Lab 04: Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation

Joseph Patrick C. Galvez

American Military University

ISSC262: Red Team and Blue Team Security

Mr. Brian Burnett

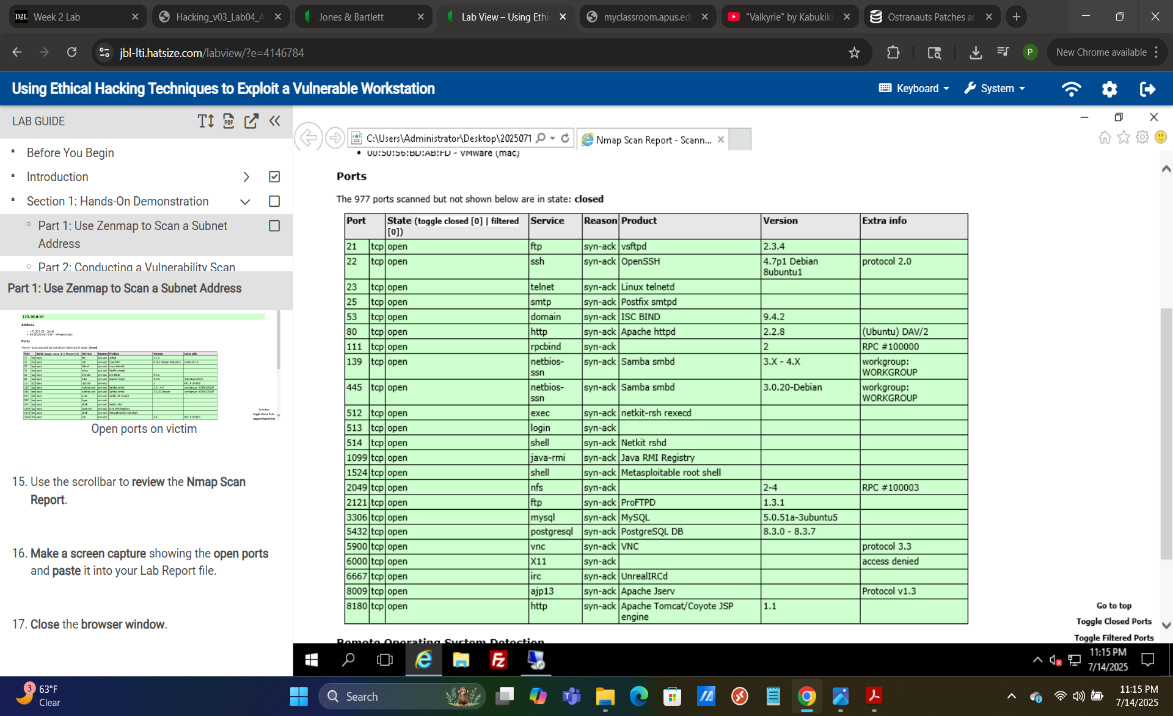
7/16/25

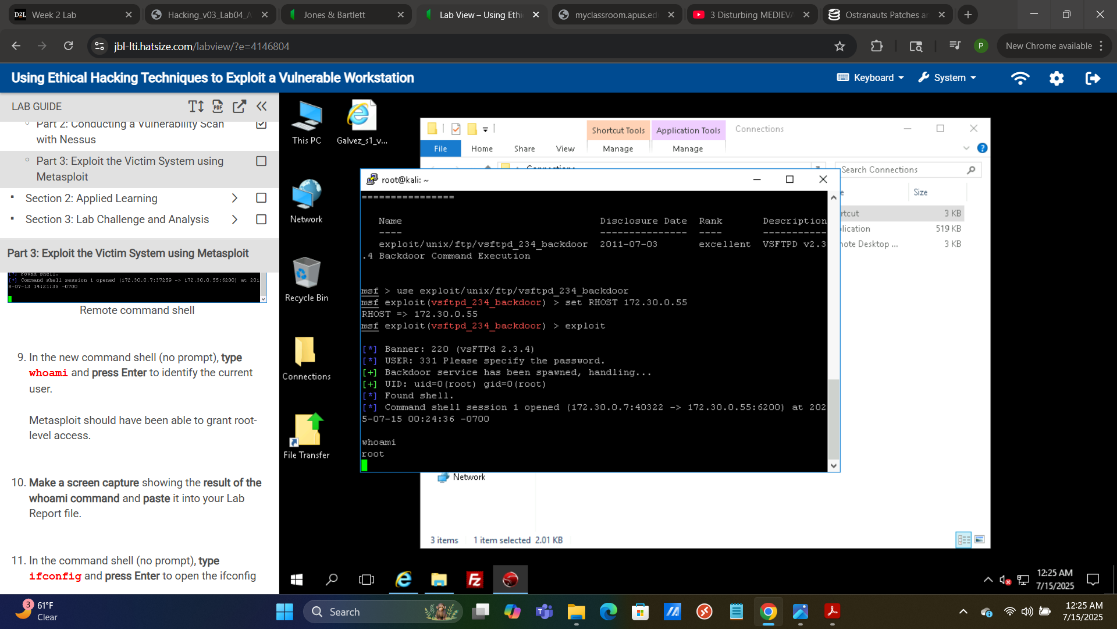
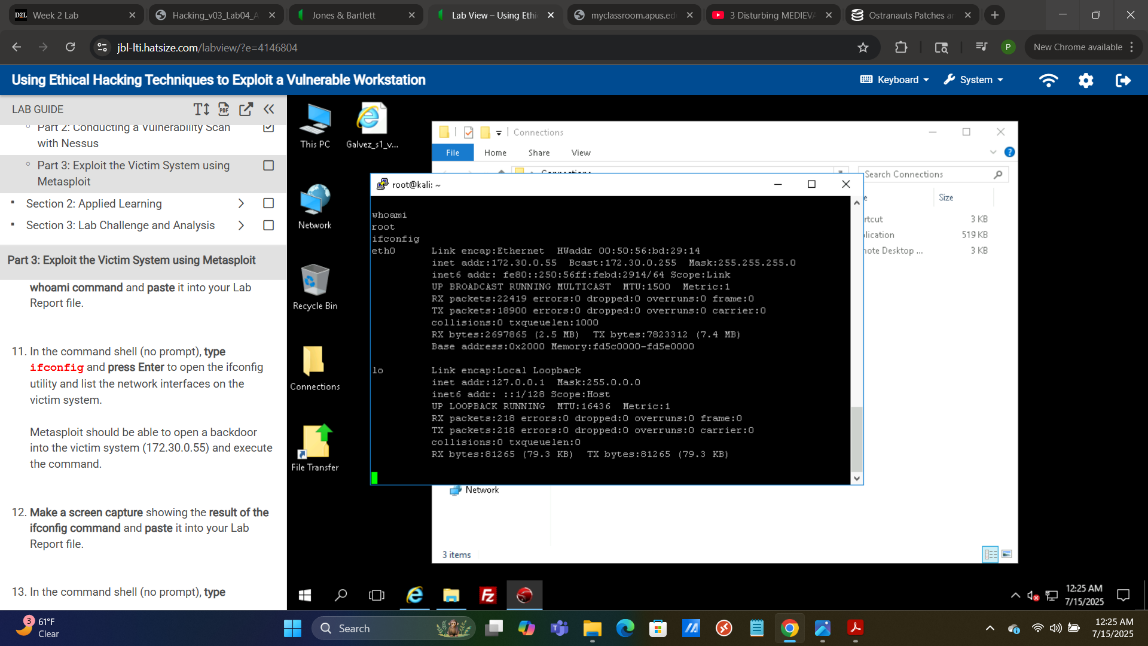
Lab 04: Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation

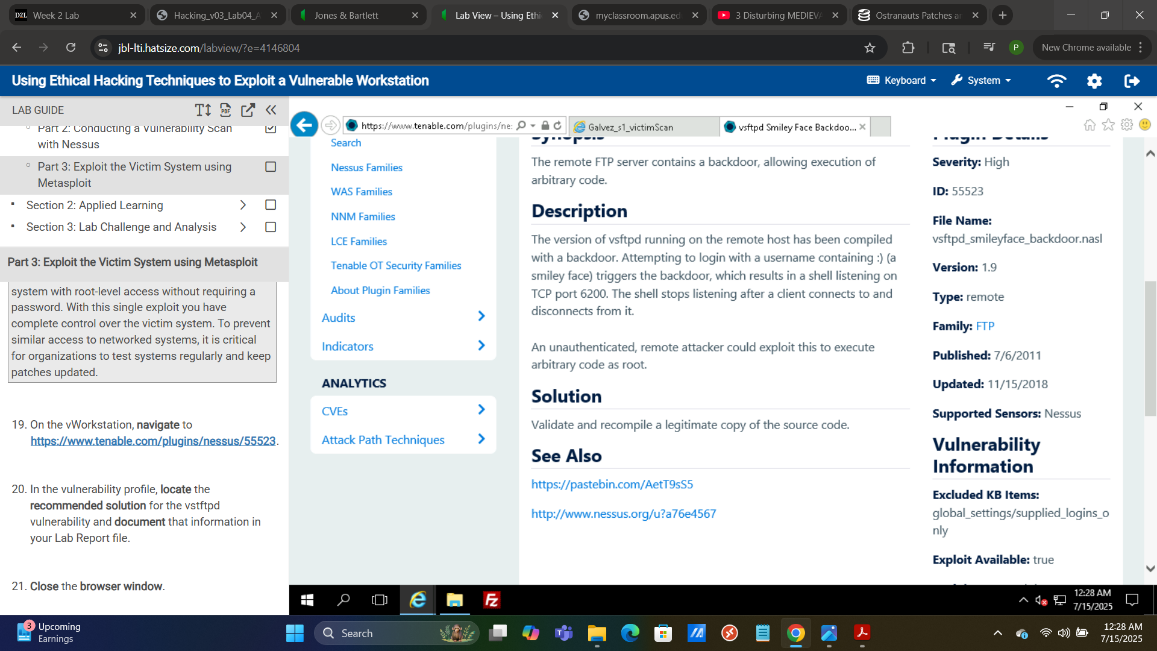
The purpose of this lab is to introduce students to ethical hacking through the use of tools to conduct the five phases of ethical hacking: reconnaissance, scanning, enumeration, exploit, and post-attack activities. The lab consisted of using tools such as Zenmap for reconnaissance, Nessus for scanning, Metasploit for exploitation and post-attack activities.

# Methodology

## Section 1

[[1]](#footnote-1)A computer screen shot of a computer screen

AI-generated content may be incorrect.[[2]](#footnote-2)[[3]](#footnote-3)[[4]](#footnote-4)

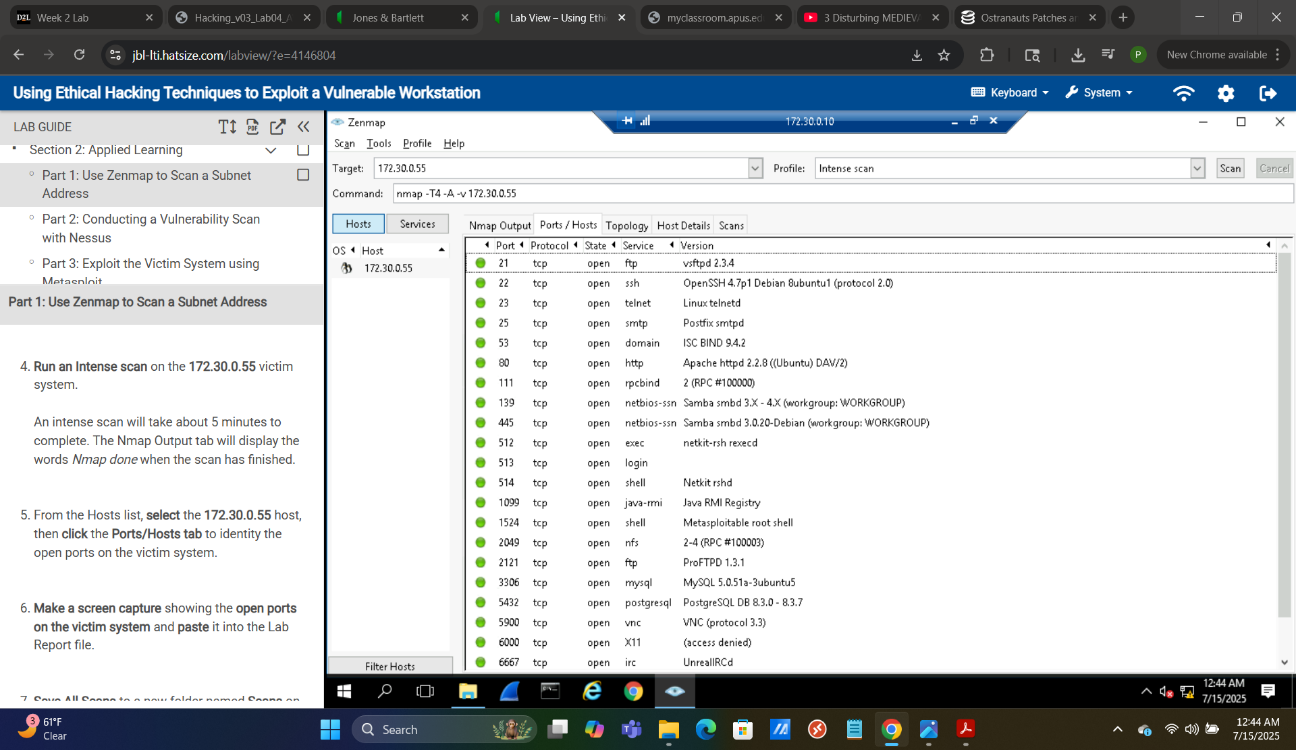
[[5]](#footnote-5)A computer screen shot of a computer screen

