# CompTIA PenTest+

## Exam PT0-002

CompTIA PenTest+ Exam PT0-002

# Lesson 4

## Evaluating Human and Physical Vulnerabilities Intelligence

# Objectives

- Given a scenario, perform a social engineering or physical attack.
- Explain use cases of the following tools during the phases of a penetration test.

Lesson 4

# Topic 4A

## Exploit the Human Psyche

# Using Social Engineering

- Uses psychological manipulation to exploit our willingness to trust
- It’s essential to evaluate potential targets and determine how susceptible they are to specific types of social engineering
  - The team might try to get to know their target on a personal level, by using social media or other method to gain trust
- The next step is to motivate the target to take some action or provide useful information.
  - One common method is pretexting - communicate a lie or half-truth in order to get someone to believe a falsehood.

# Obtaining Intel using Elicitation

- Acquiring data to launch an attack using the following methods:
  - **Request** - ask the target for information
  - **Interrogation**—poses as an authority figure to obtain actionable intel.
  - **Surveys** are used to informally collect data from the target.
  - **Observation**—observing the target's behavior and day-to-day routine
- Elicitation is useful when used in a variant of phishing called a business email compromise
  - An attacker impersonates a high-level executive or hijack their email account.

# Deceiving the Victim

- **Hoax** is when the attacker presents a fictitious situation as real.
  - For example, a pop-up that says an antivirus program has identified the presence of malware on a target's system
- **Baiting –** an attacker will leave bait, such as an infected USB drive, in an area where a victim can find the device.
  - The goal is to get the victim to pick up the drive and then insert it into a computer so that the malware can infect the system.

# Phishing and Pharming

- **Phishing** is a social engineering attack where the malicious actor tries to try to lure the victim into divulging sensitive information.
  - Leverages technical tricks—like spoofing the FROM headers in email—to make it more convincing.
- **Pharming** - An attacker entices the victim into navigating to a malicious web page that has been set up to look official.
  - The victim interacts with the site to provide sensitive information to the attacker, by filling out a fake "login" form

# Dispatching Email

- Email is one of the original ways to send malware and continues to be an idea method to launch an attack.
- **Spam** is unsolicited email that is sent to multiple victims
  - Can also include malvertising, which is email that looks like a normal ad, but instead includes malicious code.
  - Is often used when phishing: the attacker sends unsolicited email to as many targets as possible, hoping that at least some users will act on them.

# Using Spearphishing

- A phishing attack that targets a specific person or group
- Requires the attacker to gather specific people-based information on their targets before launching the attack.
  - The information is then used to create a custom message.
- The custom email has a better chance of having the target open the message and complete some action.

# Targeting Using Text or VoIP

- **Vishing** (VoIP phishing) is like regular phishing in that a hacker will call the party and request confidential information.
- **SPIT** (spam over internet telephony) sends unwanted messages to phone recipients.
- IM can also be used to launch an attack. Methods include:
  - **Spim** (Instant messaging spam) uses instant messaging to send a large volume of unsolicited messages to multiple recipients on the same platform.
  - **SMiShing** is a SMS phishing attack in which the attacker entices their victim through SMS text messages.

# Baiting and Redirecting the Victim

- Malicious actors use our sense of curiosity to bait victims into completing some action.
- A common form of baiting is called a USB drop key attack.
  - A malicious actor drops a thumb drive preloaded with malicious software  in a public area to entice someone to pick it up and plug it into their computer.
  - This kind of attack will rely on the victim's computer having autorun enabled so that the malicious code is executed immediately.
  - The malware, depending on its nature, may then spread outward and start infecting other hosts on the network.

# Enticing the Victim

- An attacker can entice a user to manually open a file and run the malicious code on by disguising it in the following ways:
    - As something fun, such as a video game
    - As something useful, such as an antivirus program
    - As something mysterious, such as a file with cryptic names
- An attacker can also redirect victims using typosquatting
    - This method exploits the typing mistakes that users may make when attempting to navigate to a website.

# Launching a Watering Hole Attack

- Can download and trigger an exploit on a victim without any direct contact from the malicious actor.
- The technique used in a watering hole attack can be used in other ways as well, such as a supply chain attack
  - Supply chain attack can have more damaging effects.
  - Infecting the target organization can result in downstream liability

# Impersonating and Imitating

- The act of pretending to be someone or something.
- Malicious actors couple pretexting and impersonation
  - Many times, is done using the phone or email.
- Prior to launching an attack, they might conduct research on a target to create a credible story to d establish trust

# Using Different Tactics

- Part of the impersonation ploy involves different tactics:
  - Leverage our need to obey an authority figure.
  - Implying scarcity or a sense of urgency
  - Malicious actors also prey on fear
- **Social proof** is when someone copies the actions of others in order to appear competent or cooperative in the eyes of others.
- **Likeness** is another conformity quality. Demonstrating that you can *conform* with the group can increase your likability.

