PEARSON IT CERTIFICATION

Save 10% on Exam Voucher
See Inside

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA®

PenTest+

PT0-002

OMAR SANTOS

Special Offer

Save 80% on Premium Edition eBook and Practice Test

The *CompTIA PenTest+ PT0-002 Cert Guide Premium Edition and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You also receive two additional practice exams with links for every question mapped to the PDF eBook.

See the card insert in the back of the book for your Pearson Test Prep activation code and special offers.

10. Which of the following are methods of influence often used by social engineers? (Choose all that apply.)
    a. Authority
    b. Scarcity
    c. Urgency
    d. All of these answers are correct.

Foundation Topics

Pretexting for an Approach and Impersonation

Influence, interrogation, and impersonation are key components of social engineering. *Elicitation* is the act of gaining knowledge or information from people. In most cases, an attacker gets information from a victim without directly asking for that particular information.

How an attacker *interrogates* and interacts with a victim is crucial for the success of a social engineering campaign. An interrogator can ask good open-ended questions to learn about an individual's viewpoints, values, and goals. The interrogator can then use any information the target revealed to continue to gather additional information or to obtain information from another victim.

It is also possible for an interrogator to use closed-ended questions to get more control of the conversation and to lead the conversation or to actually stop the conversation. Asking too many questions can cause the victim to shut down the interaction, and asking too few questions may seem awkward. Successful social engineering interrogators use a narrowing approach in their questioning to gain as much information as possible from the victim.

Interrogators pay close attention to the following:

- The victim's posture or body language
- The color of the victim's skin, such as the face color becoming pale or red
- The direction of the victim's head and eyes
- Movement of the victim's hands and feet
- The victim's mouth and lip expressions
- The pitch and rate of the victim's voice, as well as changes in the voice
- The victim's words, including their length, the number of syllables, dysfunctions, and pauses

Key Topic

With ***pretexting***, or ***impersonation***, an attacker presents as someone else in order to gain access to information. In some cases, it can be very simple, such as quickly pretending to be someone else within an organization; in other cases, it can involve creating a whole new identity and then using that identity to manipulate the receipt of information. Social engineers may use pretexting to impersonate individuals in certain jobs and roles even if they do not have experience in those jobs or roles.

For example, a social engineer may impersonate a delivery person from Amazon, UPS, or FedEx or even a bicycle messenger or courier with an important message for someone in the organization. As another example, someone might impersonate an IT support worker and provide unsolicited help to a user. Impersonating IT staff can be very effective because if you ask someone if he or she has a technical problem, it is quite likely that the victim will think about it and say something like, "Yes, as a matter of fact, yesterday this weird thing happened to my computer." Impersonating IT staff can give an attacker physical access to systems in an organization. An attacker who has physical access can use a USB stick containing custom scripts to compromise a computer in seconds.

Pharming is a type of impersonation attack in which a threat actor redirects a victim from a valid website or resource to a malicious one that could be made to appear as the valid site to the user. From there, an attempt is made to extract confidential information from the user or to install malware in the victim's system. Pharming can be done by altering the host file on a victim's system, through DNS poisoning, or by exploiting a vulnerability in a DNS server. Figure 4-1 illustrates how pharming works.

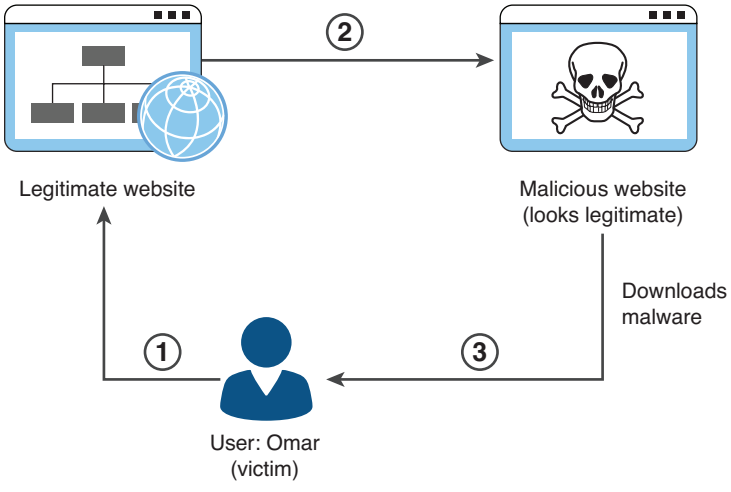

FIGURE 4-1 Pharming Example

The following steps are illustrated in Figure 4-1:

Step 1. The user (Omar) visits a legitimate website and clicks on a legitimate link.

