**Social Engineering and Security Awareness Training**

Muhammad Abdullah

Student ID:

Cybersecurity

Dublin Business School

# ***Part 1: Describe in detail how social engineering works and evaluate why such techniques are effective. (10 marks)***

# **Ans:**

# Social engineering is the act of exploiting human weaknesses to gain access to personal information and protected systems. Social engineering relies on manipulating individuals rather than hacking computer systems to penetrate a target's account.

# Social engineering attacks are a type of cybercrime wherein the attacker fools the target through impersonation. They might pretend to be your boss, your supplier, someone from our IT team, or your delivery company. Regardless of who they're impersonating, their motivation is always the same — extracting money or data.

# **Example:**

# Phishing. Phishing is a social engineering technique in which an attacker sends fraudulent emails, claiming to be from a r**eputable and trusted source. E.g.**

# Vishing and Smashing

# Pretexting.

# Baiting.

# Tailgating and Piggybacking.

# Quid Pro Quo.

# **Real life Scenario:**

# Due to a social engineering and BEC scam, Cabarrus County, in the United States, suffered a loss of USD 1.7 million in 2018. Using malicious emails, hackers impersonated county suppliers and requested payments to a new bank account. According to the investigation, after the money was transferred, it was diverted to several accounts. In the emails, the scammers presented apparently legitimate documentation.

# 

# ***Social Engineering Demo* C:\Users\lazzy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\1.PNGC:\Users\lazzy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\2.PNG C:\Users\lazzy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\3.PNGC:\Users\lazzy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\4.PNGC:\Users\lazzy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\5.PNG**

# **C:\Users\lazzy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\6.PNGC:\Users\lazzy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\7.PNGC:\Users\lazzy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\8.PNGC:\Users\lazzy\AppData\Local\Microsoft\Windows\INetCache\Content.Word\9.PNG**

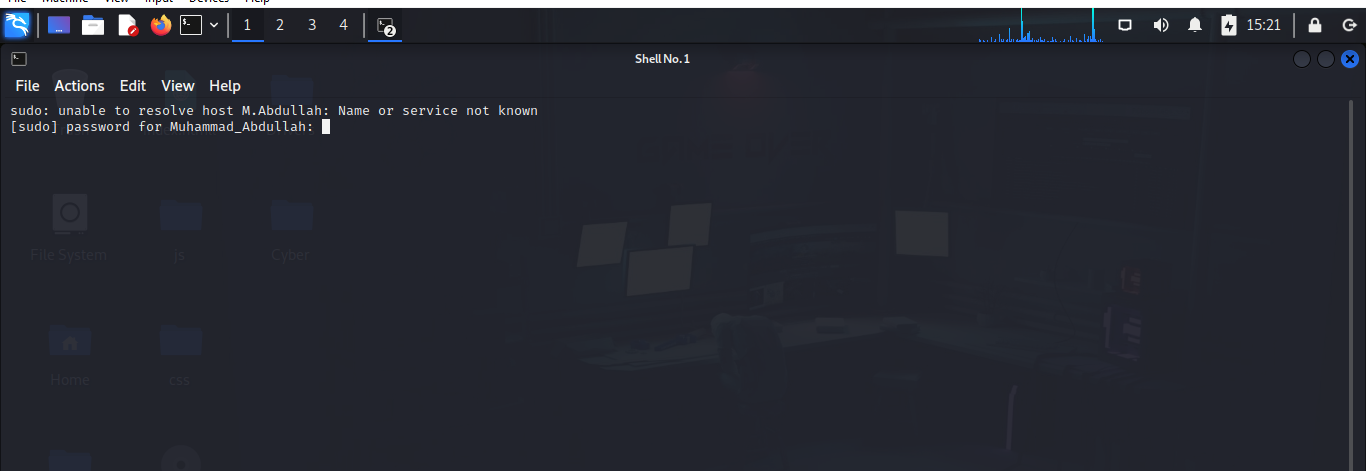
**Part 3: Demonstrate a Social Engineering Attack with Kali Linux** (20 Marks) https://github.com/trustedsec/social-engineer-toolkit

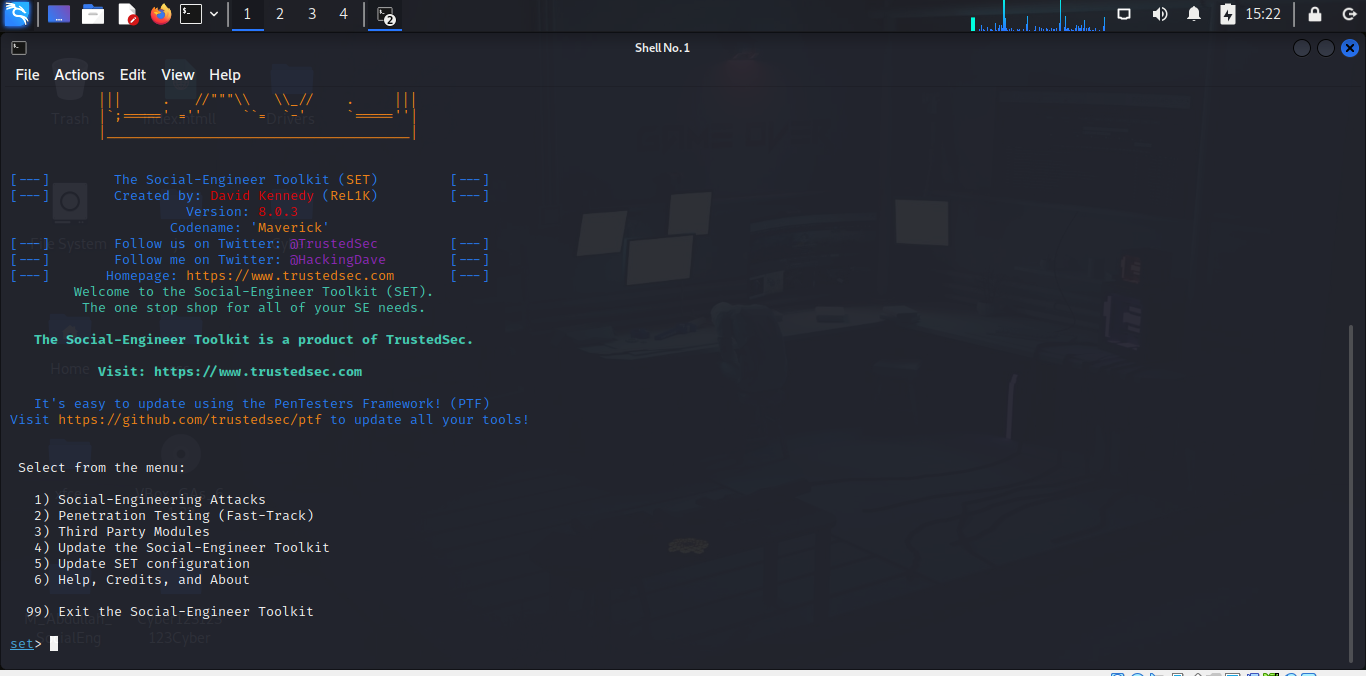
*You are required to simulate a social engineering attack using the SET (Social Engineering Toolkit) in Kali Linux.*

