Exam Report: 6.11.5 Practice Questions

Date: 1/22/2020 9:17:06 am
Time Spent: 30:50

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 60%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

You want to set up a service to allow multiple users to dial in to the office server from modems on their home computers. What service should you implement?

○ ISDN

● ~~PPP~~

➡ ○ RAS

○ RIP

Explanation

RAS stands for Remote Access Service, which enables users to dial in to a server from remote locations. ISDN is a digital communications network that uses existing phone lines. PPP is a remote access protocol. You will likely configure your RAS server to accept PPP connections. RIP stands for Routing Information Protocol and allows routers to share information.

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_01]

Question 2: Correct

You often travel away from the office. While traveling, you would like to use a modem on your laptop computer to connect directly to a server in your office and access files.

You want the connection to be as secure as possible. Which type of connection will you need?

○ Intranet

○ Virtual private network

○ Internet

➡ ● Remote access

Explanation

Use a remote access connection to connect directly to a server at a remote location.

You could use a VPN connection through the internet to connect to the server security. However, the connection would involve connecting first to the internet through a local ISP, then establishing a VPN connection to the server. While the VPN connection through the internet is secure, it is not as secure as a direct remote connection to the server.

An intranet is an internal network that only internal users can access.

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_02]

▼ **Question 3:** Incorrect

Which of the following are methods for providing centralized authentication, authorization, and accounting for remote access? (Select two.)

☐ PKI

☑ ~~AAA~~

➡ ☑ RADIUS

➡ ☐ TACACS+

☐ 802.1x

☐ EAP

Explanation

Both RADIUS and TACACS+ are protocols used for centralized authentication, authorization, and accounting with remote access. Remote access clients send authentication credentials to remote access servers. Remote access servers are configured as clients to the RADIUS or TACACS+ servers and forward the authentication credentials to the servers. The servers maintain a database of users and policies that control access for multiple remote access servers.

AAA stands for authentication, authorization, and accounting, and is a generic term that describes the functions performed by RADIUS/TACACS+ servers. A public key infrastructure (PKI) is a system of certificate authorities that issue certificates. 802.1x is an authentication mechanism for controlling port access. 802.1x uses RADIUS/TACACS+ servers. EAP is an authentication protocol that enables the use of customized authentication methods.

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_03]

▼ **Question 4:** Correct

Which of the following are characteristics of TACACS+? (Select two.)

☐ Uses UDP

☐ Allows of two different servers, one for authentication and authorization, and another for accounting

➡ ☑ Allows three different servers, one each for authentication, authorization, and accounting

➡ ☑ Uses TCP

Explanation

TACACS+ was originally developed by Cisco for centralized remote access administration. TACACS+:

- Provides three protocols, one each for authentication, authorization, and accounting. This allows each service to be provided by a different server.
- Uses TCP.
- Encrypts the entire packet contents.
- Supports more protocol suites than RADIUS.

RADIUS is used by Microsoft servers for centralized remote access administration. RADIUS:

- Combines authentication and authorization using policies to grant access.
- Uses UDP.
- Encrypts only the password.
- Often uses vendor-specific extensions. RADIUS solutions from different vendors might not be compatible.

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_05]

Question 5: Correct

Which of the following are differences between RADIUS and TACACS+?

➡ ● RADIUS combines authentication and authorization into a single function; TACACS+ allows these services to be split between different servers.

○ RADIUS encrypts the entire packet contents; TACACS+ only encrypts the password.

○ RADIUS supports more protocols than TACACS+.

○ RADIUS uses TCP; TACACS+ uses UDP.

Explanation

TACACS+ provides three protocols, one each for authentication, authorization, and accounting. This allows each service to be provided by a different server. In addition, TACACS+:

- Uses TCP
- Encrypts the entire packet contents
- Supports more protocol suites than RADIUS

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_06]

Question 6: Correct

RADIUS is primarily used for what purpose?

○ Managing RAID fault-tolerant drive configurations

➡ ● Authenticating remote clients before access to the network is granted

○ Managing access to a network over a VPN

○ Controlling entry gate access using proximity sensors

Explanation

RADIUS (Remote Authentication Dial-In User Service) is primarily used for authenticating remote clients before access to the network is granted. RADIUS is based on RFC 2865. RADIUS maintains client profiles in a centralized database. RADIUS offloads the authentication burden for dial-in users from the normal authentication of local network clients. For environments with a large number of dial-in clients, RADIUS provides improved security, easier administration, improved logging, and less performance impact on LAN security systems.

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_08]

Question 7: Incorrect

Which of the following is a characteristic of TACACS+?

● ~~Supports only TCP/IP~~

➡ ○ Encrypts the entire packet, not just authentication packets

○ Requires that authentication and authorization are combined in a single server

○ Uses UDP ports 1812 and 1813

Explanation

TACACS+ was originally developed by Cisco for centralized remote access administration. TACACS+:

- Provides three protocols, one each for authentication, authorization, and accounting. This allows each service to be provided by a different server.
- Uses TCP port 49.
- Encrypts the entire packet contents, not just authentication packets.
- Supports more protocol suites than RADIUS.

RADIUS is used by Microsoft servers for centralized remote access administration. RADIUS:

- Combines authentication and authorization using policies to grant access.
- Allows for the separation of accounting to different servers. However, authentication and authorization remain combined on a single server.
- Uses UDP ports 1812 and 1813.
- Uses a challenge/response method for authentication. RADIUS encrypts only the password using MD5.

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_09]

▼ **Question 8:** Correct

Which of the following ports are used with TACACS?

