2.1.11 Section Quiz

Candidate: Seolito Rodríguez (rodriguez77)
Date: 5/13/2021 8:53:05 pm • Time spent: 06:01

Score: (80%) Passing Score: (80%)

Question 1: ✔ Correct

Which of the following BEST describes an unknown penetration test?

➡ The penetration tester has no information regarding the target or network.

The penetration tester is given partial information about the target or network.

The penetration tester simulates an insider threat.

The penetration tester is given full knowledge of the network.

EXPLANATION

An unknown penetration test (also called a black box penetration test) is when the penetration tester has no information about the target or network. This test can be done by an external tester and is best for simulating an outside attack that ignores insider threats.

A known penetration test (also called a white box penetration test) is the opposite of an unknown penetration test. The penetration tester is given full knowledge of the network, computer systems, and infrastructure.

A partially known penetration test (also called a grey box penetration test) is when the penetration tester is given partial information about the target or network, such as IP configurations or emails lists. This test simulates an insider threat.

Question 2: ✔ Correct

Which type of test simulates an insider threat by giving the tester partial information about the network and computer systems?

- Unknown
- Penetration
- Known
- ➡ Partially known

EXPLANATION

A partially known test (also called a grey box test) simulates an insider threat. The penetration tester is given partial information about the network and computer systems. This can be IP configurations, email lists, computer names, or other information an insider would realistically have.

A known test (also called a white box test) is the opposite of an unknown test. The penetration tester is given full knowledge of the network, computer systems, and infrastructure.

An unknown test (also called a black box test) is when the penetration tester has no information about the target or network. This test can be done by an external tester and is best for simulating an outside attack that ignores insider threats.

Question 3: ✕ Incorrect

Which type of testing is typically done by an internal tester who has full knowledge of the network, computer system, and infrastructure?

Unknown

Penetration

~~Partially known~~

➡ Known

EXPLANATION

A known test (also called a white box test) is the opposite of an unknown test (also called a black box test). The penetration tester is given full knowledge of the network, computer systems, and infrastructure.

An unknown test (also called a black box test) is when the penetration tester has no information about the target or network. This test can be done by an external tester and is best for simulating an outside attack that ignores insider threats.

A partially known test (also called a grey box test) simulates an insider threat. The penetration tester is given partial information about the network and computer systems. This can be IP configurations, email lists, computer names, or other information an insider would realistically have.

Question 4: ✔ Correct

Threats are usually ranked from high to low. A higher number indicates a dangerous threat. A lower number indicates threats that may be annoyances but aren't necessarily malicious in nature. What is this high-to-low scale known as?

- Indicator standards
- Intelligence cycle
- ➡ Confidence level
- InfraGard

EXPLANATION

When reviewing threat feeds, you may notice a confidence-level rating. Higher numbers indicate higher threat potential. Low numbers indicate threats that may be annoyances, but aren't necessarily malicious in nature.

Knowing how and when to use threat intelligence can be challenging. Some organizations use the security intelligence cycle to provide a standard approach for managing their intelligence strategy.

Indicators are bits of information that can be used to identify or describe a known threat. Indicators could include unusual activity, a unique file name, attack methods, or malicious commands. Managing threat information on a large scale could become messy without a standardized method for sharing information. Indicator standards include STIX, TAXII, and OpenIoC.

InfraGard provides a site for security collaboration between the FBI and industry professionals.

Question 5: ✓ Correct

There are five phases in the security intelligence life cycle. During which phase do you gather and process information from your internal sources, such as system and application logs?

Feedback

➡ Collection

Requirements

Dissemination

EXPLANATION

The collection phase is when you start pulling information from your previously identified sources. Information can then be gathered from internal sources, such as system and application logs. Additional information can be pulled from external, open-, or closed-sourced sources.

During the requirements phase, you determine what specific research you need to do.

The next phase is to disseminate the intelligence by distributing it to members of your security team and to members of your organization's leadership team.

Consider any feedback that you get from the reports you sent out. This can help you improve the requirements the next time through the cycle.

