Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/22/2022 8:46:07 pm • Time spent: 01:32

Score: 90%

Passing Score: 80%

Question 1: ✔ Correct

Where should an organization's web server be placed?

- DMZ
- Intranet
- Honeynet
- Extranet

EXPLANATION

A web server should be placed in the demilitarized zone (DMZ). The DMZ is a network that contains publicly accessible resources. The DMZ is located between the private network and an untrusted network (such as the internet) and is protected by a firewall.

An intranet is a private network (LAN) that employs internet information services for internal use only. Since a website should be publicly available, its server should not be placed on the intranet.

An extranet is a privately controlled network that is distinct from the intranet. An extranet is located between the internet and a private LAN. An extranet is often used to grant resource access to business partners, suppliers, and even customers outside of an organization. The web server shouldn't be placed here.

A honeynet is a special network created to trap potential attackers. A web server would not be placed in a honeynet.

REFERENCES

3.1.1 Physical Security

3.1.2 Physical Security Facts

3.1.3 Implement Physical Security

3.2.4 Physical Network Protection Facts

5.2.4 DMZ Facts

q_sec_zone_dmz_secp7.question.fex

Question 2: ✔ Correct

Which of the following is a privately controlled portion of a network that is accessible to some specific external entities?

- Extranet
- MAN
- Internet
- Intranet

EXPLANATION

An extranet is a privately controlled portion of a network that is accessible to some specific external entities. Often, those external entities are business partners, suppliers, distributors, vendors, or customers.

An intranet is a LAN that employs the technology of the internet (namely, TCP/IP, web servers, and email).

The internet is the global TCP/IP-based network that supports most web and email communications.

A metropolitan area network (MAN) is a LAN that is spread across several city blocks, across a business park, or across a campus.

REFERENCES

5.1.3 Security Zone Facts

q_sec_zone_extranet_secp7.question.fex

Question 3: ✔ Correct

You want to create a collection of computers on your network that appear to have valuable data but actually store fake data that could entice a potential intruder. Once the intruder connects, you want to be able to observe and gather information about the attacker's methods.

Which feature should you implement?

- NIPS
- NIDS
- Honeynet
- Extranet

EXPLANATION

A honeypot is a device or virtual machine that entices intruders by displaying a vulnerable trait or flaw or by appearing to contain valuable data. A honeynet is a network of honeypots.

A network-based IDS (NIDS) is a dedicated device installed on a network that's used to analyze all traffic on the network. An NIPS is a network-based intrusion prevention system that can take actions in response to intrusion.

An extranet is a privately controlled network located between the internet and a private LAN, but distinct from both. An extranet is often used to grant resource access to business partners, suppliers, and even customers outside of the organization.

REFERENCES

5.1.3 Security Zone Facts

q_sec_zone_honeynet_secp7.question.fex

Question 4: ✔ Correct

A honeypot is used for which purpose?

- To entrap intruders
- To disable an intruder's system
- To prevent sensitive data from being accessed
- ➡ To delay intruders in order to gather auditing data

EXPLANATION

A honeypot is used to delay intruders in order to gather auditing data. A honeypot is a fake network or system that hosts false information but responds as a real system should. Honeypots usually entice intruders to spend considerable time on the system and allow extensive logging of the intruder's activities. A honeypot often allows companies to discover and even prosecute intruders.

Honeypots should not be used to entrap intruders. Entrapment is an illegal activity. Honeypots are not direct countermeasures to preventing unwanted access. Rather, they are an enticement to prevent intruders from getting into the private network in the first place. Honeypots rarely take offensive action against intruders. They may prevent malicious activities from being launched by an intruder, but they do not direct attacks at him or her.

REFERENCES

5.1.3 Security Zone Facts

q_sec_zone_honeypot_secp7.question.fex

Question 5: ✔ Correct

Which of the following devices can apply quality of service and traffic-shaping rules based on what created the network traffic?

- Proxy server
- Network access control
- Application-aware devices
- All-in-one security appliances

EXPLANATION

An application-aware device can analyze and manage network traffic based on the Application layer protocol that created it. Some of these devices can also apply quality of service (QoS) and traffic-shaping rules based on the application that created network traffic.

All-in-one security appliances combine many security functions into a single device. All-in-one security appliances are also known as unified threat security devices or web security gateways.

Network access control (NAC) controls access to the network by not allowing computers to access network resources unless they meet certain predefined security requirements.

A proxy server is a type of firewall that stands as an intermediary between clients requesting resources from other servers.

REFERENCES

5.1.3 Security Zone Facts

q_sec_zone_qos_secp7.question.fex

Question 6: ✔ Correct

You are the office manager of a small financial credit business. Your company handles personal financial information for clients seeking small loans over the internet. You are aware of your obligation to secure clients records, but the budget is an issue for your company.

