OVERVIEW:

The overall objective of this lab is to get familiar with phishing and identifying it. Different tools are going to be used to help in that effort, such as URLscan.io & VirusTotal.com. Phishing challenges will then be used to help make us become more aware of phishing.

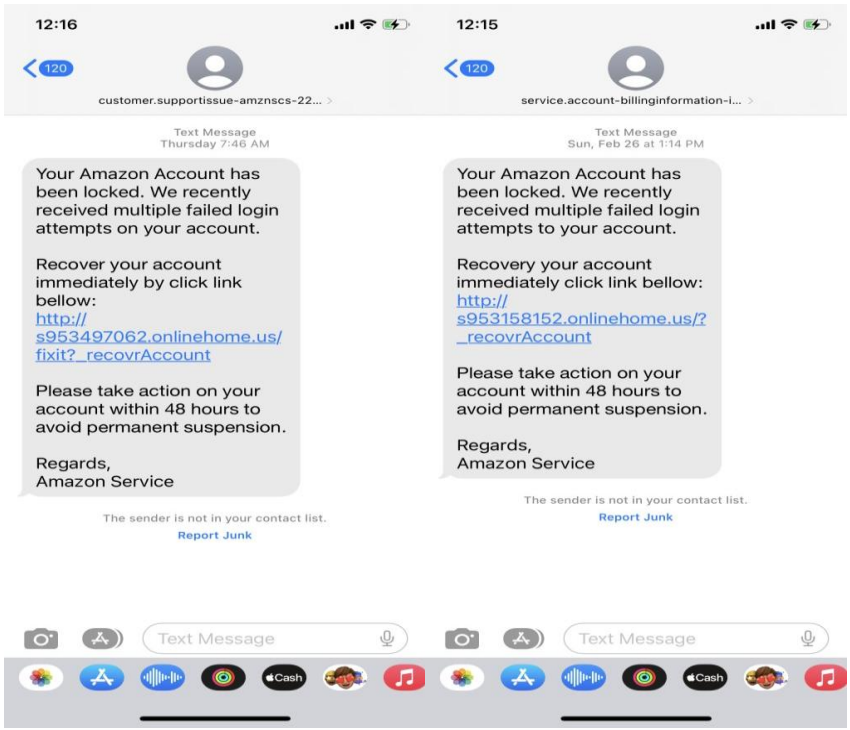
To get a better understanding of Phishing you can visit sites like https://phishingquiz.withgoogle.com/ & https://surfshark.com/blog/phishing-quiz

ANALYSIS:

Task 1: Analyze potential phishing messages

I didn't have any phishing messages in my school email. However, on my phone I get scam messages all the time, so I decided to use one of them.

Here they are:



Obviously, something that should be noted is how they come from random email accounts. The names have keywords like" customer", "support", "account". However, you would never expect an actual email from Amazon to look like that.

Another giveaway that this is a fake email is the emphasis on time and building fear. It states that you must act within 48 hours, or your account will be permanently suspended.

Notice how the links are nothing like a like you would expect from amazon. In fact, Amazon isn't even included in any of the links. It is obvious that it would not redirect you to Amazon.

Both these emails are basically the same cookie cutter format. Clearly spam. If you were to read through them, you would also notice the terrible English writing skills. I would expect a company like Amazon to have customer support that could form basic English sentences not "recover your account immediately by click link bellow"

