Cisco Cybersecurity Essentials

Started on	Thursday, 16 November 2023, 9:36 PM
State	Finished
Completed on	Thursday, 16 November 2023, 9:50 PM
Time taken	14 mins 30 secs
Marks	42.00/42.00
Grade	**100.00** out of 100.00

Question **1**

Correct

Mark 2.00 out of 2.00

The CIO wants to secure data on company laptops by implementing file encryption. The technician determines the best method is to encrypt each hard drive using Windows BitLocker. Which two things are needed to implement this solution? (Choose two.)

Select one or more:

- USB stick
- EFS
- ✓ at least two volumes ✔
- backup
- password management
- ✓ TPM ✔

Refer to curriculum topic: 7.1.3
Windows provides a method to encrypt files, folders, or entire hard drives depending on need. However, certain BIOS settings and configurations are necessary to implement encryption on an entire hard disk.

The correct answers are: at least two volumes, TPM

Question **2**

Correct

Mark 2.00 out of 2.00

A user is asked to analyze the current state of a computer operating system. What should the user compare the current operating system against to identify potential vulnerabilities?

Select one:

- ◉ a baseline ✔
- ○ a blacklist
- ○ a pentest
- ○ a whitelist
- ○ a vulnerability scan

Refer to curriculum topic: 7.1.1
A baseline allows a user to perform a comparison of how a system is performing. The user can then compare the result to baseline expectations. This process allows the user to identify potential vulnerabilities.

The correct answer is: a baseline

Question **3**

Correct

Mark 2.00 out of 2.00

Companies may have different operation centers that handle different issues with the IT operations. If an issue is related to network infrastructure, what operation center would be responsible?

Select one:

- HR
- HVAC
- SOC
- NOC ✔

Refer to curriculum topic: 7.3.1
Operation centers support different areas of the operation including the network and security. Each one focuses on particular parts of the IT structure. The center that supports security would be the SOC.

The correct answer is: NOC

Question **4**

Correct

Mark 2.00 out of 2.00

Which three items are malware? (Choose three.)

Select one or more:

- email
- attachments
- keylogger ✔
- virus ✔
- Trojan horse ✔
- Apt

Refer to curriculum topic: 7.1.1
Email could be used to deliver malware, but email by itself is not malware. Apt is used to install or remove software within a Linux operating system. Attachments could contain malware, but not always.

The correct answers are: Trojan horse, virus, keylogger

Question **5**

Correct

Mark 2.00 out of 2.00

A user calls the help desk complaining that the password to access the wireless network has changed without warning. The user is allowed to change the password, but an hour later, the same thing occurs. What might be happening in this situation?

Select one:

- rogue access point ✔
- weak password
- user laptop
- password policy
- user error

Refer to curriculum topic: 7.1.2
Man-in-the-middle attacks are a threat that results in lost credentials and data. These type of attacks can occur for different reasons including traffic sniffing.

The correct answer is: rogue access point

Question **6**

Correct

Mark 2.00 out of 2.00

A user is proposing the purchase of a patch management solution for a company. The user wants to give reasons why the company should spend money on a solution. What benefits does patch management provide? (Choose three.)

Select one or more:

- Updates cannot be circumvented. ✔
- Updates can be forced on systems immediately. ✔
- Administrators can approve or deny patches. ✔
- Patches can be written quickly.
- Patches can be chosen by the user.
- Computers require a connection to the Internet to receive patches.

Refer to curriculum topic: 7.1.1
A centralized patch management system can speed up deployment of patches and automate the process. Other good reasons to using an automated patch update service include the following:

- Administrators control the update process.
- Reports are generated.
- Updates are provided from a local server.
- Users cannot circumvent the update process.

The correct answers are: Administrators can approve or deny patches., Updates can be forced on systems immediately., Updates cannot be circumvented.

Question **7**

Correct

Mark 2.00 out of 2.00

A new PC is taken out of the box, started up and connected to the Internet. Patches were downloaded and installed. Antivirus was updated. In order to further harden the operating system what can be done?

