

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 servers, 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.

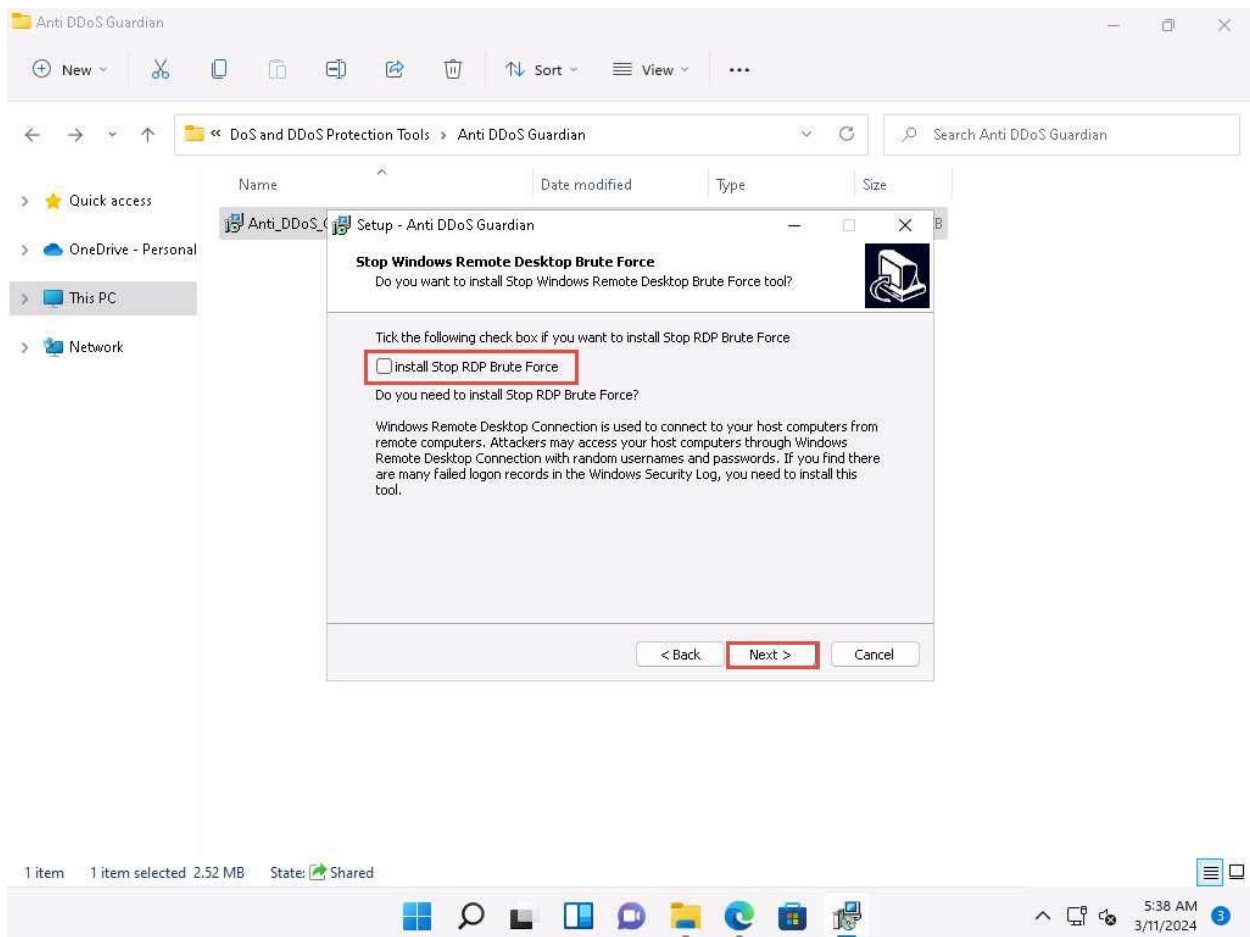
In this task, we will use the **Windows Server 2019** and **Windows Server 2022** machines to perform a DDoS attack on the target system, **Windows 11**.

1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv13 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**.

