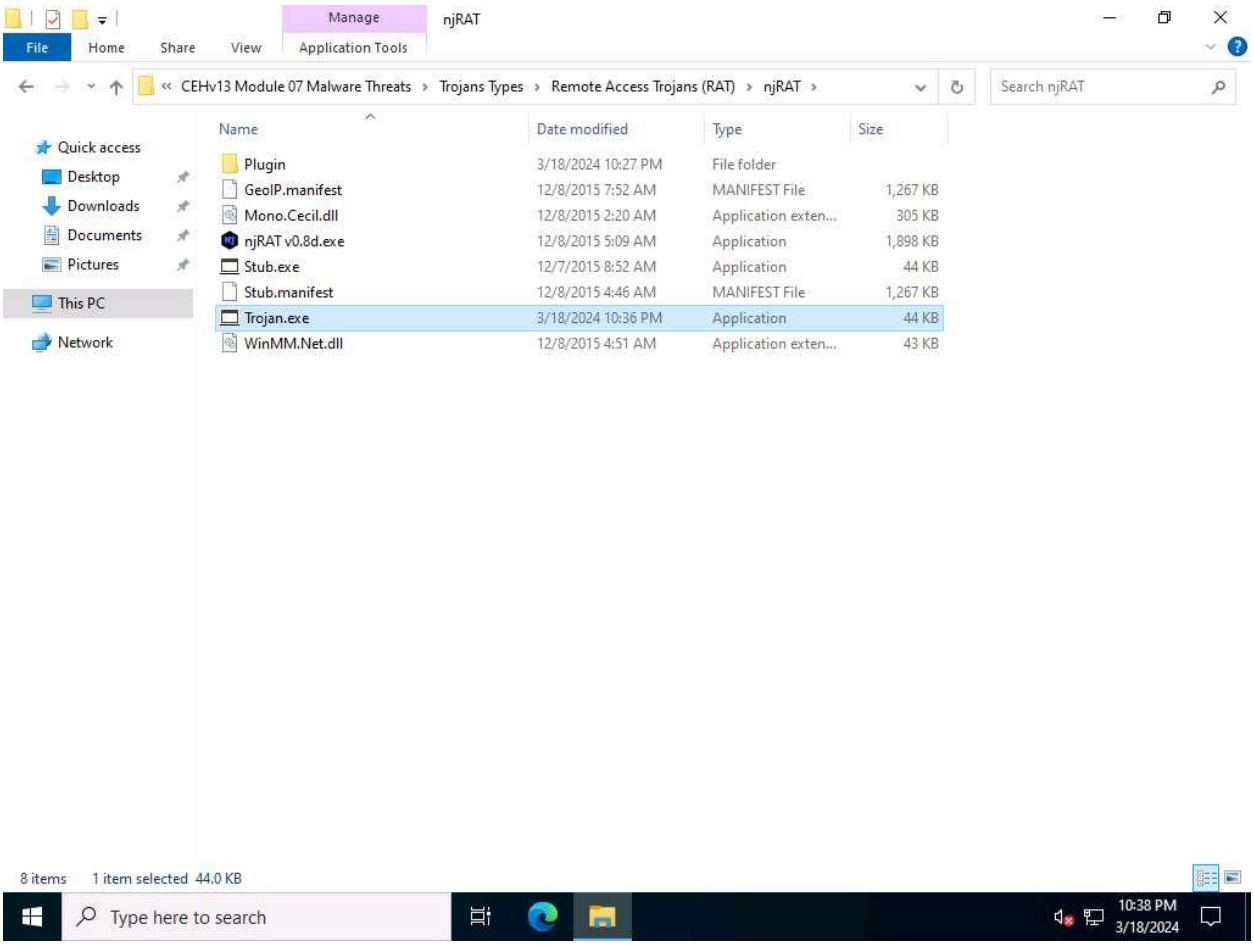
6. Minimize njRAT window. You can observe that a **Trojan.exe** file has been created at the location **E:\CEH-Tools\CEHv13 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.



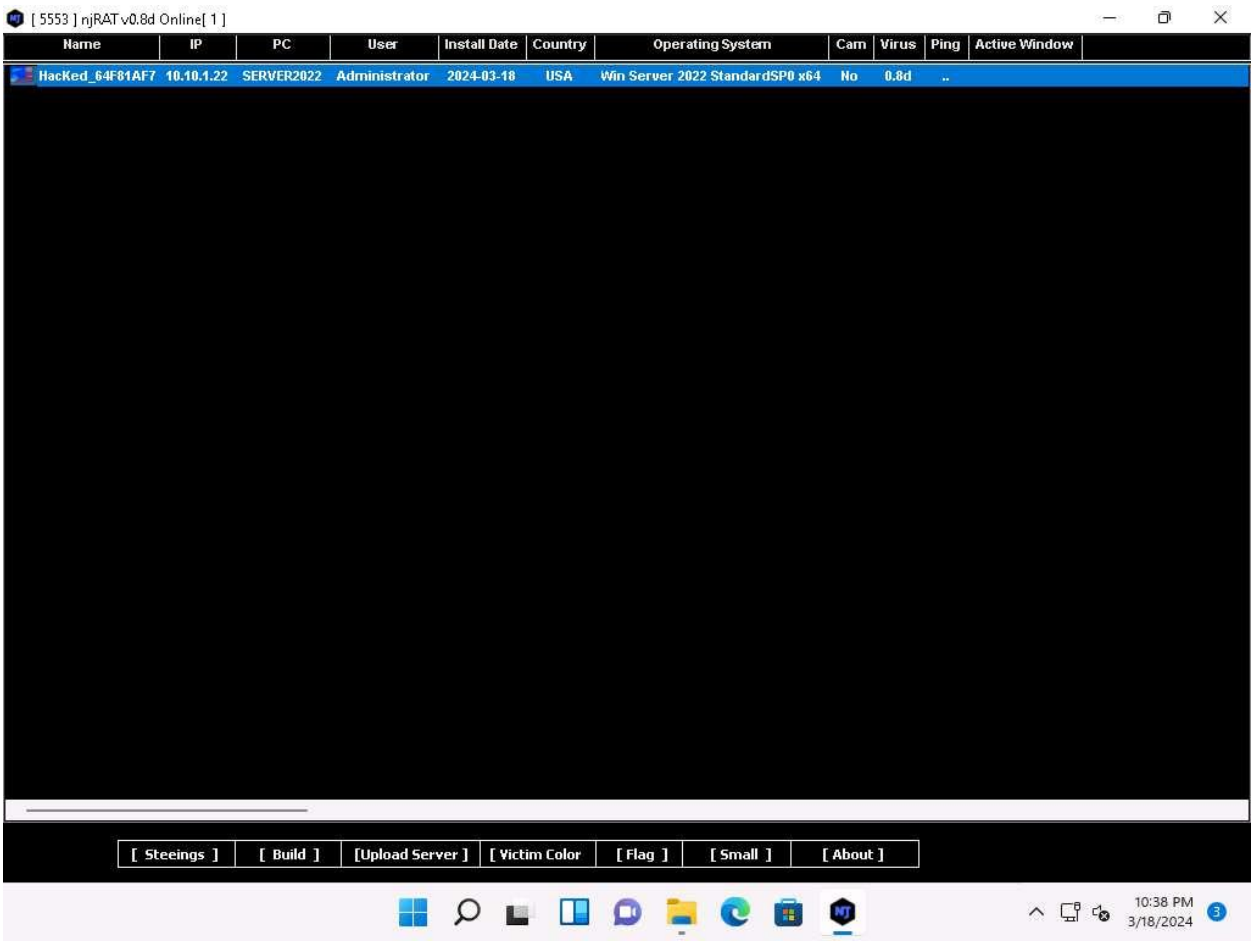
7. Click Windows Server 2022 to switch to the **Windows Server 2022** machine.
   Click Ctrl+Alt+Delete to activate the machine, login with **CEH\Administrator/Pa$$w0rd**.

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

8. Navigate to **Z:\CEHv13 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe**.

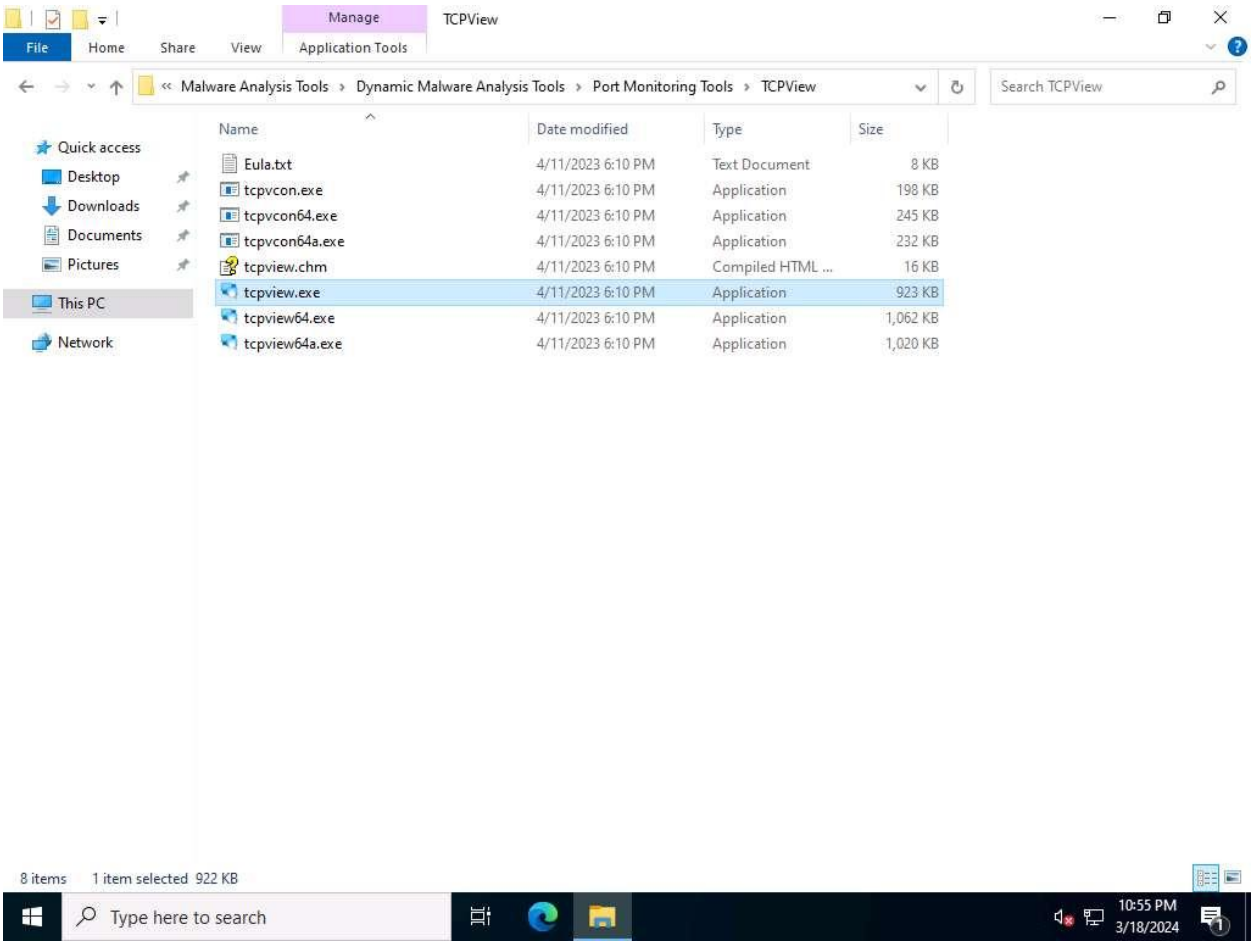


9. Observe that a connection has been established by the njRAT client. Click Windows 11 to switch to the **Windows 11** machine. Switch to **njRAT** window to observe the established connection.

