|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |
| **Lab Report** |
| COURSE: Cyber 262  LAB: Metasploit Lab  Submitted BY: Jack Morgan  Date: 02/14/2022  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 8](#_Toc50470228)

# INTRODUCTION

During this lab we are going to be exploring penetration testing and performing a syn flood attack on the practice labs client 1. Performing this will allow for us to understand what a syn flood dos attack is like, how we can detect an attack and measures we can take to combat these attacks. We will also be using the Sparta program under the Linux client in practice labs to scan for available ports and clients to attacck prior to preforming our attack. Being able to perform these tasks is crucial for penetration testors to learn how to prevent these attacks prior to their occurance.

# SCREEN CAPTURES

***Figure (1):*** Take a screen shot of **PLABKALI** of the Services running on either **192.168.0.4** or **192.168.0.5**

Graphical user interface, text, application

Description automatically generated

Figure : This screenshot shows the Sparta client identifying the open clients that we can attack.

***Figure (2):***Take a screen shot of one of the **NMAP** text files showing information you could possibly use later. ***HINT:*** Files with the “.gnmap” extension usually have good data but choose a file you think is interesting.

Graphical user interface, application

Description automatically generated

Figure : Screenshot shows various .gnmap files with valuable information that could be used for an attack

***Figure (3):*** Take a screen shot to show that your search found the **synflood**.

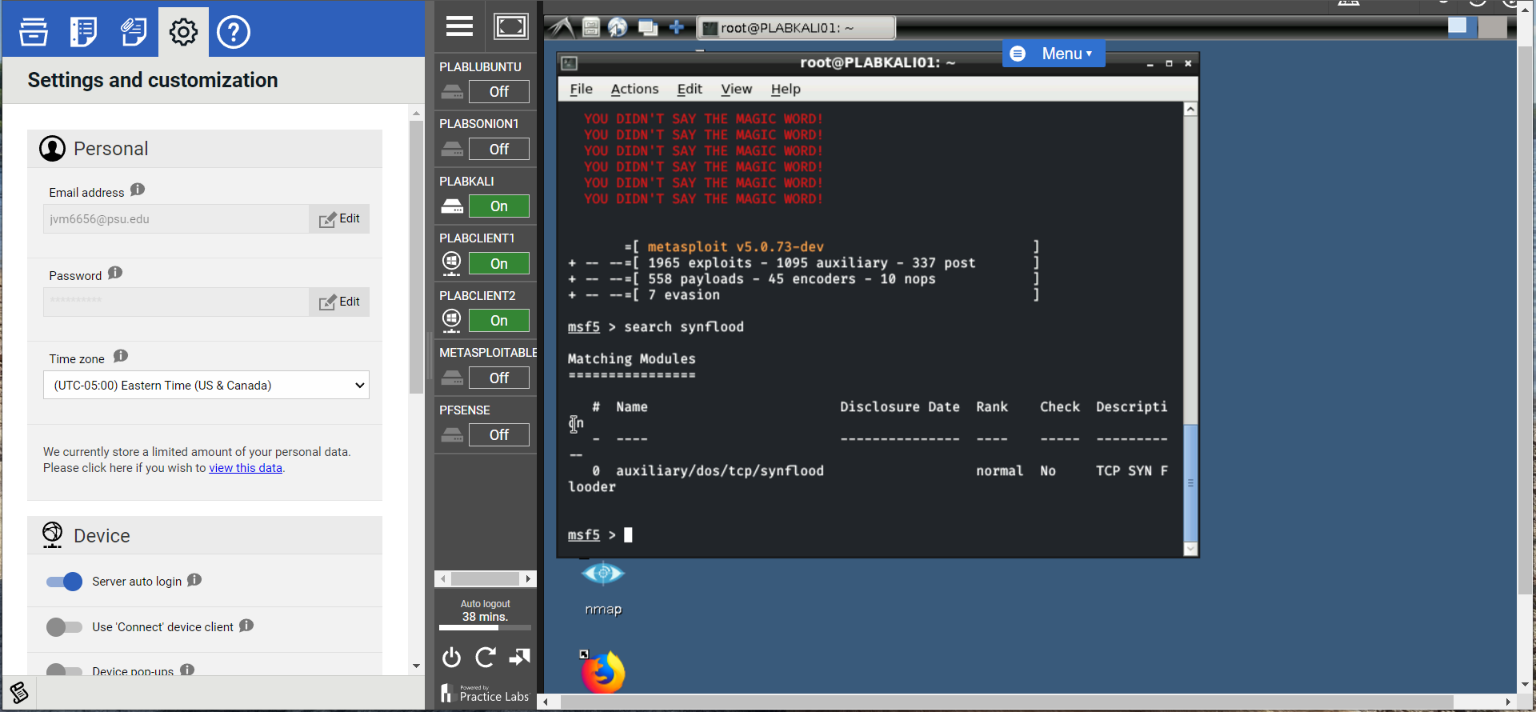


Figure : Screenshot displays access to the metasploit that we used to search for the synflood command

