CYB206

GROUP 4

EMAIL PHISHING

PARTICIPANTS:

MBONU SOMTOCHUKWU BHU/22/04/09/0027

TERSOR KING SOLOMON BHU/22/04/09/0078

ISA SAMUEL LASOBOK BHU/22/04/09/0067

EZIJOTA SOLOMON ENITIE BHU/22/04/09/0018

EJIKE NNAEMEKA GODSTIME BHU/22/04/09/0057

What is phishing?

Phishing is a common type of cyber attack that targets individuals through email,

text

messages, phone calls, and other forms of communication. A phishing attack aims

to

trick the recipient into falling for the attacker’s desired action, such as revealing

financial information, system login credentials, or other sensitive information.

As a popular form of social engineering, phishing involves psychological

manipulation

and deception whereby threat actors masquerade as reputable entities to mislead

users into performing specific actions. These actions often involve clicking links to

fake websites, downloading and installing malicious files, and divulging private

information, like bank account numbers or credit card information.

Since the mid-1990s, the term “phishing” has been used to identify hackers who use

fraudulent emails to “fish for” information from unsuspecting users. However,

phishing

attacks have become increasingly sophisticated and are now broken down into

different types, including email phishing, [spear phishing](https://www.proofpoint.com/us/threat-reference/spear-phishing), [smishing](https://www.proofpoint.com/us/threat-reference/smishing), vishing, and

whaling. Each type is characterized by specific channels and methods of execution –

email, text, voice, social media, etc. – all with a similar underlying intention.

## Types of Phishing Attacks

Phishing is a cybercrime where attackers try to trick you into giving up personal

information.

Here are some common types:

### 

### 

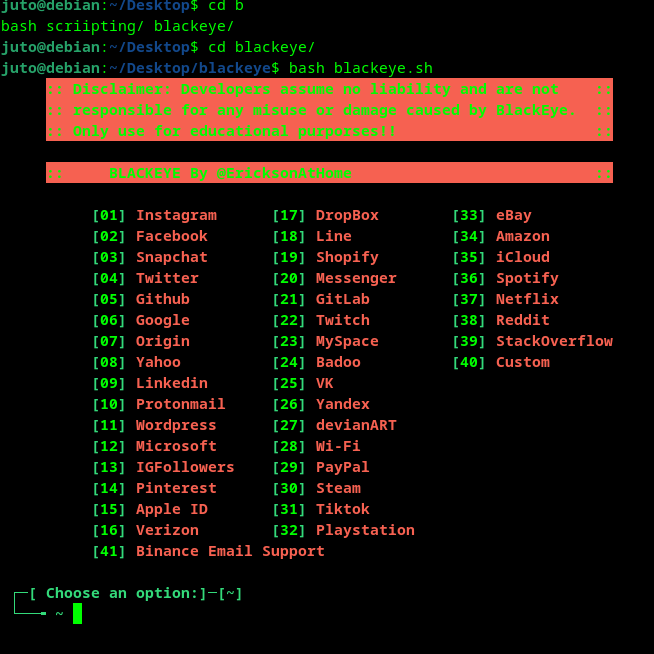
### **Email-Based Attack**

* **Standard Email Phishing:** This is the most common type, where you get an email
* pretending to be from a known company asking for your information.
* **Malware Phishing:** These emails try to get you to click on a link or download a file that installs harmful software on your computer.
* **Spear Phishing:** This is a targeted attack where the email is personalized to you, making it more convincing.
* **Clone Phishing:** The attacker copies a real email, changes the link or attachment to a malicious one, and sends it to your contacts.
* **BEC (Business Email Compromise):** This targets businesses, pretending to be a trusted employee asking for money or information.

**SIMULATION**

n this scene we will be simulating the emailing phishing, for this we will be using

kali

hack tool called “blackeye”

**BlackEye** is an open-source LAN phishing tool primarily used for penetration t

essential to understand that this tool can be misused for malicious activities.

