|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |
| **Lab Report** |
| COURSE: Cyber 262  Lab : Host Based Network Defense  Submitted BY: Jack Morgan  Date: 01/21/2022  Instructor: Hozza |
| *By submitting this report I certify that this is my work and was not copied from other sources. Any use of public materials is cited.* |

Table of Contents

[INTRODUCTION 3](#_Toc50470226)

[SCREEN CAPTURES 4](#_Toc50470227)

[REFLECTION 15](#_Toc50470228)

# INTRODUCTION

For our first lab of the year, we will be delving into host based network defense and inspecting both sides of the equation, attackers and defenders. We will be inspecitving defensive aspects such as firewalls and penetration testing and looking into tools such as Zenmap and Ncrack to scan the victim and crack their passwords. We will also be utalizing ideas such as zero trust defense, which is the idea of denying all trafic in firewalls for the most optimal form of protection. Although basic concepts, all ideas in this lab are crucial to understand for our future experimentation and exploration in cybe security.

# SCREEN CAPTURES

***Figure 1.1: Take a screen shot showing your ID was added to the system.***

***Graphical user interface, text

Description automatically generated***

Figure .1: Adding user profile to accounts

***Figure 1.2: Take a screen shot showing the Zenmap scan on the Kali server.***

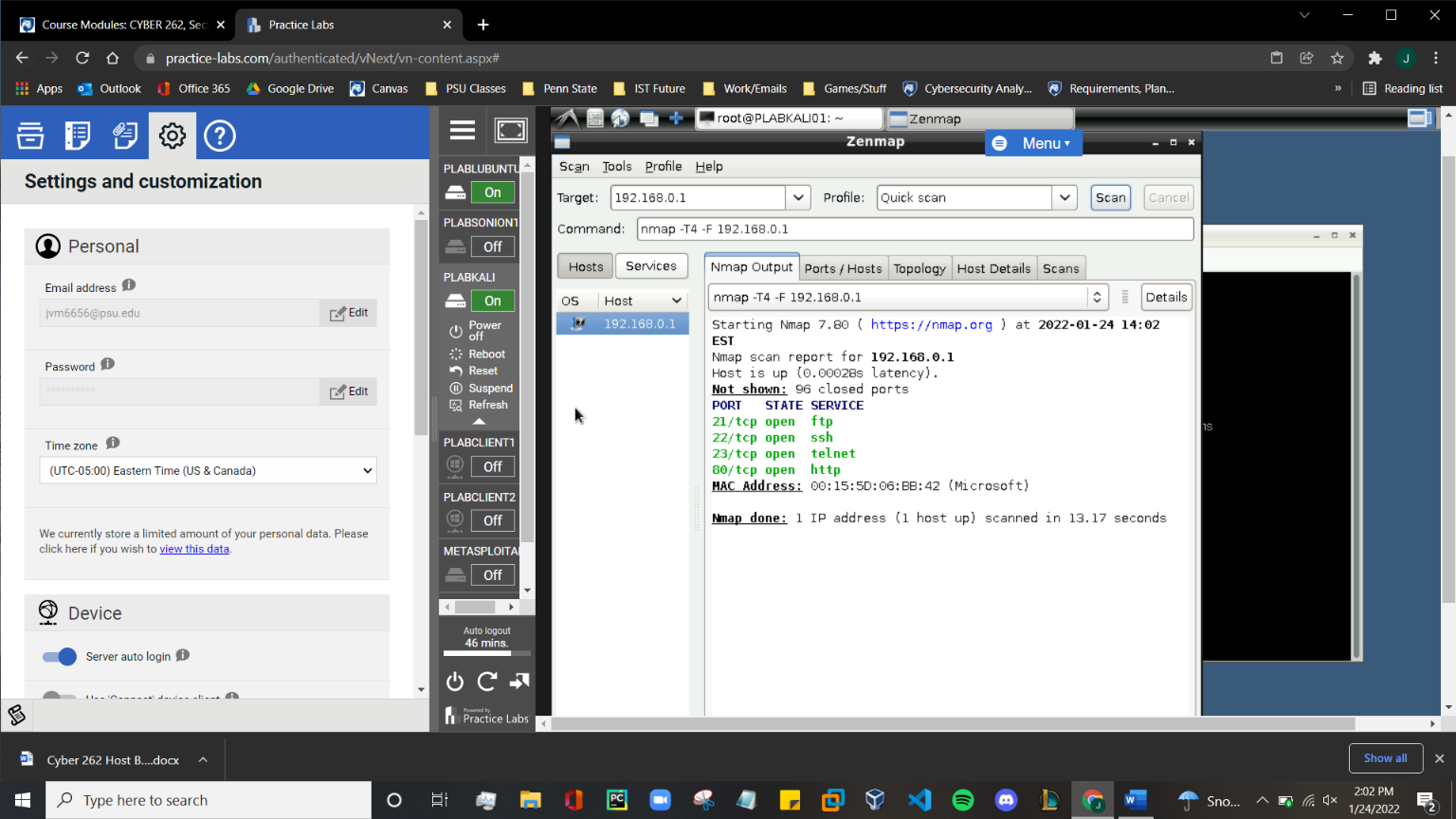
******

Figure : Using zenmap to check active ports

***Figure 1.3: Take a screen shot showing the password cracked by Ncrack.***

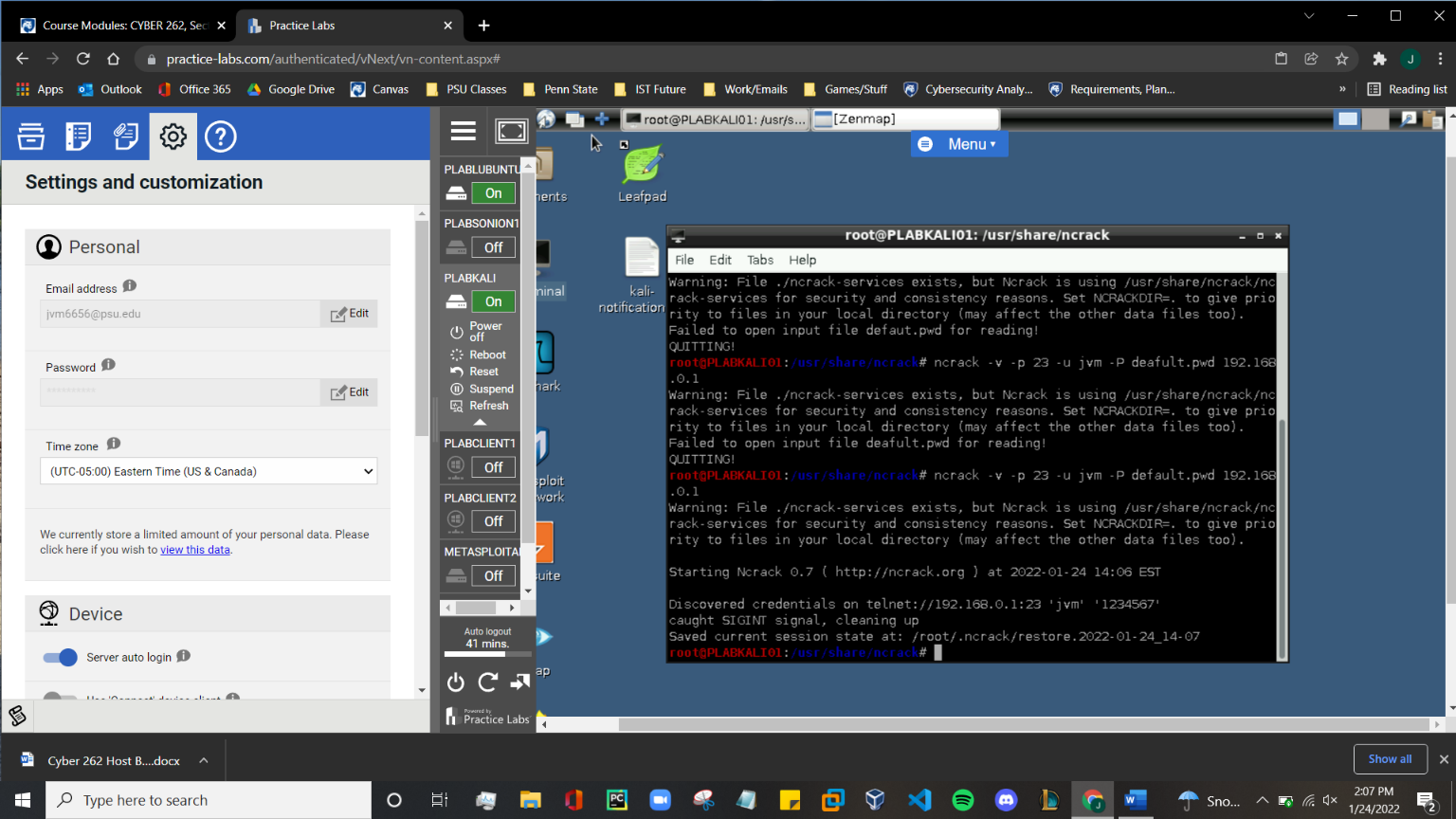
******

Figure : Using ncrack to crack the password of the user account

***Figure 1.4: Take a screen shot showing the telnet went through using the ID and password you found***

***Graphical user interface, text

Description automatically generated***

Figure : Using telnet to confirm that we can connect to the port

***Figure 2.1: From the Attacker machine try to telnet to the Victim (192.169.0.1) and a screen shot of the command prompt.***

