Exam Report: 6.13.4 Practice Questions

Date: 1/22/2020 12:13:13 pm
Time Spent: 13:40

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 58%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following identifies an operating system or network service based on its response to ICMP messages?

- Firewalking
- Fingerprinting
- Port scanning
- Social engineering

Explanation

Fingerprinting identifies an operating system or network service based on its response to ICMP messages. Portions of the original ICMP request are repeated (or quoted) within the response. Each operating system quotes this information back in a slightly different manner.

Port scanning pings every port on an external interface or attempts a connection in order to discover which ports are open and active, and which are not. *Firewalking* uses traceroute to discover which services can pass through a firewall or a router. *Social engineering* exploits human nature to obtain information, often by impersonating someone of authority and requesting data.

References

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_01]

Question 2: Correct

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

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

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

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_02]

Question 3: Incorrect

You have decided to perform a double-blind penetration test. Which of the following actions would you perform *first*?

- Engage in social engineering
- Perform operational reconnaissance
- Inform senior management
- ~~Run system fingerprinting software~~

Explanation

Before starting a penetration test (also called a *pen test*), it is important to define the Rules of Engagement (ROE), or the boundaries of the test. Important actions to take include:

- Obtain a written and signed authorization from the highest possible senior management
- Delegate personnel who are experts in the areas being tested
- Gain approval from the internet provider to perform the penetration test
- Make sure that all tools or programs used in the test are legal and ethical
- Establish the scope and timeline
- Identify systems that will not be included in the test

Reconnaissance, social engineering, and system scanning are all actions performed during a penetration test. However, no actions should be taken before approval to conduct the test is obtained.

References

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_03]

Question 4: Incorrect

Which of the following activities are typically associated with a penetration test? (Select two.)

- [ ] Interviewing employees to verify that the security policy is being followed
- [ ] Running a port scanner
- [ ] Creating a performance baseline
- [x] Attempting social engineering
- [x] ~~Running a vulnerability scanner on network servers~~

Explanation

Penetration testing is an organization's attempt to circumvent security controls to identify vulnerabilities in their information systems. It simulates an actual attack on the network and is conducted from outside the organization's security perimeter. Penetration testing helps assure the effectiveness of an organization's security policy, security mechanism implementations, and deployed countermeasures.

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 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 to check for weaknesses, but not 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

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_04]

Question 5: Incorrect

What is the main difference between vulnerability scanning and penetration testing?

- Vulnerability scanning is performed with a detailed knowledge of the system; penetration testing begins with no knowledge of the system.
- Vulnerability scanning is performed within the security perimeter; penetration testing is performed outside of the security perimeter.
- ~~The goal of vulnerability scanning is to identify potential weaknesses; the goal of penetration testing is to attack a system.~~
- Vulnerability scanning uses approved methods and tools; penetration testing uses hacking tools.

Explanation

Penetration testing simulates an actual attack on the network and is conducted from outside the organization's security perimeter. Vulnerability scanning is typically performed internally by users with administrative access to the system.

The goal of both vulnerability scanning and penetration testing is to identify the effectiveness of security measures and weaknesses that can be fixed. While some penetration testing is performed with no knowledge of the network, penetration testing could be performed by testers with detailed information about the systems. Both vulnerability scanning and penetration testing can use similar tools, although illegal tools should be avoided in both activities.

References

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_05]

Question 6: Correct

What is the primary purpose of penetration testing?

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

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 approval before starting a penetration testing 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

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_06]

Question 7: Correct

Which of the following types of penetration test teams will provide you information that is most revealing of a real-world hacker attack?

- Partial-knowledge team
- Split-knowledge team
- Full-knowledge team

Zero-knowledge team

Explanation

A zero-knowledge team is a penetration testing team which most closely simulates a real-world hacker attack as they must perform all of the initial blind reconnaissance.

A full-knowledge team is least like a real-world hacker, as they already know everything about the environment. A partial-knowledge team is closer to a real-world hacker than a full-knowledge team, but not as close as a zero-knowledge team. A a split-knowledge team is not a generally-accepted standard penetration team. Split knowledge refers to a separation of duties concept.

References

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_07]

Question 8: Incorrect

A security administrator is conducting a penetration test on a network. She connects a notebook system running Linux to the wireless network and then uses NMAP to probe various network hosts to see which operating system they are running.

Which process did the administrator use in the penetration test in this scenario?