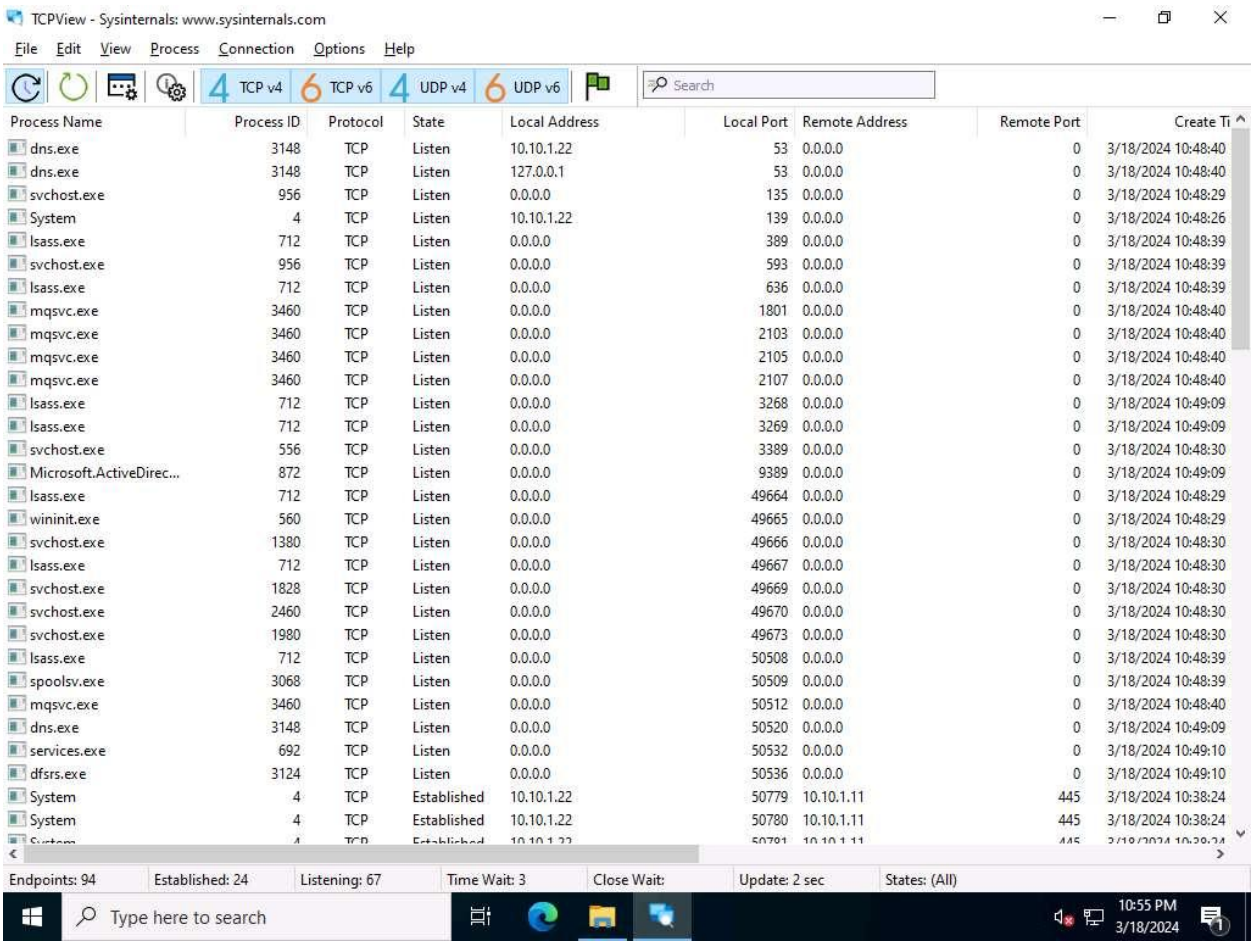


10. Now, let us analyze this process on **Windows Server 2022** using **TCPView** tool. Click Windows Server 2022 to switch back to the **Windows Server 2022** machine.
11. Navigate to **Z:\CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView** and double-click **tcpview.exe** to launch the application.

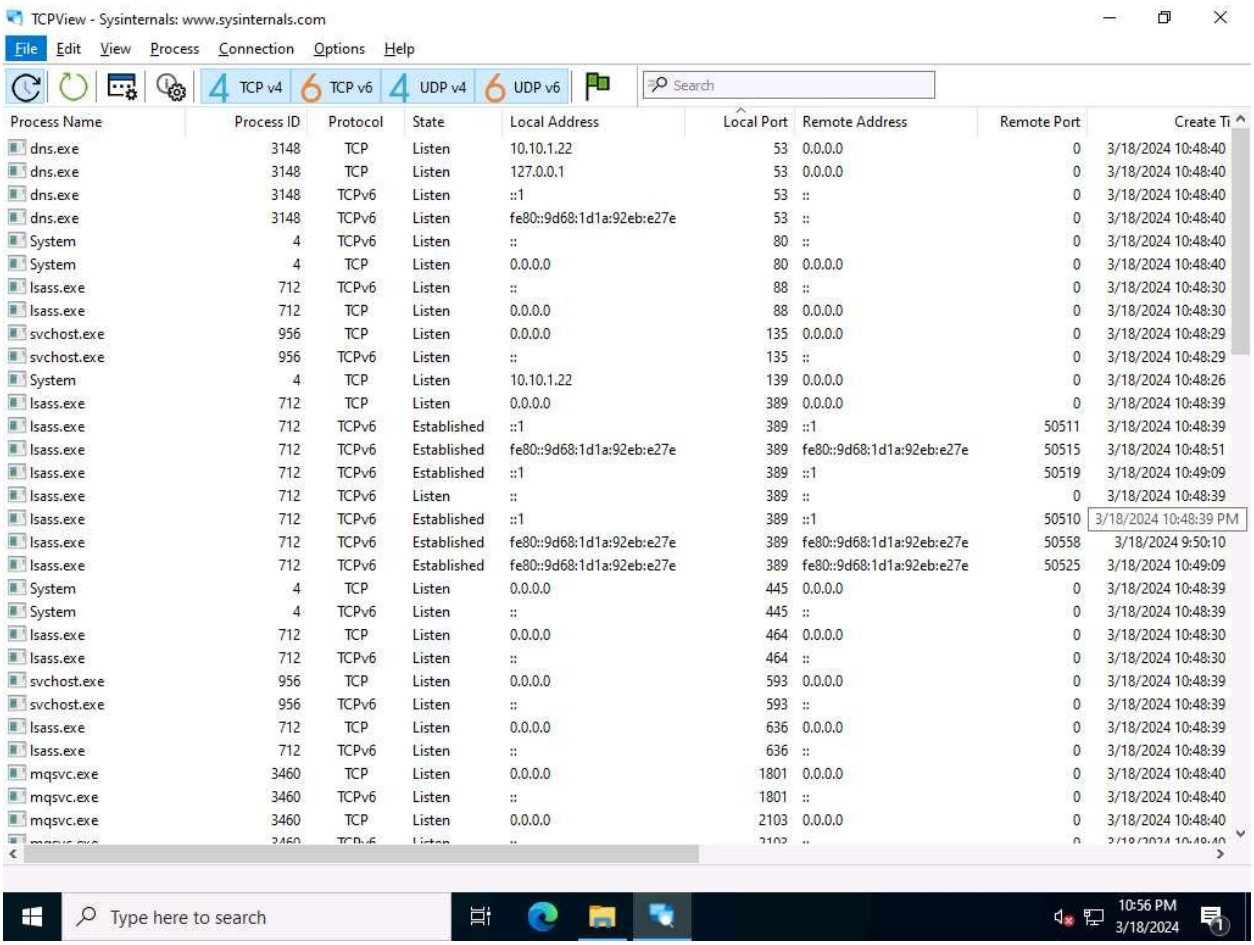
If a **User Account Control** pop-up appears, click **Yes**.



12. If a **TCPView License Agreement** window appears, click the **Agree** button to agree to the terms and conditions.
13. The **TCPView** main window appears, displaying the details such as Process Name, Process ID, Protocol, State, Local Address, Local Port, Remote Address, Remote Port, as shown in the screenshot.

