

# Chp 6 NS

Candidate: Dunkan Gibson (dunkan.gibson)  
Date: 3/2/2022 9:18:38 pm • Time spent: 08:04

Score: 88%

Passing Score: 80%



## Question 1: ✓ Correct

You have hired ten new temporary employees to be with the company for three months.

How can you make sure that these users can only log on during regular business hours?

- Configure account lockout in Group Policy
- Configure account expiration in user accounts
- Configure day/time restrictions in user accounts
- Configure account policies in Group Policy

### EXPLANATION

Use day/time restrictions to limit the days and hours when users can log on.

Configure account expiration to disable an account after a specific date. Use account policies in Group Policy to configure requirements for passwords. Use account lockout settings in Group Policy to automatically lock accounts when a specific number of incorrect passwords are entered.

### REFERENCES

-  [6.6.9 Hardening Authentication Facts](#)

`q_harden_auth_time_secp7.question.fex`

**Question 2:** ✓ Correct

Which of the following principles is implemented in a mandatory access control model to determine object access by classification level?

- Principle of least privilege
- Need to Know
- Clearance
- Separation of duties
- Ownership

**EXPLANATION**

Need to Know is used with mandatory access control environments to implement granular control over access to segmented and classified data.

Separation of duties is the security principle that states that no single user is granted sufficient privileges to compromise the security of an entire environment.

Clearance is the subject classification label that grants a user access to a specific security domain in a mandatory access control environment.

Ownership is the access right in a discretionary access control environment that gives a user complete control over an object. This is usually because he or she created the object.

**REFERENCES**

-  6.1.4 Access Control Best Practices

[q\\_acct\\_bstpract\\_need\\_secp7.question.fex](#)

**Question 3:** ✓ 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?

- Ticket**
- Voucher
- Coupon
- Hashkey

**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 4:** ✓ Correct

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

- Digital certificate
- Client-to-server ticket
- Ticket-granting ticket
- Digital signature

**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 5:** ✓ Correct

A smart card can be used to store all but which of the following items?

- Identification codes
- Digital signature
- Cryptography keys
- Biometric template original

**EXPLANATION**

A smart card cannot store biometric template originals, as those are physical components of the human body.

A smart card can store digital signatures, cryptography keys, and identification codes.

**REFERENCES**

-  6.2.3 Authentication Facts

q\_authent\_smart\_secp7.question.fex

**Question 6:** ✓ Correct

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?

- Intranet
- Virtual private network
- Remote access
- Internet

**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 7:** ✓ Correct

Which type of group can be used for controlling access to objects?

-  Security
- Distribution
- DACL
- Authorization

**EXPLANATION**

Only security groups can be used for controlling access to objects.

A discretionary access control list (DACL) is an implementation of discretionary access control (DAC).

Distribution groups cannot be used for controlling access to objects.

Authorization is the process of controlling access to resources such as computers, files, or printers.

**REFERENCES**

-  6.3.3 Authorization Facts

q\_authorize\_security\_secp7.question.fex

**Question 8:** ✓ Correct

Which of the following is a password that relates to things that people know, such as a mother's maiden name or a pet's name?

- Dynamic
- One-time
- Cognitive
- Passphrase

**EXPLANATION**

Cognitive passwords relate to things that people know, such as a mother's maiden name or a pet's name.

Dynamic passwords change upon each consecutive login.

One-time passwords are only valid for a single use.

A passphrase is a password long enough to be a phrase.

**REFERENCES**

- 6.2.3 Authentication Facts

q\_authent\_know\_01\_secp7.question.fex

**Question 9:**  Incorrect

You want to ensure that all users in the Development OU have a common set of network communication security settings applied.

Which action should you take?

- Create a GPO folder policy for the folders containing the files.
-   Create a GPO computer policy for the computers in the Development OU.
- Create a GPO computer policy for the Computers container.
- Create a GPO user policy for the Development OU.

**EXPLANATION**

Network communication security settings are configured in the Computer Policies section of a GPO.

Built-in containers (such as the Computers container) and folders cannot be linked to a GPO.

**REFERENCES**

-  6.5.9 Group Policy Facts

q\_gpo\_computer\_01\_secp7.question.fex

**Question 10:** ✓ Correct

What is the process of controlling access to resources such as computers, files, or printers called?

