

Exam Report: 2.5.7 Practice Questions

Date: 4/4/29 4:27:30 pm
Time Spent: 12:55

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 40%



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

Hannah is working on the scope of work with her client. During the planning, she discovers that some of the servers are cloud-based servers. Which of the following should she do?

- ☐ Tell the client she can't perform the test.
- ➡ ☒ Add the cloud host to the scope of work.
- ☐ Get a non-disclosure agreement.
- ☐ Not worry about this fact and test the servers.

Explanation

Since Hannah is in the planning stage, she will need to add the cloud host to the scope of work. Cloud-based systems require some extra steps before penetration testing can begin. The issue is that the systems aren't owned by the client, but by the cloud hosting provider. An organization might be required to conduct penetration tests to meet regulations. But, in this case, the cloud provider must also authorize the penetration test and will need to be involved and approve the scope of work.

A non-disclosure agreement is a common legal contract that outlines confidential material or information that will be shared during the assessment and the restrictions placed on it.

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance
[e_framework_legal_ethics_eh1.exam.xml Q_LEGAL_ETHICS_CLOUD_BASE_01_EH1]

▼ Question 2: Incorrect

During an authorized penetration test, Michael discovered his client's financial records. Which of the following should he do?

- ☐ Continue digging and look for illegal activity.
- ➡ ☐ Ignore the records and move on.
- ☒ ~~Make a backup of the records for the client.~~
- ☐ Sell the records to a competitor.

Explanation

During a penetration test, the ethical hacker will run across or gain access to highly sensitive data. This could include clients' financial information, customer data, passwords, and more. In this situation, the hacker is expected to keep this information confidential and not view any more than is necessary for reporting purposes.

The penetration tester has no reason to make a backup of the records.

The penetration tester should not continue digging and look for illegal activity.

The penetration tester should not sell or divulge any information.

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance

[e_framework_legal_ethics_eh1.exam.xml Q_LEGAL_ETHICS_CORP_POLICY_01_EH1]

▼ Question 3: Incorrect

During a penetration test, Heidi runs into an ethical situation she's never faced before and is unsure how to proceed. Which of the following should she do?

- ☐ Ignore the situation and just move on.
- ☒ ~~Trust her instincts and do what she feels is right.~~
- ➡ ☐ Reach out to an attorney for legal advice.
- ☐ Talk with her friend and do what they suggest.

Explanation

Whenever a penetration tester is unsure of how to proceed with a situation, a lawyer should be contacted to make sure no laws are broken.

Heidi should not trust her instincts and do what she thinks is best, as she could easily become liable for a number of actions.

Heidi should not just ignore the situation; she should obtain more information about ethically performing her tasks.

Heidi should not reach out to her friend, as this violates confidentiality. Additionally, her friend may not completely understand the legal requirements for the situation.

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance

[e_framework_legal_ethics_eh1.exam.xml Q_LEGAL_ETHICS_CORP_POLICY_03_EH1]

▼ Question 4: Incorrect

What are the rules and regulations defined and put in place by an organization called?

- ☐ Scope of work
- ☐ Rules of engagement
- ☒ ~~Master service agreement~~
- ➡ ☐ Corporate policies

Explanation

Corporate policies are the rules and regulations that are defined and put in place by an organization. As part of the risk assessment and penetration test, these policies should be reviewed and tested.

The master service agreement is a contract where parties agree to the terms that will govern future actions. This makes future services and contracts much easier to handle and define.

The rules of engagement define exactly how work will be carried out.

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

References


TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance

[e_framework_legal_ethics_eh1.exam.xml Q_LEGAL_ETHICS_CORP_POLICY_04_EH1]

▼ Question 5: Correct

Which of the following is a common corporate policy that would be reviewed during a penetration test?



-  ☒ Password policy
- ☐ Parking policy
- ☐ Purchasing policy
- ☐ Meeting policy

Explanation

The password policy will usually state how many and what types of characters a password should contain. The policy will also state when the password can be changed.

Meeting policies and procedures would not be reviewed during a penetration test.

Purchasing policies and procedures would not be reviewed during a penetration test.

Parking policies and procedures would not be reviewed during a penetration test.


References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance

[e_framework_legal_ethics_eh1.exam.xml Q_LEGAL_ETHICS_CORP_POLICY_05_EH1]

▼ Question 6: Correct

Which of the following policies would cover what you should do in case of a data breach?

-  ☒ Sensitive data handling policy
- ☐ Corporate data policy
- ☐ Password policy
- ☐ Update frequency policy

Explanation

The policy for handling sensitive data should detail who has access to data, how data is secured, and what to do if an unauthorized person gains access to the data.

The password policy usually states how many and what types of characters a password should contain. The policy also states when the password can be changed.

