Exam Report: 5.3.8 Practice Questions

Date: 4/1/21 2:21:20 am
Time Spent: 5:22

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 80%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

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

○ Intranet

➡ ● Extranet

○ MAN

○ Internet

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

References

LabSim for Security Pro, Section 5.3.
[All Questions SecPro2017_v6.exm SEC_APPLIANCE_01]

Question 2: 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. Budget is an issue for your company.

Which item would provide the best security for this situation?

○ Network Access Control system

➡ ● All-in-one security appliance

○ Proxy server with access controls

○ Firewall on your gateway server to the Internet

Explanation

An all-in-one security appliance would provide the best overall protection. The all-in-one security appliance takes up the least amount of space and requires 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

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

LabSim for Security Pro, Section 5.3.
[All Questions SecPro2017_v6.exm SEC_APPLIANCE_02]

▼ **Question 3:** 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 will use the computers to search the internet for research paper content. The school budget is limited.

Which content filtering option would you choose?

○ Block specific DNS domain names

○ Block all content except for content you have identified as permitted

➡ ● Restrict content based on content categories

○ 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

LabSim for Security Pro, Section 5.3.
[All Questions SecPro2017_v6.exm SEC_APPLIANCE_03]

▼ **Question 4:** Correct

Match the application-aware network device on the right with the appropriate description on the left. Each description may be used once, more than once, or not at all.

Application-aware proxy

✓ Improves application performance

Application-aware firewall

✓ Enforces security rules based on the application that is generating network traffic instead of the traditional port and protocol

Application-aware IDS

✓ Analyzes network packets to detect malicious payloads targeted at application-layer services

Explanation

An application-aware device has the ability to analyze and manage network traffic based on the application-layer protocol that created it. Examples include the following:

- An *application-aware firewall* can enforce security rules based on the application that is generating network traffic instead of the traditional port and protocol.

- An *application-aware IDS* or *IPS* can analyze network packets to detect malicious payloads targeted at application-layer services (such as a web server).
- An *application-aware proxy* manages traffic based on the application-layer protocol(s) it supports, such as FTP or HTTP. This allows an application-aware proxy to prevent the application client from performing undesirable actions. It can also improve application performance. For example, an HTTP proxy can be configured to cache frequently-accessed web pages.

A network access control (NAC) solution defines security measures that must be in place for a computer requesting access to the network.

References

LabSim for Security Pro, Section 5.3.
[All Questions SecPro2017_v6.exm SEC_APPLIANCE_04]

▼ **Question 5:** Incorrect

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 will 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 anti-virus software and the latest operating system patches are installed.

Which solution should you use?

○ VLAN

○ NIDS

➡ ○ NAC

○ NAT

● ~~DMZ~~

Explanation

Network Access Control (NAC) controls access to the 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:

- Anti-virus 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 the 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.

Network Address Translation (NAT) modifies the IP addresses in packets as they travel from one network (such as a private network) to another (such as the internet). NAT allows you to connect a private network to the internet without obtaining registered addresses for every host. Hosts on the private network share the registered IP addresses.

References

LabSim for Security Pro, Section 5.3.
[All Questions SecPro2017_v6.exm SEC_APPLIANCE_05]