|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |
| **Lab Report** |
| COURSE: Cyber 262  Lab : Two-factor Authentication  Submitted BY: Jack Morgan  Date: 04/25/2022  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 6](#_Toc50470228)

# INTRODUCTION

In this lab, we will be exploring two-factor authentication and how to apply an extra layer of protection to our systems. We will be doing this by generating secret keys then applying this secret key to a downloaded program to generate authentication codes. These codes will in turn allow us to SSH to the ubuntu server after entering the password, hence a second layer of protection on top of the password. Although not as deep as a topic as some of the other labs we have performed, this lab provides more meaning to the idea of two factor authentication rather than just suggesting it during our flash briefings.

# SCREEN CAPTURES

***Figure (1.1):*** *Take a screen shot of your secret key. Note: The secret key will be unique for everyone.*

***The following screen shot shows the generation of our secret key which we will use to generate our authentication code to gain access to the plabubuntu server via ssh.***

Graphical user interface

Description automatically generated

***Question (1.2):*** *Explain the meaning of “Time Skew” and “Rate Limiting”. Be sure to explain what impact they might have on 2FA.*

**Time Skew:** A time skew is used to delay the amount of time between 2 given inputs. This allows us to generate a code for the authentication code and then take the time to attempt an ssh with that code before it automatically generates a new one.

**Rate Limiting:** Rate limiting puts a limitation on the number of requests a user can put in for a specific command or action. This makes it so that if a user attempts to submit multiple requests for an authentication code that multiple won’t generate and create problems for the system.

***Figure (3.1):*** *Take a screen shot of the valid SSH connection.*

***The following screen shot displays the successful ssh connection to the plabubuntu server utilizing putty and the authenticator verification code we generated using the downloaded program.***

Graphical user interface, text

Description automatically generated

***Question (3.2):*** *Explain which tool provides the second factor for authentication in this lab, namely the challenge response.*

After entering in the password for the ubuntu server, we utilized WinAuth to generate an authentication code based on our secret key we generated to confirm we are the user attempting to ssh to the ubuntu server.

***Question (3.3):*** *Explain how the 2FA authenticator can prevent a replay attack. Please be sure to mention the design feature the prevents replay.*

If a user was able to sniff the packets and detect the password a user would use to ssh to the ubuntu server, they would then be denied access without knowledge of an authentication code. This makes it so that an authentication code is required to ssh to the ubuntu server.

# REFLECTION

During this lab, we went through the process of generating secret keys, downloading programs and then generating authentication codes to ssh into specific servers. This was a much simpler lab than the previous ones we performed this year, however it provides a lot of clarity towards the flash briefings as many students stated that 2FA was a key defensive measure without explain how to perform 2FA. As young cyber engineers, it is crucial that we learn 2FA to not only protect our systems and our company’s systems, but to protect ourselves from loss of crucial data.