

Exam Report: 6.9.10 Practice Questions

Date: 1/22/2020 8:23:03 am
Time Spent: 18:32

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 79%



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

Which of the following functions can a port scanner provide? (Select two.)

- ☐ Testing virus definition design for false positives
- ➔ ☒ Discovering unadvertised servers
- ☐ Auditing IPsec encryption algorithm configuration
- ➔ ☒ Determining which ports are open on a firewall

Explanation

Port scanners can determine which TCP/UDP ports are open on a firewall and identify servers that may be unauthorized or running in a test environment. Many port scanners provide additional information, including the host operating system and version, of any detected servers. Hackers use port scanners to gather valuable information about a target, and system administrators should use the same tools for proactive penetration testing and ensuring compliance with all corporate security policies.

References

LabSim for Security Pro, Section 6.9.
[All Questions SecPro2017_v6.exm VULN_ASSESS_01]

▼ Question 2: Correct

Which of the following is the type of port scan that does not complete the full three-way TCP handshake, but rather listens only for either SYN/ACK or RST/ACK packets?

- ☐ TCP ACK scan
- ☐ TCP connect scan
- ➔ ☒ TCP SYN scan
- ☐ TCP FIN scan

Explanation

A TCP SYN scan is the type of port scan that does not complete the full three-way TCP handshake, but rather listens only for either SYN/ACK packets (which indicate that a port is listening) or RST/ACK packets (which indicate that a port is not listening).

A TCP connect scan uses a full TCP three-way handshake and establishes a session with each port. A TCP FIN scan sends FIN packets to ports and listens for RST responses for closed ports, which indicate which ports are open. A TCP ACK scan is used to map out a firewall's filtering rules.


References

LabSim for Security Pro, Section 6.9.
[All Questions SecPro2017_v6.exm VULN_ASSESS_02]

▼ Question 3: Correct

You want to make sure that a set of servers will only accept traffic for specific network services. You have verified that the servers are only running the necessary services, but you also want to make sure that the servers will not accept packets sent to those services.

Which tool should you use?

- ☐ IPS
- ☐ System logs
- ☐ IDS
-  ☒ Port scanner
- ☐ Packet sniffer

Explanation

Use a port scanner to check for open ports on a system or a firewall. Compare the list of opened ports with the list of ports allowed by your network design and security policy. Typically, a port is opened when a service starts or is configured on a device. Open ports for unused services expose the server to attacks directed at that port.

Use a packet sniffer to examine packets on the network. With a packet sniffer, you can identify packets directed towards specific ports, but you won't be able to tell if those ports are open. Examine system logs to look for events that have happened on a system, which might include a service starting, but would not likely reflect open ports.

An intrusion detection system (IDS) is a special network device that can detect attacks and suspicious activity. A *passive* IDS monitors, logs, and detects security breaches, but takes no action to stop or prevent the attack. An *active* IDS (also called an *intrusion protection system* or IPS) performs the functions of an IDS, but can also react when security breaches occur.


References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_03]

▼ Question 4: Incorrect

You want to be able to identify the services running on a set of servers on your network. Which tool would best give you the information you need?

-  ☐ Vulnerability scanner
- ☒ Protocol analyzer
- ☐ Port scanner
- ☐ Network mapper

Explanation

Use a vulnerability scanner to gather information about systems, such as the applications or services running on the system. The vulnerability scanner often combines functions found in other tools and can perform additional functions, such as identifying open firewall ports, missing patches, and default or blank passwords.

A *port scanner* is a tool that probes systems for open ports. The port scanner will tell you which ports are opened in the firewall, but it cannot identify services running on a server if the firewall port has been closed. A *network mapper* is a tool that can discover devices on the network and shows those devices in a graphical representation. Network mappers typically use a ping scan to discover devices and a port scanner to identify open ports on those devices.