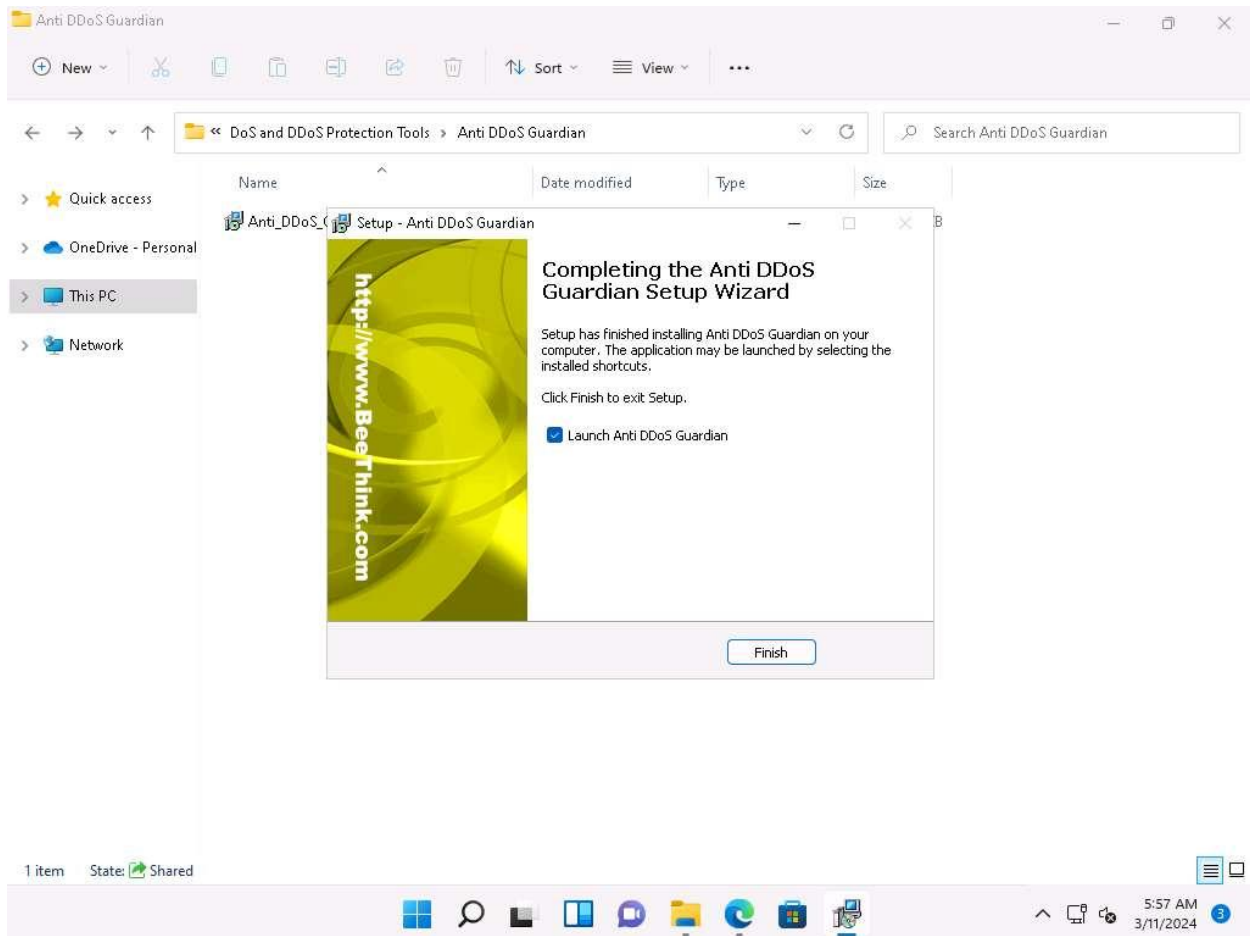
If an **Open File - Security Warning** pop-up appears, click **Run**.

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**.

