Performing Reconnaissance from the WAN

ETHICAL HACKING & LAB # 1

Student Info
Name : SRIJA PABBA
Student ID: 00866719
Email:
spabb6@unh.newhaven.edu

Table of Contents

Executive Summary

Highlights

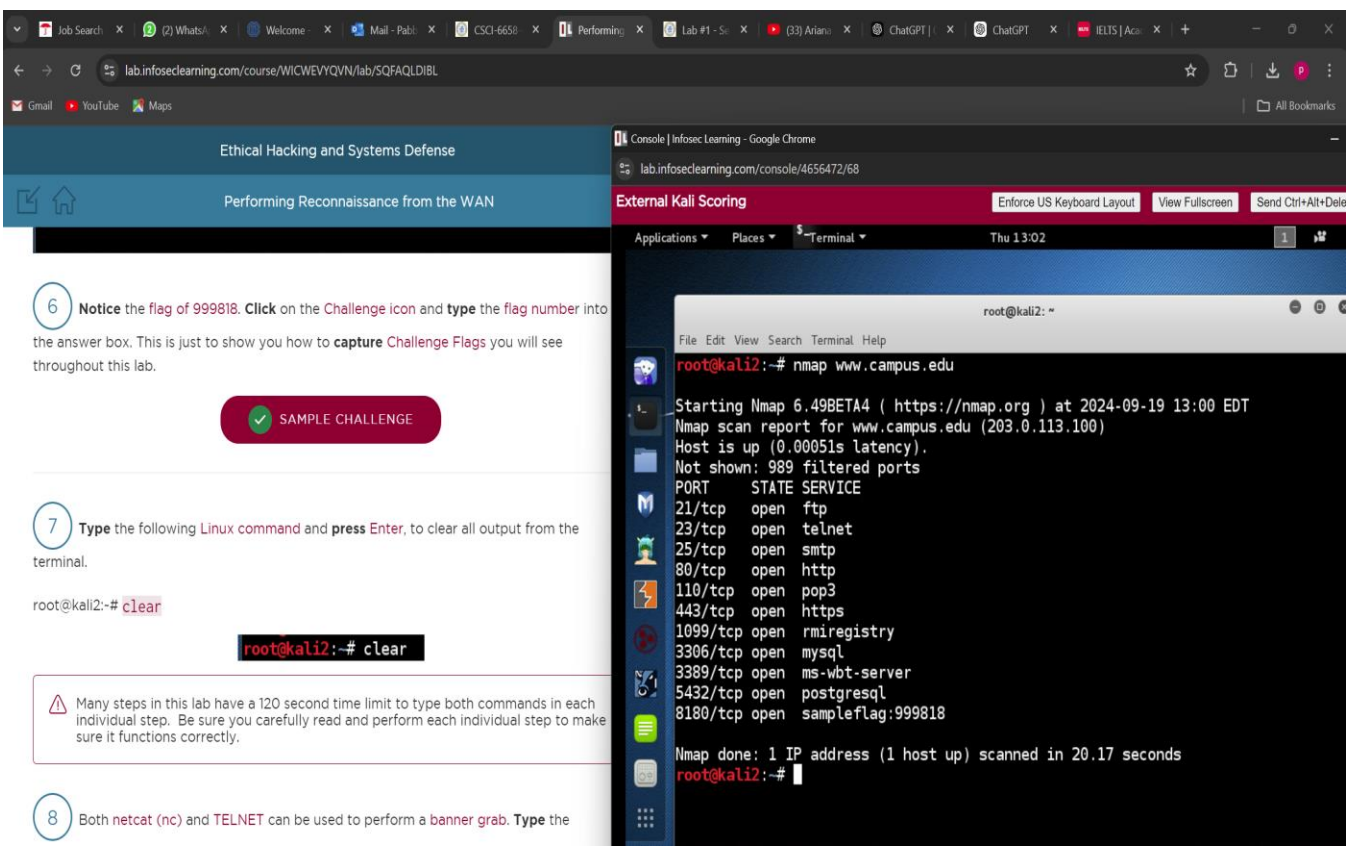
In this lab, I will engage in external reconnaissance by scanning a network protected by a pfSense firewall. Using a Kali 2 Attack Machine, I will conduct port scanning and banner grabbing to identify open ports and discover the operating systems and applications running on machines behind the firewall. The lab will conclude with me obtaining administrator credentials and using Remote Desktop Protocol (RDP) to access a Windows Server.

Objectives

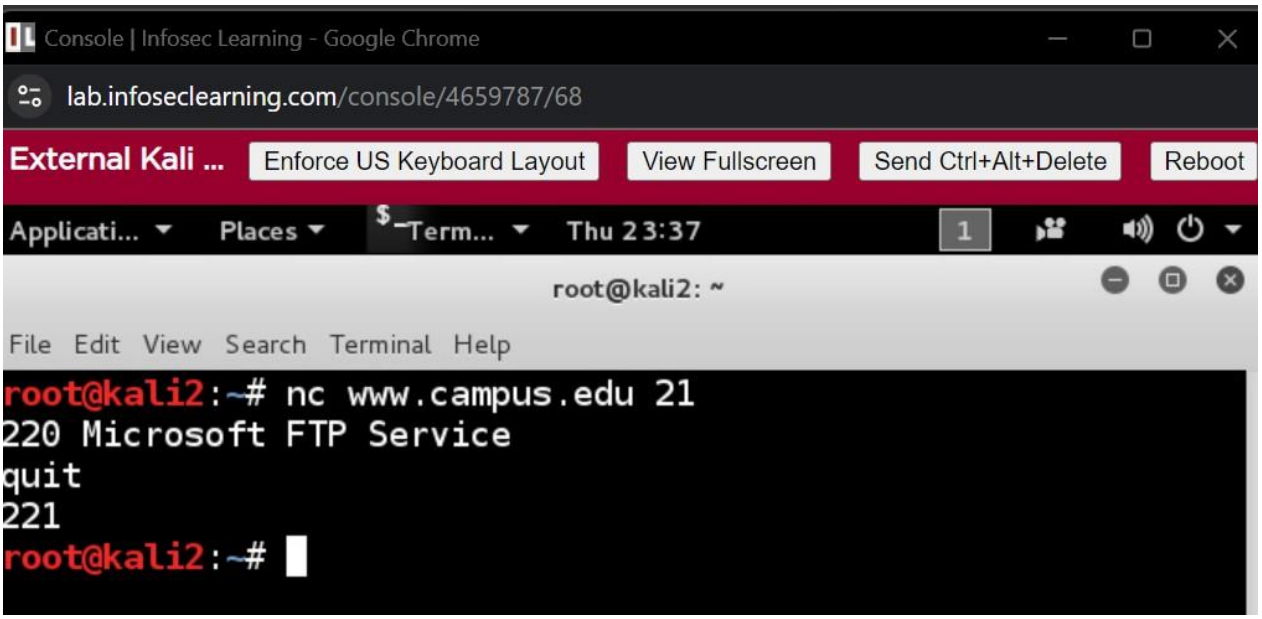
The objective of this lab is for me to practice network reconnaissance techniques by identifying exposed services and vulnerabilities through the pfSense firewall. I will use tools such as nmap to scan ports, perform OS and service identification, retrieve hashed passwords from the `/etc/shadow` file, and ultimately gain access to a Windows Server using the discovered credentials.