How often and when updates are pushed out to computers should be defined in the organization's policies. This update schedule needs to be frequent enough to ensure that the network systems have the latest security patches and should not impact business operations.

Corporate policies are the rules and regulations that have been defined and put in place by the organization. As part of the risk assessment and penetration test, these policies should be reviewed and tested.


References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance

[e_framework_legal_ethics_eh1.exam.xml Q_LEGAL_ETHICS_CORP_POLICY_07_EH1]

▼ Question 7: Correct

Yesenia was recently terminated from her position, where she was using her personal cell phone for business purposes. Upon termination, her phone was remotely wiped. Which of the following corporate policies allows this action?

- ☐ Password policy
-  ☒ BYOD policy
- ☐ Update policy
- ☐ Corporate policy

Explanation

The BYOD policy must define the level of access employees have to company hardware and data and state clearly what happens on termination of employment. Usually, when an employee leaves the company, the device can be remotely wiped, and the employee needs to understand that they are giving the organization rights and access to do this.

The password policy will usually state how many and what type of characters a password should contain. The policy will also state when the password can be changed.

How often and when updates are pushed out to computers should be defined in the organization's policies. This update schedule needs to be frequent enough to ensure that the network systems have the latest security patches and should not impact business operations.

Corporate policies are the rules and regulations that have been defined and put in place by the organization. As part of the risk assessment and penetration test, these policies should be reviewed and tested.

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance

[e_framework_legal_ethics_eh1.exam.xml Q_LEGAL_ETHICS_CORP_POLICY_08_EH1]

▼ Question 8:

Incorrect

During a penetration test, Mitch discovers child pornography on a client's computer. Which of the following actions should he take?

☐ Delete the files and continue with the penetration test.

☒ ~~Ignore the files and continue with the penetration test.~~

➡ ☐ Immediately stop the test and report the finding to the authorities.

☐ Stop the test, inform the client, and let them handle it.

Explanation

If, during the scope of the penetration test, the hacker discovers evidence of illegal activity, they are legally obligated to report the evidence to the appropriate authorities.

If the penetration tester does anything besides reporting this to the authorities, they can be held legally liable.

Deleting the files would be illegal.

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance

[e_framework_legal_ethics_eh1.exam.xml Q_LEGAL_ETHICS_ETHICAL_SCENARIO_01_EH1]

▼ Question 9:

Correct

Heather is working for a cybersecurity firm based in Florida. She will be conducting a remote penetration test for her client, who is based in Utah. Which state's laws and regulations will she need to adhere to?

☐ Both companies will need to adhere to Utah's laws.

☐ Heather will adhere to Florida's laws, and the client will adhere to Utah's laws.

➡ ☒ Both companies need to agree on which laws to adhere to.

☐ Both companies will need to adhere to Florida's laws.

Explanation

In a scenario like this, there is not a standard that states which set of laws should be followed. Generally, in a case like this, the penetration tester and organization need to agree on which laws to adhere to. Whenever there are any questions or concerns regarding laws and regulations, a lawyer should be consulted.

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance

[e_framework_legal_ethics_eh1.exam.xml Q_LEGAL_ETHICS_FACTS_01_EH1]

▼ Question 10: Incorrect

United States Code Title 18, Chapter 47, Section 1029 deals with which of the following?

- ☐ Fraud and related activity regarding identity theft.
- ☐ Fraud and related activity involving computers.
- ➡ ☐ Fraud and related activity involving access devices.
- ☒ ~~Fraud and related activity involving electronic mail.~~

Explanation

Section 1029 refers to fraud and related activity involving access devices. An access device is defined as any application or hardware that is created specifically to generate any type of access credentials.

Section 1030 refers to fraud and related activity with computers. This section covers pretty much any device that connects to a network.

Section 1028A refers to fraud and related activity related to identity theft.

Section 1037 refers to fraud and related activity involving electronic mail.

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance

[e_framework_legal_ethics_eh1.exam.xml Q_LEGAL_ETHICS_FEDERAL_LAW_01_EH1]

▼ Question 11: Incorrect

Which of the following best describes the Wassenaar Arrangement?

- ☐ A law that defines the security standards for any organization that handles cardholder information.
- ☒ ~~A law that defines how federal government data, operations, and assets are handled.~~
- ☐ Standards that ensure medical information is kept safe and is only shared with the patient and medical professionals.
- ➡ ☐ An agreement between 41 countries to enforce similar export controls for weapons, including intrusion software.

Explanation

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is an agreement between 41 countries that generally hold similar views on human rights. The arrangement encourages the participating countries to hold similar export controls on weapons, including banning some and requiring licensing for others. This also includes intrusion software.

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 really any other type of payment cards.

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

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance

[e_framework_legal_ethics_eh1.exam.xml Q_LEGAL_ETHICS_THIRD_PARTY_02_EH1]

▼ Question 12: Incorrect

Which of the following best describes the rules of engagement document?

