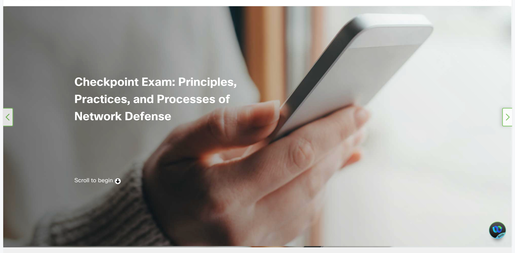

Checkpoint Exam: Principles, Practices, and Processes of Network Defense

Scroll to begin

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

There are **24 questions** in total.

Items on this exam support the following Cybersecurity skills:

- Use cybersecurity concepts to document a network security posture.
- Configure security measures on network devices and Linux 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

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

- edge router
- switch
- internal router
- ✓ firewall

Question 2

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

- risk management
- asset management
- vulnerability management
- ✓ configuration management

Question 3

Match the term to the description.

Categories:		Options:
vulnerabilities	A	C potential dangers to a protected asset
assets	B	B information or equipment valuable enough to an organization to warrant protection
threats	C	A weaknesses in a system or design

Question 4

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

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

Question 5

What is a characteristic of the security artichoke, defense–in–depth approach?

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

Question 6

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

- employee
- security
- data
- ✓ company

Question 7

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

- ✓ continuous video surveillance
- security traps
- biometrics access
- exit sensors
- a gate

Question 8

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

- ✓ Wireshark
- SIEM
- SPAN
- SNMP

Question 9

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

- ✓ It identifies the ever increasing attack surface to threats.
- It serves to preserve an audit trail of all new purchases.
- It allows for a build of a comprehensive AUP.
- It prevents theft of older assets that are decommissioned.

Question 10

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
- 1
- 0
- 1+0

Question 11

What is a purpose of implementing VLANs on a network?

- ✓ They can separate user traffic.
- They allow switches to forward Layer 3 packets without a router.
- They eliminate network collisions.
- They prevent Layer 2 loops.

Question 12

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?

- WPA3
- WPA2
- ✓ Open Authentication
- WPA

Question 13

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 when downloaded?

- ✓ Create a hash of the program file that can be used to verify the integrity of the file after it is downloaded.
- Encrypt the program and require a password 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 14

What is a strength of using a hashing function?

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

Question 15

What is an example of the implementation of physical security?

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

Question 16

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?

- ✓ HTTPS
- FTPS
- HTTP
- WPA2
- SSH

Question 17

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

- ✓ authentication
- identification
- authorization
- access

Question 18

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

- encryption for only the data
- ✓ hidden passwords during transmission
- encryption for all communication
- separate processes for authentication and authorization
- ✓ single process for authentication and authorization

Question 19

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?

- grpol.msc
- account policy
- ✓ secpol.msc
- system administration
- password policy

Question 20

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

- encryption
- guard dogs
- ✓ hiring practices
- ✓ policies and procedures
- ✓ background checks
- intrusion detection system (IDS)

Question 21

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

- nondiscretionary
- attribute-based
- discretionary
- ✓ mandatory

Question 22

What is privilege escalation?

- ✓ Vulnerabilities in systems are exploited to grant higher levels of privilege than someone or some process should have.
- Someone is given rights because she or he has received a promotion.
- A security problem occurs when high ranking corporate officials demand rights to systems or files that they should not have.
- Everyone is given full rights by default to everything and rights are taken away only when someone abuses privileges.

Question 23

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

- ✓ discretionary access control
- nondiscretionary access control
- mandatory access control

mandatory access control

attribute-based access control

Question 24

What is the purpose of the network security authentication function?

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

You've submitted your answers!

Reset

Review Assessment

You've scored 100%.

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.	100%