

# CEH Module 10: DOS & DDOS

## Assignment - 06

(Marepalli Rakesh)

---

### Given Lab Scenario

DoS and DDoS attacks have become popular, because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous, because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of these attacks includes loss of goodwill, disabled networks, financial loss, and disabled organizations. In a DDoS attack, many applications pound the target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable. The attacker initiates the DDoS attack by sending a command to the zombie agents.

These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim's machine instead of as zombie agents, because of the spoofing of the source IP address. Hence, they send the requested information (response to connection request) to the victim. The victim's machine is flooded with unsolicited responses from several reflector computers at once. This may reduce performance or may even cause the victim's machine to shut down completely.

As an expert ethical hacker or pen tester, you must have the required knowledge to perform DoS and DDoS attacks to be able to test systems in the target network. In this lab, you will gain hands-on experience in auditing network resources against DoS and DDoS attacks.

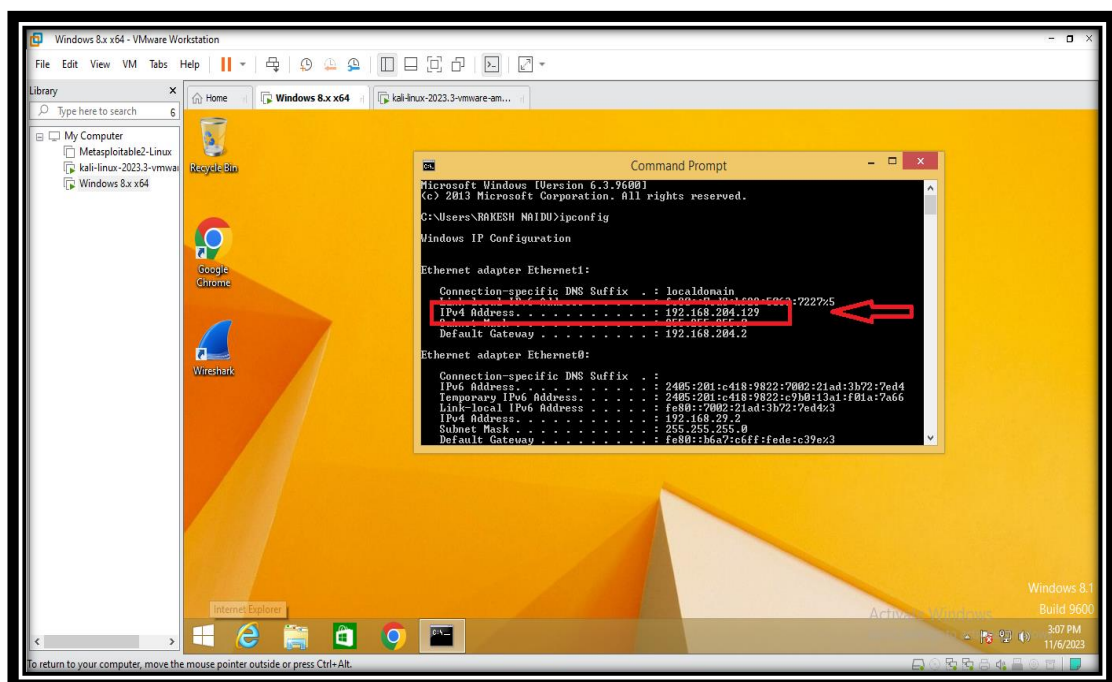
### Given Lab Objectives:

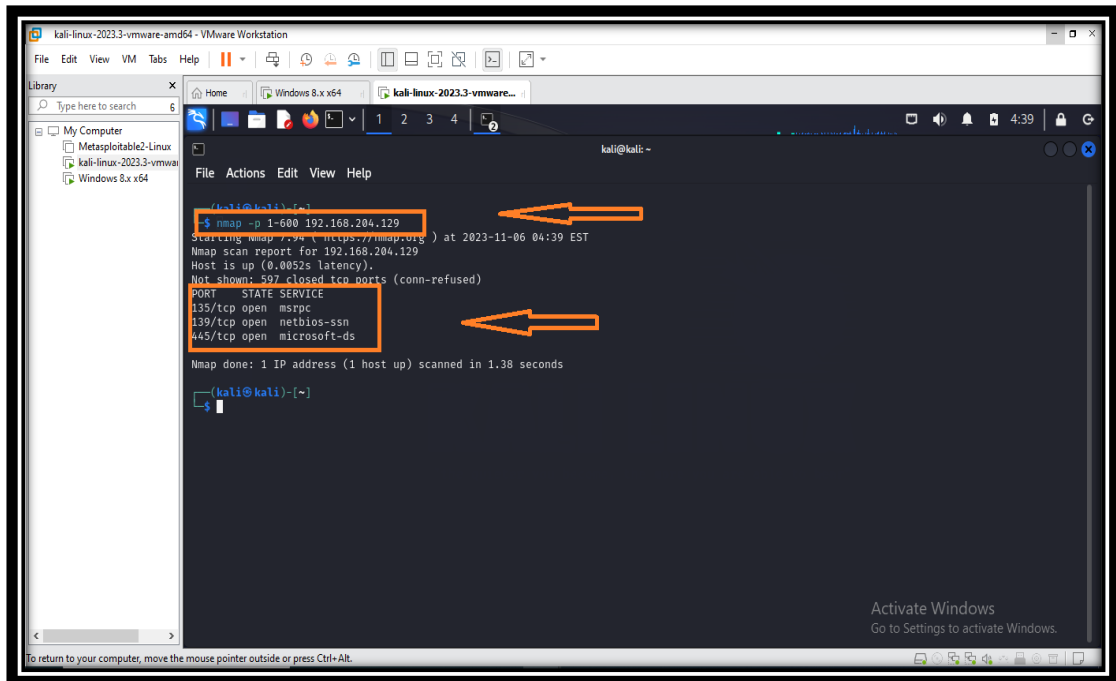
- Perform a DoS attack (SYN flooding) on a target host using Metasploit
- Perform a DoS attack on a target host using hping3
- Perform a DDoS attack using HOIC