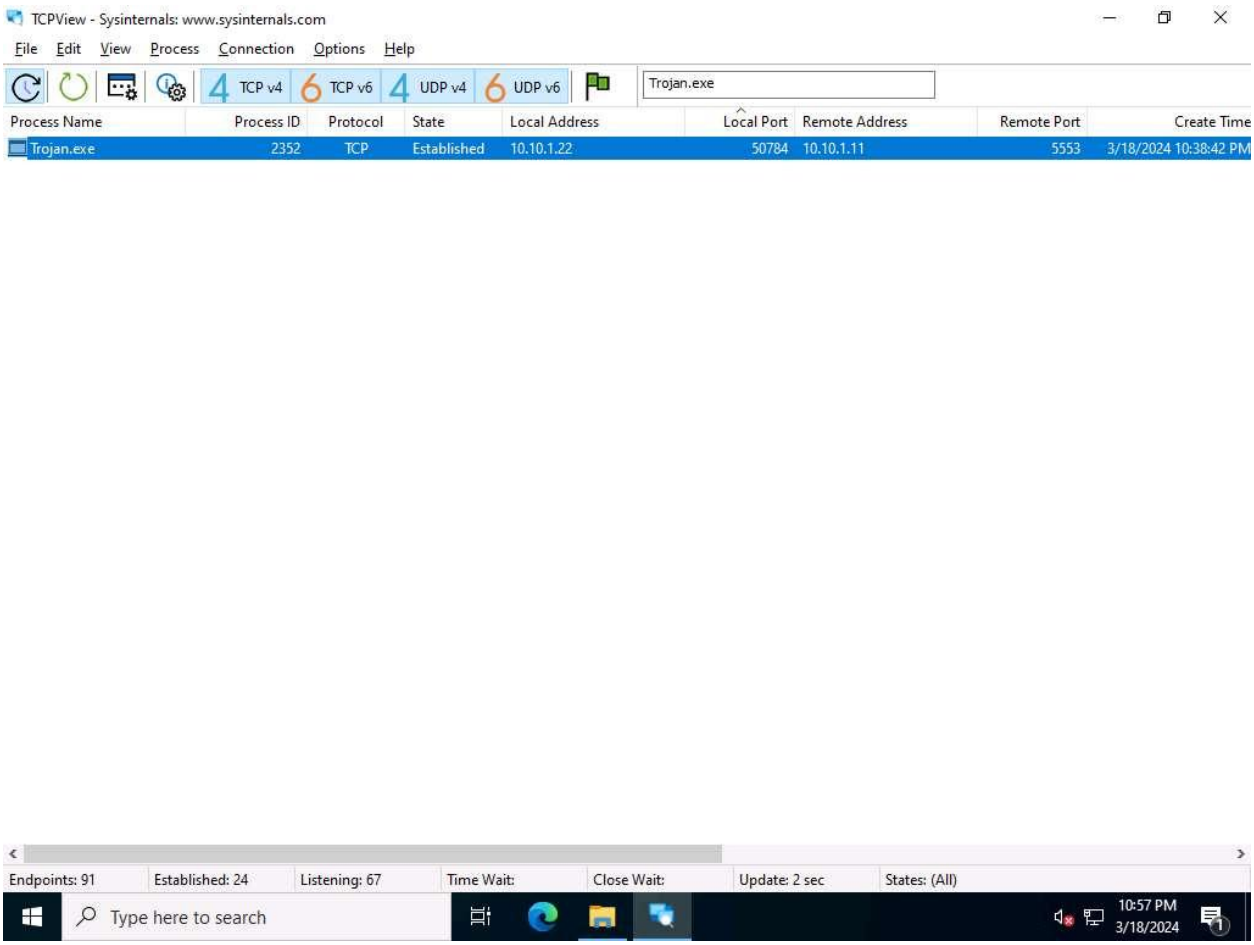


14. TCPView performs **Port monitoring**. Click the **Local Port** tab to view the ports in serial order.
15. Observe the protocols running on different ports under the **Protocol** column.

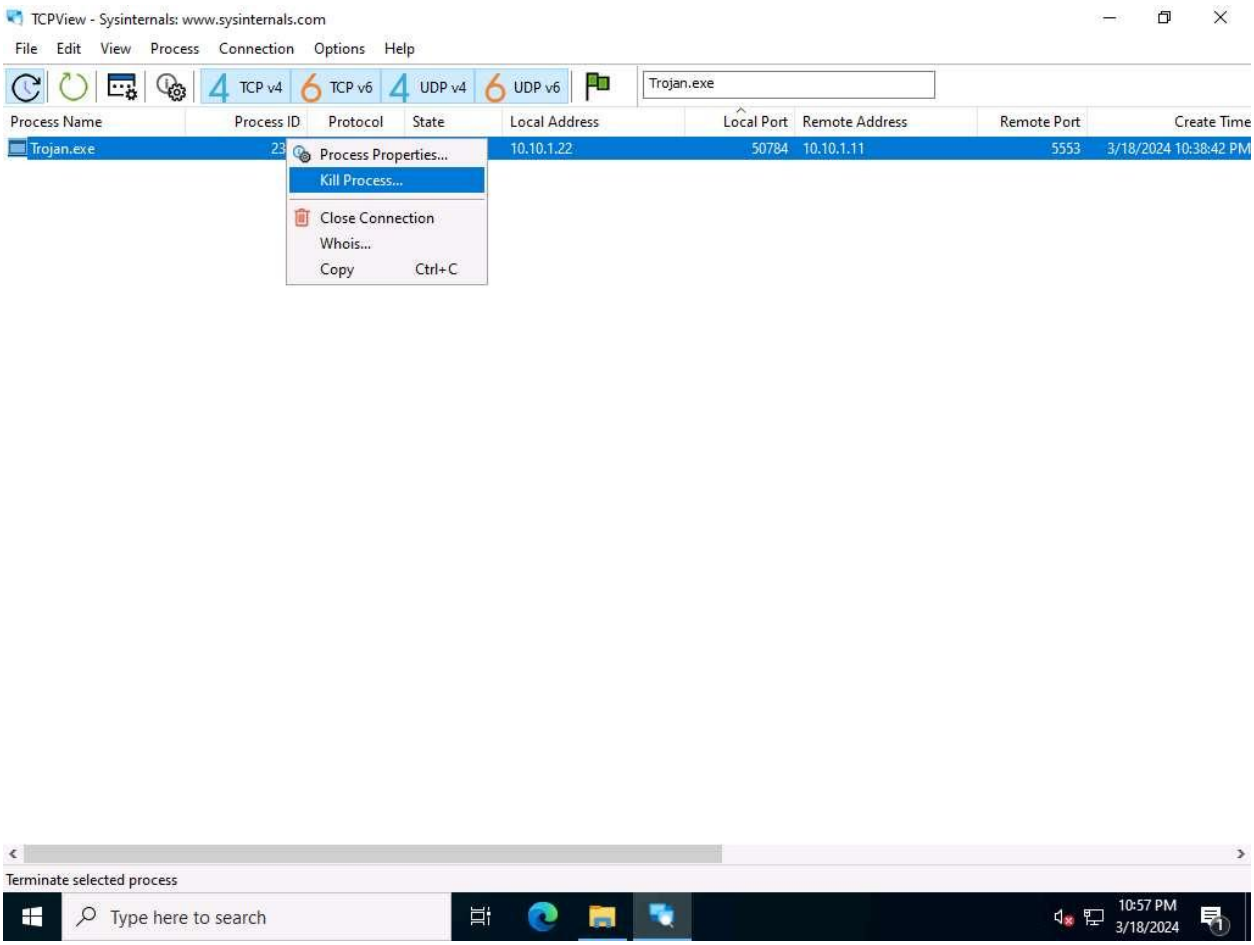


16. As you have executed a malicious application, now search for the **Trojan.exe** process in the TCPView.

17. You can observe that the **Trojan.exe** malicious program is running on the **Windows Server 2022** machine. You can see details such as **Remote Address** and **Remote Port**.

