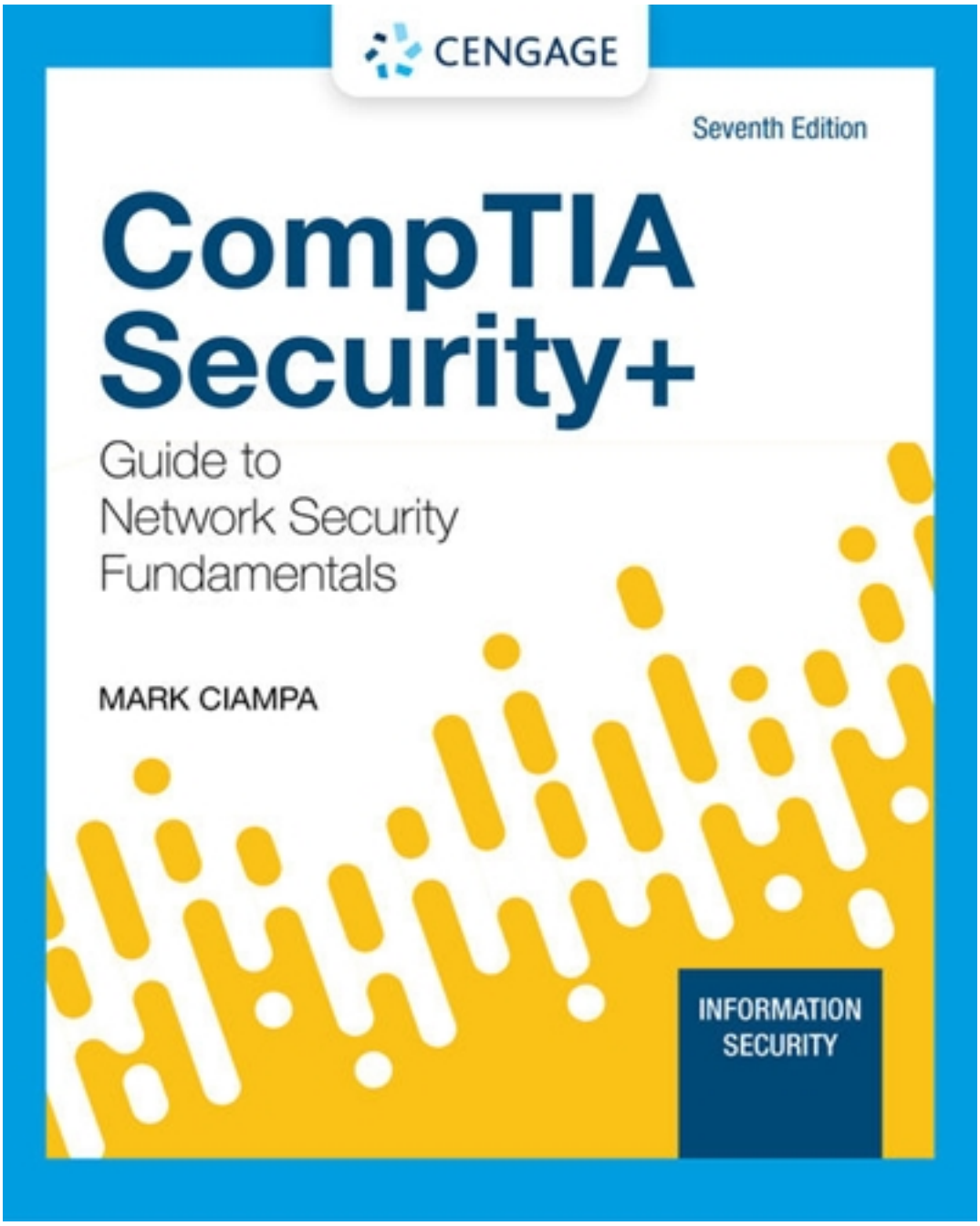
Solutions for CompTIA Security Guide to Network Security Fundamentals 7th Edition by Ciampa

CLICK HERE TO ACCESS COMPLETE Solutions



Solutions

Module 1

<question type="mc">
1. After Bella earned her security certification, she was offered a promotion. As she reviewed the job responsibilities, she saw that in this position she will report to the CISO and will be a supervisor over a group of security technicians. Which of these generally recognized security positions has she been offered?

a. Security administrator
b. Security technician
c. Security officer
d. Security manager

Analysis**:**
a. Incorrect. A security administrator manages daily operations of security technology and may analyze and design security solutions within a specific entity as well as identifying users' needs.
b. Incorrect. This position is generally an entry-level position for a person who has the necessary technical skills. Technicians provide technical support to configure security hardware, implement security software, and diagnose and troubleshoot problems.
c. Incorrect. A security officer is not one of the generally recognized security positions.
d. Correct. The security manager reports to the CISO and supervises technicians, administrators, and security staff.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
2. Which of the following is false about the CompTIA Security+ certification?

a. Security+ is one of the most widely acclaimed security certifications.
b. Security+ is internationally recognized as validating a foundation level of security skills and knowledge.
c. The Security+ certification is a vendor-neutral credential.
d. Professionals who hold the Security+ certification earn about the same or slightly less than security professionals who have not achieved this certification.

Analysis**:**

c. Incorrect. The Security+ certification is a vendor-neutral credential.
d. Correct. The value for an IT professional who holds a CompTIA security certification is significant. On average, an employee with a CompTIA certification will command a salary that is between 5 to 15 times higher than their counterparts with similar qualifications but lacking a certification.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
3. Which of the following is true regarding the relationship between security and convenience?

a. Security and convenience are inversely proportional.
b. Security and convenience have no relationship.
c. Security is less importance than convenience.
d. Security and convenience are equal in importance.

