Performing Non-Technical Tests

- Perform Social Engineering Tests
- Perform Physical Security Tests on Facilities

Basic Components of Social Engineering Attacks

- Target evaluation
  - Assess target's susceptibility to attack and their awareness of cybersecurity.
- Pretexting
  - Communicate a lie or incomplete truth to get victim to believe a falsehood.
- Psychological manipulation
  - Exploit human decision making and cognitive biases to craft more effective attacks.
- Building relationships
  - Get victim more friendly and comfortable to enhance trust level.
- Motivation
  - Motivate target to take action.

Motivation Techniques

Motivation Technique	Description
Authority	• People tend to obey authority figures. • Example: Attacker posing as police officer.
Scarcity	• People attach value to uncommon objects/ideas. • Example: Attacker rewarding victim with unique collectible.
Urgency	• People attach value to temporary objects/ideas. • Example: Attacker giving a "limited time offer."
Social proof	• People tend to want to fit in and conform with a group. • Example: Attackers install fake AV, victim does the same to appear competent.
Likeness	• People are more trusting of those like them. • Example: Attacker tries to be charming and persuasive to specific people.
Fear	• People will do irrational things to purge themselves of fear. • Example: Attacker convincing a victim they will lose money if they don't comply.

Phishing (Slide 1 of 2)

A tactic in which an attacker attempts to obtain sensitive information from a user by posing as a trustworthy figure through email.

- Also used more generally to refer to any such trick over electronic communications.
- One of the most common and effective social engineering tactics.
  - Easy to distribute.
  - Impersonal.
  - Can leverage technical tricks like spoofing FROM headers.
- Example: Attacker sends email claiming to be from victim's bank.
  - Contents tell victim to send their password so account can be reset.
  - If victim doesn't comply, bank will terminate the account.
  - Leverages urgency and fear as motivators.
  - Victim receives email with spoofed headers and thinks it's legitimate.
  - Victim complies with fraudulent request.

Phishing (Slide 2 of 2)

Subject: Parcel ID0000606787 delivery problems, please review
From: "FedEx TechConnect" <floyd.gregory@antonystagg.com>
Date: 12/9/16 7:50 pm
To: [redacted]

Dear Customer,

Your parcel was successfully delivered December 07 to FedEx Station, but our courier cound not contact you.

Please review delivery label in attachment!

Thank you,
Floyd Gregory,
Office Clerk.

Types of Phishing (Slide 1 of 2)

- SMiShing
  - Phishing done over text messages (SMS).
  - Users may ignore unknown texts more readily than email.
- Vishing
  - Phishing done over telephone/VoIP.
  - Real-time voice conversations can generate more trust.
- Pharming
  - Phishing that entices users through a spoofed website.
  - Victim interacts with site to provide info.

Types of Phishing (Slide 2 of 2)

- Spear phishing
  - Phishing that targets specific individuals or groups.
  - Customized messages are more effective.
- Whaling
  - Spear phishing that targets wealthy and/or powerful people.
  - High risk, high reward.

Impersonation

The act of pretending to be someone you are not.

- Many social engineering attacks use impersonation.
- Relies on target not being able to identify attacker.
- Example: Attacker pretends to be a help desk worker.
  - Calls employee and asks for their password.
  - Target may be less suspicious if they don't know who works at the help desk.
- Can be more effective in face-to-face interactions.
  - People want to avoid appearing rude or dismissive.
  - May be less likely to question an impostor.
  - Relies on target not knowing what the real person looks like.

Elicitation (Slide 1 of 2)

The process of collecting or acquiring data from human beings.

- Different than information gathered *about* human beings.
- People may themselves provide key insight.
  - Certain knowledge may only be available this way.
- An approach used in social engineer attacks.
- Specific types:
  - Requests
  - Interrogation
  - Surveys
  - Observation

Elicitation (Slide 2 of 2)

- BEC often uses elicitation.
  - Attacker impersonates executive.
  - Sends email to financial personnel requesting transfer of funds.
  - Personnel approves transfer.

Subject: Payment --URGENT--
From: "Carl Henderson" <carl.henderson@greenecityphysicians.com>
Date: 1/3/18 3:05 pm
To: maria.nunes@greenecityphysicians.com

Hi Maria,

Check the enclosed for instructions on a payment that was supposed to go out last week. Please process ASAP.