- Conditional access
- Authentication
- Authorization
- Mandatory access control

**EXPLANATION**

Authorization is the process of controlling access to resources such as computers, files, or printers.

Mandatory access control (MAC) is an access control system based on classifications of subjects and objects to define and control access.

Conditional access is a way to enforce access control while also encouraging users to be productive wherever they are.

Authentication is the verification of the issued identification credentials.

**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\_authorize\_authorize\_secp7.question.fex

**Question 11:** ✓ Correct

Which of the following utilities could you use to lock a user account? (Select two.)

- userdel**
- usermod**
- useradd**
- ulimit**
- passwd**

**EXPLANATION**

Use the following utilities to lock a user account:

- **passwd -l** disables (locks) an account. This command inserts !! before the password in the /etc/shadow file.
- **usermod -L** disables (locks) an account. This command inserts ! before the password in the /etc/shadow file.

The **useradd** command creates new user accounts, and **userdel** deletes user accounts from the system.

The **ulimit** command is used to limit computer resources.

**REFERENCES**

-  6.7.3 Linux User Commands and Files

q\_linux\_usr\_cmd\_lockout\_02\_secp7.question.fex

**Question 12:**

✓ Correct

Which **chage** option keeps a user from changing their password every two weeks?

- W 33
- -m 33
- M 33
- a 33

**EXPLANATION**

Using **chage -m 33** forces a user to keep his or her password for 33 days. This sets the minimum number of days that must pass after a password change before a user can change the password again. Be aware of the other **chage** options:

- -M sets the maximum number of days before the password expires.
- -W sets the number of days before the password expires that a warning message displays.

The **chage -a** option is not a valid option.

**REFERENCES**

-  6.7.12 Linux User Security and Restriction Facts

q\_linux\_sec\_reuse\_secp7.question.fex

**Question 13:** ✓ Correct

You are teaching new users about security and passwords.

Which of the following is the BEST example of a secure password?

- 8181952
- JoHnSmITh
- Stiles\_2031
- T1a73gZ9!

**EXPLANATION**

The most secure password is T1a73gZ9! because it is eight or more characters in length and combines uppercase and lowercase characters, special symbols, and numbers.

The least secure password is 8181952 because it appears to be a birthday. JoHnSmITh is not secure because it is still a name. Stiles\_2031 is more secure but not as secure as random numbers and letters.

**REFERENCES**

-  6.6.9 Hardening Authentication Facts

q\_harden\_auth\_complex\_03\_secp7.question.fex

**Question 14:** ✓ Correct

Which of the following commands is used to change the current group ID during a login session?

- newgrp**
- usermod**
- groupmod**
- groups**

**EXPLANATION**

The **newgrp** command is used to change the current group ID during a login session. If the optional -f flag is given, the user's environment is reinitialized as though the user had logged in. Otherwise, the current environment (including the current working directory) remains unchanged. You can use this when working in a directory in which all the files must have the same group ownership.

The **usermod** command modifies group membership for a user account.

The **groups** command displays the primary and secondary group membership for the specified user account.

The **groupmod** command modifies the existing group.

**REFERENCES**

-  6.8.2 Linux Group Commands

q\_linux\_grps\_cmds\_newgrp\_secp7.question.fex

**Question 15:** ✓ Correct

RADIUS is primarily used for what purpose?

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

**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 16:**

✓ Correct

John, a user, is attempting to install an application but receives an error that he has insufficient privileges. Which of the following is the MOST likely cause?

- John has a local standard user account.
- John has a local administrator account.
- John needs to log in with a Microsoft account.
- The application is not a valid Windows application.

**EXPLANATION**

If John is receiving an error that he has insufficient privileges to install an application, the most likely cause is that he has a local standard user account. Standard users have limited permissions. For example, standard users:

- Can use applications (but they cannot install them)
- Can change some settings that apply only to them
- Cannot run applications in an elevated state

John is not a local administrator, as he would not receive an error message in that case.

The application is a valid Windows application, otherwise the installation would not be able to start.

Logging in with a Microsoft account would not give John the privileges to install an application.

**REFERENCES**

-  6.4.2 Windows Operating System Roles Facts

q\_win\_osroles\_user\_secp7.question.fex

**Question 17:**  Incorrect

Which of the following identifies the type of access that is allowed or denied for an object?

- User rights
- DACL
- SACL
-   Permissions

**EXPLANATION**

Permissions define the rights and access users and groups have with objects. Permissions are applied to objects such as files and folders.