***Figure (4):***Take a screen shot to verify that telnet worked.

Graphical user interface, text

Description automatically generated

Figure : Shows active telnet command to the plabclient1

***Figure (5):*** Take a screen shot to show that telnet is not working during the SYN Flooding Attack.

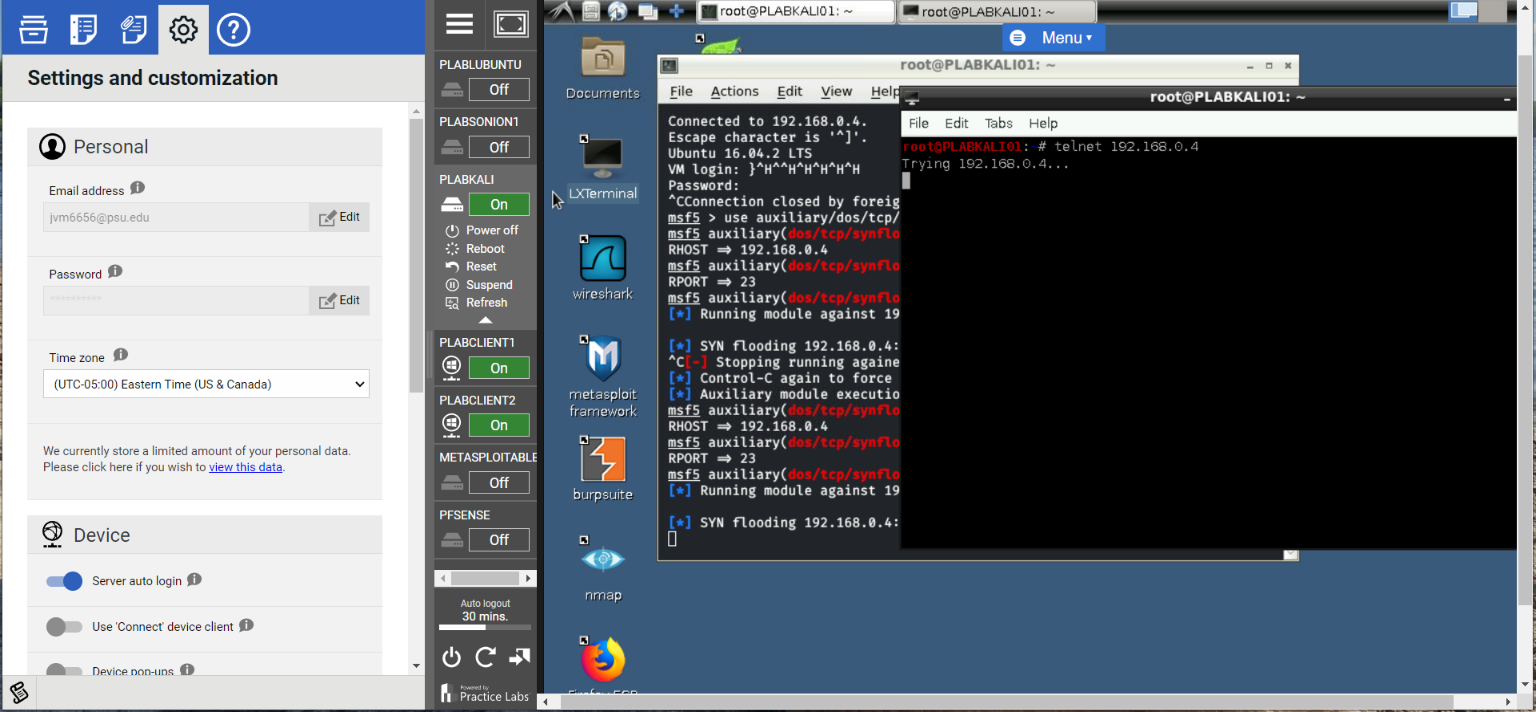


Figure : Screenshot shows an active telnet command that is not working due to the synflood attack

***Figure (6):*** Take a screen shot of showing the active telnet connection. ***Hint:*** your screen shot should be of PLABCLIENT server.