## Objective: 01

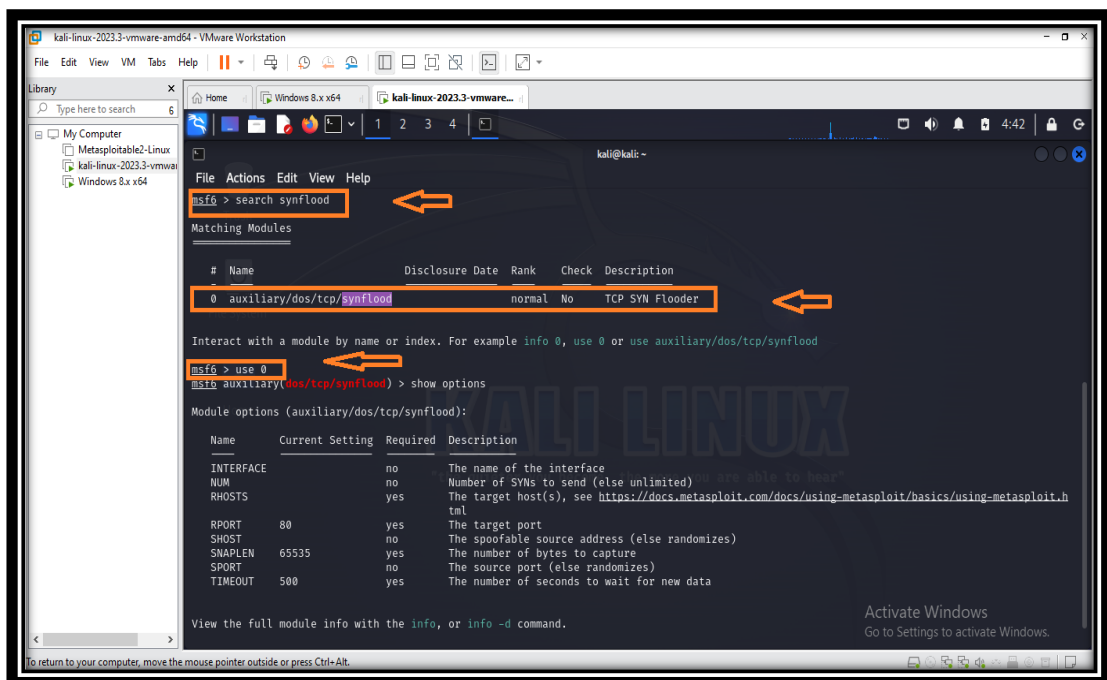
### Perform a DoS attack (SYN flooding) on a target host using Metasploit

- A SYN flood attack is a type of Denial of Service (DoS) attack that targets the three-way handshake process in the Transmission Control Protocol (TCP), a fundamental protocol in the functioning of the internet. By overwhelming a target server with a flood of SYN (synchronize) requests without completing the handshake, the attacker can exhaust the server's resources, rendering it unavailable to legitimate users.
- Metasploit, a widely known and versatile penetration testing framework, is an invaluable tool for both security professionals and malicious actors. It provides a range of modules and exploits that can be used to test and assess the security of systems. In this assignment, we will explore how a SYN flood attack can be executed using Metasploit.
- For this assignment, I set up a virtual environment using VMware, which included a Kali Linux VM and a Windows 8 VM. After launching the VMs, I identified the IP address of the Windows 8 VM, which was 192.168.204.129. To initiate the assignment, I performed a port scanning operation from the Kali Linux terminal using the 'nmap' command. I focused the scan on ports within the range of 1-600 to optimize time and resource usage. The objective was to identify open ports on my victim machine, which, in this case, was the Windows 8 VM. The scan revealed that port 135 was open.



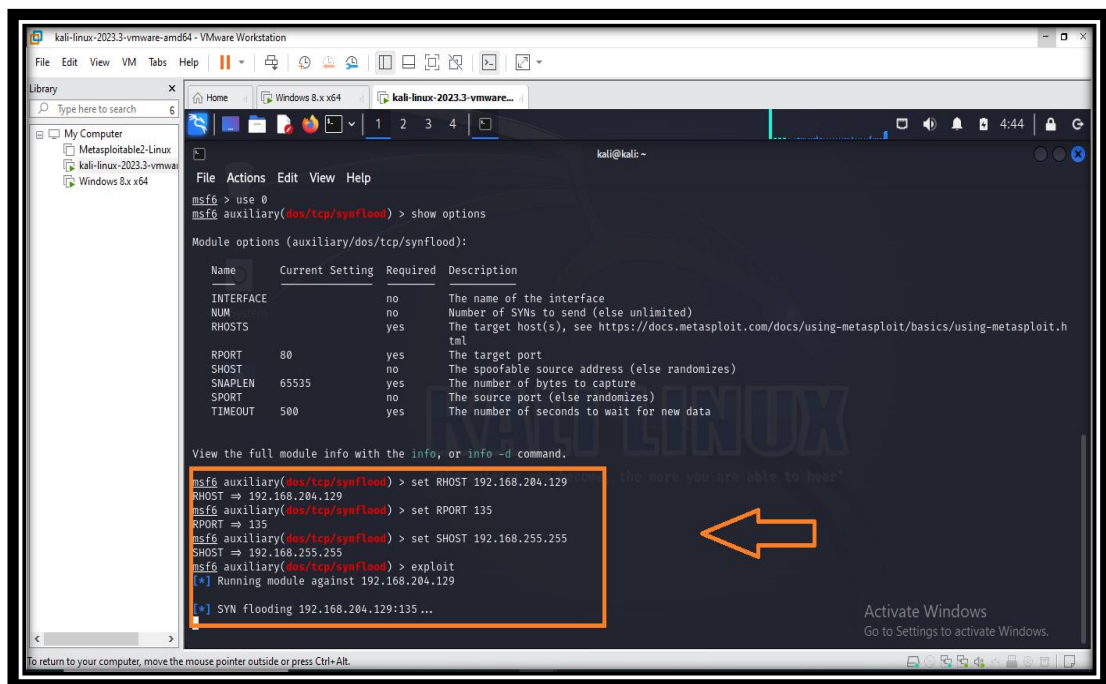


- With port 135 identified as a potential target, I prepared for a Denial of Service (DoS) attack. I opened another terminal in Kali Linux and launched the 'msfconsole' using 'sudo msfconsole' command. Within the Metasploit console, I located and executed the 'synflood' module by selecting option '0.'

