

Exam Report: 9.10.9 Practice Questions

Date: 1/28/2020 7:19:44 pm
Time Spent: 2:44

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 67%



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

Which of the following protocols uses port 443?

- ☐ S-HTTP
- ➡ ☒ HTTPS
- ☐ S/MIME
- ☐ SSH

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 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

LabSim for Security Pro, Section 9.10.
[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_01]

▼ Question 2: Correct

You are purchasing a hard disk from an online retailer over the internet. What does your browser use to ensure that others cannot see your credit card number on the internet?

- ☐ VPN
- ☐ IPsec
- ☐ PPTP
- ➡ ☒ SSL

Explanation

Your web browser uses SSL (Secure Sockets Layer) to ensure safe web transactions. URLs that begin with HTTPS:// trigger your web browser to use SSL.

References

LabSim for Security Pro, Section 9.10.
[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_02]

▼ Question 3: Correct

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

☐ SSL ☒ ESP☐ L2TP ☒ AH☐ EPS

Explanation

IPsec is implemented through two separate protocols, 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

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_03]

▼ Question 4: Incorrect

Which of the following network layer protocols provides authentication and encryption services for IP-based network traffic?

☐ L2TP☒ ~~SSL~~ ☐ IPsec☐ TCP

Explanation

IPsec is security implementation that provides security for all other TCP/IP based protocols that operate above the network layer. IPsec provides authentication through a protocol called IPsec Authentication Header (AH) and encryption services through a protocol called IPsec Encapsulating Security Payloads (ESP).

The Transmission Control Protocol (TCP) is a transport layer connection protocol that provides data transmission services. It is not a secure protocol, and it relies on other measures, such as IPsec, to provide security. The Secure Sockets Layer (SSL) is an application/session layer protocol that is designed to secure network traffic from certain other protocols, such as Hypertext Transfer Protocol (HTTP) and Post Office Protocol version 3 (POP3). It does not provide security for protocols lower in the TCP/IP protocol stack, such as TCP and UDP. The Layer 2 Tunneling Protocol (L2TP) is a protocol used to encapsulate Point-to-Point Protocol (PPP) traffic.

References

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_04||/]

▼ Question 5: Correct

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

☐ HTTPS☐ SMTP ☒ SSL

☐ SNMP ☒ TLS

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

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_06]

▼ Question 6: Incorrect

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

- ☐ Provide both authentication and encryption.
-  ☐ Create a security association between communicating partners.
- ☐ Encrypt packet contents.
- ☒ ~~Provide authentication services.~~
- ☐ Ensure dynamic key rotation and select initialization vectors (IVs).

Explanation

The 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

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_07]

▼ Question 7: Incorrect

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

-  ☐ RSA
- ☒ ~~IKE~~
- ☐ KEA
- ☐ ECC
-  ☒ Diffie-Hellman

Explanation

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

SSL uses RSA or the 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

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_08]

▼ Question 8: Correct

Which of the following is a secure alternative to FTP that uses SSL for encryption?

☐ SFTP

☐ SCP

➡ ☒ FTPS

☐ RCP

Explanation

FTP Secure (FTPS) adds SSL or TLS to FTP to secure login credentials and encrypt data transfers. FTPS requires a server certificate.

Secure Shell File Transfer Protocol (SFTP) is a file transfer protocol that uses Secure Shell (SSHv2) to secure data transfers. SFTP is not FTP that uses SSH, but rather a secure transfer protocol that is different from FTP. Secure Copy Protocol (SCP) uses the Secure Shell protocol (SSHv1) to secure file transfers and login credentials. Remote Copy Protocol (RCP) is an unsecured protocol for file transfer.

References

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_10]

▼ Question 9: Correct

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

➡ ☒ SSH

☐ FTP

☐ POP3

➡ ☒ Telnet

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.

References

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_11]

▼ Question 10: Correct

Which protocol does HTTPS use to offer greater security in web transactions?

➡ ☒ SSL

☐ Kerberos

☐ User name and password authentication

☐ IPsec

Explanation

HTTPS uses Secure Sockets Layer (SSL) to offer greater security in web transactions.

Kerberos allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. IPsec (IP security) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream.

References

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_12]

▼ Question 11: Correct

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

➡ ☒ HTTPS

☐ SMTP

☐ SSH

☐ DNS

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 for secure interactive control of remote systems. DNS is a system that is distributed throughout the internetwork to provide address/name resolution.

References

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_13]

▼ Question 12: Correct

Telnet is inherently insecure because its communications is in plaintext and easily intercepted. Which of the following is an acceptable alternative to Telnet?

☐ SLIP

➡ ☒ SSH

☐ Remote Desktop

☐ SHTTP

Explanation

SSH (Secure Shell) is a secure and acceptable alternative to Telnet. SSH allows for secure interactive control of remote systems. SSH uses RSA public key cryptography for both connection and authentication. SSH uses the IDEA algorithm for encryption by default, but is also able to use Blowfish and DES.

Remote Desktop, while a remote control mechanism, is limited in use to a few versions of Windows, and is not very secure.

References

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_16]

▼ Question 13: Incorrect

SSL (Secure Sockets Layer) operates at which layer of the OSI model?

➡ ☐ Session

☐ Application



☒ Transport

☐ Presentation

Explanation

SSL (Secure Sockets Layer) operates at the Session layer of the OSI model.

SSL operates over TCP port 443. SSL was developed by Netscape to secure internet-based client/server interactions. SSL authenticates the server to the client using public key cryptography and digital certificates. SSL encrypts the entire communication session between a server and a client. SSL can be used to protect Web (HTTP) traffic as well as telnet, FTP, and email.

References

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_18]

▼ Question 14: Incorrect

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

- ➡ ☐ The current date and time must fall within the server's certificate validity period.
- ☐ All DNS resolution must point to the corporate intranet routers.
- ☒ ~~The certificate must be non-expiring and self-signed by the sysadmin.~~
- ☐ Master secrets are verifiable from asymmetric keys.

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 with 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

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_19]

▼ Question 15: Correct

You want to allow traveling users to connect to your private network through the internet. Users will connect from various locations, including airports, hotels, and public access points such as coffee shops and libraries. As such, you won't be able to configure the firewalls that might be controlling access to the internet in these locations.

Which of the following protocols would be most likely to be allowed through the widest number of firewalls?

- ☐ PPTP
- ➡ ☒ SSL
- ☐ IPsec
- ☐ PPPoE
- ☐ L2TP

Explanation

Ports must be opened in firewalls to allow VPN protocols. For this reason, using SSL for the VPN often works through firewalls, when other solutions do not because SSL uses port 443--a port that is often already open to allow HTTPS traffic. In addition, some NAT solutions do not work well with VPN connections.

PPTP uses port 1723, L2TP uses ports 1701 and 500, and IPsec uses UDP port 500 for the key negotiation protocol (IKE).

PPP over Ethernet (PPPoE) is used for connections that have an always on state, such as DSL or fiber optic running Ethernet. PPPoE is a modification of PPP that allows for negotiation of additional parameters that aren't typically present on a regular Ethernet network. ISPs typically implement PPPoE to control and monitor Internet access over broadband links.

References

LabSim for Security Pro, Section 9.10.

[All Questions SecPro2017_v6.exm DATA_TRANS_SEC_20]