Exam Report: 4.3.3 Practice Questions

Date: 1/20/2020 8:39:39 am
Time Spent: 4:37

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 20%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

An attacker is using an eavesdropping technique called Van Eck phreaking on a networking closet.

Which of the following describes what the attacker is doing?

- Connecting to an open switch port
- ~~Connecting to an open Ethernet port~~
- Capturing data transmissions
- Collecting electronic emissions

Explanation

Attackers who collect electronic emissions coming from your networking closet are using an eavesdropping technique called Van Eck phreaking. A Faraday cage can be used to prevent this type of attack.

References

LabSim for Security Pro, Section 4.3.
[All Questions SecPro2017_v6.exm PHYS_NET_02]

Question 2: Correct

One of the ways attackers can access unencrypted data being transmitted on your network is by collecting electronic emissions that come from your networking closet or Ethernet cables.

Which of the following solutions could bog down the infrastructure?

- Employing a protective distribution system, or PDS
- Use Ethernet port locking devices
- Place your network closet inside a Faraday cage
- Configure all data transmissions to be encrypted

Explanation

If all data transmissions were encrypted, then there really would be no need to protect against emissions. However, encrypting and decrypting information takes a lot of processing resources. If all communications in a network were encrypted, it could bog down the infrastructure, so you must implement physical protections, such as:

- Placing your network closet inside a Faraday cage
- Employing a protective distribution system, or PDS
- Using Ethernet port locking devices

References

LabSim for Security Pro, Section 4.3.
[All Questions SecPro2017_v6.exm PHYS_NET_03||/]

Question 3: Incorrect

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 and prevent anyone from reconfiguring the network to set up remote access or backdoor access.

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

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

Explanation

Placing your networking equipment in a locked cage that is inside a locked room that 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, which requires the use of a Faraday cage.

References

LabSim for Security Pro, Section 4.3.
[All Questions SecPro2017_v6.exm PHYS_NET_01]

Question 4: Incorrect

To keep your data center safe, you have done the following:

- Restricted physical access to employees who strictly need to get in the data center.
- Required employees to enter a password using a pin pad to enter the data center.
- Deployed a Faraday cage to keep sensitive network devices safe from external electrical fields.

Which of the following measures will NOT improve physical security in the data center?

- ( ) Implement a checkout policy.
- (•) ~~Grant employee access to hardware on a need to know basis.~~
- ( ) Set up video surveillance in the data center.
- ( ) Place all servers in secured cabinets.

Explanation

A checkout policy ensures that company-owned hardware does not leave the organization's premises without a manager's approval, but hardware in a data center should never be allowed to leave the building.

References

LabSim for Security Pro, Section 4.3.
[All Questions SecPro2017_v6.exm PHYS_NET_05]

Question 5: Incorrect

Physical security is an obvious requirement for network security, but it is often easy to overlook or forget to plan for it.

Which of the following is NOT a benefit of physical security?

- ~~Untrained employees cannot misuse equipment.~~
- Network resources are safer from natural disasters.
- Terrorists cannot walk in off the street and change the network configuration.
- Sensitive data is protected from unauthorized access.
- Employee passwords are stronger.

Explanation

Physical security does NOT entail training employees to use strong passwords. Strong passwords are implemented by establishing security policies and awareness training.

Physical security can protect a network from misuses of equipment by untrained employees or contractors. It can also protect the network from hackers, competitors, and terrorists walking in off the street and changing equipment configurations. Physical security can also protect resources from natural disasters such as floods, fires, storms, and earthquakes. Depending on your particular network design customer, physical security should be installed to protect core routers, demarcation points, cabling, modems, servers, hosts, backup storage, and so on. Because physical security is such an obvious requirement, it is easy to forget to plan for it, but it should never be overlooked or considered less important than other security mechanisms.

References

LabSim for Security Pro, Section 4.3.
[All Questions SecPro2017_v6.exm PHYS_NET_04]