

Analyzing Phishing Techniques That
Bypass Spam Detection
Cybersecurity, Email Security

CDAC, Noida
CYBER GYAN VIRTUAL INTERNSHIP
PROGRAM

Submitted By:

Dinesh Pradhan

Project Trainee, (May-June) 2024

BONAFIDE CERTIFICATE

This is to certify that this project report entitled “Analyzing Phishing Techniques That Bypass Spam Detection” submitted to CDAC Noida, is a Bonafede record of work done by “Dinesh Pradhan” under my supervision from 15-05-2024 to 25-06-2024.

HEAD OF THE DEPARTMENT

SUPERVISOR

Declaration by Author

This is to declare that this report has been written by me/us. No part of the report is plagiarized from other sources. All information included from other sources have been duly acknowledged. I/We aver that if any part of the report is found to be plagiarized, I/we are shall take full responsibility for it.

Name of Author: Dinesh Pradhan

TABLE OF CONTENTS

1. Introduction
 1. Problem Statement
2. Learning Objective
 1. How Phishing works
 2. Type of Phishing
 - i. Spear Phishing
 - ii. Email/spam Phishing
 - iii. Link Manipulation
 - iv. Malvertising
 - v. Vishing (Voice Phishing)
 - vi. Smishing (SMS Phishing)
 - vii. Ransomware
3. Approach
 1. Tools and Technology used
 2. Infrastructure Overview
 3. Api Integration
4. Implementation
 1. Environment Setup
 - i. Install VirtualBox and Kali Linux VM
 2. Tools installation and configuration
 - i. Gophish
 - ii. Black-eye
 - iii. Spamassassin
 - iv. Rspamd
 - v. Mutt
 3. Execution
 - i. Using Gophish
 4. Analyzing and detecting phishing mail and content
 - i. Spamassassin
 - ii. Scanning using API's
 1. Phishtank
 2. VirusTotal
 3. Zerobounce
 5. How phishing technique bypass spam-filter
5. Conclusion and Recommendation
6. References

Acknowledgement

I am deeply appreciative of the efforts of all the individuals and organizations that have assisted in the successful completion of this project, which focused on the analysis of phishing techniques that circumvent spam detection processes.

In the first place, I would like to express my gratitude to Ms. Kajal Kashyap, our project supervisor, for her invaluable guidance, support, and encouragement during the course of this research. The direction and depth of this investigation have been significantly influenced by her insights and expertise.

I am also appreciative of the Centre for Development of Advanced Computing (CDAC), Noida, for granting me access to critical datasets and instruments. These resources were essential for the execution of thorough analyses and evaluations.

I am grateful for the collective support and contributions.

Analysing Phishing Techniques That Bypass Spam Detection

1. Introduction:

Phishing is a type of cyber-attack in which an attacker impersonates a legitimate entity to deceive an individual into providing sensitive information like personal data like username, password, financial details etc. This attack is carried out by contacting the target by emails, telephone, text messages or fake websites. The primary goal of the attacker is to steal the personal information of the individual, commit fraud, installing malicious software in the victim's machine.



1. Problem Statement:

Phishing attacks have become increasingly sophisticated, leveraging various techniques to bypass traditional spam detection mechanisms. These attacks often involve deceptive tactics that trick users into divulging sensitive information such as usernames, passwords, and financial details. Despite the advancements in spam detection technology, phishers continuously evolve their methods to evade these defences.

One of the primary challenges is that traditional spam filters rely on heuristic rules and pattern recognition to identify and block phishing emails. However, phishers use techniques such as URL obfuscation, domain spoofing, and polymorphic phishing kits to create emails that appear legitimate to both users and automated detection systems. Additionally, the use of social engineering tactics further complicates the identification and prevention of phishing attempts.

Understanding the techniques that phishers employ to bypass spam detection is crucial for several reasons:

- i. **Improving Detection Mechanisms:** By analysing the methods used by phishers, security professionals can develop more effective detection algorithms and update spam filters to recognize and block these advanced threats.

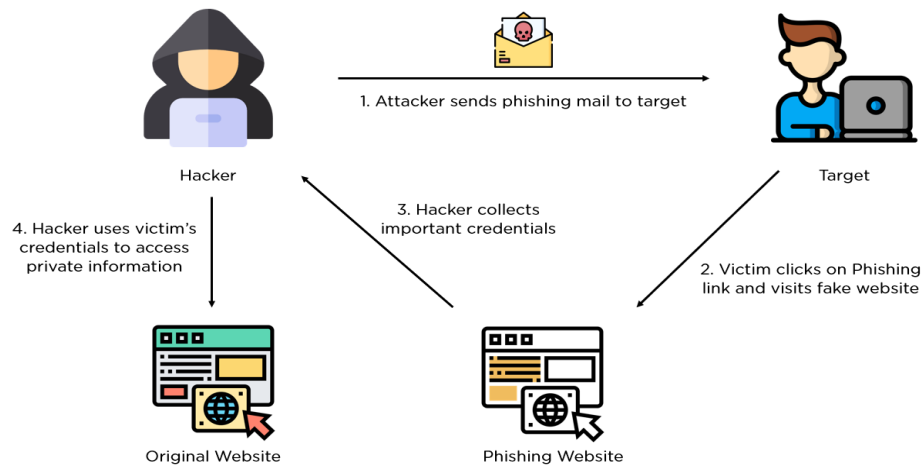
- ii. **Enhancing Cybersecurity Measures:** Knowledge of these techniques allows organizations to implement stronger cybersecurity practices and educate users about the latest phishing tactics, reducing the likelihood of successful attacks.
- iii. **Mitigating Risks:** As phishing attacks often serve as entry points for larger security breaches, understanding and countering these threats can significantly mitigate the risks associated with data breaches, financial losses, and reputational damage.

This project aims to analyse the latest phishing techniques that bypass spam detection systems, providing insights into their mechanisms and suggesting countermeasures to enhance cybersecurity defences.

2. Learning objective:

Let's first learn about how phishing works:

In this cyber attack the attacker impersonates as some authenticate or trusted entity to fool an individual.

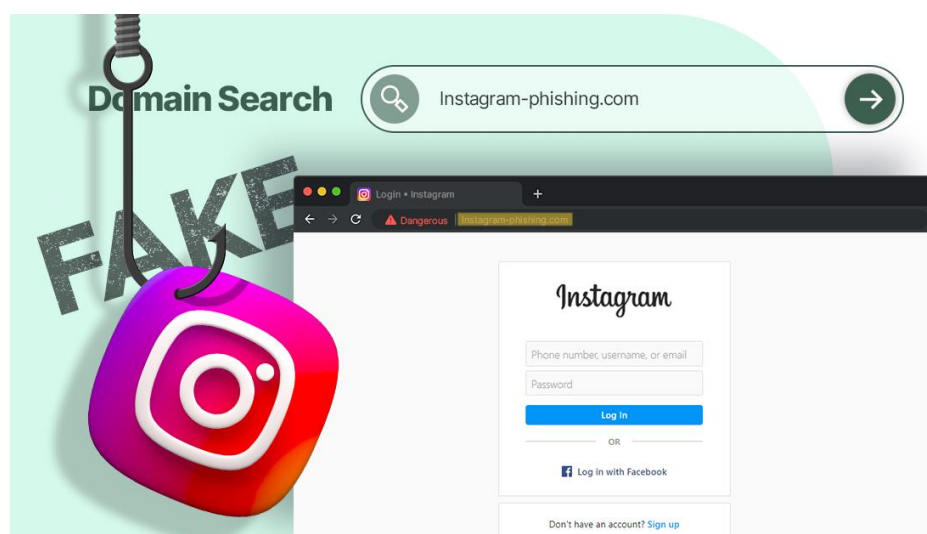


In the above picture it demonstrated clearly how phishing works:

- First the attacker sends some sort of email or SMS or via many techniques to fool an individual.

Like they use some sort of advertisement links or security threats or may be some loan related or banking related issue.

- Then the individual sees the message and click the link which direct the user into different website which acts as a phishing website (Basically a website made by attacker). which looks similar to some popular websites like Instagram or Facebook etc.



In the above picture you can see clearly the webpage is similar to Instagram login page but the URL is not original (instagram.com) that is (Instagram-phishing.com).

- Then the target uses his credential to login, at the same time the credential directly reaches to the attacker.
- And the attacker makes the website like when you login in the phishing website you will be directed to original website.

And the user can't notice it he thinks like he entered the password wrong.

- At last Attacker uses the credential to access private information of the target.

Then!