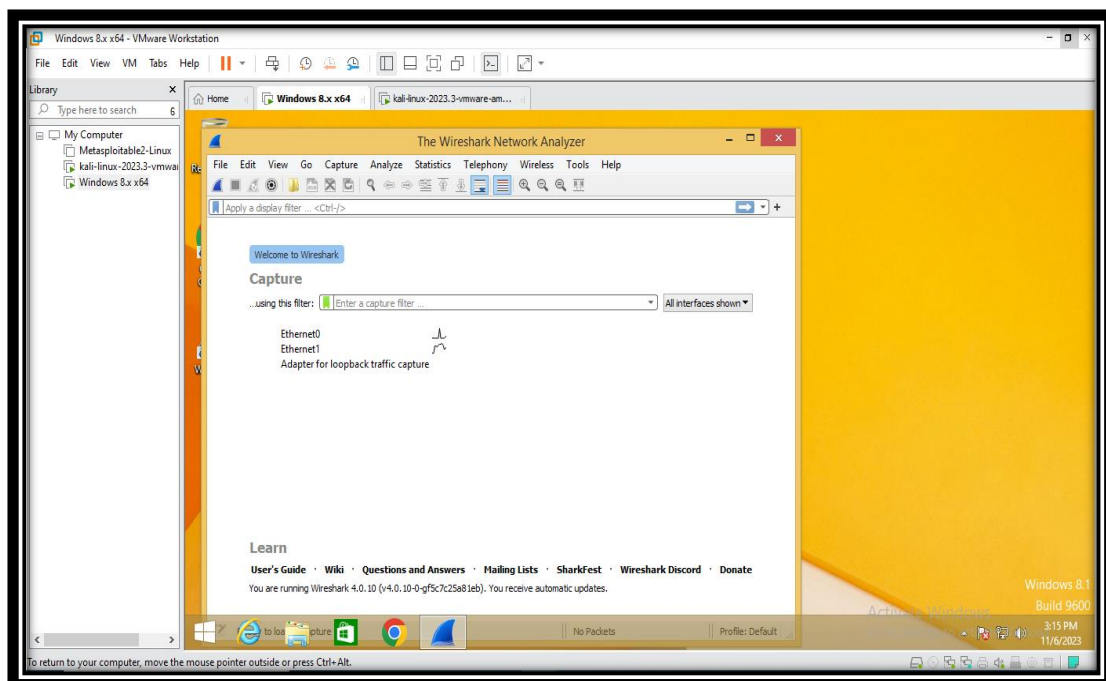


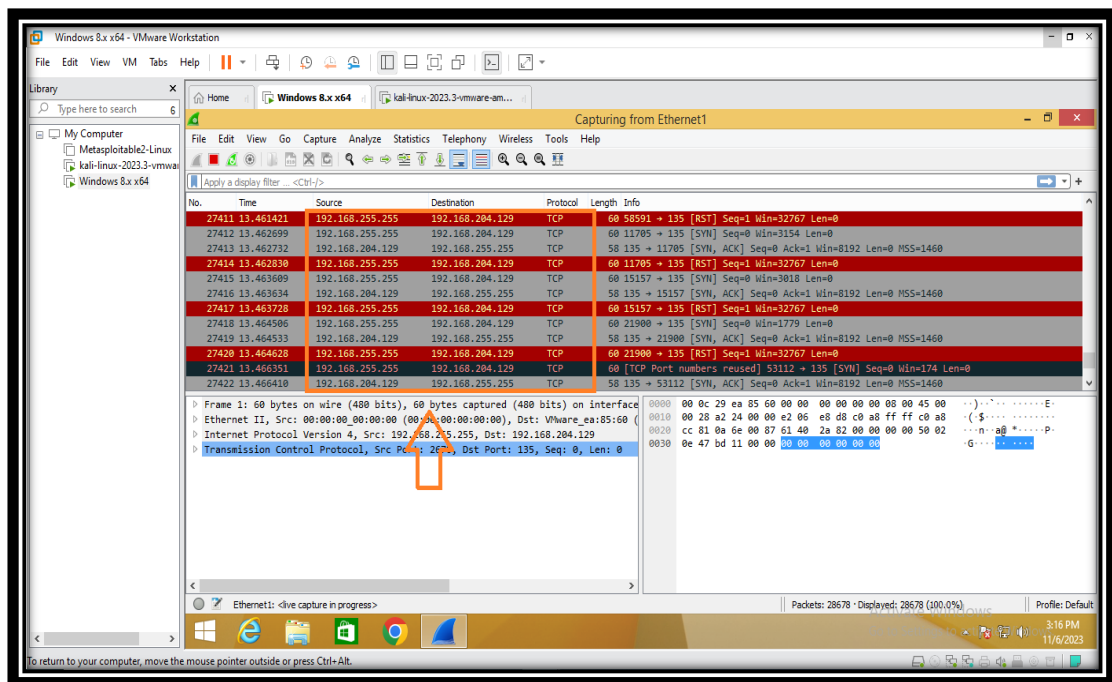
- Before proceeding with the SYN Flood attack, I configured the attack parameters. The 'show options' command provided several options, including 'RHOST,' 'RPORT,' 'SHOST,' and more. I configured 'RHOST' with the victim's IP address (192.168.204.129), 'RPORT' with the target port (135), and 'SHOST' with the spoofed

source IP, set to 192.168.255.255. With the setup complete, I initiated the attack by entering 'exploit'.



- To assess the impact of the SYN Flood DoS attack, I switched back to my Windows 8 VM, where I had previously installed Wireshark to capture network packets. Upon opening Wireshark, I observed a significant in flux of SYN TCP packets.



