Lab 2: Detect and Protect Against DoS and DDoS Attacks

Lab Scenario

DoS/DDoS attacks are one of the foremost security threats on the Internet; thus, there is a greater necessity for solutions to mitigate these attacks. Early detection techniques help to prevent DoS and DDoS attacks. Detecting such attacks is a tricky job. A DoS and DDoS attack traffic detector needs to distinguish between genuine and bogus data packets, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS or DDoS attack. One problem in filtering bogus from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS or DDoS attack. All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.

As a professional ethical hacker or pen tester, you must use various DoS and DDoS attack detection techniques to prevent the systems in the network from being damaged.

This lab provides hands-on experience in detecting DoS and DDoS attacks using various detection techniques.

Lab Objectives

- Detect and protect against DDoS attacks using Anti DDoS Guardian

Overview of DoS and DDoS Attack Detection

Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from the legitimate packet traffic.

The following are the three types of detection techniques:

- **Activity Profiling**: Profiles based on the average packet rate for a network flow, which consists of consecutive packets with similar packet header information
- **Sequential Change-point Detection**: Filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate over time
- **Wavelet-based Signal Analysis**: Analyzes network traffic in terms of spectral components

Task 1: Detect and Protect Against DDoS Attacks using Anti DDoS Guardian

Anti DDoS Guardian is a DDoS attack protection tool. It protects IIS servers, Apache serves, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Anti DDoS Guardian monitors each incoming and outgoing packet in Real-Time. It displays the local address, remote address, and other information of each network flow. Anti DDoS Guardian limits network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.

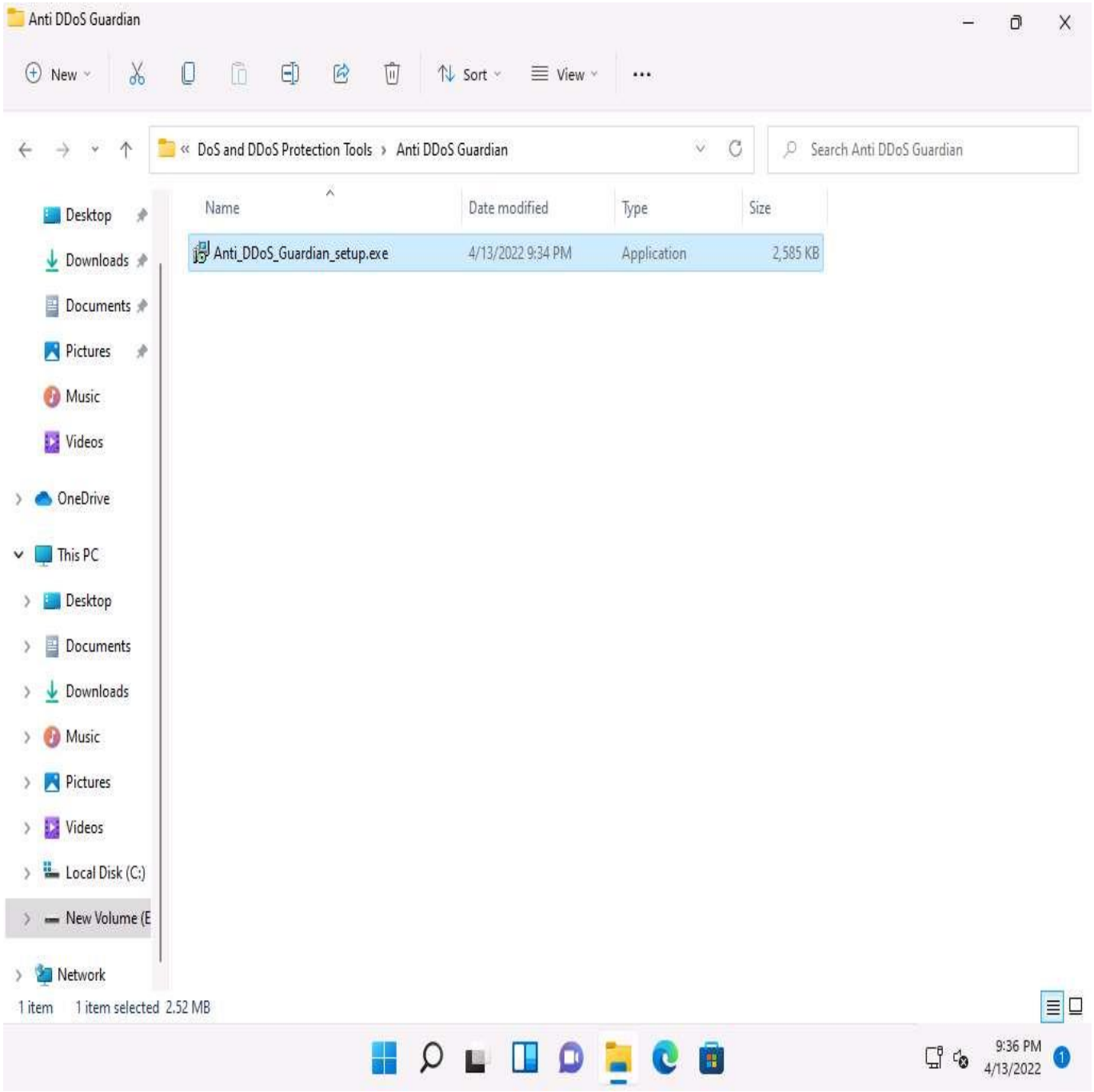
Here, we will detect and protect against a DDoS attack using Anti DDoS Guardian.

In this task, we will use the **Windows Server 2019** and **Windows Server 2022** machines to perform a DDoS attack on the target system, **Windows 11**.

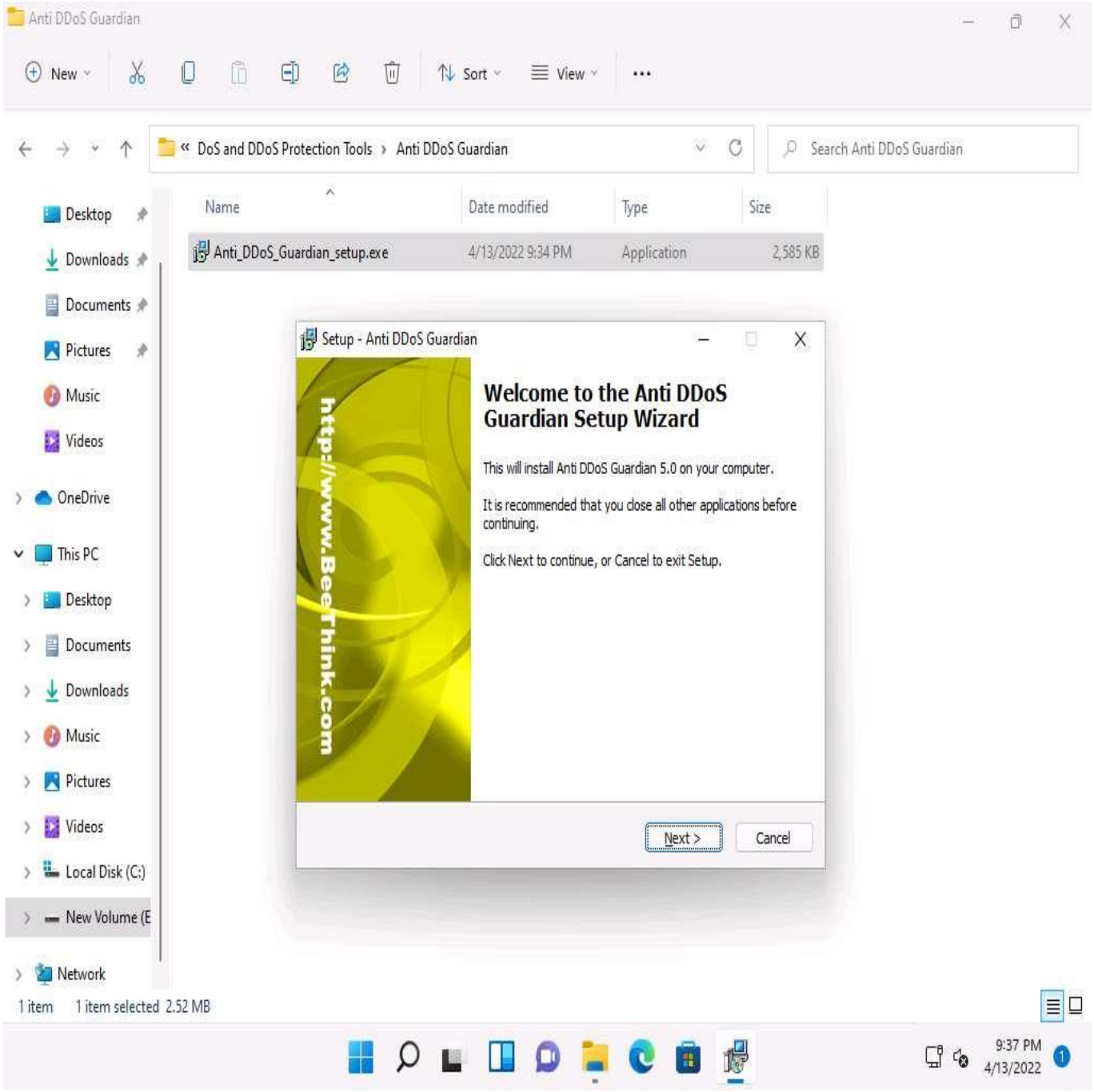
1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian** and double click **Anti_DDoS_Guardian_setup.exe.**