The main motive behind this project to understand different type of phishing techniques and analyse them.

Now let's dive into different type of phishing technique though technical aspects:

1. Spear Phishing:

In this phishing technique instead of mass mail, the attacker targets a single person, which has a highest authority in an organization. They do more research on a target in order to make attack more personalized and to increase the probability of falling the target into the trap.

Spear Phishing works in four steps:

- i. Setting an objective
- ii. Choosing a target
- iii. Researching on target
- iv. Crafting and sending a phishing email

Now let's look into these steps:

(i) Setting an objective:

The attacker would have many possible numbers of objective like spreading malware, stealing credential, stealing sensitive information etc.

(ii) Choosing a target:

Spear phishers choose targets who can provide access to desired resources either directly, by making payments, or indirectly, by downloading spyware. They often target midlevel, low-level, or new employees with elevated privileges, as these individuals may be less diligent in following policies and more susceptible to pressure tactics. Common victims include financial managers, IT administrators, and HR managers with access to sensitive data.

(iii) **Researching on target:**

Attackers research their targets to impersonate trusted sources like friends, colleagues, or bosses. The abundance of personal information shared online makes this relatively easy, enabling hackers to craft convincing spear phishing emails with minimal effort. Some hackers go further by breaking into company email accounts or messaging apps to observe their targets and gather more detailed information.

(iv) **Crafting and sending phishing email:**

Using their research, spear phishers craft targeted messages that seem highly credible. These messages include personal and professional details that the target believes only a trusted source would know.

For instance, consider Jack, an accounts payable manager at ABC Industries. An attacker can find Jack's job title, responsibilities, company email address, boss's name and title, and business partners' names and titles through his public LinkedIn profile.

Using this information, the attacker sends a convincing email that appears to come from Jack's boss:

Hi Jack,

I know you handle invoices from XYZ Systems. They informed me they're updating their payment process and need future payments sent to a new bank account. Here's their latest invoice with the new account details. Can you process the payment today?

The attached invoice is fake, and the "new bank account" belongs to the attacker. When Jack makes the payment, he transfers the money directly to the fraudster.

A phishing email usually includes visual elements to enhance its authenticity, such as a spoofed email address showing Jack's boss's display name while hiding the fraudulent sender's address. The attacker might also CC a spoofed coworker's email and include a signature with the ABC Industries company logo.

A skilled fraudster might even hack into Jack's boss's actual email account and send the message from there, leaving Jack no reason to be suspicious.

Some attackers use hybrid spear phishing tactics, combining phishing emails with text messages (SMS phishing or smishing) or phone calls (voice phishing or vishing). For example, instead of attaching a fake invoice, the email might instruct Jack to call XYZ Systems' accounts payable department at a phone number controlled by the fraudster.

2. Email/Spam Phishing

Using the most common phishing technique, attackers send the same email to millions of people, asking them to provide personal information. These emails usually create a sense of urgency, telling people to enter their account details to update information, change settings, or verify their accounts. Sometimes, the email might include a link to a fake form for accessing a new service. The information collected is then used by the attackers for illegal activities.

3. Link Manipulation

Link manipulation is a trick used by scammers where they send you a link that looks like it's going to a safe, familiar website. However, when you click on it, the link actually takes you to a fake website designed to steal your personal information.

How It Works:

- **The Deceptive Link:** You receive an email or message with a link that appears to lead to a trusted site, like your bank or a popular online store.
- **The Fake Website:** When you click on the link, instead of going to the real site, it takes you to a fake site that looks almost identical to the real one.
- **Stealing Information:** On the fake site, you might be asked to log in or provide personal details, which the scammers then steal.

4. Malvertising

Malvertising, short for "malicious advertising," involves harmful ads that can infect your computer. These ads look like normal advertisements on websites, but they contain hidden code designed to do bad things, like downloading viruses or showing unwanted content on your computer.

How It Works:

- **Malicious Ads:** You visit a website and see regular-looking ads.
- **Hidden Threats:** Some of these ads have hidden scripts, which are small pieces of code that can automatically download harmful software (malware) onto your computer without you knowing.
- **Common Exploits:** These malicious ads often exploit security weaknesses in software like Adobe PDF Reader and Flash Player to infect your computer.

5. Vishing(voice phishing)

Phone phishing, also known as vishing, involves scammers making phone calls to trick you into giving away personal information, often related to your bank account. These calls can seem very convincing because the scammers use fake caller IDs to make it look like they are calling from a legitimate organization, such as your bank.

How It Works:

- **The Fake Call:** You receive a call that appears to be from a trusted source, like your bank or a government agency.
- **The Trick:** The scammer on the other end might tell you there's an urgent problem with your account and ask you to call another number or provide personal information right away.
- **Information Theft:** Once you provide your details, the scammer uses them to steal money or commit fraud.

Why It's a Growing Concern:

- **Increased Sophistication:** Scammers are getting better at making these calls sound legitimate, using detailed scripts and fake caller IDs.
- **Widespread Impact:** More people are falling victim to these scams, leading to significant financial losses and personal distress.

6. Smishing(SMS phishing)

Smishing, or SMS phishing, is a scam where attackers use text messages to trick you into revealing personal information. These text messages often appear to be from a legitimate source and contain links that lead to fake websites designed to steal your information.

How It Works:

- **Deceptive Text Message:** You receive a text message that looks like it's from a trusted entity, such as your bank, a delivery service, or even a government agency.
- **Enticing Link:** The message might claim there's an urgent issue, such as a problem with your account or a package delivery, and ask you to click on a link to resolve it.
- **Phishing Website:** Clicking the link takes you to a fake website that looks real. The site asks you to enter personal details, like your login credentials or credit card number.

7. Ransomware

Ransomware is a type of malicious software that locks you out of your computer or encrypts your files, making them inaccessible until you pay a ransom to the attacker. This malware often gets installed through tricks that deceive you into clicking on a link, opening an email attachment, or interacting with a malicious advertisement.

How It Works:

- **Social Engineering Attack:** You might receive an email or see an ad that looks legitimate and prompts you to click on a link or download an attachment.
- **Infection:** Once you click the link or open the attachment, the ransomware installs itself on your computer.
- **Lockout or Encryption:** The ransomware then locks your entire computer or encrypts important files, rendering them unusable.
- **Ransom Demand:** A message appears demanding payment (usually in cryptocurrency) to unlock your computer or decrypt your files.

Why It's a Serious Threat:

- **Data Loss:** You can lose access to important documents, photos, and other files.
- **Financial Impact:** Paying the ransom doesn't guarantee that you'll get your files back, and it encourages attackers to continue their activities.
- **Operational Disruption:** For businesses, ransomware can cause significant downtime and disrupt operations.

3. Approach:

Tools and Technologies Used:

To analyze phishing techniques and their evasion of spam detection mechanisms, the following tools and technologies were utilized:

1. **Virtualization Platform:**
 - **VirtualBox:** Used to host Kali Linux as the operating system for testing and running various security tools.
2. **Operating System:**
 - **Kali Linux:** Chosen for its pre-installed penetration testing tools and security features.
3. **Phishing Campaign Tool:**
 - **GoPhish:** Utilized for creating and executing phishing campaigns to simulate real-world attacks.
 - **Ngrok:** Used for tunneling local servers to the internet to simulate phishing sites.
4. **Phishing Tools:**
 - **BlackEye:** Employed for creating convincing phishing pages that mimic legitimate websites to deceive victims.
5. **APIs Used:**
 - **Phishtank API:** Integrated to fetch and analyze phishing URLs reported by the community.
 - **VirusTotal API:** Utilized for scanning and analyzing suspicious files and URLs for malware and phishing indicators.
 - **ZeroBand API:** Leveraged for threat intelligence and to enhance phishing detection capabilities.
6. **Spam Detection Tool:**
 - **SpamAssassin:** Configured to filter and detect spam and phishing emails based on a set of rules and heuristics.
7. **Network Security Tool:**
 - **Rspamd:** Used for scanning and filtering emails for spam, phishing attempts, and other malicious content.
8. **Email Client:**
 - **Mutt:** Command-line email client used to read and analyze email content received during phishing simulations.

