Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Social Engineering

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Chapter Outline

- **Definition, Phases, and Impact**
- **Common Targets and Social Media**

Definition, Phases, and Impact

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

What is Social Engineering

- Any attack that is nontechnical in nature and involves human interaction in some type of way. The attacker preys on the victims ignorance, trust, or moral obligation. Other times they will use threats or promise tremendous rewards for information.
- Why does it work?
  - Lack of a technological fix
  - Insufficient security policies
  - Difficult to detect social engineering
  - Lack of training

Social Engineering Phases

- **Use footprinting methods to gather details about the target.**
  - **Dumpster diving, phishing websites, employees, company tours, etc.**
- **Find a specific person or group who mas access to the information you require.**
  - **Frustrated, overconfident, or arrogant people readily provide information.**
- **Create a relationship with the intended victim through conversation or other means.**
- **Exploit that relationship to gain the desired information.**

Impact of Social Engineering

- **Economic loss**
  - **May cause the victim or the victim's company to lose money through deception, lost productivity, or identity theft.**
- **Terrorism**
  - **The victim can be coerced into actions through threats or physical violence.**
- **Loss of privacy**
  - **The attacker can steal private information.**

Impact of Social Engineering

- **Lawsuits**
  - **The attacker's actions could result in legal troubles for the victim.**
- **Temporary or permanent closure**
  - **Depending on the scope of the attackers breach, the victim's company could be forced to close.**
- **Loss of goodwill**
  - **Due to a breach, the company could lose the good will of the public.**

Common Targets and Social Media

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Common Targets

- **Receptionists**
  - They do not have a security minded role.
  - Usually see when employees come and go from work.
  - Have the ability to hear about a lot of things going on around the office.
- **Help desk personnel**
  - Have valuable information about the infrastructure.
  - Can be accessed through fictious support emails.
- **Executives**
  - Focused on business, sales, and finance; not security.
- **Users**
  - Not prepared for social engineering attacks.
  - Handle day-to-day information.

Social Media

- **Social media is an easy way to gather information because of the amount of data users post.**
  - **Photos**
  - **Location information**
  - **Friend information**
  - **Business information**
  - **Likes and dislikes**
  - **Personal data**
  - **Vacation information**

Social Media

- **Counter measures to limit the threat of social engineering through social media include:**
  - **Always verify contacts and only connect to people you know.**
  - **Avoid reusing passwords across multiple websites.**
  - **Don’t post everything online, specifically avoid posting personal information.**
  - **Keep company information that is shared to a bare minimum.**