Thanks,
Carl Henderson, CFO
Greene City Physicans Group

Hoaxes (Slide 1 of 2)

An element of social engineering in which the attacker presents a fictitious situation as real.

- Similar to a scam, but not always about the money.
- Examples:
  - Antivirus warnings that are themselves malware.
  - Emails that request an advanced payment to access larger sums of money in the future.
  - Emails that say an account has been flagged for suspicious activity.
  - Blog posts offering false advice that leads to damage.

Hoaxes (Slide 2 of 2)

Subject: Humbly requesting your assistance
From: "John Baker" <john.baker@googlemail.example>
Date: 4/21/18 12:23 pm
To: fred.michaels@greenecityphysicians.com

Dearest Sir,

I hope you are doing well and that your family is joyful in this time. I am corresponding to inform you of a **great opportunity** that will benefit myself and yourself financially.

My name I John Baker, and I recently returned to my home nation of England after visiting the nation of Nigeria. I am a bank officer and just learned of an account that was opened in our bank in the year **2008**. According to our records, none has accessed this account since 10 years. This account was opened by the late **Solomon Okafor**, a respectable Nigerian prince who recently passed. Mr. Okafor had no next of kin and I have come to the conclusion that no man in his country is aware of this account.

I therefore seek a reliable individual such as yourself that will play the role of next of kin in extracting the funds totaling **£4,000,000.00**. If this matter is not settled urgently then the Treasury of England will claim the account. I am willing to offer you 40% of the available funds with the remaining 60% applying to my own self.

Please respond swiftly and we will get this matter settled.

Yours truly,
John Baker

Baiting

A social engineering attack in which an attacker leaves physical media in a location where someone else might pick it up and use it.

- Exploits people's natural curiosity.
- Unusual objects/situations can catch the eye.
- Commonly used to leave USB drives in public near a workspace.
  - Employee picks up drive and plugs it into their computer.
  - Drive has been pre-loaded with malware.
- More effective if autorun is enabled.
  - Infection happens automatically and can spread within the network.
- Malicious code can be disguised if autorun is disabled.
  - Something fun
  - Something useful
  - Something mysterious

URL Hijacking (Slide 1 of 2)

A social engineering attack in which an attacker exploits the typing mistakes that users may make when attempting to navigate to a website.

- Also called typosquatting.
- Example: Typing **comtpia.org**.
  - Browser doesn't know this is a mistake.
  - User is sent to literal website.
  - Attacker already registered domain.
- Typosquatted domain may be overtly malicious or look similar to the real thing.

URL Hijacking (Slide 2 of 2)

- Also encompasses:
  - Wrong TLD (**comptia.gov**).
  - Obfuscated subdomains (**login.comp.tia.org**).
  - Different word form (**thecomptia.org**).
- Companies expend effort to combat this.
  - Some URLs fall through the cracks.

Spam and Spim

Spam: An attack where the user's inbox is flooded with unsolicited messages.

- Advertisements, promotions, get-rich-quick schemes, etc.
- Initially referred to email only, but the term may be used more generally.
- Often used in conjunction with phishing.
- Spim is spam over IM.
  - Attacker might send a message over Facebook.
  - Promises a great deal on a product by following a link.
  - Harder to pull off due to IM's synchronous nature.
  - Still known to work on non-tech-savvy users.
- Filters in email/IM clients make spam/spim less effective.
  - Volume is still so great that it snares users every day.

Shoulder Surfing

A social engineering attack in which the attacker observes a target's behavior without the target noticing.

- Target is typically at their computer.
  - Working on sensitive info.
  - Typing credentials.
- Attacker is behind target and sees what's on the screen or keys being pressed.
- Not always literally looking over target's shoulder.
  - Can record behavior with a camera from a distance.
  - Recording exists for future reference.
  - Can just leave camera while it's recording and walk away.
  - Return later to obtain footage.

Tailgating

An attack where the attacker slips in through a secure area while following an authorized employee.