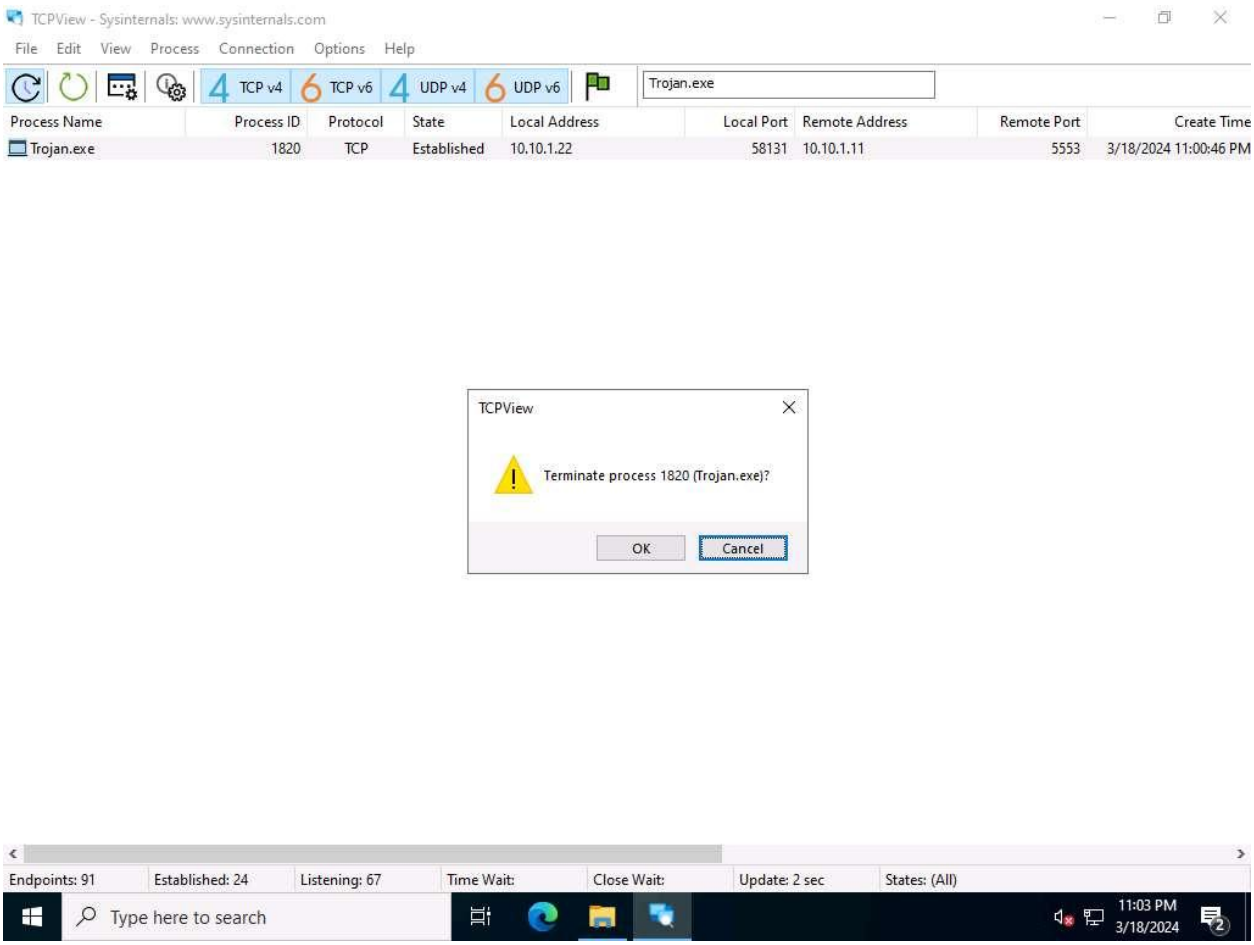


18. You can right-click the process **Trojan.exe**; select **Kill Process…** to end the running process.

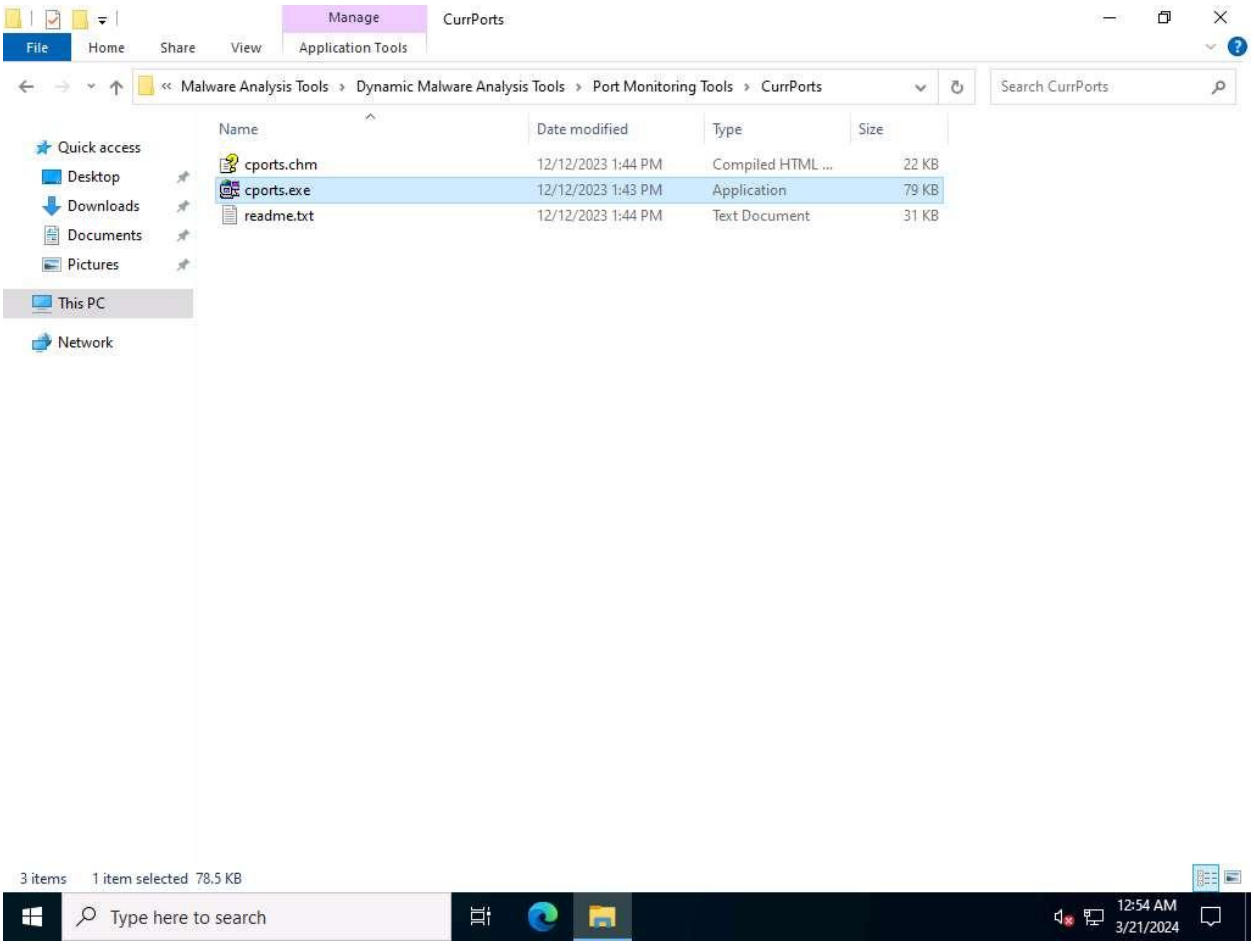


19. For this task, do not Kill the process in this step as we are going to use this running process for the next task; click **Cancel**.

Normally, if a **TCPView** dialog box appears, click **OK** to terminate the process.

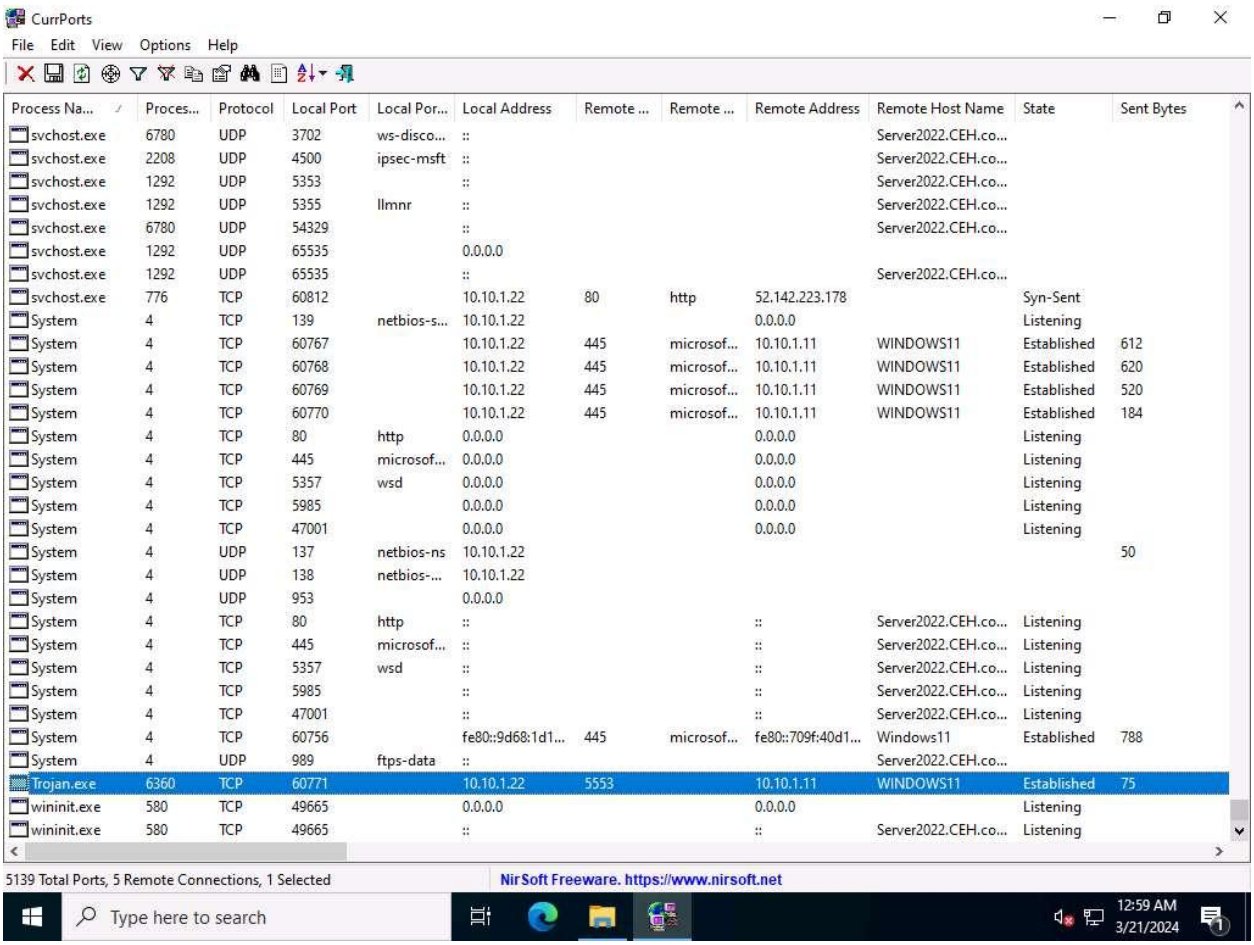


20. This way, you can view all processes running on the machine and stop unwanted or malicious processes that may affect your system. If you are unable to stop a process, you can view the port on which it is running and add a firewall rule to block the port.
21. Close the **TCPView** window.
22. Now, let us analyze this process on **Windows Server 2022** using **CurrPorts**.
23. Navigate to **Z:\CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts** and double-click **cports.exe**.

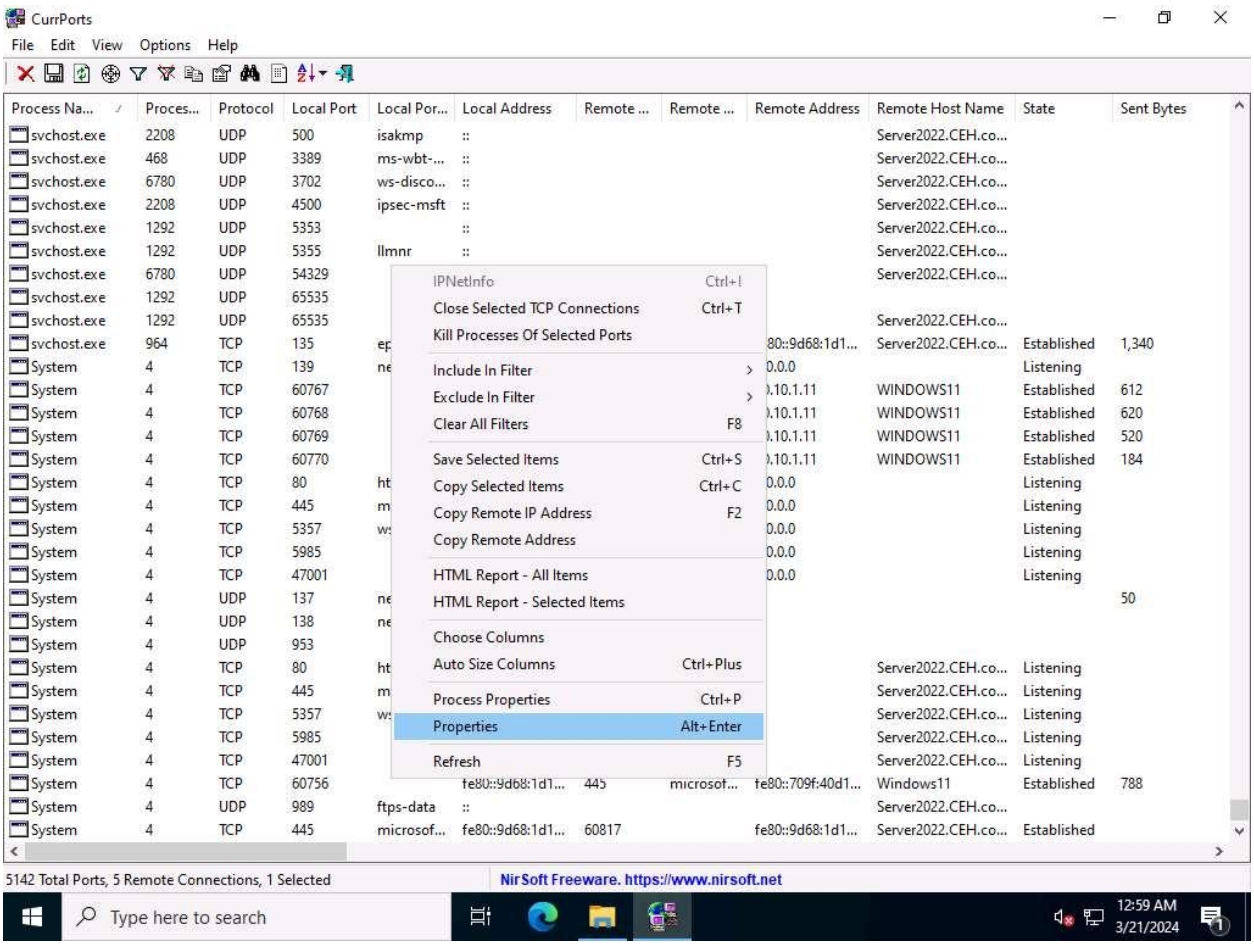


24. The **CurrPorts** window appears, displaying a list of currently open TCP/IP and UDP ports on the machine.

25. Scroll-down to search for **Trojan.exe** process running on the machine, as the shown in the screenshot. It is evident from the above screenshot that the process is connected to the machine on **port 5553**.