Lab Description Details

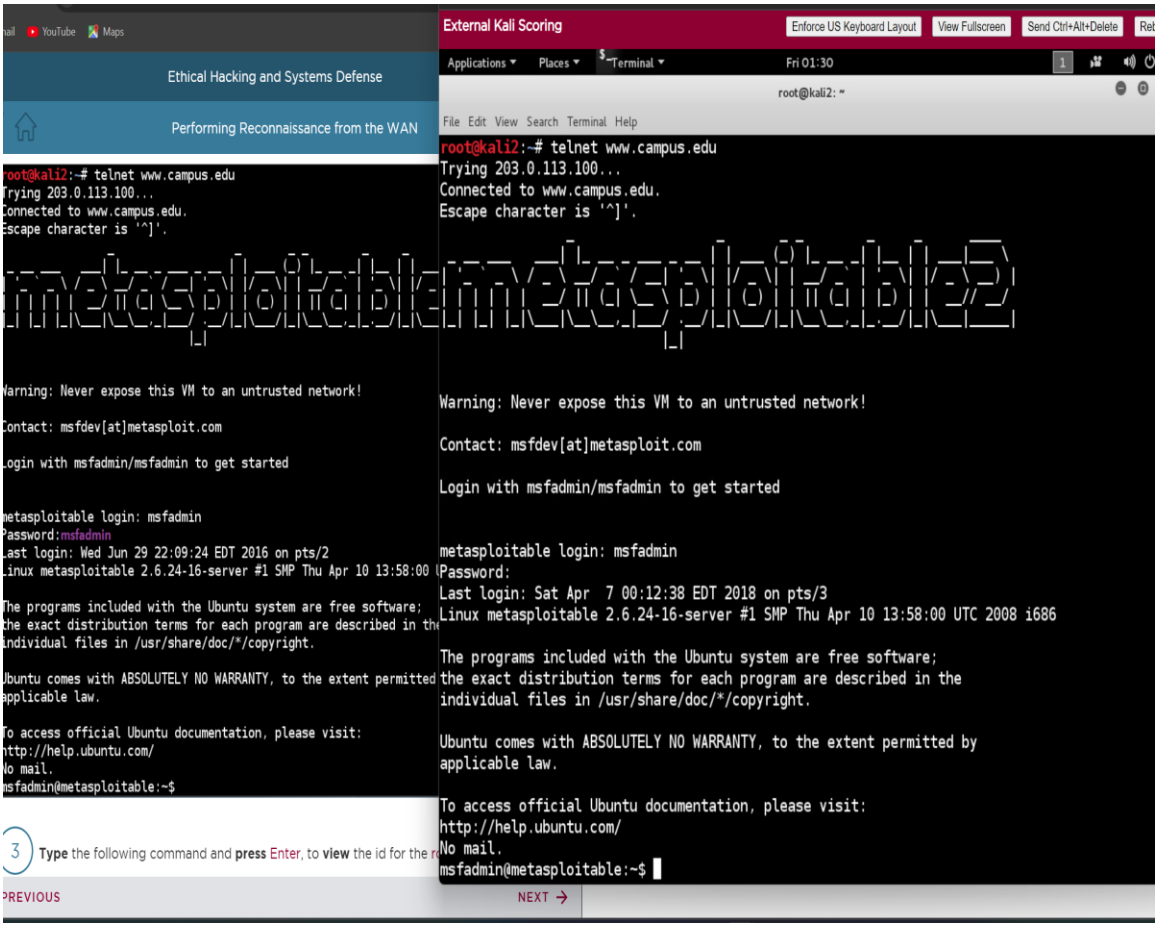
Nmap scan on www.campus.edu



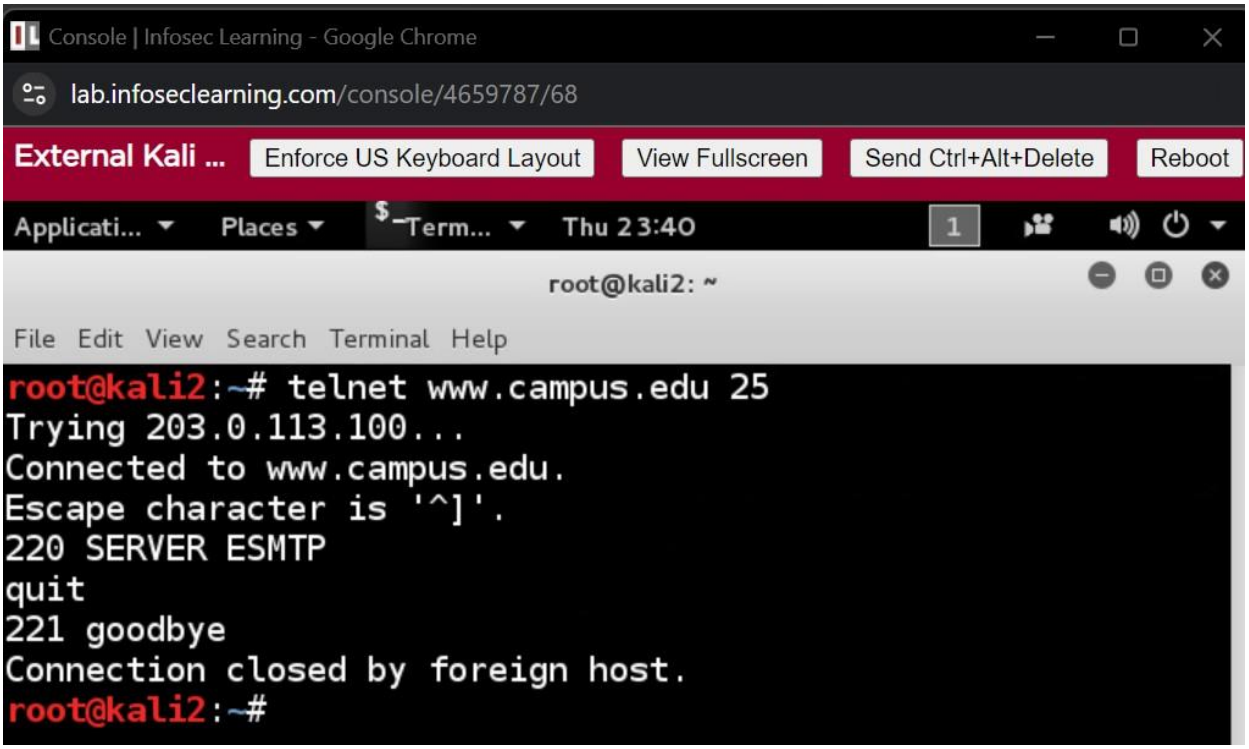
NC www.campus..edu on port 21



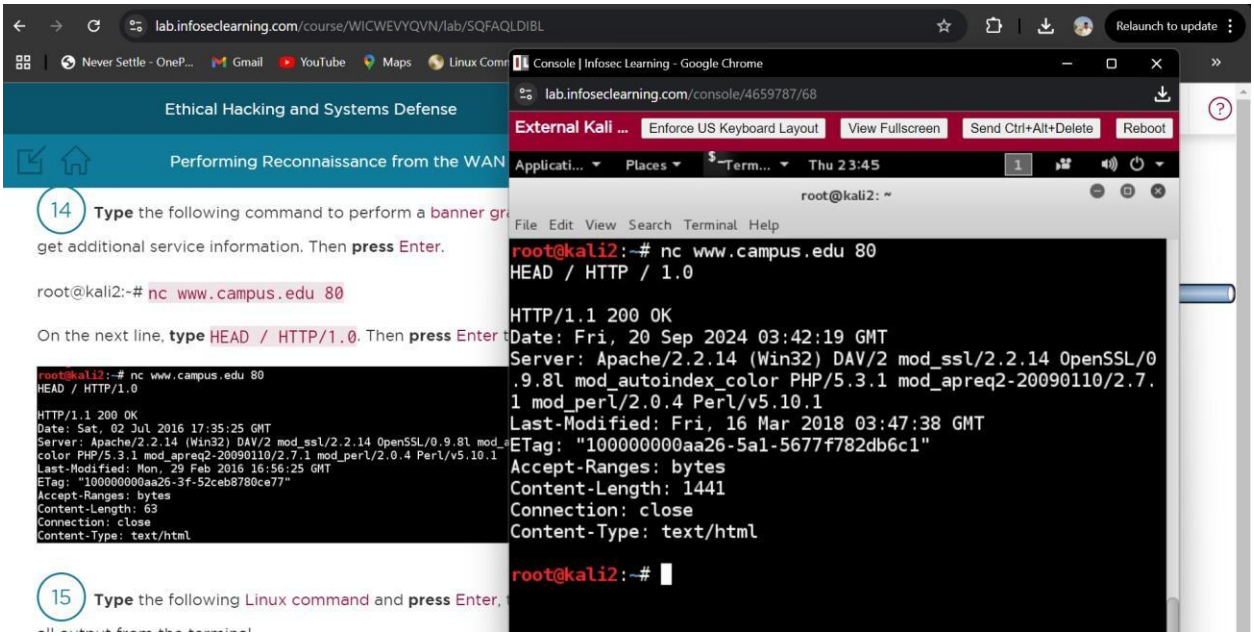
