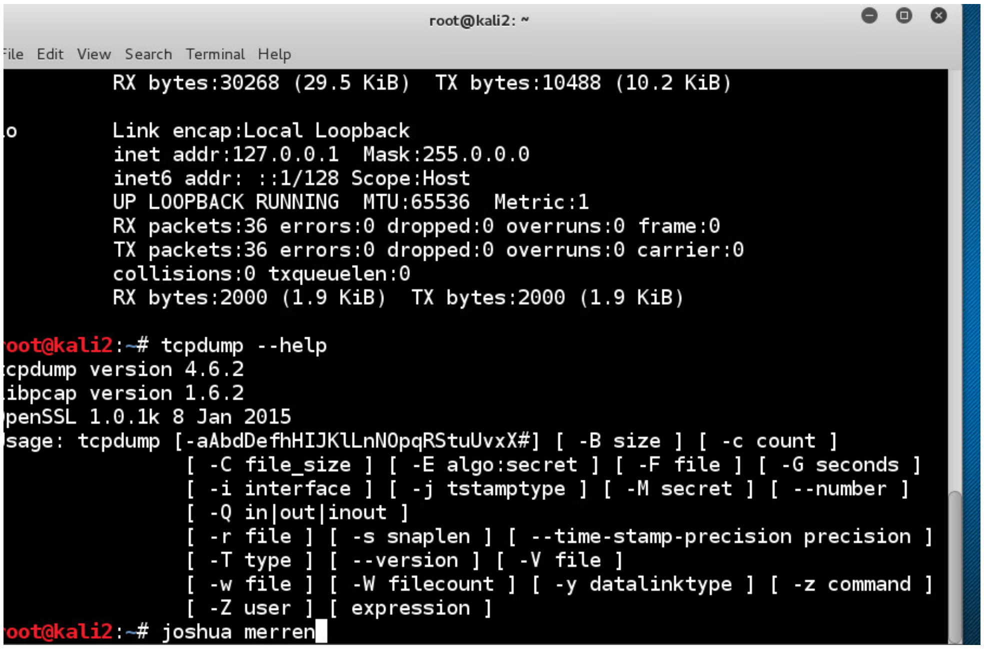
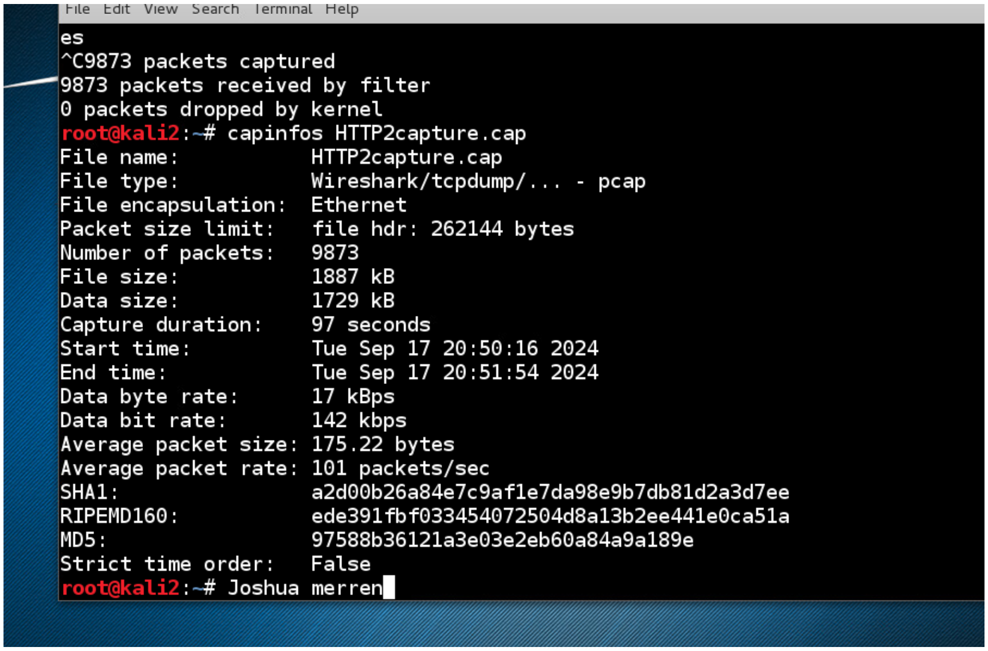
Southern New Hampshire University

