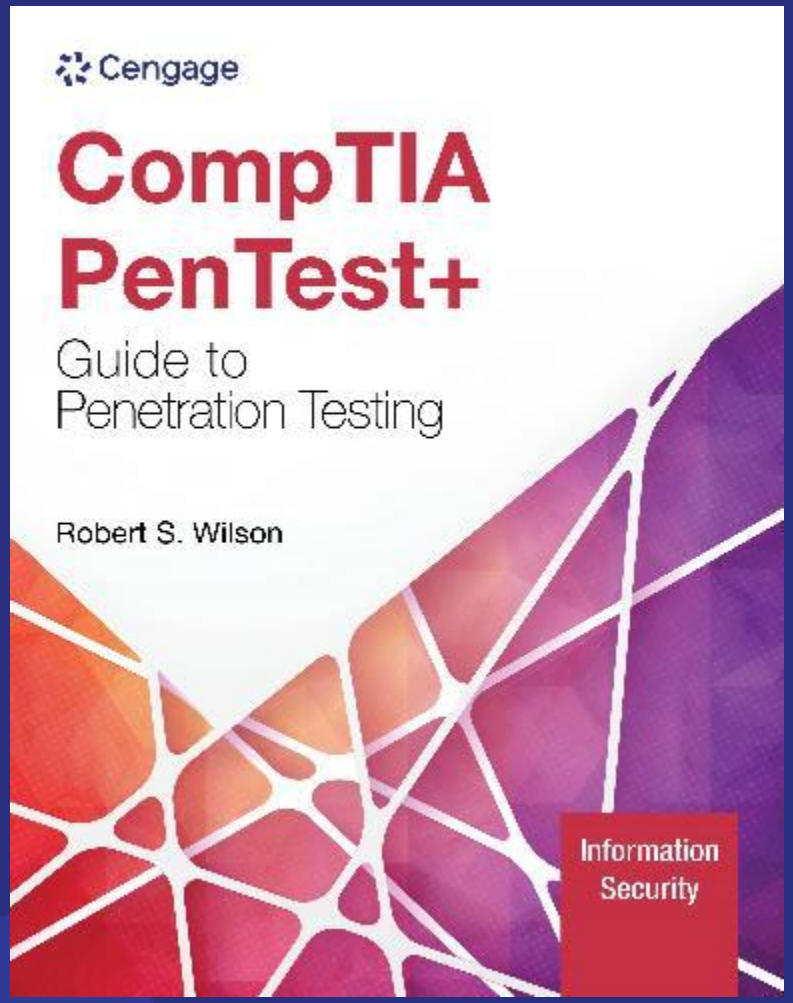


CompTIA PenTest+ Guide to Penetration Testing, 1e

Module 11: Social Engineering and Physical Attacks

Module Objective

By the end of this module, you should be able to:

1. Describe social engineering and its motivations
2. Describe the psychology of social engineering and the aspects of human nature that can be leveraged by social engineers
3. Describe the tactics used in person-to-person social engineering
4. Describe some of the technology and technology-based attacks used in social engineering
5. Describe social engineering tools
6. Describe social engineering physical attacks and methods

Social Engineering (the Art of the Con) (1 of 7)

Setting the Stage

- Social engineering – threat actor manipulating a person with intent to trick them into performing actions to compromise personal or organizational security
- Social engineers are con artists who practice in the technical realm
- Human vulnerabilities are targets for social engineer exploitation
- Email, text messages, web sites, phone calls, or in-person attacks occur
- Pen testers seek to find and mitigate weakness in processes, procedures, and security that allow for social engineer success

Social Engineering (the Art of the Con) (2 of 7)

Setting the Stage

- Social engineers typically create a pretext for an approach or a believable situation that legitimizes the threat actor
- Simple or complex believable scenarios increase attack success
  - Creating a plausible situation that the victim will believe and will compel them to take action
  - Creating a character or persona that the victim will believe is legitimate
- Once target is convinced, threat actor launches call to action: what action the attacker wants target to perform

Social Engineering (the Art of the Con) (3 of 7)