Teleport on port 23



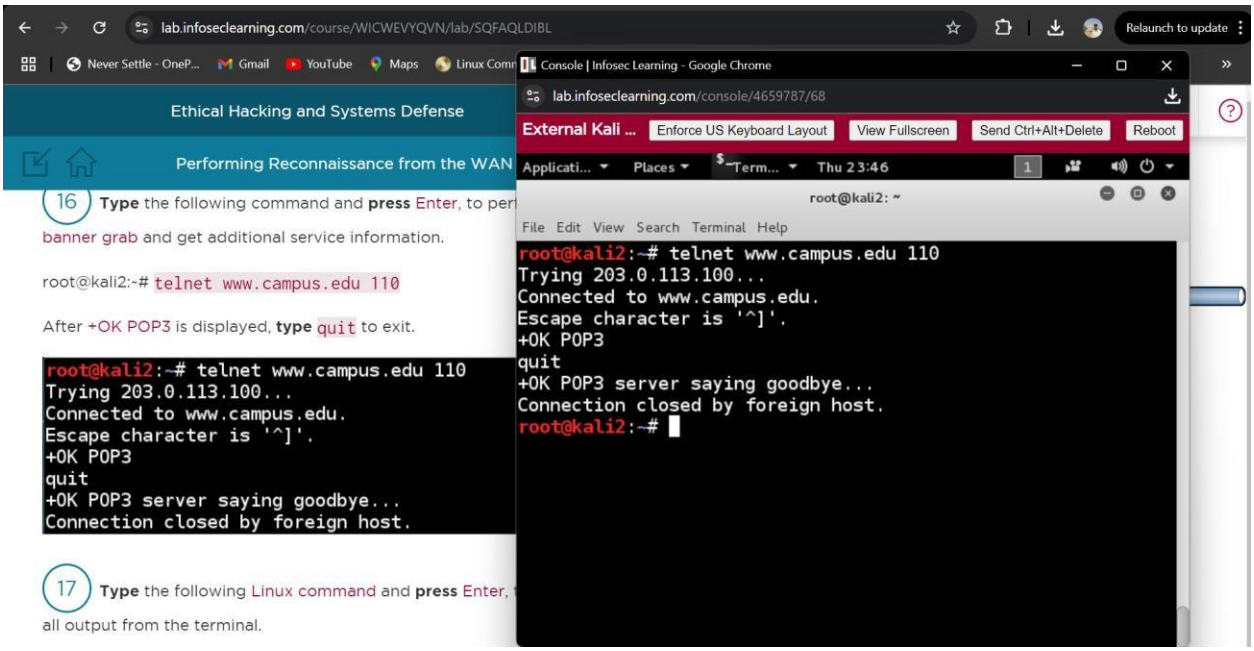
telnet scan on www.campus.edu 25



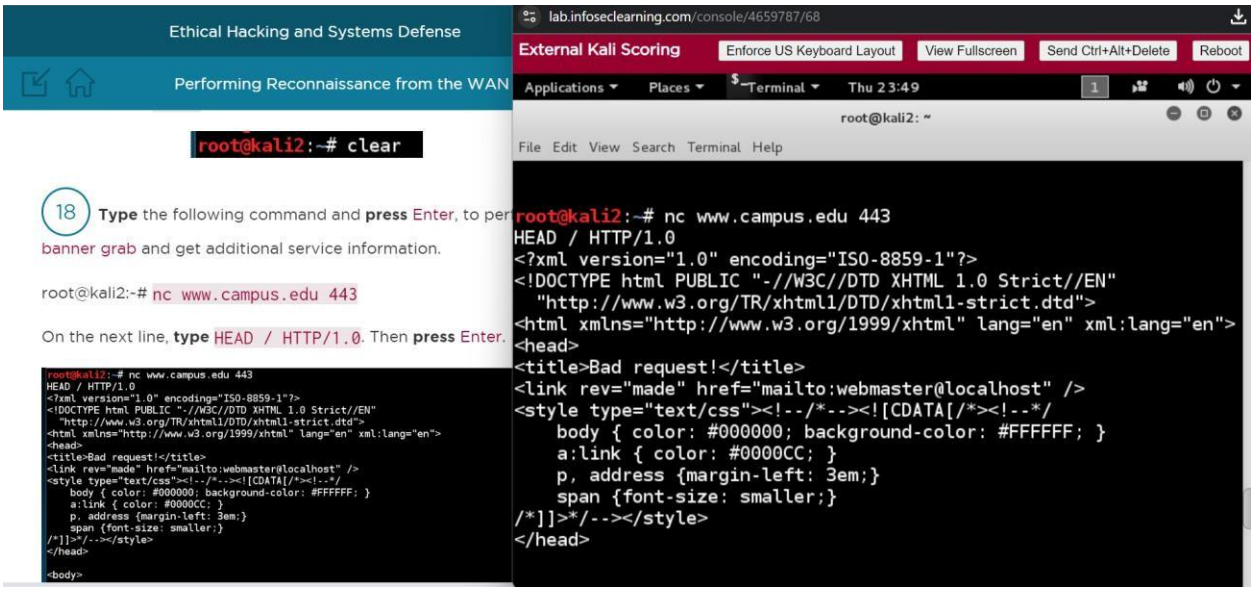
NC on www.campus.edu over port 80



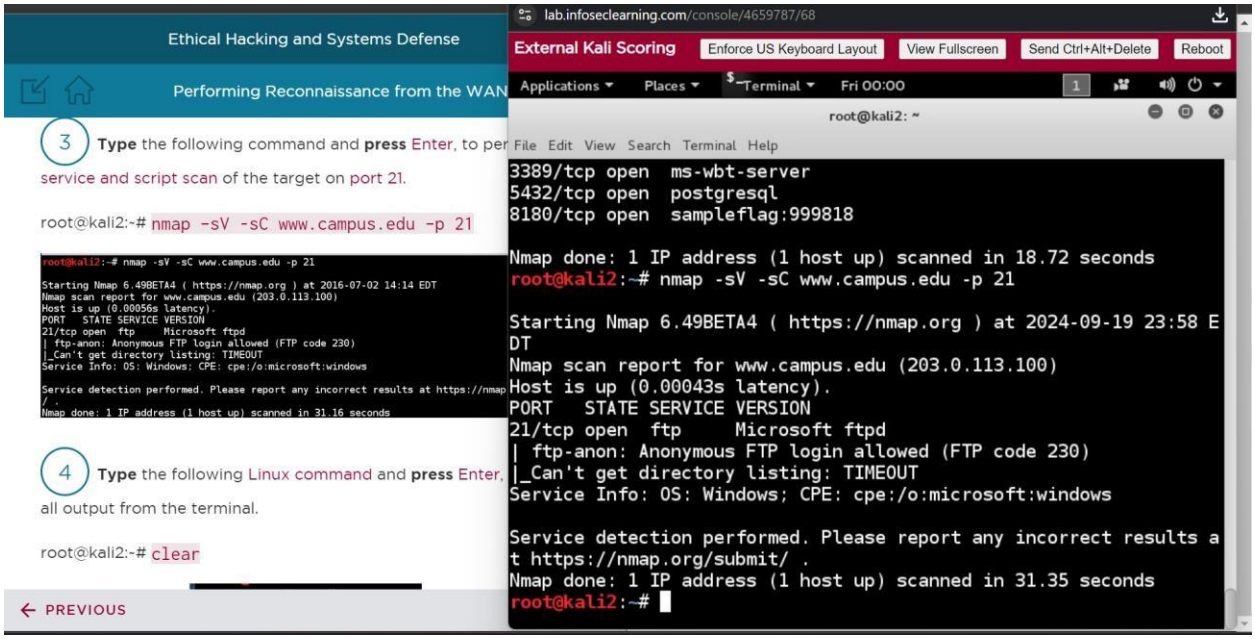
