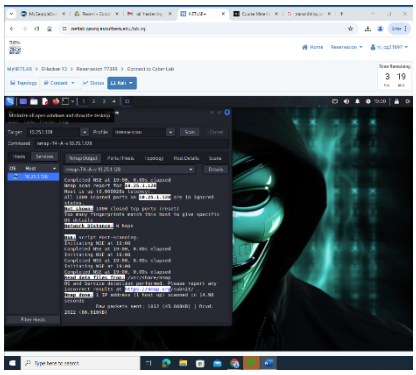
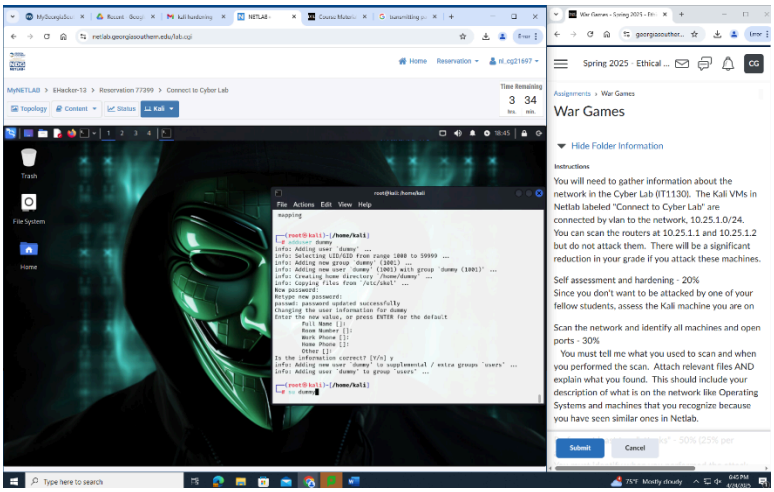
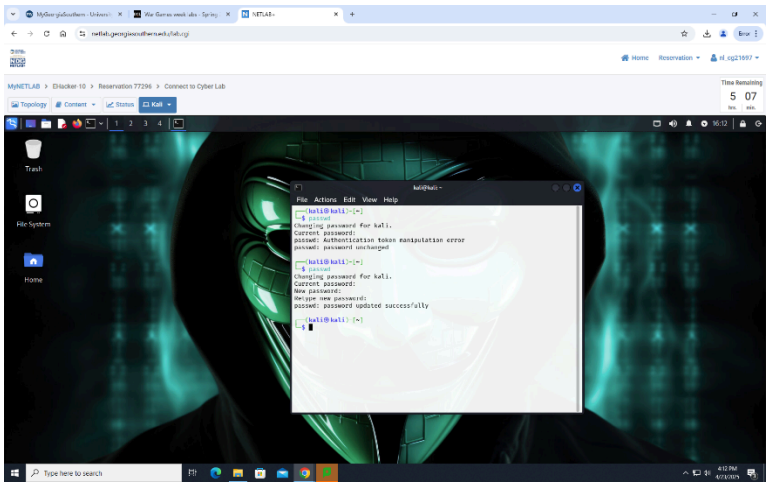
Self-assessed & Hardened My Systems

I performed a host based vulnerability scan using Zenmap to identify open ports and potential weaknesses in the system. The scan result indicated that all ports were in a filtered or ignored state, suggesting existing firewall protections were active.

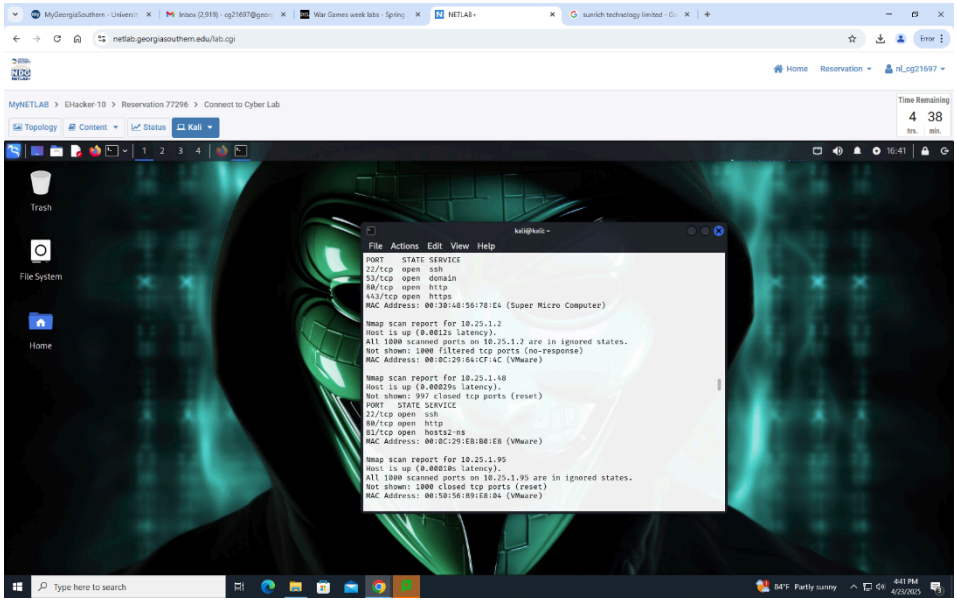


To enhance system security, I implemented basic system hardening measures. This included updating my password to a unique, secure value to prevent credential duplication. Additionally, I created a non privileged user account to reduce the risk of accidental data exposure or administrative misuse, aligning with the principle of least privilege





Scanned the network and identified all machines and open ports using Zenmap & NMAP- I performed a subnet wide scan of the 10.25.1.0/24 network using Nmap. This scan identified all active hosts on the network, their IP addresses, open ports, and corresponding MAC addresses.



The results showed that most MAC addresses were associated with VMware, indicating that these hosts were likely virtual machines used by classmates. Additionally, I identified several other unique MAC address vendors, including:

- Super Micro Computer at 10.25.1.1, which likely represents a physical infrastructure component such as a router or server
- Sunrich Technology Limited, which may correspond to OEM hardware systems
- Proxmox Server Solutions GmbH, which could indicate either a Proxmox Virtual Environment (PVE) host or a bare metal system running Proxmox NIC

Performed Two DoS Attacks- As part of the offensive security component of the lab, I conducted a Denial of service (DoS) attack simulation using hping3 in flood mode. In this simulation I targeted a virtual machine located at IP address 10.25.1.130.

The attack was executed in a controlled environment and ran for approximately 7 minutes, during which hping3 reported transmitting a total of 55,364,431 packets. The goal of the simulation was to overwhelm the target systems network interface and observe its behavior under high traffic load conditions.

I captured screenshots at the start and end of the attack to document the process and packet transmission statistics for reporting purposes.