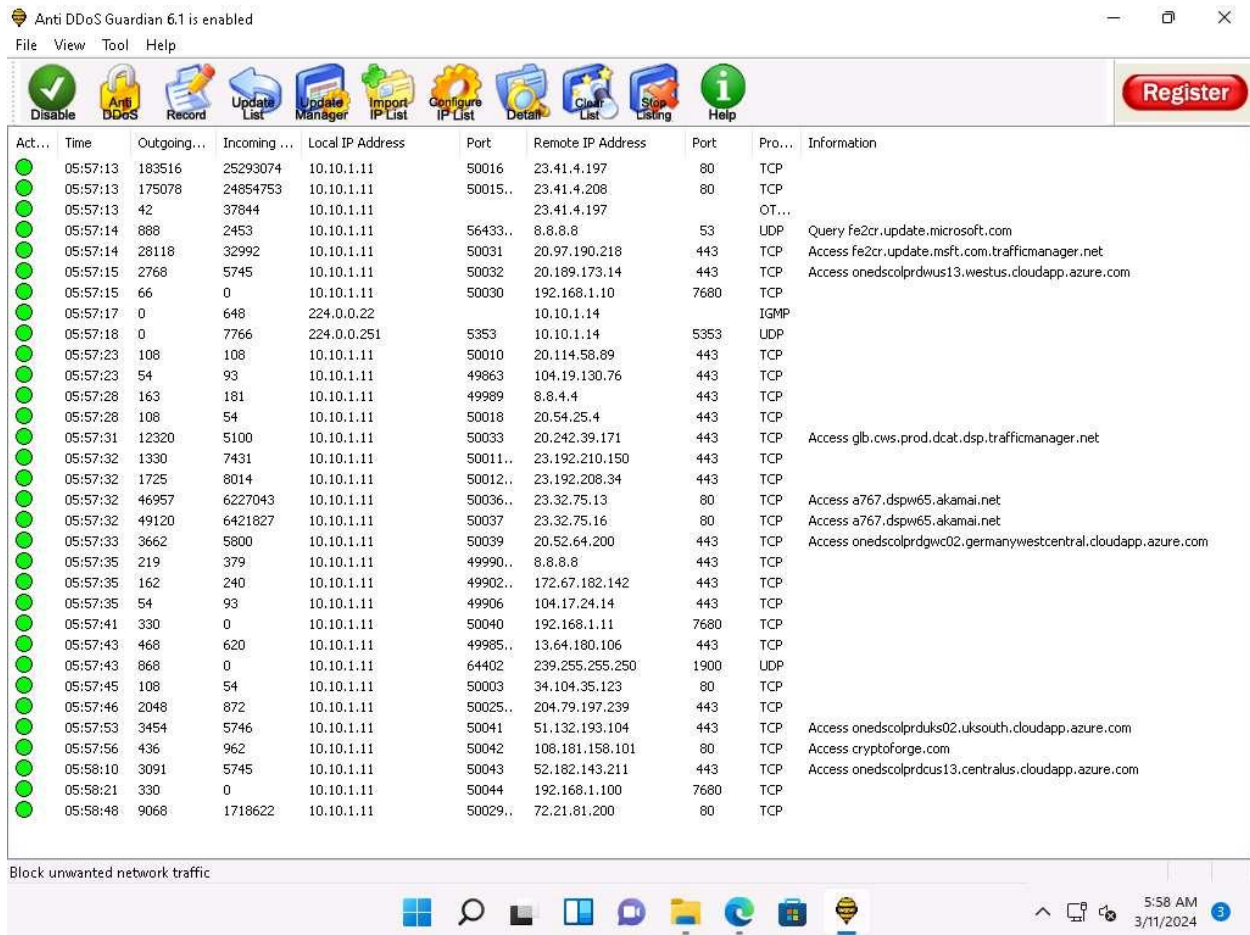


4. The **Select Additional Tasks** wizard appears; check the **Create a desktop shortcut** option, and click **Next**.
5. The **Ready to Install** wizard appears; click **Install**.

6. The **Completing the Anti DDoS Guardian Setup Wizard** window appears; ensure that **Launch Anti DDoS Guardian** option is selected 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. The **Anti DDoS Guardian** window appears, displaying information about incoming and outgoing traffic, as shown in the screenshot.



9. Now, click [Windows Server 2019](#) to switch to the **Windows Server 2019**. Login using **Administrator/P@ssw0rd**.

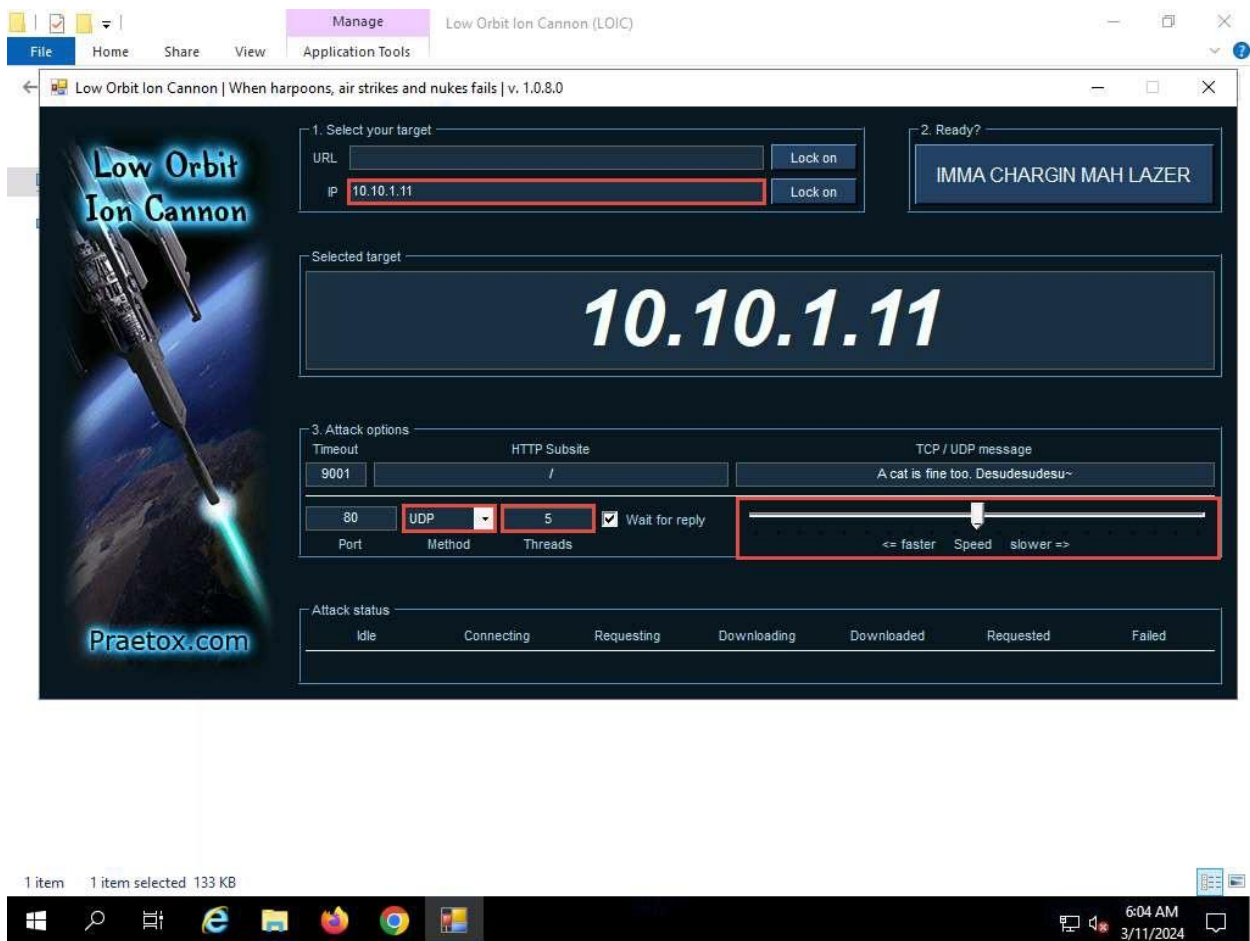
10. Navigate to **Z:\CEHv13 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