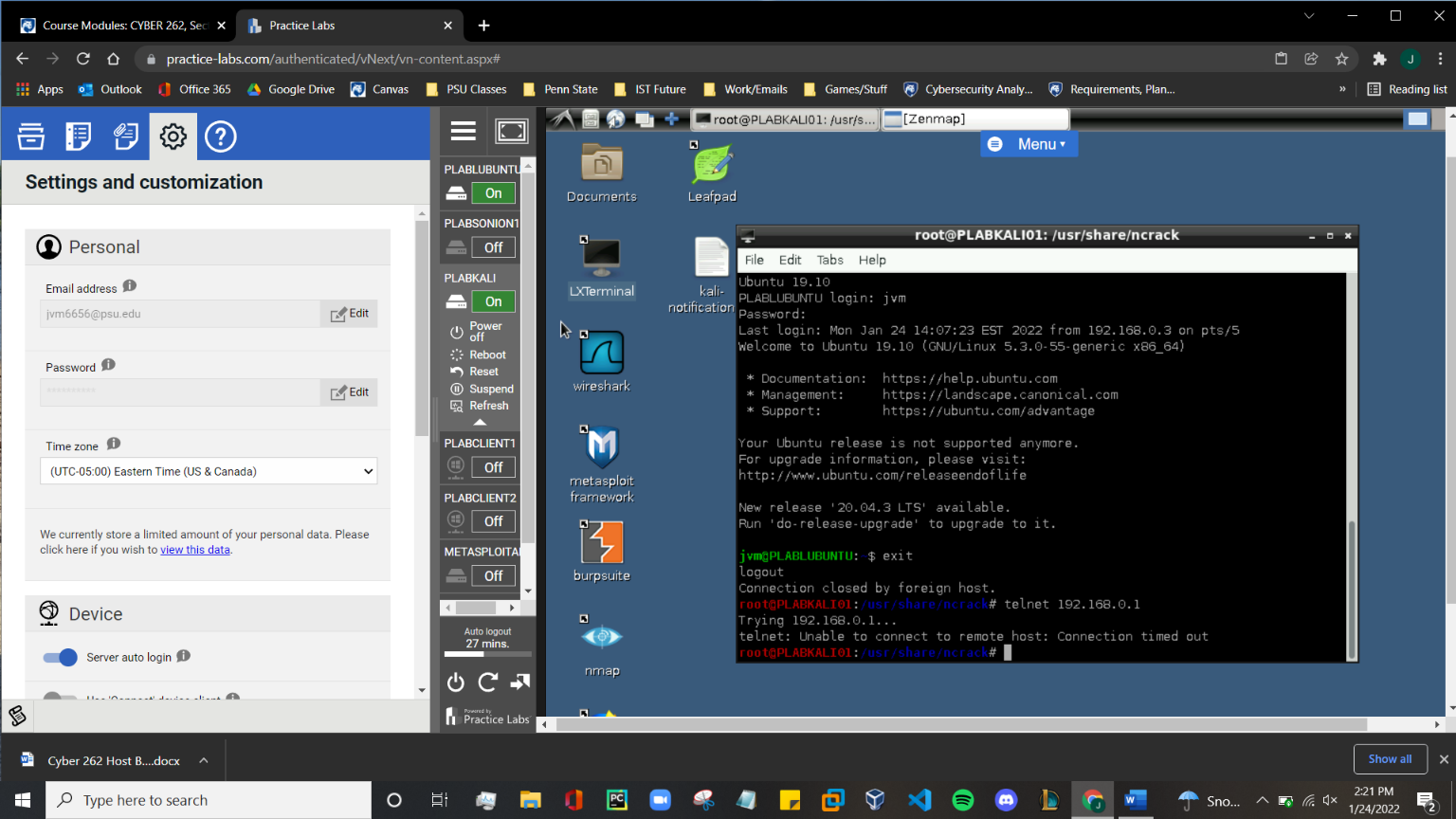
******

Figure : Telnet to victim fails because firewall is active

***Figure 2.2: Take a screen shot illustrating the ufw status to prove you are using default deny.***

***Graphical user interface, text, application, chat or text message

Description automatically generated***