Analysis**:**
a. Correct. The relationship between these two is inversely proportional so that as security is increased, convenience is decreased.
b. Incorrect. There is a relationship between security and convenience.
c. Incorrect. Security is never less important than convenience.
d. Incorrect. Security and convenience are not equal in importance.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
4. Which of the following of the CIA Triad ensures that the information is correct, and no unauthorized person has altered it?

a. Confidentiality
b. Integrity
c. Availability
d. Assurance

b. Correct. Integrity ensures that the information is correct and no unauthorized person or malicious software has altered the data.
c. Incorrect. Availability ensures that data is accessible only to authorized users and not to unapproved individuals.
d. Incorrect. Assurance is not part of the CIA Triad.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
5. Which of the following is not used to describe those who attack computer systems?

a. Threat actor
b. Hacker
c. Malicious agent
d. Attacker

Analysis**:**
a. Incorrect. In cybersecurity, a threat actor is a term used to describe individuals or entities who are responsible for cyber incidents against the technology equipment of enterprises and users.
b. Incorrect. In the past, the term hacker referred to a person who used advanced computer skills to attack computers
c. Correct. A threat actor is also called a malicious actor, not a malicious agent.
d. Incorrect. The generic term attackers is commonly used.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
6. Which of the following is not true regarding security?

a. Security is a goal.
b. Security includes the necessary steps to protect from harm.

a. Incorrect. Sometimes security is defined as the state of being free from danger, which is the goal of security.
b. Incorrect. Since complete security can never be fully achieved, the focus of security is more often on the process instead of the goal. In this light, security can be defined as the necessary steps to protect from harm.
c. Incorrect. Since complete security can never be fully achieved, the focus of security is more often on the process instead of the goal.
d. Correct. Information security should not be viewed as a war to be won or lost. Just as crimes such as burglary can never be completely eradicated, neither can attacks against technology devices. The goal is not a complete victory but, instead, maintaining equilibrium: as attackers take advantage of a weakness in a defense, defenders must respond with an improved defense. Information security is an endless cycle between attacker and defender.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
7. Luna is reading a book about the history of cybercrime. She read that the very first cyberattacks that occurred were mainly for what purpose?

a. Fortune
b. Fame
c. Financial gain
d. Personal security

Analysis**:**
a. Incorrect. Later threat actors purposed fortune, not the first cyberattackers.
b. Correct. Early cyberattackers were trying to show off their skills to generate fame.
c. Incorrect. Financial security is the same as fortune, and later threat actors pursued fortune.
d. Incorrect. Threat actors do not try to achieve personal security through their attacks.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

a. Authorization
b. Confidentiality
c. Availability
d. Integrity

Analysis:
a. Incorrect. Authorization provides approval to access.
b. Correct. Confidentiality ensures that only authorized parties can view the information.
c. Incorrect. Availability ensures that data is accessible to only authorized users and not to unapproved individuals.
d. Incorrect. Integrity ensures that the information is correct and no unauthorized person or malicious software has altered the data.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
9. Which type of hacker will probe a system for weaknesses and then privately provide that information back to the organization?

a. Black hat hackers
b. White hat hackers
c. Gray hat hackers
d. Red hat hackers

Analysis:
a. Incorrect. Black hat hackers are threat actors who violate computer security for personal gain (such as to steal credit card numbers) or to inflict malicious damage (corrupt a hard drive).
b. Correct. Also known as ethical attackers, these white hat hackers attempt to probe a system (with an organization's permission) for weaknesses and then privately provide that information back to the organization.
c. Incorrect. Gray hat hackers are attackers who attempt to break into a computer system without the organization's permission (an illegal activity) but not for their own advantage; instead, they publicly disclose the attack in order to shame the organization into taking action.
d. Incorrect. There is no category of red hat hackers.

Bloom's:
</metadata>

<question type="mc">
10. Complete this definition of information security: That which protects the integrity, confidentiality, and availability of information _____.

a. on electronic digital devices and limited analog devices that can connect via the Internet or through a local area network
b. through a long-term process that results in ultimate security
c. using both open-sourced as well as supplier-sourced hardware and software that interacts appropriately with limited resources
d. through products, people, and procedures on the devices that store, manipulate, and transmit the information

Analysis:
a. Incorrect. All analog devices and not just limited analog devices can be protected through security.
b. Incorrect. Security never results in ultimate protection.
c. Incorrect. The appropriateness of the interaction does not play a role in security.
d. Correct. The products, people, and procedures on the devices that store, manipulate, and transmit the information provide the security.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
11. Which of the following groups have the lowest level of technical knowledge?

a. Script kiddies
b. Hactivists
c. State actors
d. Insiders

Analysis:
a. Correct. Script kiddies are individuals who want to perform attacks, yet they lack the technical knowledge to carry out these attacks. Script kiddies instead do their work by downloading freely available automated attack software (scripts) and use it to perform their malicious acts.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
12. Which of the following groups use Advanced Persistent Threats?

a. Brokers
b. Criminal syndicates
c. Shadow IT
d. State actors

Analysis:
a. Incorrect. These sell their knowledge of a weakness to other attackers or governments.
b. Incorrect. Criminal syndicates are moving from traditional criminal activities to more rewarding and less risky online attacks.
c. Incorrect. Shadow IT are employees who become frustrated with the slow pace of acquiring technology, so they purchase and install their own equipment or resources in violation of company policies.
d. Correct. These attacks use innovative attack tools (advanced) and once a system is infected it silently extracts data over an extended period of time (persistent). APTs are most commonly associated with state actors.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
13. Which of the following is not a reason why a legacy platform has not been updated?

a. Limited hardware capacity
b. An application only operates on a specific OS version
c. Neglect
d. No compelling reason for any updates

Analysis:

c. Incorrect. Overlooking a system that is rarely used can cause updates to not be installed.
d. Correct. There is always a reason to install updates, and that reason is security.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
14. How do vendors decide which should be the default settings on a system?

a. Those that are the most secure are always the default settings.
b. There is no reason behind why specific default settings are chosen.
c. Those settings that provide the means by which the user can immediately begin to use the product.
d. The default settings are always mandated by industry standards.