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

11. The **Low Orbit Ion Cannon** main window appears.

12. Perform the following settings:

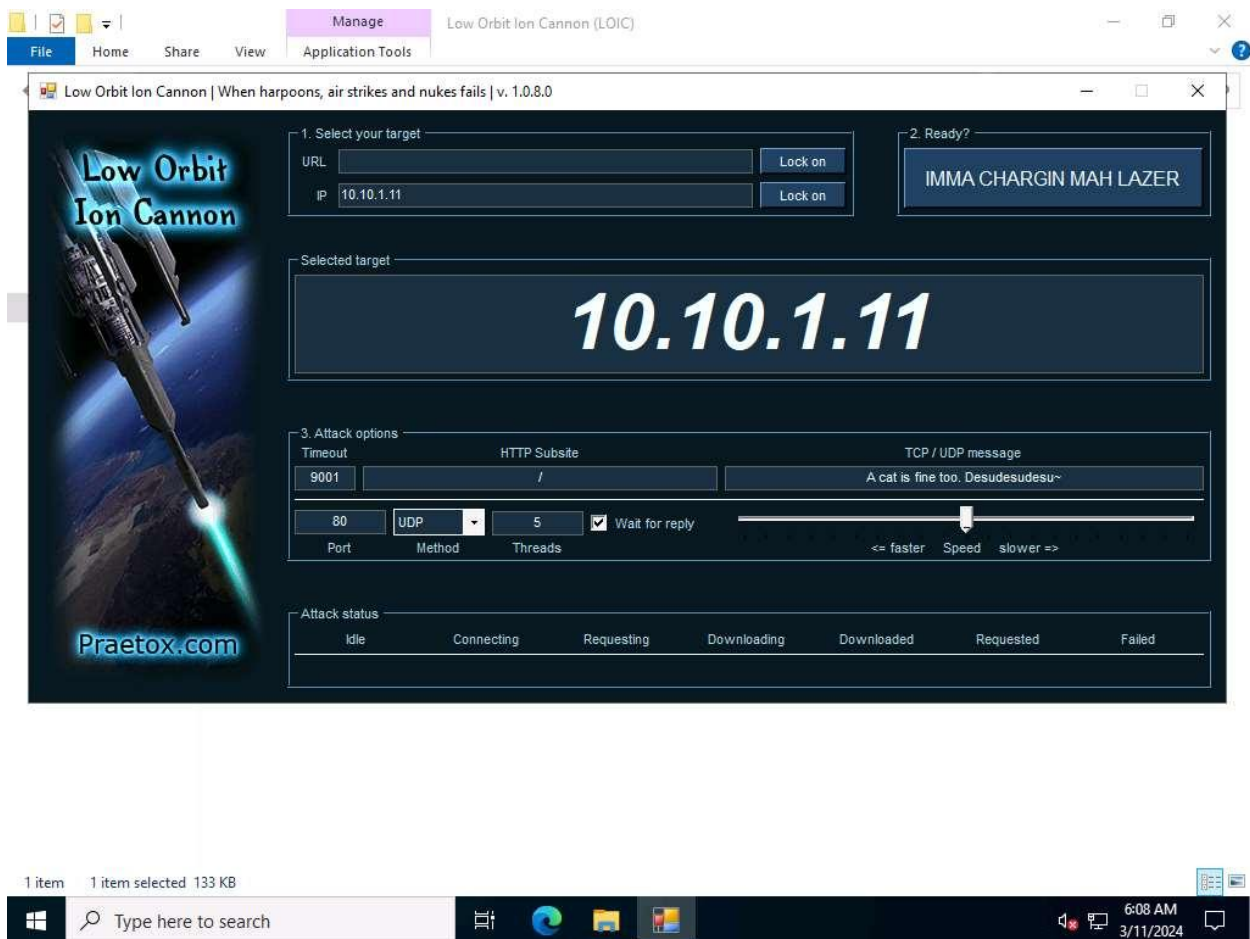
- Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.1.11**), and then click the **Lock on** button to add the target devices.
- Under the **Attack options** section, select **UDP** from the drop-down list in **Method**. Set the thread's value to **5** under the **Threads** field. Slide the power bar to the middle.



13. Now, switch to the **Windows Server 2022** machine and follow **Steps#10-12** to launch LOIC and configure it.

To switch to the **Windows Server 2022**, click [Windows Server 2022](#).

14. 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.



15. Click [Windows 11](#) to switch back to the **Windows 11** machine and observe the packets captured by **Anti DDoS Guardian**.
16. 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]**).