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

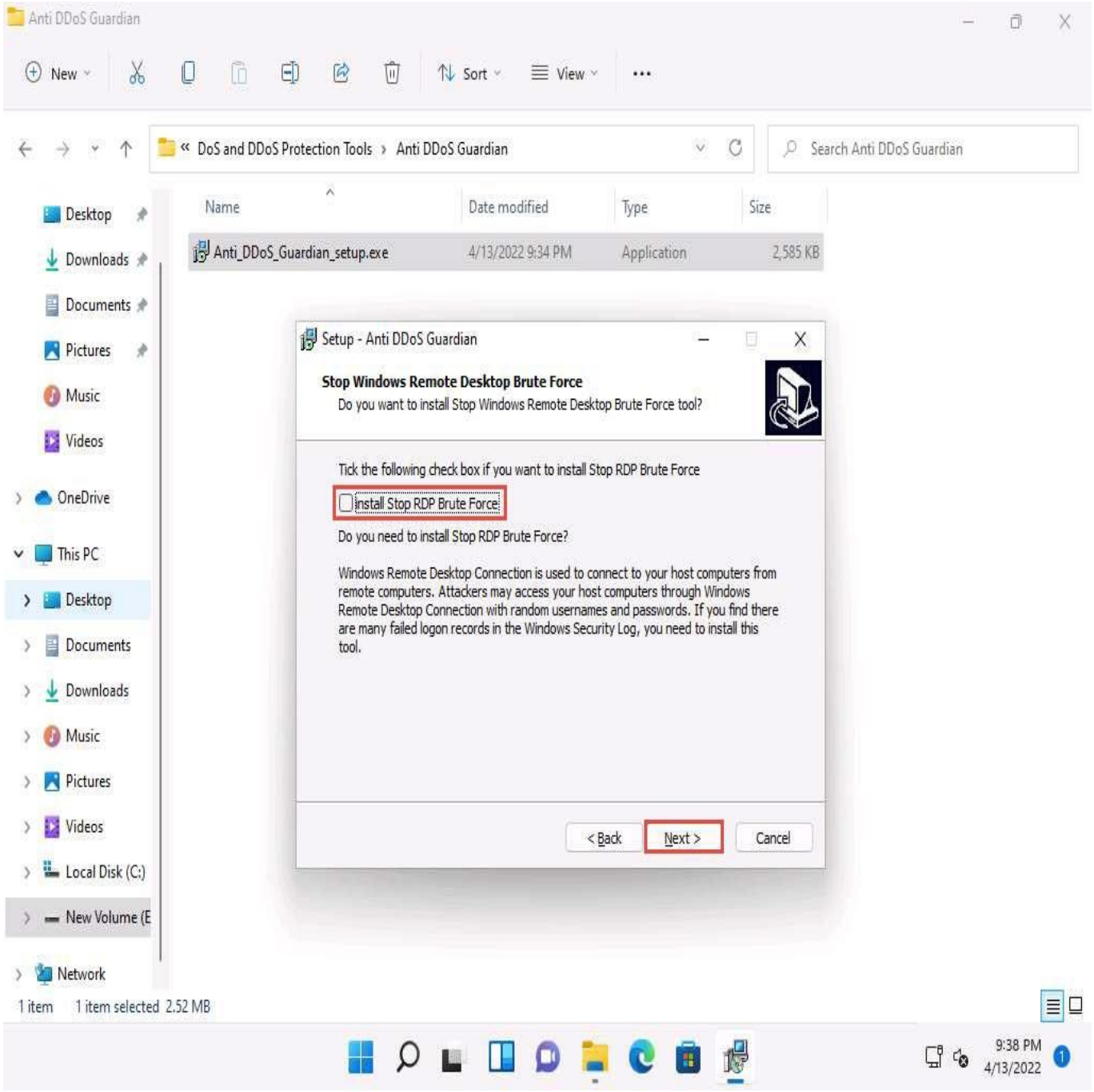
If an **Open File - Security Warning** pop-up appears, click **Run**.



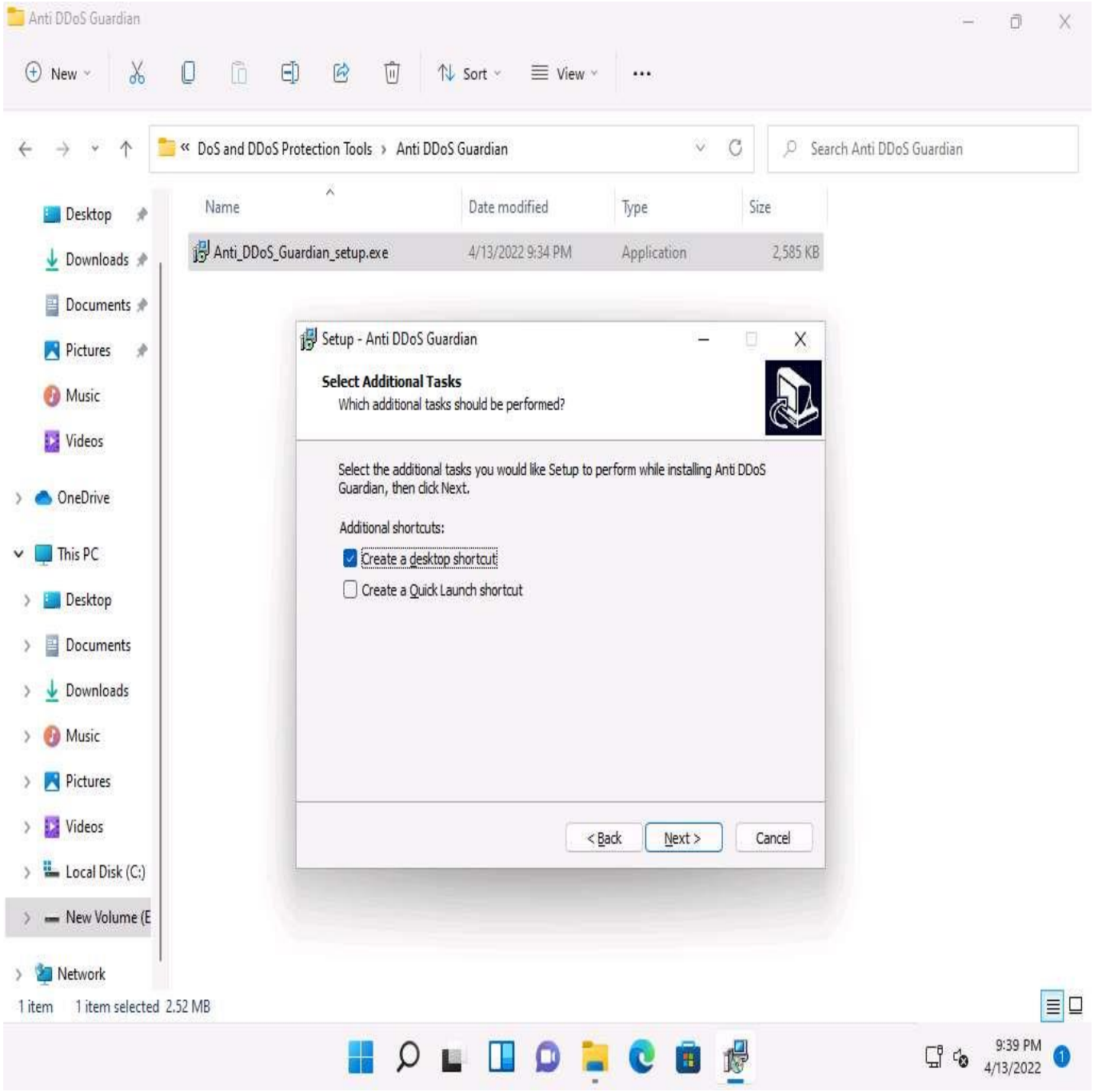
2. The **Setup - Anti DDoS Guardian window** appears; click **Next**. Follow the wizard-driven installation steps to install the application.