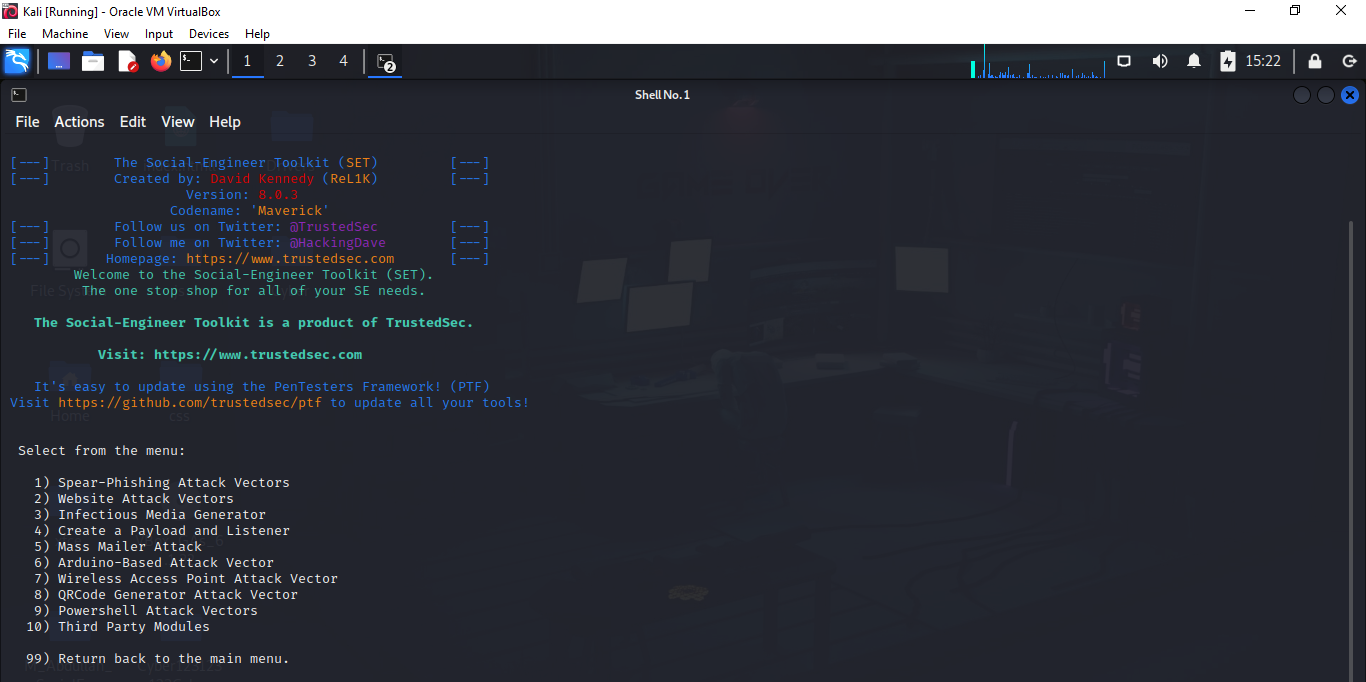
1. Perform a Website Cloning Attack. (Option 1-> Option 2 -> Option 3). Choose a website of your choice (the website should have a homepage which contains a login form/option (i.e. accepts a username + password via text boxes).
2. Have SET make a clone of the site, and harvest user information from the cloned site that the attacker could use to capture login details from an unsuspecting victim.
3. View and analyse the output report from SET to view the harvested data. For your report, detail what has occurred and use screenshots to accompany your answer.
4. Alternatively: discard steps 1 to 3... instead... Explain and demonstrate another attack of your choice from the SET.

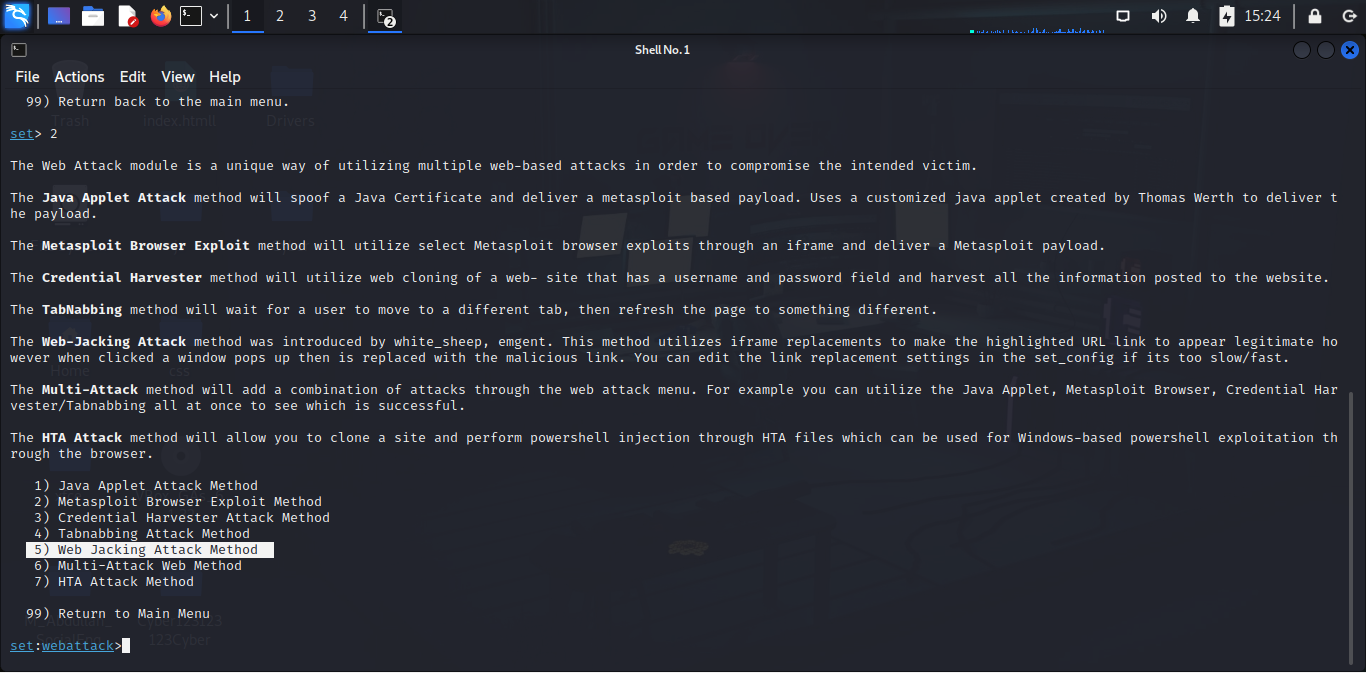
Ans:

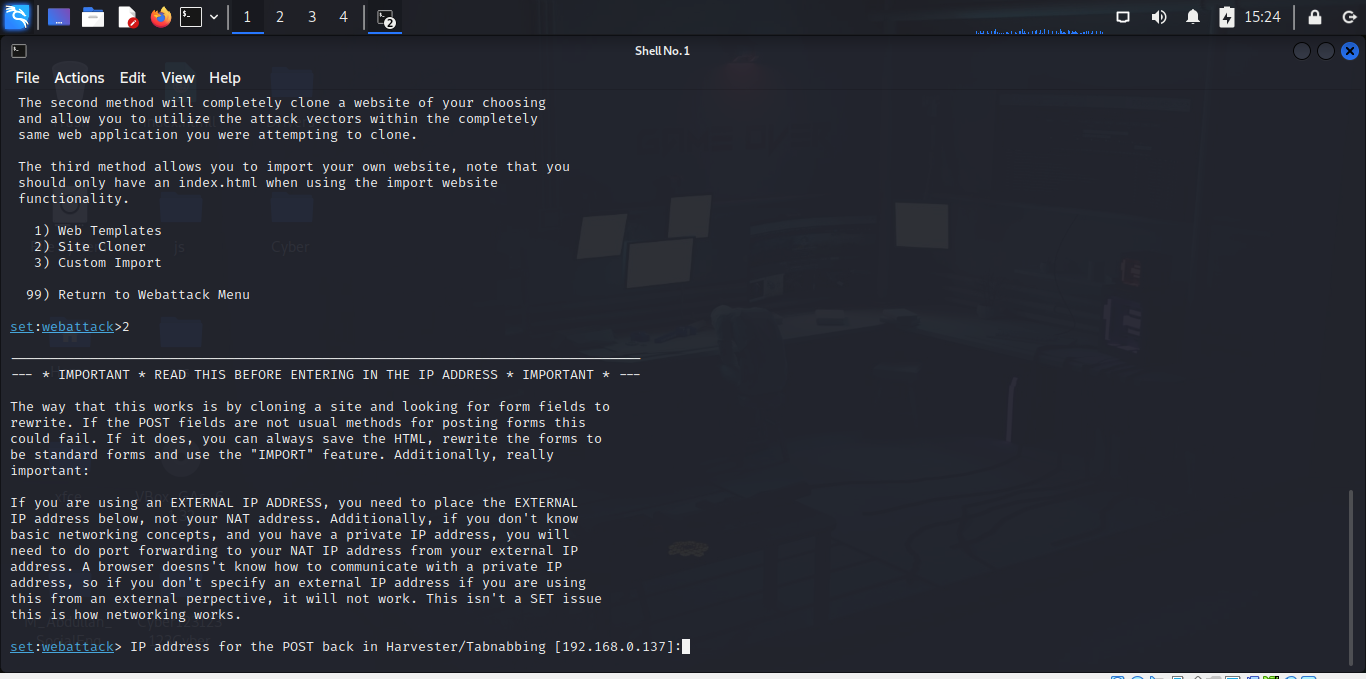
Social engineering toolkit is a free and open-source tool that is used for social engineering attacks such as phishing, faking phone numbers, sending SMS, etc. it's a free tool available in Kali Linux.

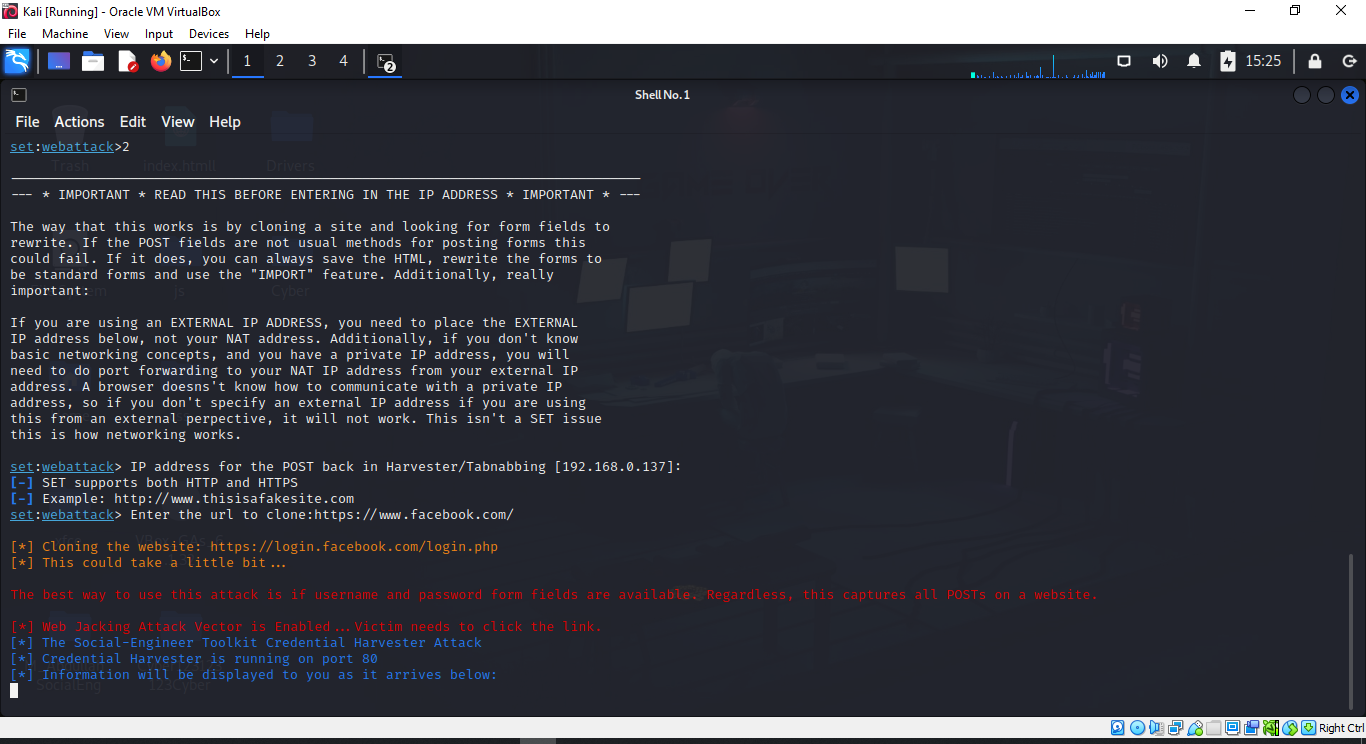
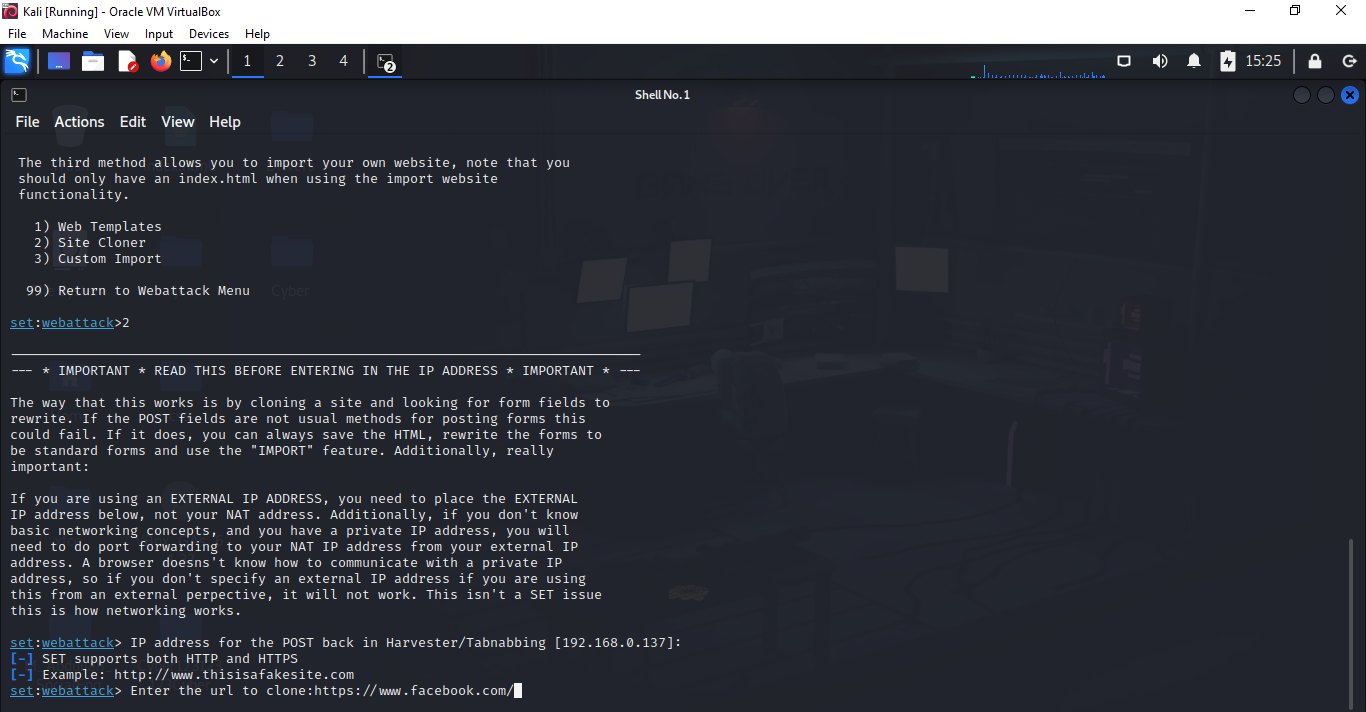
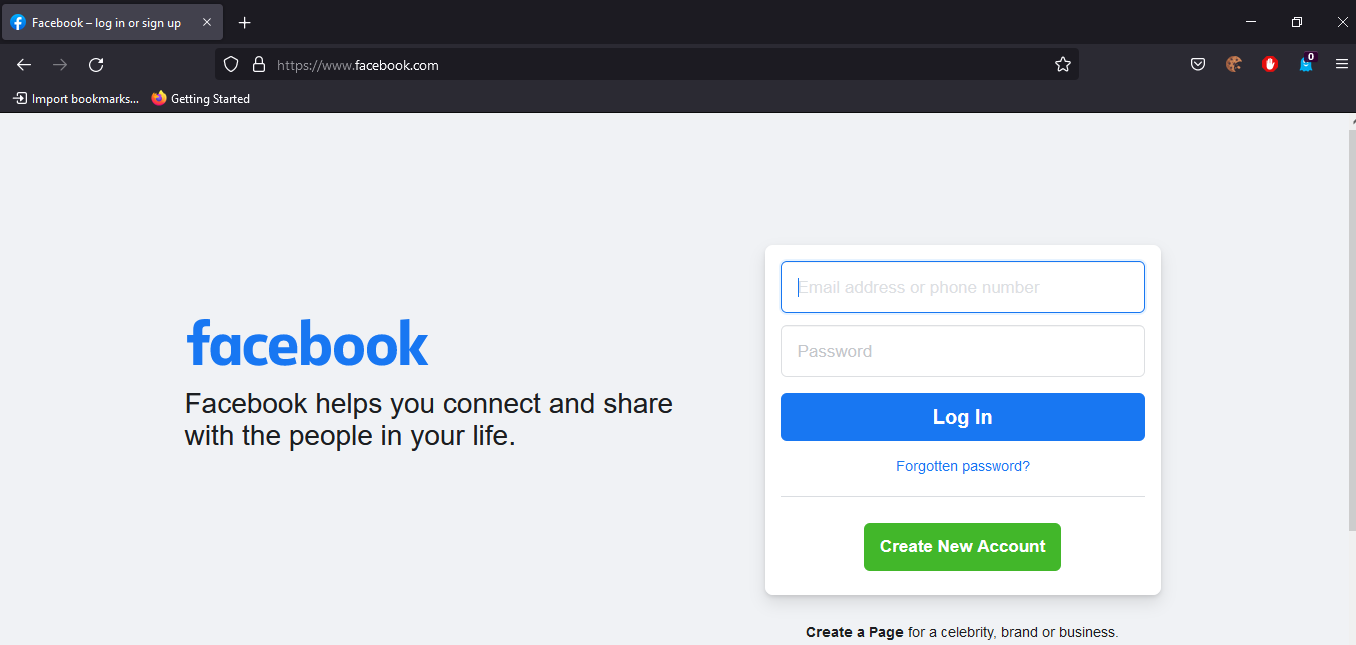
First of all I install the Social Engineering toolkit by provided link  

