Exam Report: 13.6.4 Practice Questions

Date: 12/2/2019 11:32:03 am
Time Spent: 3:05

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 86%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You can use a variety of methods to manage the configuration of a network router. Match the management option on the right with its corresponding description on the left. (Each option may be used once, more than once, or not at all.)

SSL
- ✓ Uses public-key cryptography

HTTP
- ✓ Transfers data in clear text

SSH
- ✓ Uses public-key cryptography

Telnet
- ✓ Transfers data in clear text

Console port
- ✓ Cannot be sniffed

Explanation

The following router management options transfer data in clear text and should not be used:

- HTTP
- Telnet

The following management options use public-key cryptography to protect data transferred between the router and the management station:

- SSL (used in conjunction with HTTP)
- SSH

The most secure way to manage a router's configuration is to connect the management station to the router's console port. This creates a dedicated transmission path that can't be sniffed by hosts on the network.

References

LabSim for Network Pro, Section 13.6.
[netpro18v5_all_questions_en.exm RT-7.4-4]

Question 2: Correct

Telnet is inherently insecure because its communication is in plaintext and is easily intercepted.

Which of the following is an acceptable alternative to Telnet?

- SHTTP
- SLIP
- ➡ SSH
- Remote Desktop

Explanation

SSH (Secure Shell) is a secure and acceptable alternative to Telnet. SSH allows 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 able to use Blowfish and DES.

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

References

LabSim for Network Pro, Section 13.6.
[netpro18v5_all_questions_en.exm NP05_2-10 #35]

Question 3: 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?

- PPPoE
- PPTP
- L2TP
- IPsec
- ➡ SSL

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. 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 the negotiation of additional parameters that are typically not present on a regular Ethernet network. ISPs typically implement PPPoE to control and monitor internet access over broadband links.

References

LabSim for Network Pro, Section 13.6.
[netpro18v5_all_questions_en.exm NP09_6-3 #MCS4]

Question 4: Correct

Which of the following protocols can be used to securely manage a network device from a remote connection?

- [x] SSH
- [ ] TLS
- [ ] SFTP
- [ ] Telnet

Explanation

SSH allows for secure interactive control of remote systems. SSH is a secure and acceptable alternative to Telnet.

SFTP is a file transfer protocol that uses Secure Shell (SSH) to secure data transfers. TLS ensures that messages being transmitted on the Internet are private and tamper proof. TLS is often used to add security to other protocols.

References

LabSim for Network Pro, Section 13.6.
[netpro18v5_all_questions_en.exm NP09_1-1 #5]

Question 5: Correct

Which security protocols use RSA encryption to secure communications over an untrusted network? (Select two.)

- [ ] Internet security association and key management protocol
- [x] Secure sockets layer
- [ ] Point-to-point tunneling protocol
- [x] Transport layer security

Explanation

Transport layer security (TLS) and its predecessor secure sockets layer (SSL) are cryptographic protocols that secure communications over untrusted IP networks such as the internet using RSA encryption. They use asymmetric cryptography to first verify the identity of both communicating parties and then to exchange a symmetric encryption key. This symmetric key is then used to encrypt data being sent between both hosts.

The point-to-point tunneling protocol (PPTP) does not provide an encryption mechanism and must be used with other protocols to secure communications. The internet security association and key management protocol (ISAKMP) is used to manage security keys, not to directly encrypt data communications.

References

LabSim for Network Pro, Section 13.6.
[netpro18v5_all_questions_en.exm MCM4]

Question 6: Incorrect

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

- [x] ~~HTTPS~~
- [ ] SNMP
- [ ] TLS
- [x] SSL
- [ ] 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 e-mail. SNMP is a network management protocol.

References

LabSim for Network Pro, Section 13.6.
[netpro18v5_all_questions_en.exm NP09_1-1 #7]

Question 7: Correct

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

- Kerberos
- Username and password authentication
- SSL
- IPsec

Explanation

HTTPS uses secure sockets layer (SSL) to offer greater security in web transactions.

References

LabSim for Network Pro, Section 13.6.
[netpro18v5_all_questions_en.exm NP05_2-10 #192]