Exam Report: 2.3.4 Practice Questions

Date: 4/4/29 3:57:31 pm
Time Spent: 1:23

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 40%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following documents details exactly what can be tested during a penetration test?

- Scope of Work
- Rules of Engagement
- Non-Disclosure Agreement
- Master Service Agreement

Explanation

The scope of work is a very detailed document that defines exactly what software, and hardware, test types, and facility features are going to be included in the penetration test. This document is also referred to as the statement of work.

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

The master service agreement is a contract where parties agree to most of the terms that will govern future actions.

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

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_CHOOSE_TARGET_01_EH1]

Question 2: Correct

After performing a risk assessment, an organization must decide what areas of operation can be included in a penetration test and what areas cannot be included. Which of the following describes the process?

- Avoidance
- Tolerance
- Mitigation
- Transference

Explanation

After a risk assessment is performed and vulnerable areas identified, the organization needs to decide their tolerance level for performing a penetration test. Areas of risk that can be tolerated need to be placed in the scope of work, whereas those critical areas may need to be place out of scope, or off-limits.

When a risk can be avoided, it should be. This is known as risk avoidance.

Transference is the process of moving the risk to another entity.

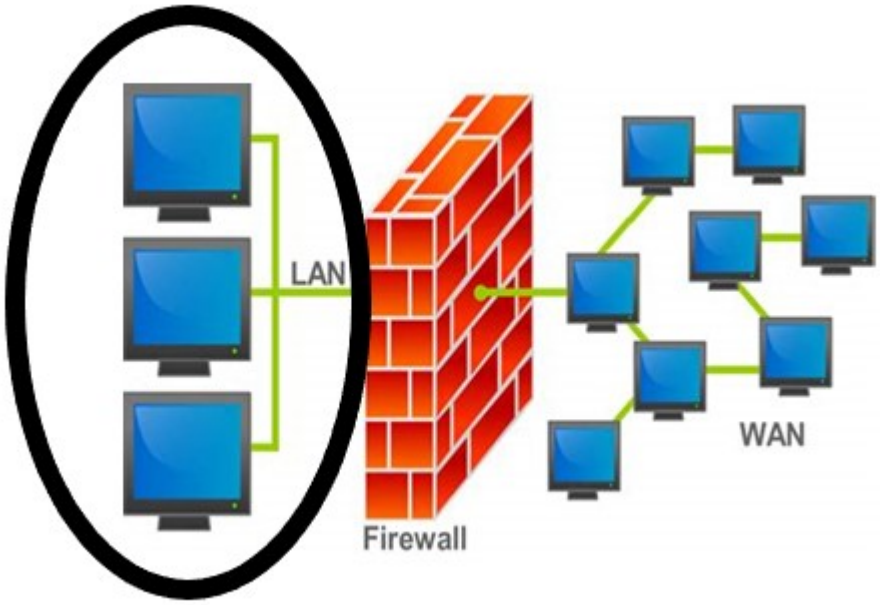
Risk mitigation is also called risk reduction. Sometimes the risks cannot be transferred or avoided. In this case, steps must be taken to reduce the damage that can occur.

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_DETERMINE_TOL_01_EH1]

Question 3: Incorrect

You are performing a penetration test of a local area network (LAN). Refer to the circled area on the network diagram. network. Which of the following types of penetration tests is being performed?



- External
- Internal
- ~~Black Box~~
- Gray Box

Explanation

An internal test will focus on any systems that logically resides behind the firewall. These can be off-site or on-site.

An external test will focus on any publicly facing system, such as a web server that resides in the DMZ.

A black box test means that the ethical hacker has no information about the target or network.

A gray box test means that the ethical hacker is given partial information about the network and computer systems.

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_PENTEST_PLAN_01_EH1]

Question 4: Correct

Miguel is performing a penetration test on a web server. Miguel was given only the server's IP address and name. Which of the following best describes the type of penetration test Miguel is performing?

- Black box

Internal

External

White box

Explanation

An external test focuses on any publicly facing system, such as a web server that resides in the DMZ.

An internal test focuses on any systems that logically resides behind the firewall. These can be offsite or onsite.

A black box test occurs when an ethical hacker has no information about the target or network.

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

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_PENTEST_PLAN_02_EH1]

Question 5: Correct

Which of the following elements is generally considered the weakest link in an organization's security?

Servers

Human

Physical

Network

Explanation

It is commonly accepted that the weakest link in any security model is the human element. If included in the scope of work, social engineering techniques can be used to test the people in an organization.

Physical security can be included in the penetration test if specified in the scope of work. This includes testing doors, locks, and cameras.

The network system is often included in penetration tests. This includes all data traffic and physical connections.

Servers may or may not be included in the penetration test. While the servers should be tested for vulnerabilities, a backup plan needs to be implemented in case the server goes down during the test.

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_PENTEST_PLAN_03_EH1]

Question 6: Incorrect

Which of the following best describes social engineering?

A stealthy computer network attack in which a person or group gains unauthorized access for an extended period.

Sending an email that appears to be from a bank to trick the target into entering their credentials on a malicious website.

~~The process of analyzing an organization's security and locating security holes.~~

The art of deceiving and manipulating others into doing what you want.

Explanation

Social engineering is the art of deceiving and manipulating others into doing what you want. Social engineering techniques can occur during in-person interactions. For example, a social engineer may dress

as pest control professional to gain access to a building.
The process of analyzing an organization's security and locating security holes is known as threat modeling.

An Advanced Persistent Threat (APT) is a stealthy computer network attack in which a person or group gains unauthorized access for an extended period.