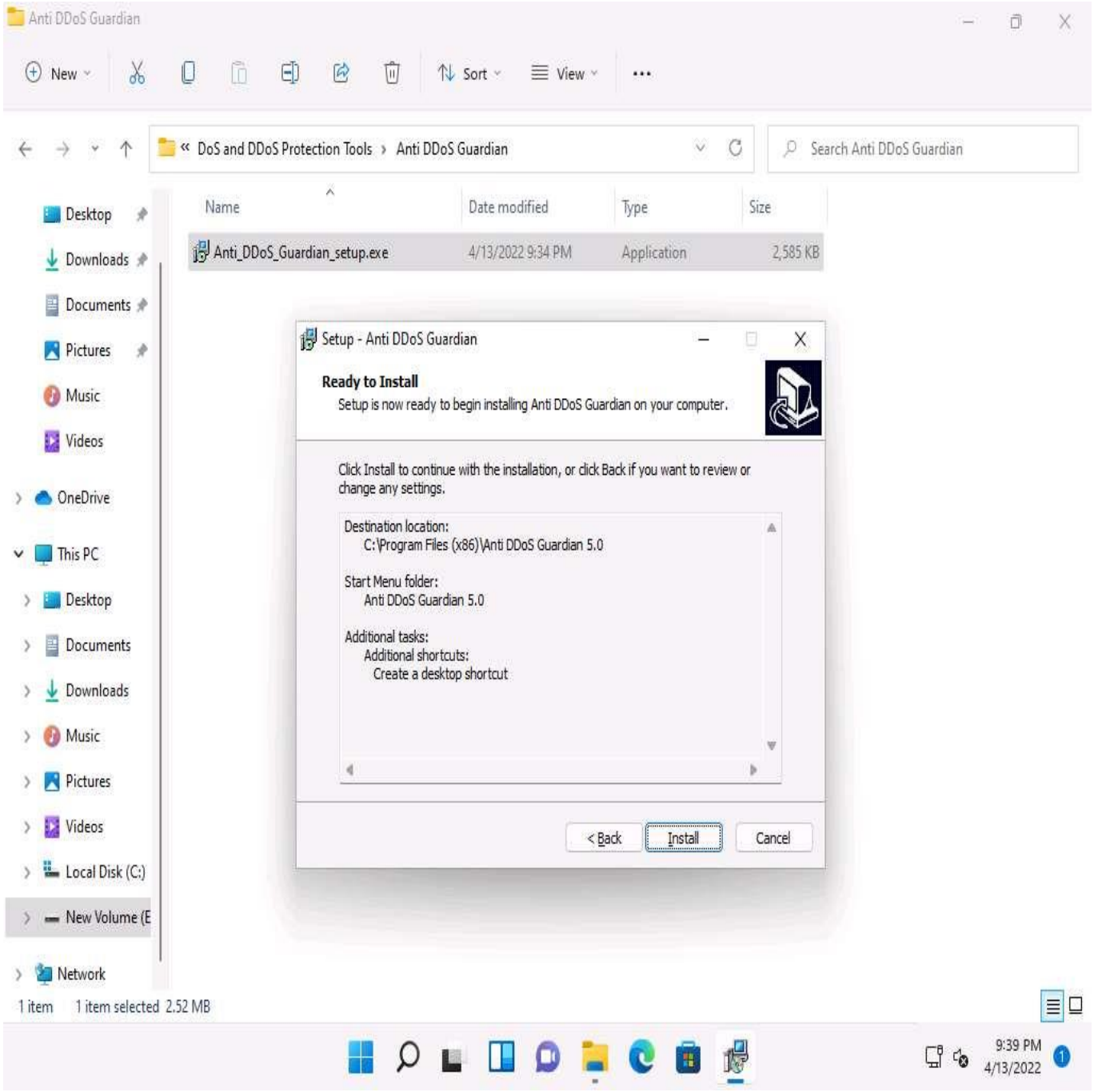
3. ☐ In the **Stop Windows Remote Desktop Brute Force** wizard, uncheck the **install Stop RDP Brute Force** option, and click **Next**.



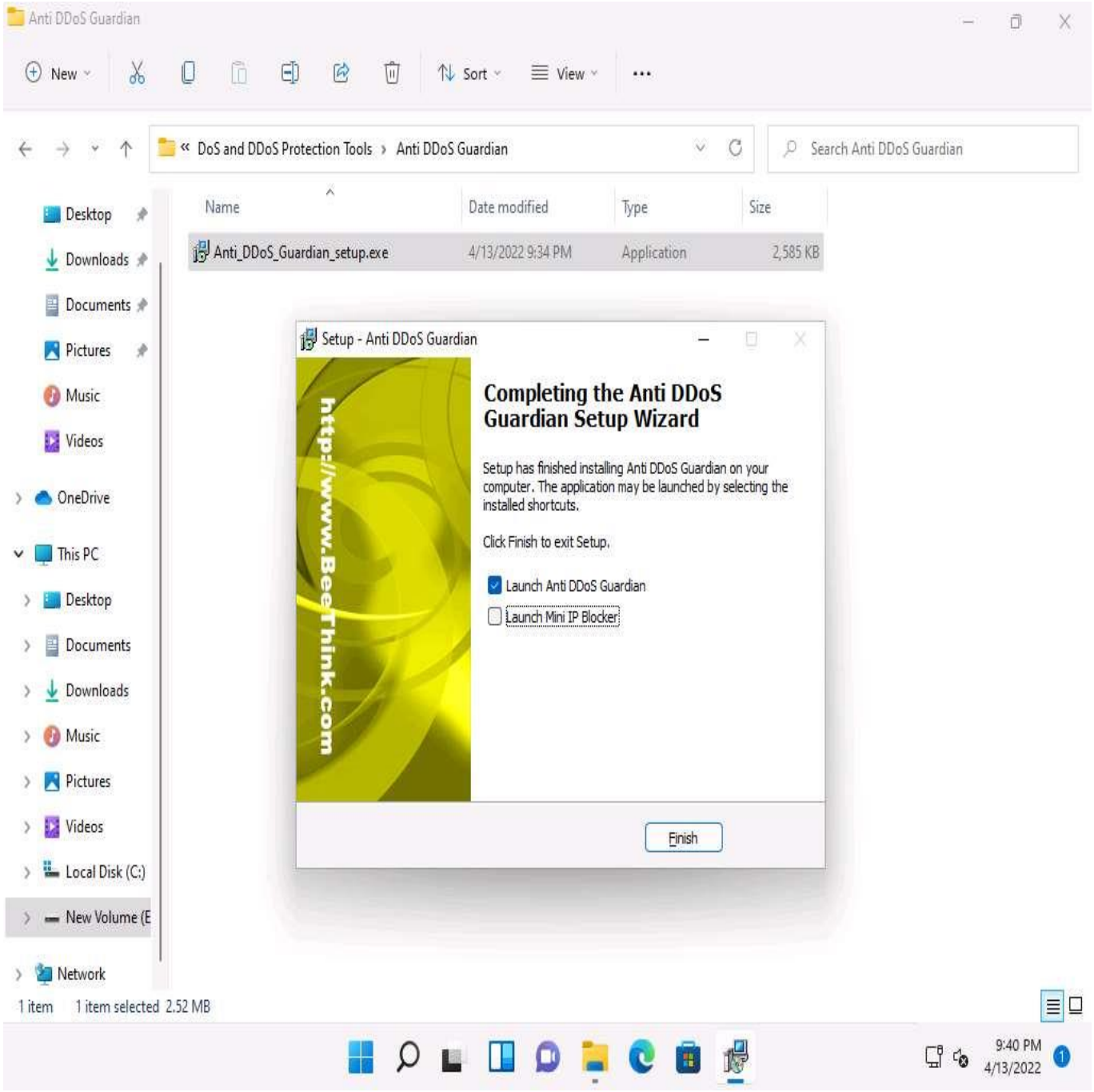
4. ☐ The **Select Additional Tasks** wizard appears; check the **Create a desktop shortcut** option, and click **Next**.