Setting the Stage

- Goal of a social engineering attack will drive the pretext
- Motivation of the social engineering ploy may include:
  - Activist cause
  - Fun or prank
  - Ego
  - Gain of knowledge or insider info
  - Revenge
  - Theft of money or financial motive
  - Pen testing
- Example scenario: Calls, emails, or text messages from a fake security company claiming a technical emergency on the victim's computer that must be remedied immediately
  - Motivation or goal is to get victim to give attacker login credentials

Social Engineering (the Art of the Con) (4 of 7)

The Psychology of Social Engineering

- Understanding human nature is key to successful social engineering
- Attackers employ innate human nature to exploit them or use their internal drive
  - Trust – victim must experience trust to perform attacker request
  - Authority – power to request desired action
  - Urgency – helps drive victim to quick action without typical caution
  - Fear – if potential harm is possible, victim may yield to attacker's will

Social Engineering (the Art of the Con) (5 of 7)

The Psychology of Social Engineering

- Attackers employ human's innate nature to exploit them or use their internal drive (continued)
  - Scarcity – quick victim action required or opportunity may be missed
  - Helpful nature – human trait to provide assistance often exploited
  - Similarity – Relationship or commonality of victim with threat actor may generate victim motivation
  - Reciprocation – making victim feel indebted can be leveraged to perform reciprocal task for attacker

Social Engineering (the Art of the Con) (6 of 7)

Person-to-Person Social Engineering

- Threat actors may choose to engage a social engineering target directly
- Impersonation – may involve dressing in a disguise or even in authentic uniforms as part of the social engineering attack
- Friendly Elicitation – direct questioning of a target may arouse suspicion
  - Friendly chitchat more successful in drawing out info
- Quid Pro Quo – threat actor may give or offer something of value to victim in attempt to make them feel indebted and return favor

Social Engineering (the Art of the Con) (7 of 7)

Person-to-Person Social Engineering

- Interviews and Interrogation – controlling the conversation with the intended victim, making them feel at ease while seeking information
  - Interrogation is much less friendly engagement with target
- Shoulder Surfing – peeking at a victim as they perform an action such as typing a password or PIN, directly in person or at distance with binoculars
- Bribery – not-so-subtle tactic to gain information from target by way of money or another valuable gift
  - Bribery in many circumstances may be illegal

Discussion Activity 11-1

Some would consider social engineering an art form, and much can be said about the skillsets that help make an effective social engineer.

Discuss what personality traits might make a person a successful social engineer. Will these traits vary based on the type of social engineering being attempted? Are there traits that would preclude someone from being a good social engineer?

Using Technology for Social Engineering (1 of 11)

