Project Report

Email Phishing Simulation

By- Abhinav Lather

->What is a Phishing attack?

- Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine. Phishing is a common type of cyber attack that everyone should learn about in order to protect themselves.
- A phisher may use public resources, especially social networks, to collect background information about the personal and work experience of their victim. These sources are used to gather information such as the potential victim's name, job title, and email address, as well as interests and activities. The phisher can then use this information to create a reliable fake message.

Protection Steps

User education

One way to protect your organization from phishing is user education. Education should involve all employees. High-level executives are often a target. Teach them how to recognize a phishing email and what to do when they receive one. Simulation exercises are also key for assessing how your employees react to a staged phishing attack.

Security technology

No single cybersecurity technology can prevent phishing attacks. Instead, organizations must take a layered approach to reduce the number of attacks and lessen their impact when they do occur. Network security technologies that should be implemented include email and web security, malware protection, user behavior monitoring, and access control.

Tools Used

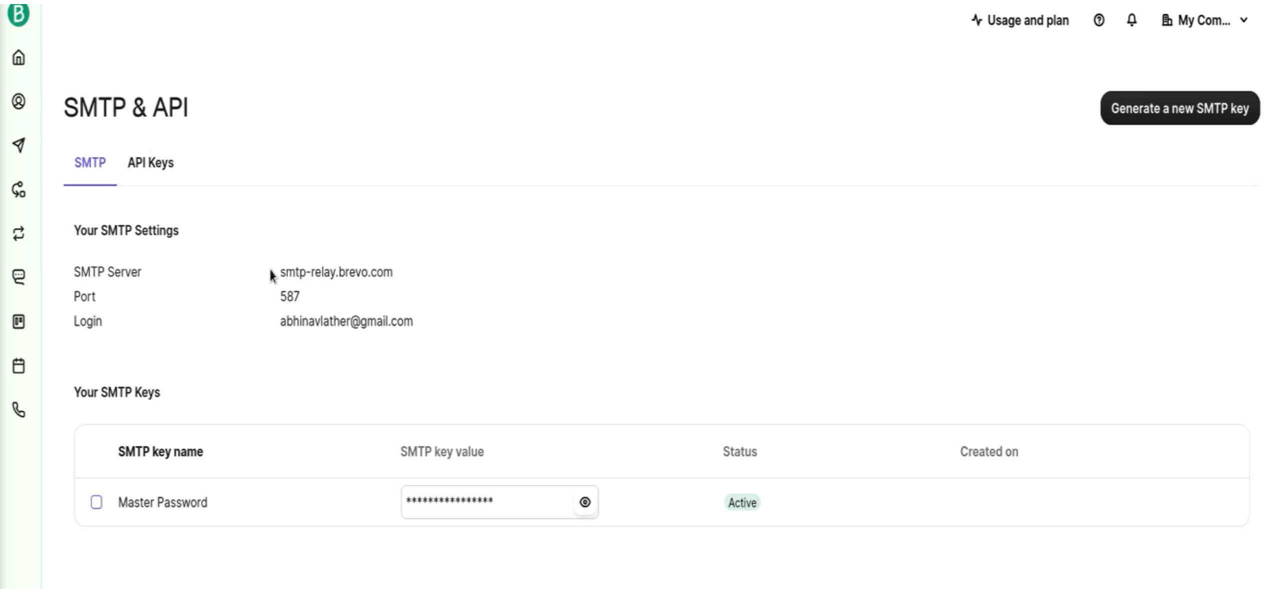
1.Brevo:-

- Also known as sendinblue(former name) Brevo is an online platform which provides the user with an SMTP serer and a port number.
- The server and port number helps to send any email with a different username which looks authentic.
- The body of the email can contain a message which tends the receiver to open an real looking link which is fake and can cause harm to the person in some way.

