CCNA Security v2.0 Chapter 11 Exam Answers

itexamanswers.net/ccna-security-v2-0-chapter-11-exam-answers.html

February 9, 2016

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. Which security test is appropriate for detecting system weaknesses such as misconfiguration, default passwords, and potential DoS targets?

- **vulnerability scanning***
- network scanning
- integrity checkers
- penetration testing

Explanation: There are many tests used to assess the operational status of networks and systems. Weaknesses in systems such as blank or default passwords, or misconfigurations that would make a system a target of a DoS attack can be detected through vulnerability scanning.

2. How does network scanning help assess operations security?

- It can simulate attacks from malicious sources.
- It can log abnormal activity.
- **It can detect open TCP ports on network systems.***
- It can detect weak or blank passwords.

3. What is the objective of the governing policy in the security policy hierarchy structure?

- It covers all rules pertaining to information security that end users should know about and follow.
- **It outlines the company's overall security goals for managers and technical staff.***
- It provides general policies on how the technical staff should perform security functions.
- It defines system and issue-specific policies that describe what the technical staff does.

4. Which type of security policy document is it that includes implementation details that usually contain step-by-step instructions and graphics?

- best practices document
- **procedure document***
- standards document
- guideline document

5. What is the purpose of a security awareness campaign?

- to teach skills so employees can perform security tasks
- **to focus the attention of employees on security issues***
- to provide users with a training curriculum that can ultimately lead to a formal degree
- to integrate all the security skills and competencies into a single body of knowledge

6. What is the goal of network penetration testing?

- detecting configuration changes on network systems
- detecting potential weaknesses in systems
- **determining the feasibility and the potential consequences of a successful attack***
- detecting weak passwords

Explanation: There are many security tests that can be used to assess a network. Penetration testing is used to determine the possible consequences of successful attacks on the network. Vulnerability scanning can detect potential weaknesses in systems. Password cracking can detect weak passwords. Integrity checkers can detect and report configuration changes.

7. What network security testing tool has the ability to provide details on the source of suspicious network activity?

- **SIEM**
- SuperScan
- Zenmap
- Tripwire

Explanation: There are various network security tools available for network security testing and evaluation. SuperScan is a Microsoft port scanning software that detects open TCP and UDP ports on systems. Nmap and Zenmap are low-level network scanners available to the public. Tripwire is used to assess if network devices are compliant with network security policies. SIEM is used to provide real-time reporting of security events on the network.

8. What network scanning tool has advanced features that allows it to use decoy hosts to mask the source of the scan?

- Nessus
- Metasploit
- Tripwire
- **Nmap***

Explanation: There are various network security tools available for network security testing and evaluation. Nessus can scan systems for software vulnerabilities. Metasploit is used for penetration testing and IDS signature development. Tripwire is used to assess if network devices are compliant with network security policies. Nmap is a low-level network scanner available to the public that an administrator can use to identify network layer protocol support on hosts. Nnmap can use decoy hosts to mask the source of the scan.

9. What network testing tool can be used to identify network layer protocols running on a host?

- SIEM
- **Nmap***
- L0phtcrack
- Tripwire

10. What type of network security test would be used by network administrators for detection and reporting of changes to network systems?

- penetration testing
- vulnerability scanning
- **integrity checking***
- network scanning

Explanation: There are many security tests that can be used to assess a network. Penetration testing is used to determine the possible consequences of successful attacks on the network. Integrity checking is used to detect and report changes made to systems. Vulnerability scanning is used to find weaknesses and misconfigurations on network systems. Network scanning is used to discover available resources on the network.

11. What testing tool is available for network administrators who need a GUI version of Nmap?

- Nessus
- SIEM
- **Zenmap***
- SuperScan

Explanation: Nmap and Zenmap are low-level network scanners available to the public. Zenmap is the GUI version of Nmap. SuperScan is a Microsoft port scanning software that detects open TCP and UDP ports on systems. Nessus can scan systems for software vulnerabilities. SIEM is used to provide real-time reporting of security events.

12. Which initial step should be followed when a security breach is found on a corporate system?

- Create a drive image of the system.
- **Isolate the infected system.***
- Establish a chain of custody.
- Photograph the system.

13. What step should be taken after data is collected, but before equipment is disconnected, if a security breach is found on a system?

- Create a drive image of the system.
- Isolate the infected system.
- **Photograph the system.***
- Determine if data tampering has occurred.

14. Which security program is aimed at all levels of an organization, including end users and executive staff?

- educational degree programs
- certificate programs
- **awareness campaigns***
- firewall implementation training courses

15. What is implemented by administration to instruct end users in how to effectively conduct business safely within an organization?