Which item would provide the BEST security for this situation?

- Network access control system
- Proxy server with access controls
- All-in-one security appliance
- Firewall on your gateway server to the internet

EXPLANATION

An all-in-one security appliance would provide the best overall protection. All-in-one security appliances take up the least amount of space and require the least amount of technical assistance for setup and maintenance.

Security functions in an all-in-one security appliance can include the following:

- Spam filter
- URL filter
- Web content filter
- Malware inspection
- Intrusion detection system (IDS)

In addition to security functions, all-in-one security appliances can include the following:

- Network switch
- Router
- Firewall
- Tx uplink (integrated CSU/DSU)
- Bandwidth shaping

REFERENCES

5.1.5 Security Solution Facts

q_sec_sol_appliance_secp7.question.fex

Question 7: ✔ Correct

You are implementing security at a local high school that is concerned with students accessing inappropriate material on the internet from the library's computers. The students use the computers to search the internet for research paper content. The school budget is limited.

Which content filtering option would you choose?

- ➡ Restrict content based on content categories.
- Block specific DNS domain names.
- Block all content except for content you have identified as permissible.
- Allow all content except for the content you have identified as restricted.

EXPLANATION

Restricting content based on categories would provide the most protection with the least amount of research and involvement.

All other options require research to identify specific content or websites, which could allow access to undesirable websites or prevent access to necessary websites.

REFERENCES

5.1.5 Security Solution Facts

q_sec_sol_content_secp7.question.fex

Question 8: ✔ Correct

Which of the following BEST describes a honeyfile?

- ➡ A single file setup to entice and trap attackers.
- A file that has been digitally signed.
- A file used to authenticate.
- A default file in the /etc/security directory.

EXPLANATION

A honeyfile is a single file setup to entice and trap attackers and to figure out what they're trying to do.

A token is a device or a file used to authenticate.

A honeyfile could be placed in the /etc/security directory. The file would not be a default file in the directory.

A digitally signed file is like putting a lock on the document.

REFERENCES

5.1.5 Security Solution Facts

q_sec_sol_honey_files_secp7.question.fex

Question 9: ✔ Correct

Members of the sales team use laptops to connect to the company network. While traveling, they connect their laptops to the internet through airport and hotel networks.

You are concerned that these computers could pick up viruses that could spread to your private network. You would like to implement a solution that prevents the laptops from connecting to your network unless antivirus software and the latest operating system patches are installed.

Which solution should you use?

- NAC
- VLAN
- DMZ
- NIDS

EXPLANATION

Network access control (NAC) controls access to a network by not allowing computers to access network resources unless they meet certain predefined security requirements. Conditions that can be part of the connection requirements include requiring that computers have:

- Antivirus software with up-to-date definition files
- An active personal firewall
- Specific operating system critical updates and patches

A client that is determined healthy by the NAC is given access to the network. An unhealthy client, who has not met all the checklist requirements, is either denied access or can be given restricted access to a remediation network, where remediation servers can be contacted to help the client to become compliant.

A demilitarized zone (DMZ) is a buffer network (or subnet) that sits between a private network and an untrusted network (such as the internet). A virtual LAN (VLAN) is a logical grouping of computers based on switch port. VLAN membership is configured by assigning a switch port to a VLAN. An intrusion detection system (IDS) is a special network device that can detect attacks and suspicious activity. A network-based IDS (NIDS) scans network traffic looking for intrusion attempts.

REFERENCES

5.1.5 Security Solution Facts

q_sec_sol_nac_secp7.question.fex

Question 10: ✕ Incorrect

A proxy server can be configured to do which of the following?

- Act as a unified threat security device or web security gateway.
- ➡ Restrict users on the inside of a network from getting out to the internet.
- Allow all content except for the content you have identified as restricted.
- ~~Block all content except for the content you have identified as permissible.~~

EXPLANATION

Proxies can be configured to:

- Restrict users on the inside of a network from getting out to the internet.
- Restrict access by user or by specific website.
- Restrict users from using certain protocols.
- Use access controls to control inbound or outbound traffic.
- Shield or hide a private network to provide online anonymity and make it more difficult to track web surfing behavior.
- Cache heavily accessed web content to improve performance.

An internet content filter is software used to monitor and restrict content delivered across the web to an end user. Two types of configurations are commonly used, which are:

- Allow all content except for the content you have identified as restricted.
- Block all content except for the content you have identified as permissible.

All-in-one security appliances combine many security functions into a single device. All-in-one security appliances are also known as unified threat security devices or web security gateways.

REFERENCES

5.1.5 Security Solution Facts

q_sec_sol_proxy_secp7.question.fex