Select one:

- Install a hardware firewall.
- Remove the administrator account.
- Turn off the firewall.
- Remove unnecessary programs and services. ✔
- Disconnect the computer from the network.
- Give the computer a nonroutable address.

Refer to curriculum topic: 7.1.1
When hardening an operating system, patching and antivirus are part of the process. Many extra components are added by the manufacturer that are not necessarily needed.

The correct answer is: Remove unnecessary programs and services.

Question **8**

Correct

Mark 2.00 out of 2.00

Why is WPA2 better than WPA?

Select one:

- mandatory use of AES algorithms ✔
- reduced keyspace
- reduced processing time
- supports TKIP

Refer to curriculum topic: 7.1.2
A good way to remember wireless security standards is to consider how they evolved from WEP to WPA, then to WPA2. Each evolution increased security measures.

The correct answer is: mandatory use of AES algorithms

Question **9**

Correct

Mark 2.00 out of 2.00

A user makes a request to implement a patch management service for a company. As part of the requisition the user needs to provide justification for the request. What three reasons can the user use to justify the request? (Choose three.)

Select one or more:

- no opportunities for users to circumvent updates ✔
- the ability to control when updates occur ✔
- the ability to obtain reports on systems ✔
- the likelihood of storage savings
- the need for systems be directly connected to the Internet
- the ability of users to select updates

Refer to curriculum topic: 7.1.1
A patch management service can provide greater control over the update process by an administrator. It eliminates the need for user intervention.

The correct answers are: the ability to obtain reports on systems, the ability to control when updates occur, no opportunities for users to circumvent updates

Question **10**

Correct

Mark 2.00 out of 2.00

The manager of desktop support wants to minimize downtime for workstations that crash or have other software-related issues. What are three advantages of using disk cloning? (Choose three.)

Select one or more:

- ensures system compatibility
- creates greater diversity
- cuts down on number of staff needed
- ensures a clean imaged machine ✔
- can provide a full system backup ✔
- easier to deploy new computers within the organization ✔

Refer to curriculum topic: 7.1.4
Disk cloning can be an efficient way to maintain a baseline for workstations and servers. It is not a cost cutting method.

The correct answers are: easier to deploy new computers within the organization, can provide a full system backup, ensures a clean imaged machine

Question **11**

Correct

Mark 2.00 out of 2.00

The company has many users who telecommute. A solution needs to be found so a secure communication channel can be established between the remote location of users and the company. What is a good solution for this situation?

Select one:

- fiber
- T1
- modem
- PPP
- VPN ✔

Refer to curriculum topic: 7.1.1
When a VPN is used, a user can be at any remote location such as home or a hotel. The VPN solution is flexible in that public lines can be used to securely connect to a company.

The correct answer is: VPN

Question **12**

Correct

Mark 2.00 out of 2.00

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?

Select one:

- **grpol.msc**
- system administration
- password policy
- account policy
- **secpol.msc** ✔

Refer to curriculum topic: 7.2.2
Local policies are not group policies and only work on the local machine. Local policies can, however, be overridden if the machine is part of a Windows domain.

The correct answer is: **secpol.msc**

Question **13**

Correct

Mark 2.00 out of 2.00

Which service will resolve a specific web address into an IP address of the destination web server?

Select one:

- DNS ✔
- ICMP
- DHCP
- NTP

Refer to curriculum topic: 7.3.1
DNS resolves a website address to the actual IP address of that destination.

The correct answer is: DNS

Question **14**

Correct

Mark 2.00 out of 2.00

A company wants to implement biometric access to its data center. The company is concerned with people being able to circumvent the system by being falsely accepted as legitimate users. What type of error is false acceptance?

Select one:

- Type I
- CER
- false rejection
- Type II ✔

Refer to curriculum topic: 7.4.1
There are two types of errors that biometrics can have: false acceptance and false rejection. False acceptance is a Type II error. The two types can intersect at a point called the crossover error rate.