- Network enumeration
- Active fingerprinting
- Firewalking
- ~~Passive fingerprinting~~

Explanation

Active fingerprinting was used by the administrator in this scenario. Active fingerprinting is a form of system enumeration that is designed to gain as much information about a specific computer as possible. It identifies operating systems based upon ICMP message quoting characteristics. Portions of an original ICMP request are repeated (or quoted) within the response, and each operating system quotes this information back in a slightly different manner. Active fingerprinting can determine the operating system and even the patch level.

Passive fingerprinting is similar to active fingerprinting. However, it does not utilize the active probes of specific systems. Network enumeration (also called network mapping) involves a thorough and systematic discovery of as much of the corporate network as possible, using:

- Social engineering
- Wardriving
- War dialing
- Banner grabbing
- Firewalking

Firewalking uses traceroute techniques to discover which services can pass through a firewall or a router. Common firewalking tools are Hping and Firewalk.

References

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_08]

Question 9: Correct

A security administrator is conducting a penetration test on a network. She connects a notebook system to a mirror port on a network switch. She then uses a packet sniffer to monitor network traffic to try to determine which operating systems are running on network hosts.

Which process did the administrator use in the penetration test in this scenario?

- Network enumeration
- Active fingerprinting

Firewalking

Passive fingerprinting

Explanation

In this scenario, the administrator uses passive fingerprinting. Passive fingerprinting is a form of system enumeration that is designed to gain as much information about network computers as possible. It passively listens to network traffic generated by network hosts and attempts to identify which operating systems are in use based upon the ICMP message quoting characteristics they use. Portions of original ICMP requests are repeated (or quoted) within each response. Each operating system quotes this information back in a slightly different manner.

Active fingerprinting works in much the same manner as passive fingerprinting. However, it utilizes active probes of specific systems instead of passive monitoring.

Network enumeration (also called network mapping) involves a thorough and systematic discovery of as much of the corporate network as possible, using:

- Social engineering
- Wardriving
- War dialing
- Banner grabbing
- Firewalking

Firewalking uses traceroute techniques to discover which services can pass through a firewall or a router. Common firewalking tools are **Hping** and **Firewalk**.

References

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_09]

Question 10: Incorrect

Which of the following are included in an *operations penetration* test? (Select two.)

~~Scanning various ports on remote hosts looking for well-known services.~~

Duplicating captured packets without altering or interfering with the flow of traffic on that medium.

Looking through discarded papers or media for sensitive information.

Sneaking into a building without authorization.

Eavesdropping or obtaining sensitive information from items that are not properly stored.

Explanation

In an *operations penetration* test, the tester attempts to gain as much information as possible using the following methods:

- In *Dumpster diving*, the attacker looks through discarded papers or media for sensitive information.
- With *over-the-shoulder reconnaissance*, attackers eavesdrop or obtain sensitive information from items that are not properly stored.
- Using *social engineering*, attackers act as imposters with the intent to gain access or information.

Scanning various ports on remote hosts looking for well-known services (known as *port scanning*) and duplicating captured packets without altering or interfering with the flow of traffic on that medium (known as *sniffing*) are both types of *electronic penetration* tests. Sneaking into a building without authorization is a *physical penetration* test.

References

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_10]

Question 11: Correct

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

- Vulnerability mapping
- Enumeration
- Reconnaissance
- Privilege escalation

Explanation

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

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

References

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_11]

Question 12: Correct

Drag each penetration test characteristic on the left to the appropriate penetration test name on the right.

White box test
- The tester has detailed information about the target system prior to starting the test.

Grey box test
- The tester has the same amount of information that would be available to a typical insider in the organization.

Black box test
- The tester has no prior knowledge of the target system.

Single blind test
- Either the attacker has prior knowledge about the target system, or the administrator knows that the test is being performed.

Double blind test
- The tester does not have prior information about the system and the administrator has no knowledge that the test is being performed.

Explanation

Penetration testing is classified by the knowledge that the attacker and system personnel have prior to the attack.

- In a black box test, the tester has no prior knowledge of the target system.
- In a white box test, the tester has detailed information prior to starting the test.
- In a grey box test, the tester has the same amount of information that would be available to a typical insider in the organization.
- A single blind test is one in which one side has advanced knowledge. For example, either the attacker has prior knowledge about the target system, or the defender has knowledge about the impending attack.
- A double blind test is one in which the penetration tester does not have prior information about the system and the network administrator has no knowledge that the test is being performed. The double blind test provides more accurate information about the security of the system.

References

LabSim for Security Pro, Section 6.13.
[All Questions SecPro2017_v6.exm PENE_TEST_12]