CYB 310 Module Three Lab Worksheet

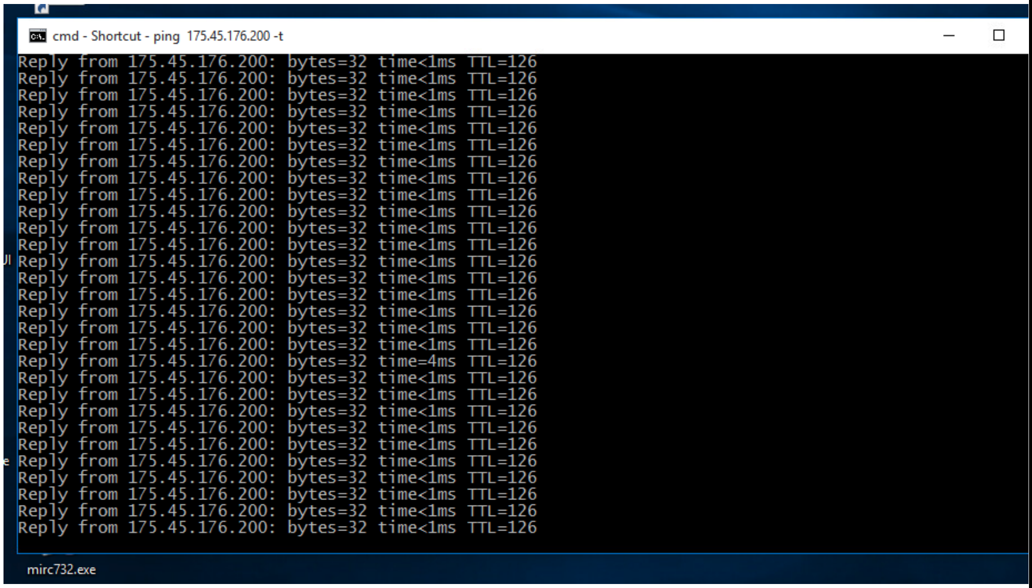
Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information.

Lab: Performing a Denial-of-Service Attack From the WAN

Prompt	Response
In the lab section, “TCP Flood,” **Step 11**, include your name after the command prompt and take a screenshot of your name with the output from running the *tcpdump* command.	 RX bytes:30268 (29.5 KiB) TX bytes:10488 (10.2 KiB) o Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:36 errors:0 dropped:0 overruns:0 frame:0 TX packets:36 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:2000 (1.9 KiB) TX bytes:2000 (1.9 KiB) oot@kali2:~# tcpdump --help cpdump version 4.6.2 ibpcap version 1.6.2 penSSL 1.0.1k 8 Jan 2015 sage: tcpdump [-aAbdDefhHIJKlLnNOpqRStuUvxX#] [-B size] [-c count] [-C file_size] [-E algo:secret] [-F file] [-G seconds] [-i interface] [-j tstamptype] [-M secret] [--number] [-Q in|out|inout] [-r file] [-s snaplen] [--time-stamp-precision precision] [-T type] [--version] [-V file] [-w file] [-W filecount] [-y datalinktype] [-z command] [-Z user] [expression] oot@kali2:~# joshua merren
In the lab section, “HTTP2 Flood,” **Step 16,** add your name at the command prompt after you run the *capinfos HTTP2capture.cap* command. Take a screenshot of your name and the output for the total number of packets captured in the number of packets data.	 es ^C9873 packets captured 9873 packets received by filter 0 packets dropped by kernel root@kali2:~# capinfos HTTP2capture.cap File name: HTTP2capture.cap File type: Wireshark/tcpdump/... - pcap File encapsulation: Ethernet Packet size limit: file hdr: 262144 bytes Number of packets: 9873 File size: 1887 kB Data size: 1729 kB Capture duration: 97 seconds Start time: Tue Sep 17 20:50:16 2024 End time: Tue Sep 17 20:51:54 2024 Data byte rate: 17 kBps Data bit rate: 142 kbps Average packet size: 175.22 bytes Average packet rate: 101 packets/sec SHA1: a2d00b26a84e7c9af1e7da98e9b7db81d2a3d7ee RIPEMD160: ede391fbf033454072504d8a13b2ee441e0ca51a MD5: 97588b36121a3e03e2eb60a84a9a189e Strict time order: False root@kali2:~# Joshua merren