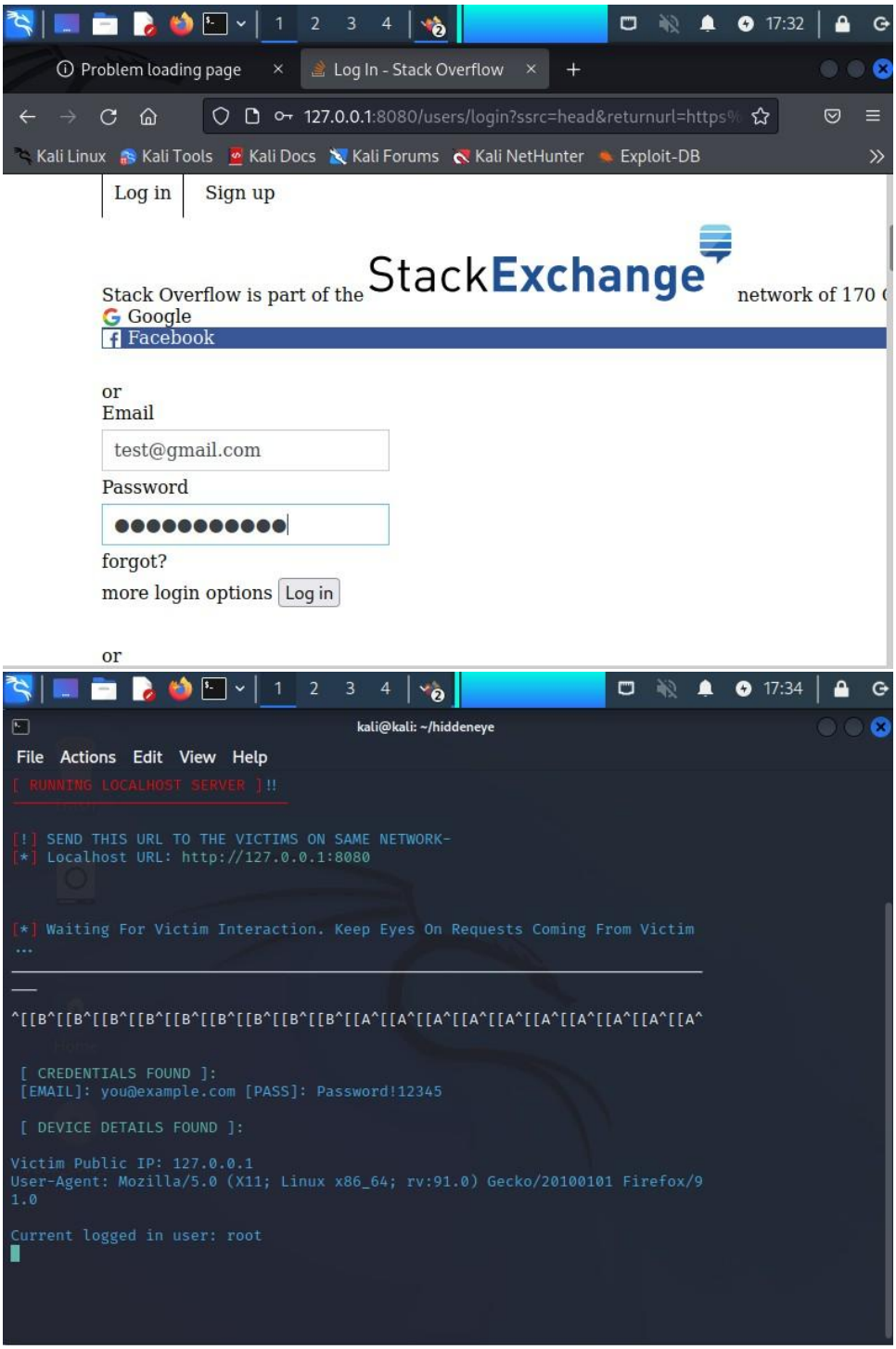
If you were to inspect the link and the sender further you would most likely find that they came from outside the United States.

Task 2: Creating and understanding a phishing campaign

A phishing campaign was created and analyzed using a Kali Linux VM. The HiddenEye tool was installed and configured to demonstrate how attackers can deploy phishing techniques to harvest credentials. This hands-on exercise provided insight into phishing methodologies, highlighting the importance of security awareness and defensive measures.

A KALI VM was used for task 2. The following code was used in the terminal.

- git clone https://gitlab.com/An0nUD4Y/hiddeneye.git
- sudo apt update
  sudo apt install python3-pip
- cd hiddeneye
  sudo pip3 install -r requirements.txt
- sudo python3 HiddenEye.py



This screenshot displays the credentials obtained using HiddenEye during the phishing campaign simulation. It demonstrates how attackers can extract sensitive information, emphasizing the importance of cybersecurity awareness and preventive measures to mitigate phishing threats.