Anti DDoS Guardian 6.1 is enabled

File View Tool Help



Register

Act...	Time	Outgoing...	Incoming...	Local IP Address	Port	Remote IP Address	Port	Pro...	Information
●	06:04:09	63261	12569	10.10.1.11	50140..	20.189.173.9	443	TCP	Access onedscolprdwus08.westus.cloudapp.azure.com
●	06:04:15	31673	51319	10.10.1.11	50142..	13.89.179.10	443	TCP	Access onedscolprdcus12.centralus.cloudapp.azure.com
●	06:04:21	72200	13974564	10.10.1.11	50152..	23.40.41.58	80	TCP	Access a122.dscg3.akamai.net
●	06:04:23	18101	28740	10.10.1.11	50154..	52.182.143.213	443	TCP	Access onedscolprdcus16.centralus.cloudapp.azure.com
●	06:04:29	13956	1914337	10.10.1.11	50162..	23.40.41.32	80	TCP	Access a122.dscg3.akamai.net
●	06:04:31	1365	7367	10.10.1.11	50164	20.231.239.246	443	TCP	Access reroute443.trafficmanager.net
●	06:04:31	5561	26381	10.10.1.11	50167..	204.79.197.203	80..	TCP	Access a-0003.a-msedge.net
●	06:04:31	1632	23783	10.10.1.11	50168	52.96.165.2	443	TCP	Access ooc-g2.tm-4.office.com
●	06:04:31	81739	14434524	10.10.1.11	50169..	23.40.41.4	80	TCP	Access a122.dscg3.akamai.net
●	06:04:31	1556	8336	10.10.1.11	50171	52.113.194.132	443	TCP	Access s-0005.s-msedge.net
●	06:04:31	1638	8373	10.10.1.11	50173	13.107.246.70	443	TCP	Access part-0042.t-0009.t-msedge.net
●	06:04:33	1320	0	10.10.1.11	50179..	20.20.10.10	7680	TCP	
●	06:05:03	22413	34121	10.10.1.11	50211..	20.189.173.16	443	TCP	Access onedscolprdwus17.westus.cloudapp.azure.com
●	06:05:10	6226	12836	10.10.1.11	50236..	51.104.167.245	443	TCP	Access array608.prod.do.dsp.mp.microsoft.com
●	06:05:15	14353	22790	10.10.1.11	50242..	20.189.173.8	443	TCP	Access onedscolprdwus07.westus.cloudapp.azure.com
●	06:05:18	3758	5746	10.10.1.11	50251	20.42.73.25	443	TCP	Access onedscolprdeus06.eastus.cloudapp.azure.com
●	06:05:49	15235	22685	10.10.1.11	50269..	20.189.173.12	443	TCP	Access onedscolprdwus11.westus.cloudapp.azure.com
●	06:05:52	52570	35523	10.10.1.11	50275..	13.85.23.206	443	TCP	Access glb.cws.prod.dcat.dsp.trafficmanager.net
●	06:06:01	0	220	10.10.1.11		38.104.127.57		ICMP	
●	06:06:33	4148	7464	10.10.1.11	50313..	51.104.167.255	443	TCP	Access array609.prod.do.dsp.mp.microsoft.com
●	06:07:34	0	75	224.0.0.251	5353	10.10.1.22	5353	UDP	
●	06:07:34	0	69	224.0.0.252	5355	10.10.1.22	53543	UDP	
●	06:07:42	0	108	224.0.0.22		10.10.1.22		IGMP	
●	06:07:42	0	4460	239.255.255.250	3702	10.10.1.22	53544	UDP	
●	06:07:43	34273	57260	10.10.1.11	50339..	40.74.98.194	443	TCP	Access onedscolprdjpw02.japanwest.cloudapp.azure.com
●	06:07:53	154656	34516	10.10.1.11	445	10.10.1.22	64050..	TCP	
●	06:08:09	25901	31982	10.10.1.11	50356	20.163.45.186	443	TCP	Access fe2cr.update.msft.com.trafficmanager.net
●	06:08:25	10437	11708	10.10.1.11	50388..	20.189.173.13	443	TCP	Access onedscolprdwus12.westus.cloudapp.azure.com
●	06:09:06	0	8832566	10.10.1.11	80	10.10.1.22	55027..	UDP	
●	06:09:06	764592	0	10.10.1.11		10.10.1.22		ICMP	
●	06:09:16	1074162	0	10.10.1.11		10.10.1.19		ICMP	
●	06:09:35	1336	3721	10.10.1.11	50404	20.54.24.231	443	TCP	Access array614.prod.do.dsp.mp.microsoft.com
●	06:09:37	9712	17346	10.10.1.11	50405..	20.52.64.201	443	TCP	Access onedscolprdgwc05.germanywestcentral.cloudapp.azure.com

Block unwanted network traffic



6:15 AM 3/11/2024

Anti DDoS Guardian 6.1 is enabled

File View Tool Help

Disable Anti DDoS Record Update List Update Manager Import IP List Configure IP List Details Clear List Stop Listing Help

