

Exam Report: 7.4.10 Practice Questions

Date: 4/4/5 5:51:41 pm
Time Spent: 1:06

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 14%

View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1:

Incorrect

The results section of an assessment report contains four sub-topics. Which of the following sub-sections contains the origin of the scan?

- ☒ Classification
- ☐ Target
- ☒ Assessment
- ☐ Services

Explanation

Classification contains the origin of the scan.

Target includes each host's detailed information.

Services defines the network services by their names and ports.

Assessment provides the scanner's assessment of the vulnerability.

References

TestOut Ethical Hacker Pro - 7.4 Vulnerability Assessment

Tools\assessment_tools_eh1.exam.xml Q_VULN_ASSESSMENT_TOOLS_ASSESS_REPORT_01_EH1]

▼ Question 2:

Incorrect

Karen received a report of all the mobile devices on the network. This report showed the total risk score, summary of revealed vulnerabilities, and remediation suggestions. Which of the following types of software generated this report?

- ☐ A port scanner
- ☒ A malware scanner
- ☐ An antivirus scanner
- ☒ A vulnerability scanner

Explanation

A vulnerability scanner detects and classifies system weaknesses in computers, networks, and communications equipment, as well as predicts the effectiveness of countermeasures.

A port scanner is an application designed to probe a server or host for open ports.

An antivirus scanner is a component of an antivirus software package that scans a hard drive for viruses and other harmful items.

A malware scanner scans the computer to prevent malware infection.

References

TestOut Ethical Hacker Pro - 7.4 Vulnerability Assessment

Tools\assessment_tools_eh1.exam.xml Q_VULN_ASSESSMENT_TOOLS_ASSESS_REPORT_02_EH1]

▼ Question 3: Incorrect

Which of the following includes a list of resolved vulnerabilities?

- ➡ ☐ Security vulnerability summary
- ☐ Statistical vulnerability report
- ☐ Security vulnerability report
- ☒ ~~Statistical vulnerability summary~~

Explanation

A security vulnerability summary includes a list of resolved vulnerabilities and also covers every device or server that was scanned. It gives you information about current security flaws and vulnerabilities, including severity level, and lists resolved vulnerabilities.

A security vulnerability report gives you information on all the scanned devices and servers, including open and detected ports, as well as new vulnerabilities. It also gives suggestions for remediation with links to patches.

References

TestOut Ethical Hacker Pro - 7.4 Vulnerability Assessment

Tools\assessment_tools_eh1.exam.xml Q_VULN_ASSESSMENT_TOOLS_ASSESS_REPORT_03_EH1]

▼ Question 4: Incorrect

Which of the following best describes Qualys Vulnerability Management assessment tool?

- ☒ ~~It has more than 50,000 vulnerability tests with daily updates.~~
- ➡ ☐ It is a cloud-based service that keeps all your data in a private virtual database.
- ☐ It scans for known vulnerabilities, malware, and misconfigurations.
- ☐ It scans for more than 6,000 files and programs that can be exploited.

Explanation

Qualys Vulnerability Management is a cloud-based service that keeps all your data in a virtual private database. Qualys is easy to use and is capable of scanning large enterprises. Data is always encrypted during transit and at rest, so even though it is cloud-based, your data is secure. Only their scanners reside in your network.

Nessus Professional is an assessment solution that resides on your network. This makes it more suitable for smaller organizations. It scans for known vulnerabilities, malware, and misconfigurations.

OpenVAS is a vulnerability scanner that has more than 50,000 vulnerability tests with daily updates.

Nikto is a web server scanner. It tests for outdated versions of more than 1250 servers. It also scans for more than 6,000 files and programs that can be exploited.

References

TestOut Ethical Hacker Pro - 7.4 Vulnerability Assessment

Tools\assessment_tools_eh1.exam.xml Q_VULN_ASSESSMENT_TOOLS_ASSESS_TOOL_01_EH1]

▼ Question 5: Incorrect

Clive, a penetration tester, is scanning for vulnerabilities on the network, specifically outdated versions of Apple iOS. Which of the following tools should he use?

- ➡ ☐ Nessus

- ☐ Nikto
- ☒ ~~NetScan~~
- ☐ Retina CS

Explanation

Nessus offers scanning on mobile devices and will let you know which devices are unauthorized or non-compliant. It also identifies outdated versions of Apple iOS and highlights devices that have not connected for a period of time.

Retina CS for Mobile provides comprehensive vulnerability management for smartphones, mobile devices, and tablets.

NetScan is a tool that provides discovery through network and port scanning.

Nikto is a web server scanner. It tests for outdated versions of more than 1,250 servers.

References

TestOut Ethical Hacker Pro - 7.4 Vulnerability Assessment

[Tools_in_assessment_tools_eh1.exam.xml Q_VULN_ASSESSMENT_TOOLS_MOBILE_TOOL_01_EH1](#)

▼ Question 6: Correct

You are looking for a vulnerability assessment tool that detects vulnerabilities in mobile devices and gives you a report containing a total risk score, a summary of revealed vulnerabilities, and remediation suggestions. Which of the following vulnerability assessment tools should you use?

- ☐ Network Scanner
- ➡ ☒ SecurityMetrics Mobile
- ☐ Nessus Professional
- ☐ Retina CS for Mobile

Explanation

SecurityMetrics Mobile detects vulnerabilities in mobile devices. It can help you protect customers' data and avoid unwanted app privileges, mobile malware, device theft, connectivity issues, threats to device storage, and unauthorized account access. You can expect a report containing a total risk score, a summary of revealed vulnerabilities, and remediation suggestions.

Nessus Professional is an assessment solution that resides on your network. This makes it more suitable for smaller organizations. It scans for known vulnerabilities, malware, and misconfigurations. Nessus also provides reporting and remediation, as well as ongoing monitoring.

Retina CS for Mobile provides comprehensive vulnerability management for smartphones, mobile devices, and tablets. It can scan, prioritize, and fix smartphone vulnerabilities. It analyzes and reports its findings from a centralized data warehouse.

Network Scanner is a tool that provides an understanding of the use of a network. It generates reports of security issues and vulnerabilities that auto-saves and can be backed up to your web storage.

References

TestOut Ethical Hacker Pro - 7.4 Vulnerability Assessment

[Tools_in_assessment_tools_eh1.exam.xml Q_VULN_ASSESSMENT_TOOLS_MOBILE_TOOL_02_EH1](#)

▼ Question 7: Incorrect

Which of the following would be the best open-source tool to use if you are looking for a web server scanner?

- ☒ ~~NetScan~~
- ➡ ☐ Nikto

☐ Nessus☐ OpenVAS

Explanation

Nikto is a web server scanner. It tests for outdated versions of more than 1,250 servers, scans for more than 6,000 files and programs that can be exploited, and checks for version-specific problems on more than 270 servers. It is important to note that this tool creates a large footprint by leaving a high volume of entries in the web server's log files.

OpenVAS is a vulnerability scanner that has more than 50,000 vulnerability tests with daily updates.

Nessus offers scanning on mobile devices and will let you know which devices are unauthorized or non-compliant. It also identifies outdated versions of Apple iOS and highlights devices that haven't connected for a period of time.

NetScan is a tool that provides discovery through network and port scanning. It can find vulnerabilities, security flaws, and open ports in your network.

References

TestOut Ethical Hacker Pro - 7.4 Vulnerability Assessment

[Tools\assessment_tools_eh1.exam.xml Q_VULN_ASSESSMENT_TOOLS_OPEN_TOOL_01_EH1\]](#)