Analysis:
a. Incorrect. Rarely are the most secure settings chosen as default.
b. Incorrect. There is a reason for selecting default settings—those that enable the user to immediately begin utilizing the product.
c. Correct. Default settings are chosen that allow the user to quickly begin using the product.
d. Incorrect. There are no industry standards for default settings.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
15. Which tool is most commonly associated with state actors?

a. Closed-Source Resistant and Recurrent Malware (CSRRM)
b. Advanced Persistent Threat (APT)
c. Unlimited Harvest and Secure Attack (UHSA)
d. Network Spider and Worm Threat (NSAWT)

Analysis:
a. Incorrect. This is a fictitious name and does not exist.

d. Incorrect. This is a fictitious name and does not exist.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
16. What is the term used to describe the connectivity between an organization and a third party?

a. System integration
b. Platform support
c. Resource migration
d. Network layering

Analysis:
a. Correct. Almost all third parties today require that they can access the organization's computer network. This gives these external entities the ability to perform their IT-related functions (such as outsourced code development) and even do basic tasks such as submitting online invoices. This connectivity between the organization and the third party is known as system integration.
b. Incorrect. This is a fictitious name and does not exist.
c. Incorrect. This is a fictitious name and does not exist.
d. Incorrect. This is a fictitious name and does not exist.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
17. What is an objective of state-sponsored attackers?

a. To right a perceived wrong
b. To amass fortune over of fame
c. To spy on citizens
d. To sell vulnerabilities to the highest bidder

Analysis:

c. Correct. Instead of using an army to march across the battlefield to strike an adversary, governments are increasingly employing their own state-sponsored attackers for launching cyberattacks against their foes. These are known as state actors. Their foes may be foreign governments or even citizens of its own nation that the government considers hostile or threatening.
d. Incorrect. Brokers sell vulnerabilities to the highest bidder.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
18. Which of the following is not an issue with patching?

a. Difficulty patching firmware
b. Few patches exist for application software
c. Delays in patching OSs
d. Patches address zero-day vulnerabilities

Analysis**:**
a. Incorrect. Firmware, or software that is embedded into hardware, provides low-level controls and instructions for the hardware. Updating firmware to address a vulnerability can often be difficult and requires specialized steps. Some firmware cannot be patched.
b. Incorrect. Outside of the major application software such as Microsoft Office, patches for application software are uncommon. This is because there is no automated process to identify which computers have installed the application, to alert users to a patch, or to distribute the patch.
c. Incorrect. Modern operating systems—such as Red Hat Linux, Apple macOS, Ubuntu Linux, and Microsoft Windows—frequently distribute patches. These patches, however, can sometimes create new problems, such as preventing a custom application from running correctly. Organizations that have these types of applications usually test patches when they are released to ensure that they do not adversely affect any customized applications. In these instances, the organization delays the installation of a patch from the developer’s online update service until the patch is thoroughly tested.
d. Correct. Patches are intended to address vulnerabilities, which includes zero-day vulnerabilities.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

19. Which of the following is not a recognized attack vector?

a. Supply chain
b. Social media
c. On-prem
d. Email

Analysis:
a. Incorrect. A supply chain is a network that moves a product from the supplier to the customer. Today's supply chains are global in scope: manufacturers are usually thousands of miles away overseas and not under the direct supervision of the enterprise that is selling the product. The fact that products move through many steps in the supply chain—and that many of these steps are not closely supervised—has opened the door for malware to be injected into products during their manufacturing or storage. Supply chains also serve as third party vulnerabilities.
b. Incorrect. Threat actors will often use social media as a vector for attacks. For example, an attacker may read social media posts to determine when an employee will be on vacation and then call the organization's help desk pretending to be that employee to ask for "emergency" access to an account
c. Correct. On-prem is a vulnerability and not a recognized attack vector.
d. Incorrect. A large percentage of all malware is delivered through email to an unsuspecting user. The goal is to trick the user to open an attachment that contains malware or click on a hyperlink that takes the user to a fictitious website.

<metadata>
LO:
A-head:
Bloom's:
</metadata>

<question type="mc">
20. What is the category of threat actors that sell their knowledge of vulnerabilities to other attackers or governments?

a. Cyberterrorists
b. Competitors
c. Brokers
d. Resource managers

Analysis:
a. Incorrect. Cyberterrorists attack a nation's network and computer infrastructure to cause disruption

<metadata>
LO:
A-head:
Bloom's:
</metadata>

Instructor Manual

Ciampa, CompTIA Security+ Guide to Network Security Fundamentals , ISBN 9780357424377, Module 1: Security Fundamentals

Table of Contents

Purpose and Perspective of the Module

This module introduces the security fundamentals that form the basis of the Security+ certification. It begins by defining information security and then examines the attackers and how they function. It also covers vulnerabilities, categories of attacks, and the impacts of attacks.

Cengage Supplements

The following product-level supplements provide additional information that may help you in preparing your course. They are available in the Instructor Companion Site.

- Transition Guide (provides information about what's new from edition to edition)
- Test Bank (contains assessment questions and problems)
- Solution and Answer Guide (offers solutions, answers, and feedback)
- PowerPoint (provides text-based lectures and presentations)
- MindTap Educator Guide (provides information about the activities included in MindTap)
- MindTap Transition Guide (compares what has changed or been renamed from edition to edition)

Module Objectives

The following objectives are addressed in this module:

1. Define information security and explain why it is important
2. Identify threat actors and their attributes
3. Describe the different types of vulnerabilities and attacks
4. Explain the impact of attacks

What's New in This Module

Read about the updates and improvements in this module.

This module has been reorganized and material not found in the exam objectives has been eliminated.

Some new activities, review questions, and case projects have been created to reinforce the concepts and techniques presented in the module and to help you apply these concepts to real-world scenarios.

[return to top]

Teaching Tips

Consider the following teaching tips when assigning this module to your students.

What is Information Security?

1. Explain that the first step in understanding information security is to define it.

Understanding Security

1. Explain that security can be considered as a state of freedom from a danger. Since the goal of complete security can never be fully achieved, security can be defined as the necessary steps to protect from harm.

2. Use Figure 1-1 to help explain the relationship between security and convenience. Point out that as security is increased, convenience is often decreased.

Defining Information Security

1. Define information security as the tasks of guarding information that is in a digital format. It ensures that protective measures are properly implemented. Information security cannot completely prevent attacks or guarantee that a system is totally secure.