A discretionary access control list (DACL) is an implementation of discretionary access control (DAC).

On a Microsoft system, a user right is a privilege or action that can be taken on a system, such as logging on, shutting down, backing up the system, or modifying the system date and time.

A system access control list (SACL) is used by Microsoft for auditing in order to identify past actions performed by users on an object.

**REFERENCES**

-  6.3.3 Authorization Facts

q\_authorize\_permission\_secp7.question.fex

**Question 18:** ✓ Correct

What should you do to a user account if the user goes on an extended vacation?

- ➔ **Disable the account**
- Remove all rights from the account
- Delete the account
- Monitor the account more closely

**EXPLANATION**

Disabling the account is the best measure to protect an inactive account. This prevents the account from being used for login.

If you delete the account or the rights assigned to the account, you have to re-create the account or the rights when the user returns. Leaving the account active might expose it to attack, even if you regularly monitor it.

**REFERENCES**

- 6.5.4 Active Directory Facts

q\_actdir\_user\_01\_secp7.question.fex

**Question 19:** ✓ 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.

The screenshot shows the Windows Credential Manager interface. At the top, there is a header with the title 'Manage your credentials' and a sub-instruction 'View and delete your saved logon information for websites, connected applications and networks.' Below the header, there is a large, empty rectangular area with a blue border. To the left of this area, there is a teal-colored arrow pointing towards it. Below this area, the text 'Windows Credentials' is displayed. Underneath, there is a list entry for 'KIMSPC'. To the right of 'KIMSPC', the text 'Modified: Today' is followed by a dropdown arrow icon. The entire interface has a clean, modern design with a white background and light gray borders.

**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

**Question 20:** ✓ Correct

Group Policy Objects (GPOs) are applied in which of the following orders?

GPO linked to site, GPO linked to domain, GPO linked to organizational unit (highest to lowest), Local Group Policy.

→  Local Group Policy, GPO linked to site, GPO linked to domain, GPO linked to organizational unit (highest to lowest).

GPO linked to site, GPO linked to domain, GPO linked to organizational unit (lowest to highest), Local Group Policy.

Local Group Policy, GPO linked to site, GPO linked to domain, GPO linked to organizational unit (lowest to highest).

**EXPLANATION**

Group Policy Objects (GPOs) are applied in the following order:

- The Local Group Policy on the computer.
- GPOs linked to the site.
- GPOs linked to the domain that contains the User or Computer object.
- GPOs linked to the organizational unit (OU) that contains the User or Computer object (from the highest-level OU to the lowest-level OU).

**REFERENCES**

 6.5.9 Group Policy Facts

q\_gpo\_order\_02\_secp7.question.fex

**Question 21:** ✓ Correct

To answer this question, complete the lab using the information below.

 **You have already answered this question.**  
**You are not allowed to view the lab again.**

[Launch Lab](#)

You completed the lab correctly.

[Loading](#)**REFERENCES**

-  6.7.4 Create a User Account
-  6.7.5 Rename a User Account
-  6.8.3 Rename and Create Groups
-  6.8.4 Add Users to a Group
-  6.8.5 Remove a User from a Group

175d362d-220d-429b-8e55-b69bcf53e5fc

**Question 22:**

✓ Correct

You have just configured the password policy and set the minimum password age to 10.

What is the effect of this configuration?

- Users must change the password at least every 10 days.
- The previous 10 passwords cannot be reused.
- The password must be entered within 10 minutes of the login prompt being displayed.
-   **Users cannot change the password for 10 days.**
- The password must contain 10 or more characters.

**EXPLANATION**

The minimum password age setting prevents users from changing the password too frequently. After the password is changed, it cannot be changed again for at least 10 days.

The maximum password age setting determines how frequently a password must be changed. The minimum password length setting controls the minimum number of characters that must be in the password. Password history is used to prevent previous passwords from being reused.

**REFERENCES**

-  6.6.9 Hardening Authentication Facts

q\_harden\_auth\_reuse\_secp7.question.fex

**Question 23:**  Incorrect

To answer this question, complete the lab using the information below.