5. ☐ The **Ready to Install** wizard appears; click **Install**.

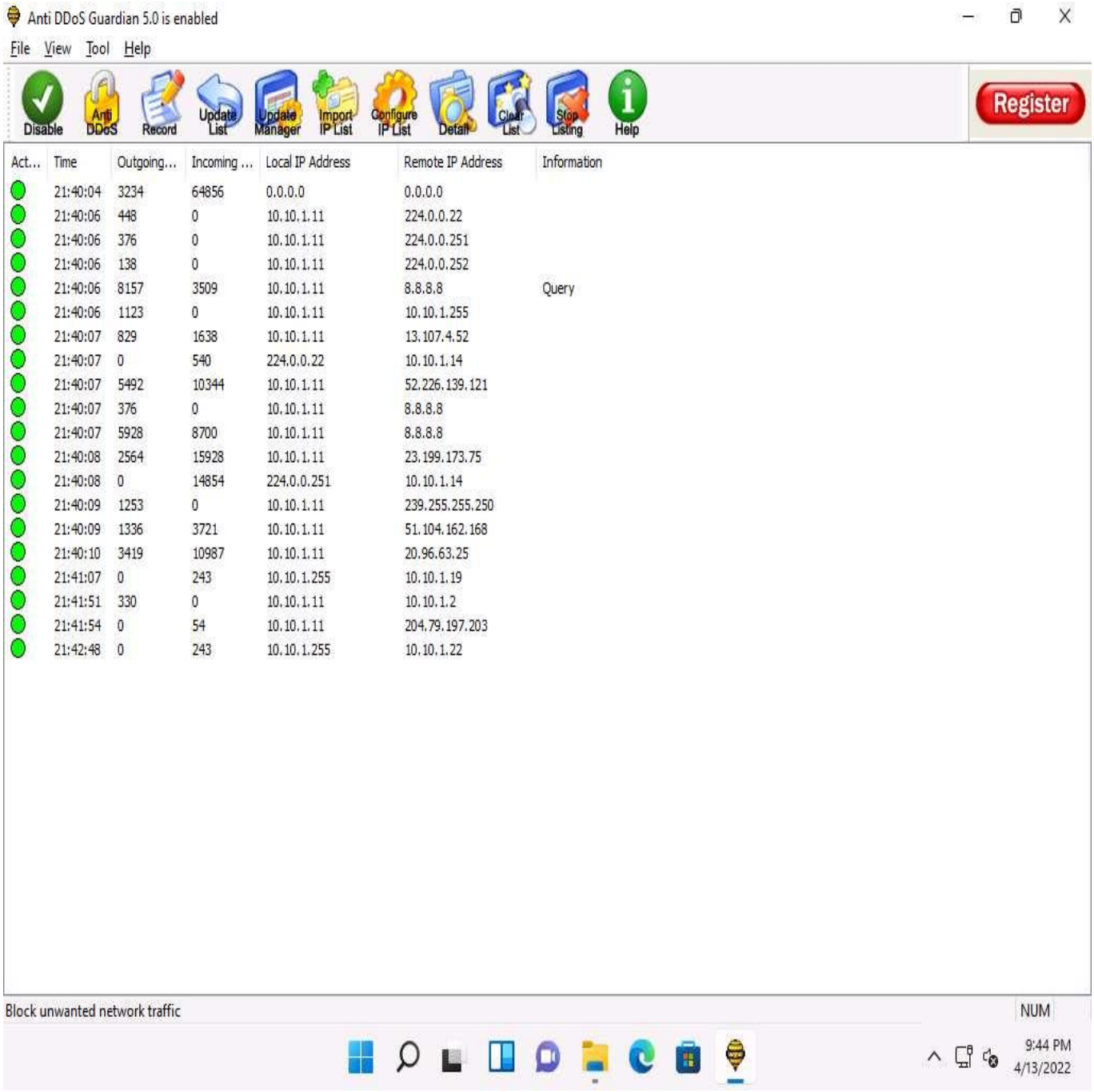


6. ☐ The **Completing the Anti DDoS Guardian Setup Wizard** window appears; uncheck the **Launch Mini IP Blocker** option and click **Finish**.