- Employee doesn't know anyone is behind them.
- Example: Employee enters lobby using an access card on locked entrance.
  - Swings door open wide and lets it close by itself.
  - Doesn't look behind them.
  - Attacker walks up, stops the door from closing, then moves in.
- Requires:
  - Doors not close too quickly.
  - Employee not paying attention.
  - No attentive security personnel waiting.

Piggybacking

An attack similar to tailgating, but the target knows someone is following them.

- Might know attacker personally and be an accomplice.
- Or, might be ignorant of the attack.
  - Example: Doesn't know attacker was terminated; lets them in like a normal day.
- More likely that target doesn't know the attacker.
  - Lets them in out of common courtesy.
  - May want to avoid confrontation.
- Less effective when:
  - Organization is small and all employees know each other well.
  - Building access is strongly controlled.

Guidelines for Performing Social Engineering Tests (Slide 1 of 2)

- Understand basic components of social engineering.
- Leverage motivation techniques.
- Launch a phishing attack to entice targets to leak sensitive info.
- Use media other than just email for phishing.
- Create a convincing forgery of a popular website.
- Capture credentials through login forms on the forged website.
- Leverage gathered data about people to spear phish specific targets.
- Consider targeting high-level personnel in phishing.

Guidelines for Performing Social Engineering Tests (Slide 2 of 2)

- Use impersonation to make attacks seem more authentic.
- Use elicitation to get targets to reveal info.
- Leverage hoaxes to make attacks more convincing.
- Drop a USB drive loaded with malware in a parking lot.
- Determine how users fall victim to mistyped URLs.
- Leverage spam techniques in phishing attacks.
- See how easy it is to observe employees without their knowledge.
- Consider how environment might make tailgating/piggybacking more/less effective.

Physical Security Controls

- You may be up against:
  - Door/hardware locks.
  - Surveillance cameras.
  - Security guards.
  - Lighting that makes nighttime intruders visible.
  - Fences, gates, and other physical barriers.
  - Mantraps.
  - Alarms and motion sensors.

Fence Jumping (Slide 1 of 2)

The act of surmounting a height-based physical barrier in order to gain access to a restricted area.

- Includes fences, gates, walls, etc.
- Might be easier to go over a short fence than around or through it.
  - Prevent people from casually walking into a restricted area.
  - Extend all around perimeter and made of a strong metal.
- Can attract suspicion if seen.

Fence Jumping (Slide 2 of 2)

- Taller fences (above 8 ft.) cannot be jumped and must be climbed.
  - Designed to be difficult to climb without effort.
  - Ladder helps you scale fence, but will draw suspicion.
- Barbed/razor wire is an even stronger anti-fence-jumping measure.
  - Situated at the top of the fence.
  - Will cause serious injury if you attempt to go over it.
  - Openings can be made with the right tools.

Dumpster Diving

The act of searching the contents of trash containers for something of value.

- Can help a pen tester claim documents with sensitive info.
- Example: Calendars with passwords written on them discarded when it’s a new year.
- Example: Hard copy official documents like financial reports.
- You may be able to piece together shredded documents.
- Organizations also dispose of computing equipment.
  - Storage drives, whole computers, etc.
  - May fail to wipe sensitive data.
- Will draw suspicion if you're seen.
  - Dumpsters usually placed out of view.
  - May be outside restricted areas for easier trash pickup.

Lock Picking and Bypassing (Slide 1 of 2)

- Organizations will lock doors, cabinets, safes, devices, etc.
- Locks can cut your physical testing short if you can't find a way around them.
- Type of lock influences how you get around it.
- Key locks are very common and require the correct key to open the lock.
  - Use pin tumblers, interchangeable cores, or wafer springs.
  - Bolt cutters/hacksaws may be able to destroy poorly made locks.
- You can also try picking a key lock.
  - A skill that requires practice and the right tools.
  - Vendors sell lock picking kits, usually for pin-tumbler locks.
  - Not very effective against high-security locks.

Lock Picking and Bypassing (Slide 2 of 2)

- Basic lock picking process:
  1. Use pick tool to raise or lower a pin until it's flush with shear line.
  2. Use torsion wrench on lock plug to hold picked pins in place.
  3. Repeat with the remaining pins.
  4. Use torsion wrench to turn plug, disengaging the lock.
- Not all locks use keys.
- Keyless lock types: Combination, access card, and biometric.
- Keyless locks must either be destroyed or bypassed.
  - Simple combination locks can be brute forced.
  - Access card and biometric locks are more difficult to bypass.
- May need to think outside the box to bypass a keyless lock.
  - What if the lock is only active during off hours?
  - Try again during a certain time.