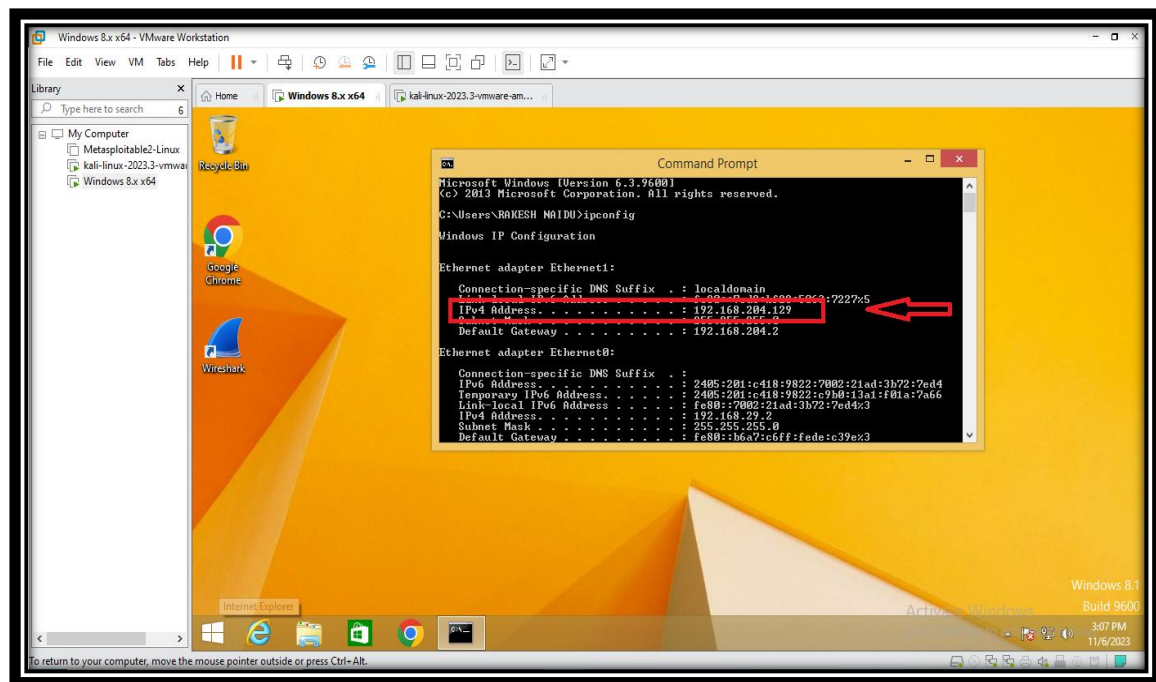


- This assignment provided valuable practical insights into the execution and consequences of a SYN Flood DoS attack, emphasizing the importance of understanding network security threats and the need for robust security measures.

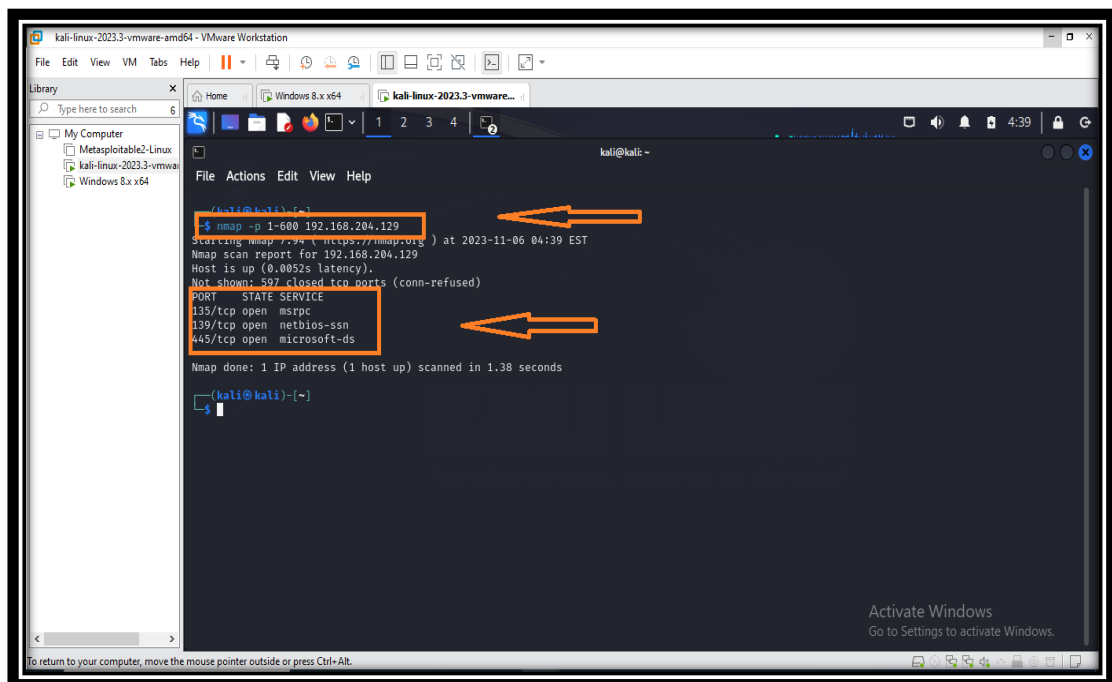
## Objective: 02

### Perform a DoS attack on a target host using hping3

- Denial of Service (DoS) attacks is one such technique, which involves flooding a target system with an overwhelming amount of traffic to disrupt its services and render them unavailable. While the objective of DoS attacks can be malicious, understanding their mechanics is crucial for building robust defence mechanisms.
- Hping3 is a versatile and powerful command-line tool that allows security professionals to test and assess the resilience of network systems, but it can also be misused by malicious actors.
- To initiate the assignment, I launched VMware and started both a Kali Linux VM and a Windows VM. In preparation for the task, I first accessed the Windows VM's command prompt to identify its IP address, which was confirmed as 192.168.204.129.