○ 22

➡ ● 49

○ 50 and 51

○ 1812 and 1813

○ 3389

Explanation

Terminal Access Controller Access-Control System (TACACS) uses TCP and UDP ports 49.
Port 22 is used by Secure Shell (SSH). Protocol numbers 50 and 51 are used by IPsec. Ports 1812 and 1813 are used by Remote Authentication Dial-In User Service (RADIUS). Port 3389 is used by Remote Desktop Protocol (RDP).

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_10]

▼ **Question 9:** Incorrect

You have a network with three remote access servers, a RADIUS server used for authentication and authorization, and a second RADIUS server used for accounting.

Where should you configure remote access policies?

○ On the RADIUS server used for accounting

➡ ○ On the RADIUS server used for authentication and authorization

● ~~On each of the remote access servers~~

○ On one of the remote access servers

Explanation

Remote access policies are used for authorization for remote access clients. For larger deployments with multiple remote access servers, you can centralize the administration of remote access policies by using an AAA server (authentication, authorization, and accounting server). Configure remote access policies on the AAA server that is used for authorization.

In a small implementation, user accounts and remote access policies are defined on the remote access server. With this configuration, if you have multiple remote access servers, you must define user accounts and policies on each remote access server. *Accounting* is an activity that tracks or logs the use of the remote access connection. Accounting is often used by ISPs to bill for services based on time or the amount of data downloaded.

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_12]

▼ **Question 10:** Incorrect

Which of the following is the best example of remote access authentication?

○ A user logs on to an e-commerce site that use SSL.

➡ ○ A user establishes a dial-up connection to a server to gain access to shared resources.

● ~~A user connects to a computer on the LAN using Remote Desktop.~~

○ A user accesses a shared folder on a server.

Explanation

Remote access allows a host to connect remotely to a private server or a network to access resources on that server or network. Remote access connections are typically used to connect remotely to servers at your office, but can also describe the type of connections used to connect to an internet service provider (ISP) for internet access. A remote access server (RAS) is a server configured to allow remote access connections.

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_13]

▼ **Question 11:** Incorrect

You are configuring a dial-up connection to a remote access server. Which protocols would you choose to establish the connection and authenticate, providing the most secure connection possible? (Select two.)

➡ □ PPP

➡ ☑ CHAP

□ PAP

□ PPPoE

□ SLIP

Explanation

Choose PPP and CHAP for the connection.

Choose point-to-point protocol (PPP) for the connection. PPP is preferred over serial line interface protocol (SLIP) because it can negotiate encryption protocols to use for the connection. Point-to-point protocol over Ethernet (PPPoE) is similar to PPP, but is used for a cable (not a dial-up) connection.

Choose challenge handshake authentication protocol (CHAP) for authentication. CHAP uses hashing to protect the passwords and allows re-authentication. Avoid using password authentication protocol (PAP) because it transmits credentials in the clear (unencrypted).

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_16]

▼ **Question 12:** Correct

Which of the following authentication protocols transmits passwords in cleartext, and is, therefore, considered too insecure for modern networks?

○ EAP

○ CHAP

○ RADIUS

➡ ● PAP

Explanation

The password authentication protocol (PAP) is considered insecure because it transmits password information in clear text. Anyone who sniffs PAP traffic from a network can view the password information from a PAP packet with a simple traffic analyzer.

The challenge handshake protocol (CHAP) uses a three-way handshake to authenticate users. During this handshake, a hashed value is used to authenticate the connection. The extensible authentication protocol (EAP) is an enhanced authentication protocol that can use a variety of authentication methods, including digital certificates and smart cards. The Remote Authentication Dial-In User Service (RADIUS) is an authentication system that allows the centralization of remote user account management.

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_17]

Question 13: Correct

Which of the following is a feature of MS-CHAP v2 that is not included in CHAP?

○ Three-way handshake

➡ ● Mutual authentication

○ Hashed shared secret

○ Certificate-based authentication

Explanation

MS-CHAP v2 allows for *mutual authentication*, where the server authenticates to the client.

Both CHAP and MS-CHAP use a three-way handshake process for authenticating users with user names and passwords. The password (or shared secret) value is hashed. The hash is sent for authentication, not the shared secret, .

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_14]

Question 14: Correct

CHAP performs which of the following security functions?

➡ ● Periodically verifies the identity of a peer using a three-way handshake

○ Links remote systems together

○ Protects user names

○ Allows the use of biometric devices

Explanation

CHAP periodically verifies the identity of a peer using a three-way handshake. CHAP ensures that the same client or system exists throughout a communication session by repeatedly and randomly re-testing the validated system. This test involves the security server sending a challenge message to the client. The client then performs a one-way hash function on the challenge and returns the result to the security

server. The security server performs its own function on the challenge and compares its result with the result received from the client. If they don't match, the session is terminated.
CHAP does provide protection for both passwords and user names. However, stating that it only protects user names is incomplete and, therefore, not the best answer. CHAP does not link remote systems together--a VPN protocol is needed for that purpose. CHAP does not function as a device driver or interoperability mechanism for biometric devices.

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_15]

▼ **Question 15:** Correct

Which remote access authentication protocol periodically and transparently re-authenticates during a logon session by default?

○ PAP

○ Certificates

○ EAP

➡ ● CHAP

Explanation

CHAP is the only remote access authentication protocol that periodically and transparently re-authenticates during a logon session by default.

PAP, EAP, and certificates do not re-authentication mid-session.

References

LabSim for Security Pro, Section 6.11.
[All Questions SecPro2017_v6.exm REMOTE_ACC_18]