Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 1/29/2022 7:28:28 pm • Time spent: 04:13

Score: 80% Passing Score: 80%

Question 1: ✔ Correct

An employee stealing company data could be an example of which kind of threat actor?

- External threat
- Non-persistent threat
- Persistent threat
- ➡ Internal threat

EXPLANATION

An internal threat consists of someone like an employee that uses their authorized privileges to carry out an attack.

A persistent threat is one that has a goal of remaining undetected and retaining access. While an internal threat could also be persistent, it does not need to be.

A non-persistent threat is generally a one-time event in which the malicious actor doesn't care if the attack is noticed. Again, it could also be an internal threat, but an internal threat does not necessarily have to be non-persistent.

An external threat attacks from the outside and seeks to gain unauthorized access to data.

Question 2: ✔ Correct

Which of the following is the BEST definition of the term *hacker?*

- A threat actor whose main goal is financial gain.
- The most organized, well-funded, and dangerous type of threat actor.
- Any individual whose attacks are politically motivated.
- ➡ A general term used to describe any individual who uses their technical knowledge to gain unauthorized access to an organization.
- A threat actor who lacks skills and sophistication but wants to impress their friends or garner attention.

EXPLANATION

The term *hacker* is a general term used to describe any individual who uses their technical knowledge to gain unauthorized access to an organization.

The following are specific types of hackers, also known as threat actors:

- A hacktivist is any individual whose attacks are politically motivated.
- A nation state is the most organized, well-funded, and dangerous type of threat actor.
- An organized crime threat actor is a group of cybercriminals whose main goal is financial gain.
- A script kiddie is a threat actor who lacks skills and sophistication but wants to impress their friends or garner attention. Script kiddies carry out an attack by using scripts or programs written by more advanced hackers.

Question 3: ✔ Correct

Which of the following threat actors seeks to defame, shed light on, or cripple an organization or government?

- Competitor
- Hacktivist
- Insider
- Nation state
- Script kiddie

EXPLANATION

A hacktivist is any individual whose attacks are politically motivated. Instead of seeking financial gain, hacktivists want to defame, shed light on, or cripple an organization or government. Hacktivists often work alone. Occasionally, they create unified groups with like-minded hackers. For example, the website wikileaks.org is a repository of leaked government secrets, some of which have been obtain by hacktivists.

Script kiddies are usually motivated by the chance to impress their friends or garner attention in the hacking community. Insider threat actors can be motivated by negative feelings toward their employer, bribes from a competitor, or personal financial gain. Competitors could be motivated by financial gain, competitor defamation, or obtaining industry secrets.

There are two primary motives for nation state attacks,seeking to obtain sensitive information (such as government secrets) or seeking to cripple the target's network or infrastructure.

Question 4: ✔ Correct

The IT manager in your organization proposes taking steps to deflect a potential threat actor. The proposal includes the following:

- Create and follow onboarding and off-boarding procedures.
- Employ the principal of least privilege.
- Have appropriate physical security controls in place.

Which type of threat actor do these steps guard against?

- Hacktivist
- Competitor
- Script kiddie
- ➡ Insider

EXPLANATION

Because insiders are one of the most dangerous and overlooked threats to an organization, you need to take the appropriate steps to protect against them, such as requiring mandatory vacations, creating and following onboarding and off-boarding procedure, employing the principal of least privilege, and having appropriate physical security controls in place.

A script kiddie is an individual who carries out an attack by using scripts or programs written by more advanced hackers.

A hacktivist is any individual whose attacks are politically motivated.

A competitor threat actor carries out attacks on behalf of an organization and targets competing companies.

Question 5: ✕ Incorrect

A script kiddie is a threat actor who lacks knowledge and sophistication. Script kiddie attacks often seek to exploit well-known vulnerabilities in systems.

What is the BEST defense against script kiddie attacks?

- ~~Build a comprehensive security approach that uses all aspects of threat prevention and protection.~~
- Keep systems up to date and use standard security practices.
- Properly secure and store data backups.
- Have appropriate physical security controls in place.
- Implement email filtering systems.

EXPLANATION

Because script kiddies lack knowledge and sophistication, their attacks often seek to exploit well-known vulnerabilities in systems. As such, defense against script kiddies involves keeping systems up-to-date and using standard security practices.

Having appropriate physical security controls in place is one of the steps that can be used to protect insider threat actors. Implementing email filtering systems and proper securing and storing data backups are two of the steps that can be used to protect against organized crime threat actors.

Because nation states use so many different attack vectors and unknown exploits, defending against these attacks involves building a comprehensive security approach that uses all aspects of threat prevention and protection.

Question 6: ✔ Correct

A hacker scans hundreds of IP addresses randomly on the internet until they find an exploitable target. What kind of attack is this?

