Exam Report: 5.4.5 Practice Questions

Date: 1/20/2020 7:55:43 pm
Time Spent: 3:48

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 100%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You have a company network that is connected to the internet. You want all users to have internet access, but you need to protect your private network and users. You also need to make a web server publicly available to internet users.

Which solution should you use?

- Use a single firewall. Put the web server and the private network behind the firewall.
- Use firewalls to create a DMZ. Place the web server inside the DMZ and the private network behind the DMZ.
- Use firewalls to create a DMZ. Place the web server and the private network inside the DMZ.
- Use a single firewall. Put the web server in front of the firewall and the private network behind the firewall.

Explanation

A *demilitarized zone* (DMZ), also called a *screened subnet*, is a buffer network (or subnet) that sits between the private network and an untrusted network (such as the internet). A common configuration uses two firewalls, one connected to the public network and one connected to the private network. Publicly-accessible resources (servers) are placed inside the screened subnet. Examples of publicly-accessible resources include web, FTP, or email servers. Private resources that are not accessible from the internet are placed behind the DMZ (behind the inner firewall).

Placing the web server inside the private network would mean opening ports in the firewall leading to the private network, which could expose other devices to attack. Placing the web server outside of the firewall would leave it unprotected.

References

LabSim for Security Pro, Section 5.4.
[All Questions SecPro2017_v6.exm DMZ_01]

Question 2: Correct

You have used firewalls to create a demilitarized zone. You have a web server that needs to be accessible to internet users. The web server must communicate with a database server for retrieving product, customer, and order information.

How should you place devices on the network to best protect the servers? (Select two.)

- [x] Put the web server inside the DMZ.
- [ ] Put the web server on the private network.
- [ ] Put the database server inside the DMZ.
- [x] Put the database server on the private network.

Explanation

Publicly-accessible resources (servers) are placed inside the DMZ. Examples of publicly-accessible resources include web, FTP, or email servers. Devices that should not be accessible to public users are placed on the private network. If you have a public server that communicates with another server, such as a database server, and that server should not have direct contact with public hosts, place the server on the private network and allow only traffic from the public server to cross the inner firewall.

References

LabSim for Security Pro, Section 5.4.
[All Questions SecPro2017_v6.exm DMZ_02]

Question 3: Correct

Of the following security zones, which one can serve as a buffer network between a private secured network and the untrusted internet?

- Padded cell
- Intranet
- Extranet
- DMZ

Explanation

A DMZ or demilitarized zone is a network placed between a private secured network and the untrusted internet to grant external users access to internally controlled services. The DMZ serves as a buffer network.

An intranet is a private network that happens to employ internet information services. An extranet is a division of a private network that is accessible to a limited number of users, such as business partners, suppliers, and certain customers. A padded cell is an intrusion detection countermeasure used to delay intruders sufficiently to record meaningful information about them for discovery and prosecution.

References

LabSim for Security Pro, Section 5.4.
[All Questions SecPro2017_v6.exm DMZ_03]

Question 4: Correct

Which of the following is likely to be located in a DMZ?

- Domain controller
- FTP server
- Backup server
- User workstations

Explanation

An FTP server is the most likely component from this list to be located in a DMZ (demilitarized zone) or a buffer subnet. A DMZ should only contain servers that are to be accessed by external visitors. Often, it is assumed that any server placed in the DMZ will be compromised. Therefore, no mission-critical or sensitive systems are located in a DMZ.

A domain controller may appear in a DMZ when the DMZ is an entire isolated domain, but this is not common. User workstations are never located in a DMZ. Backup servers, unless specifically deployed for the DMZ only, are never located in a DMZ.

References

LabSim for Security Pro, Section 5.4.
[All Questions SecPro2017_v6.exm DMZ_04]

Question 5: Correct

In which of the following situations would you most likely implement a demilitarized zone (DMZ)?

- [x] You want to protect a public web server from attack.
- [ ] You want internet users to see a single IP address when accessing your company network.
- [ ] You want to encrypt data sent between two hosts using the internet.
- [ ] You want to detect and respond to attacks in real time.

Explanation

Use a demilitarized zone (DMZ) to protect public hosts on the internet, such as a web server, from attack. The DMZ uses an outer firewall that prevents internet attacks. Inside the DMZ are all publicly-accessible hosts. A second firewall protects the private network from the internet.

Use a Virtual Private Network (VPN) to encrypt data between two hosts on the Internet. Use Network Address Translation (NAT) to hide internal IP addresses from the internet. Use an Intrusion Prevention System (IPS) to detect and respond to threats in real time.

References

LabSim for Security Pro, Section 5.4.
[All Questions SecPro2017_v6.exm DMZ_05]

Question 6: Correct

Which of the following terms describes a network device that is exposed to attacks and has been hardened against those attacks?

- [ ] Multi-homed
- [ ] Kernel proxy
- [x] Bastion or sacrificial host
- [ ] Circuit proxy

Explanation

A bastion or sacrificial host is one that is unprotected by a firewall. The term *bastion host* is used to describe any device fortified against attack (such as a firewall). A *sacrificial host* might be a device intentionally exposed to attack, such as a honeypot.

Circuit proxy and kernel proxy are types of firewall devices. Multi-homed describes a device with multiple network interface cards.

References

LabSim for Security Pro, Section 5.4.
[All Questions SecPro2017_v6.exm DMZ_06]