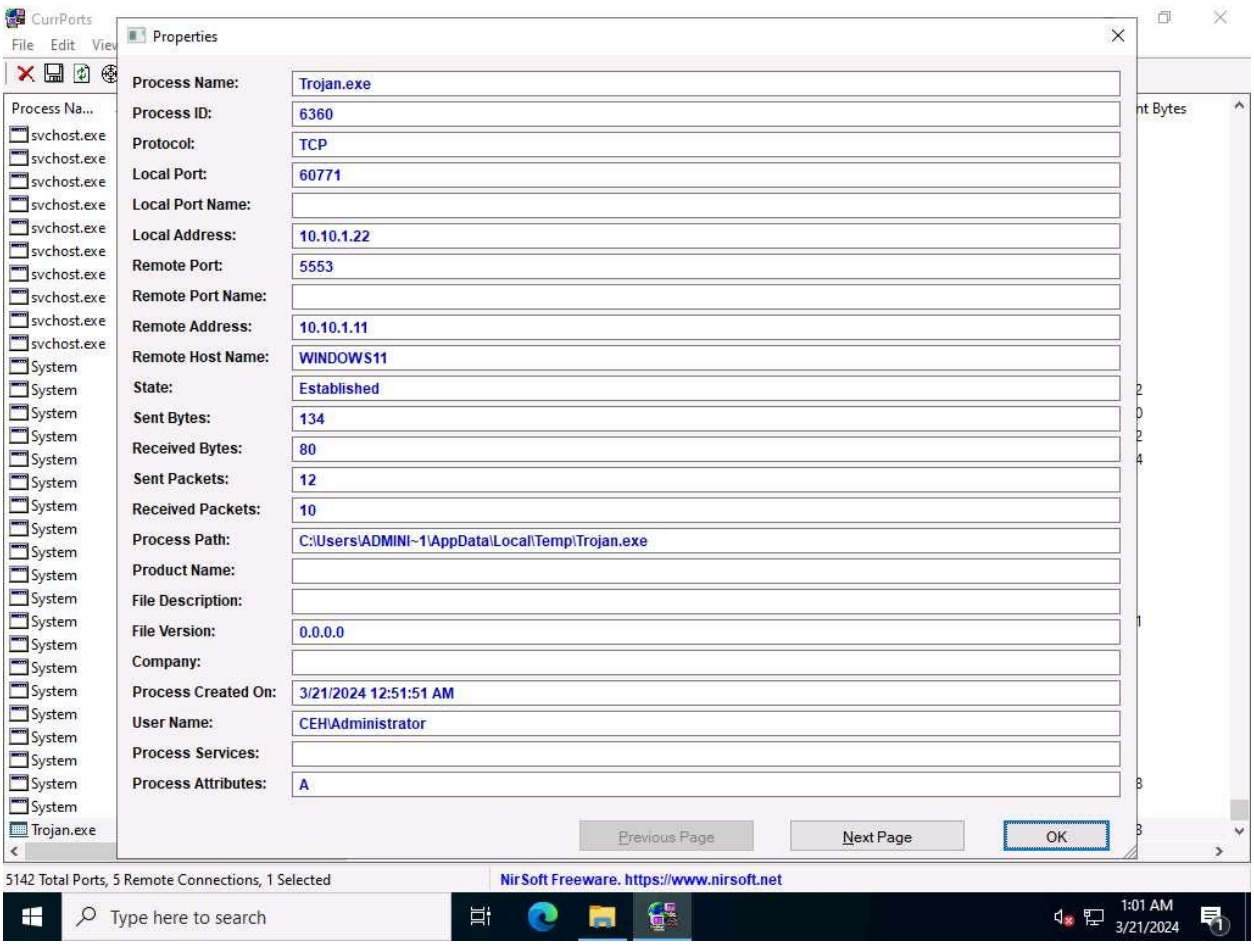


26. You can view the properties of the process by right-clicking on the process and clicking **Properties** from the **Context** menu.



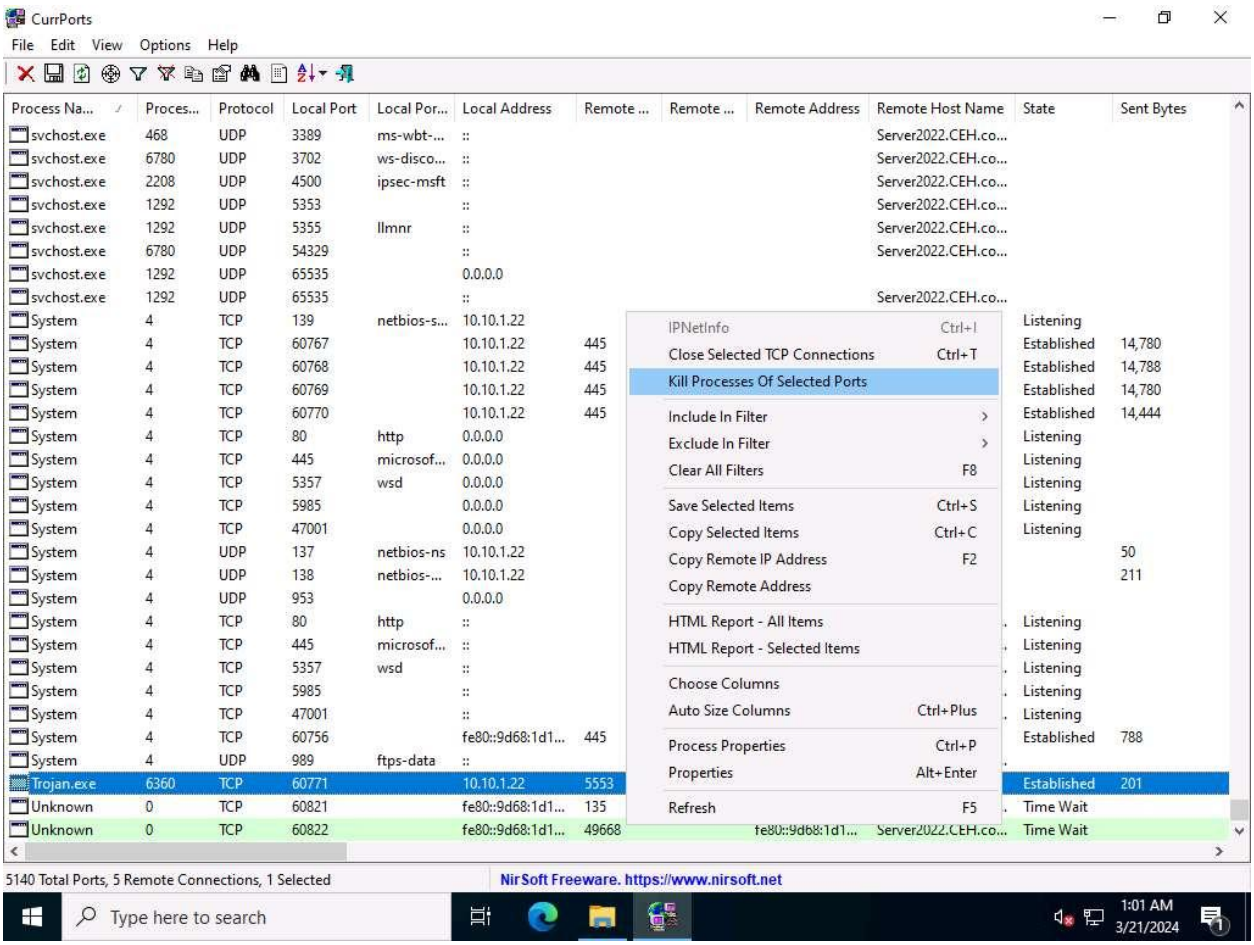
27. The **Properties** window appears, displaying information related to the process such as the name of the process, its process ID, Remote Address, Process Path, Remote Host Name, and other details.