Register

Act...	Time	Outgoing...	Incoming...	Local IP Address	Port	Remote IP Address	Port	Pro...	Information
●	05:59:16	0	150	224.0.0.251	5353	10.10.1.19	5353	UDP	
●	05:59:16	97	0	10.10.1.11	5353	224.0.0.251	5353	UDP	
●	05:59:16	106	9990074	10.10.1.11	5355..	10.10.1.19	61395..	UDP	
●	05:59:21	0	108	224.0.0.22		10.10.1.19		IGMP	
●	05:59:21	0	4464	239.255.255.250	3702	10.10.1.19	62319	UDP	
●	05:59:32	0	1268	10.10.1.255	138..	10.10.1.22	138..	UDP	
●	05:59:41	1980	0	10.10.1.11	50049..	192.168.10.101	7680	TCP	
●	06:00:21	660	0	10.10.1.11	50051..	10.0.0.16	7680	TCP	
●	06:00:50	162	278	10.10.1.11	49933..	96.7.157.142	443	TCP	
●	06:00:53	54	237	10.10.1.11	49857	151.101.1.44	443	TCP	
●	06:00:53	54	127	10.10.1.11	49859	35.208.249.213	443	TCP	
●	06:00:53	54	127	10.10.1.11	49868	35.213.89.133	443	TCP	
●	06:01:19	1242	0	10.10.1.11	138	10.10.1.255	138	UDP	
●	06:01:36	462927	39898	10.10.1.11	445	10.10.1.19	49716..	TCP	
●	06:02:05	27781	12406	10.10.1.11	50054..	20.189.173.3	443	TCP	Access onedscolprdwus02.westus.cloudapp.azure.com
●	06:02:06	17266	219402	10.10.1.11	50055	40.119.249.228	443	TCP	Access settings-prod-sea-2.southeastasia.cloudapp.azure.com
●	06:02:31	54	127	10.10.1.11	49956	34.117.35.28	443	TCP	
●	06:02:52	2065	8652	10.10.1.11	50057	20.191.46.109	443	TCP	
●	06:03:03	441719	286923	10.10.1.11	50059..	40.65.209.51	443	TCP	Access tsfe.trafficmanager.net
●	06:03:04	100771	79686	10.10.1.11	50060..	20.166.126.56	443	TCP	Access glb.cws.prod.dcat.dsp.trafficmanager.net
●	06:03:05	4445	13413	10.10.1.11	50064..	23.41.4.206	80	TCP	Access a1683.dscd.akamai.net
●	06:03:05	207446	36864133	10.10.1.11	50065..	23.40.41.25	80	TCP	Access a122.dscg3.akamai.net
●	06:03:05	15114	23059	10.10.1.11	50066..	20.189.173.7	443	TCP	Access onedscolprdwus06.westus.cloudapp.azure.com
●	06:03:05	112495	20033879	10.10.1.11	50067..	23.40.41.18	80	TCP	Access a122.dscg3.akamai.net
●	06:03:14	1672492	291051514	10.10.1.11	50072..	72.21.81.240	80	TCP	Access cs11.wpc.v0cdn.net
●	06:03:14	59357	9562958	10.10.1.11	50076..	23.40.41.11	80	TCP	Access a122.dscg3.akamai.net
●	06:03:14	10030	17086	10.10.1.11	50077..	20.189.173.6	443	TCP	Access onedscolprdwus05.westus.cloudapp.azure.com
●	06:03:20	4423	46534	10.10.1.11	50081..	13.107.5.88	443	TCP	Access e-0009.e-msedge.net
●	06:03:20	1740	3402	10.10.1.11	50083..	192.229.211.108	80	TCP	Access fp2e7a.wpc.phicdn.net
●	06:03:21	6509	62751	10.10.1.11	50086..	23.41.4.207	80	TCP	Access a1683.dscd.akamai.net
●	06:03:21	3269	0	10.10.1.11		8.8.8.8		ICMP	
●	06:03:32	3732	5650	10.10.1.11	50097	20.42.65.85	443	TCP	Access onedscolprdwus05.eastus.cloudapp.azure.com
●	06:03:34	10514	17182	10.10.1.11	50100..	20.189.173.5	443	TCP	Access onedscolprdwus04.westus.cloudapp.azure.com
●	06:03:35	6176	11438	10.10.1.11	50109..	20.189.173.18	443	TCP	Access onedscolprdwus15.westus.cloudapp.azure.com

Block unwanted network traffic

6:16 AM 3/11/2024

17. 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.

18. 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**.

19. You can use various options from the left-hand pane such as **Clear**, **Stop Listing**, **Block IP**, and **Allow IP**. Using the **Block IP (B)** option blocks the IP address sending the huge number of packets.