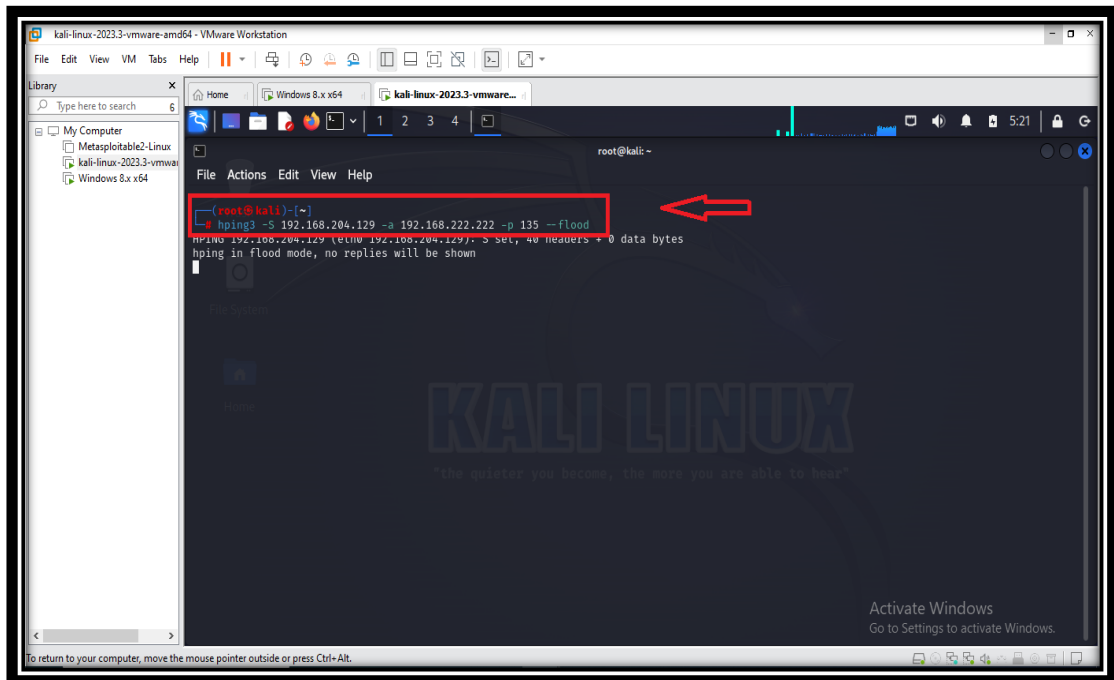


- Subsequently, I shifted to the Kali Linux VM and utilized its terminal to execute a port scanning operation aimed at identifying any open ports on my Windows VM. Employing the 'nmap' command, I specified the range of ports to be scanned as 1 to 600 to ensure efficient use of time and resources. The scan revealed the presence of three open ports. Among the open ports, I selected port 135 as the target for my DoS attack using hping3.

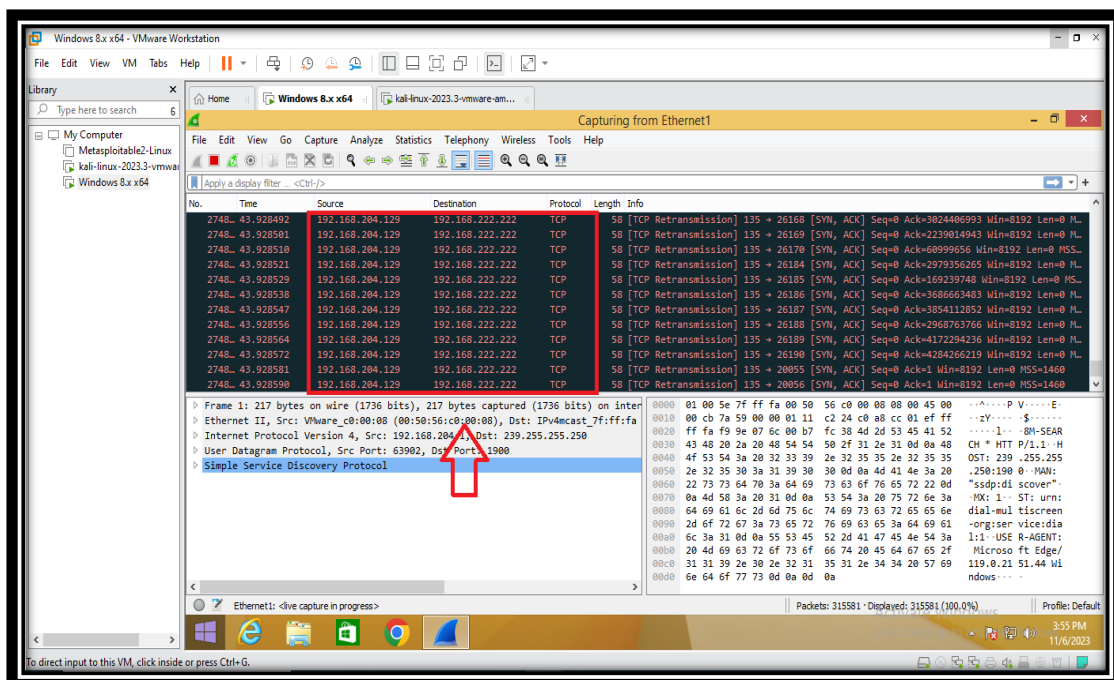




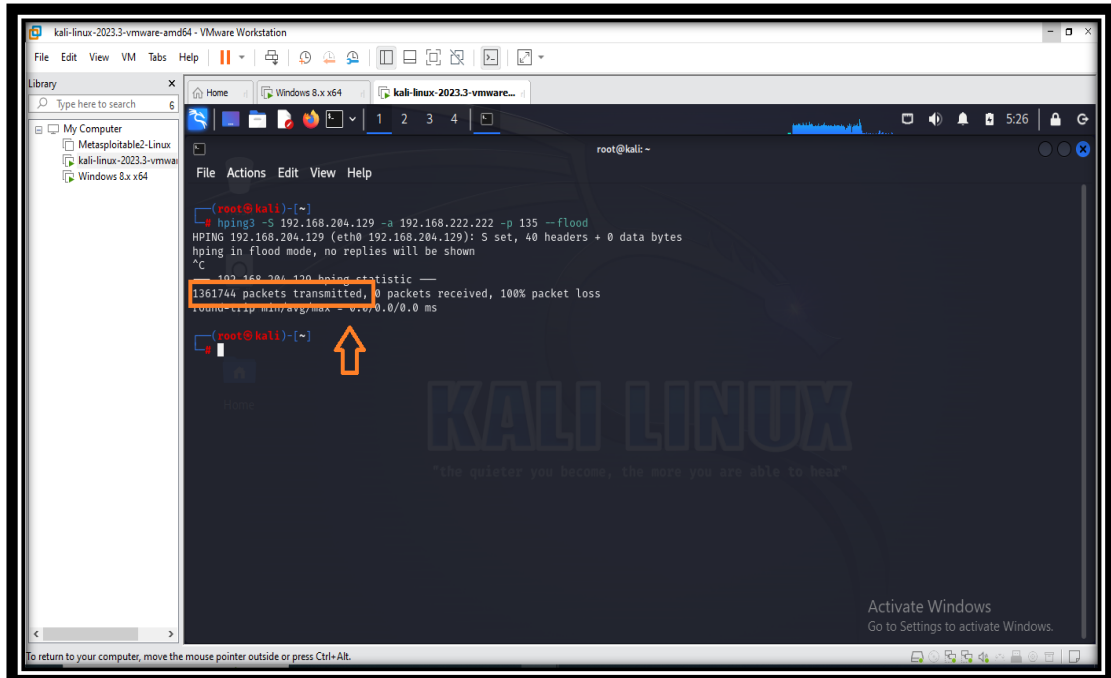
- With the target port determined, I proceeded to execute the DoS attack using hping3. In another terminal on Kali Linux, I issued the command 'hping3 -s 192.168.204.129 -a 192.168.222.222 -p 135 --flood.' This command configuration specified the following: '-s' for sending SYN packets, '-a' for spoofed IP, '-p' for the target port (135), and '--flood' to flood the target with packets.