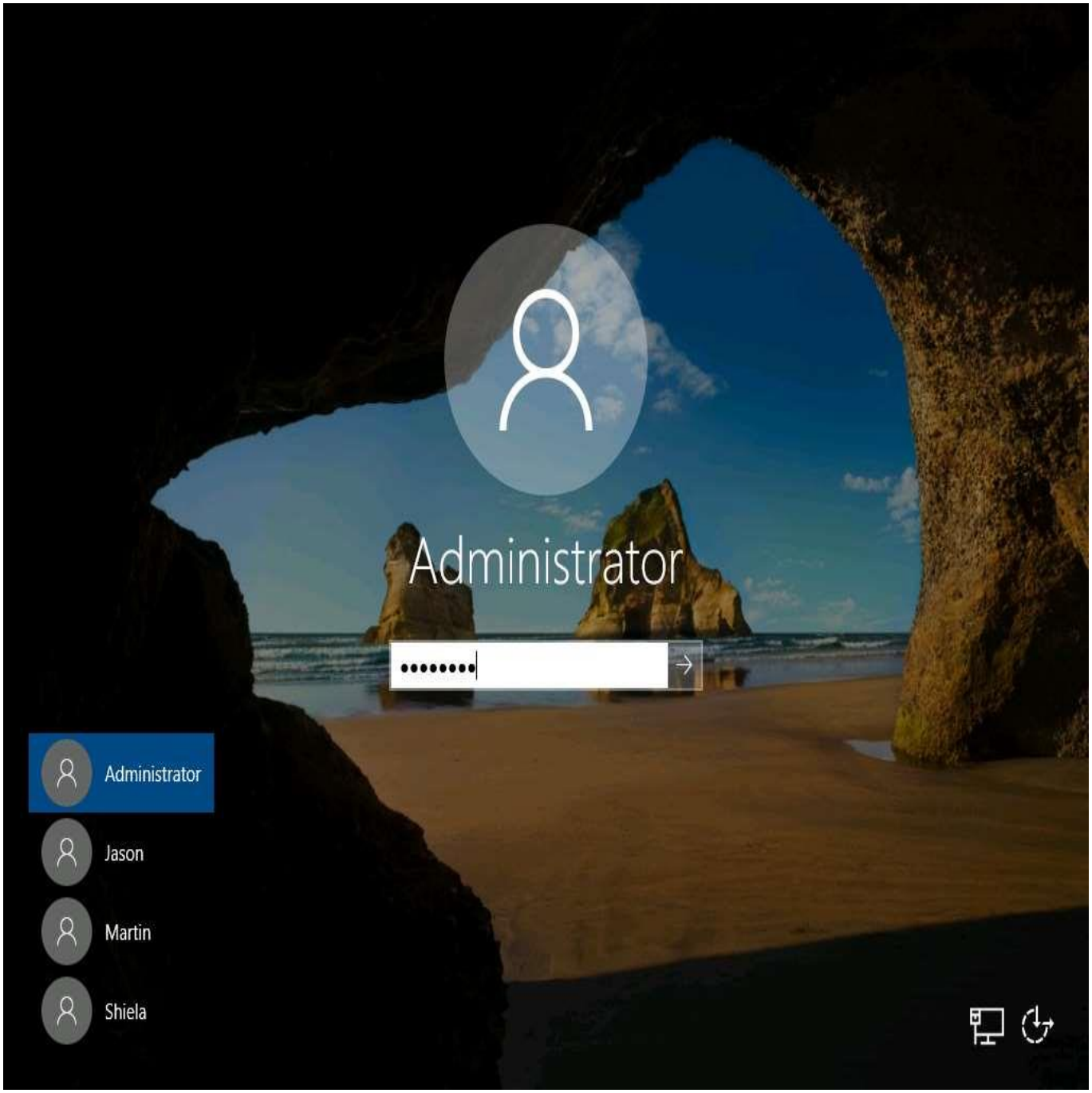


7. ☐ The **Anti-DDoS Wizard** window appears; click **Continue** in all the wizard steps, leaving all the default settings. In the last window, click **Finish**.
8. ☐ Click **Show hidden icons** from the bottom-right corner of **Desktop** and click the **Anti DDoS Guardian** icon.

9. ☐ The **Anti DDoS Guardian** window appears, displaying information about incoming and outgoing traffic, as shown in the screenshot.

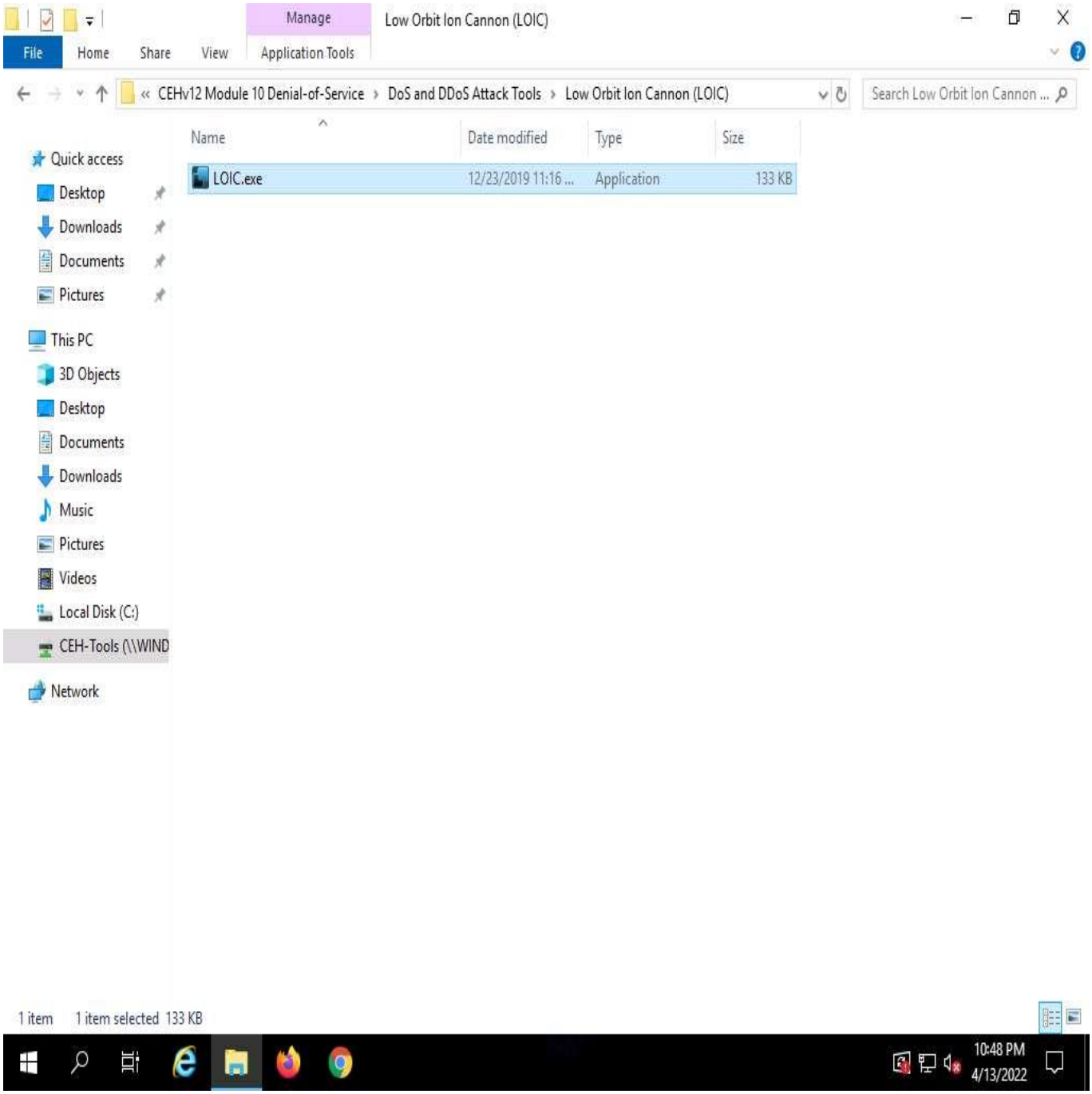


10. Now, click Windows Server 2019 to switch to the **Windows Server 2019** and click Ctrl+Alt+Delete to activate the machine. By default, **Administrator** profile is selected, click Pa$$w0rd to enter the password and press **Enter** to log in.

