Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/8/2022 7:28:05 pm • Time spent: 02:54

Score: 100% Passing Score: 80%

Question 1: ✔ Correct

Your company has five salesmen who work out of the office and frequently leave their laptops laying on their desks in their cubicles. You are concerned that someone might walk by and take one of these laptops. Which of the following is the BEST protection implementation to address your concerns?

- Implement screen saver passwords.
- Encrypt all company data on hard drives.
- Use cable locks to chain the laptops to the desks.
- Require strong passwords in the Local Security Policy.

EXPLANATION

In this case, your main concern is that someone might steal the laptops. The best protection against physical theft is to secure the laptops in place using a cable lock.

Requiring strong passwords or using encryption might prevent unauthorized users from accessing data on the laptops, but these measures do not prevent physical theft.

Question 2: ✔ Correct

Your networking closet contains your network routers, switches, bridges, and some servers. You want to make sure an attacker is not able to gain physical access to the equipment in the networking closet. You also want to prevent anyone from reconfiguring the network to set up remote access or backdoor access.

Which of the following measures are the best ways to secure your networking equipment from unauthorized physical access? (Select two. Each measure is part of a complete solution.)

- [ ] Place your networking equipment in a Faraday cage.
- [x] Place your networking equipment in a locked cage.
- [ ] Place your networking equipment in a Van Eck cage.
- [x] Place your networking equipment in a room that requires key card entry.
- [ ] Place your networking equipment in a TEMPEST cage.

EXPLANATION

Placing your networking equipment in a locked cage inside of a locked room that also requires key card access is the best way to physically secure your network from an attacker who would attempt to gain physical access.

A Faraday cage prevents attackers from using Van Eck phreaking to gather electronic emissions coming from your networking closet. The government uses a special emission security specification called TEMPEST that requires the use of a Faraday cage.

Question 3: ✔ Correct

You are an IT consultant. You are visiting a new client's site to become familiar with their network. As you walk around their facility, you note the following:

- When you enter the facility, a receptionist greets you and escorts you through a locked door to the work area where the office manager sits.
- The office manager informs you that the organization's servers are kept in a locked closet. An access card is required to enter the server closet.
- She informs you that server backups are configured to run each night. A rotation of tapes are used as the backup media.
- You notice the organization's network switch is kept in the server closet.
- You notice that a router/firewall/content filter all-in-one device has been implemented in the server closet to protect the internal network from external attacks.
- The office manager informs you that her desktop system no longer boots and asks you to repair or replace it, recovering as much data as possible in the process. You take the workstation back to your office to work on it.

Which security-related recommendations should you make to this client?

- Replace the tape drive used for backups with external USB hard disks.
- Keep the network infrastructure devices (switch and all-in-one device) in a locked room separate from network servers.
- ➡ Implement a hardware checkout policy.
- Upgrade the server closet lock to a biometric authentication system.

EXPLANATION

In this scenario, you should recommend the client implement a hardware checkout policy. A checkout policy ensures that hardware containing sensitive data does not leave the organization's premises without approval and without recording the device's serial number, make, and model number.

A biometric server room lock is probably not necessary in this scenario. It is acceptable to keep servers and network devices, such as routers and switches, in the same room, as long as that room is kept secure. There's no security advantage to using external hard drives instead of tape backup media.

Question 4: ✔ Correct

Which of the following is the most important thing to do to prevent console access to the router?

- Implement an access list to prevent console connections.
- ➡ Keep the router in a locked room.
- Disconnect the console cable when not in use.
- Set the console and enable secret passwords.

EXPLANATION

To control access to the router console, you must keep the router in a locked room. A console connection can only be established with a direct physical connection to the router. If the router is in a locked room, only those with access are able to make a console connection. In addition, even if you had set console passwords, users with physical access to the router could perform router password recovery and gain access.

Question 5: ✔ Correct

Burning, pulping, and shredding are three ways to securely dispose of data in which form?

- Cloud
- Disk
- ➡ Paper
- Tape

EXPLANATION

Although tape and disk could be destroyed by industrial shredders, pulping can only be done to paper by using water and chemicals to dissolve the paper.

Data in the cloud must be disposed of with tools from the cloud provider.

Question 6: ✔ Correct

A computer or small network that is not connected to the rest of the network or the internet is known as:

- ➡ Air gap
- Faraday cage
- DMZ
- Vault

EXPLANATION

An air gap is a physical break between a computer or a small network to isolate it from potential threats.

DMZ is incorrect because a DMZ is connected to other network segments.

A vault provides physical protection for network equipment.

A Faraday cage prevents wireless emissions from being leaked.

Question 7: ✔ Correct

Which device is used to allow a USB device to charge but blocks the data transfer capabilities of the device?

- Bollard
- Faraday cage
- Air gap
- ➡ USB data blocker

EXPLANATION

A USB data blocker prevents data from being transmitted while allowing the device to draw power. This is useful for charging devices on unknown USB ports, such as those at public charging stations.

An air gap is a network or device not connected to the rest of the network.

A bollard is physical protection to keep a vehicle from crashing into a secured area.

A Faraday cage prevents wireless emissions from being leaked.

Question 8: ✔ Correct

Which device is often employed by power companies to protect cabling infrastructure from having cables added or removed and to prevent emissions from being retrieved from the air?

- USB data blocker
- Air gap
- ➡ PDS
- Faraday cage

EXPLANATION

A protective distribution system (PDS) keeps cabling secure while also preventing electronic emissions.

A USB data blocker prevents data from being transmitted while allowing the device to draw power.

An air gap is a network or device not connected to the rest of the network.

A Faraday cage prevents wireless emissions from being leaked, but it does not protect cabling.

Question 9: ✔ Correct

Which special network area is used to provide added protection by isolating publicly accessible servers?

- VLAN
- Internet
- Intranet
- ➡ DMZ

EXPLANATION

A demilitarized zone (DMZ) is an area of the network where extra security is placed to protect the internal network from publicly accessible servers like web servers and email servers.

A VLAN may be used to create a DMZ, but it is not inherently a DMZ.

The internet and intranet zones are the areas on the outside and inside of a network that a DMZ is designed to protect.

Question 10: ✔ Correct

A Faraday cage is used to prevent what from leaving an area?

- Computers
- Network packets
- Electromagnetic emissions
- Hackers

EXPLANATION

Faraday cages are used to prevent electromagnetic emissions like wireless signals from leaving the cage. They are generally used in very high-security areas.

Network packets could leave a Faraday cage through a shielded cable.

Hackers and computers could be physically moved outside of a Faraday cage.