Exam Report: 11.4.5 Practice Questions

Date: 11/6/2019 9:27:06 am
Time Spent: 10:54

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

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

➡ ☑ TACACS+

☐ EAP

☐ 802.1x

☐ AAA

☐ PKI

➡ ☑ RADIUS

Explanation

Both RADIUS and TACACS+ are protocols used for centralized authentication, authorization, and accounting used 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 allows the use of customized authentication methods.

References

LabSim for Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm NP09 6-4 MCM1]

Question 2: Correct

You have decided to implement a remote access solution that uses multiple remote access servers. You want to implement RADIUS to centralize remote access authentication and authorization.

Which of the following is a required part of your configuration?

○ Configure the remote access servers as RADIUS servers.

○ Obtain certificates from a public or private PKI.

○ Configure remote access clients as RADIUS clients.

➡ ● Configure the remote access servers as RADIUS clients.

Explanation

When configuring a RADIUS solution, configure a single server as a RADIUS server. Then configure all remote access servers as RADIUS clients.

Certificate-based authentication can be used with a RADIUS solution, but is not a requirement.

References

LabSim for Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm NP09 6-4 MCS5]

Question 3: Correct

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

□ Allows the possibility of two different servers, one for authentication and authorization, and another for accounting.

➡ ☑ Uses TCP.

➡ ☑ Allows the possibility of three different servers, one each for authentication, authorization, and accounting.

□ Uses UDP.

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 Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm NP09 6-4 MCM3]

Question 4: 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 Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm NP09 6-4 MCS6]

▼ Question 5: Correct

Which of the following protocols can be used to centralize remote access authentication?

○ SESAME

○ Kerberos

○ CHAP

○ EAP

➡ ◉ TACACS

Explanation

Centralized remote access authentication protocols include:

- Remote Authentication and Dial-In User Service (RADIUS)
- Terminal Access Controller Access Control System (TACACS)

Password authentication protocol (PAP) and challenge handshake authentication protocol (CHAP) are authentication protocols used between the client and the server. Kerberos and Secure European System for Applications in a Multi-Vendor Environment (SESAME) are single sign-on protocols.

References

LabSim for Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm SSCP-3 NEW [218]]

▼ Question 6: Correct

RADIUS is primarily used for what purpose?

○ Managing RAID fault-tolerant drive configurations.

○ Managing access to a network over a VPN.

○ Controlling entry gate access using proximity sensors.

➡ ◉ Authenticating remote clients before access to the network is granted.

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 benefits include improved security, easier administration, improved logging, and less performance impact on LAN security systems.

References

LabSim for Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm SSCP-3 SP [865]]

Question 7: Correct

Which of the following is a characteristic of TACACS+?

○ Supports only TCP/IP.

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

○ Uses UDP ports 1812 and 1813.

➡ ● Encrypts the entire packet, not just authentication packets.

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 Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm SP08_3-7 1]

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). Ports 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 Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm SP08_3-7 5]

Question 9: Correct

You are configuring your computer to dial up to the internet. What protocol should you use?

○ SMTP

➡ ● PPP

○ VPN

○ PPTP

Explanation

PPP, or point-to-point protocol, lets you dial up and connect to the internet.

References

LabSim for Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm NP05_2-16 #48]

Question 10: Incorrect

Which of the following protocols or services is commonly used on cable internet connections for user authentication?

➡ ○ PPPoE

● ~~RDP~~

○ PPP

○ RRAS

Explanation

The point-to-point protocol over Ethernet (PPPoE) is commonly used on cable internet connections for user authentication. Like its dial-up counterpart, the point-to-point protocol (PPP), PPPoE requires that users provide authentication information before a connection is granted.

The Routing and Remote Access Service (RRAS) is a software program used on Windows systems to provide remote connectivity capabilities to users. Although it could be used for authentication services on a cable internet access system, it is not commonly used for this purpose. The point-to-point protocol (PPP) is a user authentication system commonly deployed on dial-up remote access connections. Remote Desktop Protocol (RDP) is the protocol used by Windows Terminal Services applications, including Remote Desktop.

References

LabSim for Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm NP05_2-16 #76]

Question 11: Correct

You have just signed up for internet access using a local provider that gives you a fiber optic line into your house. From there, Ethernet and wireless connections are used to create a small network within your home.

Which of the following protocols would be used to provide authentication, authorization, and accounting for the internet connection?

○ RDP

○ L2TP

○ PPP

➡ ● PPPoE

○ ICA

Explanation

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 are typically not present on a regular Ethernet network. ISPs typically implement PPPoE to control and monitor internet access over broadband links.

The point-to-point protocol (PPP) is used for dial-up connections. RDP and ICA are Remote Desktop protocols. L2TP is a VPN protocol.

References

LabSim for Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm NP09_6-3 #MCS6]

▼ Question 12: Incorrect

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

➡ ○ RAS

○ RIP

○ ISDN

● ~~PPP~~

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 Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm NP05_2-16 #32]

▼ Question 13: 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 on that server that you need.

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

○ Intranet

➡ ● Remote access

○ Virtual private network

○ Internet

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 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 Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm NP05_2-16 #144]

▼ Question 14: Correct

Which type of device is required to implement port authentication through a switch?

○ Layer 3 switch

➡ ● RADIUS server

○ Proxy server

○ Router

Explanation

Port authentication is provided by the 802.1x protocol and allows only authenticated devices to connect to the LAN through the switch. 802.1x requires a RADIUS server (also called an AAA server) to validate the authentication credentials.

A router or a Layer 3 switch are required to enable communication between VLANs. A proxy server controls access based on URL or other upper-layer information.

References

LabSim for Network Pro, Section 11.4.
[netpro18v5_all_questions_en.exm NP09_3-3 #14]