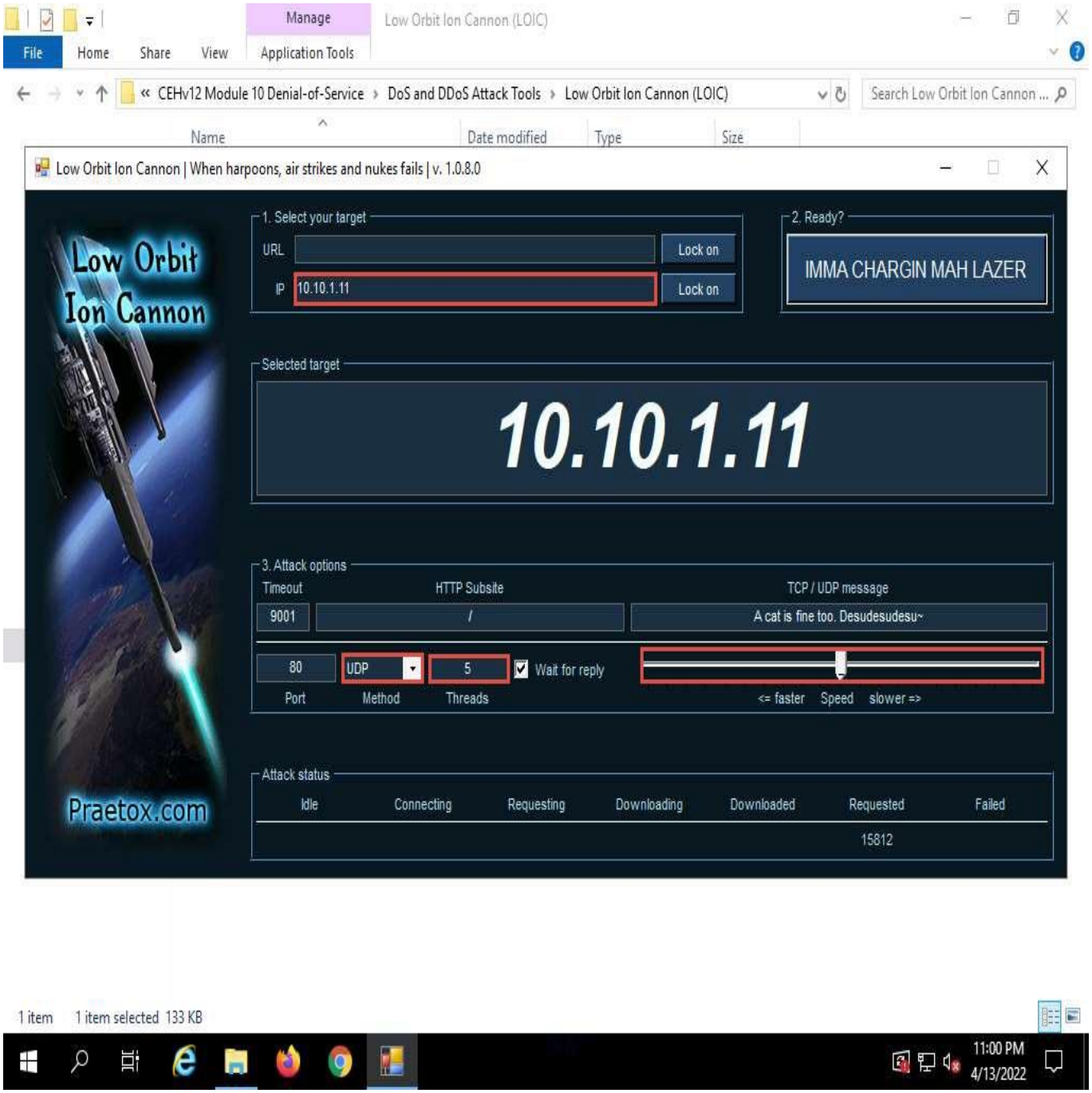


11. Navigate to **Z:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

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



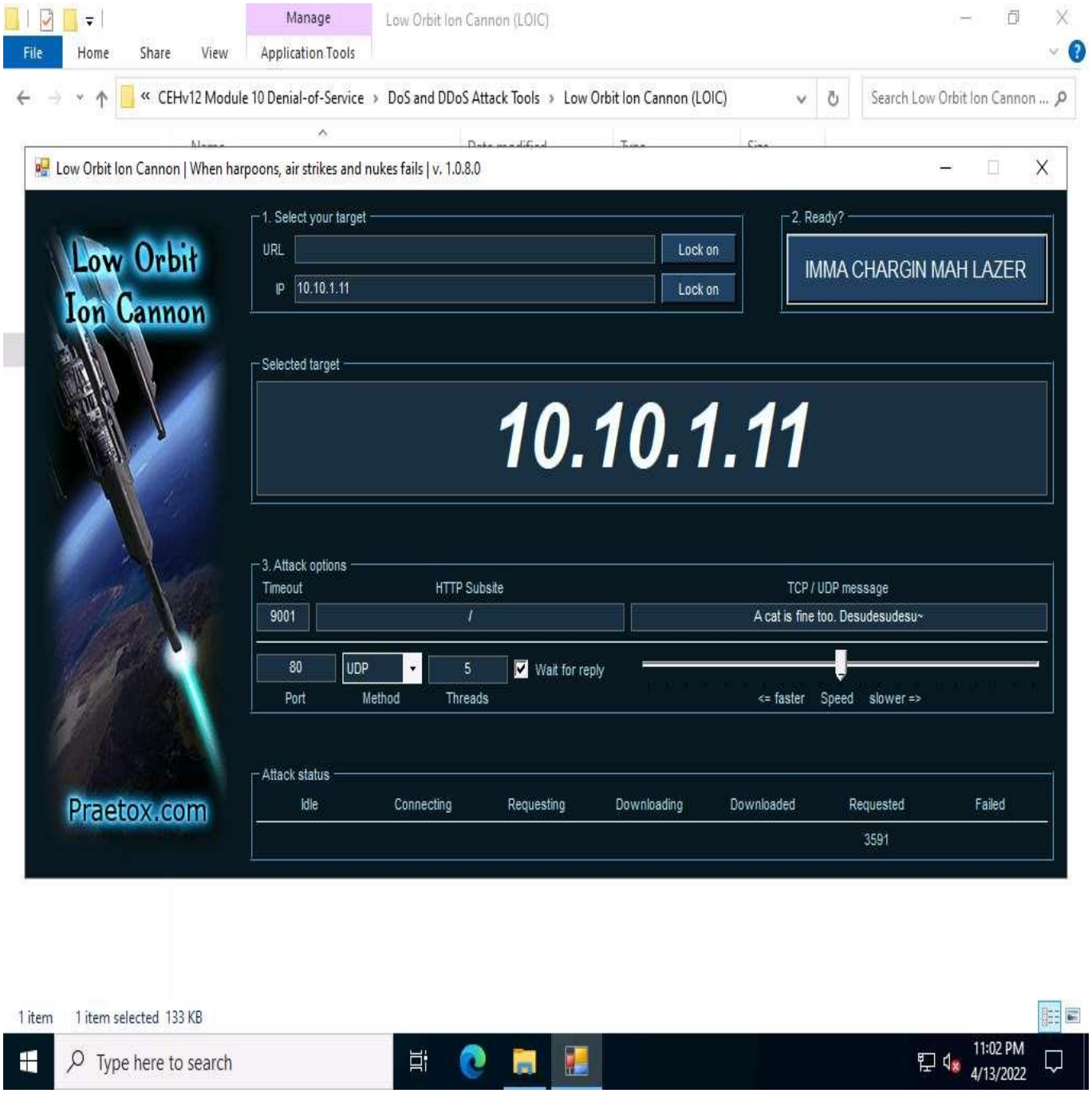
12. ☐ The **Low Orbit Ion Cannon** main window appears.
13. ☐ Perform the following settings:
    - Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.1.11**), and then click the **Lock on** button to add the target devices.
    - Under the **Attack options** section, select **UDP** from the drop-down list in **Method**. Set the thread's value to **5** under the **Threads** field. Slide the power bar to the middle.



