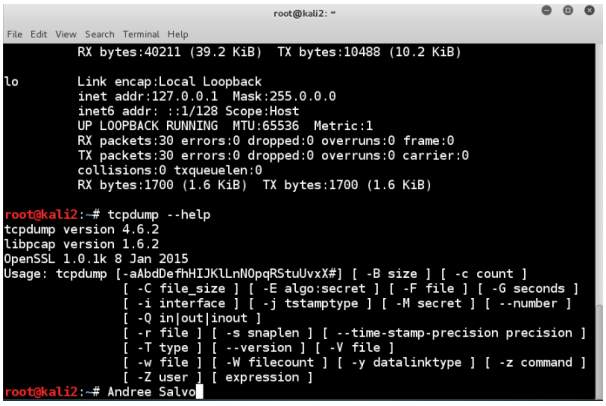
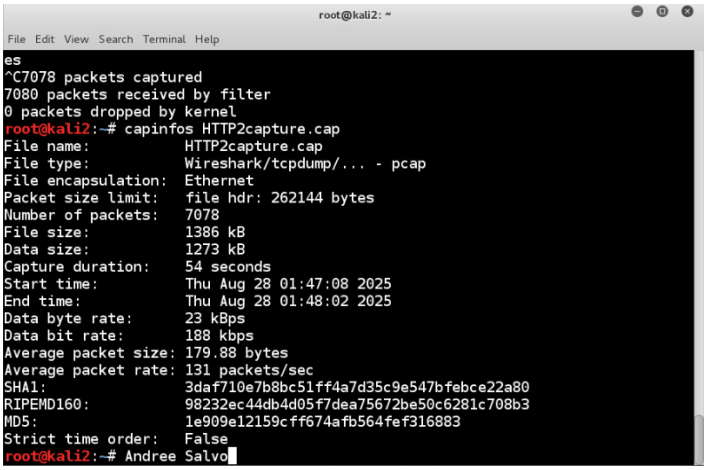
Southern New Hampshire University

CYB 310 Module Three Lab Worksheet

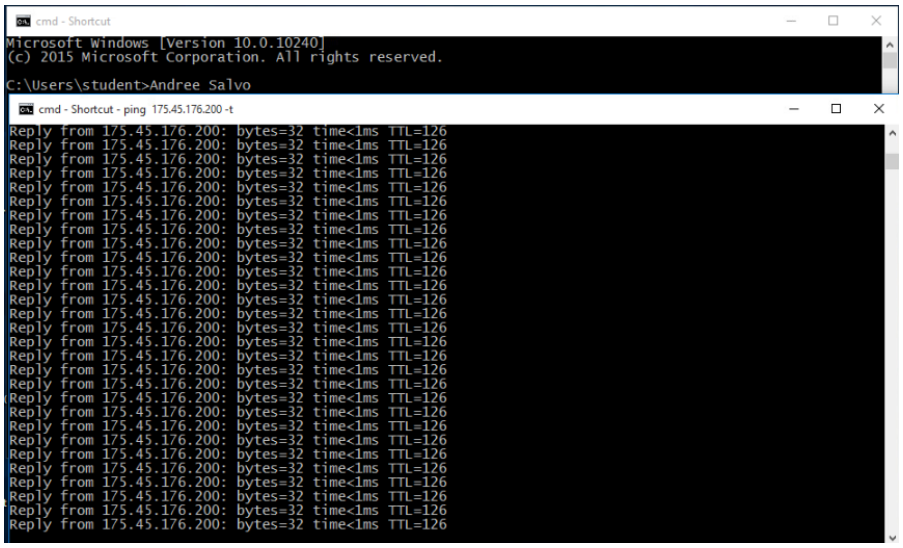
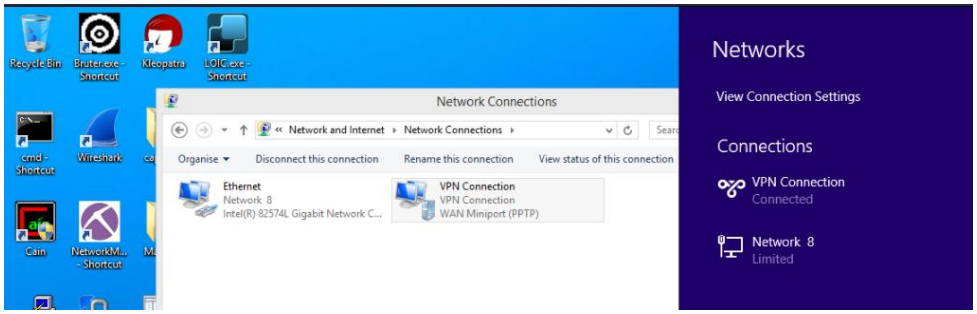
Andree Salvo
Southern New Hampshire University
CYB 310 – 13007
Instructor: Raschid Muller

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.	
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.	
How can the Low Orbit Ion Cannon (LOIC) tool be used in the daily work an analyst would do?	Analysts can perform LOIC legitimately for security testing, intrusion detection, traffic analysis, and incident response training to strengthen defense systems; however, using LOIC for unauthorized DDoS attacks is both illegal and unethical.

Prompt	Response
What are two examples of information the LOIC tool could retrieve?	The Low Orbit Ion Cannon (LOIC) doesn’t retrieve any information; the tool only generates flooded traffic stress. However, an analyst can observe the target server's response and network traffic patterns to see how a system reacts under load.

Lab: Implementing NAT and Allowing Remote Access

Prompt	Response
In the lab section, "Understanding NAT," **Step 27,** take a screenshot of the display of the output from the ping command executed in Step 8.	
In the lab section, "Secure Remote Login," **Step 34,** take a screenshot of the VPN window after logging in to the network.	
What useful information can be retrieved using NMAP and Wireshark together?	By using Nmap and Wireshark together, analysts can identify open ports and services on a target while capturing and analyzing network traffic to validate findings and detect anomalies together.
Why would it be important to map the network using tools, such as NMAP and Wireshark, prior to configuring NAT?	It's essential to map the network using tools like Nmap and Wireshark before configuring NAT, as this allows for understanding the existing devices, services, and traffic flows, ensuring that the translation rules can be applied correctly without disrupting any communication.