28. Once you are done examining the properties associated with the process, click **OK**.



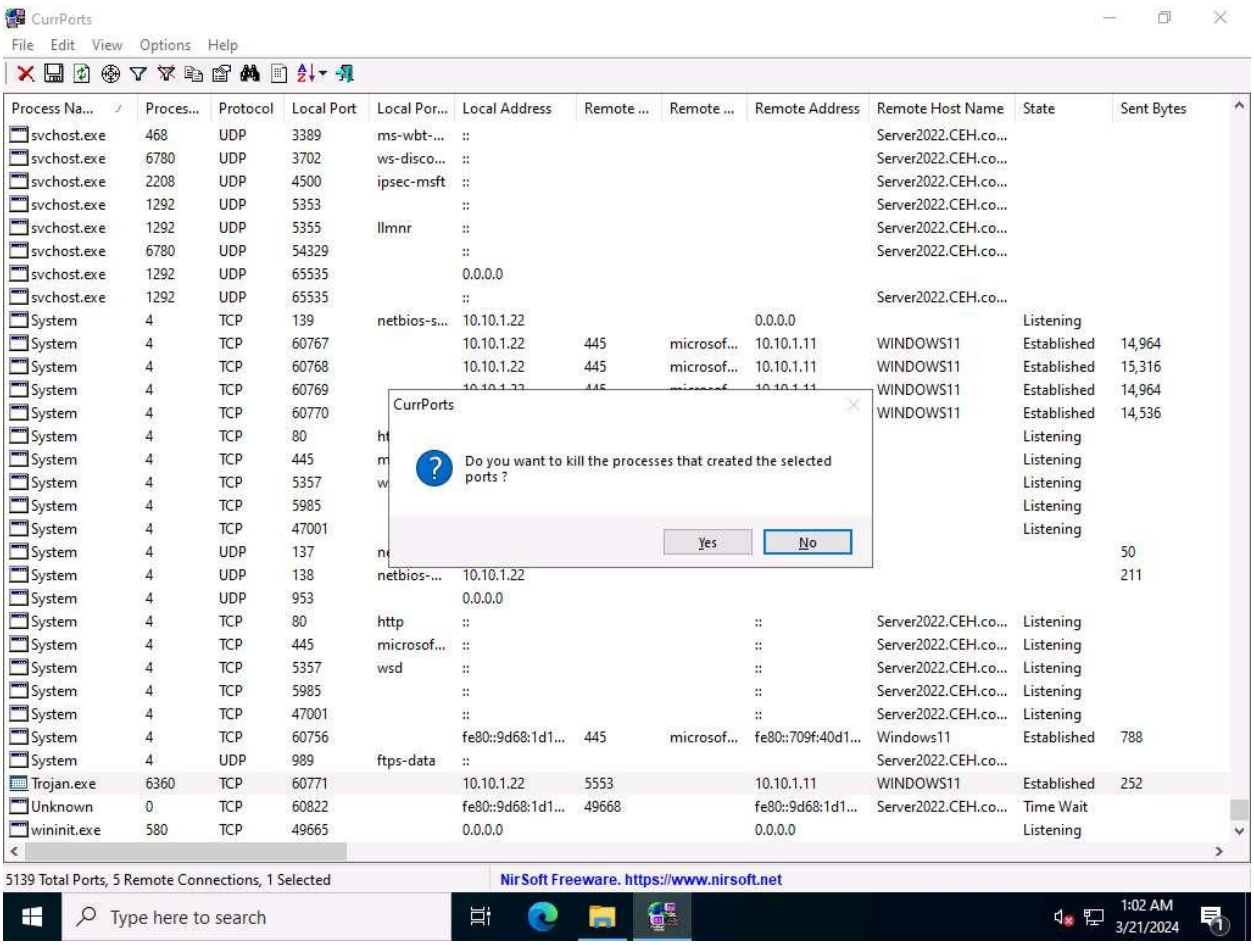
29. Because **Trojan.exe** is a malicious process, you may end the process by right-clicking on it and selecting **Kill Processes Of Selected Ports** from the context menu.

30. Alternatively, you may select **Close Selected TCP Connections**, so that the port closes, and the attacker can never regain connection through the port unless you open it.



31. Do not Kill the process at this step, as this running process will be used for the next task; when the **CurrPorts** dialog-box appears click **No**.

Normally, when the **CurrPorts** dialog-box appears, you would click **Yes** to close the connection.



32. This way, you can analyze the ports open on a machine and the processes running on it.
33. If a process is found to be suspicious, you may either kill the process or close the port.
34. Close all open windows.
35. You can also use other port monitoring tools such as **TCP Port/Telnet Monitoring** (https://www.dotcom-monitor.com), **PRTG Network Monitor** (https://www.paessler.com), **SolarWinds Open Port Scanner** (https://www.solarwinds.com) or to perform port monitoring.

Question 7.4.1.1

Run njRAT from the attacker machine (Windows 11) and gain control over the victim machine (Windows Server 2022). On the Windows Server 2022 machine, use the TCPView tool to find the connections created by the Trojan. What is the remote port used by the Trojan server?

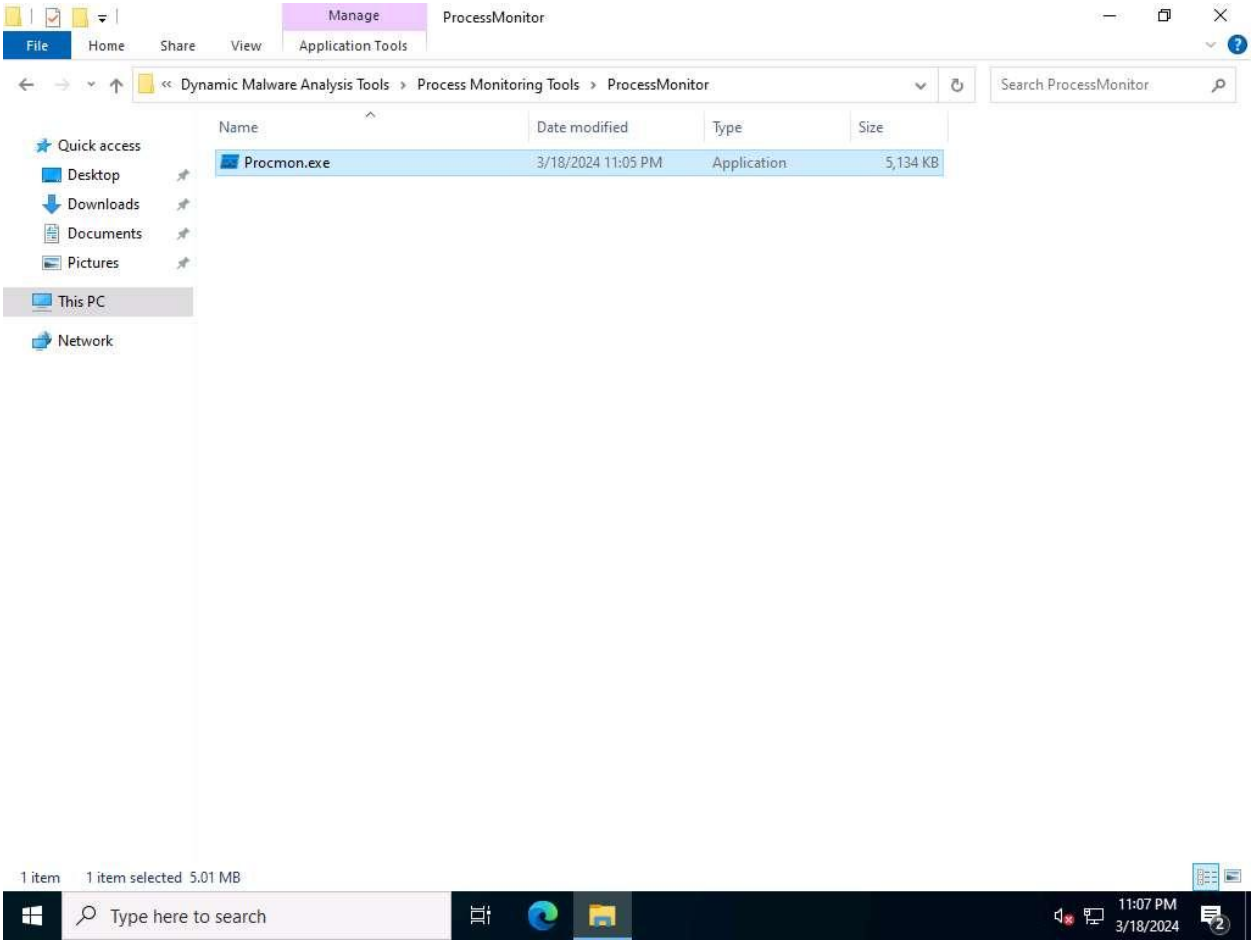
Task 2: Perform Process Monitoring using Process Monitor

Process monitoring will help in understanding the processes that malware initiates and takes over after execution. You should also observe the child processes, associated handles, loaded libraries, functions, and execution flow of boot time processes to define the entire nature of a file or program, gather information about processes running before the execution of the malware, and compare them with the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all processes that malware starts.

Process Monitor is a monitoring tool for Windows that shows the real-time file system, Registry, and process and thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon. It adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, and simultaneous logging to a file. Unique features of Process Monitor make it a core utility in system troubleshooting and vital to the malware hunting toolkit.

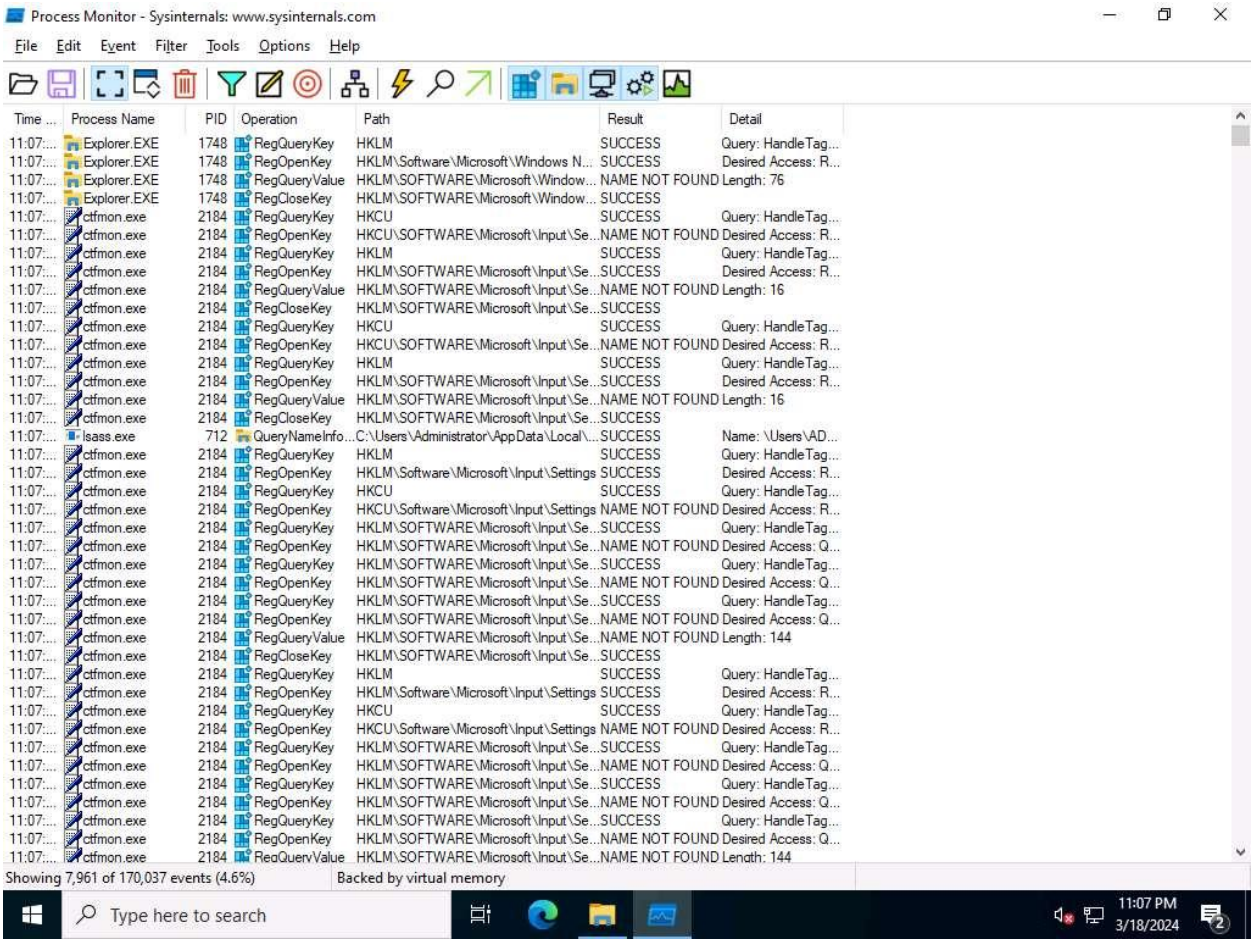
Here, we will use the Process Monitor tool to detect suspicious processes.