RFID (Slide 1 of 2)

A standard for identifying and keeping track of objects' physical locations through the use of radio waves.

- Many different applications.
- In physical security, used with ID badges.
- RFID tag is attached to badge.
  - Includes antenna and microchip.
- Lock containing RFID reader sends signal to surrounding area.
- Tag's antenna picks up signal and microchip returns signal to reader.
- Reader receives signal and opens lock if authenticated.

RFID (Slide 2 of 2)

- RFID badges don't need to be waved in front of reader.
  - Can be inside bag, on someone's shirt, etc.
- RFID authentication systems can support granular access.
  - Personnel issued unique badges.
  - Badge is a "key" that mitigates lock picking.

Badge Cloning (Slide 1 of 2)

The act of copying authentication data from an RFID badge's microchip to another badge.

- Enables attacker to obtain credentials without stealing badge.
- Can be done through handheld RFID writers.
  - Inexpensive and easy to use.
  - Hold up badge to writer, press the copy button, hold up blank badge, write the copy.
- Can also be done through RFID receivers concealed in bags and several feet away.
- Most effective against 125kHz EM4100 protocol.
  - Doesn't support encryption.
  - Transmits data to any nearby receivers.

Badge Cloning (Slide 2 of 2)

- Newer badge technology uses higher frequencies.
  - Faster data rate.
  - Supports encryption and only broadcasts certain attributes.
- Encryption-based badges can still be cloned.
  - Requires Android device with NFC and a cloning app.
  - App comes with default keys issued by manufacturer.
  - If organization doesn't change keys, badges can be cloned.

Motion Detection Bypassing (Slide 1 of 2)

- Motion detection systems detect movement to identify unauthorized physical access.
- Sensors placed at key entrances/exits.
  - Most detect changes to infrared spectrum.
  - Some detect human-based emissions.
  - Some detect blocking patterns.
  - Some detect deviations from baseline.
- Sensors will trigger alarms or fail-safes.
- Simple bypassing involves finding blind spots.
  - Identify what zones are covered by sensors.
  - Stay out of these zones.
  - Not always feasible if zones are too wide or sensors are hard to find.

Motion Detection Bypassing (Slide 2 of 2)

- Try placing material over sensor (cardboard, Styrofoam, glass, etc.).
- Try placing material over your own body if you can't reach sensor.
  - Not always effective and requires moving slowly and a large blocking object.
- Blocking tactics won't fool all sensors.
- Try focusing an infrared light at a sensor.
  - Stops human-based infrared and doesn't rely on blocking.
  - Not effective against baseline-comparing sensors.

Guidelines for Performing Physical Security Tests on Facilities (Slide 1 of 2)

- Identify physical security controls in place at target organization.
- Look for low fences to entrances and other restricted areas.
- Consider using a ladder to scale a taller fence.
- Consider the danger of scaling a fence with barbed or razor wire.
- Look for dumpsters that may contain sensitive materials.
  - Calendars with passwords.
  - Sensitive business documents.
  - Storage devices and computing equipment.

Guidelines for Performing Physical Security Tests on Facilities (Slide 2 of 2)

- Practice with a lock picking tool.
- Find other ways around keyless locks.
- Use a handheld RFID writer to clone badges using the 125kHz EM4100 protocol.
- Conceal cloning tool in a bag to read data from several feet away.
- Use an Android device/app to clone encrypted RFID badges that use default keys.
- Identify the area a motion sensor covers.
- Leverage motion sensor blind spots to move through a building.
- Consider using a piece of material to block a motion sensor.
- Focus infrared light on a sensor to fool it.

Reflective Questions

1. What concerns do you have when it comes to conducting social engineering tests?

2. What kind of physical security have you encountered at the places you've worked? Have you worked in high-security organizations, or are you more familiar with organizations that have little to no physical security? How might the relative security of these organizations impact a pen test?