

Exam Report: 6.12.9 Practice Questions

Date: 1/22/2020 10:06:39 am

Candidate: Garsteck, Matthew

Time Spent: 18:26

Login: mGarsteck

Overall Performance

Your Score: 53%

View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1:

Correct

When using Kerberos authentication, which of the following terms is used to describe the token that verifies the user's identity to the target system?

- ☐ Hashkey
- ➡ ☒ Ticket
- ☐ Coupon
- ☐ Voucher

Explanation

The tokens used in Kerberos authentication are known as *tickets*. Tickets perform a number of functions, including notifying the network service of the user who has been granted access and authenticating the identity of the person when they attempt to use that network service.

The terms coupon and voucher are not associated with Kerberos or any other commonly implemented network authentication system. The term hashkey is sometimes used to describe a value that has been derived from some piece of data when that value is then used to access a service. However, the term hashkey is not associated with Kerberos.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_01]

▼ Question 2:

Incorrect

Which of the following are required when implementing Kerberos for authentication and authorization? (Select two.)

- ☐ PPPoE
- ☒ RADIUS or TACACS+ server
- ☐ PPP
- ➡ ☒ Ticket granting server
- ➡ ☐ Time synchronization

Explanation

Kerberos grants *tickets* (also called a security *token*) to authenticated users and to authorized resources. A ticket granting server (TGS) grants tickets that are valid for specific resources on specific servers. Kerberos requires that all servers within the process have synchronized clocks to validate tickets, so a centralized time server or other method for time synchronization is required.

Both RADIUS and TACACS+ are protocols used for centralized authentication, authorization, and accounting used with remote access. PPP and PPPoE are protocols used for remote access connections.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_02]

▼ Question 3: Incorrect

Which of the following are requirements to deploy Kerberos on a network? (Select two.)

- ☐ Blocking of remote connectivity
- ☐ A directory service
- ➡ ☐ A centralized database of users and passwords
- ☒ ~~Use of token devices and one-time passwords~~
- ➡ ☒ Time synchronization between devices

Explanation

Kerberos requires that there be a centralized database of users and passwords, as well as time synchronization. The user database is usually maintained on the KDC itself or on a separate pre-authentication server system. Time synchronization is required to stamp a consistent expiration date within the ticket granting ticket (TGT).

Kerberos can function across remote links. Therefore, remote connectivity does not need to be blocked. Kerberos is based on passwords, but can be deployed within an environment that employs tokens and one-time passwords. However, this is not a requirement of Kerberos. Kerberos is often deployed simultaneously with a directory service, such as Active Directory, but Kerberos does not require a directory service to be present. Kerberos can function as a stand-alone, single-sign on solution.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_03]

▼ Question 4: Incorrect

Which ports does LDAP use by default? (Select two.)

- ☐ 161
- ➡ ☐ 636
- ☐ 110
- ➡ ☒ 389
- ☐ 69

Explanation

LDAP (Lightweight Directory Access Protocol) uses ports 389 and 636 by default. Port 636 is used for LDAP over SSL. This is the secure form or mode of LDAP. Unsecured LDAP uses port 389.

Port 69 is used by TFTP. Port 110 is used by POP3. Port 161 is used by SNMP.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_04]

▼ Question 5: Correct

You want to deploy SSL to protect authentication traffic with your LDAP-based directory service. Which port does this action use?

- ☐ 60
- ☐ 80
- ☐ 389
- ☐ 443
-  ☒ 636
- ☐ 2208

Explanation

To use SSL for LDAP authentication, use port 636. Port 80 is used for HTTP, while port 443 is used for HTTPS (HTTP with SSL). Simple LDAP authentication uses port 389.


References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_05]

▼ Question 6: Incorrect

Your LDAP directory services solution uses simple authentication. What should you always do when using simple authentication?

-  ☐ Use SSL
- ☐ Use IPsec and certificates
- ☐ Use Kerberos
- ☒ Add SASL and use TLS

Explanation

Protect LDAP simple authentication by using SSL to protect authentication traffic. LDAP simple authentication uses cleartext for user name and password exchange. Protect this exchange with SSL.

While you can protect authentication using SASL, this requires changing the authentication mode of LDAP from simple to SASL. When using SASL, you can use a wide range of solutions, such as TLS, Kerberos, IPsec, or certificates.


References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_06]

▼ Question 7: Correct

You want to use Kerberos to protect LDAP authentication. Which authentication mode should you choose?

- ☐ Mutual
- ☐ EAP
- ☐ Simple
-  ☒ SASL

Explanation

Choose SASL (Simple Authentication and Security Layer) authentication mode to use Kerberos with LDAP. SASL is extensible and lets you use a wide variety of protection methods.

LDAP authentication modes include Anonymous, Simple, and SASL. EAP is an extensible authentication protocol for remote access, not LDAP.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_07]

▼ Question 8: Correct

A user has just authenticated using Kerberos. Which object is issued to the user immediately following login?

- ➡ ☒ Ticket granting ticket
- ☐ Digital certificate
- ☐ Client-to-server ticket
- ☐ Digital signature

Explanation

Kerberos works as follows:

1. The client sends an authentication request to the authentication server.
2. The authentication server validates the user identity and grants a ticket granting ticket (TGT). The TGT validates the user identity and is good for a specific ticket granting server.
3. When the client needs to access a resource, it submits its TGT to the TGS. The TGS validates that the user is allowed access and issues a client-to-server ticket.
4. The client connects to the service server and submits the client-to-server ticket as proof of access.
5. The SS accepts the ticket and allows access.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_08]

▼ Question 9: Correct

Which of the following protocols uses port 88?

