Exam Report: 2.4.4 Practice Questions

Date: 4/4/29 4:00:12 pm
Time Spent: 6:03

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 54%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which type of penetration test is required to ensure an organization is following federal laws and regulations?

- Goal-based
- Objective-based
- Compliance-based
- White box

Explanation

Compliance-based penetration tests are required to ensure an organization follows federal laws and regulations.

A goal-based penetration test focuses on end results. The test's goals are specific, but the methods for reaching them are determined by the hacker himself.

An objective-based test focuses on the overall security of the organization and its data security. When people think of a penetration test, this is often what they think of.

A white box test occurs when an ethical hacker is given full information about the target or network.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_COMPBASE_PENTEST_01_EH1]

Question 2: Correct

Which of the following defines the security standards for any organization that handles cardholder information for any type of payment card?

- HIPAA
- PCI DSS
- DMCA
- FISMA

Explanation

The Payment Card Industry Data Security Standards (PCI DSS) defines the security standards for any organization that handles cardholder information for debit cards, credit cards, prepaid cards, and any other type of payment cards.

The Health Insurance Portability and Accountability Act (HIPPA) was created as health records and data started being stored electronically. Its goal is to create a set of standards that would ensure this

information is kept safe and is only shared with the patient and medical professionals that need it.

The Digital Millennium Copyright Act (DMCA) was enacted in 1998 to protect copyrighted works.

The Federal Information Security Management Act (FISMA) was signed into law in 2002 and defines how federal government data, operations, and assets are handled.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_COMPBASE_PENTEST_02_EH1]

Question 3: Correct

Michael is performing a penetration test for a hospital. Which federal regulation does Michael need to ensure he follows?

- PCI DSS
- HIPAA
- DMCA
- FISMA

Explanation

The Health Insurance Portability and Accountability Act (HIPPA) was created as health records and data started being stored electronically. Its goal is to create a set of standards that would ensure this information is kept safe and is only shared with the patient and medical professionals that need it.

The Payment Card Industry Data Security Standards (PCI DSS) defines the security standards for any organization that handles cardholder information for debit cards, credit cards, prepaid cards, and any other type of payment cards.

The Digital Millennium Copyright Act (DMCA) was enacted in 1998 to protect copyrighted works.

The Federal Information Security Management Act (FISMA) was signed into law in 2002 and defines how federal government data, operations, and assets are handled.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_COMPBASE_PENTEST_03_EH1]

Question 4: Correct

Charles found a song he wrote being used without his permission in a video on YouTube. Which law will help him protect his work?

- PCI DSS
- FISMA
- DMCA
- HIPAA

Explanation

The Digital Millennium Copyright Act (DMCA) was enacted in 1998 to protect copyrighted works.

The Payment Card Industry Data Security Standards (PCI DSS) defines the security standards for any organization that handles cardholder information for debit cards, credit cards, prepaid cards, and any other type of payment cards.

The Health Insurance Portability and Accountability Act (HIPPA) was created as health records and data started being stored electronically. Its goal is to create a set of standards that would ensure this information is kept safe and is only shared with the patient and medical professionals that need it.

The Federal Information Security Management Act (FISMA) was signed into law in 2002 and defines

how federal government data, operations, and assets are handled.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_COMPBASE_PENTEST_04_EH1]

Question 5: Correct

Which of the following best describes what FISMA does?

- Defines the security standards for any organization that handles cardholder information
- Defines standards that ensure medical information is kept safe.
- Defines how federal government data, operations, and assets are handled.
- Implements accounting and disclosure requirements that increase transparency.

Explanation

The Federal Information Security Management Act (FISMA) was signed into law in 2002 and defines how federal government data, operations, and assets are handled.

The Sarbanes Oxley Act (SOX) was enacted in 2002 with the goal of implementing accounting and disclosure requirements that would increase transparency in corporate governance and financial reporting and formalize a system of internal checks and balances.

The Payment Card Industry Data Security Standards (PCI DSS) defines the security standards for any organization that handles cardholder information for debit cards, credit cards, prepaid cards, and any other type of payment cards.

The Health Insurance Portability and Accountability Act (HIPPA) was created as health records and data started being stored electronically. Its goal is to create a set of standards that ensure this information is kept safe and is only shared with the patient and medical professionals that need it.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_COMPBASE_PENTEST_05_EH1]

Question 6: Incorrect

Which of the following best describes what SOX does?

- Defines how federal government data, operations, and assets are handled.
- ~~Defines standards that ensure medical information is kept safe.~~
- Defines the security standards for any organization that handles cardholder information.
- Implements accounting and disclosure requirements that increase transparency.

Explanation

The Sarbanes Oxley Act (SOX) was enacted in 2002 with the goal of implementing accounting and disclosure requirements that would increase transparency in corporate governance and financial reporting and formalize a system of internal checks and balances.

The Federal Information Security Management Act (FISMA) was signed into law in 2002 and defined how federal government data, operations, and assets were handled.

The Payment Card Industry Data Security Standards (PCI DSS) defines the security standards for any organization that handles cardholder information for debit cards, credit cards, prepaid cards, and any other type of payment cards.

