CS 465

Social Engineering

Slides by Kent Seamons and Tim van der Horst
Last Updated: Nov 30, 2011

Social Engineering

Source:

The Art of Deception
Controlling the Human Element of Security

By Kevin Mitnick and William Simon

Information Security Awareness and Training

- No technology in the world can prevent social engineering attacks
- Some authorities recommend 40% of an overall security budget be targeted to awareness training

Six Tendencies of Human Nature

- Authority
  - Comply with a request from someone of authority
- Liking
  - Comply with a request from someone we like
- Reciprocation
  - Comply with a request when we are promised or given something of value
- Consistency
  - Comply after we have committed to a specific action
- Social Validation
  - Comply when doing something in line with what others are doing
- Scarcity
  - Comply when we believe the object sought is in short supply and others are competing for it, or it is available for a short period of time

Foiling Attacks

- Most attacks could be foiled if the victim simply follows two steps
  - Verify the identity of the person making the request
  - Verify whether the person is authorized

Social Engineering at BYU

- http://newsnet.byu.edu/story.cfm/37221

Advanced Persistent Threat

- Social engineering is the catalyst for many Advanced Persistent Threat (APT) attacks
  - Stuxnet was assisted through USB drives
  - Penetration testers gain a foothold using social engineering
    - Research VPs and send targeted emails with infected pdf files
    - Pose as cleaning crew inspector and plant infected USB drives

Common Social Engineering Methods

- Posing as a fellow employee
- Posing as an employee of a vendor, partner company, or law enforcement
- Posing as someone in authority
- Posing as a new employee requesting help
- Posing as a vendor or systems manufacturer calling to offer a system patch or update
- Offering help if a problem occurs, then making the problem occur, thereby manipulating the victim to call the attacker for help

Common Social Engineering Methods

- Sending free software or patch for a victim to install
- Sending a virus or Trojan Horse as an email attachment
- Using a false pop-up window asking the user to log in again or sign on with password
- Capturing victim keystrokes with expendable computer system or program
- Leaving a floppy disk or CD around the workplace with malicious software on it

Common Social Engineering Methods

- Using insider lingo and terminology to gain trust
- Offering a prize for registering at a Web site with username and password
- Dropping a document or file at company mail room for intra-office delivery
- Modifying fax machine heading to appear to come from an internal organization
- Asking receptionist to receive and forward a fax

Common Social Engineering Methods

- Asking for a file to be transferred to an apparently internal location
- Getting a voice mailbox set up so callbacks perceive attacker as internal
- Pretending to be from a remote office and asking for email access locally

Warning Signs of an Attack

- Refusal to give a callback number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of noncompliance
- Shows discomfort when questioned
- Name dropping
- Compliments or flattery
- Flirting

Common Targets of Attacks

- Unaware of value of information
  - Receptionists, telephone operators, admin assistants, security guards
- Special privileges
  - Help desk or technical support, system admins, computer operators, telephone sys admins
- Manufacturer/Vendor
  - Computer hardware, software manufacturers, voice mail systems vendors
- Specific departments
  - Accounting, human resources

Factors that Make Companies More Vulnerable to Attacks

- Large number of employees
- Multiple facilities
- Information on employee whereabouts left in voice mail messages
- Phone extension information made available
- Lack of security training
- Lack of data classification system
- No incident reporting/response plan in place