Exam Report: 6.1.3 Practice Questions

Date: 1/21/2020 3:42:15 pm
Time Spent: 3:32

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 60%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

You notice that over the last few months more and more static systems, such as the office environment control system, the security system, and lighting controls, are connecting to your network. You know that these devices can be a security threat.

Which of the following measures can you take to minimize the damage these devices can cause if they are compromised?

- Create a VLAN to use as a medium-trust network zone for these static systems to connect to.
- Create a VLAN to use as a low-trust network zone for these static systems to connect to.
- ~~Create a VLAN to use as a high-trust network zone for these static systems to connect to.~~
- Create a VLAN to use as a no-trust network zone for these static systems to connect to.

Explanation

If your network has static systems, such as IoT devices, then you probably want to have them on their own network segment. This minimizes the damage they can cause to a single network segment and makes identifying issues with them much easier. The most common way to segment networks is to create VLANs for each network zone. You do have some control over static systems, but very little, so they would best be placed in a low-trust zone.

The internet would be classified as a no-trust zone, since you have no control over it.

References

LabSim for Security Pro, Section 6.1.
[All Questions SecPro2017_v6.exm NET_THREATS_01]

Question 2: Correct

Your network devices are categorized into the following zone types:

- No-trust zone
- Low-trust zone
- Medium-trust zone
- High-trust zone

Your network architecture employs multiple VLANs for each of these network zones. Each zone is separated by a firewall that ensures only specific traffic is allowed.

Which of the following is the secure architecture concept that is being used on this network?

- Network firewalling
- Virtual local area networking
- Trust zone networking

Network segmentation

Explanation

The secure network architecture concept that is being used in this example is network segmentation. The most common way to segment networks is to create multiple VLANs for each network zone. These zones can also be separated by firewalls to ensure only specific traffic is allowed. One way to segment a network is to categorize systems into different zones (for example, a no-trust zone, low-trust zone, medium-trust zone, high-trust zone, and highest-trust zone).

References

LabSim for Security Pro, Section 6.1.
[All Questions SecPro2017_v6.exm NET_THREATS_02]

Question 3: Correct

Drag the network attack technique on the left to the appropriate description or example on the right. (Each technique may be used once, more than once, or not at all.)

Perpetrators attempt to compromise or affect the operations of a system.

Active attack

Unauthorized individuals try to breach a network from off-site.

External attack

Attempting to find the root password on a web server by brute force.

Active attack

Attempting to gather information without affecting the flow of information on the network.

Passive attack

Sniffing network packets or performing a port scan.

Passive attack

Explanation

Network attacks are classified as follows:

- **Active attack**: Active attacks are when perpetrators attempt to compromise or affect the operations of a system in some way. For example, trying to brute force the root password on a web server is considered an active attack. A distributed denial of service (DDoS) attack is also an active attack.
- **Passive attack**: Passive attacks occur when perpetrators attempt to gather information without affecting the flow of that information on the network. Packet sniffing and port scanning are passive attacks.
- **External attack**: External attacks are when unauthorized individuals try to breach a network from off-site. Remember that perpetrators of external attacks are unauthorized for any level of access to the network.
- **Inside attack**: Inside attacks are initiated by authorized individuals inside the network's security perimeter who attempt to access systems or resources to which they're not authorized. For example, an inside attack is a disgruntled employee accessing unauthorized company documents and leaking them to the public.

References

LabSim for Security Pro, Section 6.1.
[All Questions SecPro2017_v6.exm NET_THREATS_03]

Question 4: Correct

Your organization has started receiving phishing emails. You suspect that an attacker is attempting to find an employee workstation they can compromise. You know that a workstation can be used as a pivot point to gain access to more sensitive systems.

Which of the following is the most important aspect of maintaining network security against this type of attack?

Network segmentation

Identifying a network baseline

User education and training

Documenting all network assets in your organization

Identifying inherent vulnerabilities

Explanation

User education and training is the most important aspect of maintaining network security against an email phishing attack.

References

LabSim for Security Pro, Section 6.1.
[All Questions SecPro2017_v6.exm NET_THREATS_04]

Question 5: Incorrect

As a security professional, you need to understand your network on multiple levels. You should focus on the following areas:

- Entry points
- Inherent vulnerabilities
- Documentation
- Network baseline

Drag the area of focus on the left to the appropriate example on the right. (Areas of focus may be used once, more than once, or not at all.)

IoT and SCADA devices.

~~Entry points~~ Inherent vulnerabilities

Used to identify a weak network architecture or design.

Documentation

Public-facing servers, workstations, Wi-Fi networks, and personal devices.

Entry points

An older version of Windows that is used for a particular application.

~~Documentation~~ Inherent vulnerabilities

What activity looks like in normal day-to-day usage.

Network baseline

Explanation

As a security professional, you need to understand your network on multiple levels. You should focus on the following:

- **Entry points**: Recognize all vulnerabilities and entry points for possible attacks. This includes public-facing servers, workstations, Wi-Fi networks, and personal devices. Primarily, you must account for anything that connects to the network as a possible entry point.
- **Inherent vulnerabilities**: Identify inherent vulnerabilities or systems that lack proper security controls.
  For example, if your organization needs to use an older version of Windows for a particular application, then you need to identify that system as a vulnerability. IoT and SCADA devices are both systems that lack proper security controls, and therefore must be dealt with appropriately.
- **Documentation**: Document all network assets in your organization and create a suitable network diagram that you can use as a reference. This is probably one of the most important components of knowing your system. If you don't know the underlying infrastructure of your network, then you can't adequately secure it. Proper network documentation and diagrams will not only help you identify a

weak network architecture or design, but it will also protect against system sprawl and unknown systems.

- **Network baseline**: You need to know your systems' normal activity such as its regular traffic patterns, data usage, network activity, server load, et cetera. Mainly, you need to know what your network looks like in normal day-to-day usage. Knowing this allows you to identify unusual or atypical activity that can indicate an attack in progress or a compromised network. To identify a network baseline, you can use network tools that monitor network traffic and create a graphical representation of the collected data, such as Cisco's NetFlow tool.

References

LabSim for Security Pro, Section 6.1.
[All Questions SecPro2017_v6.exm NET_THREATS_05]