Figure : Default Deny is enabled so all incoming connections are denied

***Figure 3.1: Take a screen shot illustrating the changes you made in the ufw with a ufw status verbose output.***

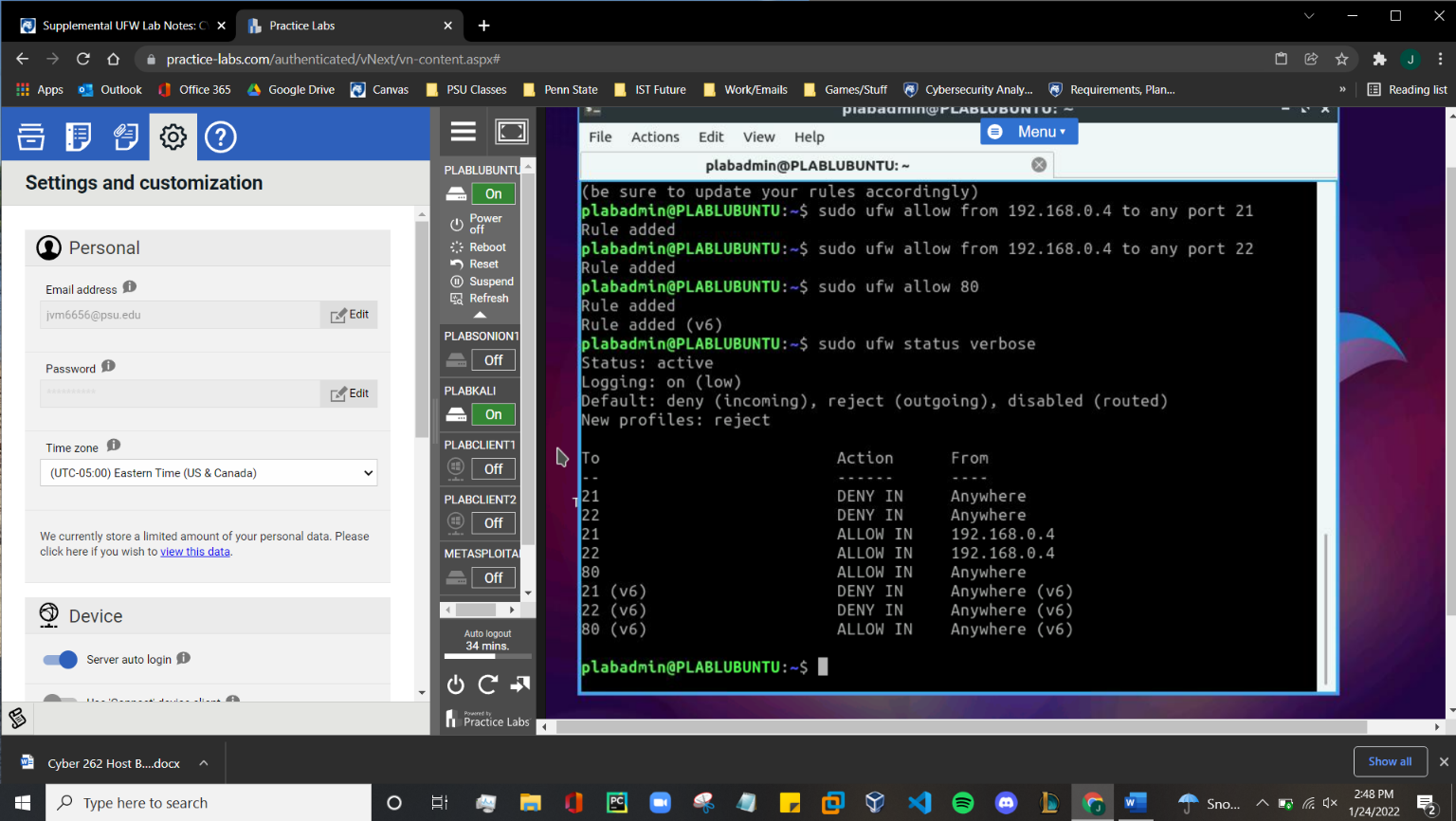
******

Figure : Denied acces from all ports except 21 and 22 from 192.168.0.1 and port 80