- ☒ ~~A very detailed document that defines exactly what is going to be included in the penetration~~

test.

- ➡ ☐ Defines if the test will be a white box, gray box, or black box test and how to handle sensitive data.
- ☐ Used as a last resort if the penetration tester is caught in the scope of their work.
- ☐ A contract where parties agree to most of the terms that will govern future actions.

Explanation

The rules of engagement define if the test will be a white box, gray box, or black box test. It should also explicitly state how to handle sensitive data and outline a process for communicating with the IT department about any issues that may arise during the test.

The scope of work is a very detailed document that defines exactly what is going to be included in the penetration test. This document is also referred to as the statement of work. This document should answer the who, what, when, where, and why of the test.

The master service agreement is a contract where parties agree to most of the terms that will govern future actions. This makes future services and contracts much easier to handle and define.

The permission to test is used as a last resort if the penetration tester is caught in the scope of their work. This get-out-of-jail-free card explains what the penetration tester is doing and that his work is authorized.

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance
[e_framework_legal_ethics_eh1.exam.xml Q_ENGAGE_CONTRACTS_FACTS_01_EH1]

▼ Question 13: Incorrect

Which of the following best describes a master service agreement?

- ➡ ☐ A contract where parties agree to the terms that will govern future actions.
- ☐ Used as a last resort if the penetration tester is caught in the scope of their work.
- ☒ ~~Defines if the test will be a white box, gray box, or black box test and how to handle sensitive data.~~
- ☐ A very detailed document that defines exactly what is going to be included in the penetration test.

Explanation

The master service agreement is a contract where parties agree to the terms that will govern future actions. This makes future services and contracts much easier to handle and define.

The rules of engagement define whether the test will be a white box, gray box, or black box test. It should also explicitly state how to handle sensitive data and how to work with the IT department if issues arise during the test.

The scope of work is a very detailed document that defines exactly what is going to be included in the penetration test. This document is also referred to as the statement of work. It should explain the who, what, when, where, and why of test.

The permission to test is used as a last resort if the penetration tester is caught in the scope of their work. This get-out-of-jail-free card explains what the penetration tester is doing and that his work is authorized.

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance
[e_framework_legal_ethics_eh1.exam.xml Q_ENGAGE_CONTRACTS_FACTS_02_EH1]

▼ Question 14: Incorrect

Which of the following best describes a non-disclosure agreement?

- ☐ A very detailed document that defines exactly what is going to be included in the penetration

test.

- ☐ A document that defines if the test will be a white box, gray box, or black box test and how to handle sensitive data.
- ➡ ☐ A common legal contract outlining confidential material that will be shared during the assessment.
- ☒ ~~A contract where parties agree to most of the terms that will govern future actions.~~

Explanation

A non-disclosure agreement (NDA) is a common legal contract that outlines confidential material or information that will be shared during the assessment and what restrictions are placed on it. This contract basically states that anything the tester finds cannot be shared except with the people specified in the document.

The rules of engagement define whether the test will be a white box, gray box, or black box test. It should also explicitly state how to handle sensitive data. If, during the test, something happens and the IT team needs to be notified, that process should also be laid out in this document.

The scope of work is a very detailed document that defines exactly what is going to be included in the penetration test. This document is also referred to as the statement of work. It should answer the who, what, when, where, and why of test.

The master service agreement is a contract where parties agree to most of the terms that will govern future actions. This makes future services and contracts much easier to handle and define.

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance
[e_framework_legal_ethics_eh1.exam.xml Q_ENGAGE_CONTRACTS_FACTS_03_EH1]

▼ Question 15: Correct

During a penetration test, Dylan is caught testing the physical security. Which document should Dylan have on his person to avoid being arrested?

- ➡ ☒ Permission to test
- ☐ Master service agreement
- ☐ Rules of engagement
- ☐ Scope of work

Explanation

The permission to test is used as a last resort if the penetration tester is caught in the scope of their work. This get-out-of-jail-free card explains what the tester is doing and that his work is authorized.

The scope of work is a very detailed document that defines exactly what is going to be included in the penetration test. This document is also referred to as the statement of work. It should answer the who, what, when, where, and why of test.

The rules of engagement will define if the test will be a white box, gray box, or black box test. It should also explicitly state how to handle sensitive data. If, during the test, something happens and the IT team needs to be notified, that process should also be laid out in this document.

The master service agreement is a contract where parties agree to most of the terms that will govern future actions. This makes future services and contracts much easier to handle and define.

References

TestOut Ethical Hacker Pro - 2.5 Legal and Ethical Compliance
[e_framework_legal_ethics_eh1.exam.xml Q_ENGAGE_CONTRACTS_FACTS_04_EH1]