Infrastructure Overview:

The project was implemented on a local development environment using VirtualBox with Kali Linux as the primary operating system. The infrastructure setup includes:

- **Kali Linux Virtual Machine:** Hosted on VirtualBox, serving as the platform for running security tools and conducting phishing simulations.
- **Phishing Campaign Configuration:**

- **GoPhish with Ngrok:** Deployed to create and launch phishing campaigns. Ngrok was used to expose local GoPhish instances to the internet for realistic testing.
- **BlackEye:** Used to clone legitimate websites and create deceptive phishing pages for the campaigns.
- **Email Analysis and Security Tools:**
 - **SpamAssassin:** Configured on the email server to analyze incoming emails for spam and phishing indicators.
 - **Rspamd:** Implemented to complement SpamAssassin by providing additional email scanning and filtering capabilities.
 -

API Integration:

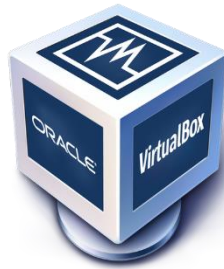
- **Phishtank API:** Used to retrieve real-time phishing URLs reported by the community and cross-check them during the phishing campaign analysis.
- **VirusTotal API:** Integrated for scanning URLs and files for malware and phishing threats, enhancing the detection capabilities of the project.
- **ZeroBand API:** Leveraged to access threat intelligence data, further improving the identification and mitigation of phishing attempts.

4. Implementation:

1. Environmental setup:

Install VirtualBox and Kali Linux VM:

- Used Oracle virtual box ([VirtualBox 7.0.18](#))

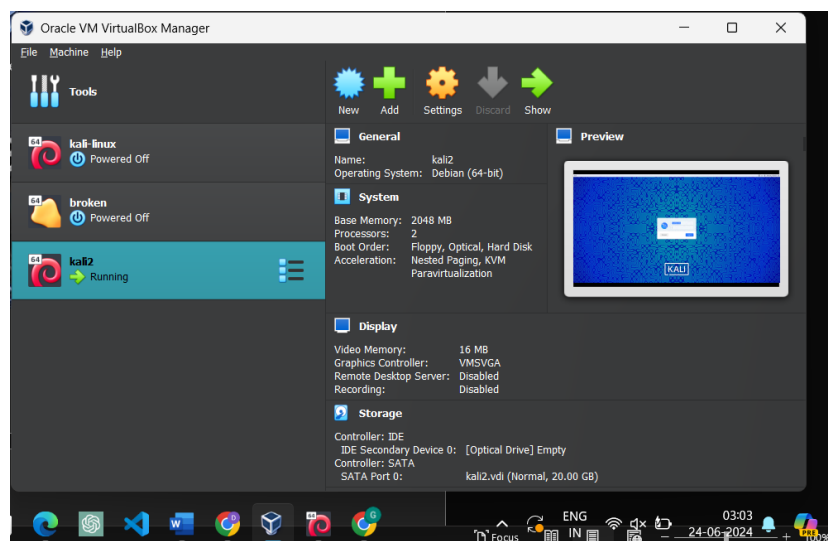


- Kali Linux image used ([Iso image](#))



You can see installation guide online.

And it should look like this:



2. Tool installation and configuration:

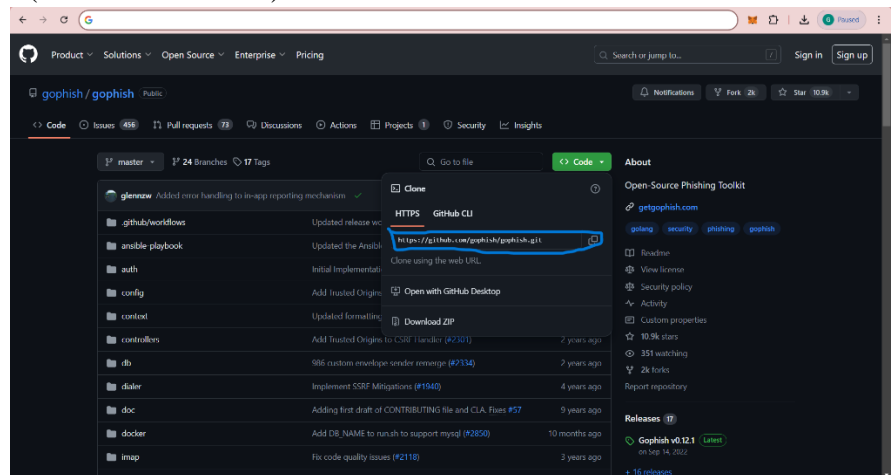
First, we will install all the necessary tools and configure them.

i. Install GoPhish and Ngrok:

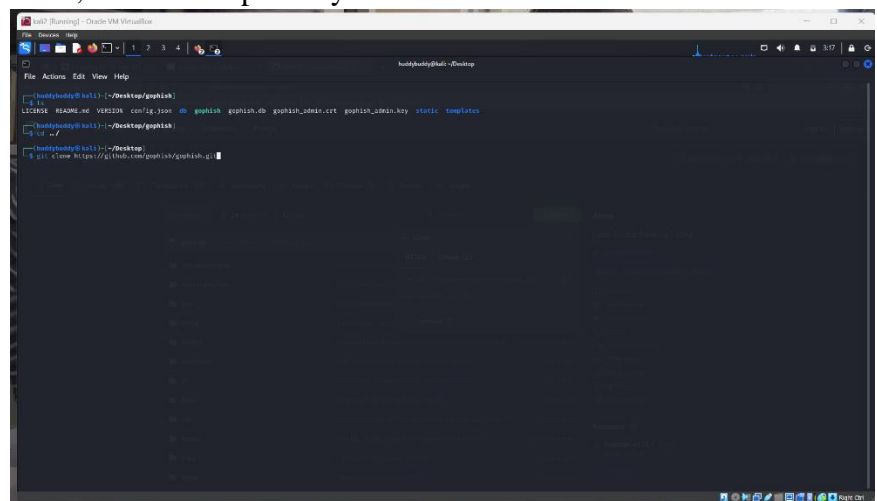
Here we use gophish for phishing campaign and ngrok for tunnelling of network .

- Let's first install gophish.

Go to [Gophish](https://github.com/gophish/gophish) and copy the repo. url for cloning the repository . (below mention url)



- Then, clone the repository.



- Repo. Has been cloned. Change directory to gophish.
\$cd gophish
- Then inside the directory there is a gophish file you will find a file name “gophish”. Then, make the gophish file executable if it is not .
\$chmod +x gophish
- Run the file by **./gophish**

- Go to browser and go to mentioned url there .

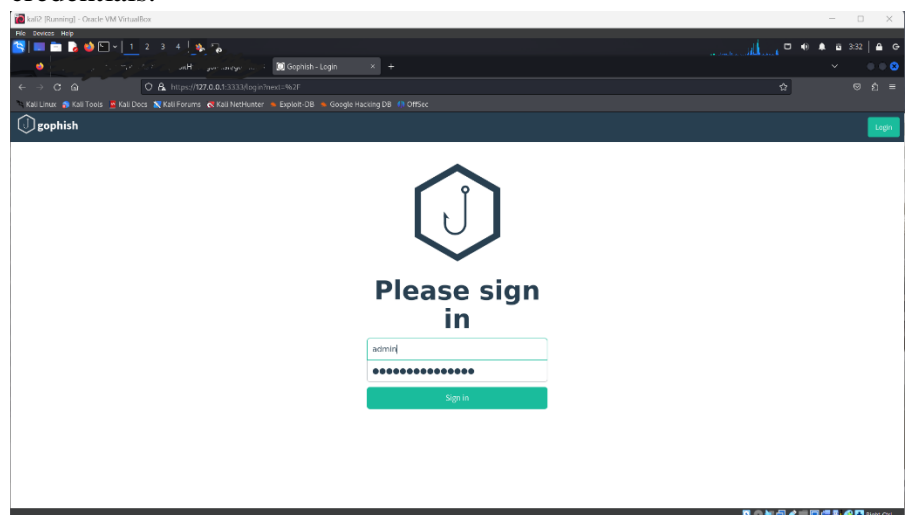
```

root@kali:~# ./gopish
time="2024-06-24T03:21:45Z" level=warning msg="No contact address has been configured."
time="2024-06-24T03:21:45Z" level=warning msg="Please consider adding a contact_address entry in your config.json"
goos: go migration: go env: current version: go2.1.12345
time="2024-06-24T03:21:45Z" level=info msg="Starting admin server at https://227.0.0.1:2222"
time="2024-06-24T03:21:45Z" level=info msg="Backup server started at https://227.0.0.1:2223"
time="2024-06-24T03:21:45Z" level=info msg="Starting IMAP monitor Manager"
time="2024-06-24T03:21:45Z" level=info msg="Starting IMAP monitor for user admin"
time="2024-06-24T03:21:45Z" level=info msg="Starting phishing server at http://0.0.0.0:80"

```

if it is your first time then most probably it will give you username and password for login .

