Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/4/2022 7:11:04 pm • Time spent: 03:36

Score: 70% Passing Score: 80%

Question 1: ✓ Correct

As a network administrator, you are asked to recommend a secure method for transferring data between hosts on a network. Which of the following protocols would you recommend? (Select two.)

- □ TDP
- ➡ ☑ SFTP
- □ RCP
- ➡ ☑ SCP
- □ FTP

EXPLANATION

The Secure File Transfer Protocol (SFTP) is a file transfer protocol that uses Secure Shell (SSH) to secure data transfers. SSH ensures that SFTP transmissions use encrypted commands and data, which prevents data from being transmitted over the network in cleartext. The Secure Copy (SCP) protocol is associated with Unix/Linux networks and is used to transfer files between systems. Like SFTP, SCP relies on SSH to ensure that data and passwords are not transmitted over the network in clear text.

The Remote Copy Protocol (RCP) and the File Transfer Protocol (FTP) are used to transfer files between computers. However, both are unsecure protocols and transmit data over the network in cleartext. Data and passwords sent over the network in clear text are in danger of being tampered with or read during transmission, making them inappropriate for many network applications.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_ftps_02_secp7.question.fex

Question 2: ✓ Correct

Which of the following protocols uses port 443?

- ➡ ● HTTPS
- ○ S/MIME
- ○ SSH
- ○ S-HTTP

EXPLANATION

Hyper Text Transfer Protocol Secure (HTTPS) is a secure form of HTTP that uses either SSL or TLS to encrypt sensitive data before it is transmitted. HTTPS uses port 443.

Secure Hypertext Transfer Protocol (S-HTTP) supports a wide variety of encryption methods, but it does not use port 443. SSH uses port 22. S/MIME is a method for encrypting emails. S/MIME does not communicate over a specific port number.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_https_01_secp7.question.fex

Question 3: ✓ Correct

Which TCP/IP protocol is a secure form of HTTP that uses SSL as a sub-layer for security?

- ○ DNS
- ○ SMTP
- ○ SSH
- ➡ ● HTTPS

EXPLANATION

HTTPS is a secure form of HTTP that uses SSL as a sub-layer for security.

SMTP is used to route electronic mail through the internetwork.

SSH allows secure interactive control of remote systems.

DNS is a system that is distributed throughout the internetwork to provide address/name resolution.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_https_02_secp7.question.fex

Question 4: ✓ Correct

Which of the following tools allow remote management of servers? (Select two.)

- □ POP3
- ➡ ☑ Telnet
- ➡ ☑ SSH
- □ FTP
- □ SSL

EXPLANATION

Both Telnet and SSH are tools for remote server management.

POP3 is for retrieving email from a remote server, and FTP is for transferring files.

Secure Socket Layer (SSL) secures messages being transmitted on the internet.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_remote_secp7.question.fex

Question 5: ✕ Incorrect

SFTP uses which mechanism to provide security for authentication and data transfer?

○ IPsec

➡ ○ SSH

○ Token devices

● ~~SSL~~

EXPLANATION

SSH File Transfer Protocol uses Secure Shell (SSH) to provide security for authentication and data transfer.

FTPS uses SSL to secure FTP traffic. You can also secure FTP traffic by establishing an IPsec tunnel between the client and the server, but IPsec is established independently of FTP in this case.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_ssh_02_secp7.question.fex

Question 6: ✕ Incorrect

When using SSL authentication, what does the client verify first when checking a server's identity?

○ Master secrets are verifiable from asymmetric keys.

○ All DNS resolution must point to the corporate intranet routers.

● ~~The certificate must be non-expiring and self-signed by the sysadmin.~~

➡ ○ The current date and time must fall within the server's certificate-validity period.

EXPLANATION

An SSL client first checks the server's certificate validity period. The authentication process stops if the current date and time fall outside of the validity period.

SSL clients verify a server's identity using the following steps:

1. The client checks the server's certificate-validity period. The authentication process stops if the current date and time fall outside of the validity period.
2. The client verifies that the issuing certificate authority (CA) is on its list of trusted CAs.
3. The client uses the CA's public key to validate the CA's digital signature on the server certificate. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA.
4. To protect against man-in-the-middle attacks, the client compares the actual DNS name of the server to the DNS name on the certificate.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_ssl_04_secp7.question.fex

▼ Question 7: ✓ Correct

Which of the following protocols are often added to other protocols to provide secure transmission of data? (Select two.)

- ➡ ☑ TLS
- ➡ ☑ SSL
- □ SNMP
- □ HTTPS
- □ SMTP

EXPLANATION

Both Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are protocols that are used with other protocols to add security. In addition, Secure Shell (SSH) can be used to add security when using unsecure protocols.

HTTPS is the secure form of HTTP that uses SSL.

SMTP is used for sending email.

SNMP is a network management protocol.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_ssl_tls_secp7.question.fex

▼ **Question 8:** ✕ Incorrect

Which of the following protocols can TLS use for key exchange? (Select two.)

☑ ~~IKE~~

☐ KEA

➡ ☑ Diffie-Hellman

➡ ☐ RSA

☐ ECC

EXPLANATION

TLS uses Diffie-Hellman or RSA to exchange session keys.

SSL uses RSA or Key Exchange Protocol (KEA) for key exchange. IPsec uses IKE for key exchange. ECC (elliptic curve cryptography) is a method that can be used in key exchange.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_tls_secp7.question.fex

▼ Question 9: ✓ Correct

IPsec is implemented through two separate protocols. What are these protocols called? (Select two.)

- □ L2TP
- ➡ ☑ ESP
- ➡ ☑ AH
- □ SSL
- □ EPS

EXPLANATION

IPsec is implemented through two separate protocols, which are IP Authentication Header and IPsec Encapsulating Security Payload. IPsec AH provides authentication and non-repudiation services to verify that the sender is genuine and data has not been modified in transit. IPsec ESP provides data encryption services for the data within the packet.

IPsec SSL and IPsec EPS are not protocols associated with IPsec.

REFERENCES

10.1.7 IPsec Facts

q_ipsec_ah_esp_01_secp7.question.fex

▼ Question 10: ✓ Correct

What is the primary function of the IKE Protocol used with IPsec?

○ Encrypt packet contents.

○ Provide both authentication and encryption.

○ Ensure dynamic key rotation and select initialization vectors (IVs).

➡ ● Create a security association between communicating partners.

○ Provide authentication services.

EXPLANATION

Internet Key Exchange (IKE) Protocol is used with IPsec to create a security association between communicating partners. It controls the negotiation of encryption methods, identifies how keys are exchanged, and sets up other parameters that control communications.

Encapsulating Security Payload (ESP) provides both authentication and encryption, while Authentication Header (AH) provides authentication only.

REFERENCES

10.1.7 IPsec Facts

q_ipsec_ah_esp_03_secp7.question.fex