Exam Report: 2.13.5 Practice Questions - Section 2.13

Date: 11/22/2015 7:55:11 pm
Time Spent: 1:53

Candidate: Belskis, Tomas
Login: t0mas9lt

Overall Performance

Your Score: 33%

Passing Score: 80%

Certification Ranking

Within your class: Within your school: Nationally:

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

▼ Question 1: Incorrect

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

☐ EAP

➡ ☑ RADIUS

☐ PKI

➡ ☐ TACACS+

☐ 802.1x

☐ AAA

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 for the use of customized authentication methods.

References

LabSim for Security Pro, Section 2.13.
[Questions.exm NP09 6-4 MCM1]

▼ Question 2: Incorrect

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 would be a required part of your configuration?

- ● ~~Configure the remote access servers as RADIUS servers.~~
- ○ Obtain certificates from a public or private PKI.
- ➡ ○ Configure the remote access servers as RADIUS clients.
- ○ Configure remote access clients 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 Security Pro, Section 2.13.
[Questions.exm NP09 6-4 MCS5]

▼ Question 3: Correct

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

- ➡ ☑ Allows for a possible of three different servers, one each for authentication, authorization, and accounting
- ➡ ☑ Uses TCP
- ☐ Allows for a possible of two different servers, one for authentication and authorization, and another for 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 Security Pro, Section 2.13.

[Questions.exm NP09 6-4 MCM3]

▼ Question 4: Correct

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

○ RADIUS uses TCP; TACACS+ uses UDP.

○ RADIUS supports more protocols than 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.

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 2.13.
[Questions.exm NP09 6-4 MCS6]

▼ Question 5: Correct

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

➡ ● TACACS

○ CHAP

○ SESAME

○ EAP

○ Kerberos

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 Security Pro, Section 2.13.
[Questions.exm SSCP-3 NEW [218]]

▼ Question 6: Correct

RADIUS is primarily used for what purpose?

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

○ Controlling entry gate access using proximity sensors

○ Managing access to a network over a VPN

○ Managing RAID fault-tolerant drive configurations

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 2.13.
[Questions.exm SSCP-3 SP [865]]

▼ Question 7: Incorrect

Which of the following is a characteristic of TACACS+?

○ Uses UDP ports 1812 and 1813

● ~~Requires that authentication and authorization are combined in a single server~~

➡ ○ Encrypts the entire packet, not just authentication packets

○ 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 and 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 2.13.
[Questions.exm SP08_3-7 1]

▼ Question 8: 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 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 2.13.
[Questions.exm SP08_3-7 5]

▼ Question 9: 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 the remote access connection. Authorization is controlled through the use of network policies (remote access policies) as well as access control lists. Authorization can restrict access based on:

- Time of day
- Type of connection (e.g. PPP or PPPoE, wired or wireless)
- Location of the resource (i.e. 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

LabSim for Security Pro, Section 2.13.
[Questions.exm SP08_3-7 6]

▼ Question 10: Incorrect

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

➡ ○ A user establishes a dialup connection to a server to gain access to shared resources

● ~~A user logs on to an e-commerce site that use SSL~~

○ A user connects using Remote Desktop to a computer on the LAN

○ 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 2.13.
[Questions.exm SP08_3-7 8]

▼ Question 11: Correct

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

○ Three-way handshake

○ Certificate-based authentication

➡ ● Mutual authentication

○ Hashed shared secret

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 usernames and passwords. The password (or shared secret) value is hashed, and the hash, not the shared secret, is sent for authentication.

References

LabSim for Security Pro, Section 2.13.
[Questions.exm NP09 6-4 MCS9]

▼ Question 12: Incorrect

CHAP performs which of the following security functions?

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

● ~~Allows the use of biometric devices~~

○ Protects usernames

○

○ Links remote systems together

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 that received from the client. If they don't match, the session is terminated.

CHAP does provide protection for both passwords and usernames. However stating that it only protects usernames 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 2.13.
[Questions.exm SSCP-3 SP [890]]

▼ **Question 13:** Incorrect

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

○ EAP

○ CHAP

➡ ○ PAP

● ~~RADIUS~~

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 smartcards. 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 2.13.
[Questions.exm SSCP-3 NP [391]]

▼ **Question 14:** Incorrect

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

● ~~Certificates~~

➡ ○ CHAP

○ EAP

○ PAP

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 2.13.
[Questions.exm SSCP-3 CP [882]]

▼ **Question 15:** Incorrect

Which of the following authentication protocols uses a three-way handshake to authenticate users to the network? (Choose two.)

□ PAP

➡ ☑ MS-CHAP

➡ □ CHAP

☑ ~~EAP~~

Explanation

Both the Challenge Handshake Protocol (CHAP) and the Microsoft Challenge Handshake Protocol (MS-CHAP) use a three-way handshake to authenticate users. During this handshake process, a hash value is created, compared and then used to authenticate the connection.

The Password Authentication Protocol (PAP) uses a username and password combination to authenticate users. PAP is considered insecure because it transmits the username and password information in clear text. Extensible Authentication Protocol (EAP) supports a number of authentication methods including smartcards and digital certificates.

References

LabSim for Security Pro, Section 2.13.
[Questions.exm NP05_2-18 #7]