2. Explain that information security is intended to protect information that has value to people and organizations. That value comes from the characteristics of the information:

    a. Confidentiality
    b. Integrity
    c. Availability

Who are the Threat Actors?

2. Explain that the term threat actor, in a generic sense, is used to describe individuals who launch attacks against other users and their computers.

3. Explain that threat actors of today have a more focused goal of financial gain.

4. List the three categories of financial cybercrime: individual users, enterprises, and governments.

5. Point out that the characteristic features of different groups of threat actors can vary widely:
    a. Sophisticated
    b. Funding and resources
    c. External or internal to the enterprise
    d. Intent and motivation

Script Kiddies

1. Define script kiddies as individuals that want to break into computers to create damage. They download automated hacking software (scripts) from Web sites and use it to break into computers.

2. Point out that script kiddies can acquire entire exploit kits from other attackers. It takes little skill to be a script kiddie.

Hacktivists

1. Mention that hacktivists are a group strongly motivated by ideology. They are likely to break into a website and change the contents as a means of making a political statement.

2. Point out that it is estimated that there are thousands of hacktivist groups worldwide supporting a wide variety of causes.

State Actors

1. Define state actors as individuals hired by governments to launch cyberattacks against the country's foes.

2. Mention that a new class of attacks called Advanced Persistent Threat (APT) have been created. Further explain that these attacks use innovative attack tools and once a system is infected it silently extracts data over an extended period.

Insiders

1. Mention that one of the largest information security threats to a business actually comes from an unlikely source: its employees, contractors and business partners.

2. Describe some of the reasons an employee would break into their company's computer, including:
    a. Disgruntled employees may be intent on retaliating against the company
    b. Industrial espionage
    c. Blackmailing

Other Threat Actors

1. Use Table 1-2 to discuss the characteristics of the different types of attackers mentioned in this section of the text.

Vulnerabilities and Attacks

1. Define vulnerability as exposed to the possibility of being attacked or harmed.
2. List and describe the categories of vulnerabilities:
    a. Platforms
    b. Configurations
    c. Third parties
    d. Patches
    e. Zero-day

Attack Vectors

1. Define attack vector. Then go over the common categories of attack vector:
    a. Email
    b. Wireless
    c. Removable media
    d. Direct access
    e. Social media
    f. Supply chain
    g. Cloud

Social Engineering Attacks

1. Explain the importance of understanding the dangers of social engineering. Discuss the principles that make psychological social engineering effective:
    a. Authority
    b. Intimidation
    c. Consensus
    d. Scarcity
    e. Urgency
    f. Familiarity

g. Trust

2. Next, go over the techniques attackers use to gain trust, such as providing a reason, projecting confidence, using evasion, and putting people at ease.

3. Discuss social engineering psychological approaches: impersonation, phishing, redirection, spam, hoaxes, and watering holes. Each of these approaches should be discussed. Pay special attention to the various types of phishing attacks as phishing is among the most widespread of social engineering attacks.

4. Finally, discuss the various physical procedures attackers use to gain information used in social engineering attacks: dumpster diving, tailgating, and shoulder surfing.

Impacts of Attacks

1. Mention that the impact of attacks can be classified as data impacts and effects on the organization. List and describe the consequences of data attacks from Table 1-6:
   a. Data loss
   b. Data exfiltration
   c. Data breach
   d. Identity theft

[return to top]

Key Terms

advanced persistent threat (APT) A class of attacks that use innovative attack tools to infect and silently extract data over an extended period of time.

attack vector A pathway or avenue used by a threat actor to penetrate a system.

attributes Characteristic features of the different groups of threat actors.

authority A social engineering principle that involves directing others by impersonating an authority figure or falsely citing their authority.

availability loss The loss that results from making systems inaccessible.

black hat hackers Threat actors who violate computer security for personal gain or to inflict malicious damage.

cloud platforms A pay-per-use computing model in which customers pay only for the online computing resources they need.

competitors Threat actors who launch attacks against an opponent's system to steal classified information.

consensus A social engineering principle that involves being influenced by what others do.

credential harvesting Using the Internet and social media searches to perform reconnaissance.

criminal syndicates Threat actors who have moved from traditional criminal activities to more rewarding and less risky online attacks.

data breach Stealing data to disclose it in an unauthorized fashion.

data exfiltration Stealing data to distribute it to other parties.

data loss The destruction of data so that it cannot be recovered.

data storage Third-party facilities used for storing important data.

default settings Settings that are predetermined by the vendor for usability and ease of use (but not security) so the user can immediately begin using the product.

direct access An attack vector in which a threat actor can gain direct physical access to the computer.

dumpster diving Digging through trash receptacles to find information that can be useful in an attack.

eliciting information Gathering data.

errors Human mistakes in selecting one setting over another without considering the security implications.

external Threat actors who work outside the enterprise.

familiarity A social engineering principle that portrays the victim as well known and well received.

financial loss The monetary loss as a result of lost productivity

firmware Software that is embedded into hardware to provide low-level controls and instructions.

gray hat hackers Attackers who attempt to break into a computer system without the organization's permission to publicly disclose the attack and shame the organization into taking action.

hacker A person who uses advanced computer skills to attack computers.

hacktivists A group of attackers that is strongly motivated by ideology.

hoax A false warning often contained in an email message claiming to come from the IT department.

hybrid warfare influence campaign Influence campaigns used on social media and other sources.

identity fraud (also called impersonation) Masquerading as a real or fictitious character and then playing out the role of that person with a victim.

identity theft Taking personally identifiable information to impersonate someone.

impersonation (also called identity fraud) Masquerading as a real or fictitious character and then playing out the role of that person with a victim.

influence campaigns Using social engineering to sway attention and sympathy in a particular direction.

insider threat Attackers who manipulate data from the position of a trusted employee.

intent/motivation Reasons for an attack by threat actors.

internal Threat actors who work inside the enterprise.

intimidation To frighten and coerce by threat.

invoice scam A fictitious overdue invoice that demands immediate payment.

lack of vendor support A lack of expertise to handle system integration.