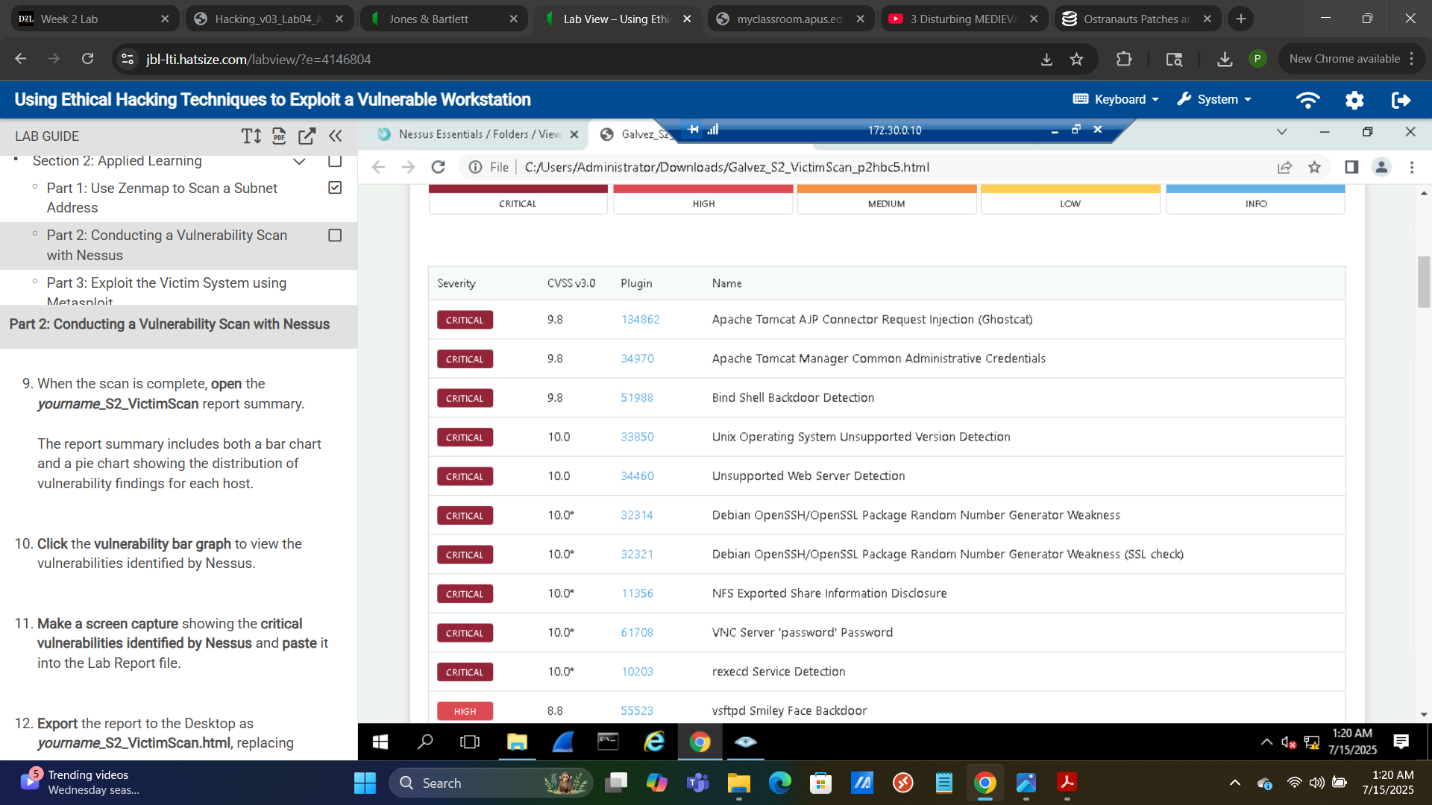
AI-generated content may be incorrect.[[6]](#footnote-6)