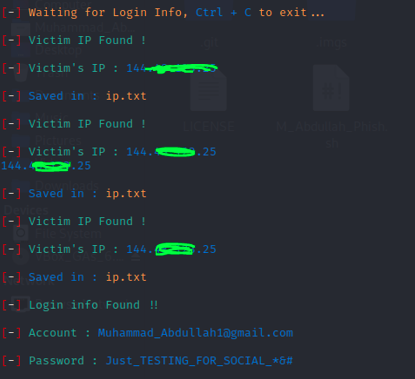
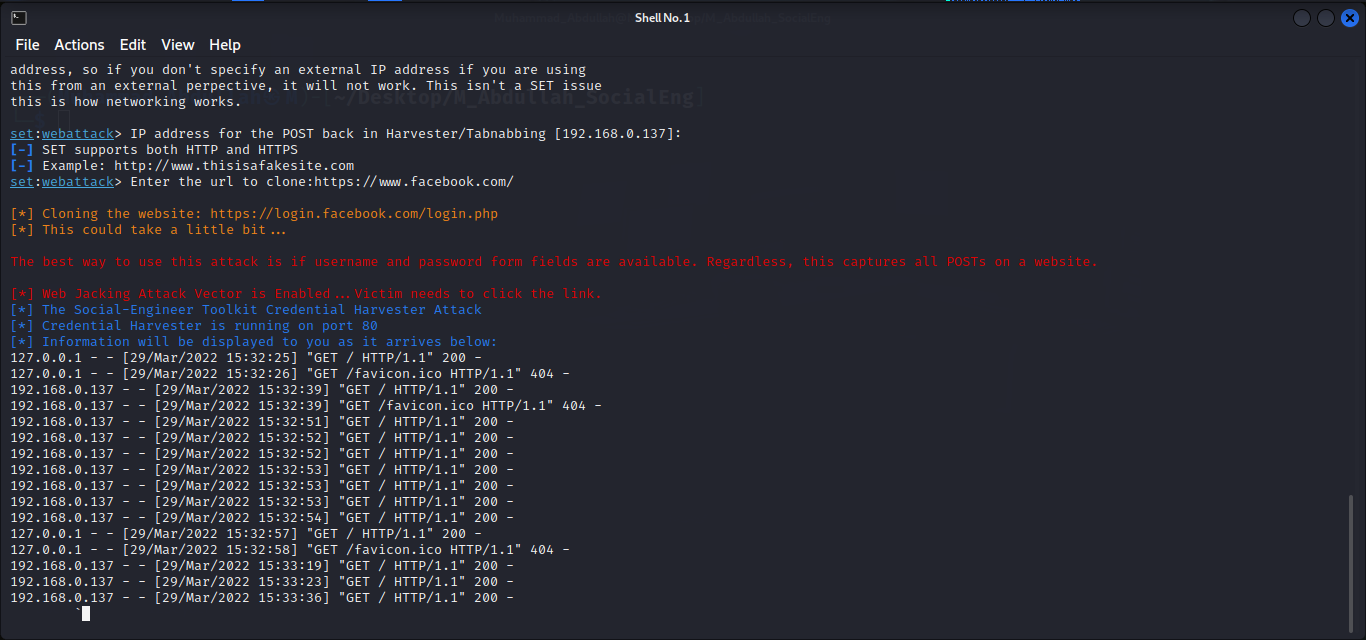
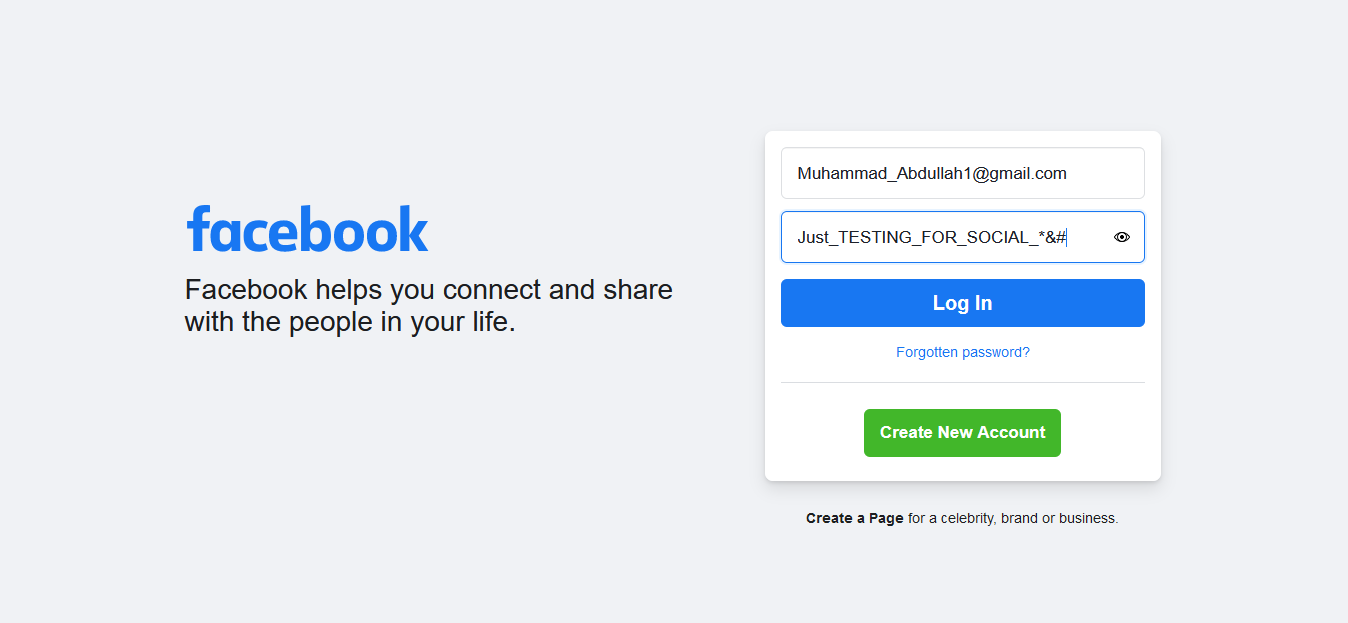
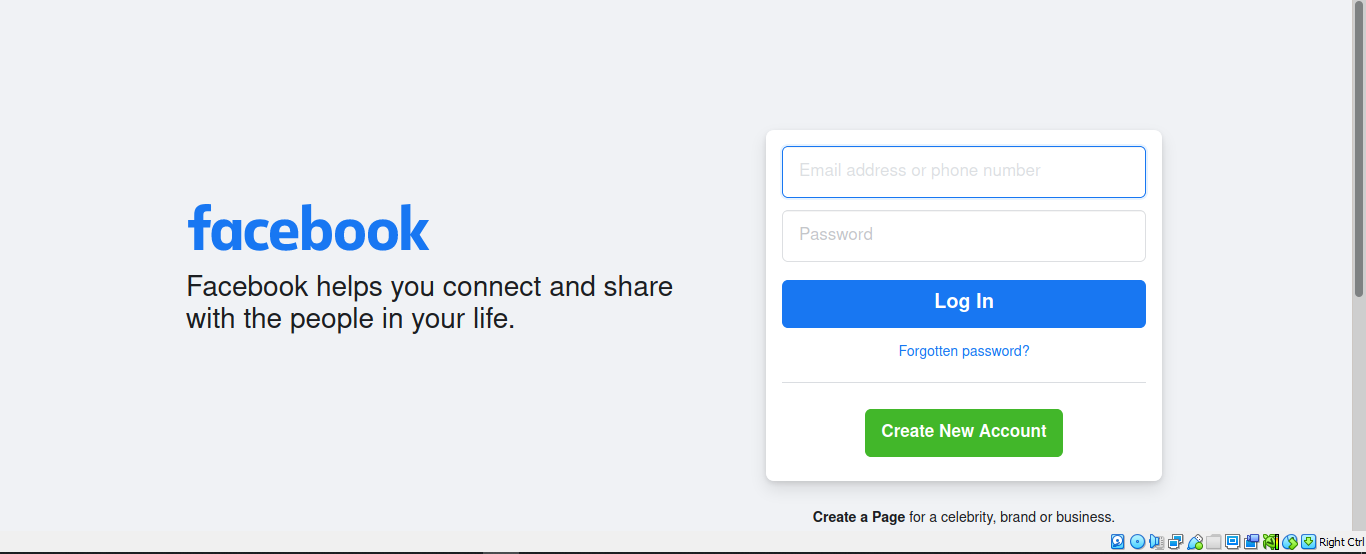
Its Required Root access I Provided it.