1. On the **Windows Server 2022** machine, navigate to **Z:\CEHv13 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Process Monitoring Tools\ProcessMonitor** and double-click **Procmon.exe** to launch the Process Monitor tool.



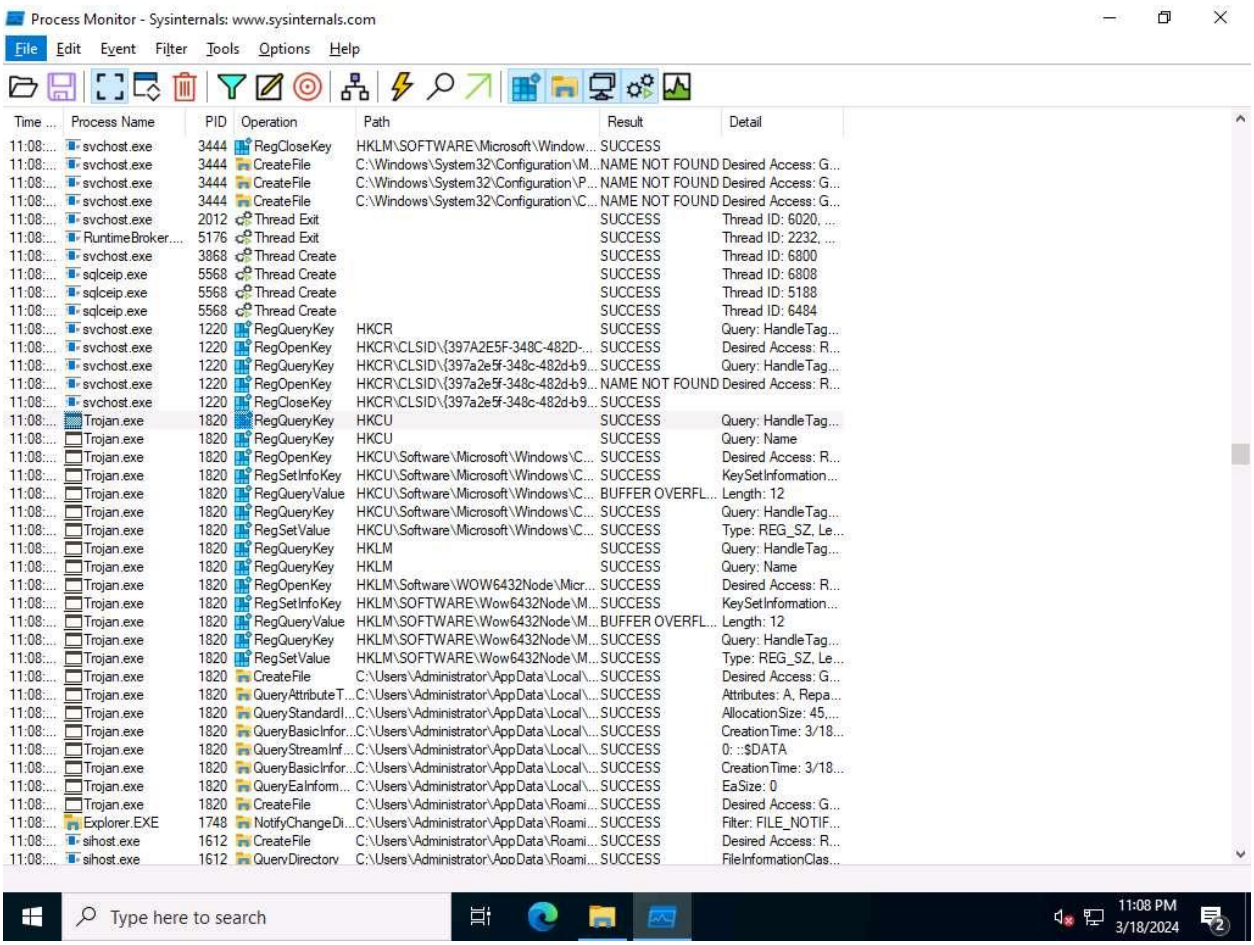
2. The **Process Monitor License Agreement** window appears; click **Agree**.

3. The **Process Monitor** main window appears, as shown in the screenshot, with the processes running on the machine.

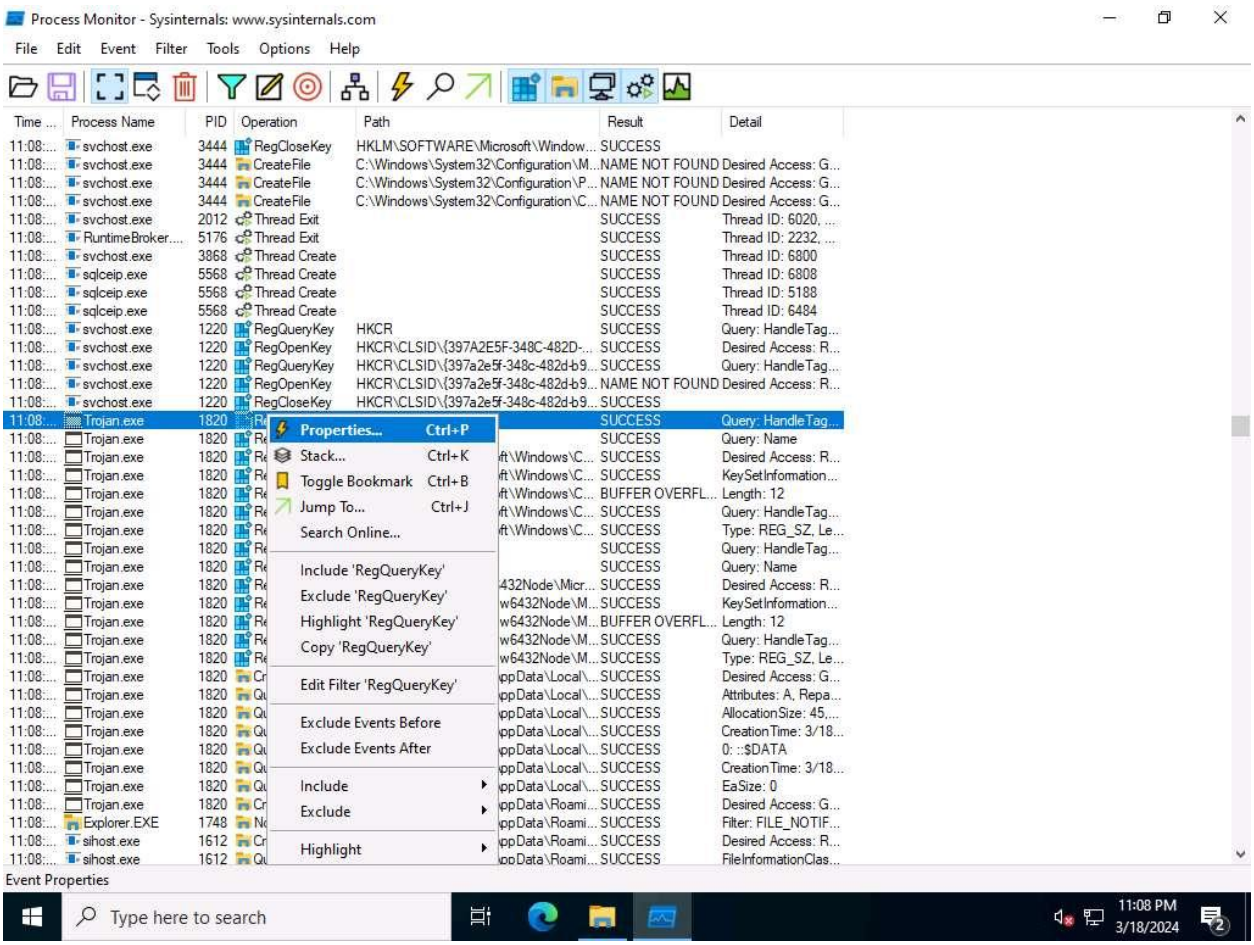


4. Scroll down to look for the **Trojan.exe** process that was executed in the previous task. If you killed the process at the end of the task, then navigate to **Z:\CEHv13 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe** to re-execute the malicious program.

5. Observe that the **Trojan.exe** process is running on the machine. Process Monitor shows the running process details such as the PID, Operation, Path, Result, and Details.