20. In the **Traffic Detail Viewer** window, click **Block IP** option from the left pane.

Anti DDoS Guardian 6.1 is enabled

File View Tool Help

Disable Anti DDoS Record Update Update Manager Import IP List Configure IP List Details Clear List Stop Listing Help

Register

Act...	Time	Outgoing...
06:04:09	63261	
06:04:15	31673	
06:04:21	72200	
06:04:23	18101	
06:04:29	13956	
06:04:31	1365	
06:04:31	5561	
06:04:31	1632	
06:04:31	81739	
06:04:31	1556	
06:04:31	1638	
06:04:33	1320	
06:05:03	22413	
06:05:10	6226	
06:05:15	14353	
06:05:18	3758	
06:05:49	15235	
06:05:52	52570	
06:06:01	0	
06:06:33	4148	
06:07:34	0	
06:07:34	0	
06:07:42	0	
06:07:42	0	
06:07:43	34273	
06:07:53	156356	
06:08:09	25901	
06:08:25	10437	
06:09:06	0	
06:09:06	1206762	0 10.10.1.11 10.10.1.22 ICMP
06:09:16	1690446	0 10.10.1.11 10.10.1.19 ICMP
06:09:35	1336	3721 10.10.1.11 50404 20.54.24.231 443 TCP Access array614.prod.do.dsp.mp.microsoft.com
06:09:37	9712	17346 10.10.1.11 50405.. 20.52.64.201 443 TCP Access onedscolprdgwc05.germanywestcentral.cloudapp.azure.com

Block unwanted network traffic

Windows Taskbar: 6:17 AM 3/11/2024

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

Anti DDoS Guardian 6.1 is enabled

File View Tool Help

Disable Anti DDoS Record Update List Update Manager Import IP List Configure IP List Details Clear List Stop Listing Help

Register

Act...	Time	Outgoing...	Incoming...	Local IP Address	Port	Remote IP Address	Port	Pro...	Information
●	06:04:15	31673	51319	10.10.1.11	50142..	13.89.179.10	443	TCP	Access onedscolprdcus12.centralus.cloudapp.azure.com
●	06:04:21	72200	13974564	10.10.1.11	50152..	23.40.41.58	80	TCP	Access a122.dscg3.akamai.net
●	06:04:23	18101	28740	10.10.1.11	50154..	52.182.143.213	443	TCP	Access onedscolprdcus16.centralus.cloudapp.azure.com
●	06:04:29	13956	1914337	10.10.1.11	50162..	23.40.41.32	80	TCP	Access a122.dscg3.akamai.net
●	06:04:31	1365	7367	10.10.1.11	50164	20.231.239.246	443	TCP	Access reroute443.trafficmanager.net
●	06:04:31	5561	26381	10.10.1.11	50167..	204.79.197.203	80..	TCP	Access a-0003.a-msedge.net
●	06:04:31	1632	23783	10.10.1.11	50168	52.96.165.2	443	TCP	Access ooc-g2.tm-4.office.com
●	06:04:31	81739	14434524	10.10.1.11	50169..	23.40.41.4	80	TCP	Access a122.dscg3.akamai.net
●	06:04:31	1556	8336	10.10.1.11	50171	52.113.194.132	443	TCP	Access s-0005.s-msedge.net
●	06:04:31	1638	8373	10.10.1.11	50173	13.107.246.70	443	TCP	Access part-0042.t-0009.t-msedge.net
●	06:04:33	1650	0	10.10.1.11	50179..	20.20.10.10	7680	TCP	
●	06:05:03	22413	34121	10.10.1.11	50211..	20.189.173.16	443	TCP	Access onedscolprdcus17.westus.cloudapp.azure.com
●	06:05:10	6226	12836	10.10.1.11	50236..	51.104.167.245	443	TCP	Access array608.prod.do.dsp.mp.microsoft.com
●	06:05:15	14353	22790	10.10.1.11	50242..	20.189.173.8	443	TCP	Access onedscolprdcus07.westus.cloudapp.azure.com
●	06:05:18	3758	5746	10.10.1.11	50251	20.42.73.25	443	TCP	Access onedscolprdcus06.eastus.cloudapp.azure.com
●	06:05:49	15235	22685	10.10.1.11	50269..	20.189.173.12	443	TCP	Access onedscolprdcus11.westus.cloudapp.azure.com
●	06:05:52	52570	35523	10.10.1.11	50275..	13.85.23.206	443	TCP	Access glb.cws.prod.dcat.dsp.trafficmanager.net
●	06:06:01	0	330	10.10.1.11		38.104.127.57		ICMP	
●	06:06:33	4148	7464	10.10.1.11	50313..	51.104.167.255	443	TCP	Access array609.prod.do.dsp.mp.microsoft.com
●	06:07:34	0	75	224.0.0.251	5353	10.10.1.22	5353	UDP	
●	06:07:34	0	69	224.0.0.252	5355	10.10.1.22	53543	UDP	
●	06:07:42	0	108	224.0.0.22		10.10.1.22		IGMP	
●	06:07:42	0	4460	239.255.255.250	3702	10.10.1.22	53544	UDP	
●	06:07:43	34273	57260	10.10.1.11	50339..	40.74.98.194	443	TCP	Access onedscolprdcus02.japanwest.cloudapp.azure.com
●	06:07:53	157266	39958(Bl...	10.10.1.11	445	10.10.1.22	64050..	TCP	
●	06:08:09	25901	31982	10.10.1.11	50356	20.163.45.186	443	TCP	Access fe2cr.update.msft.com.trafficmanager.net
●	06:08:25	10437	11708	10.10.1.11	50388..	20.189.173.13	443	TCP	Access onedscolprdcus12.westus.cloudapp.azure.com
●	06:09:06	0	1382959...	10.10.1.11	80..	10.10.1.22	55027..	UDP	
●	06:09:06	1207578	0	10.10.1.11		10.10.1.22		ICMP	
●	06:09:16	1696974	0	10.10.1.11		10.10.1.19		ICMP	
●	06:09:35	1336	3721	10.10.1.11	50404	20.54.24.231	443	TCP	Access array614.prod.do.dsp.mp.microsoft.com
●	06:09:37	9712	17346	10.10.1.11	50405..	20.52.64.201	443	TCP	Access onedscolprdcus05.germanywestcentral.cloudapp.azure.com
●	06:18:03	17329	5748	10.10.1.11	50432	104.208.16.89	443	TCP	Access onedscolprdcus11.centralus.cloudapp.azure.com