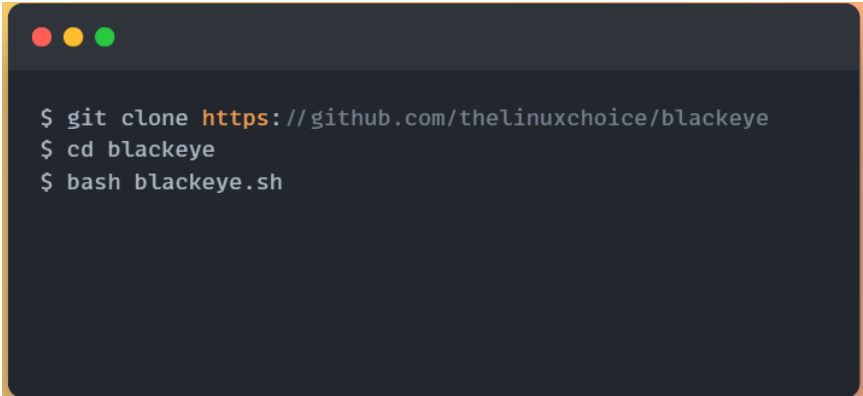
- This should be you next interface and login with you credentials.



- Now you are set with gopish setup.
- Now jump into tunnelling part, we will install ngrok(ngrok combines your reverse proxy, firewall, API gateway, and global load balancing to deliver apps and APIs.)
- Follow this installation guide([ngrok](#)) to install and configure ngrok on your system.

ii. Install Blackeye:

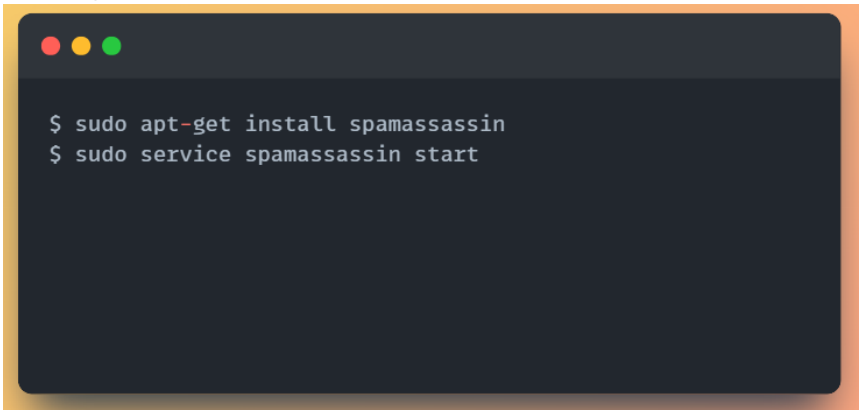
Install blackeye by following command and configure it,

A terminal window with a dark background and three colored window control buttons (red, yellow, green) in the top-left corner. It contains three lines of text: a git clone command, a cd command, and a bash command.

```
$ git clone https://github.com/thelinuxchoice/blackeye  
$ cd blackeye  
$ bash blackeye.sh
```

iii. Install and configure Spamassassin:

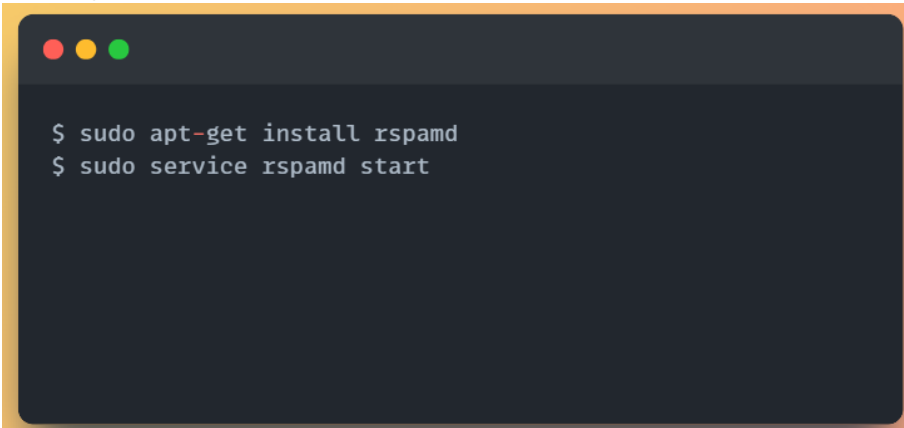
Configuration:

A terminal window with a dark background and three colored window control buttons (red, yellow, green) in the top-left corner. It contains two lines of text: a command to install spamassassin and a command to start the service.

```
$ sudo apt-get install spamassassin  
$ sudo service spamassassin start
```

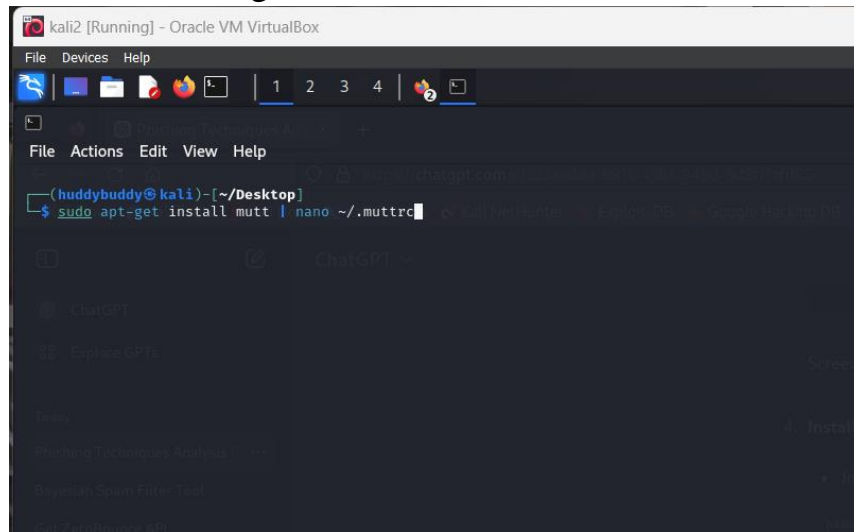
iv. Install and configure Rspamd:

Configuration:

A terminal window with a dark background and three colored window control buttons (red, yellow, green) in the top-left corner. It contains two lines of text: a command to install rspamd and a command to start the service.

```
$ sudo apt-get install rspamd  
$ sudo service rspamd start
```

v. Install and configure Mutt:



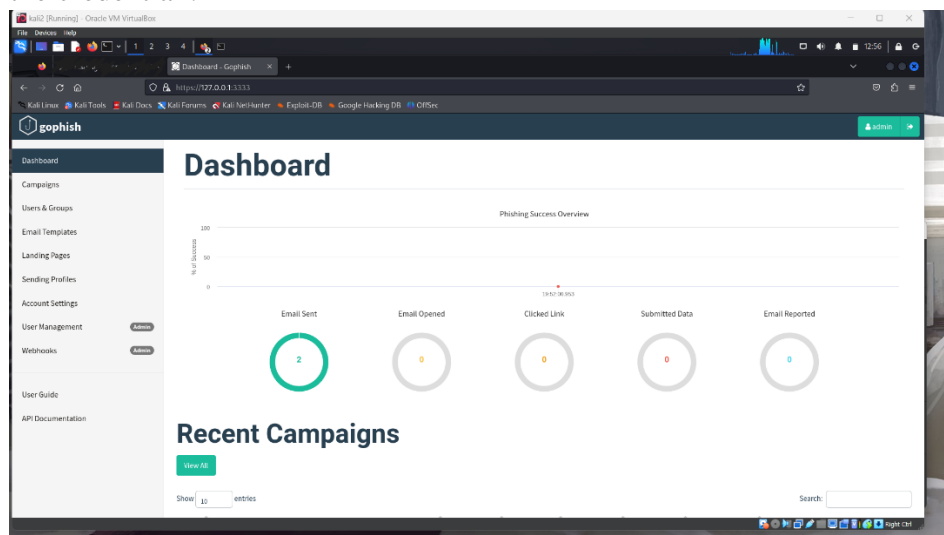
Go to ~/.muttrc to configure you email for reading email in terminal it self and it make it easier to copy the email content for spam detection .

3. Execution

Now lets' dive into phishing campaign part.

i. Using gophish

First go to the url mentioned when you run ./gophish and login using the credential .