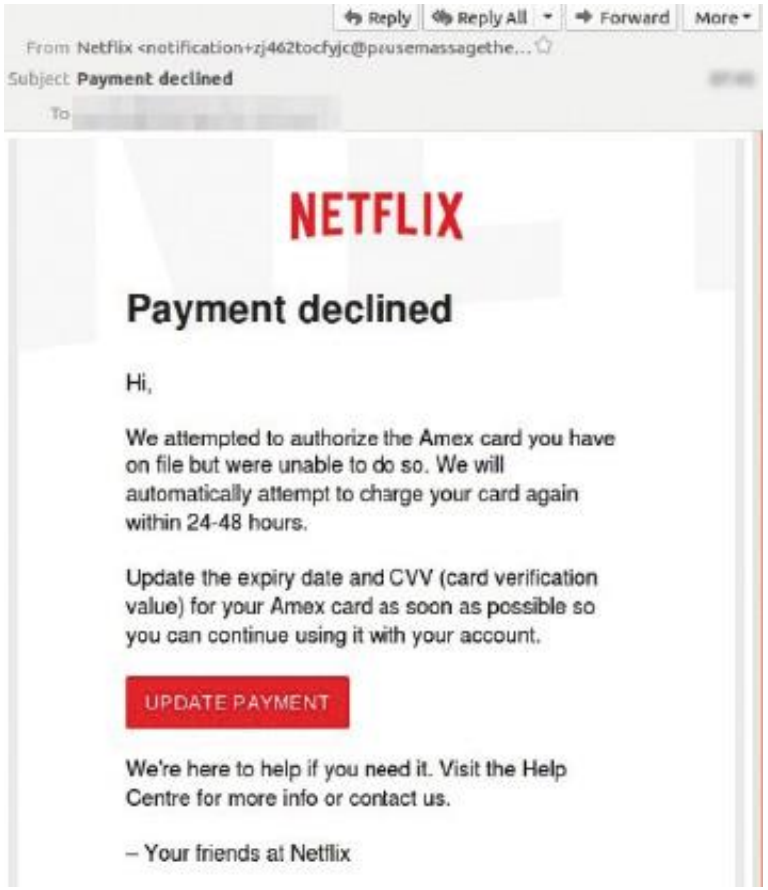
Phishing Attacks

- Phishing uses messaging technology to send unsolicited messages to targeted victims in hopes of getting them to unintentionally divulge sensitive info
- Traditional phishing uses email, and today threat actors use varying types of mail and employ psychological tactics to increase success
- Phishing emails may direct recipient to URL/web site or may seek reply with requested information
- Messages may replicate style and content of legitimate messages recipients may receive but have tricks to fool them into performing an action or disclosing sensitive information

Using Technology for Social Engineering (2 of 11)

Phishing Attacks

- Ways to detect phishing emails include but are not limited to:
  - Spelling and grammar mistakes in the message
  - Email address does not match the sending company's domain
  - Inaccurate information in the message



Example phishing email

Using Technology for Social Engineering (3 of 11)

Phishing Attacks

- Phishing attacks have evolved to include attacks of more specific targets and modern types of messaging technology
  - Spear phishing – targeting a specific group of people; for example, one department as a target rather than the whole organization
  - Whaling – phishing high-profile target such as a CEO, InfoSec Director
  - SMS phishing/smishing – phishing using SMS or text messages
  - Voice phishing/vishing – using phone calls as phishing communication technology

Using Technology for Social Engineering (4 of 11)

Website-Based Attacks

- Websites can be main vehicles for social engineering attacks or part of support for other forms
- Cloned Websites – attackers may clone exact replicas of legitimate sites but with poisoned or malicious links and files or username and password fields that direct received input to the attacker
- Watering Holes – threat actor performs recon to determine a site that may be frequented by members of target organization
  - Identified website may be targeted for compromise and weaponized
  - Example: compromise trade group site associated with victim's field

Using Technology for Social Engineering (5 of 11)

USB Drop Attacks

- Placing malware on removable media like USB thumb drive, or multiple drives and leaving them where targets may find them
- Malware may auto-launch when drive plugged in, compromising system
- Auto-spreading worms may also run from plugged-in drive
- System can be used as desired by attacker after compromise
- 2010 Stuxnet attack employed USB drop attack as part of the breach

Using Technology for Social Engineering (6 of 11)

