Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/2/2022 9:05:19 pm • Time spent: 02:20

Score: 30%

Passing Score: 80%

Question 1: ✕ Incorrect

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?

● ~~Voucher~~

○ Coupon

○ Hashkey

➡ ○ Ticket

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 that person when he or she attempts to use the 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. This term is not associated with Kerberos.

REFERENCES

6.10.2 Network Authentication Facts

q_netauth_kerberos_01_secp7.question.fex

Question 2: ✕ Incorrect

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.

Lightweight Directory Access Protocol (LDAP) authentication modes include anonymous, simple, and SASL authentication modes.

EAP is an extensible authentication protocol for remote access. It is not used in conjunction with LDAP.

REFERENCES

6.10.2 Network Authentication Facts

q_netauth_kerberos_02_secp7.question.fex

▾ Question 3: ✕ Incorrect

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

➡ ○ Ticket-granting ticket

○ Digital signature

● ~~Client-to-server ticket~~

○ Digital certificate

EXPLANATION

Kerberos functions as follows:

1. The client sends an authentication request to the authentication server.
2. The authentication server validates the user's identity and grants a ticket-granting ticket (TGT). The TGT validates the user's 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 ticket-granting server (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

6.10.2 Network Authentication Facts

q_netauth_kerberos_03_secp7.question.fex

▼ **Question 4:** ✕ Incorrect

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 Secure Sockets Layer (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

☰ 6.10.2 Network Authentication Facts

q_netauth_ldaps_01_secp7.question.fex

▾ Question 5: ✕ Incorrect

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

○ Use IPsec and certificates

● ~~Add SASL and use TLS~~

○ Use Kerberos

➡ ○ Use SSL

EXPLANATION

Protect LDAP simple authentication by using SSL to protect authentication traffic. LDAP simple authentication uses cleartext for username 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

6.10.2 Network Authentication Facts

q_netauth_ldaps_02_secp7.question.fex

Question 6: ✕ Incorrect

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

- ➡ □ 636
- □ 110
- ☑ ~~69~~
- ➡ ☑ 389
- □ 161

EXPLANATION

Lightweight Directory Access Protocol (LDAP) 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 Trivial File Transfer Protocol (TFTP). Port 110 is used by Post Office Protocol version 3 (POP3). Port 161 is used by Simple Network Management Protocol (SNMP).

REFERENCES

6.10.2 Network Authentication Facts

q_netauth_ldap_secp7.question.fex

▼ **Question 7:** ✓ Correct

What is mutual authentication?

○ Using a certificate authority (CA) to issue certificates.

○ The use of two or more authentication factors.

○ Deploying CHAP and EAP on remote access connections.

➡ ◉ A process by which each party in an online communication verifies the identity of the other party.

EXPLANATION

Mutual authentication is the process by which each party in an online communication verifies the identity of the 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 with whom they are interacting.

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

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_netauth_mutual_secp7.question.fex

Question 8: ✓ 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?

➡ ● Credential Manager

○ Local Users and Groups

○ Computer Management

○ 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 a network.

Computer Management is used to complete Windows management tasks, such as viewing event logs, managing hardware devices, and managing hard disk storage.

REFERENCES

6.10.8 Credential Management Facts

q_credmgmt_password_01_secp7.question.fex

▾ **Question 9:** ✕ Incorrect

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.)

- ☐ Kerberos
- ➡ ☐ Blowfish
- ☑ ~~HMAC-SHA1~~
- ☐ Twofish
- ➡ ☑ GPG

EXPLANATION

KWalletManager offers two encryption options for protecting stored account credentials. These two encryption options are Blowfish and 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

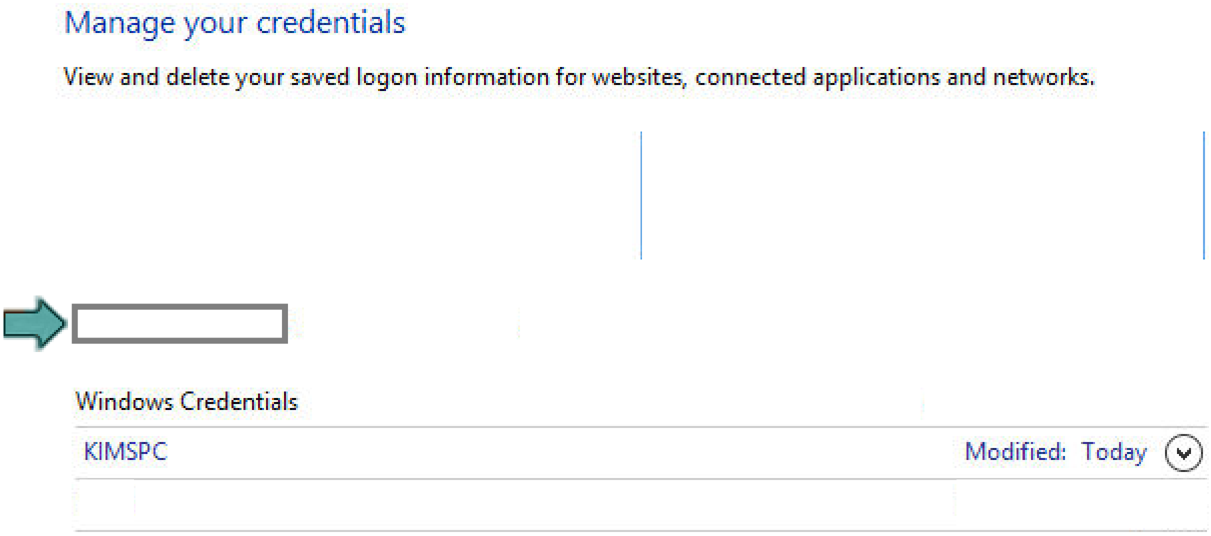
6.10.8 Credential Management Facts

q_credmgmt_password_02_secp7.question.fex

Question 10: ✓ Correct

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.

Windows Credentials

KIMSPC 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

6.10.8 Credential Management Facts

q_credmgmt_password_03_secp7.question.fex