# Review Activity: Exploit the Human Psyche

- Outline what’s involved when using social engineering
- Explain some of the ways to deceive a victim
- Compare and contrast phishing and pharming
- Discuss why email is an ideal tool to use during social engineering.
- Describe why Spearphishing is a better approach when launching a social engineering attack

# Review Activity: Exploit the Human Psyche

- List ways to use text or VoIP to target a victim
- Explain how to bait, redirect and/or entice a victim
- Outline how a watering hole attack works and how it can be used in a supply chain attack
- Describe some of the different tactics such as impersonating, and imitating to get someone to do something
- Discuss different tactics used to take advantage of human behavior

# Lab Activity

Assisted Lab: Understanding Social Engineering Toolkit (SET)

- Lab types
    - Assisted labs guide you step-by-step through tasks
    - Applied labs set goals with limited guidance
- Complete lab
    - Submit all items for grading and check each progress box
    - Select “Grade Lab” from final page
- Save lab
    - Select the hamburger menu and select “Save”
    - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
    - Select the hamburger menu and select “End”

Lesson 4

# Topic 4B

## Summarize Physical Attacks

# Assessing Physical Security

- The team will need to complete several tasks that can include:
  - Taking pictures of restricted areas and proprietary equipment
  - Stealing devices, documents, and electronic data
  - Bypassing security cameras and locks
- Evaluate physical security controls
  - Door and hardware locks
  - Physical barriers such as fences, gates, and mantraps
  - Video surveillance cameras

# Scaling Fences and Avoiding Detection

- If there are fences, the team should evaluate whether it would be feasible for someone to try and climb the fence.
- In addition to fences and barriers, the facility might have motion detection systems in place.
    - Sensors are placed in secure areas to detect movement, monitor activity, and identify unauthorized physical access.
- The team will want to evaluate to see if someone can bypass the system and if there are blind spots as you move through a building.

# Cloning an RFID Badge

- Some badges use an RFID badge system for physical security.
  - The badge hold an individual’s authorization credentials and use a proximity reader that reads data from either an RFID or NFC tag when in range.
- Badge cloning is the act of copying authentication data from an RFID badge's microchip to another badge.
  - Cloning can be done through handheld RFID writers, which are inexpensive and easy to use.

# Bypassing Locks

- Most organizations have at least one asset that is behind a lock.
- The team may be tasked to find ways to circumvent locks
  - Keyless locks must be either destroyed or bypassed.
  - Simple combination locks can be brute-forced with enough permutations
  - Access card locks and biometric scanners are difficult to bypass without the proper item or biometric profile.

# Tailgating and Piggybacking

- Tailgating is when a malicious actor slips in through a secure area
  - This is done while covertly following an authorized employee who is unaware that anyone is behind them.
- Piggybacking is essentially the same thing as tailgating, but in this case, the target knows someone is following behind them.
  - The target might either know the malicious actor personally and be involved somehow, or they might be ignorant of what the attacker is doing.

# Rummaging through Trash

- Dumpster diving is searching the contents of trash containers for something of value.

- Can help discover documents that contain sensitive information that is relevant to the organization.

- The team may be able to discover actionable intel that can give you an insight into the target's business operations.
  - Official documents
  - Storage drives

# Observing Employees

- Shoulder surfing is a social engineering attack in which the malicious actor observes a target's behavior without them noticing.
  - The malicious actor, who is behind the target, can see what's on the screen or the keys they are pressing.
- Another methods is to use the camera on a smartphone and capture pictures or video at a distance.
  - They can also set the camera down on a nearby desk, press record, and leave.
- Using a camera will allow the malicious actor to go back to that recording later and review the targets activity

# Review Activity: Summarize Physical Attacks

- List some tasks the team will need to complete when assessing physical security
- Describe some of the considerations involved when scaling fences and avoiding detection
- Outline why the team may need to clone an RFID badge, and how this can be achieved

# Review Activity: Summarize Physical Attacks

- Explain what might happen if asset to be tested is behind a lock
- Compare and contrast tailgating versus piggybacking
- Describe the benefit of dumpster diving
- Discuss ways to observe employees to learn actionable intel

