

Exam Report: 7.2.5 Practice Questions

Date: 5/2/2020 6:32:20 pm
Time Spent: 0:38

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 13%



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

Which of the following phases of the vulnerability management lifecycle implements patches, hardening, and correction of weaknesses?

- ➡ ☒ The remediation phase
- ☐ The verification phase
- ☐ The risk assessment phase
- ☐ The monitoring phase

Explanation

The remediation phase is for implementing the needed patching, hardening, and correction of weaknesses.

The risk assessment phase is for evaluating the found vulnerabilities for threat level.

The verification phase is for retesting the system to verify that your patching and hardening was effective.

The monitoring phase is when continuous system monitoring is effective.

References

TestOut Ethical Hacker Pro - 7.2 Vulnerability Management Life Cycle

[e_vuln_lifecycle_eh1.exam.xml Q_VULN_LIFECYCLE_VULN_MGNT_LIFE_CYCLE_FACTS_01_EH1]

▼ Question 2: Incorrect

Rose, an ethical hacker, has created a report that clearly identifies her findings and recommendations for locking down an organization's systems and patching problems. Which of the following phases of the vulnerability management life cycle is she working in?

- ☒ ~~Remediation~~
- ☐ Create a baseline
- ➡ ☐ Risk assessment
- ☐ Verification

Explanation

Risk assessment is the phase of evaluating the found vulnerabilities for threat level. You will need to create reports that clearly identify the problem areas to present to management. Then produce a plan of action to control the weaknesses, protect the information, and harden the systems.

Verification is the phase of retesting the system to verify that your patching and hardening was effective.

Remediation is the phase of implementing the necessary patching, hardening, and correction of weaknesses.

Create a baseline is the phase of defining the effectiveness of the current security policies and procedures.

References

TestOut Ethical Hacker Pro - 7.2 Vulnerability Management Life Cycle

[e_vuln_lifecycle_eh1.exam.xml Q_VULN_LIFECYCLE_VULN_MGNT_LIFE_CYCLE_FACTS_02_EH1]

▼ Question 3:

Incorrect

Which of the following best describes the verification phase of the vulnerability management life cycle?

- ☐ Communicate clearly to management what your findings and recommendations are for locking down the systems and patching problems.
- ➡ ☐ Proves your work to management and generates verifiable evidence to show that your patching and hardening implementations have been effective.
- ☒ ~~Is critical to ensure that organizations have monitoring tools in place and have regularly scheduled vulnerability maintenance testing.~~
- ☐ Protect the organization from its most vulnerable areas first and then focus on less likely and less impactful areas.

Explanation

The verification phase helps the security analyst to verify whether all the previous phases are effectively employed or not. So, in this phase, you retest the systems for verification. Even though you may be certain that you have corrected vulnerability issues and are confident in your work, you want to prove your work to management and have verifiable evidence to show that your patching and hardening implementations have been effective. You increase the value of your services when you can show the validity of your work.

In the risk assessment phase, it is critical to communicate clearly to management what your findings and recommendations are for locking down the systems and patching problems.

In the remediation phase, it makes the most sense to protect the organization from its most vulnerable areas first and then work to the less likely and less impactful areas.

In the monitor phase, it is critical that the organization have monitoring tools in place and have regularly scheduled vulnerability maintenance testing.

References

TestOut Ethical Hacker Pro - 7.2 Vulnerability Management Life Cycle

[e_vuln_lifecycle_eh1.exam.xml Q_VULN_LIFECYCLE_VULN_MGNT_LIFE_CYCLE_FACTS_03_EH1]

▼ Question 4:

Incorrect

You are an ethical hacker contracting with a medical clinic to evaluate their environment. Which of the following is the first thing you should do?

- ☒ ~~Decide the best times to test to limit the risk of having shutdowns during peak business hours.~~
- ➡ ☐ Define the effectiveness of the current security policies and procedures.
- ☐ Choose the best security assessment tools for the systems you choose to test.
- ☐ Create reports that clearly identify the problem areas to present to management.

Explanation

During the create a baseline phase, you start by defining the effectiveness of the current security policies and procedures. Establish the risks with how the security procedures are enforced and what may be overlooked. Try to see what the organization looks like from an outsider's perspective, as well as from an insider's point of view. No organization is immune to security gaps. Set goals with management with

start dates and end dates. Determine which systems to begin with, set up testing standards, get approval during the vulnerability assessment phase, it is important to decide the best times to test, as you don't want to risk having systems shut down during peak business hours or other sensitive times. You must also choose the best security assessment tools for the systems you choose to test.

During the risk assessment phase, you create reports that clearly identify the problem areas to present to management.