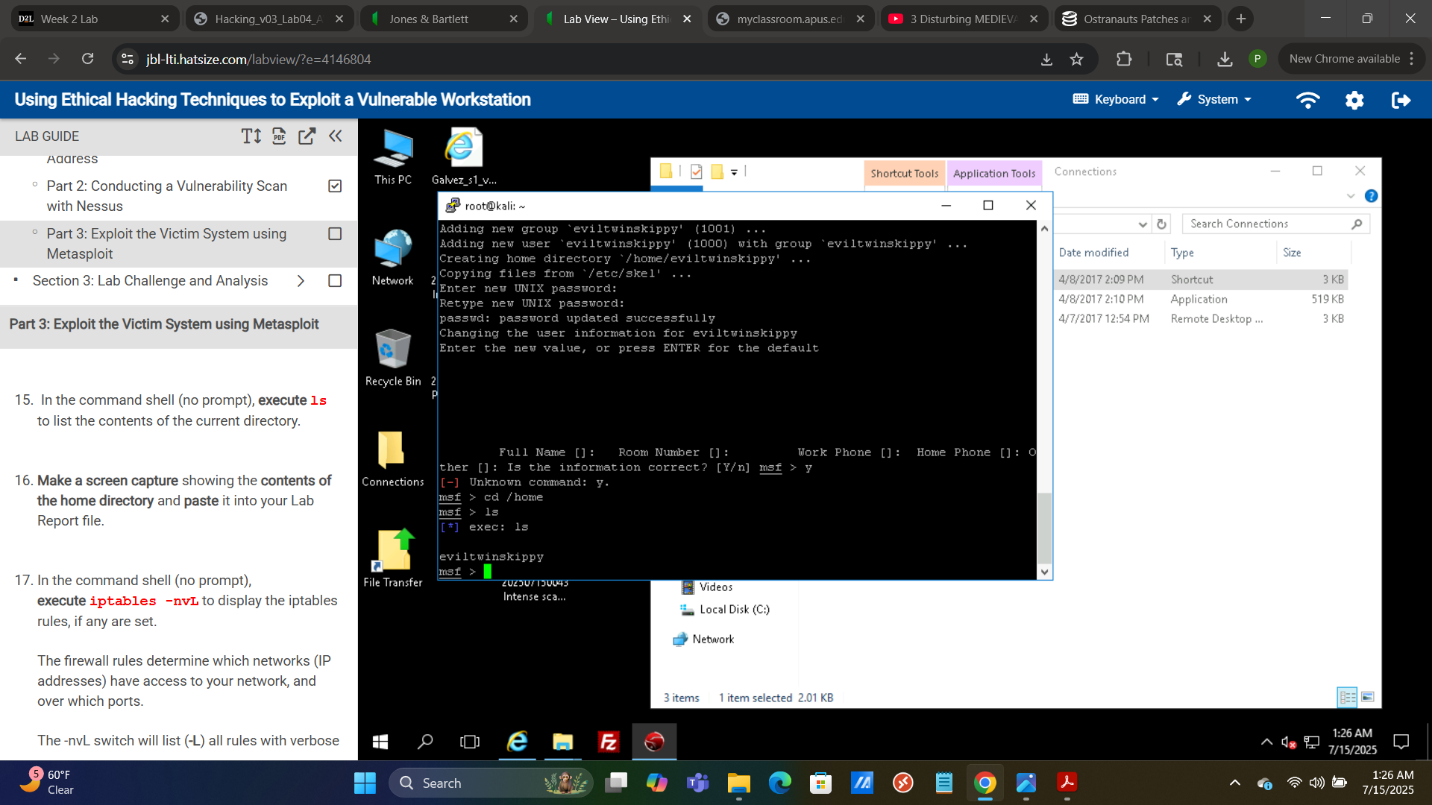
## Section 1 Executive Summary:

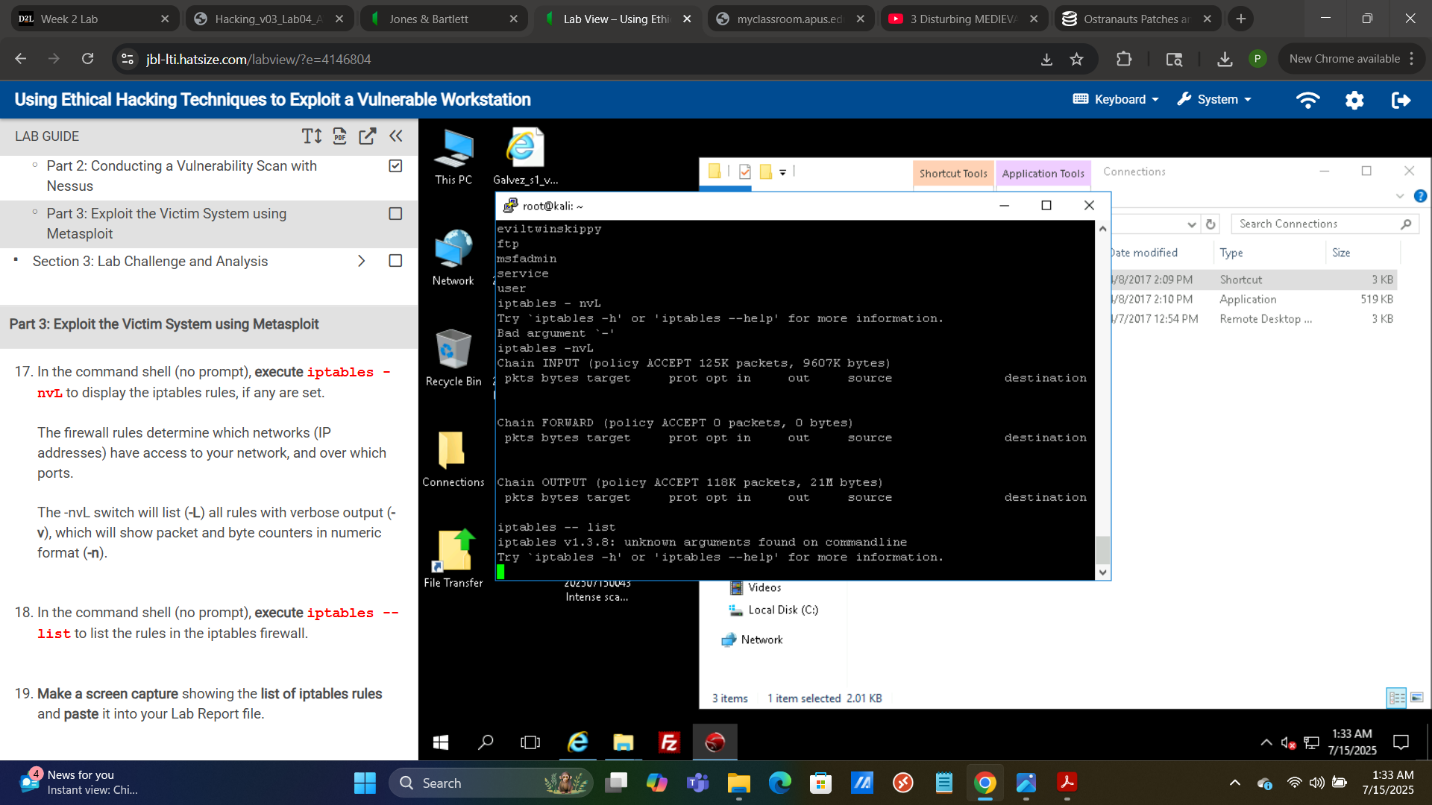
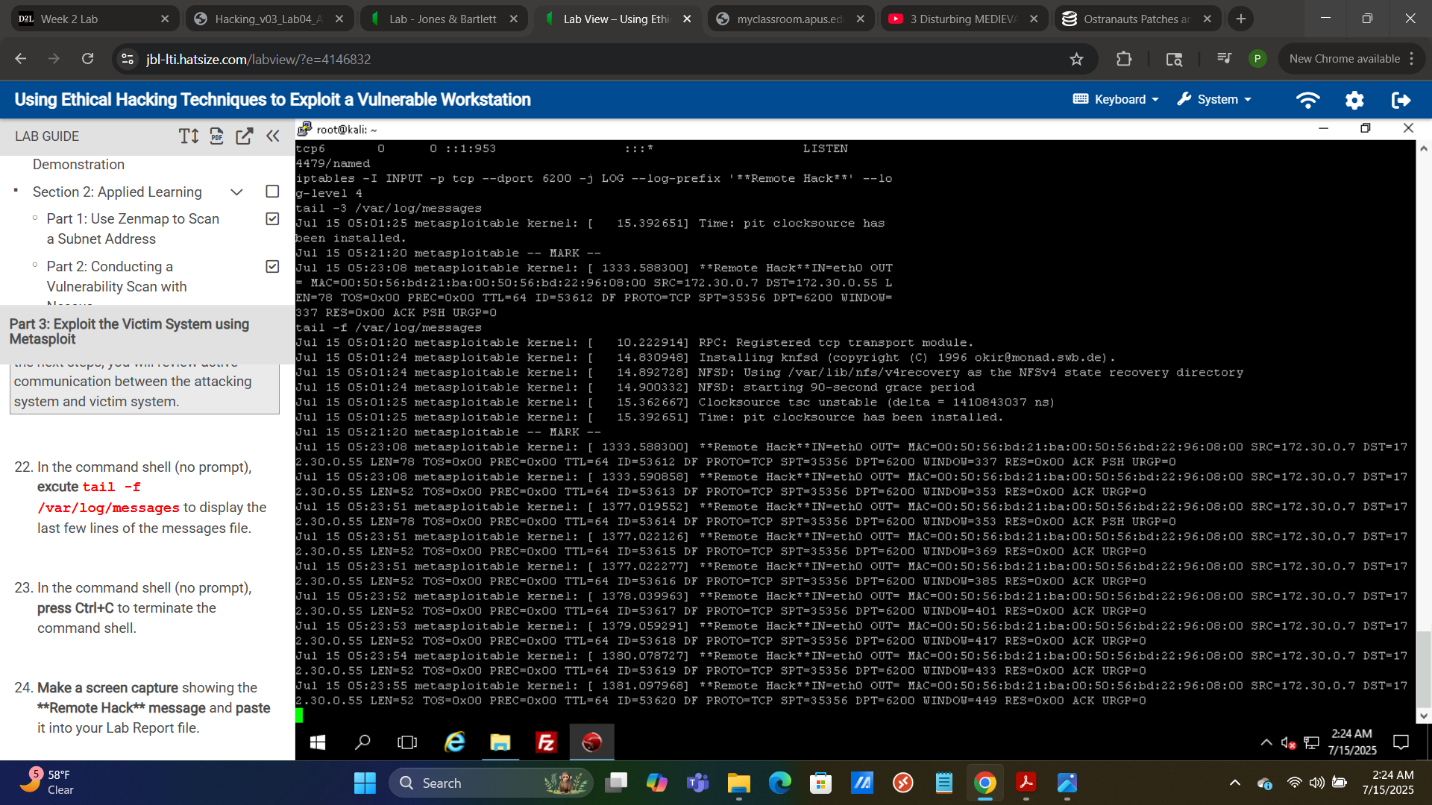
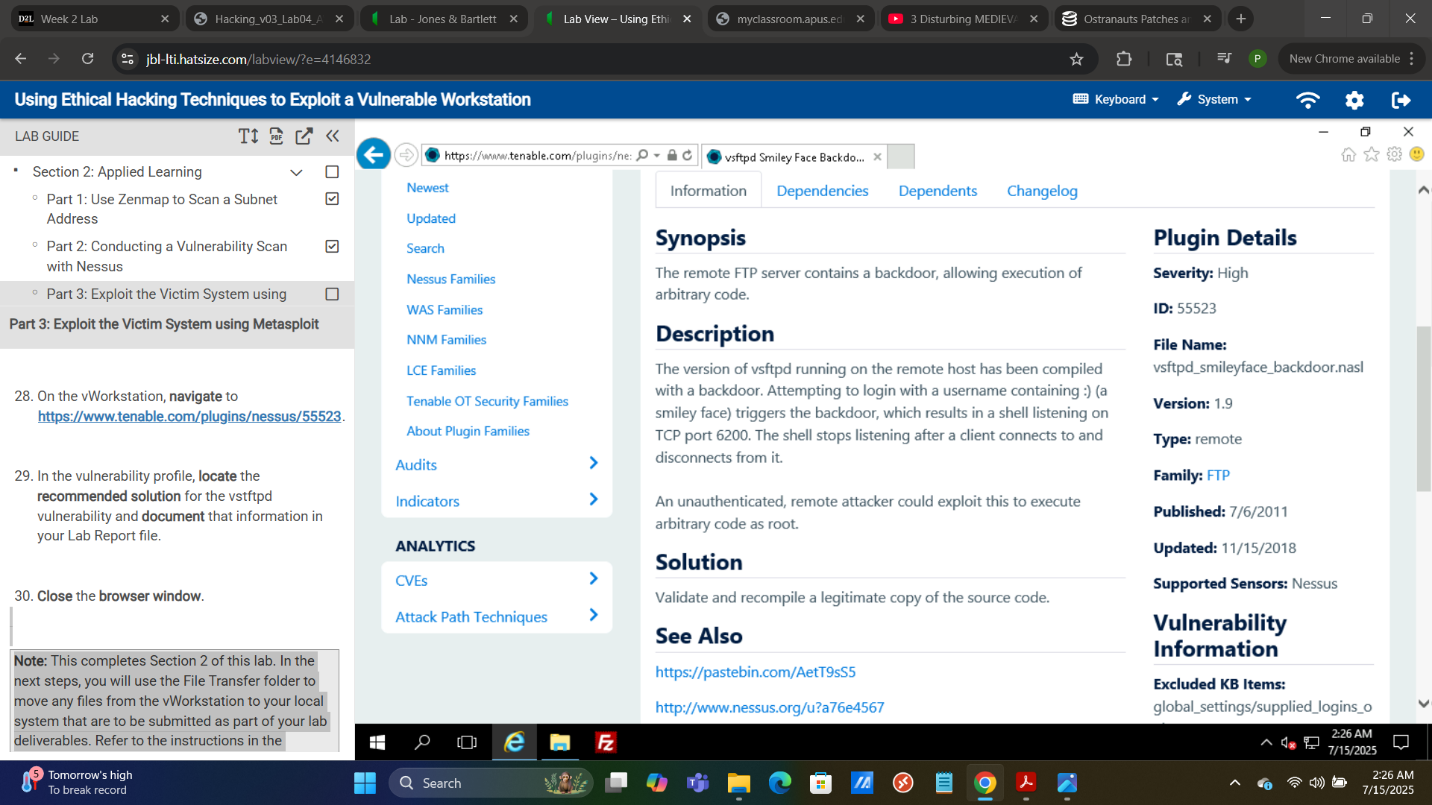
Section 1 consists of performing the five phases of ethical hacking to deploy an exploit on the target device, the exploit is a backdoor. Reconnaissance consisted of using Zenmap, which is an application that provides a gui for nmap, to locate open ports. Next Nessus was used for the scanning phase to identify vulnerabilities where 9 were identified. The exploit consisted of using a known vulnerability on vsftpd version 2.3.4. Access was maintained through the creation of a back door by the exploit on the open port 22. Post-attack activities consisted of terminating the command shell and ending the connection to the target device when the iptables rules were recorded.