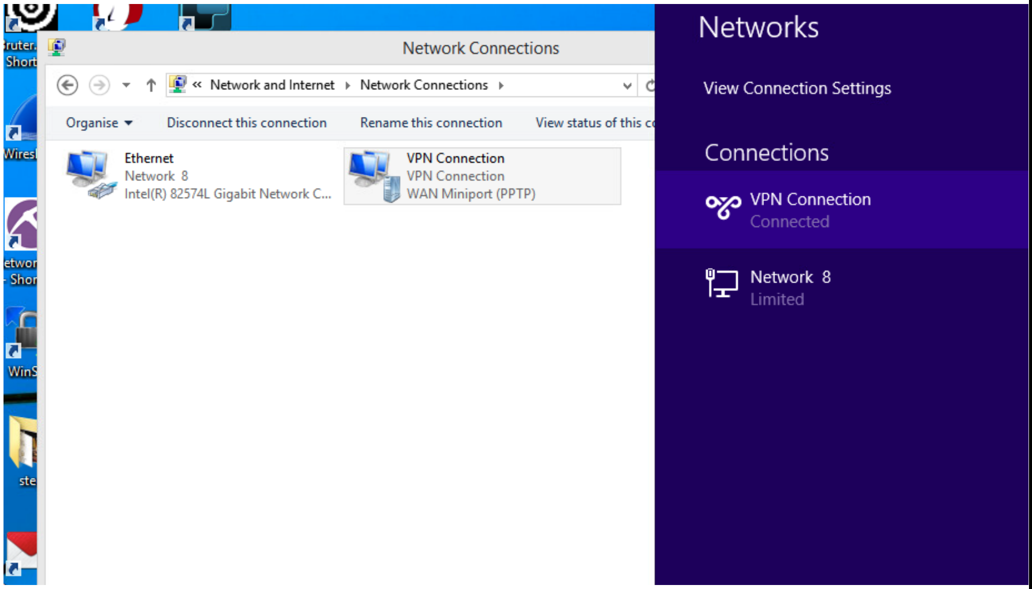
Prompt	Response
How can the Low Orbit Ion Cannon (LOIC) tool be used in the daily work an analyst would do?	The Low Orbit Ion Cannon (LOIC) is typically recognized as a stress-testing tool used to simulate Denial-of-Service (DoS) attacks. For an analyst, while not used for malicious purposes, LOIC can be a valuable tool for testing the resilience and capacity of networks to handle unexpected or high volumes of traffic. It allows analysts to identify vulnerabilities in network infrastructure before actual attacks can exploit them. By simulating controlled DoS attacks, analysts can monitor how well the network responds and implement improvements to enhance security measures and network performance.
What are two examples of information the LOIC tool could retrieve?	**Network Response:** LOIC can help retrieve data about how a network responds to high traffic loads or simulated attack scenarios, including response times and system behavior under stress. **Vulnerability Assessment:** It can provide insights into the thresholds at which network services become unavailable or degrade significantly, indicating potential vulnerabilities that would need to be looked at to prevent actual DoS attacks.

Lab: Implementing NAT and Allowing Remote Access

<table>
<tr><th>Prompt</th><th>Response</th></tr>
<tr><td>In the lab section, “Understanding NAT,” <b>Step 27,</b> take a screenshot of the display of the output from the ping command executed in Step 8.</td><td>


cmd - Shortcut - ping 175.45.176.200 -t

<pre>
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time=4ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
Reply from 175.45.176.200: bytes=32 time<1ms TTL=126
</pre>

</td></tr>
<tr><td>In the lab section, “Secure Remote Login,” <b>Step 34,</b> take a screenshot of the VPN window after logging in to the network.</td><td>


Ethernet
Network 8
Intel(R) 82574L Gigabit Network C...

VPN Connection
VPN Connection
WAN Miniport (PPTP)

VPN Connection
Connected

Network 8
Limited
</td></tr>
<tr><td>What useful information can be retrieved using NMAP and Wireshark together?</td><td>Using NMAP and Wireshark in conjunction provides comprehensive network analysis capabilities. NMAP is powerful for network scanning and inventory, helping to identify what devices are on a network, what services are running, and what ports are open. Wireshark complements this by enabling deep packet analysis and capturing and inspecting the content of packets flowing through the network. Together, they can offer detailed information on network structure, traffic flow, security loopholes, and real-time data transmission characteristics, aiding in security assessments and troubleshooting network issues.</td></tr>
</table>

Why would it be important to map the network using tools, such as NMAP and Wireshark, prior to configuring NAT?	Mapping a network with tools like NMAP and Wireshark before configuring Network Address Translation (NAT) is crucial for several reasons: 1. Understanding the network's architecture, including the operating devices and services, ensures that NAT configurations are correctly applied to the correct interfaces and devices, avoiding potential disruptions in network communications. 2. The mapping would help identify any security vulnerabilities or unauthorized services that should be looked at before they are masked behind a NAT, enhancing the network's overall security posture. 3. It assists in optimizing NAT rules and policies to ensure efficient traffic management and prevent potential network performance issues.