The Health Insurance Portability and Accountability Act (HIPPA) was created as businesses began storing health records and data electronically. HIPPA's goal is to create a set of standards that ensure medical information is kept safe and is only shared with the patient and medical professionals that need it.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_COMPBASE_PENTEST_06_EH1]

Question 7: Incorrect

Which of the following is a limitation of relying on regulations?

- They are regularly updated.
- They allow interpretation.
- They rely heavily on password policies.
- ~~The industry standards take precedence.~~

Explanation

One of the drawbacks to many federal regulations is that they rely heavily on password policies, which are often outdated.

Federal regulations are not updated regularly and can fall behind accepted best practices.

Federal regulations take precedence over industry standards because they're mandated by the government.

Federal regulations are very defined and can limit security management options.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_COMPBASE_PENTEST_07_EH1]

Question 8: Incorrect

Which of the following best describes a goal-based penetration test?

- Focuses on the overall security of the organization and its data security.
- The hacker has been given full information about the target.
- Focuses on the end results. The hacker determines the methods.
- ~~Ensures the organization follows federal laws and regulations.~~

Explanation

A goal-based penetration test focuses on end results. The goals are specific, but the methods for reaching them are determined by the hacker himself.

An objective-based test focuses on the overall security of the organization and its data security. When people think of a penetration test, this is often what they think of.

Compliance-based penetration tests are needed to ensure an organization follows federal laws and regulations.

A white box test means the ethical hacker has been given full information about a target or network.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_GOALBASE_PENTEST_01_EH1]

Question 9: Correct

A goal-based penetration test needs to have specific goals. Using SMART goals is extremely useful for this. What does SMART stand for?

- Specific/Measurable/Attainable/Relevant/Timely
- Steps/Maintainable/Affordable/Results/Tuned

- Steps/Measurable/Affordable/Results/Tuned
- Specific/Maintainable/Attainable/Relevant/Timely

Explanation

SMART goals are very useful when establishing and defining the goals of a penetration test. SMART goals help create goals that are specific, measurable, attainable, relevant, and timely (or time-bound).

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_GOALBASE_PENTEST_02_EH1]

Question 10: Incorrect

Which document explains the details of an objective-based test?

- Scope of work
- Change order
- ~~Permission to test~~
- Rules of engagement

Explanation

The scope of work is a very detailed document that defines exactly what is going to be included in a penetration test. This document is also referred to as the statement of work.

When a change to the scope of work is requested, a change order should be filled out and agreed on by all pertinent stakeholders. Once this is done, the additional tasks can be completed.

The rules of engagement document details how the test will be carried out.

The permission to test is often referred to as the get-out-of-jail-free card. Since most people in the client's organization will not know about the penetration test occurring, this document is used if the penetration tester gets caught.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_OBJBASE_PENTEST_01_EH1]

Question 11: Correct

Which of the following best describes a supply chain?

- A company sells their products on Amazon and has Amazon ship the product.
- A company stores their product at a distribution center.
- A company stocks their product at a store.
- A company provides materials to another company to manufacture a product.

Explanation

A supply chain is set up when materials from one company are needed from another to manufacture a product.

A company may work with a store to stock their products to be sold, but this is not a supply chain.

Oftentimes, companies use a third-party distribution center to ship sold products to customers, but this is not a supply chain.

Some online retailers, such as Amazon, do sometimes act as a distribution center for sellers, but this is not a supply chain because Amazon is not using the sellers' materials to create a new product.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_SPECIAL_CONSID_01_EH1]

Question 12: Incorrect

Heather has been hired to work in a firm's cybersecurity division. Her role will include performing both offensive and defensive tasks. Which of the following roles applies to Heather?

- A member of the purple team.
- ~~A gray hat hacker.~~
- A member of the red team.
- A black hat hacker.

Explanation

The purple team is a mix of red and blue team members. They basically act as a pipeline between the two teams and can work on either side.

The red team consistently works against the blue team to test the organization's security stance, while the blue team focuses on the organization's defensive security. The red team is responsible for establishing and implementing policies and closing vulnerabilities.

A black hat hacker is a skilled hacker who uses skills and knowledge for illegal or malicious purposes.

A gray hat hacker may cross the line of what is ethical, but usually has good intentions and isn't malicious like a black hat hacker.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_SPECIAL_CONSID_02_EH1]

Question 13: Incorrect

ABC company is in the process of merging with XYZ company. As part of the merger, a penetration test has been recommended. Testing the network systems, physical security, and data security have all been included in the scope of work. What else should be included in the scope of work?

- Password policies
- ~~Employee IDs~~
- Company culture
- Email policies

Explanation

During the premerger, areas such as physical security, data security, company culture, and network systems need to be tested. A penetration test during this phase can help identify shortcomings and large differences that if left unattended could lead to disastrous results after the merger or acquisition.

Email and password policies are already included in the network systems test.

Employee IDs are included in the physical security test.

References

TestOut Ethical Hacker Pro - 2.4 Assessment Types
[e_assessment_types_eh1.exam.xml Q_ASSESSMENT_TYPES_SPECIAL_CONSID_03_EH1]