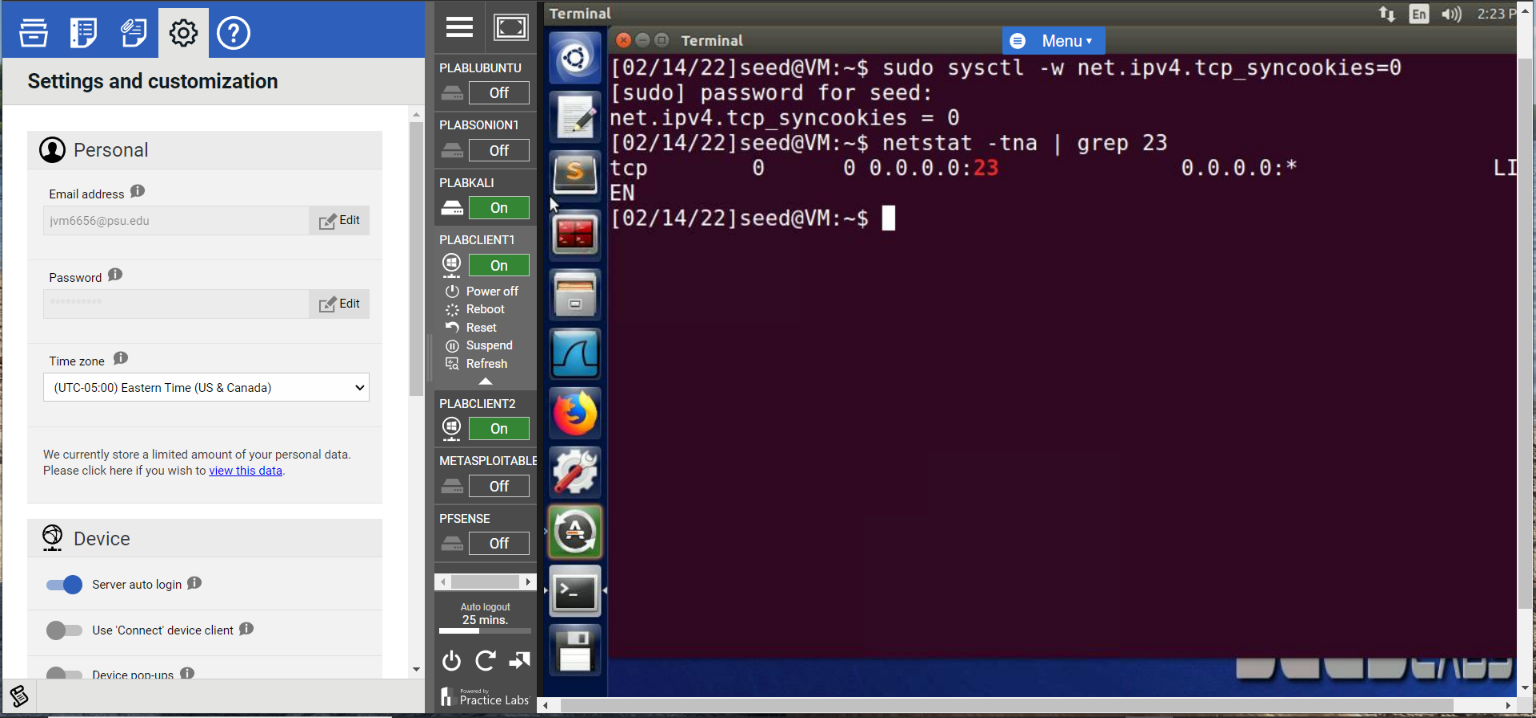


Figure : Screenshot shows the active telnet command from evidence with the seed prompt under the command line

***Figure (7):***Take a screen shot of showing the connections on port 23 during the attack using netstat

command.

***Graphical user interface

Description automatically generated***

Figure : Screenshot shows the active attack analysis on the port 23 server

***Figure (8):***Screen shot of showing netstat of second attack on **port 80**

***Graphical user interface

Description automatically generated***

Figure : Screenshot shows the port 80 analysis with the netstat command

# REFLECTION

During this lab, we performed a syn flood attack on the practice labs 1 client from our kali server to analyze what a syn flood attack looks like and how to defend against it. We performed an attack on the telnet and http ports and used netstat command to view all the attempted connections from the kali server’s attack. In addition, we learned how to use the Sparta client to scan for open ports and/or clients to attack. For penetration testers, this is crucial to learn and as a result, we now know how to perform and defend against these attacks, knowing how the attacks work will help us defend against them in the future.