Use a protocol analyzer to identify traffic that is sent on the network medium and traffic sources. Services could still be running on a server that do not generate network traffic a protocol analyzer can catch.

References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_04]

▼ Question 5: Correct

You want to identify all devices on a network along with a list of open ports on those devices. You want the results displayed in a graphical diagram. Which tool should you use?

- ☐ Port scanner
- ☐ OVAL
- ➡ ☒ Network mapper
- ☐ Ping scanner

Explanation

A network mapper is a tool that can discover devices on the network and show those devices in a graphical representation. Network mappers typically use a ping scan to discover devices and a port scanner to identify open ports on those devices.

A ping scanner only identifies devices on the network, but does not probe for open ports. A port scanner finds open ports, but might not display devices in a graphical representation. The Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system.

References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_05]

▼ Question 6: Correct

You want to use a tool to scan a system for vulnerabilities, including open ports, running services, and missing patches. Which tools should you use? (Select two.)

- ☐ LC4
- ☐ OVAL
- ☐ Wireshark
- ➡ ☒ Retina
- ➡ ☒ Nessus

Explanation

A *vulnerability scanner* is a software program that searches an application, computer, or network for weaknesses, such as open ports, running applications or services, missing critical patches, default user accounts that have not been disabled, and default or blank passwords. Vulnerability scanning tools include Nessus, Retina Vulnerability Assessment Scanner, and Microsoft Baseline Security Analyzer (MBSA).

Wireshark is a protocol analyzer. LC4 is a password cracking tool that you can use to identify weak passwords. The Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system.

References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_06]

▼ Question 7: Correct

You want to check a server for user accounts that have weak passwords. Which tool should you use?

- ☐ OVAL

☐ Nessus

➔ ☒ John the Ripper

☐ Retina

Explanation

John the Ripper is a password cracking tool. Password crackers perform cryptographic attacks on passwords. Use a password cracker to identify weak passwords or passwords protected with weak encryption.

Nessus and Retina are vulnerability scanners. While vulnerability scanners check for default user accounts and often check for accounts with blank passwords, they typically do not include password cracking features to test for weak passwords. The Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system.

References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_07]

▼ Question 8: Incorrect

Which of the following are performed by the Microsoft Baseline Security Analyzer (MBSA) tool? (Select three.)

- ➔ ☒ Check for missing patches
- ☐ Gather performance statistics for setting a baseline
- ➔ ☒ Check for open ports
- ➔ ☐ Check user accounts for weak passwords
- ☐ Analyze packets for evidence of an attack

Explanation

Microsoft Baseline Security Analyzer (MBSA) is a vulnerability scanner that can check for the following weaknesses:

- Open ports
- Active IP
- ~~Running~~ Running applications or services
- Missing critical patches
- Default user accounts that have not been disabled
- Default, blank, or common passwords

Vulnerability scanners typically do not include password cracking tools, but MBSA can perform simple checks for weak passwords.

Use a protocol analyzer to check packets for characteristics that might indicate an attack. Use a performance monitoring tool to gather information about system or network performance to identify a performance baseline.

References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_08]

▼ Question 9: Correct

Which of the following identifies standards and XML formats for reporting and analyzing system vulnerabilities?

☐ Retina

☐

- ☐ OSSTMM
- ☐ MBSA

➡ ☒ OVAL

Explanation

The Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system.

- OVAL is sponsored by the National Cyber Security division of the US Department of Homeland Security.
- OVAL identifies the XML format for identifying and reporting system vulnerabilities.
- Each vulnerability, configuration issue, program, or patch that might be present on a system is identified as a *definition*.
- OVAL *repositories* are like libraries or databases that contain multiple definitions.

Microsoft Baseline Security Analyzer (MBSA) and Retina Vulnerability Assessment Scanner are vulnerability scanning tools. The Open Source Security Testing Methodology Manual (OSSTMM) is a manual of a peer-reviewed methodology for performing security tests and metrics.

