Assignment - 3

Social engineering attack:

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Step-1: Case study analysis

- The attackers conducted extensive research on social media platforms, corporate websites, and professional networking sites to gather information about key employees, their roles, and the internal structure of XYZ Corporation.
- Based on the collected information, the attackers set up a fake login page mimicking the company's internal email system.
- The attackers sent highly targeted spear phishing emails to specific individuals within XYZ Corporation.
- The emails contained a link to the fake login page, urging recipients to log in immediately to review the new policy.

Step-2: Role play exercise:

- Social engineering targets the human factor, exploiting psychological and behavioral aspects. No matter how robust the technical security measures are, people can be manipulated, making social engineering a potent tool for cybercriminals.
- Social engineering attacks can lead to unauthorized access to systems, networks, or physical locations by tricking individuals into revealing passwords, providing access codes, or assisting attackers in circumventing security controls.

- Social engineering is often used to gather valuable information about individuals, organizations, or employees.
- Social engineering attacks may exploit employees within an organization, turning them into unwitting insiders. This can result in data breaches, intellectual property theft, or other malicious activities carried out by individuals who have been manipulated.

Step-3: Phishing email analysis:

- The email header was carefully crafted to mimic a legitimate sender address (hr_update@xyzcorp-emails.com), attempting to deceive recipients into believing it was an internal communication.
- The subject line and body of the email emphasized urgency, creating a sense of fear by stating that failure to verify the account within 24 hours would result in account suspension and potential job repercussions.
- The email included the XYZ Corporation logo and used the company's color scheme to give it an appearance of authenticity, enhancing the chances of successful deception.
- The attackers used social engineering techniques by appealing to the recipients' fear of job repercussions and the urgency of the situation. This emotional manipulation was designed to prompt hasty actions without careful consideration.

Step-4: Documenting the exploit process:

- Document the exploit process, including the commands used , the output received and any challenges

Types of social engineering attack;

Every type of cybersecurity attack involves some social engineering. For example, classic email and virus scams are laden with social overtones. Some of the standard methods used by social engineering attackers are below:

Phishing attack

- **Phishing** attackers pretend to a trusted institution or person in an attempt to convince you to uncover personal data and valuables. Attacks by using phishing are targeted in two ways:

- **Spam phishing** is a widespread attack for some users. The attacks are non-personal and try to capture any irresponsible person.

- **Phishing** and whaling use personal information to target particular users. The whaling attacks are aimed at high-profile individuals such as celebrities, upper management and higher government officials. Whether it is direct communication or by a fake website, anything you share goes directly into the seamster's pocket **.**You can also be fooled into the next stage of the phishing attack malware download. The methods used in phishing are unique methods of delivery.
- **Voice phishing (Wishing)** phone calls can be an automated messaging system recording all your inputs. The person can speak with you to build trust.
- **SMS phishing (SMS)** texts or mobile app messages may indicate a web link or follow-up via a web link or phone number. A web link, phone number, or malware attachment may be used.
- **Angler phishing** takes place on social media, where the attacker mimics the customer service team of a trusted company. They interrupt your communication with a brand and turn the conversations into private messages, where they escalate the attack.
- **Search engine phishing** attempts to place links to fake websites at the top of any search results. The advertisements will be paid or use valid optimization methods to manipulate search rankings. The links are given in email, text, social media messages and online advertisements.
- **In-session phishing** appears as an interruption to the normal web browsing. For example, you can see fake pop-ups on the webpages you are currently viewing.
- **Baiting attack**
- **Baiting** abuses your natural curiosity of exposing yourself as an attacker. The potential for something exclusive is used to exploit us. An attack involves infecting us with malware. Popular methods of baiting are:
    - USB drives are left in public places, such as libraries and parking lots.
    - Email attachment with details with free offer.

Physical breach attack

Physical violations include attackers, who would otherwise present themselves as legitimate to access unauthorized areas or information.

This type of attack is common in enterprise environments, like the government, businesses, or other organizations. Attackers pretend to be a representative of a trusted vendor for the company. Some attackers may have recently been fired in retaliation against their former employers.

- **Preceding Attack:** Trusting uses a misleading identity as a "trust" to establish trusts, such as applying directly to a vendor or facility employee. The approach requires the attacker to interact with you more actively. Once exploited, they are convinced that you are legitimate.
- **Access tailgating attack:** Tailgating or piggybacking is the act of trapping any authorized staff member in a restricted-access area.

Quid pro quo Attack

The term quid pro quo roughly means "a favor for a favor," which refers to exchanging your information for some reward or other compensation in exchange for phishing. Offer to participate in giveaways or research studies may make you aware of this type of attack.

DNS Spoofing and Cash Poisoning Attack

DNS spoofing manipulates your browser and web server to visit malicious websites when you enter a valid URL. DNS cache poisoning attacks infect our device with valid URLs or routing instructions for multiple URLs to connect to fake websites.