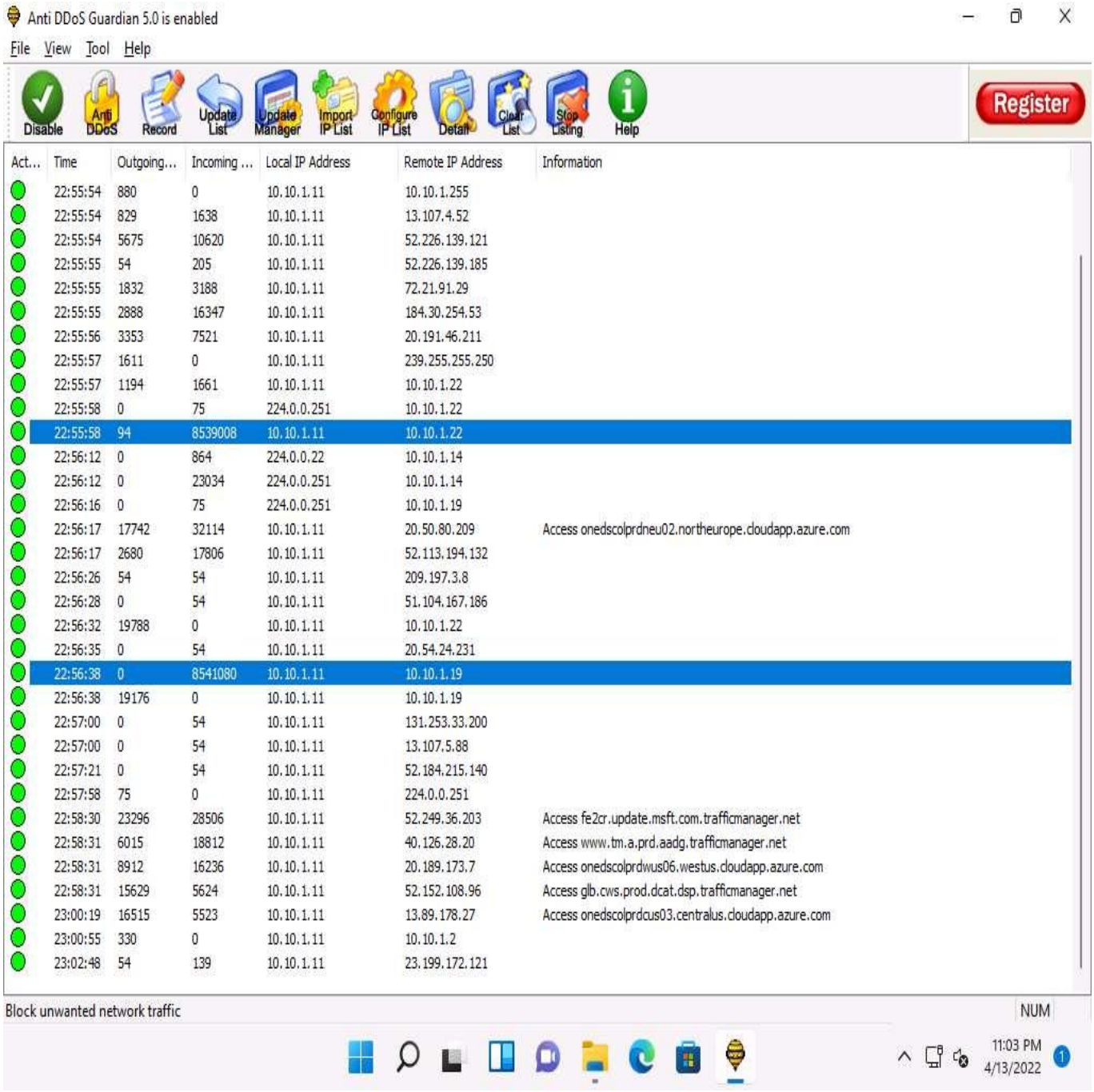
14. ☐ Now, switch to the **Windows Server 2022** machine and follow **Steps 11 - 13** to launch LOIC and configure it.

To switch to the **Windows Server 2022**, click Windows Server 2022.

15. ☐ Once **LOIC** is configured on all machines, switch to each machine (**Windows Server 2019**, and **Windows Server 2022**) and click the **IMMA CHARGIN MAH LAZER** button under the **Ready?** section to initiate the DDoS attack on the target **Windows 11** machine.



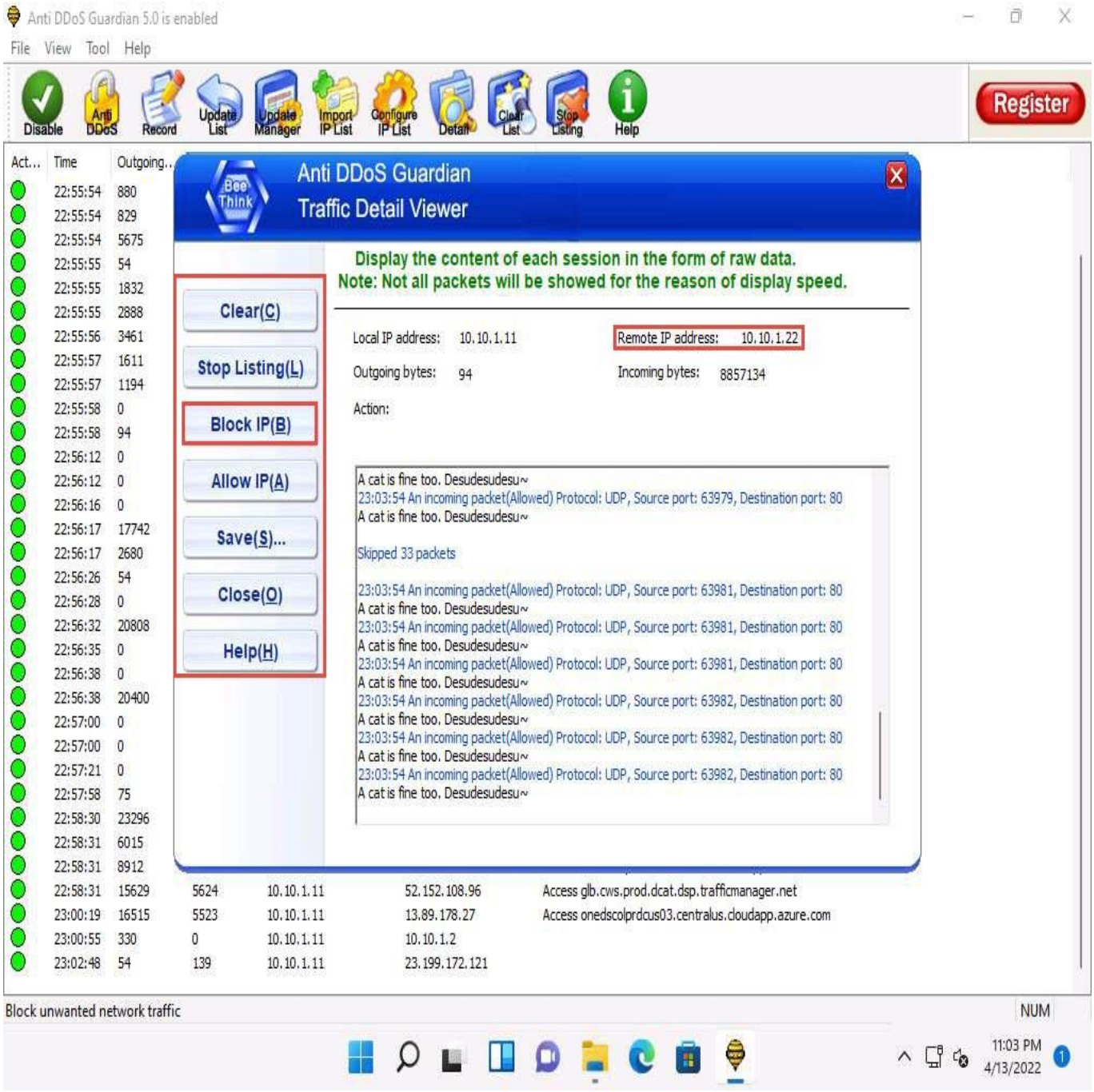
16. ☐ Click Windows 11 to switch back to the **Windows 11** machine and observe the packets captured by **Anti DDoS Guardian**.
17. ☐ Observe the huge number of packets coming from the host machines (**10.10.1.19 [Windows Server 2019**] and **10.10.1.22 [Windows Server 2022]**).