legacy platform A platform that is no longer in widespread use, often because it has been supplanted or replaced by an updated version of that earlier technology.

level of capability/sophistication Power and complexity capabilities of threat actors.

on-premises platform Software and technology located within the physical confines of an enterprise, which is usually consolidated in the company's data center.

open permissions User access over files that should have been restricted.

open ports and services Devices and services that are often configured to allow the most access so that the user can then close those ports that are specific to that organization.

outsourced code development Contracting with third parties to assist the organization in the development and writing of a software program or app.

patch An officially released software security update intended to repair a vulnerability.

pharming Exploiting how a URL is converted into its corresponding IP address to redirect traffic away from its intended target to a fake website instead.

phishing Sending an email or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information or taking action.

prepending Influencing a subject before an event occurs.

pretexting Using impersonation to obtain private information.

reconnaissance Learning as much about a person as possible in order to appear as genuine while acting as an imposter.

reputation Public perception.

resources and funding Financial capabilities of threat actors.

scarcity When something is in short supply.

script kiddies Individuals who want to perform attacks yet lack the technical knowledge to carry them out.

shadow IT Employees who become frustrated with the slow pace of acquiring technology, so they purchase and install their own equipment or resources in violation of company policies.

shoulder surfing Watching an individual enter a security code on a keypad.

smishing Using short message service (SMS) text messages to perform phishing.

social engineering Gathering data by relying on the weaknesses of individuals.

social media influence campaign An influence campaign exclusively used on social media.

spam Unsolicited email that is sent to a large number of recipients.

spear phishing Targeting specific users.

spim Spam delivered through instant messaging (IM) instead of email.

state actors Government-sponsored attackers who launch cyberattacks against the foes of the state.

supply chain A network that moves a product from the supplier to the customer and is made up of vendors that supply raw material, manufacturers who convert the material into products, warehouses that store products, distribution centers that deliver them to the retailers, and retailers who bring the product to the consumer.

system integration Connectivity between the systems of an organization and its third parties.

tailgating Following an authorized user through a door.

third parties External entities outside of the organization.

threat actor Individuals or entities who are responsible for cyber incidents against the technology equipment of enterprises and users.

trust A social engineering principle to inspire confidence in a victim.

typo squatting Purchasing the domain names of sites that are spelled similarly to actual sites.

unsecure protocols Also called insecure protocols, using protocols for telecommunications that do not provide adequate protections.

unsecured root accounts Unprotected accounts that give unfettered access to all resources.

urgency A social engineering principle that demands immediate action.

vendor management The process organizations use to monitor and manage the interactions with all external third parties with which they have a relationship.

vishing Using a telephone call to perform phishing.

watering hole attack An attack directed toward a smaller group of specific individuals, such as the major executives working for a manufacturing company.

weak configurations Configuration settings that are not properly implemented, resulting in vulnerabilities.

weak encryption Choosing a known vulnerable encryption mechanism.

whaling Targeting wealthy individuals or senior executives within a business through phishing.

white hat hackers Also known as ethical attackers, a class of hackers that probe a system with an organization's permission for weaknesses and then privately provide that information to the organization.

zero day A vulnerability that is exploited by attackers before anyone else even knows it exists.

[return to top]

Discussion Questions

You can assign these questions several ways: in a discussion forum in your LMS; as whole-class discussions in person; or as a partner or group activity in class.

1. Discussion: Hacktivists vs State-sponsored Attackers (Hacktivists, State Actors, pgs. 9-10) Duration 15 minutes.
    a. Two categories of attacker include hacktivists and state actors.
    b. What are the differences between hacktivists and state-sponsored attackers?
        i. Answer: Hacktivists often are looking to make a political statement or retaliate against an organization whose policies they disagree with. State-sponsored attackers are highly skilled attackers with plenty of technology provided by their government to achieve their goals of disrupting a foe's economy or national security.
    c. Which of the two types of attackers, hacktivists or state actors, do you think offers the highest degree of threat?
        i. Answer: Answers may vary but students should note that the threat risk depends on the type of organization. Hacktivists most likely are looking to disrupt their enemies by disabling or defacing their web site or similar actions. Their targets are likely to be limited to a single organization or group of organizations. Whereas, state actors are most likely looking to disrupt an entire nation's economy or national defense or create civil unrest.

[return to top]

Additional Activities and Assignments

1. **Phishing scams**: Research phishing scams and how to recognize them.
    a. Use the Internet to find out more about phishing scams and write a report with a series of guidelines to recognize them.
2. **Script kiddies**: Learn more about the tools used by script kiddies.
    a. Use the Internet to research some of the tools and scripting languages used by script kiddies. Create a list of the more popular tools and how they are used.

[return to top]

Additional Resources

External Videos or Playlist

- Hacking Humans: Social Engineering Techniques and How to Protect Against Them: https://www.youtube.com/watch?v=YVqurfWzB-Q&t=20s

Internet Resources

- FTC – Computer Security
  http://www.consumer.ftc.gov/topics/computer-security

- Fight Spam on the Internet!
  http://spam.abuse.net/

- How to recognize phishing e-mail messages, links, or phone calls
  http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

- Anti-Phishing Working Group
  http://www.antiphishing.org/

- SANS' Information Security Reading Room
  http://www.sans.org/reading_room/

- Zero day initiative
  http://www.zerodayinitiative.com/

External Audio Resources

- The Social-Engineer Podcast: https://www.social-engineer.org/category/podcast/

[return to top]