telnet on www.campus.edu on port 110



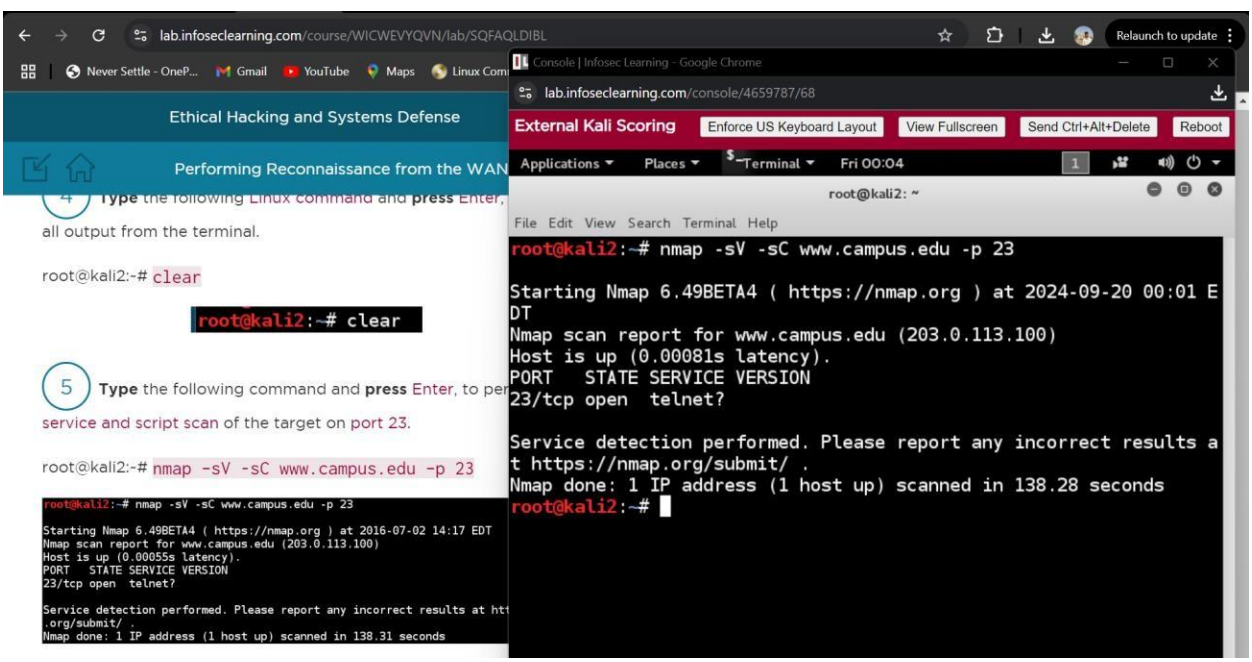
Nc on www.campus.edu over 443



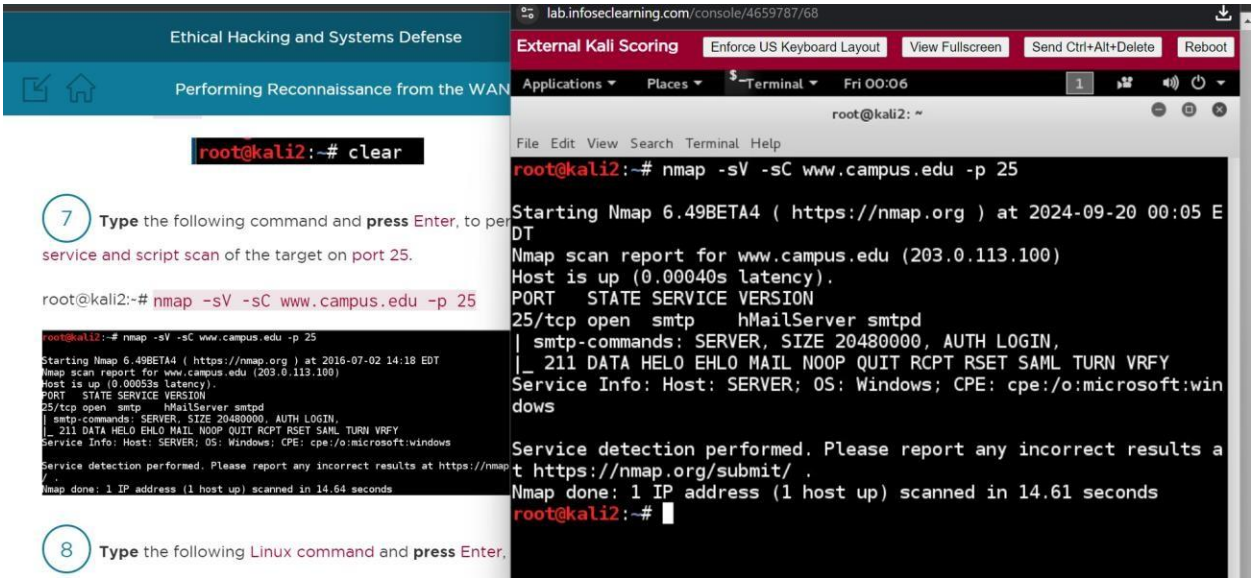
Nmap scan on www.campus.edu over port 21