Question 6: ✗ Incorrect

Which type of intelligence helps security professionals respond to incidents or make decisions on the spot?

Strategic intelligence

~~Operational intelligence~~

Data intelligence

➡ Tactical intelligence

EXPLANATION

Tactical intelligence helps security professionals respond to incidents or make decisions on the spot.

Operational intelligence impacts the way managers plan day-to-day activities.

Strategic intelligence is information that impacts an organization's big-picture objectives. These objectives could be driving business plans and priorities for the coming year.

Data intelligence takes on multiple forms, including strategic, tactical, and operational.

Question 7: ✔ Correct

Sophisticated attacks executed by highly skilled hackers with a specific target or objective in mind are classified as which type of threat?

- ➡ Advanced persistent threat
- Zero-day threat
- Known threat
- Unknown threat

EXPLANATION

Advanced persistent threats are sophisticated, continuous hacking campaigns. The goal of these campaigns is usually to gain access to a system and to gather information or cause trouble for as long as possible. These attacks are usually executed by highly skilled hackers who have a specific target or objective in mind. They are often sponsored by government entities or criminal organizations with deep pockets.

Zero-day threats are threats that do not have an existing fix. They are not included in any security scans, and there are no patches available to protect a system from them.

Known threats are threats that you can prepare for. If it is a security vulnerability, you know which patches to install or which controls to put into place to better protect your resources.

Unknown threats exploit security weaknesses that you do not have information about and that you are only generally able to prepare for.

Question 8: ✔ Correct

Threats that do not have an existing fix, do not have any security fixes, and do not have available patches are called what?

- Unknown threats
- Advanced persistent threats
- Known threats
- ➡ Zero-day threats

EXPLANATION

Zero-day threats are threats that do not have an existing fix. They are not included in any security scans, and there are no patches available to protect a system from them.

Known threats are threats that you can prepare for. If it is a security vulnerability, you know which patches to install or which controls to put into place to better protect your resources.

Unknown threats exploit security weaknesses that you do not have information about and that you are only generally able to prepare for.

Advanced persistent threats are sophisticated, continuous hacking campaigns. These attacks are usually executed by highly skilled hackers who have a specific target or objective in mind.

Question 9: ✔ Correct

Threat actors can be divided into different types based on their methods and motivations. Which type of hacker usually targets government agencies, corporations, or other entities they are protesting?

- Nation-state
- Intentional
- ➡ Hacktivist
- Criminal

EXPLANATION

Hacktivists often target government agencies, corporations, or other entities they are protesting. Hacktivists are known for defacing websites and executing denial-of-service attacks. Their main purpose is to protest others' actions and campaign for public attention.

A nation-state hacker works for a government and attempts to gain top-secret information by hacking other governments' devices.

Criminal organizations have also transitioned much of their operations to virtual settings. The internet provides a wider range of targets and provides additional options for covering their tracks.

A threat actor does not necessarily have to be an outside hacker. He or she can be an internal threat or even someone who causes a security vulnerability through negligence.

Question 10: ✔ Correct

Threat actors can be divided into different types based on their methods and motivations. Which type of hacker works for a government and attempts to gain top-secret information by hacking other governments' devices?

- Intentional
- Criminal
- Hacktivist
- ➡ Nation-state

EXPLANATION

A nation-state hacker works for a government and attempts to gain top-secret information by hacking other governments' devices. Many nations have invested in the development of their cybersecurity presence and are willing to use this presence to reach their political or economic goals. Election systems, energy grids, and intelligence agencies are common targets.

Hacktivists often target government agencies, corporations, or other entities they are protesting. Hacktivists are known for defacing websites and executing denial-of-service attacks.

Criminal organizations have also transitioned much of their operations to virtual settings. Because criminals often target individuals in different jurisdictions, prosecution can be very difficult.

A threat actor does not necessarily have to be an outside hacker. He or she can be an internal threat or even someone who causes a security vulnerability through negligence.