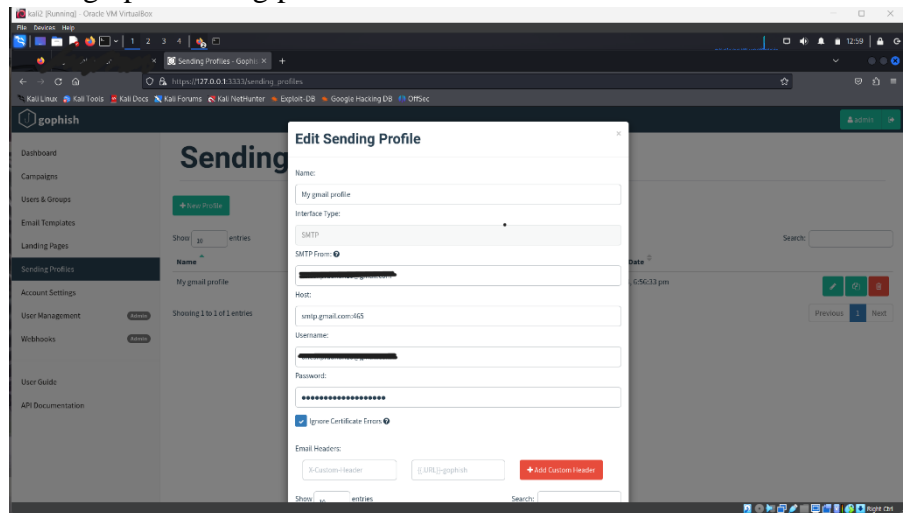


Then you will get an interface like this above.

(Don't try this without permission of a target authority)

Then follow these steps to start campaign:

Step1: Setting up a sending profile.



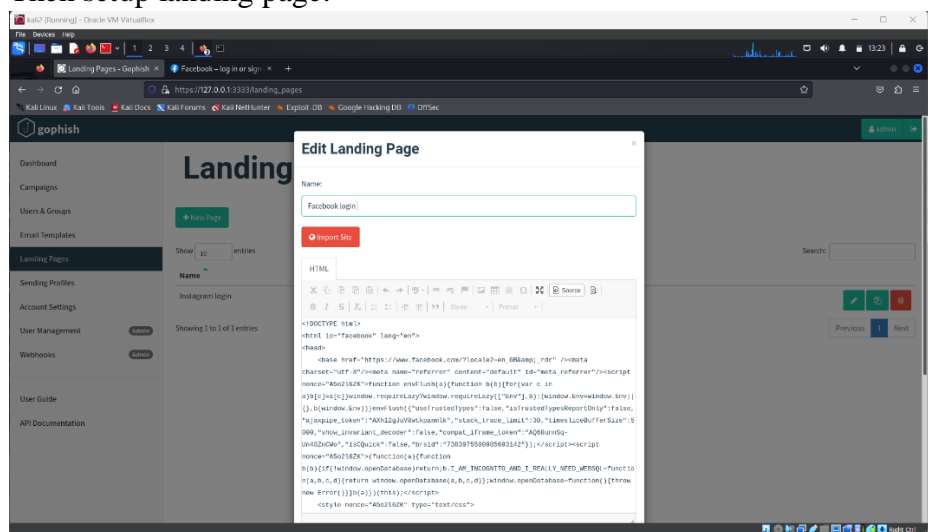
Fill the details about the sending profile.

NOTE:

- Host should be smtp.gmail.com:465
- And smtp from is the entity who is sending mail.
- Password should be not you email login password it should be app generated pass from google account. (google to find about app generated password)

Then save profile.

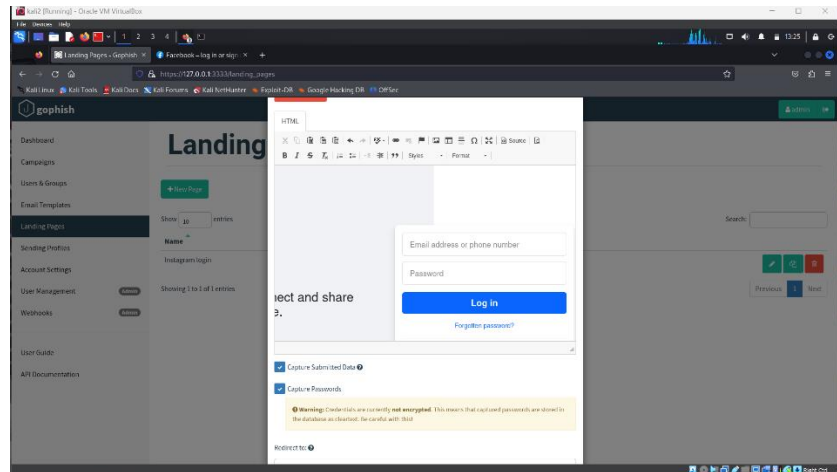
Step2: Then setup landing page.



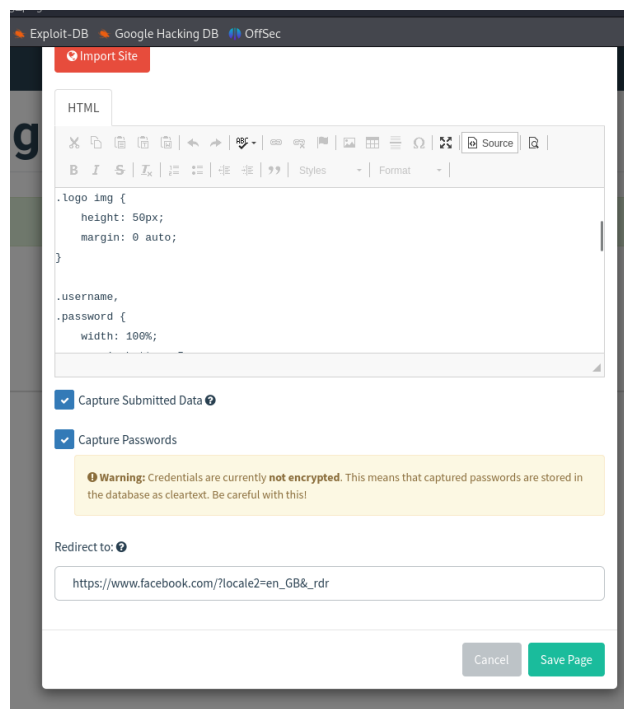
I have setup an facebook landing page.

NOTE:

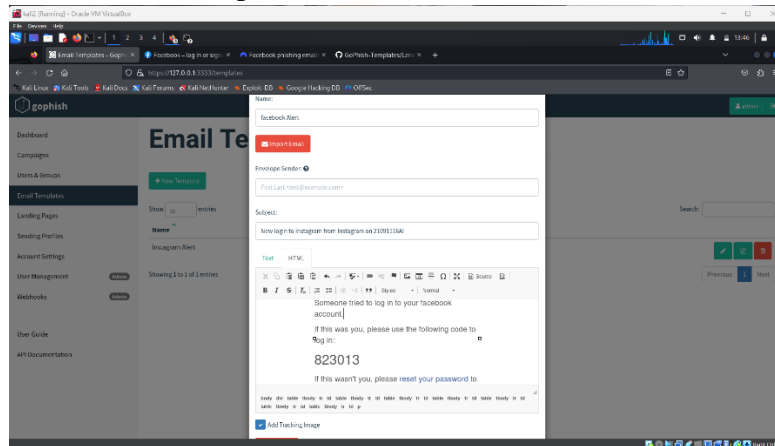
- You can see how your landing page looks like by clicking on source.
- Tick the boxes down below which will enable to capture the credential entered in websites.



And then give a landing page when credential is acquired,



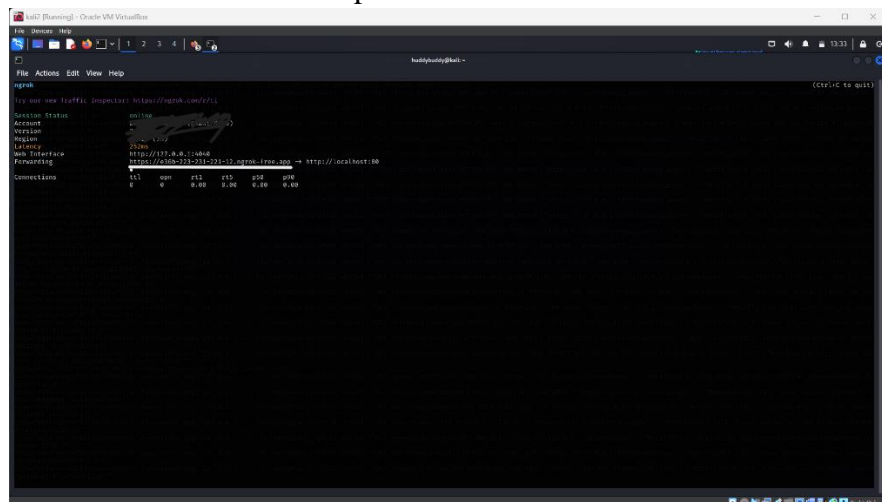
Step3:
Add an email template.