2.Sendemail:-

- It is an inbuilt tool in Kali Linux OS which takes user email,username to be used,and the body of email containing the link.
- It contains the receiver's email address where the mail is to be sent.
- When the fake link gets clicked,it takes the receiver to a fake website or can install any kind of malware on the system causing harm.

Screenshots



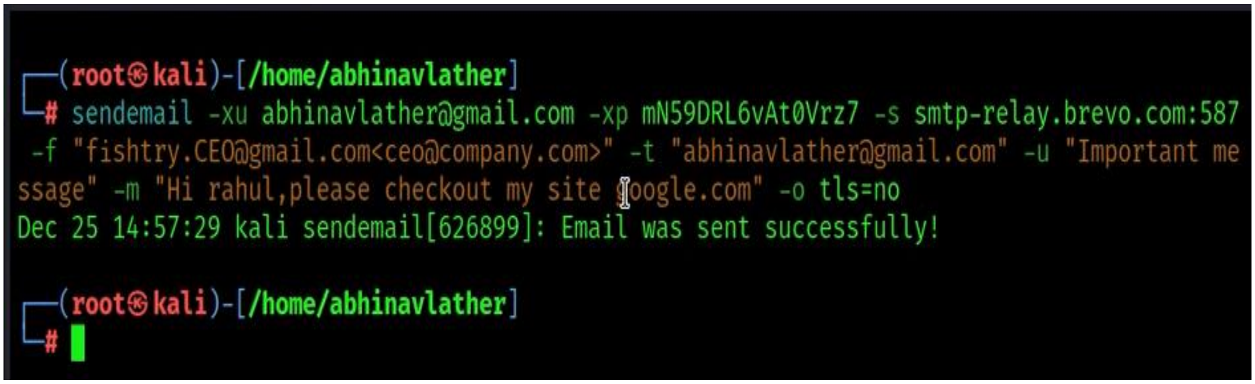
SMTP & API

Your SMTP Settings

SMTP Server	smtp-relay.brevo.com
Port	587
Login	abhinavlather@gmail.com

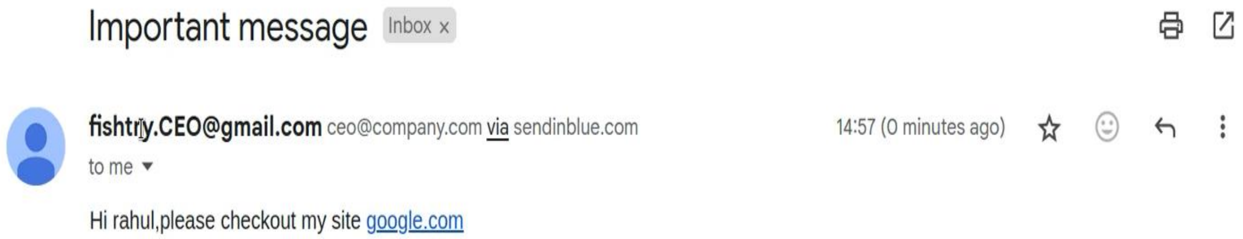
Your SMTP Keys

	SMTP key name	SMTP key value	Status	Created on
□	Master Password	****************	Active	



```
┌──(root㉿kali)-[/home/abhinavlather]
└─# sendemail -xu abhinavlather@gmail.com -xp mN59DRL6vAt0Vrz7 -s smtp-relay.brevo.com:587
 -f "fishtry.CEO@gmail.com<ceo@company.com>" -t "abhinavlather@gmail.com" -u "Important me
ssage" -m "Hi rahul,please checkout my site google.com" -o tls=no
Dec 25 14:57:29 kali sendemail[626899]: Email was sent successfully!

┌──(root㉿kali)-[/home/abhinavlather]
└─# 
```



Important message

fishtry.CEO@gmail.com ceo@company.com via sendinblue.com 14:57 (0 minutes ago)

to me ▾

Hi rahul,please checkout my site google.com