Exam Report: 2.1.6 Practice Questions

Date: 1/9/2020 1:29:54 pm
Time Spent: 15:29

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 50%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

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

- 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.
- The most organized, well-funded, and dangerous type of threat actor.
- Any individual whose attacks are politically motivated.
- A threat actor whose main goal is financial gain.

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.

References

LabSim for Security Pro, Section 2.1.
[All Questions SecPro2017_v6.exm UND_ATT_01]

Question 2: Incorrect

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

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

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. Often times, hacktivists 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 stealing industry secrets.

There are two primary motives for nation state attacks:

- Seeking to obtain sensitive information, such as government secrets.
- Seeking to cripple the target's network or infrastructure.

References

LabSim for Security Pro, Section 2.1.
[All Questions SecPro2017_v6.exm UND_ATT_03]

Question 3: Correct

The IT manager in your organization proposes taking steps to protect against 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.

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

References

LabSim for Security Pro, Section 2.1.
[All Questions SecPro2017_v6.exm UND_ATT_04]

Question 4: 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?

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

◯ 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, defending 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 them involves building a comprehensive security approach that uses all aspects of threat prevention and protection.

References

LabSim for Security Pro, Section 2.1.
[All Questions SecPro2017_v6.exm UND_ATT_02]

Question 5: Incorrect

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.

~~Breaching~~ 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.

~~Escalating privileges~~ Breaching

Configuring additional rights to do more than breach the system.

✓ Escalating privileges

Explanation

General attack strategies include the following steps:

- **Reconnaissance**: the process of gathering information about an organization, including system hardware information, network configuration, and individual user information.
- **Breach**: the penetration of system defenses. Breaches are achieved using the information gathered during reconnaissance.
- **Escalate privileges**: 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**: preparing a computer to perform additional tasks in the attack, such as installing software designed to attack other systems.
- **Exploit**: taking advantage of known vulnerabilities in software and systems. Types of exploitation include stealing information, denying services, crashing systems, and modifying/altering information.

References

LabSim for Security Pro, Section 2.1.
[All Questions SecPro2017_v6.exm UND_ATT_05]

Question 6: Correct

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.

✔ 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**: 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.
- **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.
- **Variety**: defensive layers should have variety and be diverse; implementing multiple layers of the exact same defense does not provide adequate strength against attacks.
- **Randomness**: the constant change in personal habits and passwords to prevent anticipated events and exploitation.
- **Simplicity**: security measures should provide protection, but not be so complex that you do not understand and use them.

References

LabSim for Security Pro, Section 2.1.
[All Questions SecPro2017_v6.exm UND_ATT_06]