***Figure 3.2: Take a screen shot showing which ports it has access to on the Victim.***

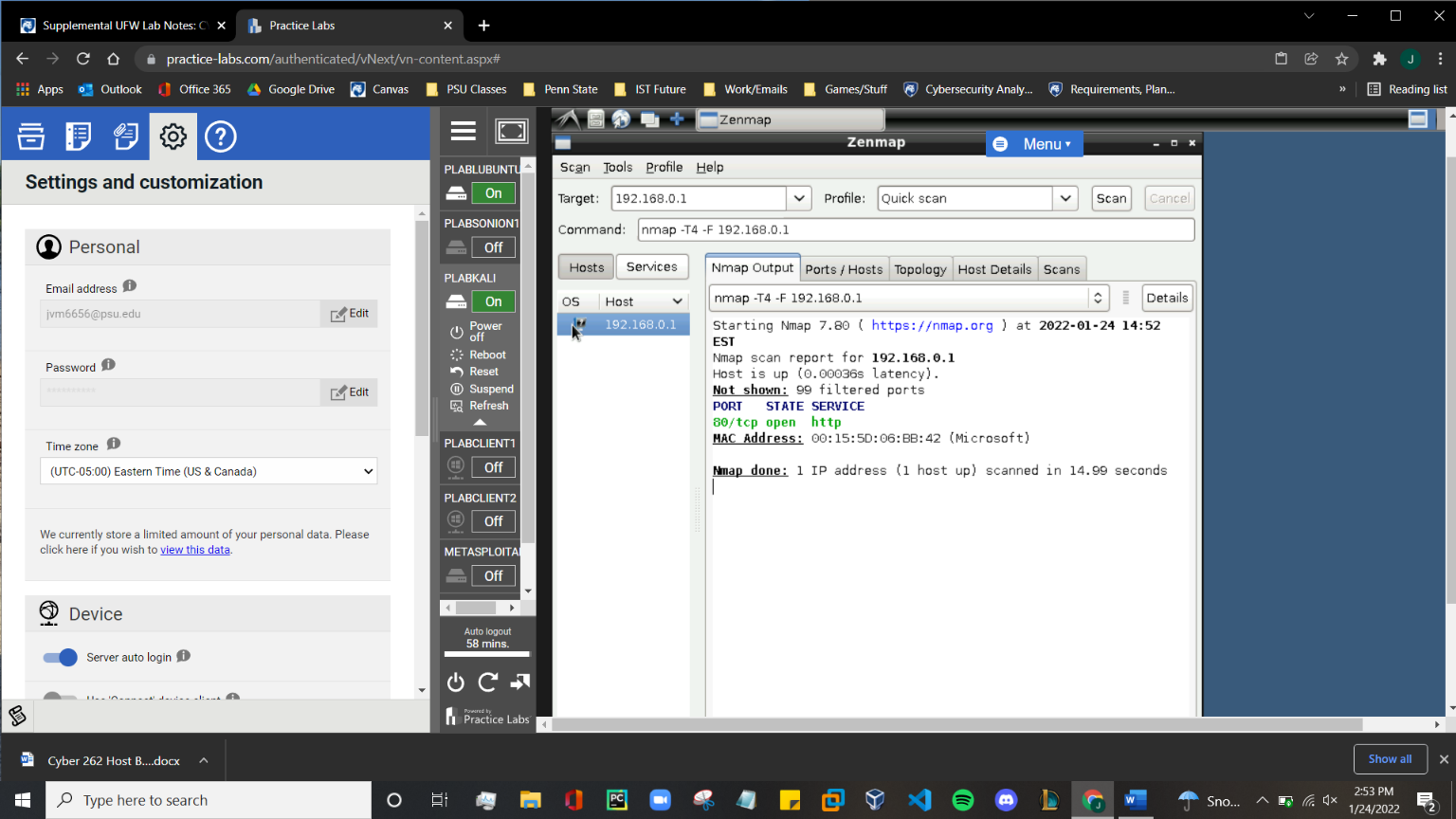
******

Figure : Showing that only port 80 is accessible from the attackers machine