Scareware Attack

Scareware is a form of malware that is used to scare you into taking action. The deceptive malware uses dangerous warnings that report fake malware infections or claim that your accounts have been compromised.

Water Hole Attack

Watering hole attacks infect popular web pages with malware to affect multiple users at the same time. Carefully planning on the part of the attacker is required to find vulnerabilities of the specific sites.

Features of Social Engineering Toolkit

- Social Engineering Toolkit is free and open source**.**
- Social Engineering Toolkit is portable, which means we can quickly switch attack vectors.
- Social Engineering Toolkit supports integration with third-party modules.
- Social Engineering Toolkit is already installed in our Kali Linux, but we can also download and install it from Github**.**
- Social Engineering Toolkit is a multi-platform tool; we can run it in Windows**,** Linux**,** and Unix**.**

Running social engineering toolkit

Step 1: our social engineering toolkit will start running.

Select option 1 – social-engineering attack.

Step 2: Now our SEToolkit has been downloaded on our system, it's, time to use it. Now, we have to select the option from the following options. Option 2 is the one we've chosen.

Website attack vectors

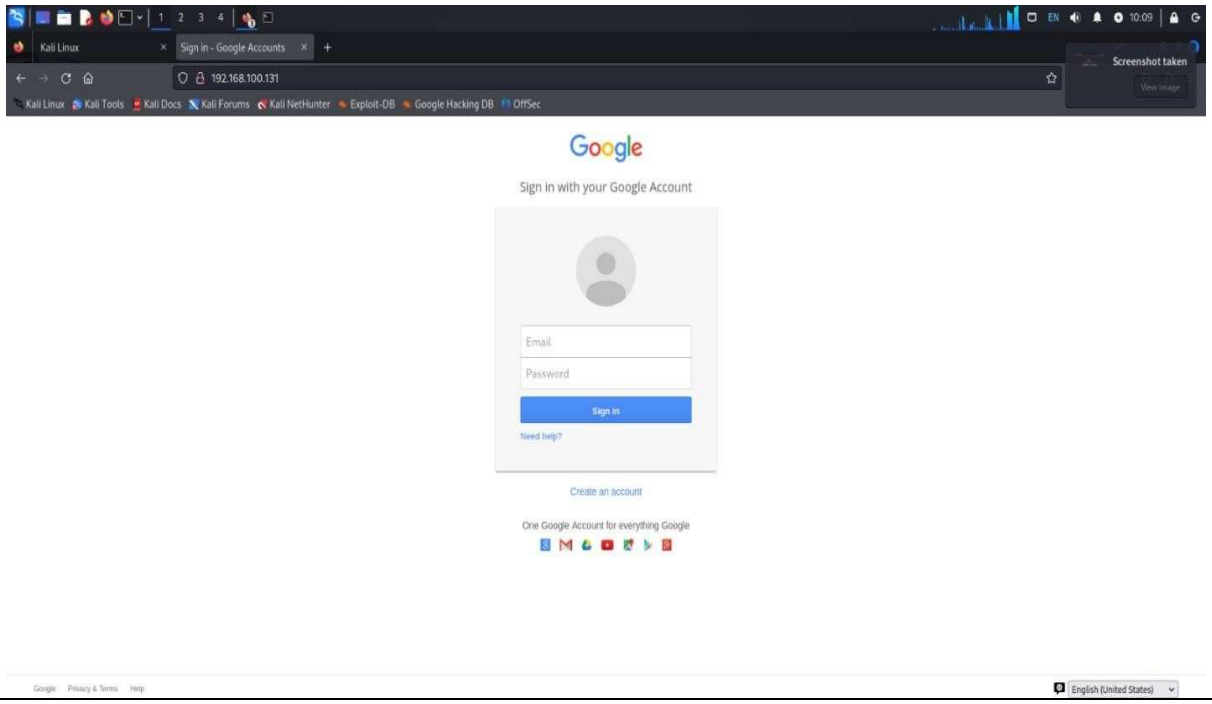
Option 2

Step 3: Now, we are ready to set up a phishing page, we'll go with option 3, which is a credential harvester attack method.

Step 4: Since we are making a phishing page; we'll go with option 1, which is a web template.

Option 1

Step 5: The social engineering tool will now create a phishing page on our localhost.

Step 6: Choose option 2 in order to create a Google phishing page, and a phishing page will be generated on our localhost.

Step 15: A phishing page for Google is being created using the social engineering toolkit. As we can see, SEToolkit generate a phishing page of Google on our localhost (i.e., on our IP address). The social engineering toolset works in this manner. The social engineering toolkit will design our phishing page. Once the victim types the id password in the fields the id password will be shown on our terminal where SET is running.