Block unwanted network traffic

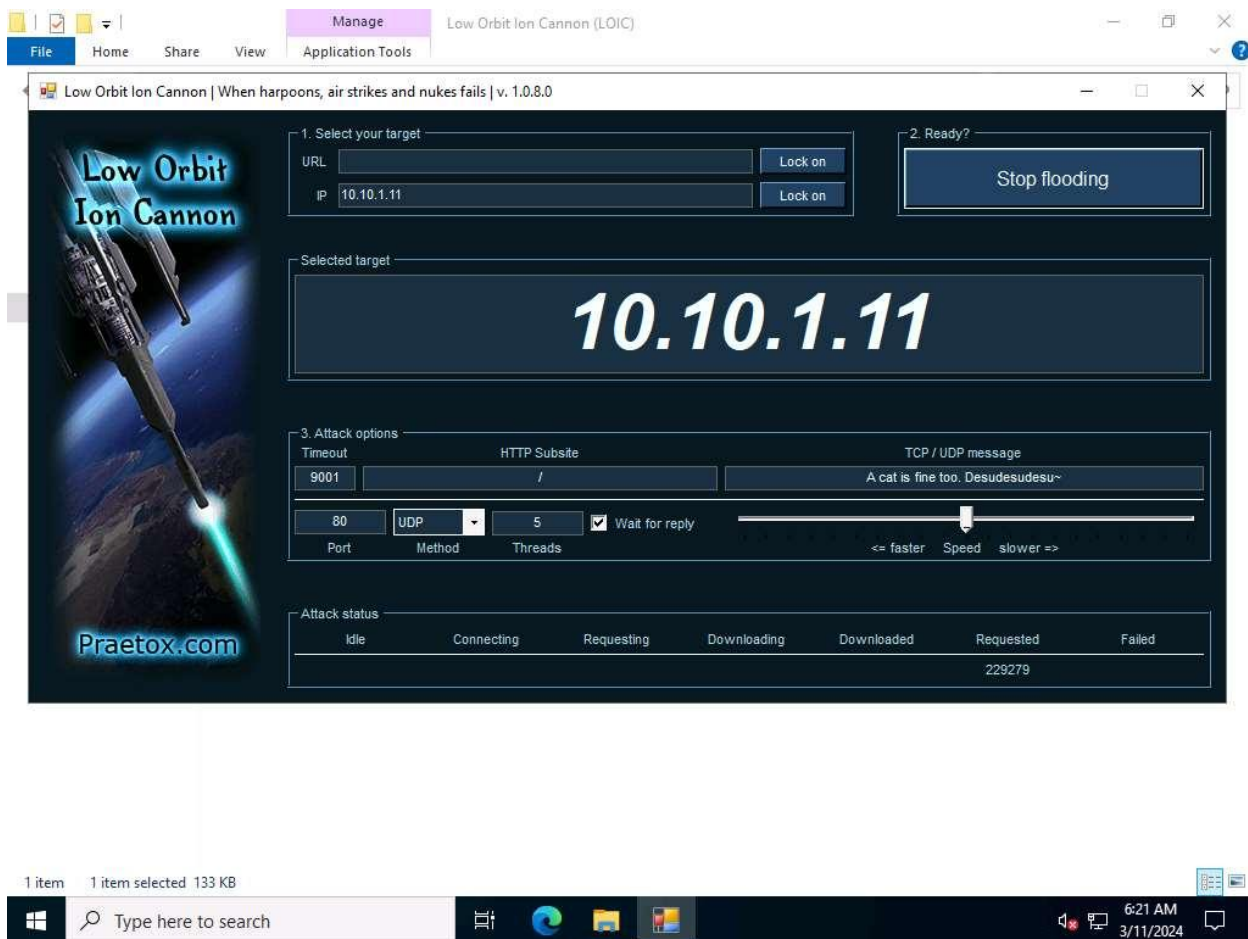
6:18 AM 3/11/2024

22. Similarly, you can **Block IP** the address of the **10.10.1.19** session.

23. 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](#).



24. This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.
25. Close all open windows and document all the acquired information.
26. 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>), **Radware DefensePro X** (<https://www.radware.com>), **F5 DDoS Attack Protection** (<https://www.f5.com>) to protect organization's systems and networks from DoS and DDoS attacks.
27. 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**.

Question 10.2.1.1

For this task, first use the LOIC tool on the Windows Server 2019 and Windows Server 2022 machines to perform a DDoS attack on the Windows 11 target system. Then, use the Anti DDoS Guardian tool on the Windows 11 machine to detect and protect against the DDoS attack. Which Anti DDoS Guardian option will you use to stop an ongoing DoS attack?