### **How BlackEye Works**

* **Template Selection:** BlackEye offers a variety of pre-designed templates for

popular websites.

* **Customization:** Users can customize these templates to suit their specific

Needs.

* **Payload Generation:** The tool generates a payload (malicious code) that

will

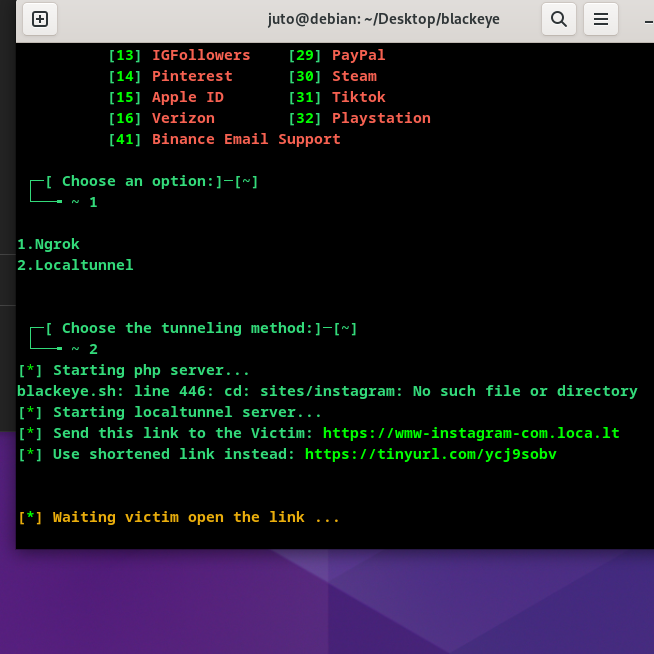
be delivered to the victim.

* **Phishing Page Creation:** BlackEye creates a phishing page that looks

identical to the legitimate website.

* **Distribution:** The phishing page is distributed to targets through various

methods like email, social engineering, or other means.

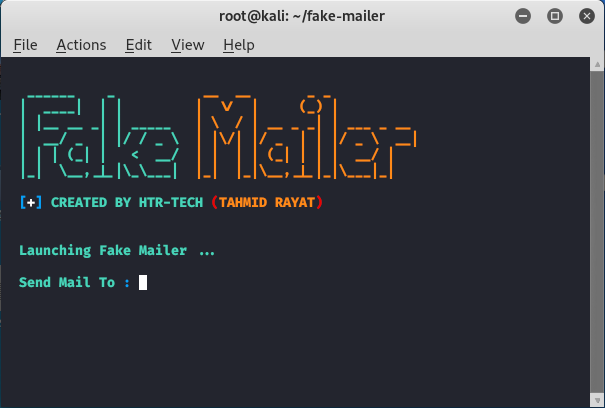


Using it can generate a dummy website and a gives us an open door to so much more.

We then send the email using another hacktool to hide are identity called “ Fake Mailer”.

**Cybersecurity researchers and law enforcement professionals often operate in a realm where anonymity is crucial.** Protecting their identities is essential to safeguarding sensitive information, deterring threats, and fostering open collaboration. Maintaining secrecy allows these individuals to freely share critical insights without fear of reprisal or exposure. This anonymity is particularly vital when handling sensitive data or investigating complex cybercrimes.

Fakemailer is a free and open-source tool available on GitHub. Fakemailer provides a command-line interface that you can run on Kali Linux. The interactive console provides a number of helpful features, such as command completion and contextual help. Fakemailer helps law and enforcement agencies to investigate cybercrimes such as cyber grooming, cyberstalking, cyberbullying, and spreading misinformation.





This way we do not have to go to the person's email ourselves.   
  
The aim here is to trick the person into thinking that we are someone we are not, like a company or an old friend.

The person then taps our generated link, giving us access to there browser which opens opportunists for many other things.