Lesson 4

# Topic 4C

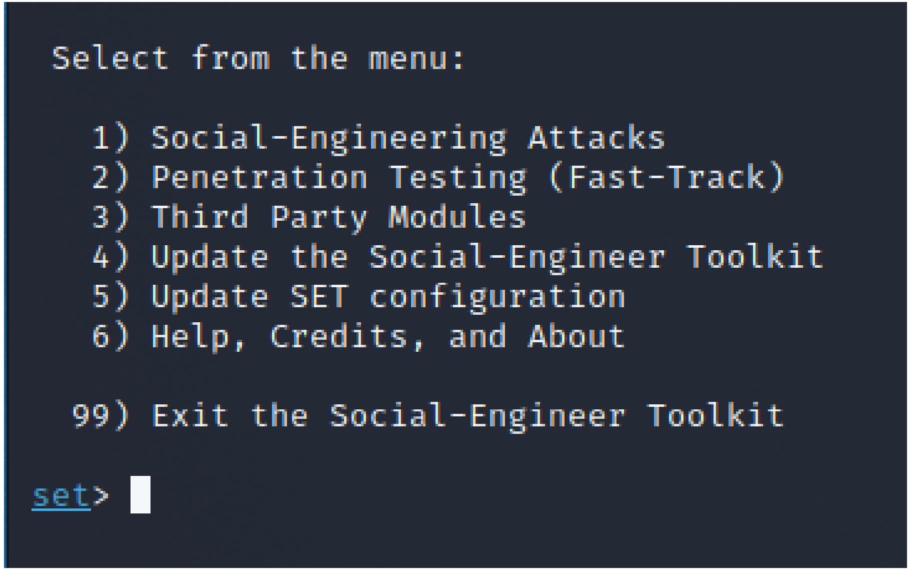
## Use Tools to Launch a Social Engineering Attack

# Discovering the Social Engineering Toolkit

- The Social Engineering Toolkit is a Python-based collection of tools that can be used when conducting a social engineering PenTest.
- You can download SET and install it on a Linux, Unix, and Windows machine or use it within Kali Linux.
- SET allows you to select from several different options that includes attacking websites, mass mailings and Spearphishing attacks.

# Exploring the Menu

- Once you launch SET, you'll be presented with a menu that shows you the most common options, as shown below:



```
 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 
```

# Selecting an Option

- In many cases, you will need to provide additional input, such as IP addresses, port numbers, or website URLs.
- When using SET, many of the attacks will walk you through what information is needed
- Prior to using SET, the team should evaluate the best methods and approach to craft an attack.

# Spoofing a Call

- Today when you make a call from a home line, you are most likely using Voice over IP (VoIP).
  - VoIP uses the Internet and network to send and receive calls
- On most phones when you get a call, the caller’s identification will come up on the device so that you can easily identify the caller.

# Launching an Attack

- VoIP uses software to make configuration changes.
- When spoofing a call, the malicious actor can make the call appear to be coming from a trusted source, such as:
  - A recognized vendor
  - A remote office
  - The president of the company

# Methods to Spoof a Call

- To spoof a VoIP call, there are a few methods you can use.
  1. Use an app where you enter the spoofed name and number
  2. Use Asterisk, a free, open-source tool to create a spoofed call.
- In addition, a malicious actor can use the spoofed phone number to listen to voicemail.
  - In some cases, the voicemail system will recognize the phone number and then prompt the user to enter a selection to listen to their voicemail.
  - The app may prompt the user to enter a password. If that is the case, the malicious actor will need to use the correct password.

# Finding the Password

- If they don’t have the password, they can search online for the default password to try on the targeted system.
- You can try to Google Hacking to find more information on VoIP phones, as shown:
  - Cisco CallManager: inurl:"ccmuser/logon.asp"
  - D -Link Phones: intitle:"D-Link DPH" "web login setting"
  - Grandstream Phones: intitle:"Grandstream Device Configuration" password

# Review Activity: Use Tools to Launch a Social Engineering Attack

- Discuss the features of the Social Engineering Toolkit
- Explain what is required after selecting an option in SET
- Outline what’s involved when spoofing a phone call.
- Describe what a malicious actor can do when spoofing a phone number.

# Lab Activity

APPLIED Lab: Understanding Spear Phishing and Credentials Attack

- Lab types
  - Assisted labs guide you step-by-step through tasks
  - Applied labs set goals with limited guidance
- Complete lab
  - Submit all items for grading and check each progress box
  - Select “Grade Lab” from final page
- Save lab
  - Select the hamburger menu and select “Save”
  - Save up to two labs in progress for up to 7 days
- Cancel lab without grading
  - Select the hamburger menu and select “End”

# Lesson 4

## Summary