Phishing and Spear Phishing

1. Phishing

Phishing is a cyber attack that involves sending fraudulent communications, often via email, that appear to come from a reputable source. The primary goal is to deceive the recipient into revealing sensitive information, such as login credentials or financial details.

How It Works

Initiation: An attacker crafts a message that mimics a legitimate entity (e.g., a bank or a service provider).

Luring the Victim: The message typically contains a call to action, such as clicking a link or downloading an attachment.

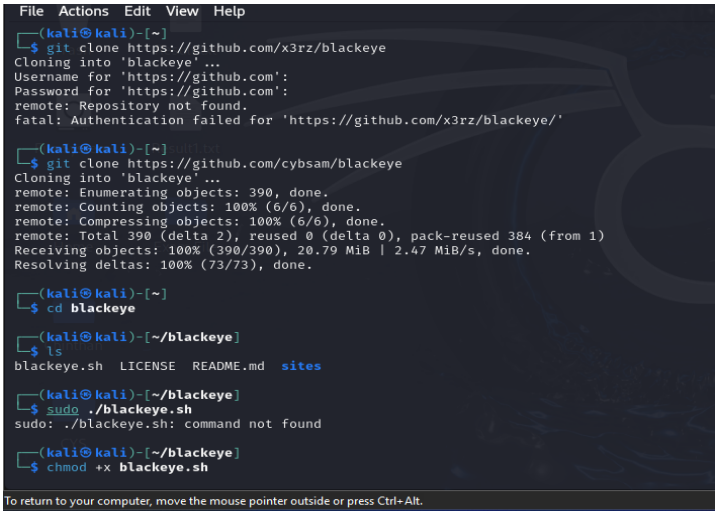
Fake Website or Malware: Clicking the link may redirect the victim to a counterfeit website designed to capture their credentials or install malware on their device.

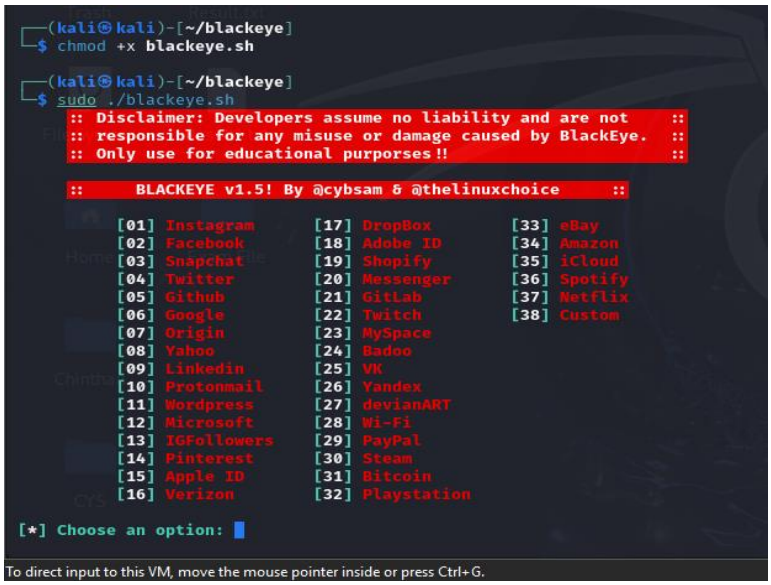
Data Collection: If successful, the attacker collects sensitive information entered by the victim on the fake site or through malware.

Brief Demo:

There are many website to do this. I choose Ngrok.

