Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/11/2022 5:41:56 pm • Time spent: 02:40

Score: 90% Passing Score: 80%

Question 1: ✔ Correct

Which step in the penetration testing life cycle is accomplished using rootkits or Trojan horse programs?

- Enumeration
- Gain access
- Reconnaissance
- ➡ Maintain access

EXPLANATION

Once a penetration tester has gained access, maintaining that access becomes the next priority. This can be done by installing backdoors, rootkits, or Trojans.

Gain access is the third phase of the penetration test life cycle and uses the information gathered in earlier phases to exploit discovered vulnerabilities.

Reconnaissance is the first phase in the penetration testing process. This is when the penetration tester begins gathering information.

Enumeration is the second phase in the penetration testing process. The penetration tester uses scanning techniques to extract information such as usernames and computer names.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_access_secp7.question.fex

Question 2: ✔ Correct

You have been hired as part of the team that manages an organization's network defense.

Which security team are you working on?

- Red
- White
- Blue
- Purple

EXPLANATION

Blue team members are the defense of the system. This team is responsible for stopping the red team's advances.

Members of the purple team work on both offense and defense. This team is a combination of the red and blue teams.

The red team members are the ethical hackers. This team is responsible for performing the penetration tests.

The white team members are the referees of cybersecurity. This team is responsible for managing the engagement between the red and blue teams. This group typically consists of the managers or team leads.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_blue_secp7.question.fex

Question 3: ✔ Correct

As part of a special program, you have discovered a vulnerability in an organization's website and reported it to the organization. Because of the severity, you are paid a good amount of money.

Which type of penetration test are you performing?

- Gray box
- White box
- Black box
- Bug bounty

EXPLANATION

Bug bounties are unique tests that are set up by organizations such as Google and Facebook. The organization sets strict guidelines and boundaries for ethical hackers to operate within. Discovered vulnerabilities are reported, and the ethical hacker is paid based on the severity of the vulnerability.

In a white box test, the ethical hacker is given full knowledge of the target or network. This test is comprehensive and thorough, but it isn't very realistic.

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 gray box 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.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_bug_bounty_secp7.question.fex

Question 4: ✔ Correct

Which phase or step of a security assessment is a passive activity?

- ➡ Reconnaissance
- Vulnerability mapping
- Enumeration
- Privilege escalation

EXPLANATION

Reconnaissance is the only step of a security assessment (penetration test) that is passive.

Enumeration, vulnerability mapping, and privilege escalation are all active events in a security assessment.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_recon_secp7.question.fex

Question 5: ✔ Correct

Which of the following activities are typically associated with a penetration test?

- ➡ ◉ Attempt social engineering.
- ○ Run a vulnerability scanner on network servers.
- ○ Create a performance baseline.
- ○ Interview employees to verify that the security policy is being followed.

EXPLANATION

Penetration testing typically uses tools and methods that are available to attackers. Penetration testing might start with attempts at social engineering or other reconnaissance activities. This may be followed by more active scans of systems and actual attempts to access secure systems.

A vulnerability scanner checks a system for weaknesses. Vulnerability scanners typically require administrative access to a system and are performed internally. They are not done to test system security. Typically, penetration testers cannot run a vulnerability scanner unless they have gained authorized access to a system.

A performance baseline is created by an administrator to identify normal network and system performance. Auditing might include interviewing employees to make sure that security policies are being followed.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_social_secp7.question.fex

Question 6: ✕ Incorrect

Which of the following is a very detailed document that defines exactly what is going to be included in the penetration test?

- Goals and guidelines
- ~~Rules of engagement~~
- Payment terms
- Scope of work

EXPLANATION

A 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 rules of engagement document defines exactly how a penetration test is to be carried out.

Goals and guidelines is not a document type. The scope of work and rules of engagement documents detail the goals and guidelines of a penetration test.

Payment terms are not a document type. Payment terms are defined in the scope of work document.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_sow_secp7.question.fex

Question 7: ✔ Correct

Which of the following uses hacking techniques to proactively discover internal vulnerabilities?

- ➡ Penetration testing
- Inbound scanning
- Passive reconnaissance
- Reverse engineering

EXPLANATION

Penetration testing is the practice of proactively testing systems and policies for vulnerabilities. This approach seeks to identify vulnerabilities internally before a malicious individual can take advantage of them. Common techniques are identical to those used by hackers and include network/target enumeration and port scanning.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_testing_01_secp7.question.fex

Question 8: ✔ Correct

What is the primary purpose of penetration testing?

- ➡ Test the effectiveness of your security perimeter.
- Evaluate newly deployed firewalls.
- Infiltrate a competitor's network.
- Assess the skill level of new IT security staff.

EXPLANATION

The primary purpose of penetration testing is to test the effectiveness of your security perimeter. Only by attempting to break into your own secured network can you be assured that your security policy, security mechanism implementations, and deployed countermeasures are effective. It is important to obtain senior management's approval before starting a penetration test or vulnerability scanning project. Often, penetration testing or vulnerability scanning is performed by an external consultant or security-outsourcing agency that is hired by your organization.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_testing_02_secp7.question.fex

Question 9: ✔ Correct

You have been hired to perform a penetration test for an organization. You are given full knowledge of the network before the test begins.

Which type of penetration test are you performing?

- White box
- Bug bounty
- Black box
- Gray box

EXPLANATION

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 it is not very realistic.

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

Bug bounties are unique tests that are set up by organizations such as Google and Facebook. The organization sets strict guidelines and boundaries for ethical hackers to operate within. Any discovered vulnerabilities are reported, and the ethical hacker is paid based on the severity of the vulnerability.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_white_box_secp7.question.fex

Question 10: ✔ Correct

You have been promoted to team lead of one of the security operations teams.

Which security team are you now a part of?

- White
- Purple
- Red
- Blue

EXPLANATION

The white team members are the referees of cybersecurity. This team is responsible for managing the engagement between the red and blue teams. This group typically consists of the managers or team leads.

Blue team members are the defense of the system. This team is responsible for stopping the red team's advances.

Members of the purple team work on both offense and defense. This team is a combination of the red and blue teams.

The red team members are the ethical hackers. This team is responsible for performing the penetration tests.

REFERENCES

11.1.2 Penetration Testing Facts

q_pene_test_white_secp7.question.fex