Practice Labs™

Answer File

CompTIA Security+ 7e

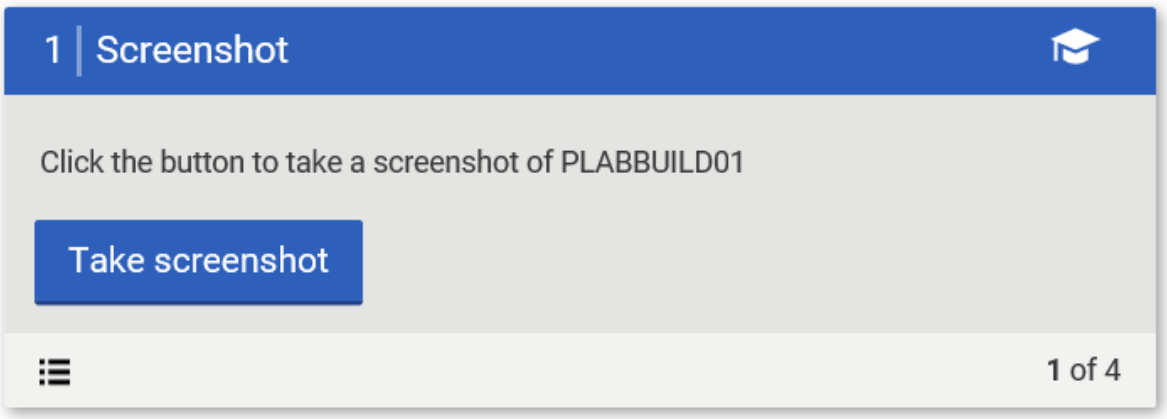
SY0-601

Contents

Introduction

The purpose of this document is to provide a quick reference guide for the inline questions found within the Practice Labs lab guides.

Screenshot assessment items are found at the end of each lab exercise. The learner should follow the steps within the lab guide and take a screenshot when they see the screenshot assessment item below.



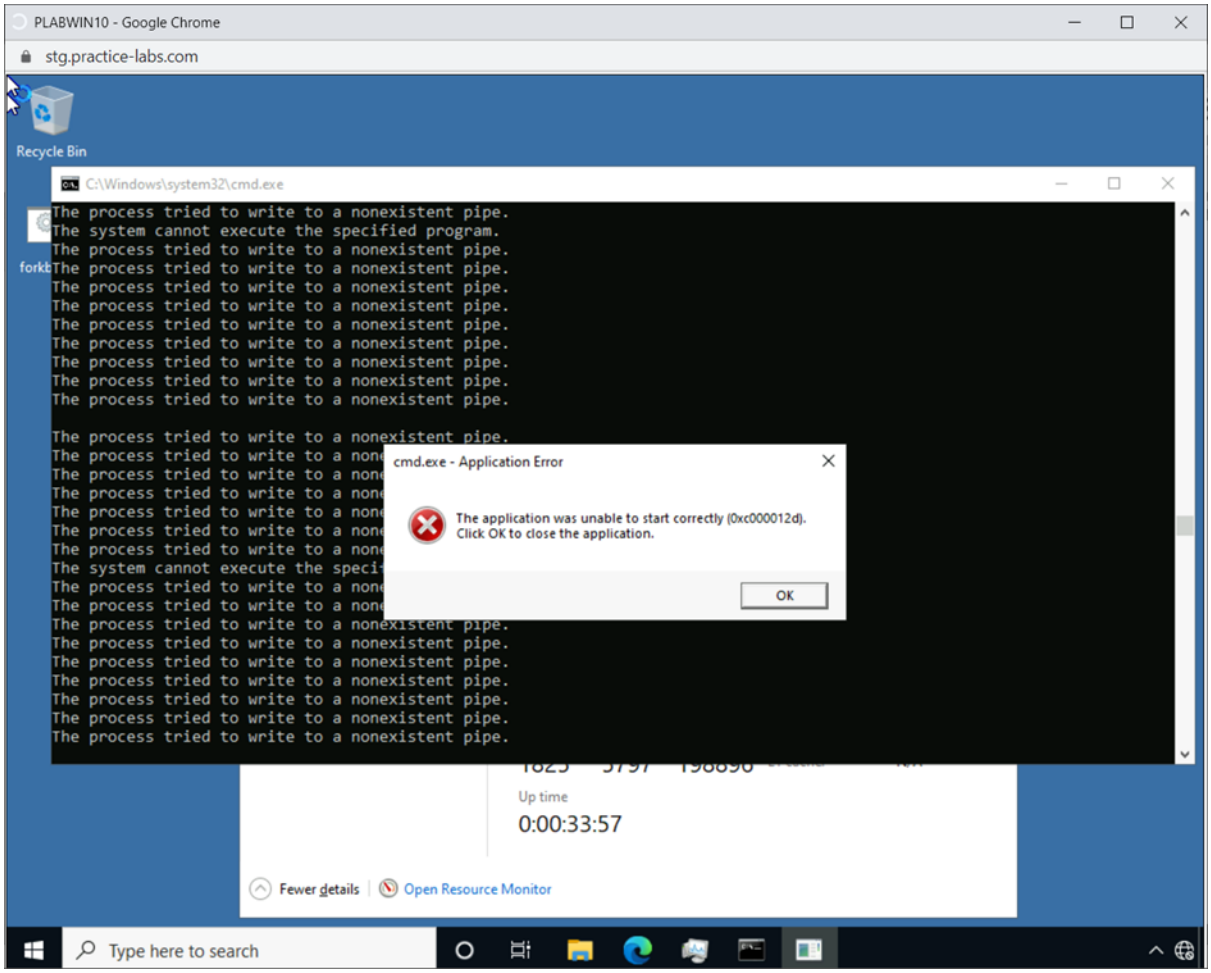
Alert: The images in this document are to be used as a guide. The screenshots taken by the learner may vary!

Module – Identifying Different Cyber Attacks

Below are the inline questions found in the summary of Identifying Different Cyber Attacks.

