What is Social Engineering: Exploiting Human Psychology in Cybersecurity

Elizabeth Bond

The Knowledge House

Cybersecurity

1. Define what social engineering is as a method of penetration testing.

Social engineering is a method of penetration testing that involves exploiting human psychology and behavior to gain access to sensitive information or systems. It is a non-technical approach to penetration testing that relies on tricking people rather than hacking technology.

According to the National Institute of Standards and Technology (NIST), social engineering is "the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes" (NIST SP 800-53). This can include techniques such as phishing emails, pretexting phone calls, baiting with USB drives, and physical impersonation.

Social engineering is an important component of any comprehensive penetration testing program, as it can help identify weaknesses in an organization's security culture and employee training. However, it should only be conducted by trained professionals and with the organization's permission.

1. Explain how social engineering works and why it is used by cyber criminals.

Social engineering works by exploiting human psychology and emotions to manipulate individuals into divulging sensitive information or performing actions that compromise security (Verizon, 2021). Cyber criminals use social engineering because it is often easier to trick a person into revealing information or taking an action than it is to hack into a system (Verizon, 2021).

There are several techniques that cyber criminals use to carry out social engineering attacks:

1. Phishing: Cyber criminals send fake emails that appear to be from a legitimate source, such as a bank or a social media site. The email may contain a link that takes the victim to a fake website that looks like the real one, where they are prompted to enter their login credentials or other sensitive information (Verizon, 2021).
2. Pretexting: Cyber criminals pretend to be someone else, such as a customer service representative or a law enforcement officer, to gain the victim's trust and obtain sensitive information (Verizon, 2021).
3. Baiting: Cyber criminals leave a physical device, such as a USB drive or a CD, in a public place in the hopes that someone will pick it up and plug it into their computer. The device may contain malware that gives the cyber-criminal access to the victim's system (Verizon, 2021).
4. Spear phishing: Cyber criminals send personalized emails that appear to be from a trusted source, such as a colleague or a friend (Verizon, 2021). The email may contain information that is relevant to the victim's interests or job, making them more likely to respond (Verizon, 2021).

According to the 2021 Verizon Data Breach Investigations Report, social engineering was the second most common tactic used by cyber criminals in data breaches, accounting for 17% of all incidents. The report notes that social engineering attacks are becoming increasingly sophisticated, and that cyber criminals are using a combination of tactics to achieve their goals.

1. Include statistics on social engineering as a form of penetration testing.

The SANS Institute conducts an annual security awareness report that includes statistics on social engineering attacks. The most recent report, the 2021 SANS Security Awareness Report: Managing Human Risk, provides the following insights:

1. In 2020, phishing attacks were the most common type of social engineering attack, with 57% of organizations reporting that they had experienced a phishing attack. (SANS, 2021)
2. Smishing (text message phishing) and vishing (voice phishing) attacks are also becoming more common, with 27% and 22% of organizations reporting that they had experienced these types of attacks, respectively. (SANS, 2021)
3. Social engineering attacks are often successful, with 28% of organizations reporting that they had experienced a data breach as a result, of a social engineering attack. (SANS, 2021)
4. Security awareness training is an effective way to reduce the risk of social engineering attacks, with 70% of organizations reporting that their training programs had helped to reduce the number of successful attacks. (SANS, 2021)

These statistics highlight the continued threat posed by social engineering attacks, and the importance of implementing effective security awareness training programs to mitigate the risks.

1. Discuss what Social Engineer Toolkit (SET - can be used in AWS) is and how it is used (Or discuss another social engineering tool used in pen testing).  You can explain how it is used within AWS (because TKH utilizes AWS) and outside of AWS.

The SANS Institute recommends several social engineering tools that can be used for pen testing. These tools can help security professionals simulate social engineering attacks and assess the vulnerability of an organization to these types of attacks. Some of the tools recommended by SANS include:

1. Social-Engineer Toolkit (SET) - a popular open-source tool that allows security professionals to create a variety of social engineering attacks, such as phishing emails and USB drops.
2. BeEF (Browser Exploitation Framework) - a tool that can be used to test an organization's vulnerability to browser-based attacks, such as clickjacking and cross-site scripting (XSS).
3. Maltego - a data mining tool that can be used to gather information about individuals and organizations for use in social engineering attacks.
4. Recon-ng - a reconnaissance tool that can be used to gather information about an organization's employees, partners, and vendors, which can be used in spear-phishing attacks.
5. SETOOLKIT - a graphical user interface (GUI) for the Social-Engineer Toolkit, which simplifies the process of creating social engineering attacks.

It's important to note that these tools should only be used for ethical and legal purposes, such as during authorized penetration testing engagements. Unauthorized use of these tools can lead to legal consequences.

1. Technical documentation - steps that clearly show how to download, install and use a social engineering tool.

Here are the general steps on how to download, install, and use a social engineering tool in Kali Linux:

1. Download the tool: Navigate to the website of the social engineering tool you want to use and download the appropriate version for Kali Linux.
2. Install the tool: Once the download is complete, open the terminal in Kali Linux and navigate to the directory where the tool was downloaded. Extract the files from the archive and follow the installation instructions provided by the tool's documentation.
3. Launch the tool: Once the installation is complete, launch the tool by typing the appropriate command in the terminal. The tool may have a graphical user interface (GUI) or may be operated from the command line.
4. Configure the tool: Configure the tool according to your needs and the target environment. Make sure to follow the tool's documentation to ensure you are using it properly and ethically.
5. Run the attack: Once the tool is configured, run the attack against the target environment. Make sure to obtain proper authorization and permission before conducting any security testing.
6. Analyze the results: After the attack is complete, analyze the results to identify vulnerabilities and weaknesses in the target environment. Use this information to remediate any issues and improve the overall security of the system.

It is important to note that: unethical use of these tools can have serious consequences and can result in legal and ethical violations.

References

National Institute of Standards and Technology (NIST). (2020). SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

Verizon. (2021). Data Breach Investigations Report. <https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf>

SANS Institute. (2021). 2021 SANS Security Awareness Report: Managing Human Risk. <https://www.sans.org/security-awareness-training/resources/2021-security-awareness-report>