Step4:
Setup a tunnel using ngrok, for directing someone to above Facebook page.

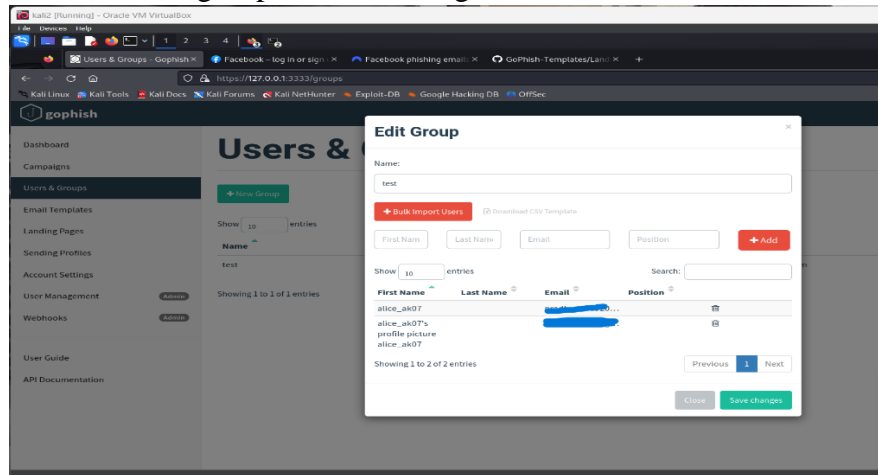
Use command , \$ ngrok http 80

Then below window will open. Below underlined



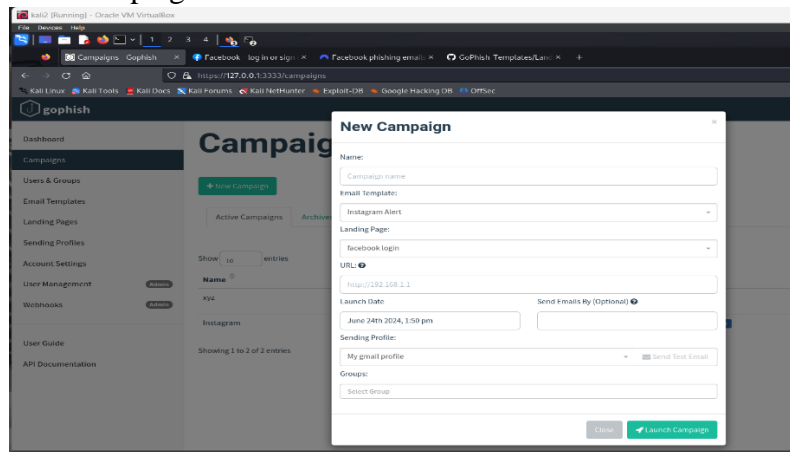
Step5:

Create user or group of users to target.



Step6:

Start campaign:

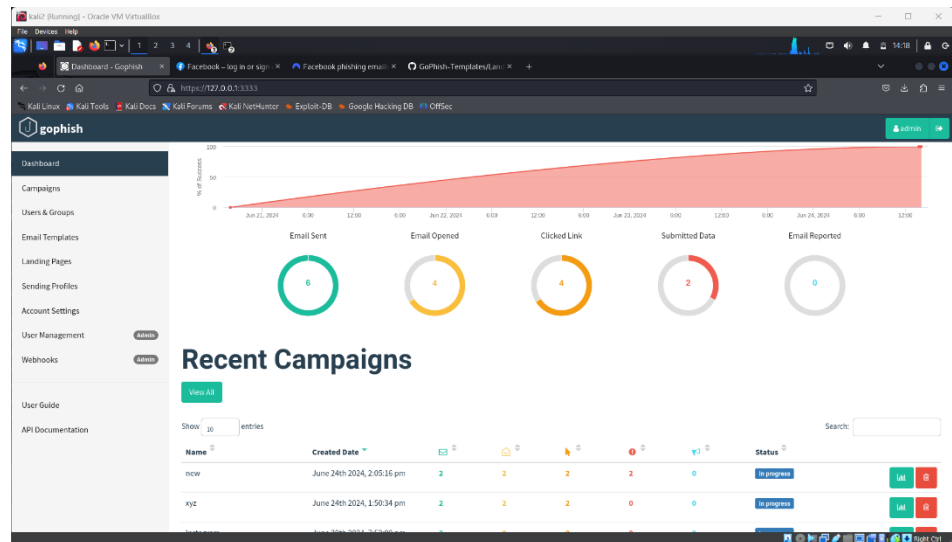


NOTE:

1. In URL section put the url copied from ngrok. Which will act as live server for you website.

Now you are done with campaign .

You can see the result in dashboard section.



Username and password will capture in dashboard section of the website .

4. Analysing and Detecting phishing mail:

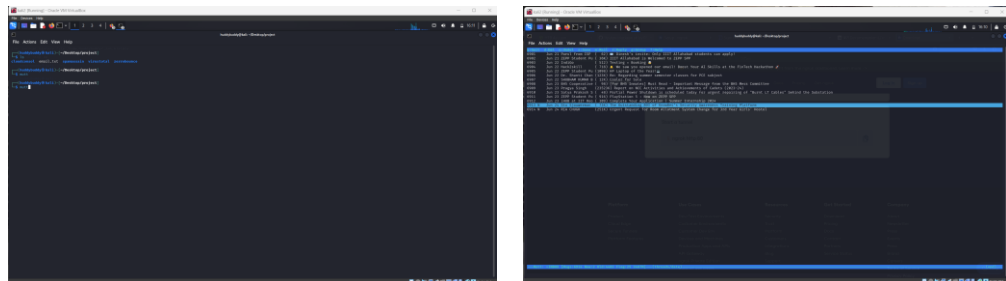
We have done phishing campaign in the above.

Now dive into how to detect mail is phishing or not using tools like spamassassin, and api's like virustotal, phishtank etc.

Before that we have to take email content so , we will use mutt for that.

Run command:

\$ mutt



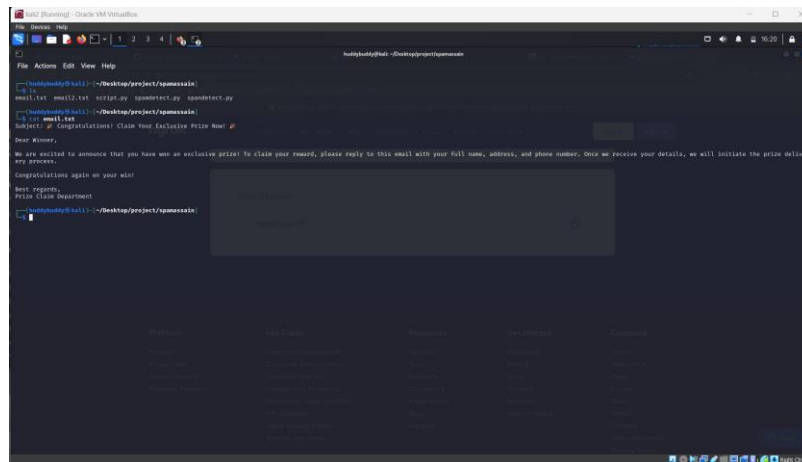
And read the mail and take email content for email filtration .

i. Scanning through Spamassassin:

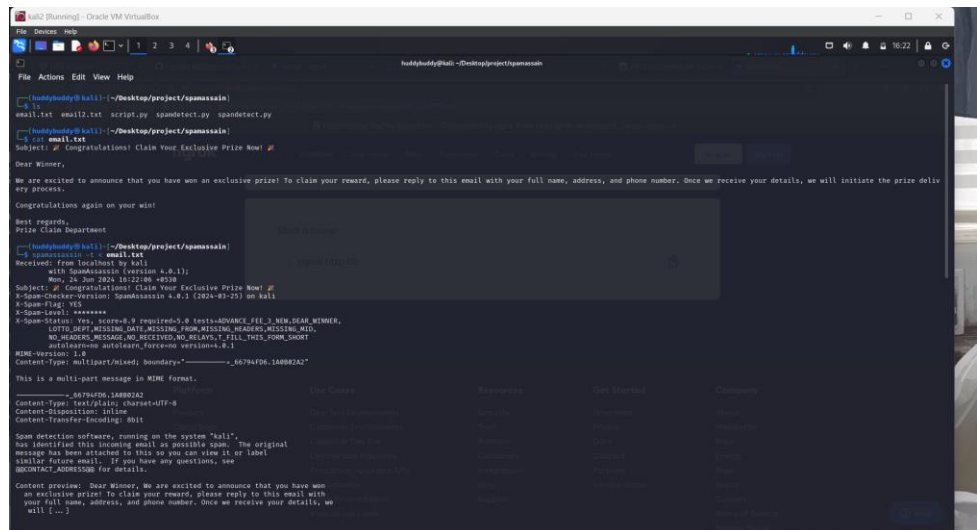
We have installed and configure spamassassin in earlier.