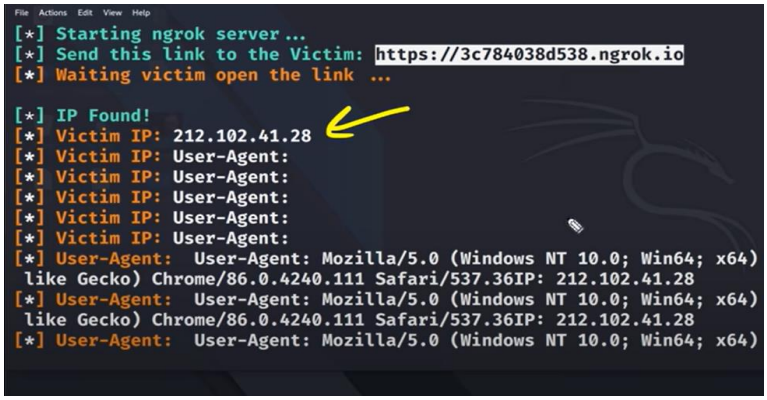
Step1: Clone the github repository to fetch the clone websites.

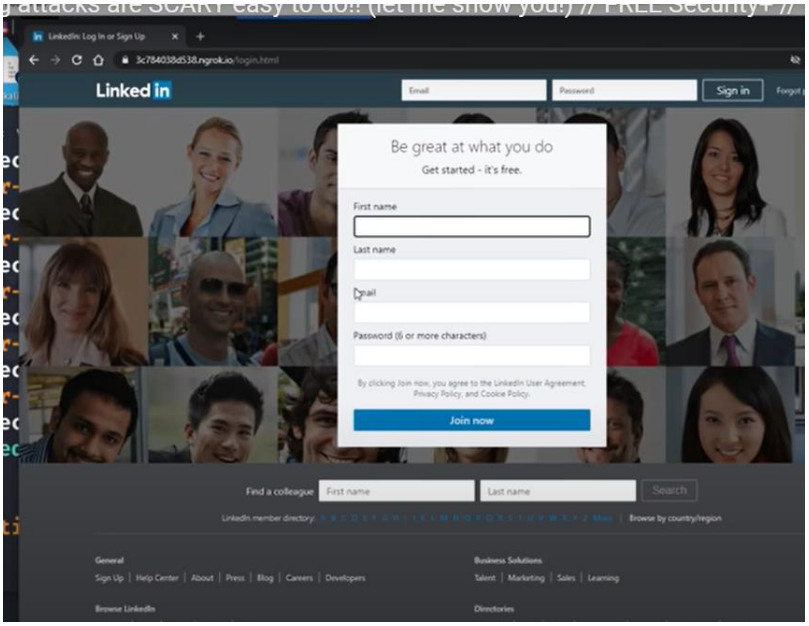




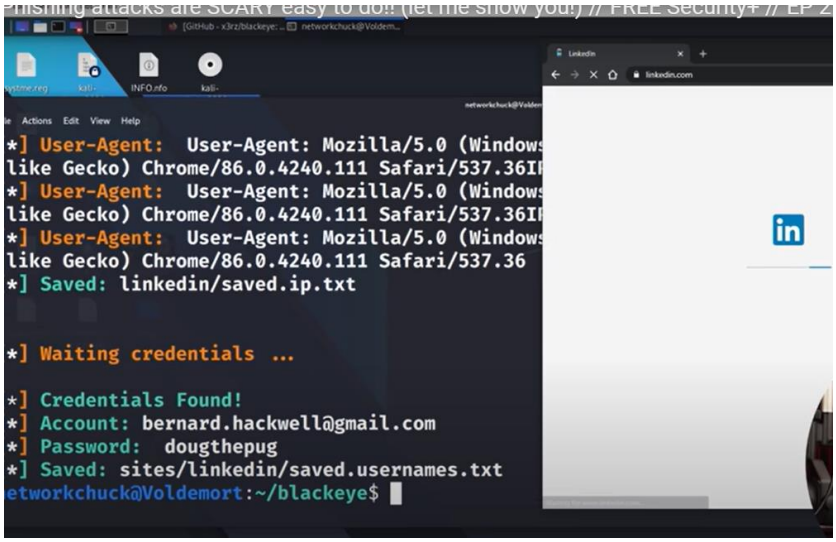
Step 2: After choosing the website it intiates ngrok and produces the website url.