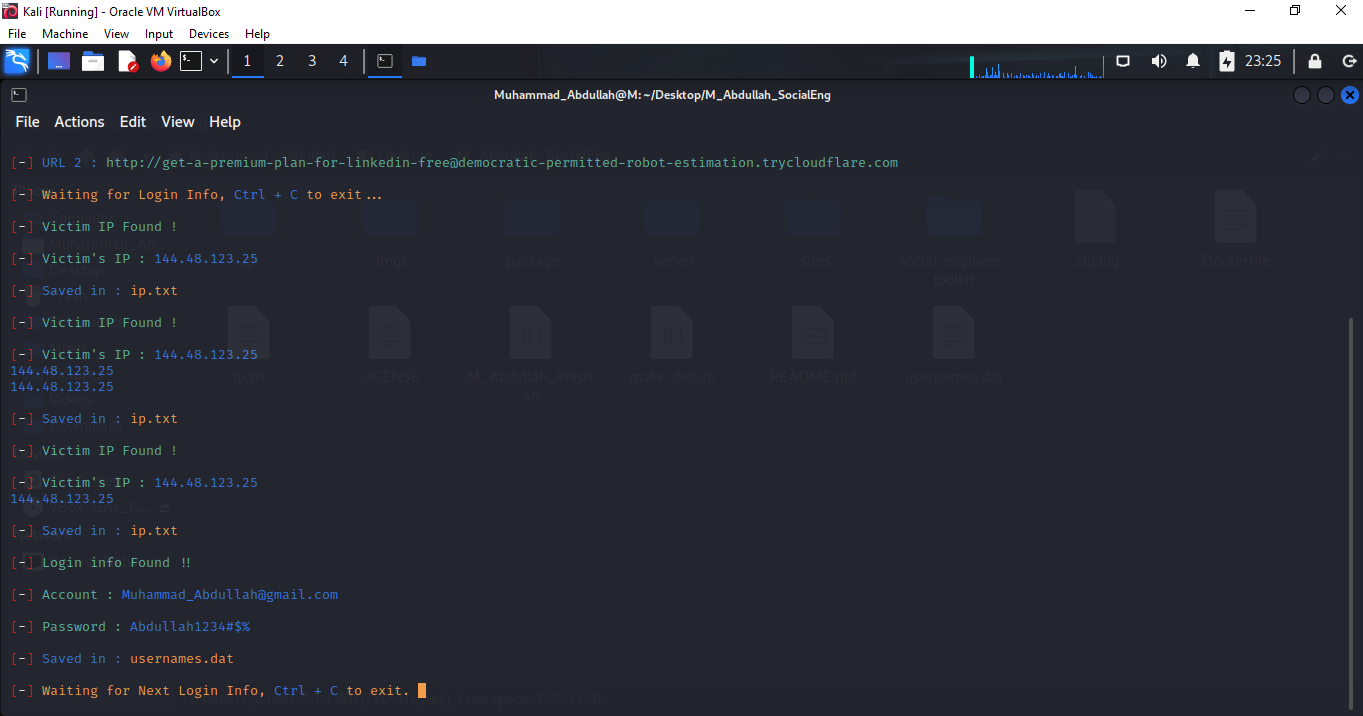
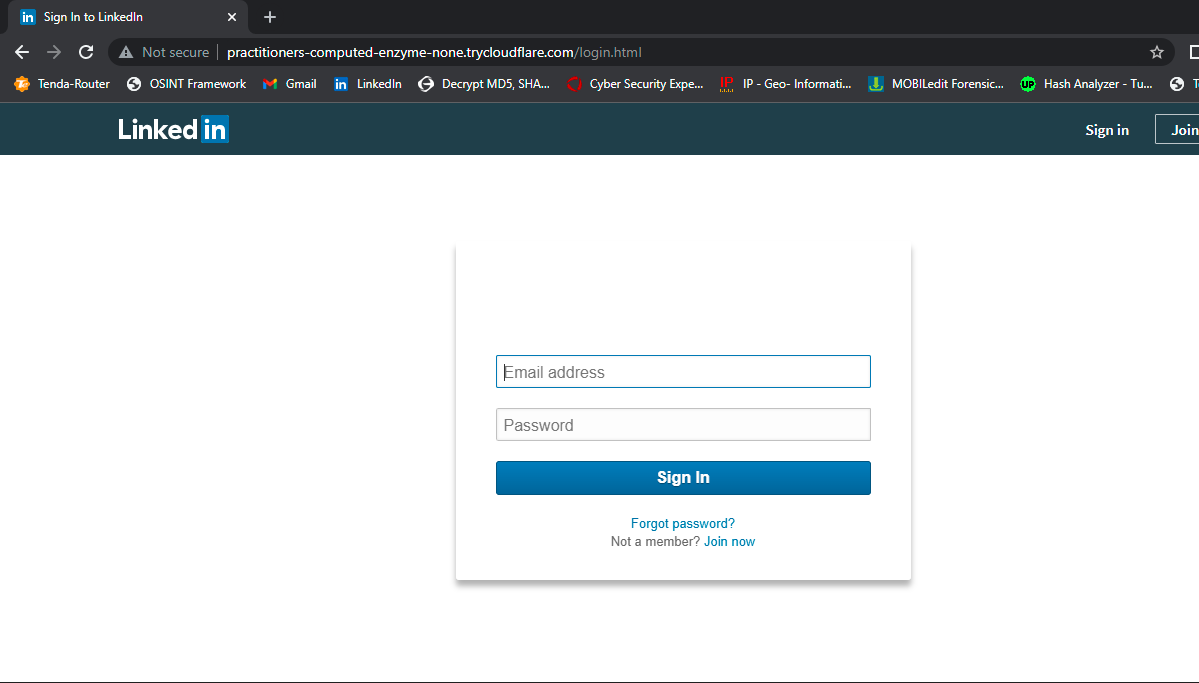
I Select option # 1