References


TestOut Ethical Hacker Pro - 7.2 Vulnerability Management Life Cycle

[e_vuln_lifecycle_eh1.exam.xml Q_VULN_LIFECYCLE_VULN_MGNT_LIFE_CYCLE_FACTS_04_EH1]

Question 5:

Incorrect

It may be tempting for an organization to feel secure after going through the process of penetration testing and the corrections and hardening that you must perform. Which of the following should you help them to understand?

- ☐ The risks associated with enforcing security procedures and what threats may have been overlooked.
- ☒ ~~They need a plan of action to control weaknesses and harden systems.~~
-  ☐ Hackers have time on their side, and there will always be new threats to security.
- ☐ How to define the effectiveness of the current security policies and procedures.

Explanation

It may be tempting for an organization to feel secure after going through the process of penetration testing and the corrections and hardening that you have performed, but it's important for you to help them understand that hackers have time on their side, and there will always be ongoing and new threats to security. Therefore, it is critical that the organization have monitoring tools in place and have regularly scheduled vulnerability maintenance testing.

Taking the results of your vulnerability testing, organizing it according to risk level, and categorizing it by levels of sensitivity and access is risk management. You will need to create reports that clearly identify the problem areas to present to management. Then produce a plan of action to control the weaknesses, protect the information, and harden the systems.

Defining the effectiveness of the current security policies and procedures is part of creating a baseline. Establish the risks with how the security procedures are enforced and what may be overlooked.

References


TestOut Ethical Hacker Pro - 7.2 Vulnerability Management Life Cycle

[e_vuln_lifecycle_eh1.exam.xml Q_VULN_LIFECYCLE_VULN_MGNT_LIFE_CYCLE_FACTS_05_EH1]

Question 6:

Incorrect

Which of the following solutions creates the risk that a hacker might gain access to the system?

- ☐ Product-based
- ☐ Tree-based
- ☒ ~~Inference-based~~
-  ☐ Service-based

Explanation

A service-based solution is when a professional like yourself is hired to provide a solution. This would involve the vulnerability management life cycle. You would conduct the testing and solutions from outside the network. The risk of this approach is that, because it is from the outside, there is some potential for a hacker to gain access to the system.

A product-based solution is when a product is purchased and administered from inside the network, so it's inside the firewall. This would make it inaccessible from outside penetration. An organization could

purchase a product and install it, hoping that it solves vulnerability issues.

With a tree-based assessment, you have a pre-set plan for testing and scanning based on some previous knowledge of the system. You then choose specific testing modes for each operating system and machine.

In an inference-based approach, you test and discover information as you go, then adjust your scan according to the information you are acquiring based on your discoveries.

References

TestOut Ethical Hacker Pro - 7.2 Vulnerability Management Life Cycle

[e_vuln_lifecycle_eh1.exam.xml Q_VULN_SOLUTIONS_ASSESS_SOLUTION_01_EH1]

▼ Question 7:

Incorrect

Which of the following assessment types relies on each step to determine the next step, and then only tests relevant areas of concern?

- ➡ ☐ Inference-based
- ☐ Service-based
- ☒ Tree-based
- ☐ Product-based

Explanation

In an inference-based approach, you test and discover information as you go and then adjust your scan according to the information you acquire based on your discoveries.

A service-based solution is when a professional like yourself is hired to provide a solution. This process involves the vulnerability management life cycle. You conduct the testing and solutions from outside the network. The risk of this approach is that because it is based from the outside, there is some potential for a hacker to gain access to the system.

A product-based solution is when a product is purchased and administered from inside the network, so it's inside the firewall. This would make it inaccessible from outside penetration. An organization could purchase a product and install it, hoping that it solves vulnerability issues.

With a tree-based assessment, you have a preset plan for testing and scanning based on some previous knowledge of the system. You then choose specific modes of testing for each operating system and machine.

References

TestOut Ethical Hacker Pro - 7.2 Vulnerability Management Life Cycle

[e_vuln_lifecycle_eh1.exam.xml Q_VULN_SOLUTIONS_ASSESS_TYPE_01_EH1]

▼ Question 8:

Incorrect

First, you must locate the live nodes in the network. Second, you must itemize each open port and service in the network. Finally, you test each open port for known vulnerabilities. These are the three basic steps in which of the following types of testing?

- ☒ Baseline
- ☐ Stress
- ➡ ☐ Penetration
- ☐ Patch level

Explanation

As you conduct vulnerability scanning, it's important to understand that there are three basic steps in penetration testing.

- First, you must locate the live nodes in the network.

- Finally, you use each open port for known vulnerabilities in the network.

Baselines are used to define what is normal behavior on the network or host.

A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it.

In a stress test, you put your workstation or server under a heavy load to test its reliability.

References

TestOut Ethical Hacker Pro - 7.2 Vulnerability Management Life Cycle

[e_vuln_lifecycle_eh1.exam.xml Q_VULN_SOLUTIONS_VULN_SCAN_PEN_STEPS_01_EH1]