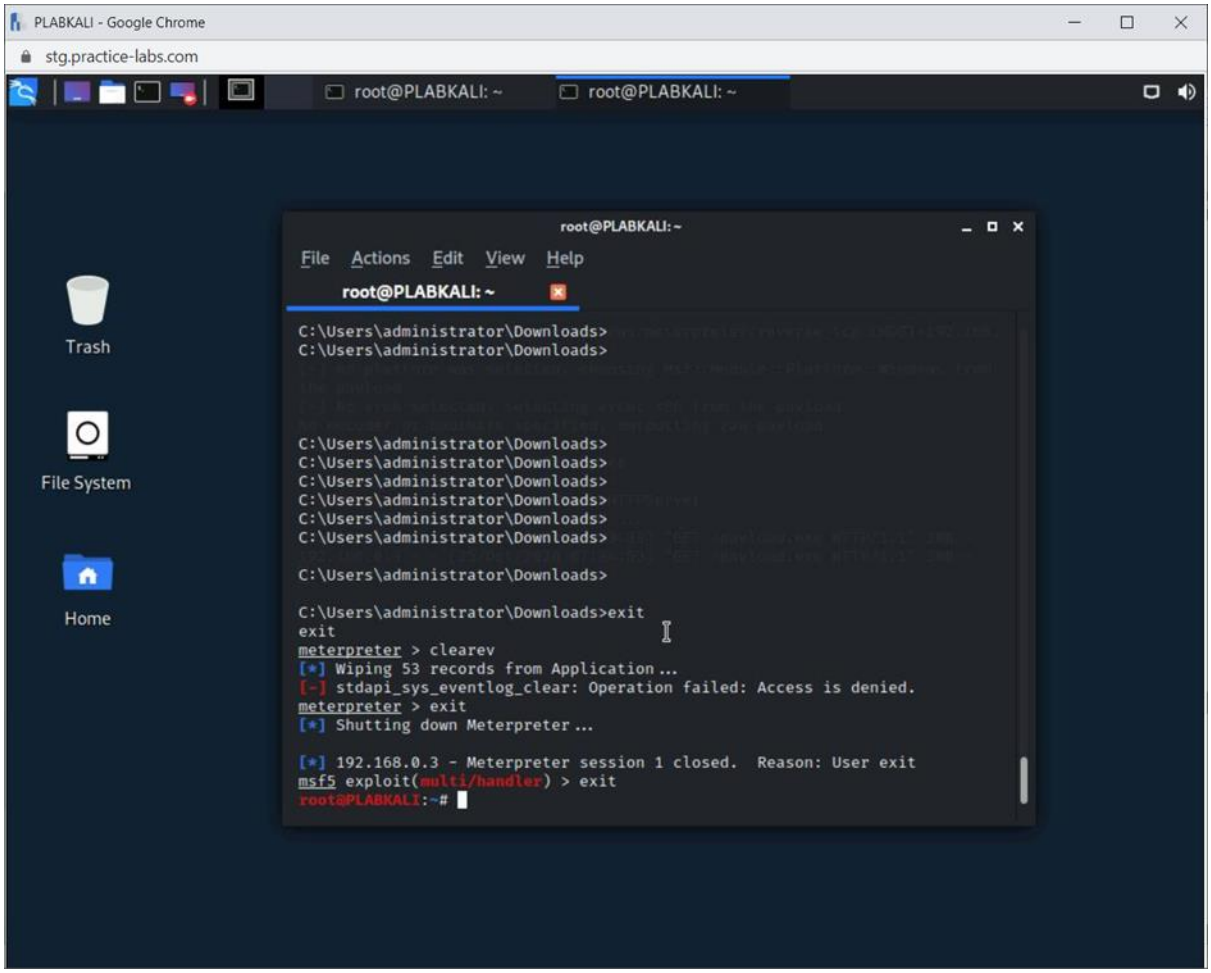
Question	Answer 1	Answer 2	Answer 3	Answer 4	Correct Answer
Which of the following malware does not harm the system but only targets the data?	**Ransomware**	Trojan	Worm	Logic bomb	1
Password spraying cyber-attack can be categorized as which of the following type of attack?	Dictionary	Wordlist	**Brute-force**	Unencrypted	3
A USB can be used to drop which of the following types of malware? [Choose all that apply]	**Backdoor**	**Trojan**	**Keyboard loggers**	**Worms**	1, 2, 3, 4
Which of the following statements are true for artificial intelligence (AI)? [Choose all that apply]	AI learns on its own without any input data	**Machine Learning or ML is a subset of AI**	**AI focuses on the broad idea of making a system execute a task**	**A self-driving car is an example of AI**	2, 3, 4
Which of the following type of attack is a pre-cursor to the collision attack?	**Birthday**	Downgrade	Brute-force	Dictionary	1

Exercise 1 – Screenshot



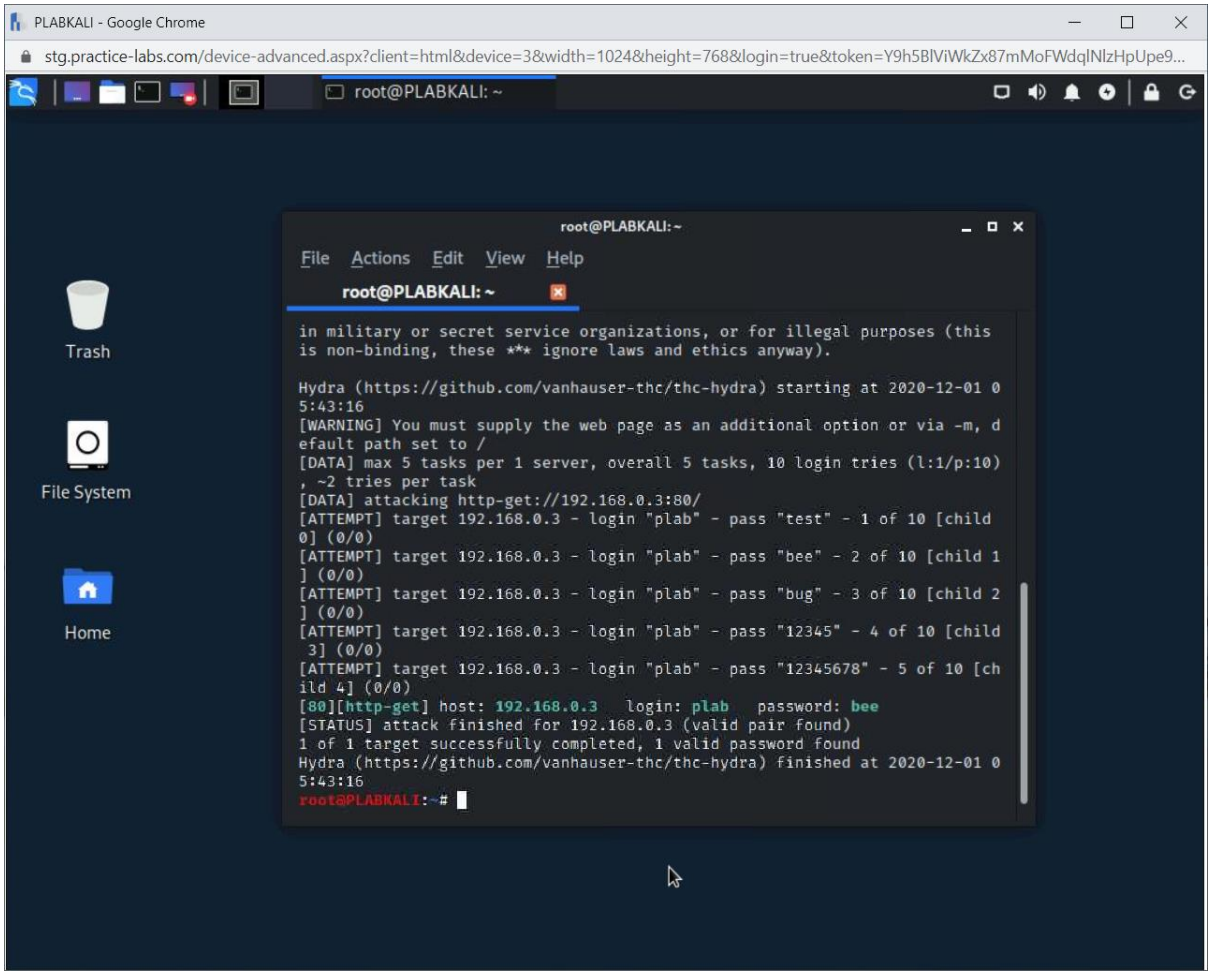
Screenshot of PLABWIN10: Showing the cmd.exe – Application Error dialog box with OK selected.