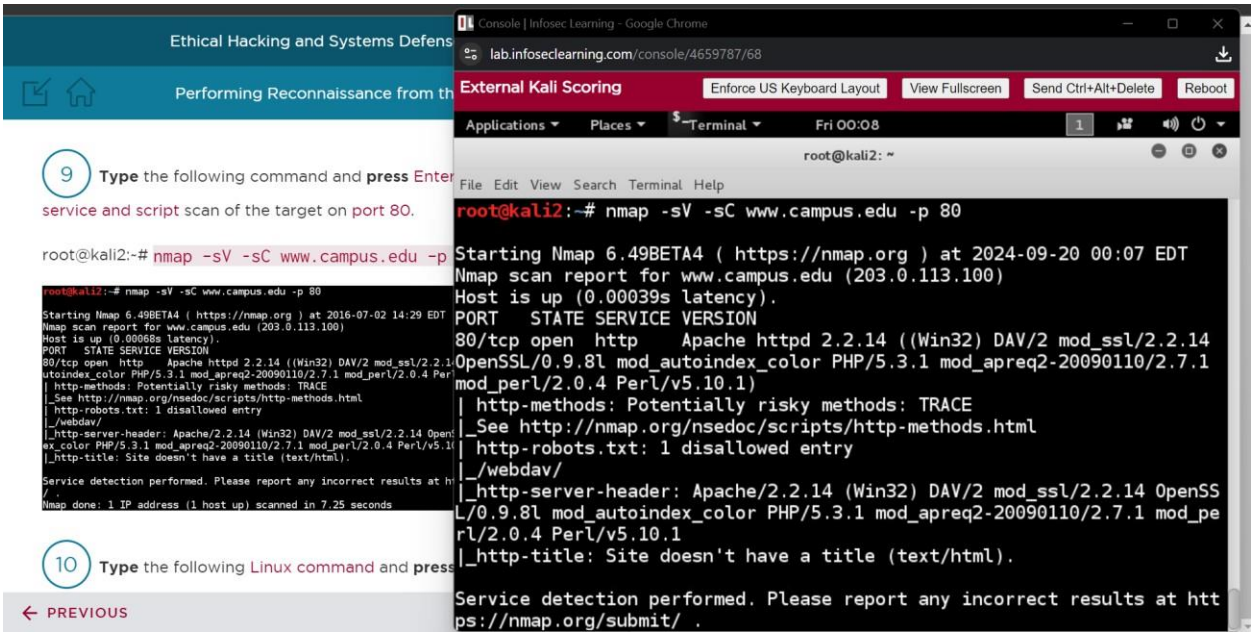
Nmap scan on www.campus.edu over port 23



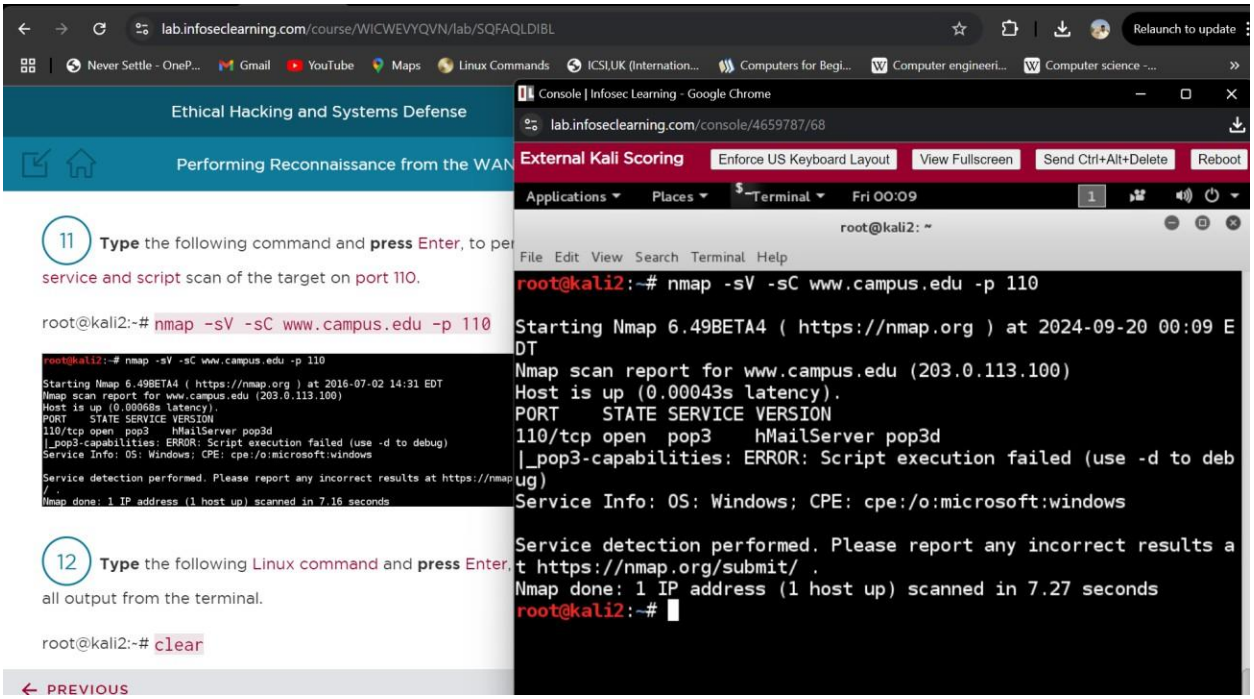
Nmap scan on www.campus.edu over port 25



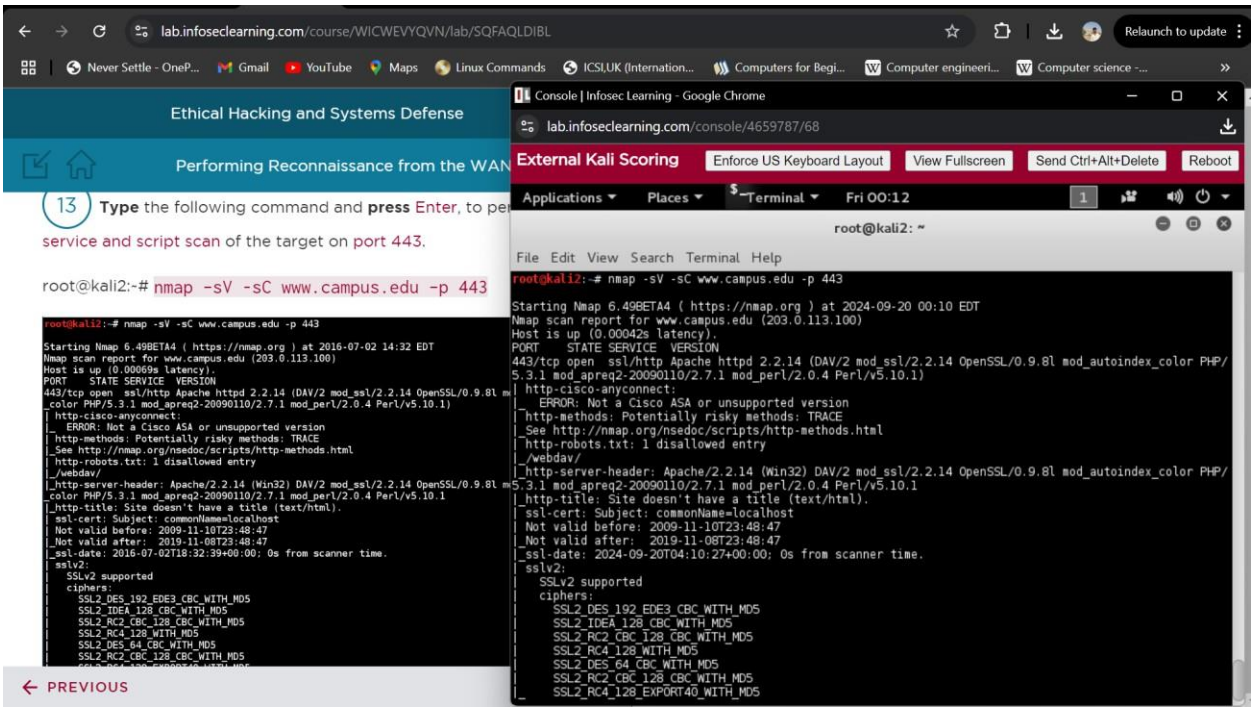
Nmap scan on www.campus.edu over port 80



