[CCNA Security Chapter 11 Exam Answers](https://itexamanswers.net/ccna-security-v2-0-chapter-11-exam-answers.html)

1. **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

There are three security policy documents:  
the standards document, which helps to maintain consistency in network operations  
the guidelines document, which gives suggestions on how to operate more securely and efficiently  
the procedures document, which gives detailed standards and guidelines that include step-by-step instructions

1. **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

A security awareness campaign is part of an effective security awareness program. The awareness campaign should focus on building security awareness and reinforcing good security practices at all levels of the organization.

1. **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

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.

1. **What network security testing tool has the ability to provide details on the source of suspicious network activity?**
   * **SIEM\***
   * SuperScan
   * Zenmap
   * Tripwire

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.

1. **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\***

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.

1. **What network testing tool can be used to identify network layer protocols running on a host?**
   * SIEM
   * **Nmap\***
   * L0phtcrack
   * Tripwire

There are various network security tools available for network security testing and evaluation. Nmap is a low-level network scanner that is available to the public that has the ability to perform port scanning and system identification. Tripwire is used to assess if network devices are compliant with network security policies. L0phtcrack can be used to perform password auditing and recovery. SIEM is used to proved real-time reporting of security events.

1. **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

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.

1. **What testing tool is available for network administrators who need a GUI version of Nmap?**
   * Nessus
   * SIEM
   * **Zenmap\***
   * SuperScan

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.

1. **What are two major components of a security awareness program? (Choose two.)**
   * technical policy
   * procedure documents
   * **awareness campaigns\***
   * guideline documents
   * **education and training\***

Security awareness programs are designed to keep everyone aware of security issues and educate staff members via the use of awareness campaigns and training and education

1. **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

There are multiple policy documents that exist for situations of varied needs. These include the following:  
End-user policy documents that cover security topics important to end users  
Standards documents that include hardware and software versioning requirements, program requirements, and any other organizational criteria that must be followed  
Guideline documents that include suggestions on how to do things more efficiently and securely. They are more flexible than standards documents and are not usually mandatory.  
Procedure documents that include details that usually contain step-by-step instructions and graphics

1. **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.

If a security breach occurs, it is necessary to follow the proper procedures.  
The infected system should be isolated immediately.  
A drive image should be taken before working with data on the hard drive of the infected system.  
After data is collected but before equipment is disconnected, there should be photographs taken of the equipment before anything else should be done.  
A chain of custody should be established identifying all evidence.

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

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.

1. **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.

Network scanning can help a network administrator strengthen the security of the network and systems by identifying open TCP and UDP ports that could be targets of an attack.

1. **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.

A security policy is often broken up into a hierarchical structure consisting of three sub-policies:  
a governing policy  
a technical policy  
an end-user policy  
The governing policy is a high-level policy that provides security guidelines for the entire company and outlines overall security goals.

1. **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.

If a security breach occurs, it is necessary to follow the proper procedures.  
The infected system should be insolated immediately.  
A drive image should be taken before working with data on the hard drive of the infected system.  
After data is collected but before equipment is disconnected, there should be photographs taken of the equipment before anything else is done.

1. **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

Awareness campaigns are designed for all levels of users and focus attention on security issues. Educational degree programs are programs at a college or university that assist a user in the study of concepts, issues, and principles as an IT security professional. Security training for IT staff would include courses that address in detail how to implement firewall technology. Certificate programs are conducted as a joint effort between schools and software or hardware vendors and are a form of training users.

1. **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

Administration can reduce the loss of intellectual capital, critical data, and physical equipment by disseminating information to end users through the use of a security awareness program

1. **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

There are multiple policy documents that exist for situations of varied needs. These include the following:  
End user policy documents that cover security topics important to end users  
Standards documents that include hardware and software versioning requirements, program requirements, and any other organizational criteria that must be followed  
Guideline documents that include suggestions on how to do things more efficiently and securely, and which are more flexible than standards documents and are not usually mandatory.  
Procedure documents that include details that usually contain step-by-step instructions and graphics

1. **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

Multiple types of security policies can exist within an organization. These may include the following:  
Acceptable use policies that define what users are allowed and not allowed to do on the various system components  
Governing policies that outline the overall security goals for managers and technical staff within a company  
Technical policies that describe what the technical staff does and defines standards that are used to connect to the network  
End-user policies that cover all rules pertaining to information security that end users should know about and follow

1. **Which type of security policy includes network access standards and server security policies?**
   * end user policy
   * **technical policy\***
   * governing policy
   * acceptable use policy

Multiple types of security policies can exist within an organization. These may include the following:  
Acceptable use policies that define what users are allowed and not allowed to do on the various system components  
Governing policies that outline the overall security goals for managers and technical staff within a company  
Technical policies that describe what the technical staff does and defines standards that are used to connect to the network  
End user policies that cover all rules pertaining to information security that end users should know about and follow

1. **Which type of security policy includes acceptable encryption methods?**
   * governing policy
   * acceptable use policy
   * **technical policy\***
   * end-user policy

Multiple types of security policies can exist within an organization. These may include the following:  
Acceptable use policies that define what users are allowed and not allowed to do on the various system components  
Governing policies that outline the overall security goals for managers and technical staff within a company  
Technical policies that describe what the technical staff does and defines standards that are used to connect to the network  
End-user policies that cover all rules pertaining to information security that end users should know about and follow

1. **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

When the content of a security policy is being determined, the audience that is targeted in the policy is the determining factor in why something is required or what the noncompliance consequences will be.

1. **Which executive position is ultimately responsible for the success of an organization?**
   * Chief Technology Officer
   * **Chief Executive Officer\***
   * Chief Security Officer
   * Chief Information Officer

In the comparison of common executive titles:  
The Chief Executive Officer, also known as the CEO is ultimately responsible for the success of an organization.  
The Chief Technology Officer is responsible for maintaining and improving existing systems.  
The Chief Information Officer is responsible for all IT and computer systems that support enterprise goals.  
The Chief Security Officer must limit exposure to liability in all areas of financial, physical, and personal risk.

1. **Match the network security testing tool with the correct function. (Not all options are used.)**
   * Question  
     Graphical user interface

     Description automatically generated
   * Answer  
     Graphical user interface, text, application, email

     Description automatically generated