CHAPTER 8

Social Engineering and Physical Attacks

Episode 8.01 - Pretext for a Social Engineering Attack

Objective 3.6 Given a scenario, perform a social engineering or physical attack

PRETEXT FOR AN APPROACH

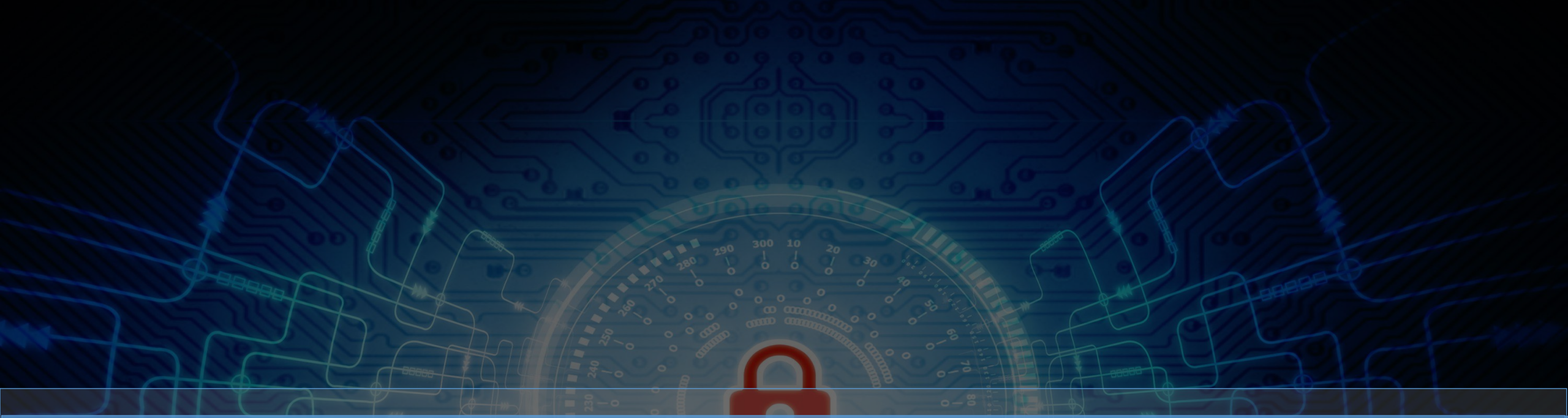
- Why would an attacker choose social engineering?
  - Often easier to trick a human than craft a technical exploit
  - Most people want to be helpful

PRETEXT FOR AN APPROACH

- How would an attacker build a pretext?
  - Encourage victims to do at least some of the work
  - Only resort to technical exploits to carry out what social engineering cannot
  - Build a storyline that sounds plausible and encourages victims to participate
- Social engineering depends on urgency, need, and consequences of inaction

QUICK REVIEW

- It’s often easier to trick a human than it is to trick a computer
- Pretext encourages victims to do some of the work
- Social engineering depends on urgency, need, and the consequences of inaction



Episode 8.02 - Remote Social Engineering

Objective 3.6 Given a scenario, perform a social engineering or physical attack

SOCIAL ENGINEERING

- Tricking or coercing people into violating security policy
- Depends on willingness to be helpful
- Human weaknesses can be leveraged
- May rely on technical aspects
- Bypasses access controls and most detection controls

PHISHING

- Phishing – people are contacted by a seemingly legitimate imposter in an attempt to extract sensitive information
  - Spear phishing
  - SMS phishing
  - Voice phishing
  - Whaling

QUICK REVIEW

- Social engineering is all about getting an authorized user to do your dirty work
- Relies on most peoples' willingness to be helpful
- Successful social engineering can bypass nearly all technical controls
- Phishing is attempting to get a valid user to click on a link to your exploit

Episode 8.03 - Spear Phishing Demo

Objective 3.6 Given a scenario, perform a social engineering or physical attack

PHISHING DEMO

- Phishing Demo

QUICK REVIEW

- Spear phishing is all about targeting a specific individual
- Crafting a realistic email is crucial
- The goal is to get a user to click on the link you sent without too much prior thought

Episode 8.04 - In-Person Social Engineering

Objective 3.6 Given a scenario, perform a social engineering or physical attack

MORE ATTACKS AND EXPLOITS

- Elicitation
  - Gathering info about a system from authorized users
- Interrogation
  - Informal interviews with crafted questions to extract info
- Impersonation
  - Pretending to be someone with authority
- Shoulder surfing
  - Watching as someone enters a username, password, PIN, etc

USB KEYS AND SOCIAL ENGINEERING

- USB key drop
  - Weaponized USB keys placed where users might pick them up and insert them into their own computers

MOTIVATION TECHNIQUES

- Motivation techniques
  - Authority
  - Scarcity
  - Social proof
  - Urgency
  - Likeness
  - Fear
- People want to be accepted and valued by others

QUICK REVIEW

- In-person social engineering often works because few people will confront someone face-to-face
- A good social engineering attacker can smooth talk their way around many controls
- Many computer users fail to understand how dangerous USB keys can be
- Dropped USB keys will often be easy access points to victim computers