Exercise 2 – Screenshot



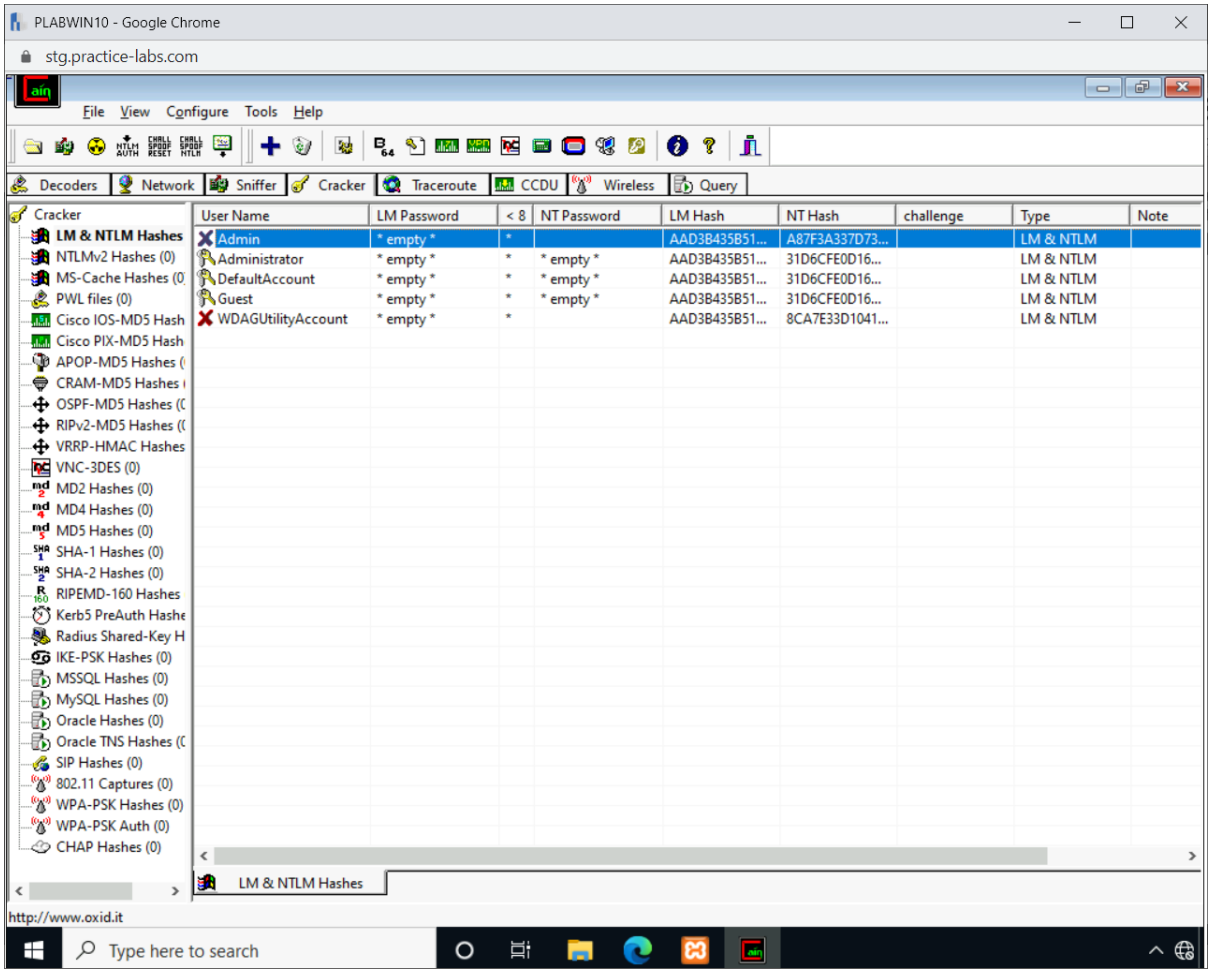
Screenshot of PLABKALI: Showing the terminal window prompt.

Exercise 3 – Screenshot



Screenshot of PLABKALI: Showing the output with the cracked password.

Exercise 4 – Screenshot



Screenshot of PLABWIN10: Showing the Cain window.

Exercise 5 – Screenshot

There is no screenshot assessment for this exercise.