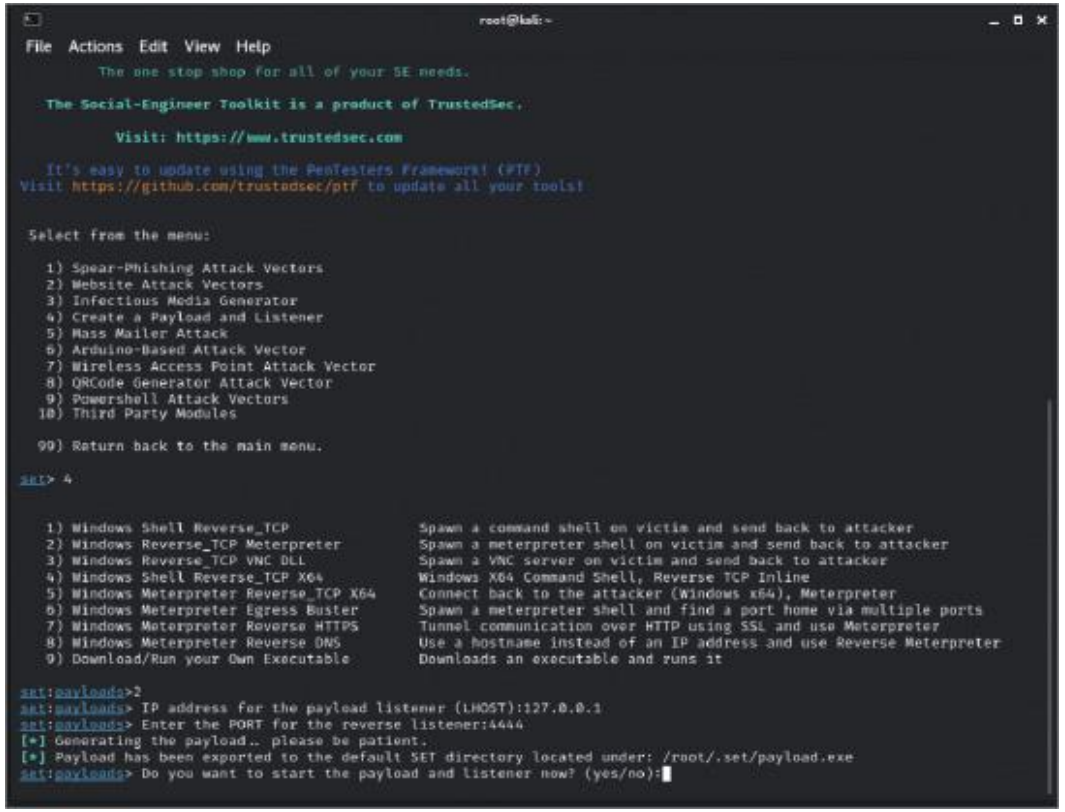
Social Engineering Tools

- Pen testers have a surprising array of tools to make social engineering more efficient, reliable, and easier than it previously was
- Social Engineering Toolkit – command-line tool included in Kali Linux
- SET integrates with Metasploit to extend functionality
- Various SET attacks include spear phishing, website attacks, mass mailer attacks, and SMS spoofing

Using Technology for Social Engineering (7 of 11)