Step 2: Whoever access this link will be notified in terminal and the terminal will wait for the victims credentials.



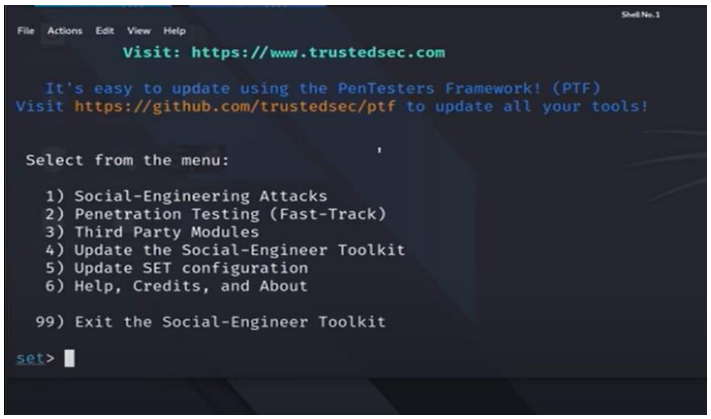


Step 3: Got the victims credentials from the fake website.

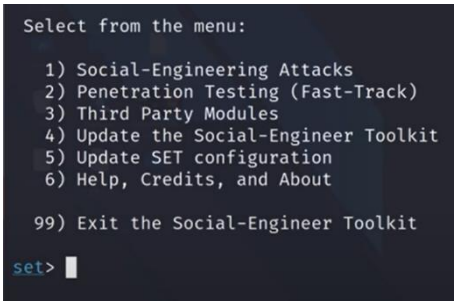


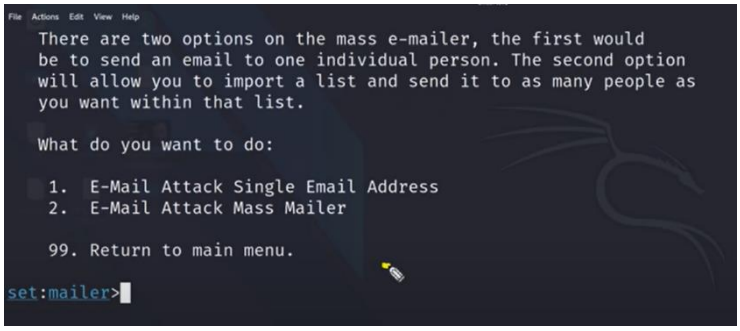
Using social Engineering Tactics, creating a phishing mail.

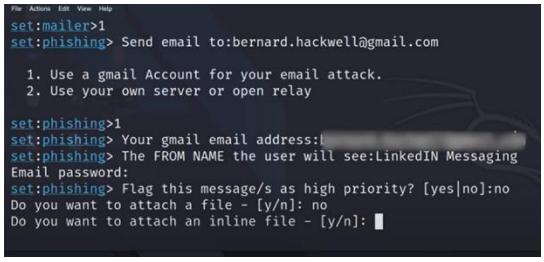
Step 4: Goto Applications→ social engineering toolkit.

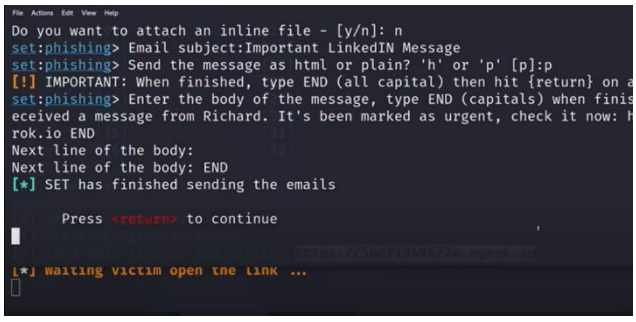


Step 5: Select the required menu and then choose the email attack. Create how the mail must be framed, enter sender receiver mail address, message.