- To gauge the impact of the DoS attack, I switched back to the Windows VM, where I had previously set up Wireshark to capture network traffic. Upon launching Wireshark, I observed a substantial influx of incoming packets from the spoofed IP address.



- Satisfied with the collected data, I returned to Kali Linux and concluded the attack by halting the previous hping3 command using 'ctrl+c.' this action revealed that approximately 1,361,755 packets had been sent to the target during the course of the DoS attack.



The screenshot shows a Kali Linux terminal window within a VMware Workstation. The terminal displays the execution of the hping3 command in flood mode. The command is: `hping3 -S 192.168.204.129 -a 192.168.222.222 -p 135 --flood`. The output shows the command running in flood mode. The statistics displayed are: `1361744 packets transmitted, 0 packets received, 100% packet loss`. An orange arrow points to the statistics line. The terminal also shows the command being interrupted with `^C`.

- This assignment provided a hands-on experience in executing a DoS attack and underscored the importance of comprehending the implications of such attacks within the context of network security.

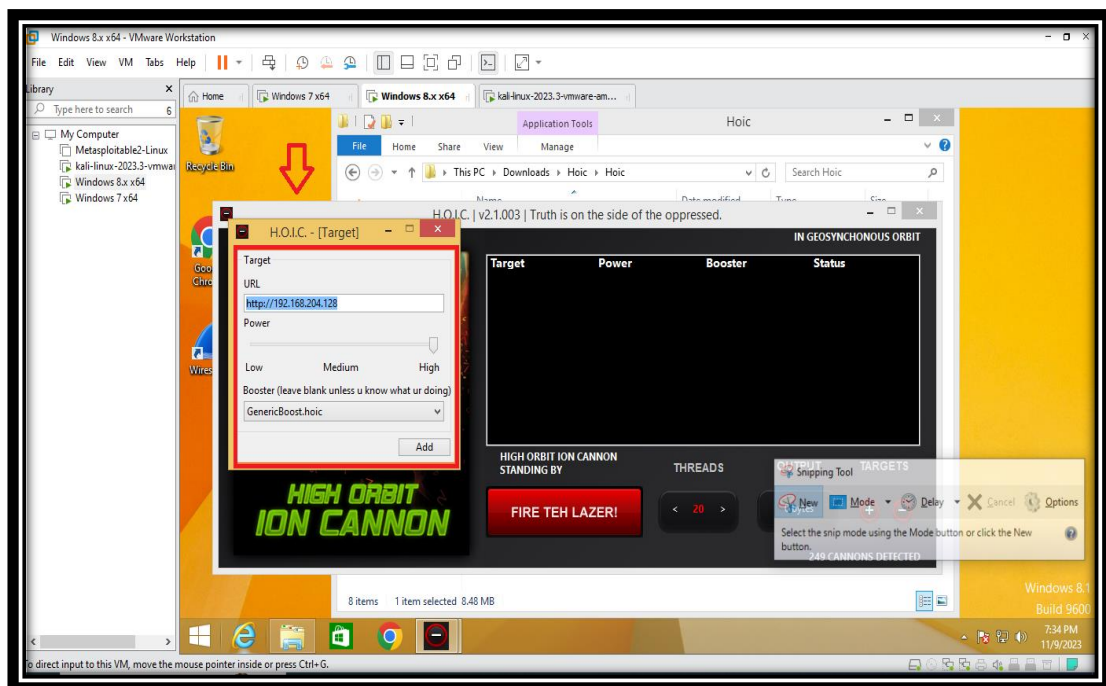
## Objective: 03

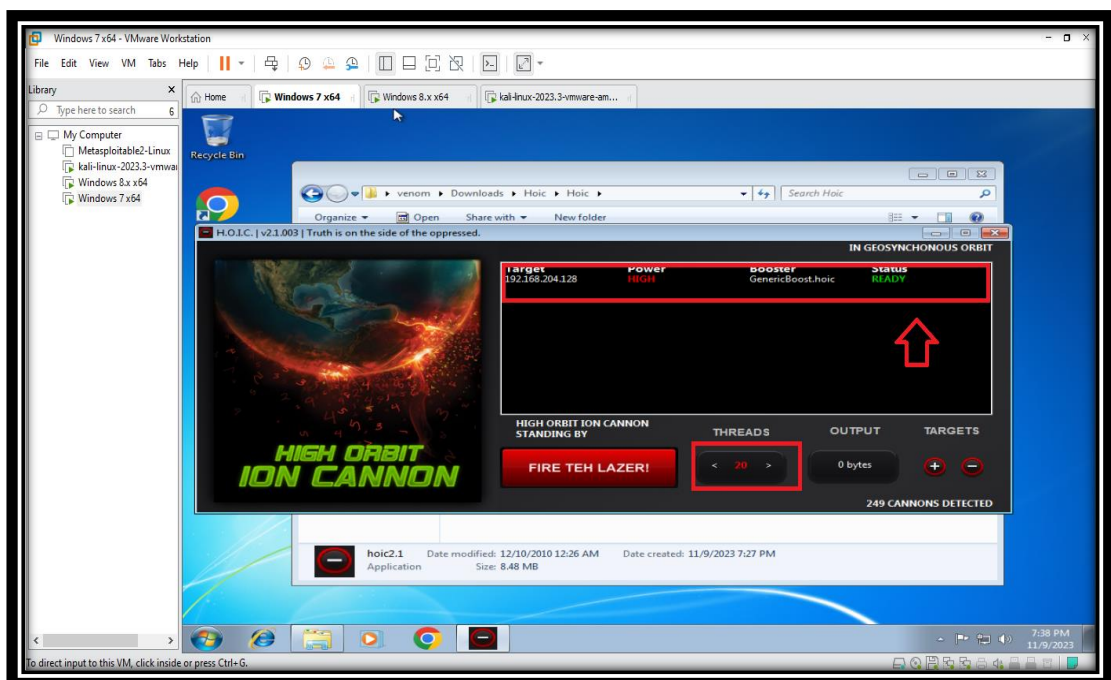
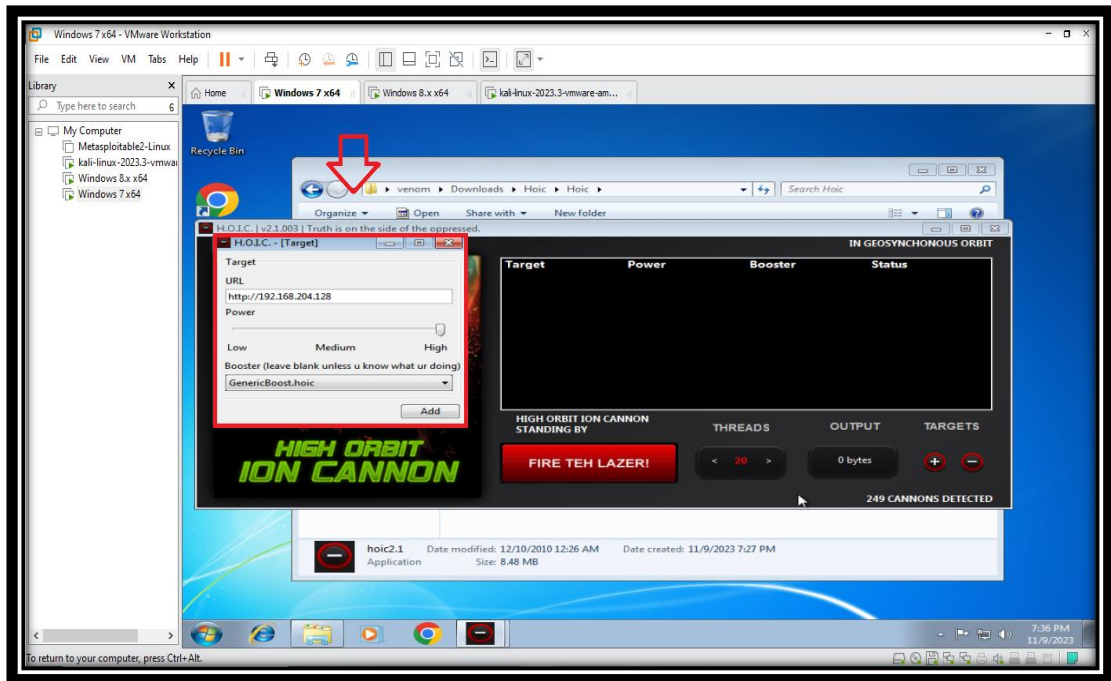
### Perform a DDoS attack using HOIC

- The High Orbit Ion Cannon (HOIC) is a well-known and open-source network stress testing and Denial of Service (DoS) tool. However, HOIC has been abused for malicious purposes, contributing to Distributed Denial of Service (DDoS) attacks on various targets. This tool allows multiple users to join forces in a coordinated effort to flood a target server with a massive volume of traffic, overwhelming its resources and causing service disruptions. It is important to emphasize that HOIC should only be used for ethical and legal purposes, such as testing one's own network security, and not for any malicious activities. Understanding its capabilities can shed light on the importance of safeguarding against DDoS attacks and the need for robust security measures in today's digital landscape.

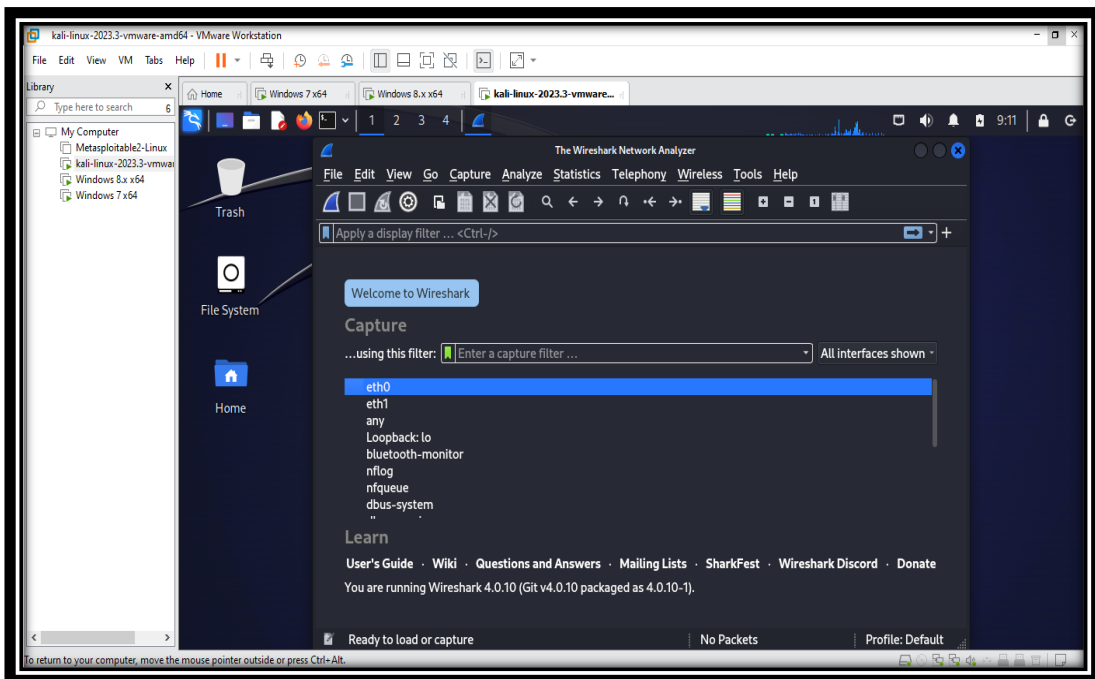
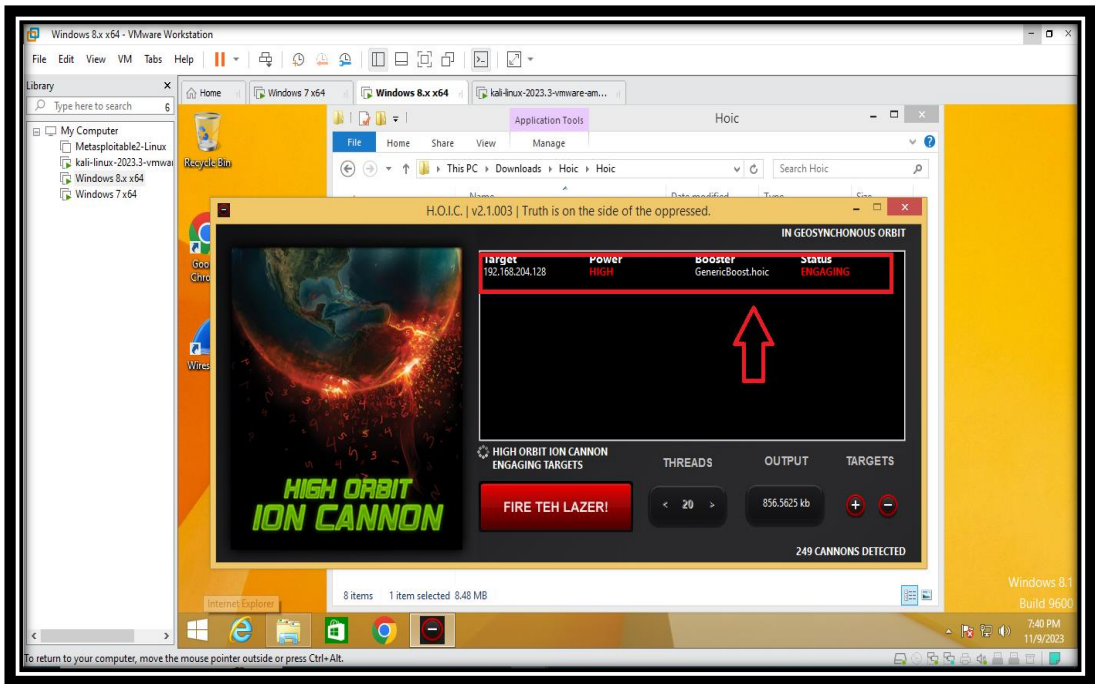