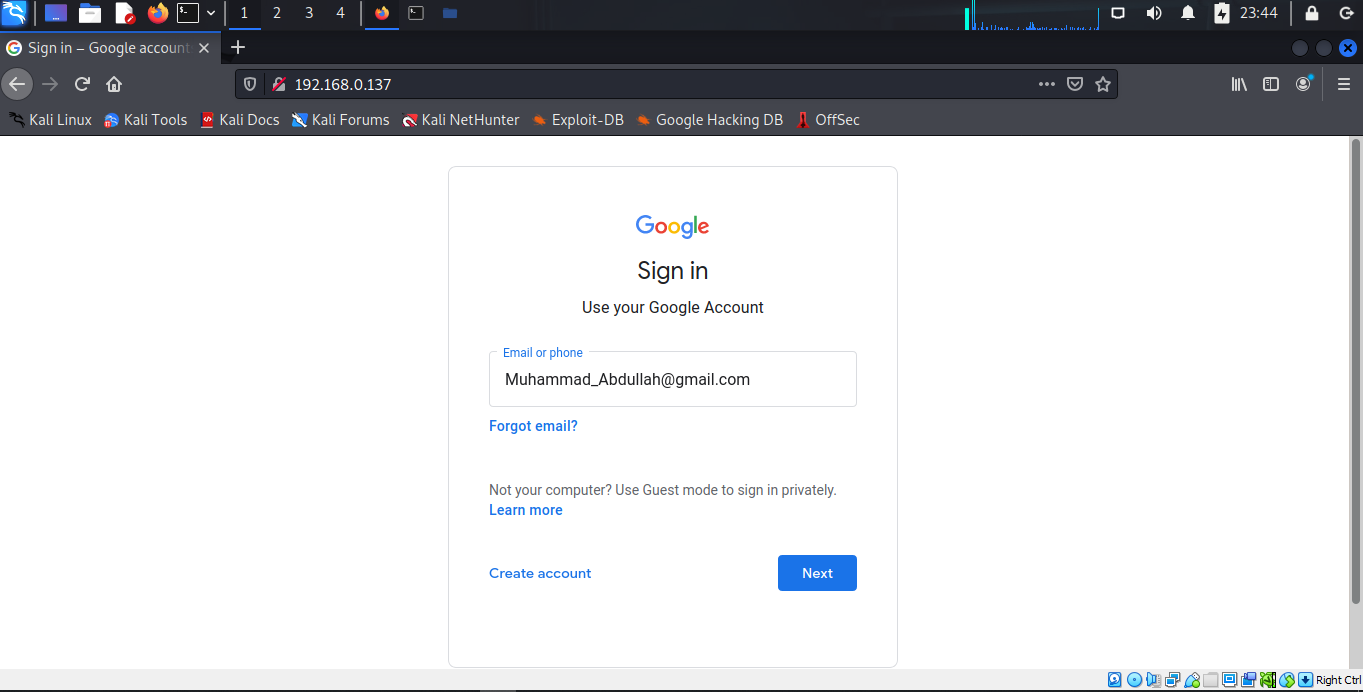
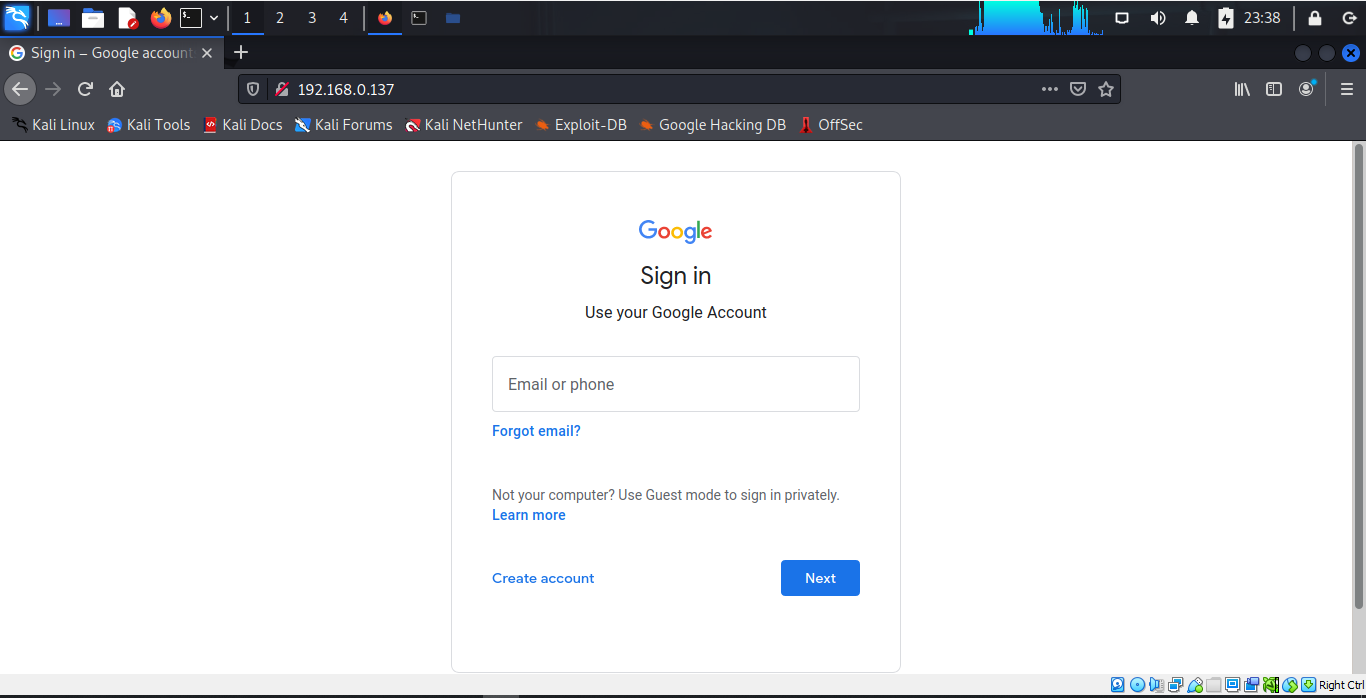
Then selected option # 2: Website attack Vectors