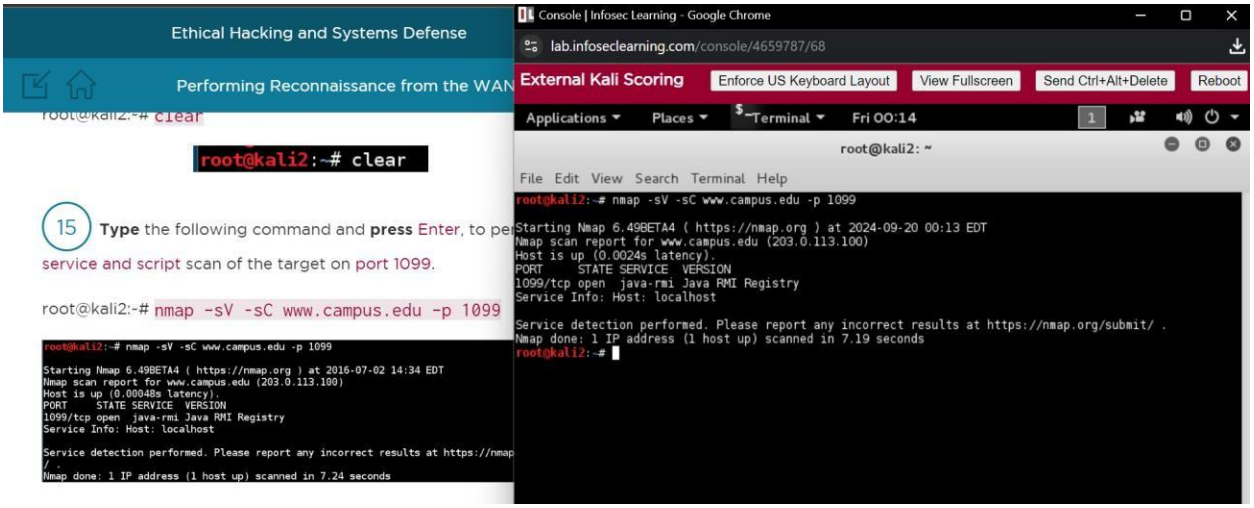
Nmap scan on www.campus.edu over port 110



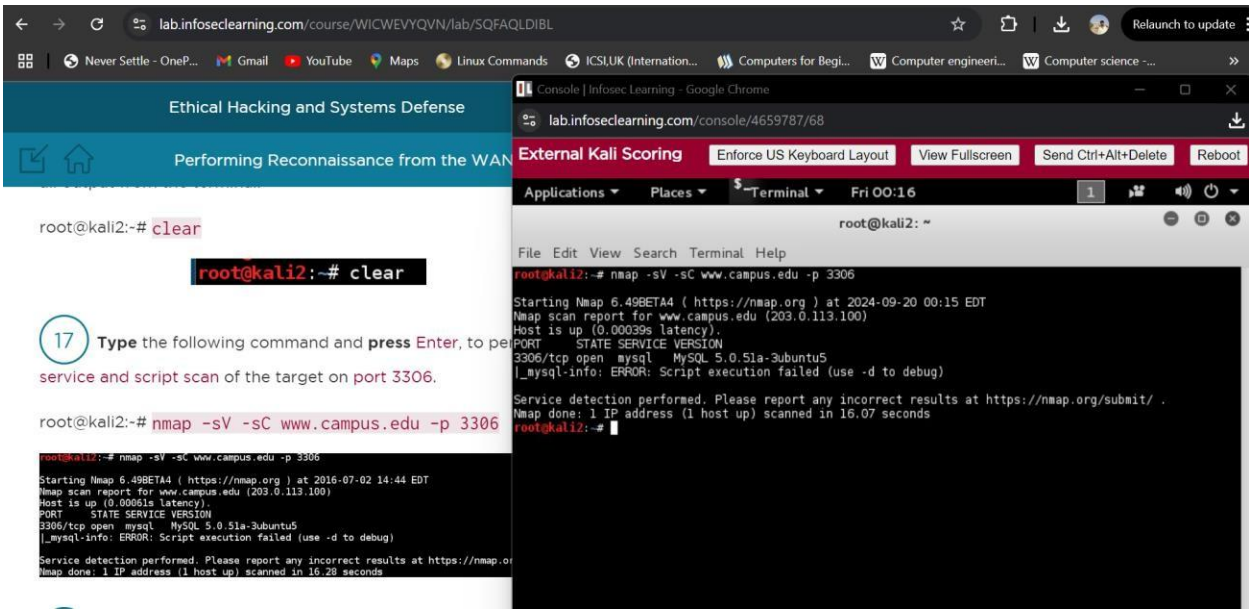
Nmap scan on www.campus.edu over port 443



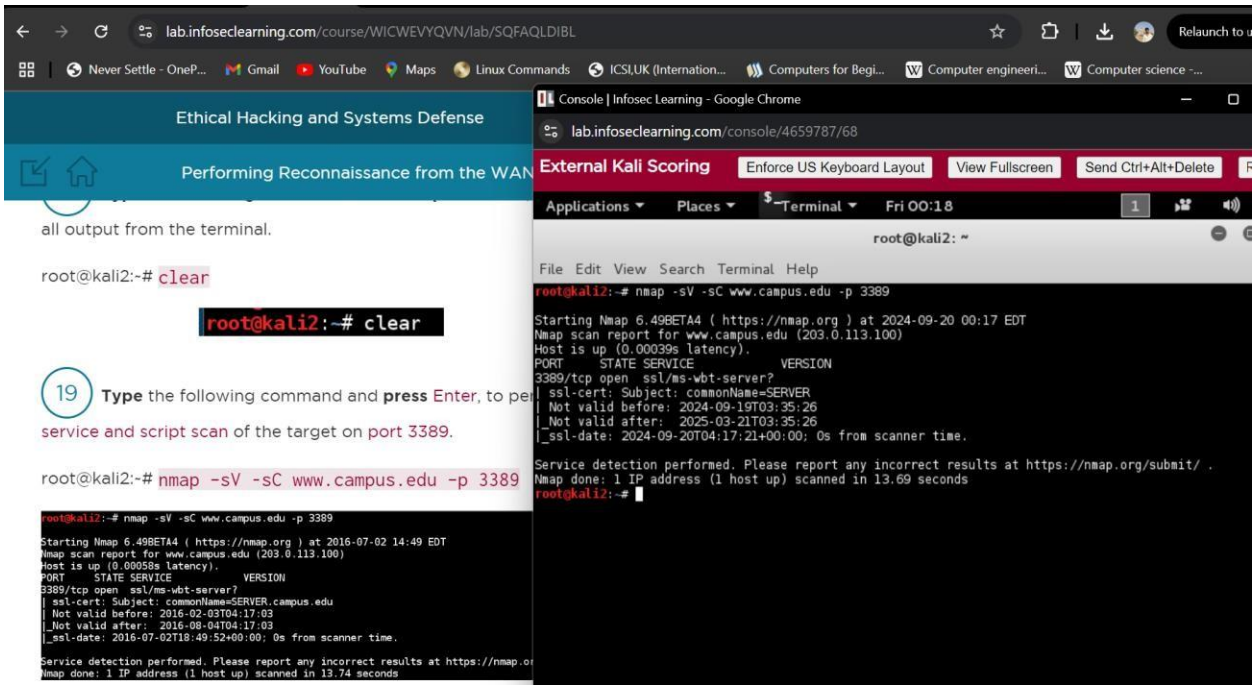
Nmap scan on www.campus.edu over port 1099