***Figure 3.3: Take a screen shot of the PLABCLIENT1 showing the SSH session.***

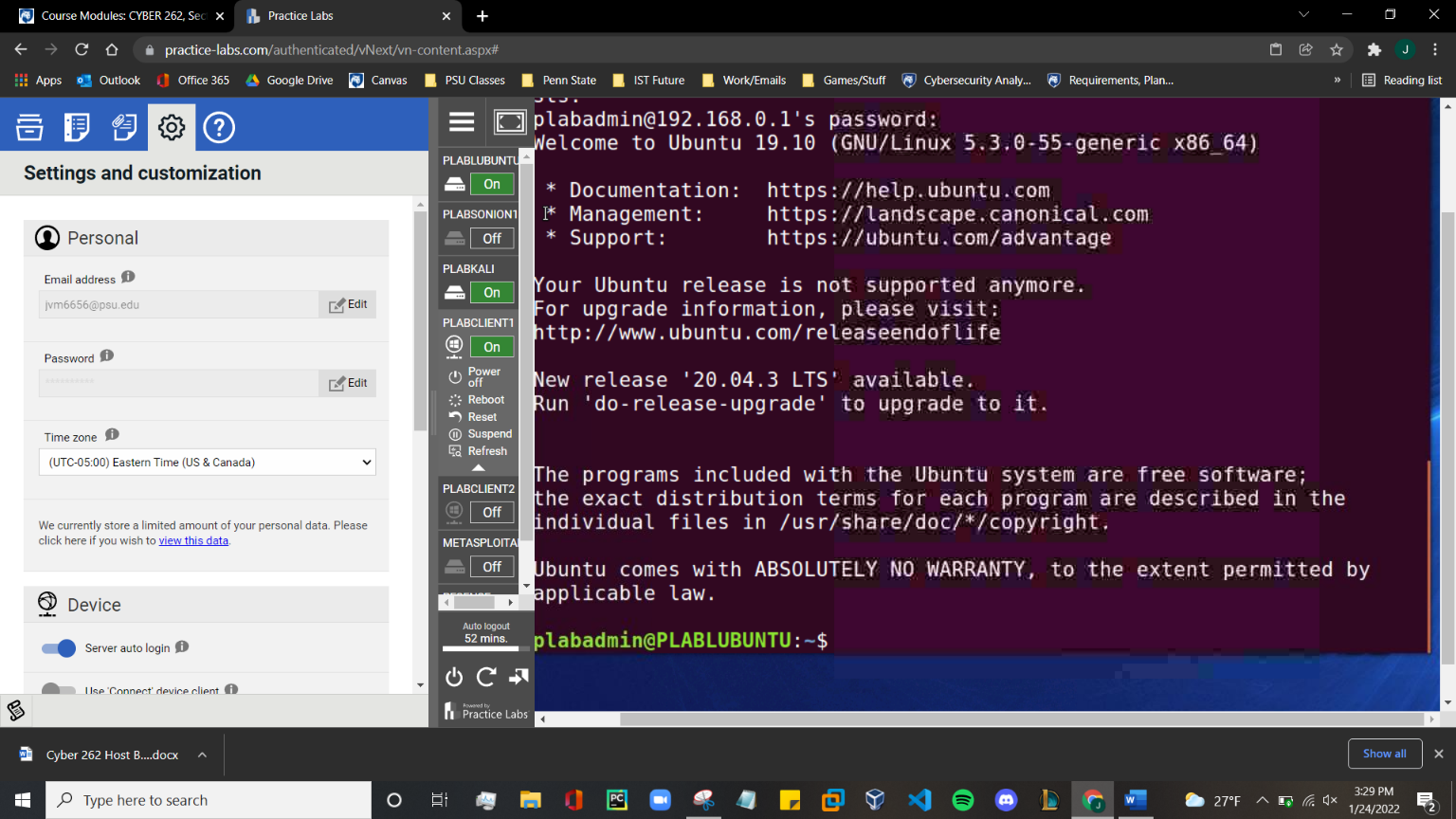
******

Figure : Showing that SSH is usable to connect from the PLABCLIENT 1 to the victims client

