Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/2/2022 9:01:21 pm • Time spent: 01:49

Score: 50%

Passing Score: 80%

Question 1: ✔ Correct

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

- [ ] AAA
- [x] TACACS+
- [x] RADIUS
- [ ] PKI
- [ ] 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. AAA is a generic term that describes the functions performed by RADIUS and 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.

EAP is an authentication protocol that enables the use of customized authentication methods.

REFERENCES

5.7.2 Network Access Control Facts

6.1.6 Access Control Model Facts

6.3.3 Authorization Facts

6.9.2 Remote Access Facts

q_remote_acc_aaa_secp7.question.fex

Question 2: ✕ Incorrect

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

- ~~Three-way handshake~~
- Mutual authentication
- Certificate-based authentication
- Hashed shared secret

EXPLANATION

MS-CHAP v2 allows mutual authentication, in which the server authenticates to the client.

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

REFERENCES

6.9.2 Remote Access Facts

q_remote_acc_chap_01_secp7.question.fex

Question 3: ✕ Incorrect

What does a remote access server use for authorization?

- ~~CHAP or MS-CHAP~~
- SLIP or PPP
- Usernames and passwords
- Remote access policies

EXPLANATION

Authorization is the process of identifying the resources that a user can access over a remote access connection. Authorization is controlled through the use of network policies (remote access policies) and access control lists (ACLs). Authorization can restrict access based on:

- Time of day
- Type of connection (PPP or PPPoE, wired or wireless)
- Location of the resource (restrict access to specific servers)

Authentication is the process of proving identity. Common protocols used for remote access authentication include PAP, CHAP, MS-CHAP, or EAP.

Usernames and passwords are used during identification and authentication as authentication credentials. SLIP and PPP are remote access connection protocols that are used to establish and negotiate parameters used for remote access.

REFERENCES

6.9.2 Remote Access Facts

q_remote_acc_policy_secp7.question.fex

Question 4: ✔ Correct

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

- EAP
- CHAP
- RADIUS
- PAP

EXPLANATION

Password Authentication Protocol (PAP) is considered unsecure because it transmits password information in cleartext. Anyone who sniffs PAP traffic from a network can view the password information from a PAP packet with a simple traffic analyzer.

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

REFERENCES

6.9.2 Remote Access Facts

q_remote_acc_ppp_secp7.question.fex

Question 5: ✕ Incorrect

You often travel away from the office. While traveling, you would like to use 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 do you need?

- Internet
- ~~Virtual private network~~
- Remote access
- Intranet

EXPLANATION

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

You could use a virtual private network (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 and 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

6.9.2 Remote Access Facts

q_remote_acc_remote_secp7.question.fex

Question 6: ✕ Incorrect

RADIUS is primarily used for what purpose?

- Controlling entry-gate access using proximity sensors
- ~~Managing access to a network over a VPN~~
- Managing RAID fault-tolerant drive configurations
- Authenticating remote clients before access to the network is granted

EXPLANATION

Remote Authentication Dial-In User Service (RADIUS) is primarily used for authenticating remote clients before access to a network is granted. RADIUS is based on RFC 2865 and 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 alleviated performance impact on LAN security systems.

REFERENCES

6.9.4 RADIUS and TACACS+ Facts

q_radius_tacacs_radius_secp7.question.fex

Question 7: ✔ Correct

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

- [x] Uses TCP
- [ ] Can be vulnerable to buffer overflow attacks
- [ ] Allows two different servers (one for authentication and authorization and another for accounting)
- [ ] Uses UDP
- [x] Allows three different servers (one each for authentication, authorization, and accounting)

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.
- Uses UDP ports 1812 and 1813 and can be vulnerable to buffer overflow attacks.

REFERENCES

6.9.4 RADIUS and TACACS+ Facts

q_radius_tacacs_tac_char_01_secp7.question.fex

Question 8: ✔ Correct

Which of the following is a characteristic of TACACS+?

- ➡ 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
- Supports only TCP/IP

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 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

6.9.4 RADIUS and TACACS+ Facts

q_radius_tacacs_tac_char_02_secp7.question.fex

Question 9: ✔ Correct

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

- RADIUS uses TCP; TACACS+ uses UDP.
- ➡ 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+.

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

6.9.4 RADIUS and TACACS+ Facts

q_radius_tacacs_tac_dif_secp7.question.fex

Question 10: ✕ Incorrect

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 port 49 for TCP and UDP.

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

6.9.4 RADIUS and TACACS+ Facts

q_radius_tacacs_tac_port_secp7.question.fex