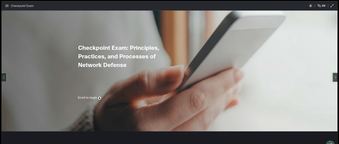
Checkpoint Exam



Checkpoint Exam: Principles, Practices, and Processes of Network Defense

Scroll to begin ↓

Welcome to the **Principles, Practices, and Processes of Network Defense Checkpoint Exam.**

There are **24 questions** in total.

Items in this exam support the following Cybersecurity skills:

- Use cybersecurity concepts to document a network security protocol.
- Configure security measures on network devices and cross and Windows endpoints.
- Implement phases of Identity lifecycle management.

You have unlimited attempts to pass the exam. **Feedback is provided** to direct you to areas that may require additional attention.

Cisco Networking Academy content is copyrighted and the unauthorized posting, distribution or sharing of this exam content is prohibited.

© 2023, Cisco Systems, Inc.

Question 1

Which type of business policy establishes the rules of conduct and the responsibilities of employees and employers?

- data
- employer
- security
- **company**

Question 2

What is a characteristic of the security whitelisting, defense-in-depth approach?

- Each layer has to be penetrated before the threat actor can reach the target data or system.
- **Trusted actors no longer have to power away each layer before reaching the target data or system.**
- Trusted actors can no longer penetrate any layers safeguarding the data or systems.
- Trusted actors can easily compromise all layers safeguarding the data or systems.

Question 3

Which security management function is concerned with the inventory and control of hardware and software configurations of systems?

- vulnerability management
- **configuration management**
- asset management
- risk management

Question 4

Match the term to the description.

Categories:		Options:
vulnerabilities	→	weaknesses in a system or design
assets	→	information or equipment provided through to the organization to support operations
threats	→	potential dangers to a protected asset

Question 5

Which network monitoring tool is in the category of network protocol analyzers?

- **wireshark**
- snort
- zmap
- sslsnf

Question 6

Which security measure is typically found both inside and outside a data center facility?

- biometrics access
- **multifactor entry turnstiles**
- wall sensors
- security traps
- a gate

Question 7

Which two options are security best practices that help mitigate BYOD risks? (Choose two.)

- Use wireless MAC address filtering.
- **Force turn on Wi-Fi when using the wireless network.**
- Decrease the wireless antenna gain level.
- Use paint that reflects wireless signals and place that prevents the signals from going outside the building.
- Only allow devices that have been approved by the corporate IT team.
- **Keep the device OS and software updated.**

Question 8

What device would be used as a second line of defense in a defense-in-depth approach?

- internal router
- switch
- edge router
- **firewall**

Question 9

What is a strength of using a hashing function?

- It can take only a fixed length message.
- Two different files can be created that have the same output.
- It is not commonly used in security.
- **It is one way function and not reversible.**
- It has a variable length output.

Question 10

A company is developing an internet store website. Which protocol should be used to transfer credit card information from customers to the company web server?

- FTPS
- SSH
- SFTP
- **HTTPS**
- pcTCP

Question 11

What is a purpose of implementing VLANs on a network?

- They prevent Layer 2 loops.
- **They can isolate user traffic.**
- They eliminate network collisions.
- They allow switches to forward Layer 2 packets without a router.

Question 12

A user is purchasing a new server for the company data center. The user wants disk striping with parity on three disks. Which RAID level should the user implement?

- **5 or 6**
- 1
- 0
- 10

Question 13

A large retail company uses EAP based authentication in conjunction with 802.1X. When the client first initiates communication on the wireless network, which type of authentication method is used by the client to associate with the AP?

- **open authentication**
- WPA2
- WPA3
- WPA

Question 14

What is an example of the implementation of physical security?

- encrypting hard all operating system and antivirus software is up to date
- encrypting all sensitive data that is stored on the servers
- establishing personal firewalls on each computer
- **qualifying employees to ask a card key when entering a secure area**

Question 15

Why is asset management a critical function of a growing organization against security threats?

- It prevents theft of older assets that are decommissioned.
- It allows for a redrill of a comprehensive ALP.
- **It identifies the best increasing attack surface to threats.**
- It serves to preserve an audit trail of all new purchases.

Question 16

A user has created a new program and wants to distribute it to everyone in the company. The user wants to ensure that when the program is downloaded that the program is not changed while in transit. What can the user do to ensure that the program is not changed while downloaded?

- Encrypt the program and require a password after it is downloaded.
- **Provide a hash of the program file that can be used to verify the integrity of the file after it is downloaded.**
- Turn off antivirus on all the computers.
- Distribute the program on a thumb drive.
- Install the program on individual computers.

Question 17

An intern has started working in the support group. One duty is to set local policy for passwords on the workstations. What tool would be best to use?

- **secpol.msc**
- password policy
- gpedit.msc
- system administration
- account policy

Question 18

Passwords, passphrases, and PINs are examples of which security term?

- identification
- **authentication**
- access
- authorization

Question 19

What is privilege escalation?

- A security problem occurs when high ranking corporate officials demand rights by systems or files that they should not have.
- **Everyone is given full rights by default to everything and rights are later deep pitts delete premious private privileges.**
- Vulnerabilities in systems are exploited to gain higher levels of privilege than someone in some process should have.
- Someone is given rights because she or he has received a promotion.

Question 20

A network administrator is configuring an AAA server to manage RADIUS authentication. Which two features are included in RADIUS authentication? (Choose two.)

- encryption for all communication
- **single process for authentication and authorization**
- encryption for only the data
- **multi-protocol during transmission**
- separate processes for authentication and authorization

Question 21

Which access control model applies the strictest access control and is often used in military and mission critical applications?

- attribute based
- nondiscretionary
- discretionary
- **mandatory**

Question 22

What are three examples of administrative access controls? (Choose three.)

- encryption
- **hiring practices**
- guard dogs
- intrusion detection system (IDS)
- **security policy procedures**
- **background checks**

Question 23

Which access control model allows users to control access to data on an owner of that data?

- nondiscretionary access control
- **discretionary access control**

attribute-based access control

mandatory access control

Question 24

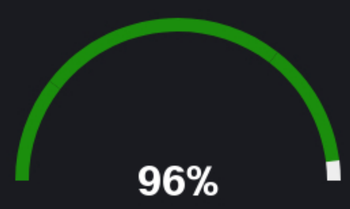
What is the purpose of the network security authentication function?

- to provide challenge and response questions
- to keep track of the actions of a user
- ✓ to require users to prove who they are
- to determine which resources a user can access

You've submitted your answers!

Reset

Review Assessment



You've scored 96%.

Congratulations, you have passed the assessment.

Here is how you performed in each of the Learning Objectives and Skills associated with this assessment.	
Module: Understanding Defense	100%
Module: System and Network Defense	100%
Module: Access Control	100%
Skill: Use cybersecurity concepts to document cybersecurity issues.	100%
Skill: Implement wireless network security measures.	100%
Skill: Configure security measures on network devices and Linux and Windows endpoints.	100%
Skill: Implement phases of identity lifecycle management.	88.2%