Task 5: Social Engineering Attacks Report

Internship Program: Oasis Infobyte (OIBSIP)

Submitted By: Daniya Shaikh

Task: Social Engineering Attacks

Introduction

Social engineering is a type of cyber attack that relies on manipulating people into revealing confidential information. Instead of exploiting technical vulnerabilities, attackers exploit human psychology, such as trust, fear, curiosity, and urgency.

These attacks are highly effective because humans are often the weakest link in security systems. Social engineering attacks can occur through emails, phone calls, messages, or face-to-face interactions.

Types of Social Engineering Attacks

1. Phishing

Phishing is the most common social engineering attack. Attackers send fake emails or messages that appear to be from trusted organizations to trick individuals into revealing sensitive information, such as login credentials or financial details.

2. Spear Phishing

Spear phishing targets specific individuals or organizations. Attackers customize messages based on the victim's personal information to increase the likelihood of success.

3. Pretexting

Pretexting involves creating a fabricated scenario to persuade a victim to provide confidential information. Attackers often impersonate authority figures, coworkers, or trusted entities.

4. Baiting

Baiting uses enticing offers to lure victims into a trap. For example, attackers may leave infected USB drives in public places, hoping someone will pick them up and connect them to a computer.

5. Tailgating

Tailgating occurs when an unauthorized person gains physical access to a secure area by following someone with legitimate access. This exploits human politeness or inattentiveness.

6. Quizzes & Surveys

Attackers may use online quizzes, surveys, or competitions to extract personal data from users without raising suspicion.

Common Targets

- Employees of organizations with access to sensitive data

Task 5: Social Engineering Attacks Report

- Individuals with public social media profiles
- High-level executives or decision-makers
- People who are prone to trust emails, phone calls, or websites

---

Preventive Measures

1. **Awareness Training**: Educate employees about different types of social engineering attacks.
2. **Verify Requests**: Always confirm the identity of people requesting confidential information.
3. **Use Multi-Factor Authentication (MFA)**: Adds an extra layer of security.
4. **Strong Password Policies**: Avoid reusing passwords and use strong, unique passwords.
5. **Regular Security Audits**: Identify vulnerabilities and improve security protocols.

Conclusion

Social engineering attacks exploit human psychology rather than technical vulnerabilities, making awareness and vigilance essential. Organizations must train employees, implement security measures, and remain cautious of unsolicited requests to mitigate these threats effectively.