- ☐ L2TP
- ☐ TACACS
- ☐ PPTP
- ☐ LDAP
- ➡ ☒ Kerberos

Explanation

Kerberos uses port 88.

Terminal Access Controller Access-Control System (TACACS) uses port 49. LDAP uses TCP and UDP ports 389. Secure LDAP uses SSL/TLS over port 636. Layer 2 tunneling protocol (L2TP) uses port 1701. Point-to-point tunneling protocol (PPTP) uses port 1723.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_09]

▼ Question 10: Incorrect

Which of the following authentication mechanisms is designed to protect a nine-character password from attacks by hashing the first seven characters into a single hash and then hashing the remaining two characters into another separate hash?

- ☒ LDAP
- ➡ ☐ LANMAN
- ☐

- ☒ NTLMv2
- ☐ NTLM

Explanation

LANMAN divides passwords longer than seven characters into two separate hashes (meaning that characters one through seven are a single hash, and characters eight through 14 are a separate hash). LANMAN passwords are protected using a hashing method called LANMAN hash that uses DES and a proprietary algorithm. LANMAN passwords are limited to a total of 14 characters. LANMAN hash is very weak and can be easily broken.

NT LAN Manager (NTLM) is the replacement for LANMAN on Microsoft networks and uses a stronger hashing method than LANMAN. NTLMv2 includes additional security enhancements and a stronger hashing method. The Lightweight Directory Access Protocol (LDAP) is a lightweight protocol that allows users and applications to read from and write to an LDAP-compliant directory service, such as Active Directory, eDirectory, and OpenLDAP.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_10]

▼ Question 11: Correct

What is mutual authentication?

- ☐ Deploying CHAP and EAP on remote access connections.
- ☐ The use of two or more authentication factors.
- ➡ ☒ A process by which each party in an online communication verifies the identity of each other party.
- ☐ Using a CA (certificate authority) to issue certificates.

Explanation

Mutual authentication is the process by which each party in an online communication verifies the identity of each other party. Mutual authentication is most common in VPN links, SSL connections, and e-commerce transactions. In each of these situations, both parties in the communication want to ensure that they know whom they are interacting with.

The use of two or more authentication factors is called two-factor authentication. CHAP and EAP are authentication protocols. Communicating hosts might use certificates issued by a trusted CA in performing mutual authentication, but using the CA is not, in itself, a definition of mutual authentication.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_11]

▼ Question 12: Incorrect

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

- ➡ ☐ TACACS
- ☐ SESAME
- ☐ CHAP
- ☒ Kerberos
- ☐ EAP

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 6.12.

[All Questions SecPro2017_v6.exm REMOTE_ACC_07]

▼ Question 13: Correct

A manager has told you she is concerned about her employees writing their passwords for websites, network files, and database resources on sticky notes. Your office runs exclusively in a Windows environment.

Which tool could you use to prevent this behavior?

- ☐ Computer Management
- ➡ ☒ Credential Manager
- ☐ Local Users and Groups
- ☐ Key Management Service

Explanation

Credential Manager securely stores account credentials for network resources, such as file servers, websites, and database resources.

Local Users and Groups manages only local account credentials. Key Management Service is used to manage the activation of Windows systems on the network. Computer Management is used to complete Windows management tasks, such as viewing the Event Log, managing hardware devices, and managing hard disk storage.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_12]

▼ Question 14: Correct

KWalletManager is a Linux-based credential management system that stores encrypted account credentials for network resources.

Which encryption methods can KWalletManager use to secure account credentials? (Select two.)

- ☐ HMAC-SHA1
- ☐ Twofish
- ☐ Kerberos
- ➡ ☒ GPG
- ➡ ☒ Blowfish

Explanation

KWalletManager offers two encryption options for protecting stored account credentials:

- Blowfish
- GPG

HMAC-SHA1 is most often used with one-time passwords. Kerberos is used for login authentication and authorization in a Windows domain. Twofish is an encryption mechanism that is similar to the Blowfish block cipher, but has not been standardized at this point.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_13]

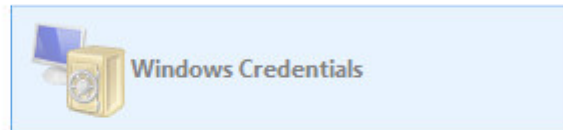
▼ Question 15: Incorrect

You want to protect the authentication credentials you use to connect to the LAB server in your network by copying them to a USB drive.

Click the option you use in Credential Manager to protect your credentials.

Manage your credentials

View and delete your saved logon information for websites, connected applications and networks.



[Back up Credentials](#)  [Restore Credentials](#)


Windows Credentials

[Add a Windows credential](#)

KIMSPC

Modified: Today 

LAB

Modified: Today 

Explanation

Within Credential Manager, use the Back up Credentials and Restore Credentials links to back up and restore credentials. It is recommended that you back up credentials to a removable device, such as a USB flash drive, to protect them from a hard disk crash on the local system.

References

LabSim for Security Pro, Section 6.12.

[All Questions SecPro2017_v6.exm NETWORK_AUTH_14]