Then Selected 5: web jacking attack method

This is the template of Facebook.com

Its creates an Facebook clone website

Then use another tool for social enginnering 

Then again use of it by using Gmail credentials (S-E-T) 

**Part 2: Provide and describe a real world example where a social engineering tactic was employed in a cyberattack.** (20 marks)

**Ans:**

**$100 Million Google and Facebook Spear Phishing Scam**

The biggest social engineering attack of all time (as far as we know) was perpetrated by Lithuanian national Evaldas Rimasauskas against two of the world’s biggest companies: Google and Facebook. Rimasauskas and his team set up a fake company, pretending to be a computer manufacturer that worked with Google and Facebook. Rimsauskas also set up bank accounts in the company’s name. The scammers then sent phishing emails to specific Google and Facebook employees, invoicing them for goods and services that the manufacturer had genuinely provided — but directing them to deposit money into their fraudulent accounts. Between 2013 and 2015, Rimasauskas and his associates cheated the two tech giants out of over $100 million.

**Russian hacking group targets Ukraine with spear phishing**

As world leaders debate the best response to the increasingly tense situation between Russia and Ukraine, Microsoft warned in February 2022 of a new spear phishing campaign by a Russian hacking group targeting Ukrainian government agencies and NGOs. The group—known as Gamaredon and tracked by Microsoft as ACTINIUM—has allegedly been targeting “organizations critical to emergency response and ensuring the security of Ukrainian territory” since 2021. The initial phase of Gamaredon’s attack relies on spear phishing emails containing malware. The emails also contain a tracking pixel that informs the cybercriminals whether it has been opened. The case is an important reminder of how cybersecurity plays an increasingly central role in international conflicts—and how all organizations should be taking steps to improve their security posture and protect against social engineering attacks.

**Deepfake Attack on UK Energy Company**

In March 2019, the CEO of a UK energy provider received a phone call from someone who sounded exactly like his boss. The call was so convincing that the CEO ended up transferring $243,000 to a “Hungarian supplier” — a bank account that actually belonged to a scammer. This “cyber-assisted” attack might sound like something from a sci-fi movie, but, according to Nina Schick, Author of “Deep Fakes and the Infocalypse: What You Urgently Need to Know”, “This is not an emerging threat. This threat is here. Now.”

**$75 Million Belgian Bank Whaling Attack**

Perhaps the most successful social engineering attack of all time was conducted against Belgian bank Crelan. While Crelan discovered its CEO had been “whaled” after conducting a routine internal audit, the perpetrators got away with $75 million and have never been brought to justice. Crelan fell victim to “whaling” — a type of spear-phishing where the scammers target high-level executives. Cybercriminals frequently try to harpoon these big targets because they have easy access to funds.

**SharePoint phishing fraud targets home workers**

April 2021 saw yet another phishing attack emerge that appears specifically designed to target remote workers using cloud-based software. The attack begins when the target receives an email—written in the urgent tone favored by phishing scammers—requesting their signature on a document hosted in Microsoft Sharepoint. The email looks legitimate. It includes the Sharepoint logo and branding familiar to many office workers. But the link leads to a phishing site designed to siphon off users’ credentials. Phishing attacks increasingly aim to exploit remote collaboration software—Microsoft research suggests nearly half of IT professionals cited the need for new collaboration tools as a major security vulnerability during the shift to working from home.

# Part B: (50/100 marks)

Security Awareness Training:

* 1. Describe the reasoning behind Security Awareness Training and the potential benefits (10 marks)

Include the following in your answer:

* + - The justification for SAT.
    - Business protections provided by SAT.
    - The importance of human factors and training in data security.

Ans:

**SAT**

Security awareness training is a strategy used by IT and security professionals to prevent and mitigate user risk. These programs are designed to help users and employees understand the role they play in helping to combat information security breaches.

*Security Awareness at Your Business*

Make sure you have Policies and Procedures in place.

Learn about and train employees on How to Properly Manage Sensitive Data.

Understand Which Security Tools You Actually Need.

Prepare your employees to Respond to a Data Breach.

Know Your Compliance Mandates.

**Justification for SAT**

Effective security awareness training helps employees understand proper cyber hygiene, the security risks associated with their actions and to identify cyber-attacks they may encounter via email and the web. The primary and foremost objective of any awareness program is to educate users on their responsibility to protect the confidentiality, availability and integrity of their organization's information.