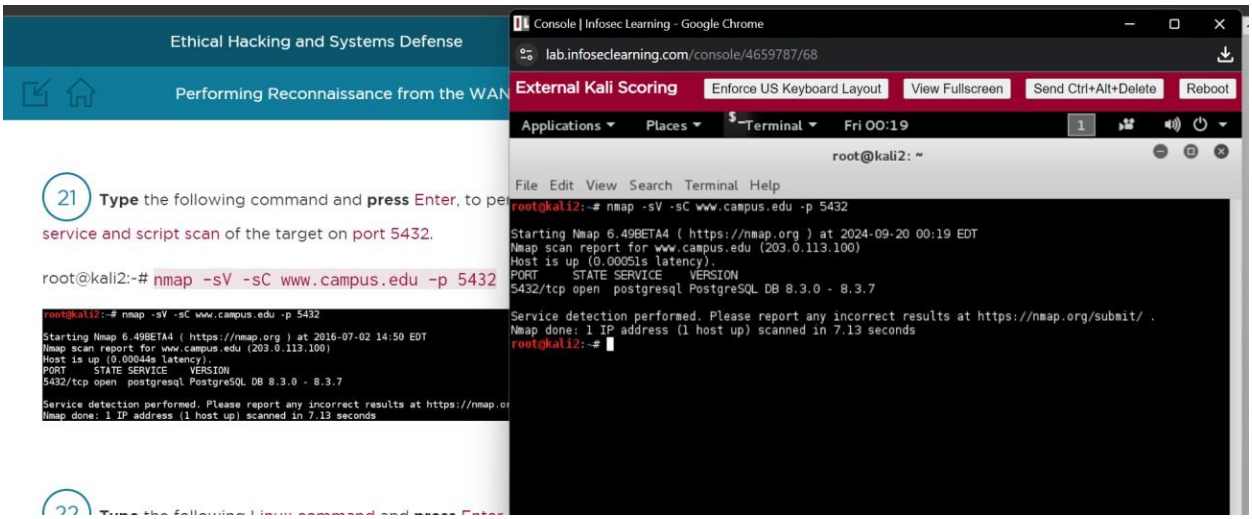
Nmap scan on www.campus.edu over port 3306



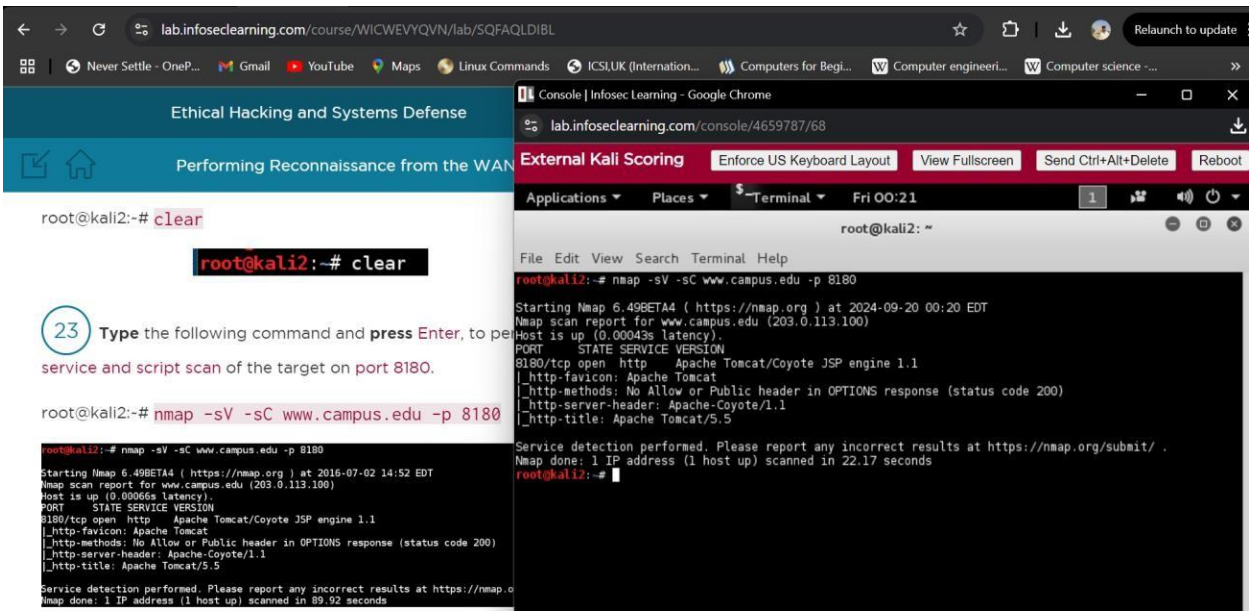
Nmap scan on www.campus.edu over port 3389

