Exam Report: 2.1.3 Practice Questions

Date: 4/29/2020 9:15:11 am
Time Spent: 13:11

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 50%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

Penetration testing is the practice of finding vulnerabilities and risks with the purpose of securing a computer or network. Penetration testing falls under which all-encompassing term?

○ Network scanning

➡ ○ Ethical hacking

● ~~Red teaming~~

○ Blue teaming

Explanation

Ethical hacking is an all-encompassing term that includes all hacking methods, so penetration testing is a part of ethical hacking.

Red teaming is the act of performing offensive security functions for an organization.

Blue teaming is the act of performing defensive security functions for an organization.

Network scanning is the process of monitoring network activities.

References

TestOut Ethical Hacker Pro - 2.1 Penetration Testing Process and Types
[e_process_types_eh1.exam.xml Q_PROCESS_TYPES_ETHICAL_HACK_01_EH1]

Question 2: Correct

Heather is performing a penetration test. She has gathered a lot of valuable information about her target already. Heather has used some hacking tools to determine that, on her target network, a computer named Production Workstation has port 445 open. Which step in the ethical hacking methodology is Heather performing?

○ Maintain access

○ Gain access

➡ ● Scanning and enumeration

○ Reconnaissance

Explanation

Scanning is the second phase in the ethical hacking methodology. The hacker uses various tools to gather in-depth information about the network, computer systems, live systems, open ports, and more. Extracting information such as usernames, computer names, network resources, shares, and services is known as enumeration. Enumeration is a part of the Scanning step.

Reconnaissance is the first phase in the ethical hacking methodology. The hacker begins gathering information about their target. This can include gathering publicly available information, using social engineering techniques, or dumpster diving.

Gaining access is the third phase in the ethical hacking methodology. In this phase, the hacker uses all the information gathered through reconnaissance and scanning and then exploits vulnerabilities to gain access.

Maintaining access is the fourth phase in the ethical hacking methodology. Once the hacker has gained access, he can use backdoors, rootkits, or Trojans to establish permanent access to the system.

References

TestOut Ethical Hacker Pro - 2.1 Penetration Testing Process and Types
[e_process_types_eh1.exam.xml Q_PROCESS_TYPES_ETHICAL_HACK_METHOD_01_EH1]

▼ Question 3: Incorrect

Which of the following is the third step in the ethical hacking methodology?

○ Reconnaissance

● ~~Scanning and enumeration~~

➡ ○ Gain access

○ Clear your tracks

Explanation

Gaining access is the third phase in the ethical hacking methodology. In this phase, the hacker uses all the information gathered through reconnaissance and scanning and then exploits vulnerabilities to gain access.

Reconnaissance is the first phase in the ethical hacking methodology. The hacker begins gathering information about their target. This can include gathering publicly available information, using social engineering techniques, or even dumpster diving.

Scanning and enumeration is the second phase in the ethical hacking methodology. The hacker will use various tools to gather in-depth information about the network, computer systems, live systems, open ports, and more. Extracting information such as usernames, computer names, network resources, shares, and services is known as enumeration. Enumeration is a part of the scanning step.

Clearing tracks is the final step in the hacking process. The hacker performs tasks such as overwriting log files to hide the fact they were ever there.

References

TestOut Ethical Hacker Pro - 2.1 Penetration Testing Process and Types
[e_process_types_eh1.exam.xml Q_PROCESS_TYPES_ETHICAL_HACK_METHOD_02_EH1]

▼ Question 4: Correct

Miguel is performing a penetration test on his client's web-based application. Which penetration test frameworks should Miguel utilize?

○ NIST SP 800-115

○ ISO/IEC 27001

➡ ● OWASP

○ OSSTMM

Explanation

The Open Web Application Security Project (OWASP) describes techniques for testing the most common web application and web service security issues.

The Open Source Security Testing Methodology Manual (OSSTMM) attempts to enforce one accepted method for a very thorough security test.

The National Institute of Standards and Technology Special Publication 800-115 (NIST SP 800-115) is a guide to the basic technical aspects of conducting information security assessments.

ISO/IEC 2701 defines the processes and requirements for an organization's information security management systems.

References

TestOut Ethical Hacker Pro - 2.1 Penetration Testing Process and Types
[e_process_types_eh1.exam.xml Q_PROCESS_TYPES_PENTEST_FRAME_01_EH1]

▼ **Question 5:** Incorrect

The penetration testing life cycle is a common methodology used when performing a penetration test. This methodology is almost identical to the ethical hacking methodology. Which of the following is the key difference between these methodologies?

● ~~Reconnaissance~~

○ Maintain access

○ Gain access

➡ ○ Reporting

Explanation

The only difference between the penetration testing life cycle and ethical hacking methodology is the focus on the documentation of the penetration test. A detailed report of the tests performed and everything that was discovered is important to a penetration test.

Reconnaissance, gaining access, and maintaining access are all steps in both methodologies.

References

TestOut Ethical Hacker Pro - 2.1 Penetration Testing Process and Types
[e_process_types_eh1.exam.xml Q_PROCESS_TYPES_PENTEST_LIFE_CYCLE_01_EH1]

▼ **Question 6:** Correct

You are executing an attack in order to simulate an outside attack. Which type of penetration test are you performing?

➡ ● Black box

○ White hat

○ White box

○ Black hat

Explanation

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

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

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

A white hat hacker is a skilled hacker who uses skills and knowledge for defensive purposes only. The white hat hacker interacts only with systems for which express access permission has been given.

References

TestOut Ethical Hacker Pro - 2.1 Penetration Testing Process and Types
[e_process_types_eh1.exam.xml Q_PROCESS_TYPES_PENTEST_TYPES_01_EH1]

▼ **Question 7:** Incorrect

Which of the following best describes a gray box penetration test?

○ The ethical hacker has no information regarding the target or network.

○ The ethical hacker is given full knowledge of the target or network.

● ~~The ethical hacker is given strict guidelines about what can be targeted.~~

➡ ○ The ethical hacker has partial information about the target or network.

Explanation

In a gray box penetration test, the ethical hacker is given partial information about the target or network, such as IP configurations and email lists. This test simulates an insider threat.

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

In a white box penetration 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.

The Scope of Work defines what can be targeted during a penetration test.

References

TestOut Ethical Hacker Pro - 2.1 Penetration Testing Process and Types
[e_process_types_eh1.exam.xml Q_PROCESS_TYPES_PENTEST_TYPES_02_EH1]

▼ **Question 8:** Correct

Randy was just hired as a penetration tester for the red team. Which of the following best describes the red team?

○ Is a team of specialists that focus on the organization's defensive security.

○ Is responsible for establishing and implementing policies.

➡ ● Performs offensive security tasks to test the network's security.

○ Acts as a pipeline between teams and can work on any side.

Explanation

The red team is made up of offensive security specialists that constantly work against the blue team to test the organization's security stance.

A blue team focuses on the organization's defensive security. They are responsible for establishing and implementing policies and closing vulnerabilities.

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.

References

TestOut Ethical Hacker Pro - 2.1 Penetration Testing Process and Types
[e_process_types_eh1.exam.xml Q_PROCESS_TYPES_RED_BLUE_01_EH1]