**Business protections provided by SAT**

Prevent Downtime. Should a breach or other security incident occur, it can be costly and take time to repair and reinstate normal business operations. Ensure Compliance. The amount of regulations businesses must adhere to continues to increase. Improve Customer Confidence.

***SAT in the form of Business***

Back up your data.

Secure your devices and network.

Encrypt important information.

Ensure you use multi-factor authentication (MFA)

Manage passphrases.

Monitor use of computer equipment and systems.

Put policies in place to guide your staff.

Train your staff to be safe online.

**Importance of human factors and training in data security**

The 'human factor' has been recognized as the weakest link in creating safe and secure digital environments – but human intuition may also be the solution to thwarting many cyber threats. Every software or security monitoring system requires human interpretation of alerts. Human factors are used by cybercriminals to effect unauthorized access, steal credentials, and infect IT systems and endpoints with malware such as ransomware. Without the human-in-the-machine effect, cybercrime would be much more difficult. Human Factor in Cybersecurity. The human factors in cybersecurity are actions or events that result in a data breach. These factors largely result from a lack of awareness, negligence, or inappropriate access control. Regardless of the reason, the cost of human errors adds up. Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems.

* 1. Practical Security Awareness Training. (20 marks)
     + Outline a plan for a SAT program for a small/medium size organization
     + Produce a 2 page information brochure detailing how the proposed SAT would be delivered to the organization. (you may attach this as appendix)

Ans:

With human error playing a key part in 95% of cybersecurity breaches, managing employee cyber risk is essential for your business to steer clear of a user-related data breach and to demonstrate regulatory compliance.

One core component of a strong human risk management (HRM) program is ongoing security awareness training that educates end-users on how to identify and combat modern threats, as well as best practices for staying security-savvy.

But deciding to launch this type of training comes with some common questions, not least of which is deciding on the security awareness training topics you should be including.

Conduct a session with these topics for awareness of employs

**Phishing attacks**

Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website.

Removable media

**Passwords and Authentication**

Standard password authentication involves a user entering their username, accompanied by a secret code or passphrase that allows them to gain access to a network, account, or application

**Physical security**

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution

**Mobile Device Security**

Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices

**Working Remotely**

Like other jobs in the computer and IT field, cybersecurity jobs are well-suited to remote work. According to the Bureau of Labor Statistics (BLS), employment of information cybersecurity analysts is projected to grow 31% from 2019 to 2029, much faster than the average for all occupations

**Public Wi-Fi**

When using public Wi-Fi, avoid websites that contain your sensitive information such as online banking sites, work-related accounts, insurance sites, online shopping sites, and so on. Use cybersecurity awareness and make sure that the sites you visit have “https” (not "http") at the beginning of the URL

**Cloud Security**

Cloud security is a discipline of cyber security dedicated to securing cloud computing systems. This includes keeping data private and safe across online-based infrastructure, applications, and platforms.

**Social Media Use**

Cybercrime has breached social media networks, thanks to both increased users and increased use. Hackers look for opportunities to gain access to people's accounts, personal or financial information, typically through suspicious links or downloads.

**Internet and Email Use**

Don't provide personal, sensitive, or confidential information online unless you are using a trusted, secure web page. At a minimum, look for “https” in the URL to indicate that there is a secure connection. Get to web sites by typing the web address indirectly. Don't click or cut and paste links in unsolicited emails.

**Social Engineering**

Don't provide personal, sensitive, or confidential information online unless you are using a trusted, secure web page. At a minimum, look for “https” in the URL to indicate that there is a secure connection. Get to web sites by typing the web address indirectly. Don't click or cut and paste links in unsolicited emails.

* 1. Case study (20 marks) Scenario:

*Your client is a growing IT business with 40 staff, 20 of these employees have been*

*recruited in last year. 90% of the staff are currently working from home. The company handles sensitive medical records as part of its typical business practice.*

Considerations

* + - What factors would need to be examined in an audit process?
    - Which risk assessment factors need to be considered?
    - Are there data policy documents which need to be in place?
    - Has the business a continuity plan in the event of a disruption to normal business?

**Work From Home**

Working from home can be great for work-life balance, flexibility and the lack of a commute, but it also brings up a whole host of cybersecurity problems. With employees relying on personal networks and sometimes their personal devices, new online tools and services, and added distractions, it has become a nightmare for an IT team to regulate security measures.

**Research Report 2021**

According to the Velocity Smart Technology Market Research Report 2021, 70% of remote workers said they had experienced IT problems during the pandemic.

**Factors would need to be examined in an audit process?**

* **Unsecure home network connection**

An unsecured network most often refers to a free Wi-Fi (wireless) network, like at a coffeehouse or retail store. It means there's no special login or screening process to get on the network, which means you and anyone else can use it.

* **More use of online tools**

With an increased reliance on technology and online tools, businesses are far more susceptible to cyber threats. More and more tasks are being completed online, from Cloud storage to emails, attachments, instant messengers, third party services and tools such as Teams, Zoom, Hangouts and Asana. This obviously opens up more avenues for cybercriminals to infiltrate company accounts.

* **Employees can’t spot scams**

Tries to gain trust. An online scam will often try to gain your trust in some way.

Emotional. Act now or the IRS will place a lien against your home.

Asks for action.

Unexpected contact.

Asks for personal info.

Overpays you.

Promises something.

Wire transfer request.

* **Weak passwords**

Even if your company makes use of VPNs, firewalls and security software, your business may still be at risk from employees using weak passwords on their accounts. Rather than try to break through tight security infrastructure, cybercriminals will firstly try to crack accounts that may have weak passwords. To do this they use a number of tools, like password generators and coding bots to continuously try and guess passwords and check accounts for repeat passwords.

* **Phishing and ransomware**

According to database, phishing emails have spiked by over 600% since the end of February as cyber-criminals look to capitalize on the fear and uncertainty generated by the COVID-19 pandemic. They work by a criminal posing as a legitimate source, usually over email, to trick the victim into sharing login details or sensitive information. The criminal will then steal this information or lock it and ask for a ransom to be paid.

* **E2E Technologies**

End to End Encryption should be use in their communication. Means If our employees work at their homes then we use VPN with tunneling process or make it end to end encryption like WhatsApp messenger system for chats.

**Protect your business from cyber threats**

Back up your data.

Secure your devices and network.

Encrypt important information.

Ensure you use multi-factor authentication (MFA)

Manage passphrases.

Monitor use of computer equipment and systems.

Put policies in place to guide your staff.

Train your staff to be safe online.

**Disruption to normal business?**

Disruptions to your business can happen at any moment. Business continuity is about having a plan to deal with difficult situations, so your organization can continue to function with as little disruption as possible.

**Business Continuity Planning**

Business Continuity Planning (BCP) is the process of creating preventive and recovery systems to deal with potential cyber threats to an organization or to ensure process continuity in the wake of a cyberattack

Reference websites:

<https://www.infosecurity-magazine.com/>

<https://www.csoonline.com/>

<https://www.troyhunt.com/>

<https://www.lastwatchdog.com/>

<https://www.akamai.com/blog>

<https://krebsonsecurity.com/>

<https://nakedsecurity.sophos.com/>

<https://securityweekly.com/blog>

<https://www.itsecurityguru.org/>