Sending an email that appears to be from a bank to trick a target into entering their credentials on a malicious website is a phishing attack. Phishing attacks are a type of social engineering attack.

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_PENTEST_PLAN_04_EH1]

Question 7: Incorrect

Which of the following is considered a mission-critical application?

- Medical database
- Support log
- ~~Customer database~~
- Video player

Explanation

Some applications are considered mission-critical and need to be off-limits to avoid any down time. This can include financial processing, medical databases, or other sensitive applications.

None of the other application types would be considered mission-critical.

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_PENTEST_PLAN_05_EH1]

Question 8: Incorrect

What does an organization do to identify areas of vulnerability within their network and security systems?

- Internal test
- ~~Scanning~~
- Risk assessment
- External test

Explanation

The purpose of a risk assessment is to identify areas of vulnerability within the organization's network. The risk assessment should look at all areas, including high value data, network systems, web applications, online information, and physical security, including operating systems and web servers. This is done before beginning a penetration test.

An internal test focuses on any systems that logically reside behind the firewall. These can be offsite or onsite.

An external test focuses on any publicly facing system, such as a web server that resides in the DMZ.

Scanning is the second step in the hacking process. The ethical hacker uses various tools to gather in-depth information about the network, computer systems, live systems, and open ports.

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_RISK_ASSESS_01_EH1]

Question 9: Incorrect

During a risk assessment, the organization determines that the risk of collecting personal data from its customers is not acceptable and stops. What method of dealing with risk is the organization using?

- Mitigation
- ~~Transference~~
- Acceptance
- Avoidance

Explanation

When you identify a risk you can avoid, you should avoid it. This action is called risk avoidance.

Transference is the process of moving the risk to another entity.

Risk mitigation is also called risk reduction. Sometimes the risks cannot be transferred or avoided. In this case, steps must be taken to reduce the damage that can occur.

Risk acceptance occurs when the organization determines that the cost and effort to mitigate a risk outweighs the risk's potential damage, so they simply accept the risk.

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_RISK_ASSESS_02_EH1]

Question 10: Correct

The following formula defines which method of dealing with risk?

Cost of Risk > Damage = Risk _____

- Transference
- Mitigation
- Acceptance
- Avoidance

Explanation

Risk acceptance occurs when the organization determines that the cost and effort to mitigate a risk outweighs the risk's potential damage, so they simply accept the risk.

When you identify a risk you can avoid, you should. This is known as risk avoidance.

Transference is the process of moving a risk to another entity.

Risk mitigation is also called risk reduction. Sometimes risks cannot be transferred or avoided. In this case, steps must be taken to reduce the damage they can inflict.

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_RISK_ASSESS_03_EH1]

Question 11: Correct

Which of the following is a consideration when scheduling a penetration test?

- Which systems are being tested?
- Who is aware of the test?
- What risks are acceptable?
- Are there any security exceptions?

Explanation

The rules of engagement must specify who is aware of the penetration test and its time frame. The less people who know, the more realistic the test will be.

The scope of work will spell out which systems are included in the penetration test.

A security exception is any deviation from standard operating security protocols.

Risk acceptance occurs when the organization determines that the cost and effort to mitigate a risk outweighs the risk's potential damage, so they simply accept the risk.

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_SCOPE_CONSIDER_01_EH1]

Question 12: Incorrect

A client asking for small deviations from the scope of work is called:

- Rules of engagement
- Security exception
- ~~Change order~~
- Scope creep

Explanation

In project management, one of the most dangerous things to look out for is scope creep. This is when the client begins asking for small deviations from the scope of work. This can cause the project to go off track and increase the time and resources needed to complete it.

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

A security exception is any deviation from standard operating security protocols. It should be determined if you will be put on a whitelist or blacklist for the test on any IPS, Firewall, or other network access control systems.

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

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_SCOPE_CREEP_01_EH1]

Question 13: Incorrect

Heather is in the middle of performing a penetration test when her client asks her to also check the security of an additional server. Which of the following documents does she need to submit before performing the additional task?

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

Explanation

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

The rules of engagement document details how the test 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 referred to as the statement of work.

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 - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_SCOPE_CREEP_02_EH1]

Question 14: Incorrect

Which of the following is a deviation from standard operating security protocols?

- Security exception
- ~~MAC filtering~~
- Blacklisting
- Whitelisting

Explanation

A security exception is any deviation from standard operating security protocols. It should be determined if you will be put on a whitelist or blacklist for the test on any IPS, Firewall, or other network access control systems.

If a device is whitelisted, traffic coming from it will be allowed through the IPS, Firewall, or network access control system.

If a device is blacklisted, it will not be allowed to connect to the network.

MAC filtering is the process of allowing or blocking traffic from a certain device based on its MAC address.

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_SECURITY_EXCEPT_01_EH1]

Question 15: Incorrect

Miguel is performing a penetration test. His client needs to add Miguel's computer to the list of devices allowed to connect to the network. What type of security exception is this?

- ~~Blacklisting~~
- Black box
- White box
- Whitelisting

Explanation

If a device is whitelisted, then traffic coming from it will be allowed through the IPS, Firewall, or network access control system.

If a device is blacklisted, it will not be allowed to connect to the network.

In a white box test, the ethical hacker is given full knowledge of the target or network. This test allows for a comprehensive and thorough test, but this is not a very realistic situation.

In a black box test, the ethical hacker has no information regarding the target or network. This type of test best simulates and outside attack and ignores insider threats.

References

TestOut Ethical Hacker Pro - 2.3 Target Selection
[e_target_selection_eh1.exam.xml Q_TARGET_SELECTION_SECURITY_EXCEPT_02_EH1]