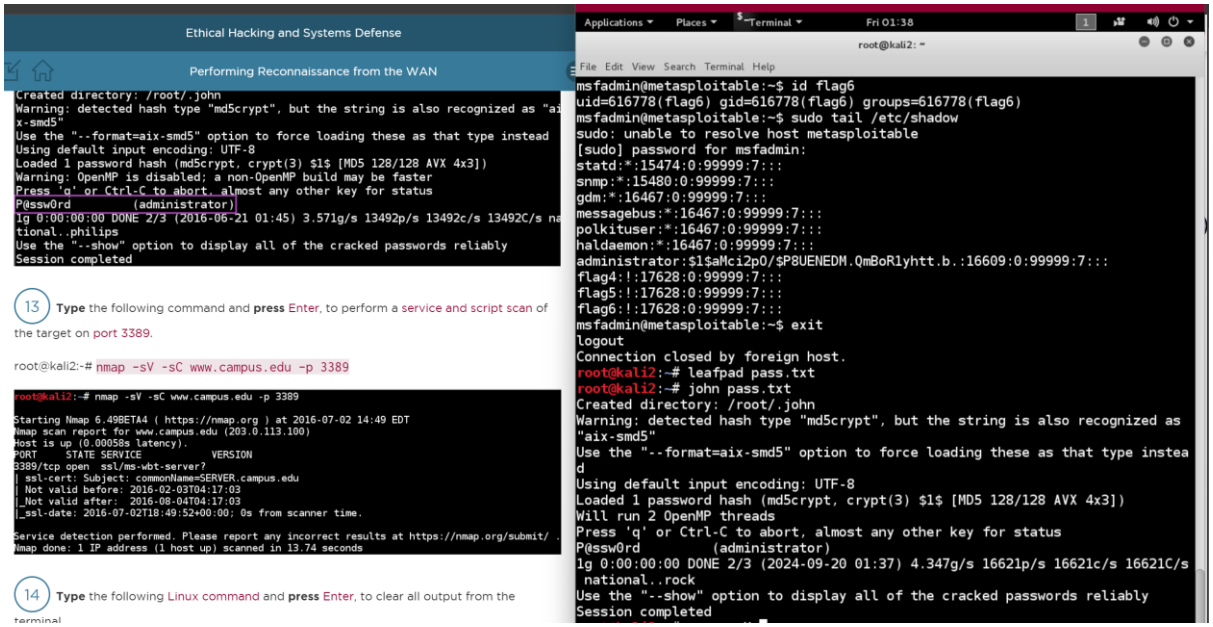


Nmap scan on www.campus.edu over port 5432



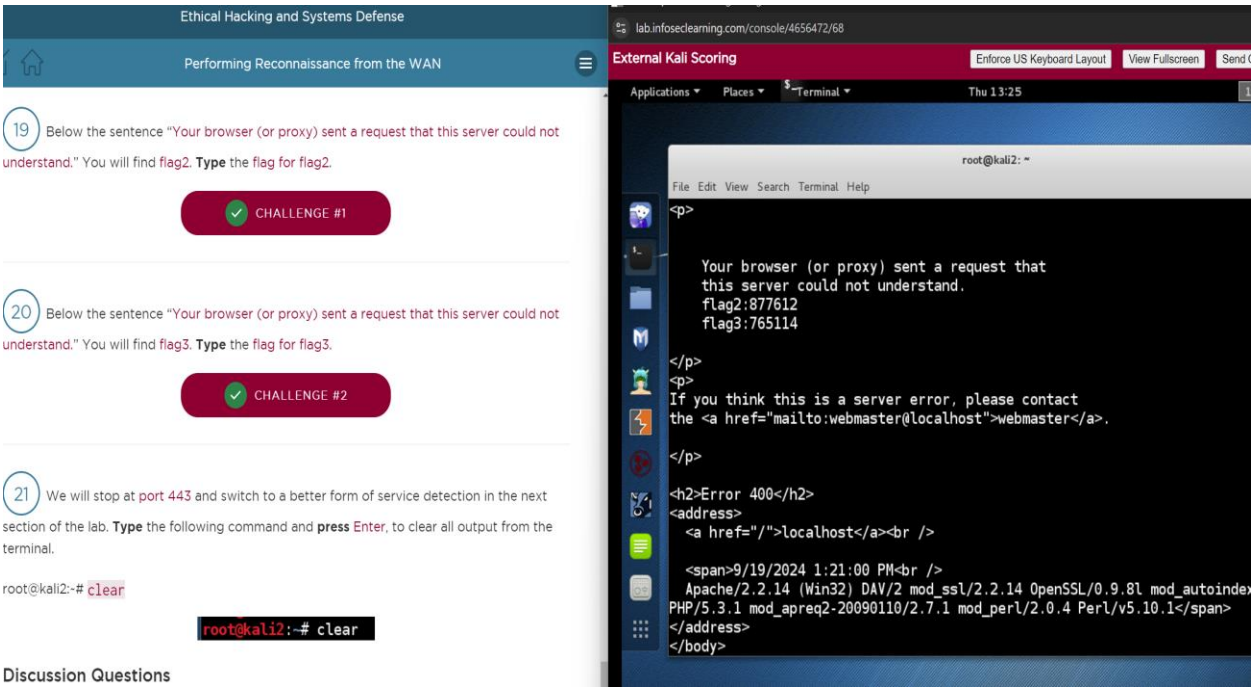
Nmap scan on www.campus.edu over port 8180

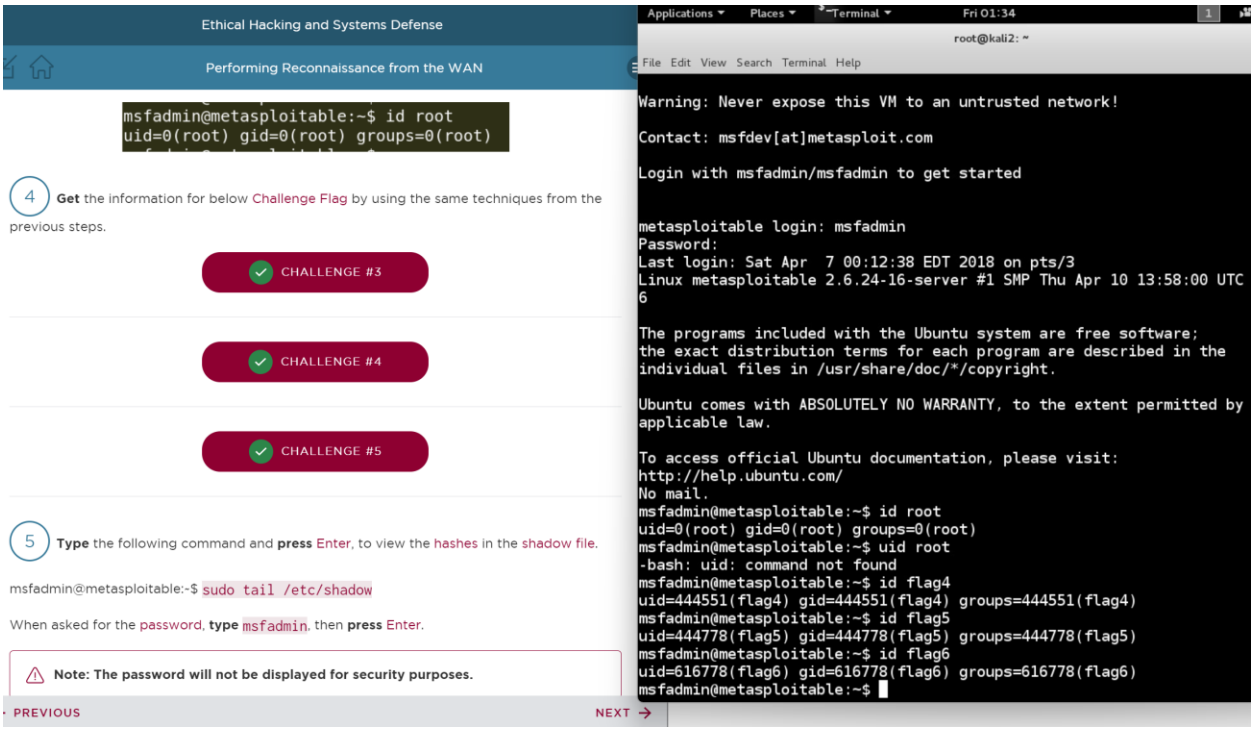




Supporting Evidence

The screenshot provides the progress in completing challenges related to identifying the flages during the lab exercise.





Conclusion & Wrap-Up

Summary with:

Observations

The Kali 2 machine successfully identified open ports on the pfSense firewall, detected Linux and Windows systems via port forwarding, retrieved the /etc/shadow file, and logged into the Windows Server using RDP.

Identified risks

Exposing services like Telnet, retrieving password hashes from /etc/shadow, and forwarding ports to internal systems pose significant security risks, leaving the network vulnerable to exploitation.

Suggested recommendations

Disable insecure services, apply strong firewall rules, update systems regularly, and enforce multi-factor authentication with monitoring to detect unauthorized access

Your successes & failures

Successfully performed port scanning, identified operating systems, retrieved sensitive files, and accessed the Windows Server via RDP

Some tasks took longer than expected, and reliance on default tools limited the depth of scanning.

Challenges

Challenges included avoiding detection during scans, cracking complex password hashes, and ensuring stable RDP access to the Windows Server.