Exam Report: 5.7.8 Practice Questions

Date: 1/21/2020 9:47:41 am
Time Spent: 12:18

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

A group of salesmen would like to access your private network through the internet while they are traveling. You want to control access to the private network through a single server.

Which solution should you implement?

- IDS
- IPS
- DMZ
- VPN concentrator
- RADIUS

Explanation

With a *remote access* VPN, a server on the edge of a network (called a VPN *concentrator*) is configured to accept VPN connections from individual hosts. Hosts that are allowed to connect using the VPN connection are granted access to resources on the VPN server or the private network.

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 RADIUS server is used to centralize authentication, authorization, and accounting for multiple remote access servers. However, clients still connect to individual remote access servers.

An intrusion detection system (IDS) is a special network device that can detect attacks and suspicious activity. A *passive* IDS monitors, logs, and detects security breaches, but takes no action to stop or prevent the attack. An *active* IDS (also called an *intrusion protection system* or IPS) performs the functions of an IDS, but can also *react* when security breaches occur.

References

LabSim for Security Pro, Section 5.7.
[All Questions SecPro2017_v6.exm VPN_01]

Question 2: Correct

A VPN is primarily used for what purpose?

- Allow the use of network-attached printers
- Allow remote systems to save on long-distance charges
- Support the distribution of public web documents
- Support secured communications over an untrusted network

Explanation

A VPN (Virtual Private Network) is used primarily to support secured communications over an untrusted network. A VPN can be used over a local area network, across a WAN connection, over the internet, and even between a client and a server over a dial-up internet connection. All of the other items listed in this question are benefits or capabilities that are secondary to this primary purpose.

References

LabSim for Security Pro, Section 5.7.
[All Questions SecPro2017_v6.exm VPN_02]

Question 3: Correct

Which VPN protocol typically employs IPSec as its data encryption mechanism?

- L2F
- PPP
- L2TP
- PPTP

Explanation

L2TP (Layer 2 Tunneling Protocol) is the VPN protocol that typically employs IPSec as its data encryption mechanism. L2TP is the recommended VPN protocol to use on dial-up VPN connections.

PPTP and PPP only support CHAP and PAP for data encryption. L2F offers no data encryption.

References

LabSim for Security Pro, Section 5.7.
[All Questions SecPro2017_v6.exm VPN_03]

Question 4: Correct

Which statement best describes IPSec when used in tunnel mode?

- The identities of the communicating parties are not protected
- Packets are routed using the original headers, and only the payload is encrypted
- IPSec in tunnel mode may not be used for WAN traffic
- The entire data packet, including headers, is encapsulated

Explanation

When using IPSec in tunnel mode, the entire data packet, including original headers, is encapsulated. New encrypted packets are created with headers indicating only the endpoint addresses. Tunneling protects the identities of the communicating parties and original packet contents. Tunneling is frequently used to secure traffic traveling across insecure public channels, such as the internet. IPSec in tunnel mode is the most common configuration for gateway-to-gateway communications.

In transport mode, routing is performed using the original headers; only the packet's payload is encrypted. Transport mode is primarily used in direct host-to-host communication outside of a dedicated IPSec gateway/firewall configuration.

References

LabSim for Security Pro, Section 5.7.
[All Questions SecPro2017_v6.exm VPN_04]

Question 5: Incorrect

Which IPSec subprotocol provides data encryption?

- ~~SSL~~
- AES
- AH

ESP

Explanation

The Encapsulating Security Payload (ESP) protocol provides data encryption for IPSec traffic.

The Authentication Header (AH) provides message integrity through authentication, verifying that data is received unaltered from the trusted destination. AH provides no privacy and is often combined with ESP to achieve integrity and confidentiality.

References

LabSim for Security Pro, Section 5.7.
[All Questions SecPro2017_v6.exm VPN_05]

Question 6: Incorrect

Which is the best countermeasure for someone attempting to view your network traffic?

- IPS
- Firewall
- Antivirus software
- ~~Access lists~~
- VPN

Explanation

Some form of encryption, such as a Virtual Private Network (VPN), is the best defense against someone viewing your network traffic. Capturing and viewing your network traffic is called *sniffing*.

Sniffing is a passive activity and does not result in traffic being generated. Rather it captures existing packets on the network. For this reason, you cannot detect or prevent sniffing using methods that examine network traffic, such as a firewall, access list, or Intrusion Prevention System (IPS). Use antivirus software to scan software for malicious code.