***Figure 3.4: Take a screen shot of the PLABCLIENT1 showing the FTP results.***

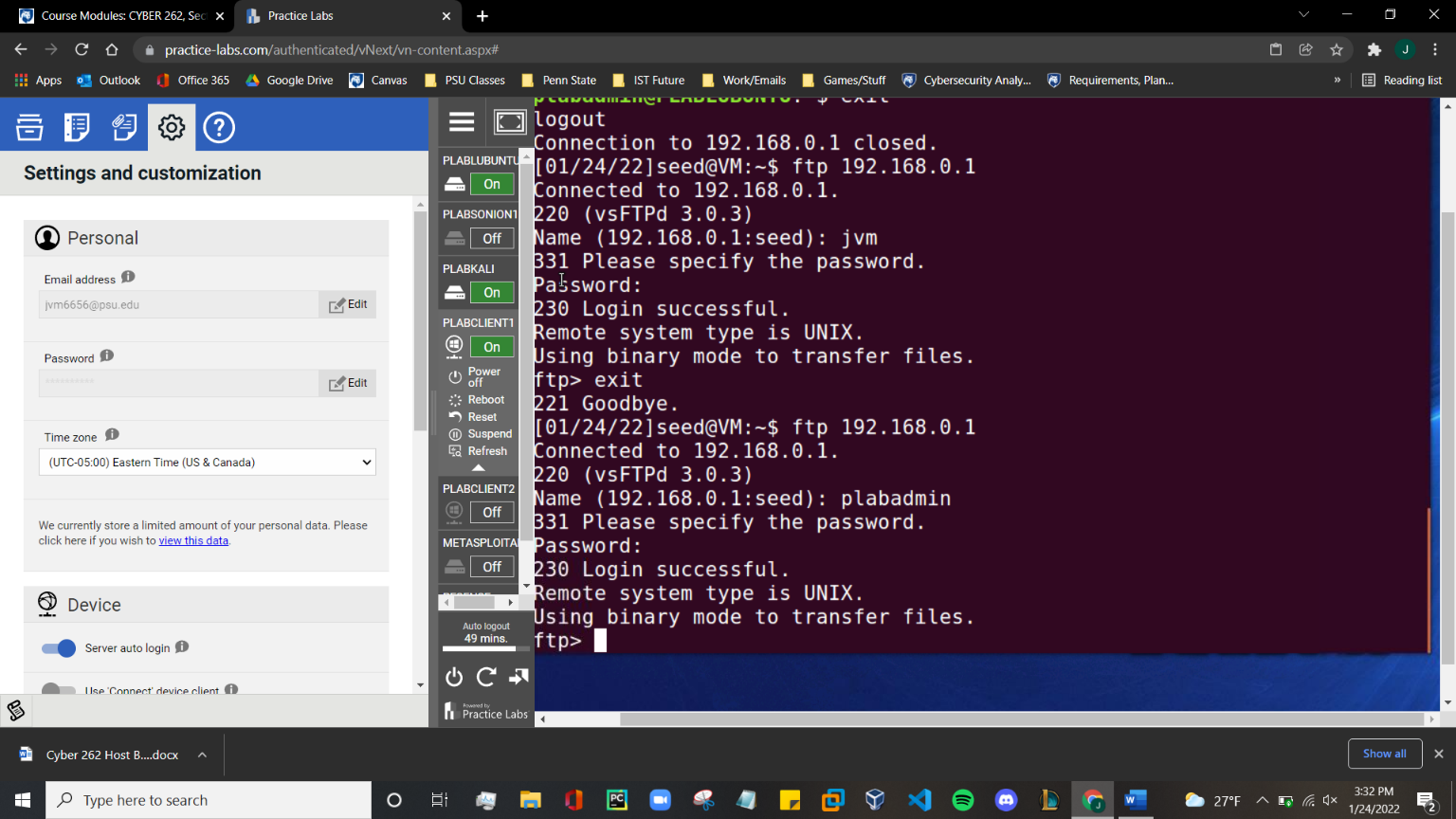
******

Figure : Using FTP to connect to the victims client from PLABCLIENT1

***Figure 3.5: Take a screen shot of the PLABCLIENT1 showing that you can run a ‘ls’ command from the ftp prompt of the victim that lists the files.***