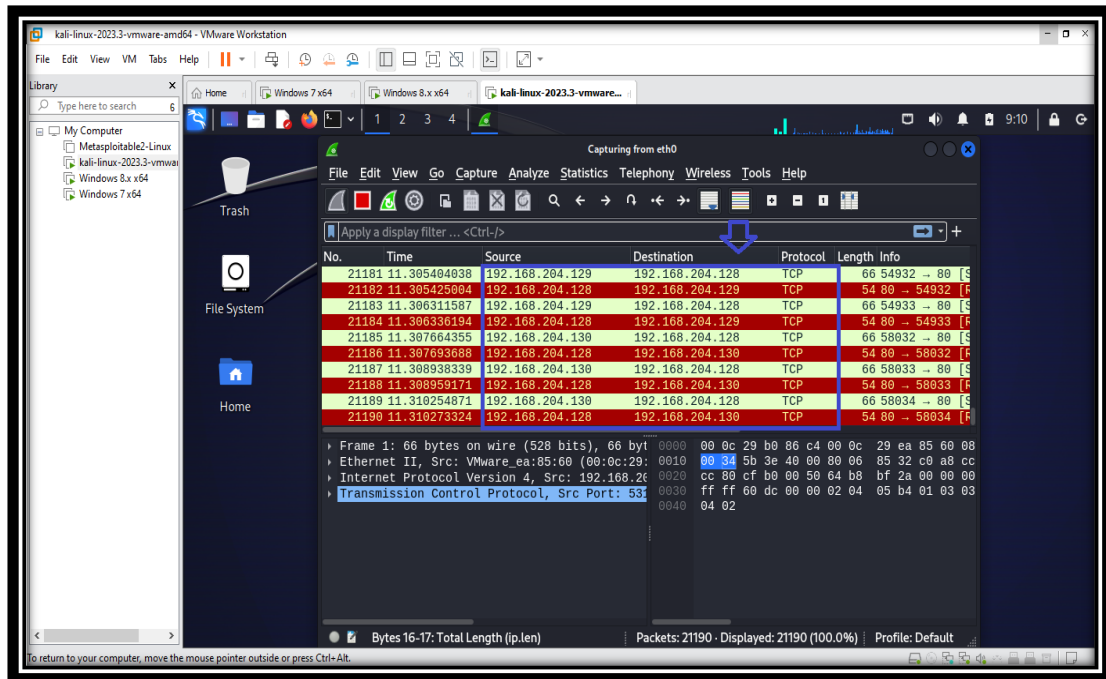
- To commence, I established a virtual environment by deploying both a Windows 7 VM and a Windows 8 VM, alongside a Kali Linux VM. Using the Kali Linux terminal, I identified its IP address, which was confirmed as 192.168.204.128.
- Subsequently, I shifted my focus to the Windows VMs. On the Windows 7 VM, I initiated the process by downloading, installing, and launching the HOIC tool. Simultaneously, I repeated the installation and activation process on the Windows 8 VM, ensuring that HOIC was operational on both Windows VMs.
- With HOIC running on both Windows VMs, I proceeded to configure and execute the DDoS attack. This entailed clicking the '+' symbol within HOIC's interface, leading to a pop-up window where I specified the victim's address, denoted as <http://192.168.204.128>. To escalate the attack's intensity, I adjusted the settings by maximizing the 'bar' and selecting the 'generic boost' mode within HOIC. Following these selections, the tool loaded and displayed 'ready' status on both Windows VMs.





- The DDoS attack was initiated by clicking the 'fire the lazer' button on both Windows VMs, after which the status transitioned from 'ready' to 'engaging.'
- To assess the impact and efficacy of the DDoS attack, I transitioned back to the Kali Linux VM, where I had previously configured Wireshark to capture network traffic. Upon launching Wireshark, I observed a significant surge in network traffic originating from both Windows VMs.





- In conclusion, this assignment offered a practical experience in executing a DDoS attack using the HOIC tool. It's worth noting that in real-world scenarios, attackers frequently deploy multiple systems to magnify the scale and impact of their attacks. In this case, I employed two Windows VMs for the attack, but it's important to recognize that the level of network traffic would considerably increase with a greater number of systems involved. This assignment not only demonstrated the mechanics of a DDoS attack but also emphasized the potential repercussions of such attacks and the importance of robust network security measures.

**Note:** I apologize for conducting this assignment on Windows 7 and 8 servers due to technical issues with my laptop, which struggles with Windows 10 and 11. Your understanding is greatly appreciated.

Submitted By  
Marepalli Rakesh  
([Marepalli.rakesh@gmail.com](mailto:Marepalli.rakesh@gmail.com))