Step 2. Omar's system is compromised, the host file is modified, and Omar is redirected to a malicious site that appears to be legitimate. (This could also be accomplished by compromising a DNS server or spoofing a DNS reply.)

Step 3. Malware is downloaded and installed on Omar's system.

TIP To help prevent pharming attacks, it is important to keep software up to date and run regular anti-malware checks. You should also change the default passwords in network infrastructure devices (including your home router). Of course, you also need to be aware of what websites you visit and be careful about opening emails.

An attack that is similar to pharming is called *malvertising*. Malvertising involves incorporating malicious ads on trusted websites. Users who click these ads are inadvertently redirected to sites hosting malware.

Social Engineering Attacks

A social engineering attack leverages the weakest link in an organization, which is the human user. If an attacker can get a user to reveal information, it is much easier for the attacker to cause harm than it is by using some other method of reconnaissance. Social engineering can be accomplished through email or misdirection of web pages and prompting a user to click something that leads to the attacker gaining information. Social engineering can also be done in person by an insider or an outside entity or over the phone.

A primary example is attackers leveraging normal user behavior. Suppose that you are a security professional who is in charge of the network firewalls and other security infrastructure equipment in your company. An attacker could post a job offer for a very lucrative position and make it very attractive to you, the victim. Suppose the job description lists benefits and compensation far beyond what you are making at your company. You decide to apply for the position. The criminal (attacker) then schedules an interview with you. Because you are likely to "show off" your skills and work, the attacker may be able to get you to explain how you have configured the firewalls and other network infrastructure devices for your company. You might disclose information about the firewalls used in your network, how you have configured them, how they were designed, and so on. This would give the attacker a lot of knowledge about the organization without requiring the attacker to perform any type of scanning or reconnaissance on the network.

Email Phishing

Key Topic

With ***phishing***, an attacker presents to a user a link or an attachment that looks like a valid, trusted resource. When the user clicks it, he or she is prompted to disclose confidential information such as his or her username and password. Example 4-1 shows an example of a phishing email.

Example 4-1 Phishing Email Example

```
Subject: PAYMENT CONFIRMATION

Message Body:

Dear sir,
We have discovered that there are occasional delays from our accounts
department in making complete payments to our suppliers.
This has caused undue reduction in our stocks and in our production
department of which suppliers do not deliver materials on time.
The purpose of this letter is to confirm whether or not payment has
been made for the attached supplies received.
Kindly confirm receipt and advise.

Attachment: SD_085_085_pdf.xz / SD_085_085_pdf.exe
MD5 Checksum of the attachment: 0x8CB6D923E48B51A1CB3B080A0D43589D
```

Spear Phishing

Key Topic

Spear phishing is a phishing attempt that is constructed in a very specific way and directly targeted to specific groups of individuals or companies. The attacker studies a victim and the victim's organization in order to be able to make emails look legitimate and perhaps make them appear to come from trusted users within the company. Example 4-2 shows an example of a spear phishing email.

In the email shown in Example 4-2, the threat actor has become aware that Chris and Omar are collaborating on a book. The threat actor impersonates Chris and sends an email asking Omar to review a document (a chapter of the book). The attachment actually contains malware that is installed on Omar's system.

Example 4-2 Spear Phishing Email Example

```
From: Chris Cleveland
To: Omar Santos
Subject: Please review chapter 3 for me and provide feedback by 2pm

Message Body:
Dear Omar,

Please review the attached document.

Regards,
Chris

Attachment: chapter.zip
MD5 Checksum of the attachment: 0x61D60EA55AC14444291AA1F911F3B1BE
```

Whaling

Key Topic

Whaling, which is similar to phishing and spear phishing, is an attack targeted at high-profile business executives and key individuals in a company. Like threat actors conducting spear phishing attacks, threat actors conducting whaling attacks also create emails and web pages to serve malware or collect sensitive information; however, the whaling attackers' emails and pages have a more official or serious look and feel. Whaling emails are designed to look like critical business emails or emails from someone who has legitimate authority, either within or outside the company. In whaling attacks, web pages are designed to specifically address high-profile victims. In a regular phishing attack, the email might be a faked warning from a bank or service provider. In a whaling attack, the email or web page would be created with a more serious executive-level form. The content is created to target an upper manager such as the CEO or an individual who might have credentials for valuable accounts within the organization.

The main goal in whaling attacks is to steal sensitive information or compromise the victim's system and then target other key high-profile victims.

Vishing

Key Topic

Vishing (which is short for *voice phishing*) is a social engineering attack carried out in a phone conversation. The attacker persuades the user to reveal private personal and financial information or information about another person or a company.