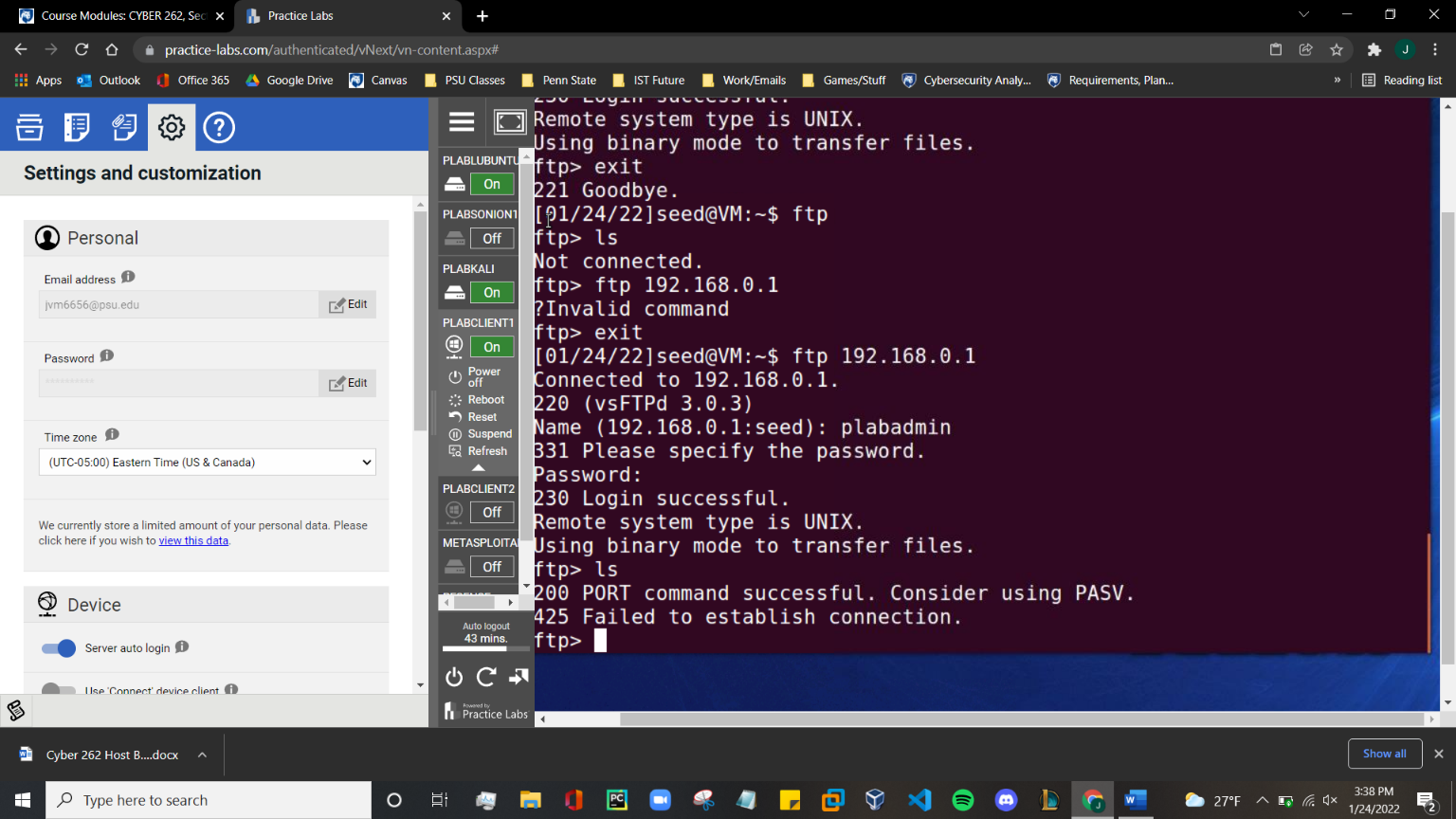
******

Figure : Attempt to use ls results Port 200 being accessible but denying port 425 which is HTTPS

***Question 3.6: Explain which option is more secure (Drop or Reject) by not immediately severing the connection.***

After briefly researching the topic and experimenting, it seems as though internet-based connections are better off using Drop so it has time to test the initial connection, where as Reject is better for non internet-based connections.

# REFLECTION

In this lab, we learned about basic cyber security defense, specifically the use of firewalls. By updating firewall preferences through ufw, we can deny or allow connection to and from specific ports that use specific protocols. On the other hand, we used ncrack and Zenmap to find accessible ports and attempt to crack passwords of known users. Although some of these skills may seem insignificant at this point, these skills will eventually become crucial to properly defend our information and maintain integrity in our systems.