## Section 2

[[7]](#footnote-7)

[[8]](#footnote-8)

[[9]](#footnote-9)[[10]](#footnote-10)A computer screen shot of a computer screen

AI-generated content may be incorrect.[[11]](#footnote-11)[[12]](#footnote-12)[[13]](#footnote-13)[[14]](#footnote-14)

## Section 2 Executive Summary:

Section 2 differs from section one in that the exploit consists of creating a new user as opposed to simply using a backdoor – it is a more established presence. Much like section 1 reconnaissance consisted of scanning for open ports with Zenmap. Scanning was performed with Nessus as well . Metaploit was used to create an exploit which utilized a backdoor much like section 1. However, the method for maintaining access differed in that a new user named “eviltwinskippy” was created using the kali root. The lab simply instructs to exit the PuTTY session once an exploit was ran to display that a remote hack was completed.

References

LTI. (n.d.). *LabVIEW*. JBL. Retrieved July 17, 2025, from https://jbl‑lti.hatsize.com/labview/?e=4149846

1. Figure 1 – Nmap scan on target device [↑](#footnote-ref-1)
2. Figure 2 – Results of Nessus Vulnerability Scan. [↑](#footnote-ref-2)
3. Figure 3 – whoami command ran on target computer kali root to confirm that this is the target device. [↑](#footnote-ref-3)
4. Figure 4 – ifconfig command ran on target computer kali root. [↑](#footnote-ref-4)
5. Figure 5 – iptables rules of the target device. [↑](#footnote-ref-5)
6. Figure 6 – ip table rules of the target device [↑](#footnote-ref-6)
7. Identified vulnerability of the target device. [↑](#footnote-ref-7)
8. Identified open ports on the target device [↑](#footnote-ref-8)
9. Vulnerabilities identified by Nessus [↑](#footnote-ref-9)
10. New user created on the target device [↑](#footnote-ref-10)
11. Contents of created user directory. [↑](#footnote-ref-11)
12. iptables rules of created user [↑](#footnote-ref-12)
13. The “\*\*Remote Hack\*\*” message confirms that the exploit has been delivered. [↑](#footnote-ref-13)
14. Solution for the exploit used in section 2 [↑](#footnote-ref-14)