Social Engineering Tools – Social Engineering Toolkit

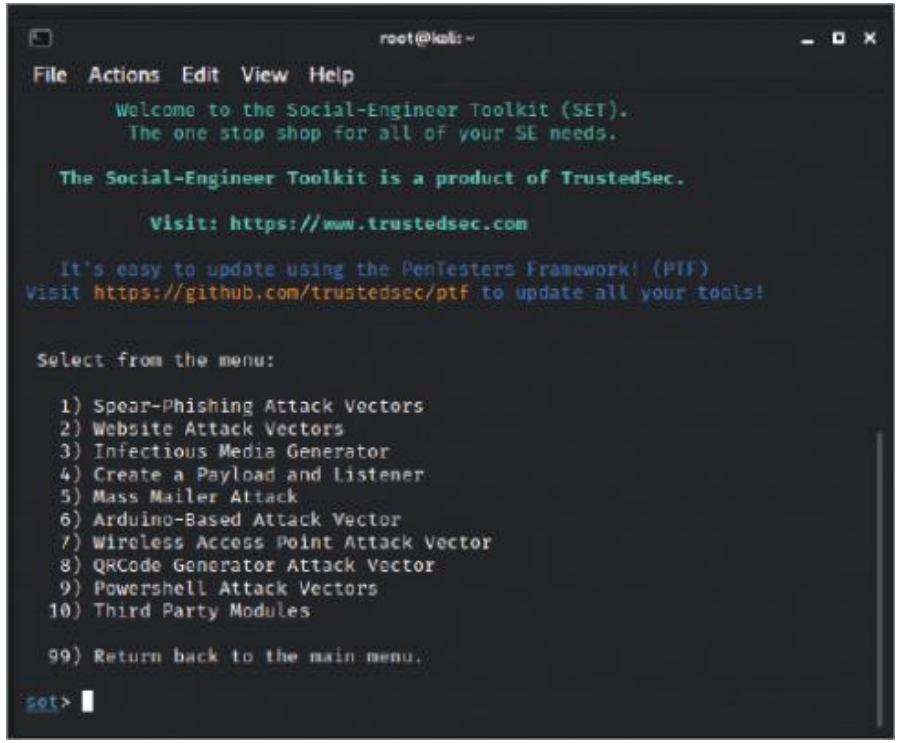
SET menu



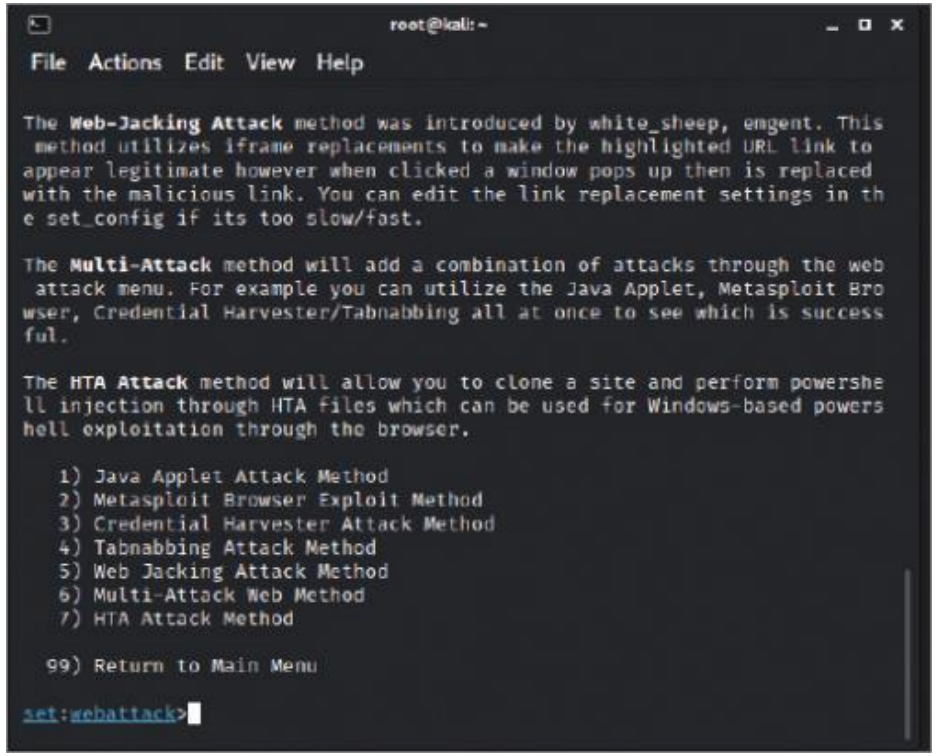
SET using Metasploit

Using Technology for Social Engineering (8 of 11)

