TASK 2
PHISHING EMAIL ANALYSIS

Date:24-06-25

Phishing is a common form of cyberattack where attackers impersonate trusted organizations to trick users into revealing sensitive information such as passwords, financial data, or personal details.

In this task, a suspicious email claiming to be from a bank was analyzed to identify key phishing indicators such as spoofed email addresses, misleading links, urgent language, and social engineering tactics. The objective was to understand how phishing emails work and how to detect them effectively.

From: First Generic Bank <accounts@firstgenericbank.com>
Subject: Please update your account information
Date: Sep 12, 2006 3:23 PM PST

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit http://www.firstgenericbank.com.account-updateinfo.com.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

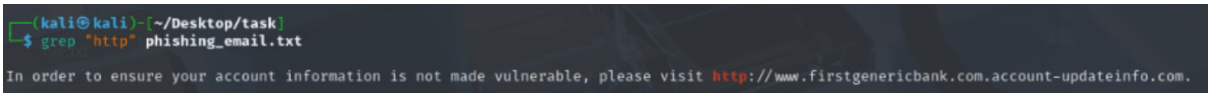
First Generic Bank

This is the phishing email that is analyzed. The email is analysed in Kali linux.
First create a file and add the text in this email to that phishing _email file.

1)Analysis the from address: using grep command to retrieve only from part of the gmail for easier analysis >grep -i ‘FROM:’ phishing_email.txt

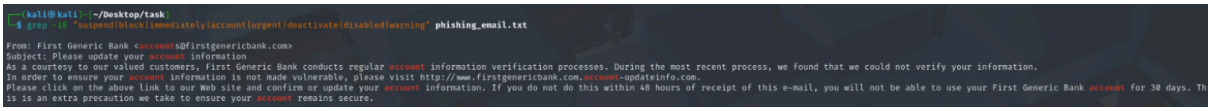
From: accounts@firstgenericbank.com
Issue: Appears legitimate but can be easily spoofed.
No SPF, DKIM, or DMARC verification detected.

2) See if there are any suspicious links:
Using >grep -i ‘http’ phishing_email.txt



Link Displayed:http://www.firstgenericbank.com.account-updateinfo.com
Actual Domain: ‘account-updateinfo.com’ is the domain name they using the bank name as the subdomain name.The real domain is unrelated to the actual bank and likely used for phishing.

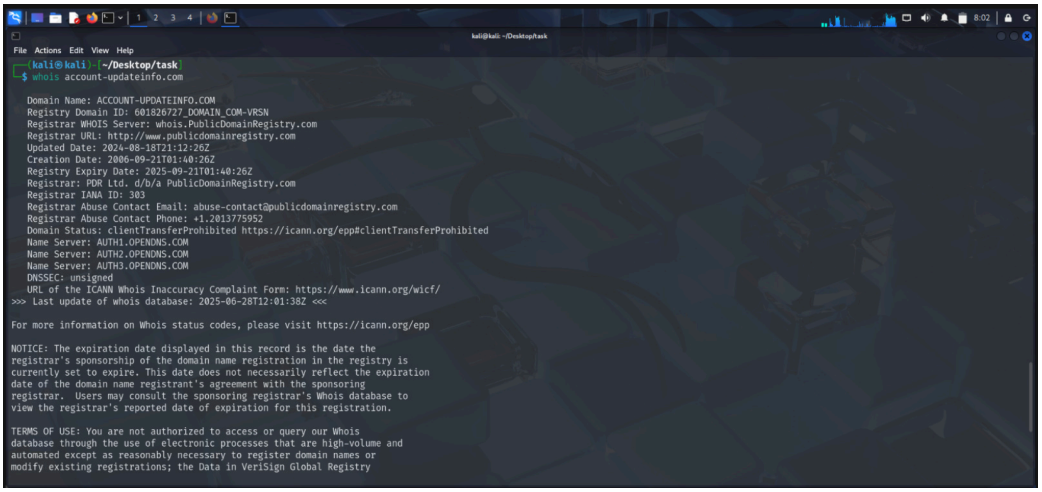
3) Any suspicious or urgent words:
Using > grep -iE ‘suspend|Block|immediately|account|urgent|deactivate|disabled|warning’ phishing_email.txt



output:There are many such urgent words that are present in the email. So should be careful It may be a phishing email.

There are many reasons above to prove the email is a phishing email.
But for further analysis we can also analyse the whois information of the domain.

4) Whois analysis:
Can be done using > whois account-updateinfo.com



This how we can simply,manually and easily verify if the email is a phishing email or not.
But nowadays the companies use firewalls,IDS and other complicated systems integrated with AI to check phishing emails.