- Insider attack
- ➡ Opportunistic attack
- Nation state attack
- Targeted attack

EXPLANATION

In this scenario, the hacker is looking for an easy target and doesn't care what they are attacking. This is considered an opportunistic attack.

If the hacker had been targeting a certain individual, company, organization, or nation, it would have been considered a targeted attack.

An insider attack is accomplished by a threat agent who has authorized access to an organization and either intentionally or unintentionally carries out an attack.

A nation state attack is accomplished by a threat agent that is a sovereign state who may wage an all-out war on a target and have significant resources and money at their disposal.

Question 7: ✔ Correct

Match the general attack strategy on the left with the appropriate description on the right. (Each attack strategy may be used once, more than once, or not all.)

Stealing information.

✔ Exploitation

Preparing a computer to perform additional tasks in the attack.

✔ Staging

Crashing systems.

✔ Exploitation

Gathering system hardware information.

✔ Reconnaissance

Penetrating system defenses to gain unauthorized access.

✔ Breaching

Configuring additional rights to do more than breach the system.

✔ Escalating privileges

EXPLANATION

General attack strategies include the following steps:

- Reconnaissance is the process of gathering information about an organization, including system hardware information, network configuration, and individual user information.
- A breach is the penetration of system defenses. Breaches are achieved using the information gathered during reconnaissance.
- An escalating privileges attack is one of the primary objectives of an attacker, which can be achieved by configuring additional (escalated) rights to do more than breach the system.
- Staging is preparing a computer to perform additional tasks in the attack, such as installing software designed to attack other systems.
- An Exploit is used to take advantage of known vulnerabilities in software and systems. Types of exploitation include stealing information, denying services, crashing systems, and modifying information.

Question 8: ✗ Incorrect

Match the general defense methodology on the left with the appropriate description on the right. (Each methodology may be used once, more than once, or not all.)

The constant change in personal habits and passwords to prevent anticipated events and exploitation.

✓ Randomness

Diversifying layers of defense.

✓ Variety

Giving users only the access they need to do their job and nothing more.

✓ Principle of least privilege

Implementing multiple security measures to protect the same asset.

✓ Layering

Eliminating single points of failure.

~~Variety~~ Layering

Giving groups only the access they need to do their job and nothing more.

✓ Principle of least privilege

EXPLANATION

General defense methodologies include the following items:

- Layering is the process of implementing multiple security measures to protect the same asset. Defense in depth or security in depth is the premise that no single layer is completely effective in securing the assets. The most secure system/network has many layers of security and eliminates single points of failure.
- When using the principle of least privilege, users or groups are given only the access they need to do their job and nothing more. When assigning privileges, be aware that it is often easier to give a user more access when they need it than to take away privileges that have already been granted.
- Defensive layers should have variety and be diverse. Implementing multiple layers of the exact same defense does not provide adequate strength against attacks.
- Randomness relies on the constant change in personal habits and passwords to prevent anticipated events and exploitation.
- Security measures should provide protection, but not be so complex that you do not understand and use them.

Question 9: ✔ Correct

Which of the following is the BEST example of the principle of least privilege?

- Lenny has been given access to files that he does not need for his job.
- Mary has been given access to all of the file servers.
- Jill has been given access to all of the files on one server.
- ➡ Wanda has been given access to the files that she needs for her job.

EXPLANATION

Wanda being given access only to what she needs to do her job is an example of the principle of least privilege.

The principle of least privilege states that users or groups are given only the access they need to do their jobs and nothing more.

Question 10: ✔ Correct

In which phase of an attack does the attacker gather information about the target?

- Breach the system
- Escalating privileges
- Exploit the system
- Reconnaissance

EXPLANATION

Reconnaissance is the phase of an attack where the attacker is gathering information about the target. This can be done electronically using scanning tools or even physically by going through dumpsters.

Escalation of privileges comes at the end of the attack when the attacker gains access to unauthorized data.

Breaching or exploiting the system is when the attacker gains access to a system on the target network using a vulnerability.

REFERENCES

- 11.2.4 Reconnaissance
- 11.2.5 Performing Reconnaissance
- 2.1.5 Attack and Defense Strategy Overview
- 2.3.1 Social Engineering Overview
- 2.3.10 Investigating a Social Engineering Attack
- 2.3.11 Identify Social Engineering
- 2.3.2 Social Engineering Overview Facts
- 2.3.3 Social Engineering Motivation
- 2.3.4 Social Engineering Motivation Facts
- 2.3.5 Social Engineering Techniques
- 2.3.6 Social Engineering Techniques Facts
- 2.3.7 Phishing and Internet-Based Techniques
- 2.3.8 Phishing and Internet-Based Techniques Facts
- 2.3.9 Use the Social Engineer Toolkit