Social Engineering Tools – Social Engineering Toolkit



SET Social engineering menu

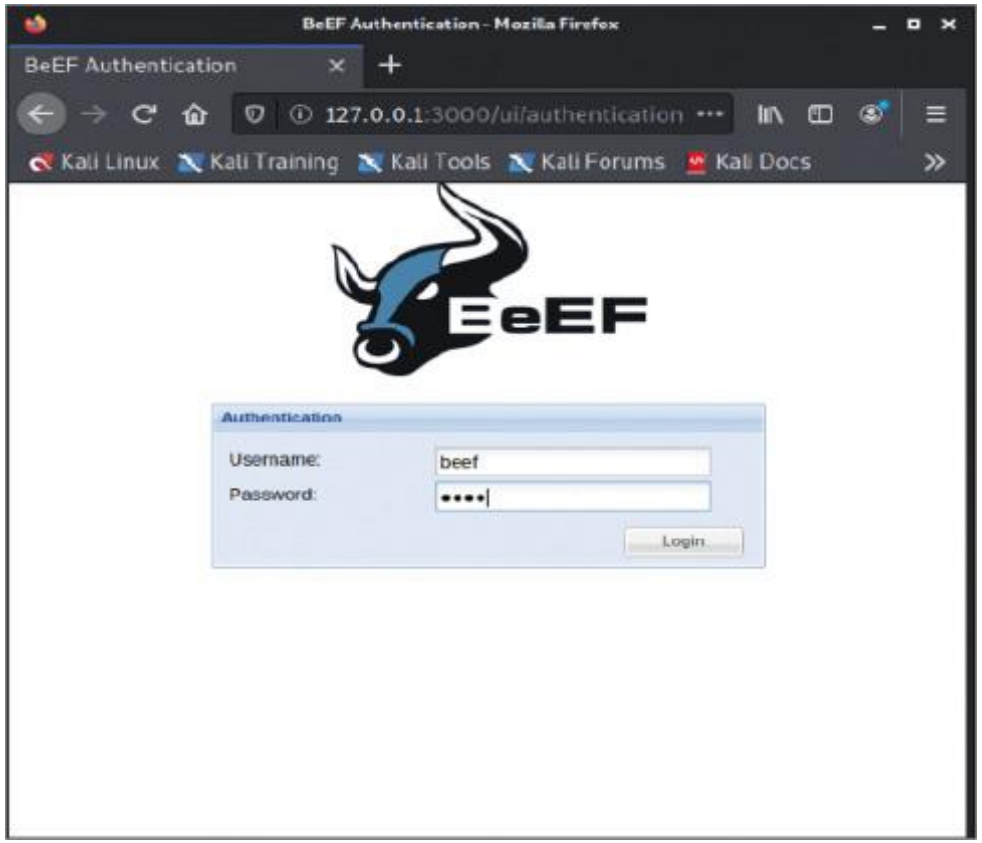


SET Website attack vectors menu

Using Technology for Social Engineering (9 of 11)

Social Engineering Tools

- Browser Exploitation Framework (BeEF)
- BeEF is a pen-testing tool to gain control over target's web browser
- Accomplished through command-and-control code injection of "hook" on compromised site visited by target
- JavaScript hook code allows for browser manipulation by BeEF if run on target browser

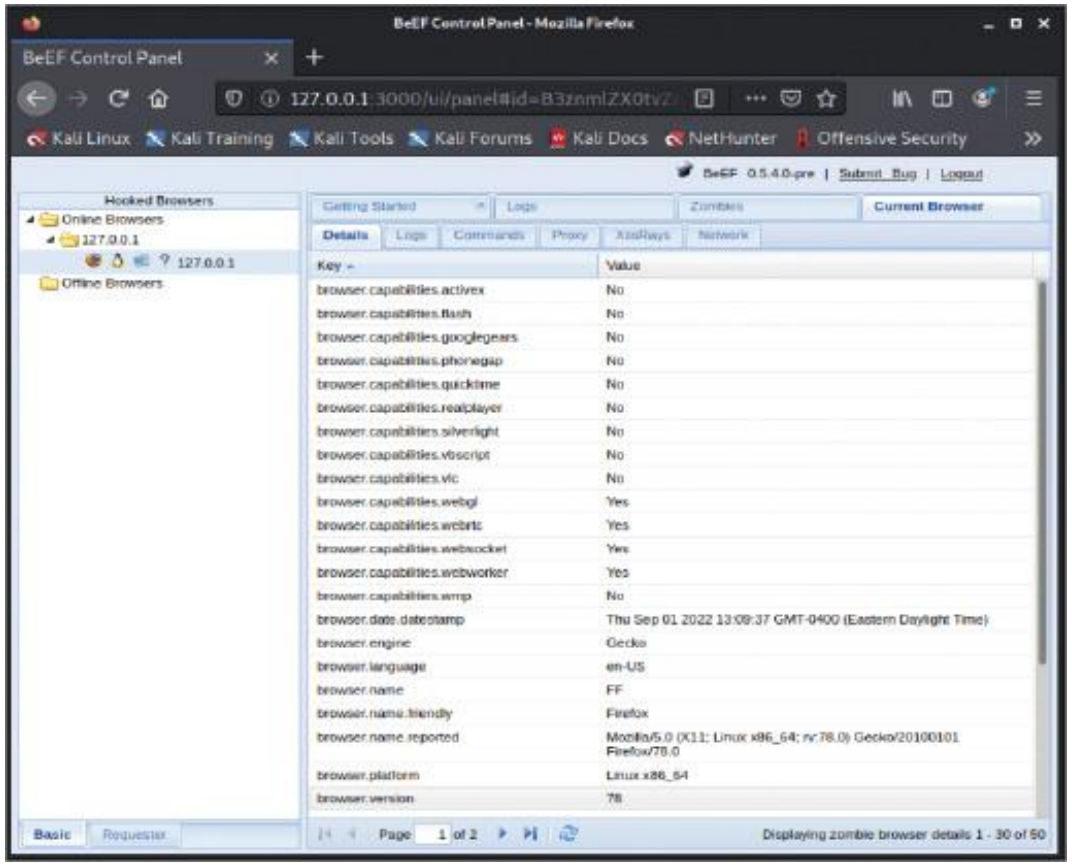


BeEF login page

Using Technology for Social Engineering (10 of 11)