Read email content by mutt and take the content to a file.

For test purpose I took a phishing mail content. now run test on it.



The test will be done by using command,
`$ spamassassin -t < email_content.txt`
 Then you will receive a report regarding the content of the mail.



The score turnout to be 8.9 which is greater than 5.

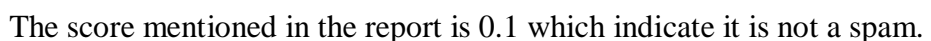
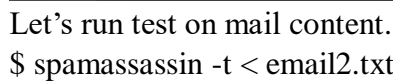
NOTE:

2. Here the scores and mentioned in every report
 - <5 mean spam free
 - >5 mean spam content

You can read the info of report online at official website of spamassassin.

Now test for a mail content which is not spam.

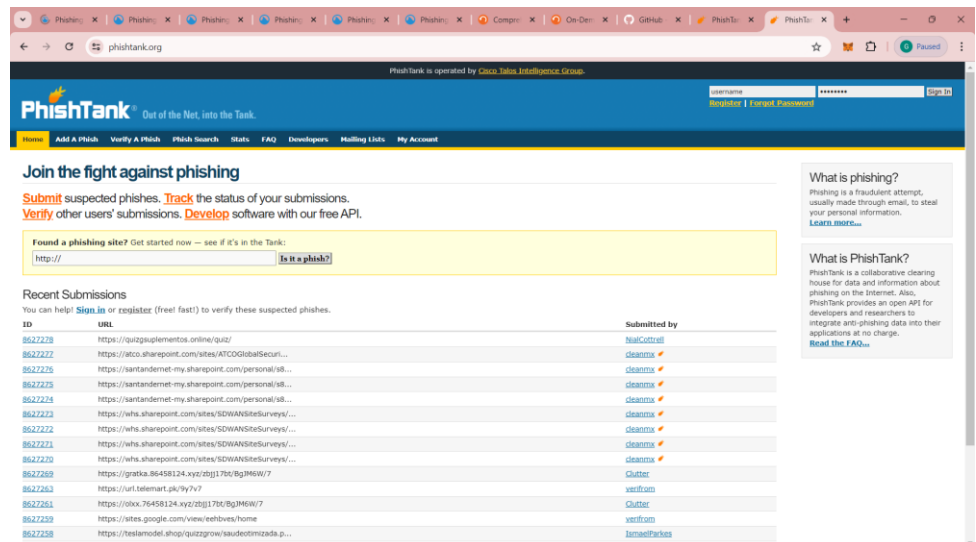
I have taken mail form my college mail id .(domain iiita.ac.in)



There is different type of free api's to test spam mail or spam content. They provide service for free to test whether an email is a spam or not.

- PhishTank is a collaborative clearing house for data and information about phishing on the Internet.

27



Also, you can obtain that by script.

```
import requests

url = "https://checkurl.phishtank.com/checkurl/"
params = {
    'format': 'json',
    'url': 'http://example.com',
    'app_key': 'YOUR_APP_KEY'
}

response = requests.post(url, data=params)
print(response.json())
```

Note:

- In place of “YOUR_APP_KEY” go to website and register you will get your own app key
- In place of URL put the URL you want to check for spam detection.

Now date (24-06-2024) phishtank temporarily not taking registration. when it allows register and you will get the response from the api of phishtank .

- **VirusTotal API:**

VirusTotal provides a public API as a free service. It provides automation for some of its online features such as to "upload and scan files, submit and scan URLs, access finished scan reports and make automatic comments on URLs and samples". Some restrictions apply for requests made through the public API, such as requiring an individual API key freely

obtained by online signing up, low priority scan queue, and limited number of requests per time frame.

You can access this ([API overview](#)) documentation on scanning ip, websites, file behaviours, domains.

Below script is an example of using api to scan a url .



```
#!/usr/bin/env python3
import requests

url = "https://www.google.com/"

headers = {
    "accept": "application/json",
    "content-type": "application/x-www-form-urlencoded"
}

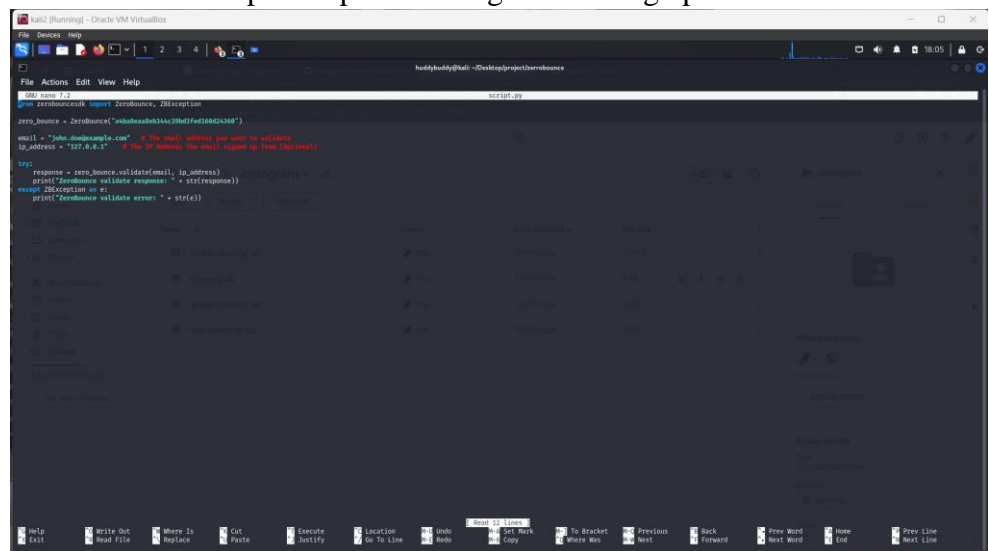
response = requests.post(url, headers=headers)

print(response.text)

# Example output:
# {"success": true, "ip": "64.233.160.101", "country": "US", "city": "Mountain View", "region": "California", "zip": "94035", "isp": "Google LLC", "mx": "aspmx.l.google.com", "txt": "v=3", "error": null}
```

- **Zerobounce API:**
ZeroBounce is a leading online email validation system created to ensure that companies sending complex and high volume emails avoid deliverability issues. The system works by reducing and eliminating invalid, abuse, complaint, inactive, and spam-trap email addresses.

Below is the example script for testing email using api .



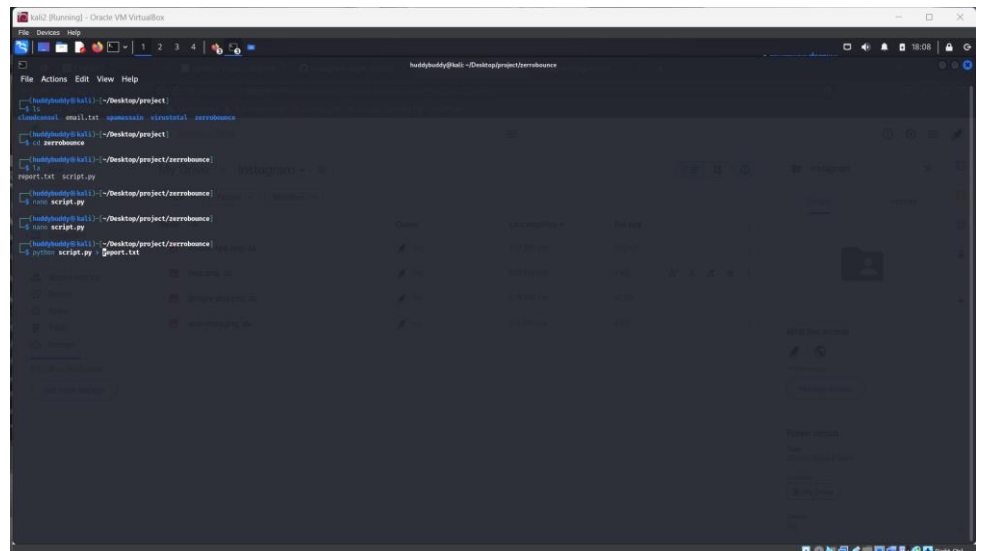
```
#!/usr/bin/env python3
import zerobounce, json

zerobounce = zerobounce.Zerobounce("apikey@zerobounce.com")

email = "john.doe@gmail.com"
ip_address = "127.0.0.1"

try:
    response = zerobounce.validate(email, ip_address)
    print("zerobounce validate response: " + str(response))
except Exception as e:
    print("zerobounce validate error: " + str(e))
```

This command runs test on a email and store the report in a report.txt file .