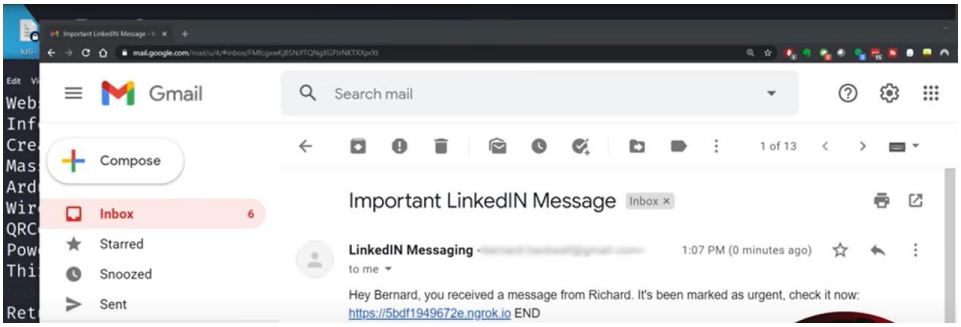






Step 6: Mail will be sent and user might enter credentials in that phishing link.

From this social engineering tactics, we can get the credentials of victim.



Same way we can have Spear phishing techniques which aims at specific person, group or organization for valuables.

2. Spear Phishing

Spear phishing is a targeted form of phishing where attackers focus on specific individuals or organizations, often using personal information to make their messages more convincing.

How It Works

Research Phase: Attackers gather detailed information about their target from social media and other public sources.

Crafting Personalized Messages: Using this information, they create tailored messages that appear credible and relevant to the victim.

Execution: The victim receives a message that seems legitimate, often prompting them to click a link or provide sensitive information.

Data Compromise: If the victim complies, their credentials are sent directly to the attacker.

Attack techniques carried out in a network environment

- **Malicious Web Links**: Attackers craft links that appear legitimate but redirect users to fake websites designed to capture credentials.
- **Keyloggers**: Deployment of keyloggers to record keystrokes, capturing sensitive information as users enter it.

- **Content Injection**: Altering legitimate website content to mislead users into providing personal information.
- **Session Hijacking**: Exploiting active sessions to intercept data between the user and a legitimate service.
- **Social Engineering Techniques**: Manipulating victims using personal information to gain compliance with malicious requests.

Tools for Phishing and Spear Phishing:

Cobalt Strike: Cobalt Strike is a penetration testing tool that includes features for creating and sending customized spear phishing emails to targeted individuals. It allows users to track interactions and embed URLs that redirect victims to malicious sites.

Social-Engineer Toolkit (SET): The Social-Engineer Toolkit (SET) is designed for social engineering attacks, including phishing and spear phishing, enabling users to clone websites and send phishing emails. It also supports various attack vectors like SMS phishing (smishing) and caller ID spoofing.

EvilGinx2: EvilGinx2 is a man-in-the-middle framework that facilitates advanced phishing attacks by capturing login credentials and session cookies from users. This tool effectively bypasses two-factor authentication by intercepting session tokens through legitimate-looking login pages.

Gophish: Gophish is an open-source phishing framework that allows users to create, manage, and analyze phishing campaigns. It provides customizable email templates and landing pages, along with analytics to track user engagement and responses.

PhishX: PhishX is a platform for creating and managing phishing simulations and training programs within organizations. It offers customizable templates for emails and landing pages while providing reporting features to assess user vulnerability.

MailSniper: MailSniper is a targeted email attack tool used in penetration testing to automate the sending of spear phishing emails. It allows customization of email

content based on the target's profile, making it effective for conducting focused attacks.

Both phishing and spear phishing rely heavily on deception and manipulation, but spear phishing is characterized by its targeted approach, making it particularly dangerous for high-profile individuals or organizations.