Social Engineering Tools

- Browser Exploitation Framework (BeEF)
- Browser hooked by BeEF can leak information from target
- BeEF Control Panel hosts many attack capabilities, including requesting access to webcam and microphone and launching malicious code



BeEF hooked website information

Using Technology for Social Engineering (11 of 11)

Social Engineering Tools

- Session Initiation Protocol (SIP) INVITE and Viproy
- Voice over IP (VoIP) includes telephony protocols such as SIP that allow for voice calls over internet protocol networks
- INVITE is Metasploit tool that allows spoofing phone calls to targets so appears as if calls come from incorrect source number
- Viproy performs pen-testing attacks across VoIP networks
- Both tools commonly used for vishing targets

Physical Attacks (1 of 6)

In-Person Physical and Remote Attacks

- Physical access to a computer system typically will result in greater level of access and control than remote access
- Physical access allows for actions such as booting system from a USB drive with a different operating system and many other possibilities
- Physical attacks during a pen test may check:
  - Security personnel
  - Security procedures
  - Entry control systems
  - Surveillance systems
  - Barriers and fences

Physical Attacks (2 of 6)

In-Person Physical and Remote Attacks

- Physical attacks must be planned and conducted with professionalism and within the SOW and ROE
- Gaining access to an unexpected or unauthorized area may result in tense situations; security or police may be summoned
- Alert Stakeholders and Contacts
  - Procedures and process for physical attacks should be in pen-test engagement agreements
  - Key personnel specified should be notified according to ROE, SOW

Physical Attacks (3 of 6)

In-Person Physical and Remote Attacks

- Reconnaissance – gathering data on target facilities is as important for physical access test as for electronic pen tests
- Laying the Groundwork – observing personnel and normal operations at a target facility can help with physical access test strategy
- Knowing access control methods for authorized personnel and entry points may help plan attack impersonating a target's employees
- Understanding times when shifts change, deliveries occur, and breaks and lunches are taken can also be of value

Physical Attacks (4 of 6)

Using Impersonation to Enter a Facility

- Looking and playing the part of an authorized person or guest increases likelihood of success
- Wearing costume or using props is common technique for social engineers who specialize in physical tests
- Being prepared with fake ID badges and names of real employees may help talk one's way into facility or out of a jam
- Impersonation can invite trouble, so be ready with contact info for target personnel that can vouch for the validity of activity

Physical Attacks (5 of 6)

Dumpster Diving

- Searching through and gathering discarded materials may result in surprisingly useful reconnaissance data for further activities

Badge Cloning

- RFID badges and similar may easily be cloned and provide tester access to target facility

Jumping the Fence

- Some facilities lend well to scaling fences or similar barriers
- Can be exceptionally dangerous when considering electrified fences and facility protections and access impediments

Physical Attacks (6 of 6)

Attacks on Locks and Entry Control Systems

- Lock picking has long been a pastime of security pros and pen testers
- Legality of lock picking and owning equipment should be confirmed
- Access to a facility master key is unlikely, unless provided, but is invaluable
- Bumping, or gently tapping key into keyhole while turning bump key, may result in some doors or locks being opened
- Many resources and groups are available to learn more about lock picking and related topics

Discussion Activity 11-2

Physical access control testing is not an activity that many associate with information security professionals. In some pen-test organizations, team members with different educational backgrounds, work experiences, or even personality traits may be the testers commonly assigned to or most successful at targeting physical attacks.

What traits, experiences, or education might make an individual particularly well suited to performing physical attacks?

Summary

By the end of this module, you should be able to:

1. Describe social engineering and its motivations
2. Describe the psychology of social engineering and the aspects of human nature that can be leveraged by social engineers
3. Describe the tactics used in person-to-person social engineering
4. Describe some of the technology and technology-based attacks used in social engineering
5. Describe social engineering tools
6. Describe social engineering physical attacks and methods