Checkout the report.txt file for more information.

5. Now let's see how phishing technique bypass spam filter.

Phishing attacks are a persistent threat in the realm of cybersecurity. Despite advances in spam filtering technologies, phishers continuously develop sophisticated techniques to evade detection. This section outlines the primary methods used by phishing emails to bypass spam filters.

1. Spoofing Legitimate Senders

Phishers often manipulate email headers and sender information to make the email appear as if it is from a trusted source. This can be achieved through:

- **Email Spoofing:** Altering the "From" address to match a legitimate domain, deceiving recipients into believing the email is from a trusted entity.
- **Domain Spoofing:** Registering domains that closely resemble legitimate ones (e.g., "amaz0n.com" instead of "amazon.com") to mislead recipients.

2. Using Compromised Accounts

Phishing emails may be sent from previously compromised accounts. These accounts are trusted by spam filters due to their legitimate history, making detection more challenging.

3. Obfuscation Techniques

Phishers employ various methods to obscure the true nature of their emails:

- **Encoding:** Using Base64 or other encoding methods to hide malicious content within the email body.
- **Image-based Emails:** Embedding the phishing message within an image to bypass text-based content filters.
- **URL Obfuscation:** Utilizing URL shorteners, redirects, or embedding malicious links within attachments to avoid detection.

4. Dynamic Content

Some phishing emails change content dynamically to evade detection mechanisms:

- **Time-based Changes:** Modifying the email content based on the time it is opened to avoid signature-based detection.
- **Geolocation:** Customizing email content based on the recipient's geographical location to enhance believability.

5. Social Engineering

Phishers leverage psychological manipulation to compel recipients to act:

- **Urgency and Fear:** Crafting messages that create a sense of urgency or fear, prompting immediate action without scrutiny.
- **Personalization:** Using information about the recipient to create more convincing and targeted messages.

6. Technical Evasion

Phishers exploit technical weaknesses in spam filters:

- **Domain Age:** Registering new domains that have not yet been blacklisted.
- **Bulletproof Hosting:** Using hosting providers known for ignoring abuse reports to host phishing content.
- **CAPTCHA:** Implementing CAPTCHA systems to prevent automated analysis of the email content by spam filters.

7. Attachment-based Phishing

Malicious attachments are a common vector for phishing attacks:

- **Malicious Attachments:** Including malware-laden files (e.g., PDFs, Word documents with macros) that execute upon being opened.
- **Polymorphic Attachments:** Regularly changing the attachment's hash to evade signature-based detection.

8. Exploiting Weaknesses in Spam Filters

Phishers frequently update their tactics to stay ahead of spam filters:

- **Text Randomization:** Adding random text or characters to the email body to make each instance unique and evade pattern detection.
- **HTML Tricks:** Using HTML tags to hide text or make it appear different from the actual content.

5. CONCLUSION AND RECOMMENDATION:

1. Findings

Through our project, we analyzed various phishing techniques using tools like GoPhish and BlackEye, and assessed their effectiveness in bypassing spam detection systems such as SpamAssassin. By leveraging APIs like PhishTank, ZeroBounce, and VirusTotal, we identified the following key findings:

- **Phishing Techniques:** Advanced phishing techniques that use social engineering and obfuscation were particularly successful in bypassing basic spam filters.
- **Spam Detection:** While SpamAssassin and similar tools are effective against common spam, they often fall short against sophisticated phishing attacks that mimic legitimate communication or use advanced evasion techniques.
- **Indicators of Compromise:** Common indicators included unusual email traffic, altered email headers, suspicious IP addresses, and unexpected changes in system files or network configurations.

2. Countermeasures:

To enhance spam detection and prevent phishing attacks, we recommend the following countermeasures: (Technical Aspect)

Enhancing Spam Filter Rules and Machine Learning Models:

- **Improving Filters:** Update and refine spam filter rules to detect more sophisticated phishing techniques. Incorporate patterns identified during our testing with GoPhish and BlackEye.
 - **Example:** Implement rules that detect obfuscation techniques and social engineering cues commonly used in phishing emails.
- **Machine Learning:** Utilize advanced machine learning models to identify anomalies in email traffic and content.
 - **Example:** Deploy deep learning models that analyze email metadata and content for subtle signs of phishing attempts.

Implementing Advanced Email Authentication Protocols

- **DMARC, DKIM, SPF:** Configure and enforce email authentication protocols to verify the legitimacy of incoming emails.
 - **Example:** Implement DMARC policies with strict enforcement, ensuring that only emails from authenticated sources are delivered to the inbox.
- **Regular Updates:** Regularly update these authentication protocols to keep up with evolving phishing tactics.

Regular Updates and Security Policies

- **System Updates:** Ensure that all spam detection systems and related software are regularly updated.
 - **Example:** Schedule automatic updates for SpamAssassin and antivirus software to incorporate the latest threat intelligence.
- **Security Policies:** Maintain comprehensive and up-to-date security policies that address email security and phishing prevention.
 - **Example:** Develop and enforce policies that require regular password changes and the use of secure email practices.

User Education and Awareness Programs

- **Training Sessions:** Conduct regular training sessions to educate users about phishing threats and how to recognize them.
 - **Example:** Use phishing simulation tools like GoPhish to conduct mock phishing attacks and improve user awareness.
- **Awareness Campaigns:** Implement ongoing awareness campaigns to keep phishing threats top of mind for all users.
 - **Example:** Distribute educational materials and alerts about recent phishing trends and best practices for email security.

As a non-technical aspect there are some countermeasures:

- Be **cautious with links:** Teach users to hover over links to see the actual URL before clicking.
- Keep **personal information private:** Educate users on the importance of not sharing personal information over email.
- Verify **the source:** Encourage users to verify the sender's email address and to be suspicious of unexpected messages.
- Use **antivirus software:** Ensure all devices are equipped with up-to-date antivirus protection.
- Regular **updates:** Keep software and systems updated to protect against vulnerabilities.
- Use **firewalls:** Implement both personal and network firewalls to add an extra layer of protection.
- Be **wary of email attachments:** Advise users to be cautious with email attachments, especially from unknown senders.
- Educate **on social engineering:** Make users aware of social engineering tactics used in phishing attacks.

- Report **suspicious emails**: Establish a protocol for reporting suspicious emails within the organization.
- Enable **multi-factor authentication**: Use MFA to add an additional layer of security for accessing sensitive accounts.

Multi-Factor Authentication (MFA):

- **MFA Implementation**: Require multi-factor authentication for accessing sensitive systems and accounts.
 - **Example**: Enforce MFA for email accounts and administrative access to systems used in your infrastructure.
- **Enhanced Security**: MFA provides an additional layer of security, making it more difficult for attackers to gain unauthorized access even if they obtain login credentials.
 - **Example**: Use MFA solutions that combine something the user knows (password) with something the user has (a mobile device or hardware token).

6. References:

1. <https://www.ibm.com/topics/spear-phishing>
2. <https://www.phishing.org/>
3. <https://phishtank.org/>
4. <https://docs.virustotal.com/>
5. <https://www.zerobounce.net/>
6. <https://www.zerobounce.net/members/API>
7. <https://spamassassin.apache.org/>
8. <https://www.wikipedia.org/>
9. <https://www.youtube.com/>
10. <https://www.kali.org/get-kali/#kali-platforms>
11. <https://www.virtualbox.org/>
12. **Gophish:** <https://getgophish.com/documentation>
13. **BlackEye :** <https://github.com/EricksonAtHome/blackeye>
14. "The Art of Deception: Controlling the Human Element of Security" by Kevin D. Mitnick and William L. Simon
15. [How Phishing Attacks Bypass Spam Filters | Infosec \(infosecinstitute.com\)](#)
- 16.