Module 6 Assessment (SK0-004)

Due May 21 at 11:59pm **Points** 20 **Questions** 20
Time Limit 45 Minutes **Allowed Attempts** 2

Instructions

You have two attempts to take this assessment with the highest score being retained. The assessment has a time limit of 45 minutes.

Suggestion: take the assessment at the beginning of the module and then after the reading and assignments are done. You can then use the results of both to gauge your learning and retention.

Take the Quiz Again

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	12 minutes	18 out of 20

Answers will be shown after your last attempt

Score for this attempt: **18** out of 20
Submitted May 17 at 9:46am
This attempt took 12 minutes.

Question 1 — 1 / 1 pts

Which statement about windows BitLocker encryption is true?

- TPM is required.
- Data encryption is tide to specific user accounts.
- The entire disk volume is encrypted.

- Individual files can be encrypted.

Question 2

1 / 1 pts

Which statement about the Encrypting File System (EFS) is true?

- A user PKI certificate is required.
- TPM is required.
- A device PKI certificate is required.
- The entire disk volume is encrypted.

Question 3

1 / 1 pts

Which of the following activities is considered server hardening?

- Adding users to a file system ACL
- Applying RAID controller firmware updates
- Creating virtual machine snapshots
- Enabling Wake-on-LAN

Question 4

1 / 1 pts

While viewing the file system contents on a Linux host, you notice some files have a permission of 764 set. What does this mean?

The file owner has read write permissions; the group has read write permissions; and everybody else has read permissions.

The file owner has read execute permissions; the group has read write permissions; And everybody else has read permissions.

The file owner has right and execute permissions; the group has read write permission; And everybody else has read permissions.

The file owner has read write execute permissions; the group has read write permissions; and everyone has read permission.

Question 5

1 / 1 pts

Which PKI key is used to encrypt an email message?

- Private key
- Public key
- Cipher key
- Asymmetric key

Question 6

1 / 1 pts

Which is an example of multifactor authentication?

- Username, password
- Username, building door code

- Smart card, ID badge
- Smart card, PIN

Question 7

1 / 1 pts

Which term describes the topmost entity in a PKI?

- Certificate authority
- Public key
- Private key
- User PKI certificate

Question 8

1 / 1 pts

A colleague needs the ability to remotely remove only corporate data from lost or stolen smartphones. What method will accomplish this?

- Selective wipe
- Remote wipe
- Full wipe
- Corporate wipe

Incorrect

Question 9

0 / 1 pts

Your company creates secondary backup tape copies: one copy is stored onsite, and the other is stored offsite. Where should onsite backup copies be secured?

- Safe
- Locked filing cabinet
- Locked server room
- Locked desk drawer

Question 10

1 / 1 pts

In the interest of securing internal network traffic, your boss asks you to ensure that all LAN traffic is encrypted. What should you configure?

- SSL
- TLS
- Cipher
- IPSec

Question 11

1 / 1 pts

Users authenticate to the VPN with a username and password. What type of authentication is this?

- Single factor authentication

- Dual factor authentication
- Multifactor authentication
- Full authentication

Question 12

1 / 1 pts

Your company stores sensitive patient health information on a database server. Any abnormal activity on that server must be logged and trigger and alert sent to administrators. What should you configure?

- (selected) IDS
- IPS
- Packet sniffer
- Disk encryption

Question 13

1 / 1 pts

How does a vulnerability scan differ from a penetration test?

- A vulnerability scan exploits discovered vulnerabilities.
- A penetration test identifies vulnerabilities but does not exploit those vulnerabilities.
- Penetration test is passive.

A vulnerability scan identifies vulnerabilities but does not exploit those vulnerabilities.

Question 14

1 / 1 pts

You discover a compromised user account on your network. After talking to the affected user, you discover that he sent his credentials to somebody posing as part of the internal IT team. What kind of method did the attacker use?

- Social engineering
- Backdoor
- Mantrap
- Insider threat

Question 15

1 / 1 pts

What is the windows cipher.exe tool used for?

- Issuing PKI certificates
- File hashing
- VPN configuration
- Encrypting files and folders

Question 16

1 / 1 pts

Users in your company occasionally transfer files to computers on air gapped networks by using removable USB drives. Your boss asks you to configure a solution that ensures data confidentiality of transferred data. What should you configure?

- Hash removable USB devices
- Compress removable USB devices
- Encrypt removable USB devices
- Use IPSec to transfer the files

Incorrect

Question 17

0 / 1 pts

Which of the following statements regarding security permissions are true? (Choose two.)

- [x] Permissions set to allow override permissions set to deny.
- [ ] Permissions set to deny override permissions set to allow.
- [ ] NTFS write permission allows file deletion.
- [x] The NTFS modify permission allows file deletion.

Question 18

1 / 1 pts

Which of the following are examples of IEEE 802.1 X-compliant devices? (Choose two.)

- [ ] Proxy server
- [x] VPN appliance
- [x] Wireless router
- [ ] Storage appliance

Question 19

1 / 1 pts

Which of the following are examples of radius clients? (Choose two.)

- [ ] Smartphone
- [x] Wireless access point
- [ ] Desktop
- [x] VPN appliance

Question 20

1 / 1 pts

Which of the following are not examples of hardening a server? (Choose two.)

- [x] Enabling all available services
- [ ] Installing the latest patches
- [ ] Closing unneeded ports

- [x] Opening additional ports to make attackers guess what ports your services are on

Quiz Score: **18** out of 20