References

LabSim for Security Pro, Section 5.7.
[All Questions SecPro2017_v6.exm VPN_06]

Question 7: Correct

PPTP (Point-to-Point Tunneling Protocol) is quickly becoming obsolete because of which VPN protocol?

- TACACS (Terminal Access Controller Access Control System)
- L2F (Layer 2 Forwarding Protocol)
- SLIP (Serial Line Interface Protocol)
- L2TP (Layer 2 Tunneling Protocol)

Explanation

PPTP (Point-to-Point Tunneling Protocol) is quickly becoming obsolete because of L2TP (Layer 2 Tunneling Protocol). L2TP was created by combining PPTP and L2F and adding in support for IPSec. The result is a very versatile, nearly universally interoperable VPN protocol that provides solid authentication and reliable data encryption.

References

LabSim for Security Pro, Section 5.7.
[All Questions SecPro2017_v6.exm VPN_07]

Question 8: Correct

What is the primary use of tunneling?

- Improving communication throughput
- Supporting private traffic through a public communication medium
- Deploying thin clients on a network
- Protecting passwords

Explanation

Tunneling is used primarily to support private traffic through a public communication medium. The most widely known form of tunneling is VPN (Virtual Private Networking). A VPN establishes a secured communications tunnel through an insecure network connecting two systems.

Tunnels are not directly associated with password theft or protection. Tunnels provide secure communications. They usually provide less-than-optimal throughput due to the additional overhead of encryption and maintaining the communications link. Terminal services or similar products are used to support thin clients, dumb terminals, or remote sessions.

References

LabSim for Security Pro, Section 5.7.
[All Questions SecPro2017_v6.exm VPN_08]

Question 9: Correct

In addition to Authentication Header (AH), IPSec is comprised of what other service?

- Encapsulating Security Payload (ESP)
- Advanced Encryption Standard (AES)
- Extended Authentication Protocol (EAP)
- Encryption File System (EFS)

Explanation

IPSec is comprised of two services. One service is named Authentication Header (AH), and the other named Encapsulating Security Payload (ESP). AH is used primarily for authenticating the two communication partners of an IPSec link. ESP is used primarily to encrypt and secure the data transferred between IPSec partners. IPSec employs ISAKMP for encryption key management.

References

LabSim for Security Pro, Section 5.7.
[All Questions SecPro2017_v6.exm VPN_09]

Question 10: Correct

A salesperson in your organization spends most of her time traveling between customer sites. After a customer visit, she must complete various managerial tasks, such as updating your organization's order database.

Because she rarely comes back to your home office, she usually accesses the network from her notebook computer using Wi-Fi access provided by hotels, restaurants, and airports.

Many of these locations provide unencrypted public Wi-Fi access, and you are concerned that sensitive data could be exposed. To remedy this situation, you decide to configure her notebook to use a VPN when accessing the home network over an open wireless connection.

Which key steps should you take when implementing this configuration? (Select two.)

- [x] Configure the VPN connection to use IPsec
- [ ] Configure the VPN connection to use PPTP
- [x] Configure the browser to send HTTPS requests through the VPN connection
- [ ]

- [ ] Configure the browser to send HTTPS requests directly to the Wi-Fi network **without** going through the VPN connection
- [ ] Configure the VPN connection to use MS-CHAPv2

Explanation

It is generally considered acceptable to use a VPN connection to securely transfer data over an open Wi-Fi network. As long as strong tunneling ciphers and protocols are used, the VPN provides sufficient encryption to secure the connection, even though the wireless network itself is not encrypted. It is recommended that you use IPsec or SSL to secure the VPN, as these protocols are relatively secure. You should also configure the browser's HTTPS requests to go through the VPN connection. To conserve VPN bandwidth and improve latency, many VPN solutions automatically reroute web browsing traffic through the client's default network connection instead of through the VPN tunnel. This behavior would result in HTTP/HTTPS traffic being transmitted over the unsecure open wireless network instead of though the secure VPN tunnel.

Avoid using PPTP with MS-CHAPv2 in a VPN over open wireless configuration, as these protocols are no longer considered secure.

References

LabSim for Security Pro, Section 5.7.
[All Questions SecPro2017_v6.exm VPN_10]