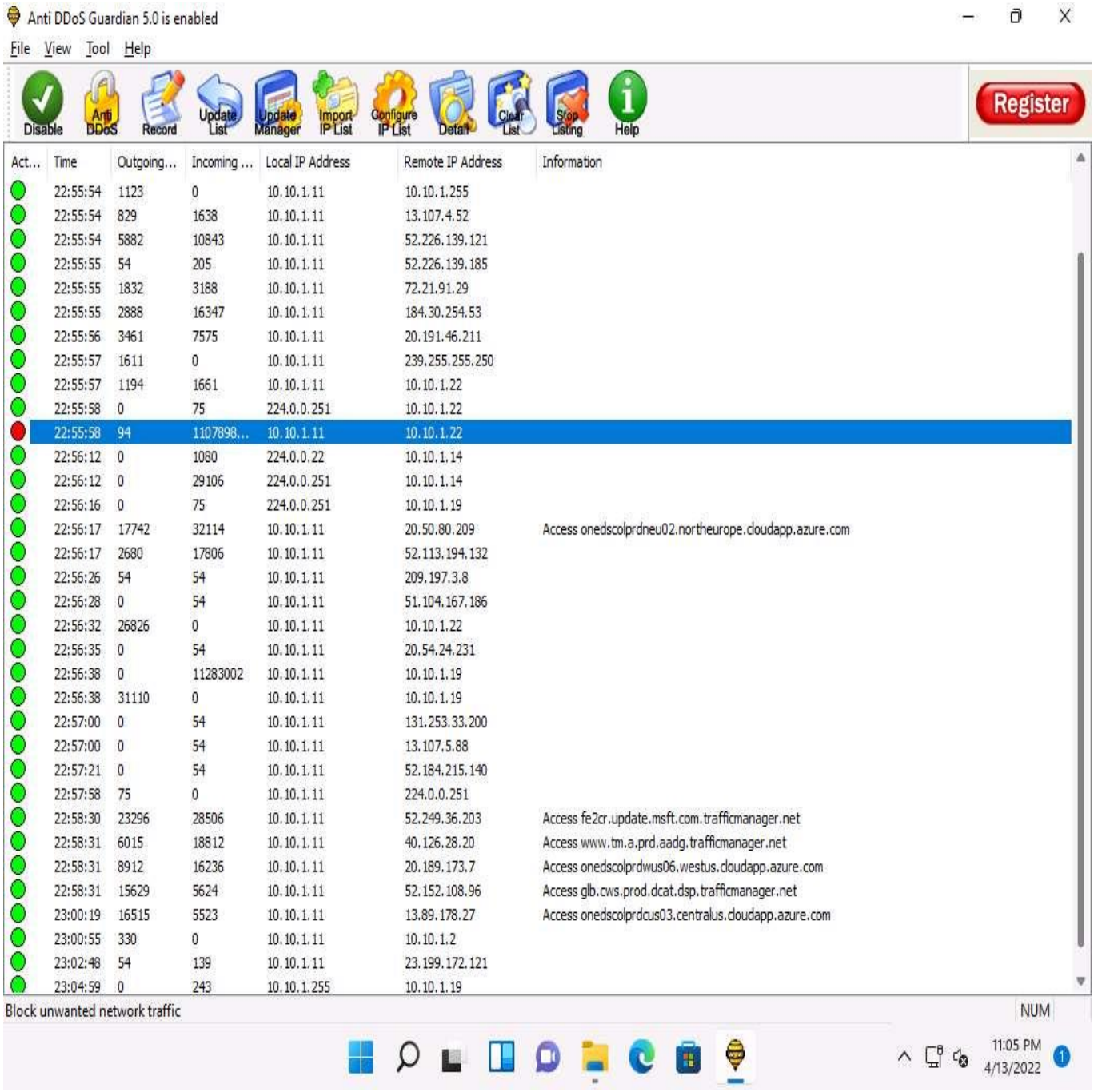
18. Double-click any of the sessions **10.10.1.19** or **10.10.1.22**.

Here, we have selected 10.10.1.22. You can select either of them.

19. The **Anti DDoS Guardian Traffic Detail Viewer** window appears, displaying the content of the selected session in the form of raw data. You can observe the high number of incoming bytes from **Remote IP address 10.10.1.22**, as shown in the screenshot.
20. You can use various options from the left-hand pane such as **Clear**, **Stop Listing**, **Block IP**, and **Allow IP**. Using the Block IP option blocks the IP address sending the huge number of packets.
21. In the **Traffic Detail Viewer** window, click **Block IP** option from the left pane.



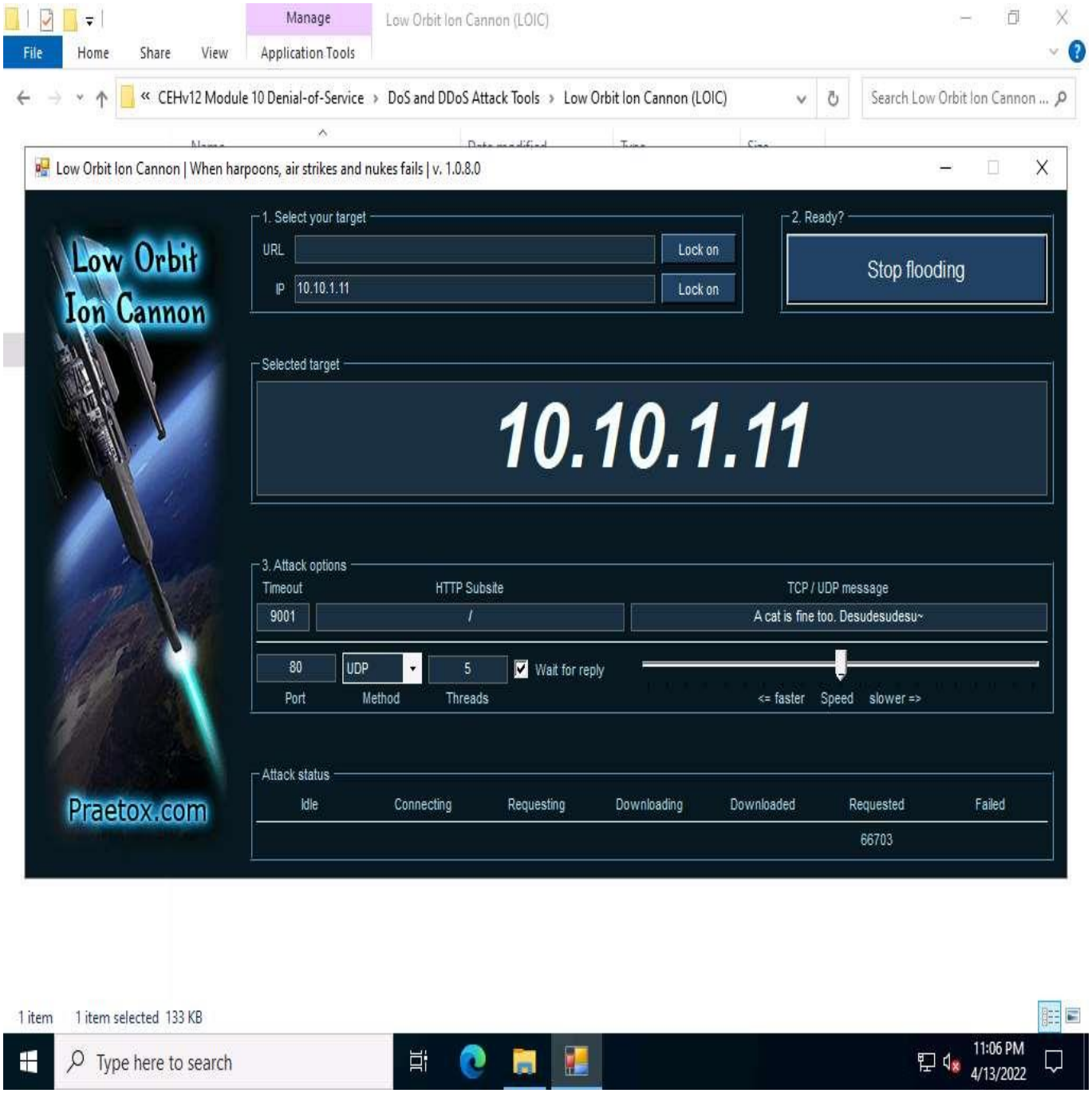
22. ☐ Observe that the blocked IP session turns red in the **Action Taken** column.



23. ☐ Similarly, you can **Block IP** the address of the **10.10.1.19** session.
24. ☐ On completion of the task, click **Stop flooding**, and then close the LOIC window on all the attacker machines. (**Windows Server 2019** and **Windows Server 2022**).

To switch to the **Windows Server 2019**, click Windows Server 2019.

To switch to the **Windows Server 2022**, click Windows Server 2022.



25. ☐ This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.
26. ☐ Close all open windows and document all the acquired information.
27. ☐ You can also use other DoS and DDoS protection tools such as, **DOSarrest's DDoS protection service** (https://www.dosarrest.com), **DDoS-GUARD** (https://ddos-guard.net), and **Cloudflare** (https://www.cloudflare.com) to protect organization's systems and networks from DoS and DDoS attacks.
28. ☐ Click Windows 11 to switch to the Windows 11 virtual machine. In **Windows 11** machine, navigate to **Control Panel** --> **Programs** --> **Programs and Features** and uninstall **Anti DDoS Guardian**.