References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_09]

▼ Question 10: Correct

You are using a vulnerability scanner that conforms to the OVAL specifications. Which of the following items contains a specific vulnerability or security issue that could be present on a system?

- ☐ Asset risk
- ☐ Threat agent
- ➡ ☒ Definition
- ☐ Library
- ☐ Repository

Explanation

The Open Vulnerability and Assessment Language (OVAL) is an international standard for testing, analyzing, and reporting the security vulnerabilities of a system. Each vulnerability, configuration issue, program, or patch that might be present on a system is identified as a *definition*.

OVAL *repositories* are like libraries or databases that contain multiple definitions.

References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_10]

▼ Question 11: Correct

You have run a vulnerability scanning tool and identified several patches that need to be applied to a system. What should you do next after applying the patches?

- ☐ Update the vulnerability scanner definition files
- ☐ Use a port scanner to check for open ports
- ➡ ☒ Run the vulnerability assessment again
- ☐ Document your actions

Explanation

After fixing an identified vulnerability, you should re-run the vulnerability scan to verify that everything

has been fixed and that additional issues are not present.

You should update definition files before you run the first scan. Using a port scanner is unnecessary because most vulnerability scanners include a check of open ports. Documenting your actions should occur after you have finished all necessary actions.

References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_11]

▼ Question 12: Correct

You want to use a vulnerability scanner to check a system for known security risks. What should you do first?

- ☐ Apply all known patches to the system
- ➡ ☒ Update the scanner definition files
- ☐ Perform a port scan
- ☐ Inform senior management of your actions

Explanation

Before using a vulnerability scanner, you should update the definition files. The definition files identify known security risks associated with the system. Some scanners update the definition files automatically, while others require you to download the latest definition files.

Applying all known patches is not a best practice. You typically only apply the patches that are required or identified as important security patches. The vulnerability scanner typically identifies the patches you should apply. A port scan checks for open ports and is, typically, a test performed as part of the vulnerability scan. Senior management does not need to be notified when you run a vulnerability scan; they do need to be informed of penetration tests before they are executed.

References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_12]

▼ Question 13: Incorrect

A security administrator logs on to a Windows server on her organization's network. She then runs a vulnerability scan on that server.

What type of scan was conducted in this scenario?

- ☒ ~~TCP SYN scan~~
- ☐ Non-credentialed scan
- ➡ ☐ Credentialed scan
- ☐ Ping scan

Explanation

In a *credentialed scan*, the security administrator authenticates to the system prior to starting the scan. A credentialed scan usually provides detailed information about potential vulnerabilities. For example, a credentialed scan of a Windows workstation allows you to probe the registry for security vulnerabilities.

In a *non-credentialed scan*, the security administrator does not authenticate to the system prior to running the scan. A *TCP SYN scan* is a common type of port scan. A *ping scan* sends ICMP echo/request packets to one or multiple IP addresses.

References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_13]

▼ Question 14: Correct

A security administrator needs to run a vulnerability scan that will analyze a system from the perspective of a hacker attacking the organization from the outside.

What type of scan should he use?

- ☐ Port scan
- ☐ Network mapping scan
- ☐ Credentialed scan

➡ ☒ Non-credentialed scan

Explanation

In a *non-credentialed scan*, the security administrator does not authenticate to the system prior to running the scan. A non-credentialed scan can be valuable because it allows the scanner to see the system from the same perspective that an attacker would see it. However, a non-credentialed scan does not typically produce the same level of detail as a credentialed scan.

In a *credentialed scan*, the security administrator authenticates to the system prior to starting the scan. A *port scan* probes systems for open ports, but does not run a full vulnerability assessment. A *network mapping scan* is a type of port scan that discovers devices on the network and then organizes those devices in a graphical display.

References

LabSim for Security Pro, Section 6.9.

[All Questions SecPro2017_v6.exm VULN_ASSESS_14]