- **security awareness program***
- governing policy
- noncompliance consequences
- technical policy

16. What are two major components of a security awareness program? (Choose two.)

- technical policy
- procedure documents
- **awareness campaigns***
- guideline documents
- **education and training***

17. Which type of documents include implementation details that usually contain step-by-step instructions and graphics?

- standards documents
- **procedure documents***
- guideline documents
- end-user policy documents

18. Which type of documents help an organization establish consistency in the operations of the network by specifying criteria that must be followed?

- guidelines
- **standards***
- procedures
- end user policies

19. Which policy outlines the overall security goals for managers and technical staff within a company?

- acceptable use policy
- technical policy
- **governing policy***
- end-user policy

20. Which type of security policy includes network access standards and server security policies?

- end user policy
- **technical policy***
- governing policy
- acceptable use policy

21. Which type of security policy includes acceptable encryption methods?

- governing policy
- acceptable use policy
- **technical policy***
- end-user policy

22. What is the determining factor in the content of a security policy within an organization?

- the security staff
- **the audience***
- the chief executive officer

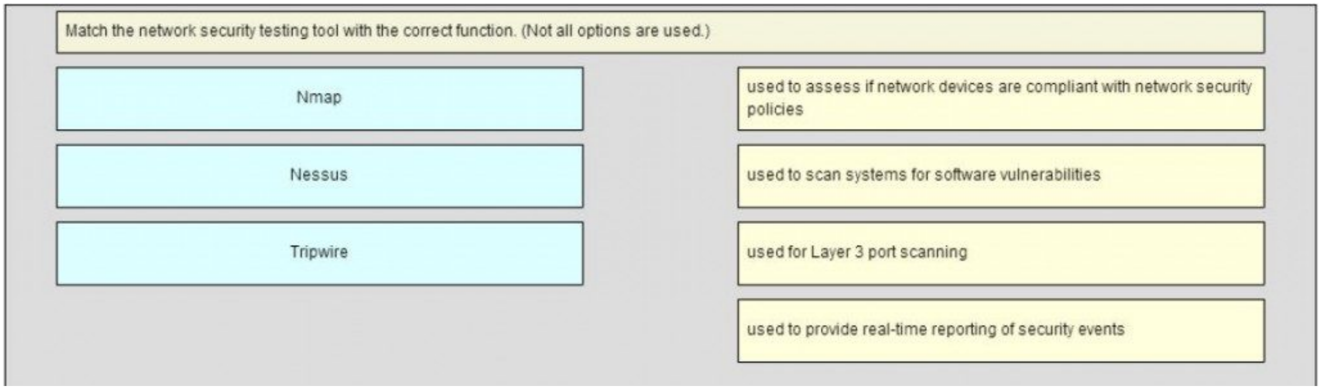
- the best practices

23. Which executive position is ultimately responsible for the success of an organization?

- Chief Technology Officer
- **Chief Executive Officer***
- Chief Security Officer
- Chief Information Officer

24. Match the network security testing tool with the correct function. (Not all options are used.)

Question



Match the network security testing tool with the correct function. (Not all options are used.)

Nmap

Nessus

Tripwire

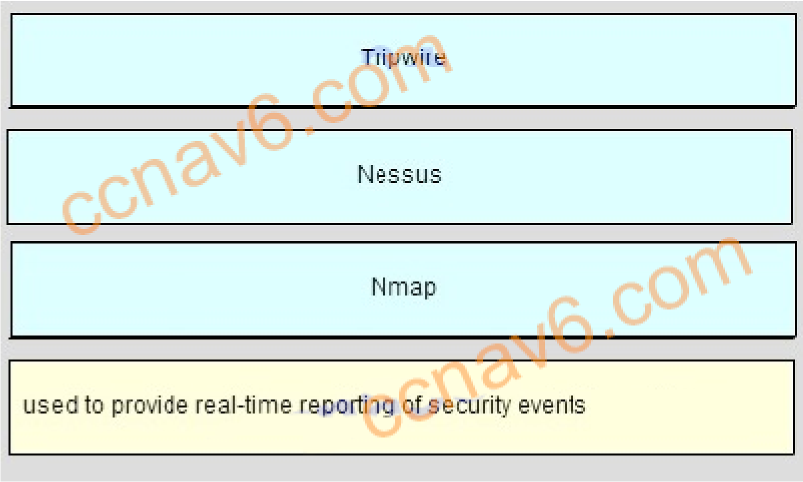
used to assess if network devices are compliant with network security policies

used to scan systems for software vulnerabilities

used for Layer 3 port scanning

used to provide real-time reporting of security events

Answer



Tripwire

Nessus

Nmap

used to provide real-time reporting of security events

Download PDF File below:

[sociallocker id="54558″]

ITexamanswers.net – CCNA Security v2.0 Chapter 11 Exam Answers.pdf

807.12 KB 1538 downloads

…

Download

[/sociallocker]