The correct answer is: Type II

Question **15**

Correct

Mark 2.00 out of 2.00

After a security audit for an organization, multiple accounts were found to have privileged access to systems and devices. Which three best practices for securing privileged accounts should be included in the audit report? (Choose three.)

Select one or more:

- Enforce the principle of least privilege. ✔
- Secure password storage. ✔
- Reduce the number of privileged accounts. ✔
- Only the CIO should have privileged access.
- No one should have privileged access.
- Only managers should have privileged access.

Refer to curriculum topic: 7.2.2
Best practices entail giving the user only what is needed to do the job. Any additional privileges should be tracked and audited.

The correct answers are: Reduce the number of privileged accounts., Secure password storage., Enforce the principle of least privilege.

Question **16**

Correct

Mark 2.00 out of 2.00

The manager of a department suspects someone is trying to break into computers at night. You are asked to find out if this is the case. What logging would you enable?

Select one:

- operating system
- audit ✔
- Windows
- syslog

Refer to curriculum topic: 7.2.2
Audit logs can track user authentication attempts on workstations and can reveal if any attempts at break-in were made.

The correct answer is: audit

Question **17**

Correct

Mark 2.00 out of 2.00

Why should WEP not be used in wireless networks today?

Select one:

- its lack of support
- its lack of encryption
- its age
- easily crackable ✔
- its use of clear text passwords

Refer to curriculum topic: 7.1.2
Despite improvements, WEP is still vulnerable to various security issues including the ability to be cracked.

The correct answer is: easily crackable

Question **18**

Correct

Mark 2.00 out of 2.00

What are three types of power issues that a technician should be concerned about? (Choose three.)

Select one or more:

- blackout ✔
- spike ✔
- flicker
- spark
- fuzzing
- brownout ✔

Refer to curriculum topic: 7.2.3
Power issues include increases, decreases, or sudden changes in power and include the following:

- Spike
- Surge
- Fault
- Blackout
- Sag/dip
- Brownout
- Inrush Current

The correct answers are: spike, brownout, blackout

Question **19**

Correct

Mark 2.00 out of 2.00

An administrator of a small data center wants a flexible, secure method of remotely connecting to servers.Which protocol would be best to use?

Select one:

- Telnet
- Secure Shell ✔
- Secure Copy
- Remote Desktop

Refer to curriculum topic: 7.2.1
Because hackers sniffing traffic can read clear text passwords, any connection needs to be encrypted. Additionally, a solution should not be operating system-dependent.

The correct answer is: Secure Shell

Question **20**

Correct

Mark 2.00 out of 2.00

A user calls the help desk complaining that an application was installed on the computer and the application cannot connect to the Internet. There are no antivirus warnings and the user can browse the Internet. What is the most likely cause of the problem?

Select one:

- permissions
- corrupt application
- computer firewall ✔
- need for a system reboot

Refer to curriculum topic: 7.1.1
When troubleshooting a user problem, look for some common issues that would prevent a user from performing a function.

The correct answer is: computer firewall

Question **21**

Correct

Mark 2.00 out of 2.00

What is the difference between an HIDS and a firewall?

Select one:

- An HIDS blocks intrusions, whereas a firewall filters them.
- A firewall allows and denies traffic based on rules and an HIDS monitors network traffic.
- A firewall performs packet filtering and therefore is limited in effectiveness, whereas an HIDS blocks intrusions.
- An HIDS monitors operating systems on host computers and processes file system activity. Firewalls allow or deny traffic between the computer and other systems. ✔
- An HIDS works like an IPS, whereas a firewall just monitors traffic.

Refer to curriculum topic: 7.1.1
In order to monitor local activity an HIDS should be implemented. Network activity monitors are concerned with traffic and not operating system activity.

The correct answer is: An HIDS monitors operating systems on host computers and processes file system activity. Firewalls allow or deny traffic between the computer and other systems.

◀ Launch Chapter 7

Jump to...

Launch Chapter 8 ▶