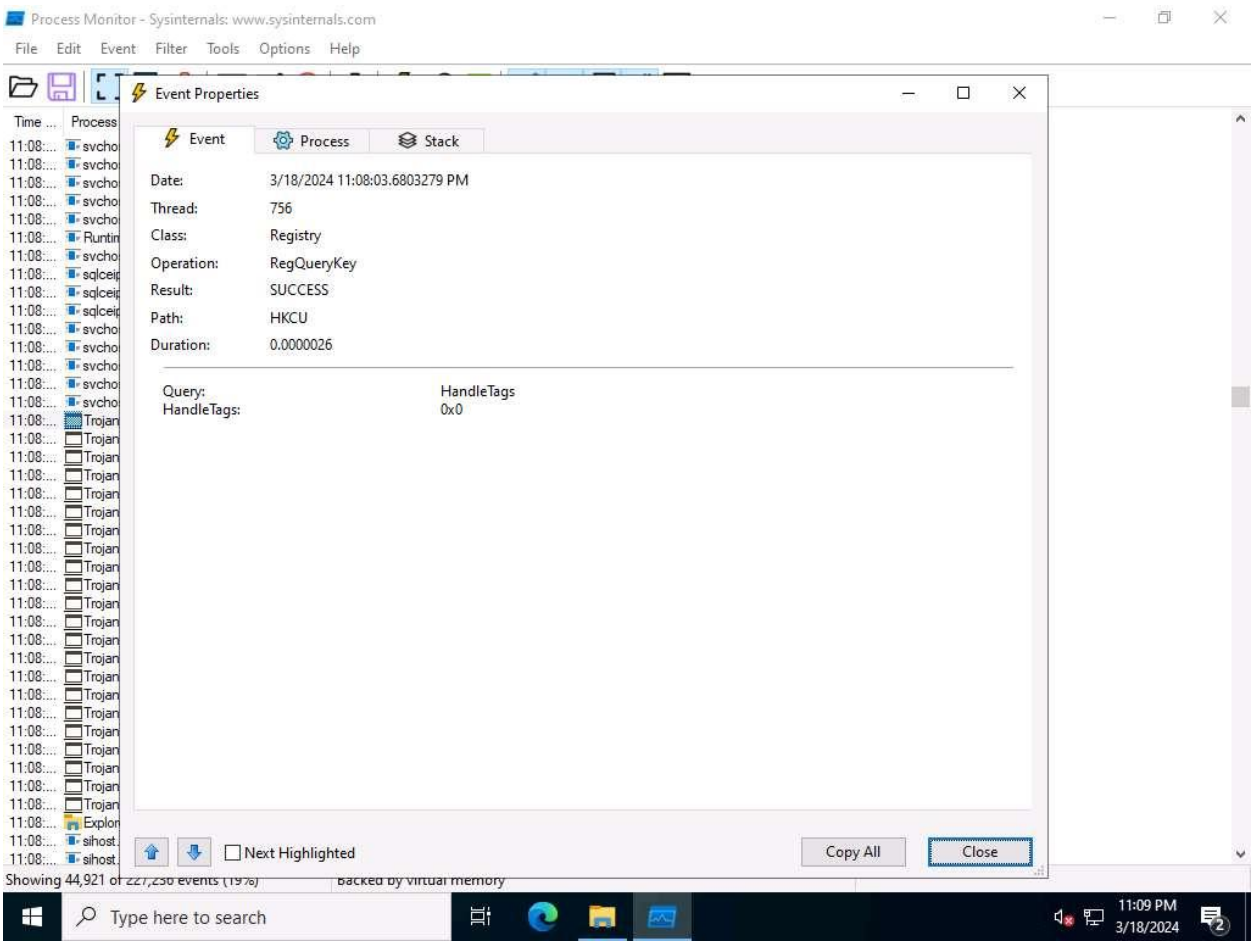


6. To view the properties of a running process, select the process (here, **Trojan.exe**), right-click on the process and select **Properties** from the context menu.

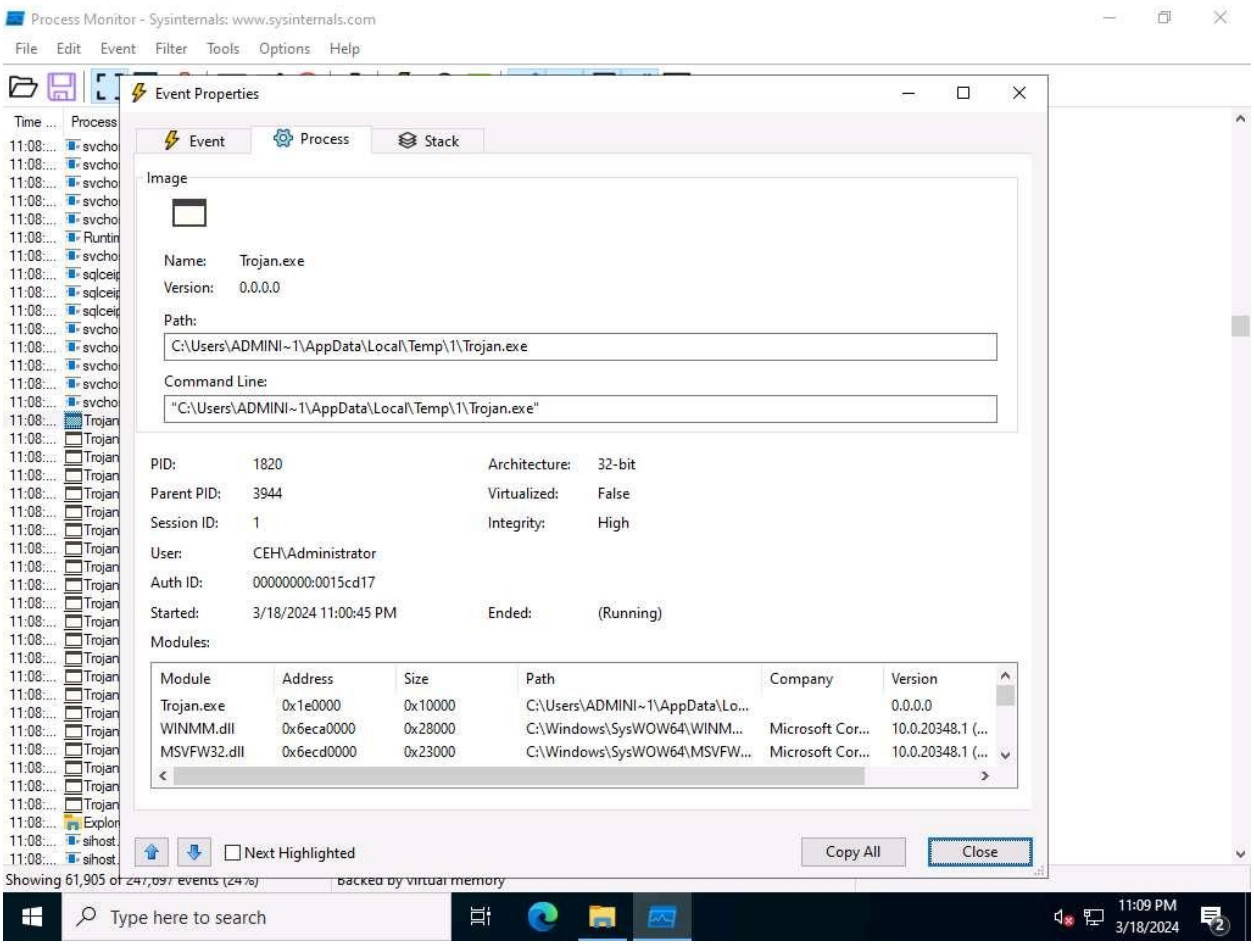


7. The **Event Properties** window appears with the details of the chosen process.

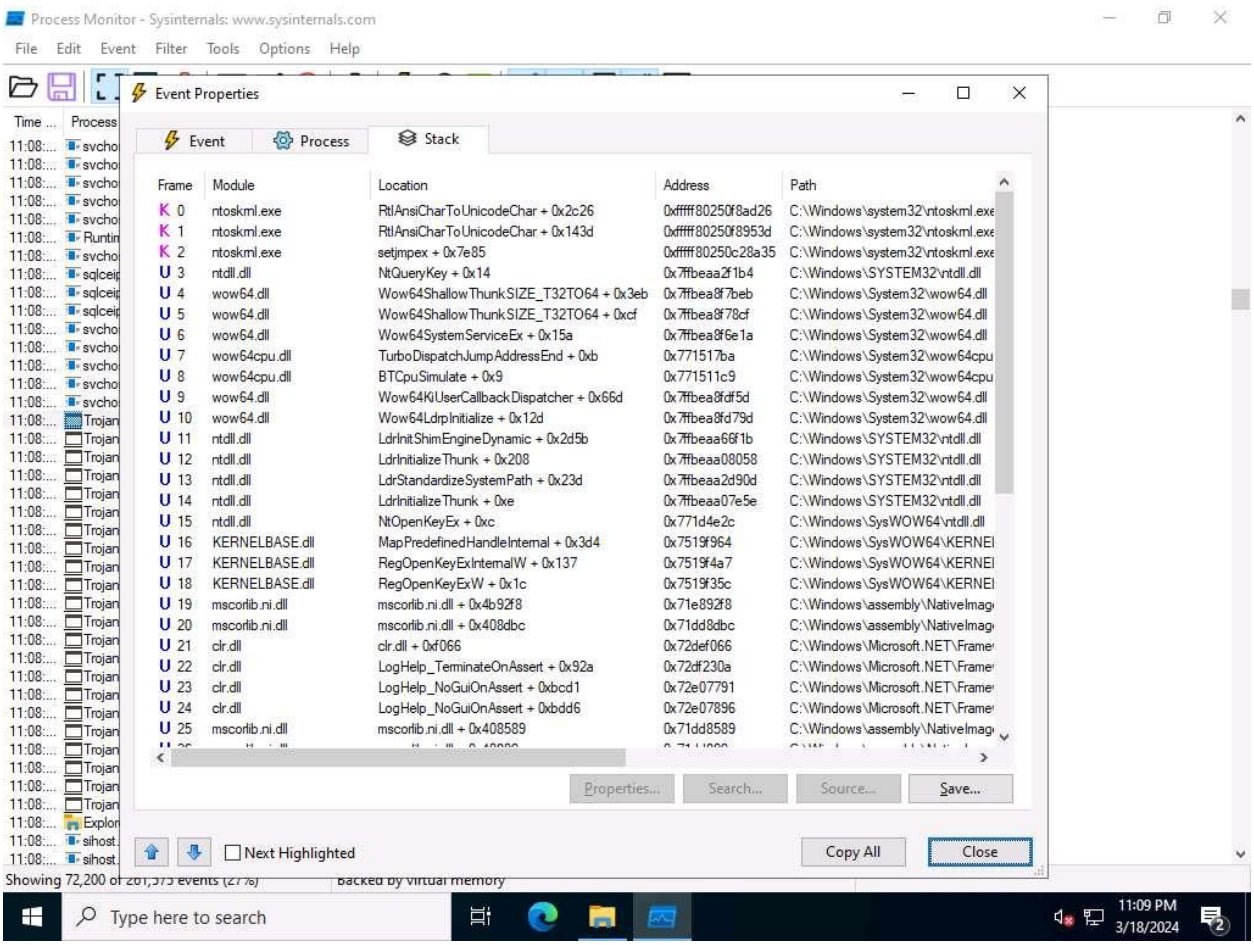
8. In the **Event** tab, you can see the complete details of the running process such as Date, Thread, Class, Operation, Result, Path, and Duration.



9. Once the analysis is complete, click the **Process** tab.
10. The **Process** tab shows the complete details of the process running, as shown in the screenshot.



11. Click the **Stack** tab to view the supported DLLs of the selected process. Once the analysis is done, click **Close**.



12. This way, you can analyze the processes running on a machine.
13. If a process is found to be suspicious, you may either kill the process or close the port.
14. Close all windows on the **Windows 11** and **Windows Server 2022** machines.
15. You can also use other process monitoring tools such as **Process Explorer** (https://docs.microsoft.com), **OpManager** (https://www.manageengine.com), **Monit** (https://mmonit.com), **ESET SysInspector** (https://www.eset.com), or **System Explorer** (https://systemexplorer.net) to perform process monitoring.

Question 7.4.2.1

Run njRAT from the attacker machine (Windows 11) and gain control over the victim machine (Windows Server 2022). On the Windows Server 2022 machine, use Process Monitor to detect suspicious processes created by the Trojan server. Determine the architecture of the malicious process that is running.