**Launch Lab****You did not attempt the lab.****REFERENCES**

-  6.7.4 Create a User Account
-  6.7.5 Rename a User Account
-  6.7.6 Delete a User
-  6.8.3 Rename and Create Groups
-  6.8.4 Add Users to a Group

b637326b-55a2-4b2e-a1e0-d07ae79429a0

**Question 24:** ✓ Correct

Which of the following commands creates a new group and defines the group password?

- groupadd -g**
- groupadd -r**
- groupadd -p**
- groupadd -c**

**EXPLANATION**

The **groupadd -p** command creates a new group while defining the group password.

The **groupadd -g** command creates a new group while defining the GUID.

The **groupadd -r** command creates a new system group.

The **groupadd -c** command is not a valid command.

**REFERENCES**

-  [6.8.2 Linux Group Commands](#)

q\_linux\_grps\_cmds\_groupadd\_secp7.question.fex

**Question 25:** ✓ Correct

An employee named Bob Smith, whose username is bsmith, has left the company. You have been instructed to delete his user account and home directory.

Which of the following commands would produce the required outcome? (Select two.)

- ➡  **userdel bsmith;rm -rf /home-bsmith**
- userdel -x bsmith**
- userdel -h bsmith**
- userdel bsmith**
- ➡  **userdel -r bsmith**

**EXPLANATION**

The **userdel -r** command deletes a user's home directory and user account. The **userdel** command by itself does not delete a user's home directory and user account. Executing **rm -rf** on the user's home directory after executing **userdel** removes the home directory. The **userdel -h** command displays the syntax and options for the **userdel** command.

**REFERENCES**

-  6.7.3 Linux User Commands and Files

q\_linux\_usr\_cmds\_user\_02\_secp7.question.fex

**Question 26:**

✓ Correct

What is the MOST important aspect of a biometric device?

- Size of the reference profile
- Enrollment time
- Throughput
- Accuracy

**EXPLANATION**

The most important aspect of a biometric device is accuracy. If an access control device is not accurate, it does not offer reliable security.

Enrollment time is how long it takes for a new user to be defined in the biometric database. Typically, an enrollment time less than two minutes is preferred. The size of the reference profile is irrelevant in most situations. Throughput is how many users a biometric device can scan and verify within a given time period. Typically, a throughput of 10 users per minute is preferred.

**REFERENCES**

-  6.2.7 Biometrics and Authentication Technologies Facts

q\_sso\_biometrics\_02\_secp7.question.fex

**Question 27:** ✓ Correct

Which of the following is an example of rule-based access control?

- Router access control lists that allow or deny traffic based on the characteristics of an IP packet.
- A computer file owner who grants access to the file by adding other users to an access control list.
- A member of the accounting team that is given access to the accounting department documents.
- A subject with a government clearance that allows access to government classification labels of Confidential, Secret, and Top Secret.

**EXPLANATION**

A router access control list that allows or denies traffic based on the characteristics of an IP packet is an example of rule-based access control.

A subject with a government clearance that allows access to government classification labels of Confidential, Secret, and Top Secret is an example of mandatory access control.

A member of the accounting team that is given access to the accounting department documents is an example of role-based access control.

A computer file owner who grants access to the file by adding other users to an access control list is an example of discretionary access control.

**REFERENCES**

-  6.1.6 Access Control Model Facts

q\_acc\_models\_rule\_secp7.question.fex

**Question 28:**  Incorrect

You want to make sure that all users have passwords over eight characters in length and that passwords must be changed every 30 days.

What should you do?

- Configure day/time settings in user accounts
-   **Configure account policies in Group Policy**
- Configure expiration settings in user accounts
- ~~Configure account lockout policies in Group Policy~~

**EXPLANATION**

Configure account (password) policies in Group Policy to enforce rules about the composition of passwords, such as minimum length, complexity, and history requirements.

Use account expiration in a user account to disable an account after a specific day. Use day/time restrictions to prevent login during certain days or hours. Account lockout disables a user account after a specified number of incorrect login attempts.

**REFERENCES**

-  6.6.9 Hardening Authentication Facts

q\_harden\_auth\_complex\_01\_secp7.question.fex

**Question 29:** ✓ Correct

A remote access user needs to gain access to resources on the server. Which of the following processes are performed by the remote access server to control access to resources?

- Authorization and accounting
- Authentication and authorization
- Identity proofing and authorization
- Identity proofing and authentication
- Authentication and accounting

**EXPLANATION**

A remote access server performs the following functions:

- Authentication is the process of proving identity. After devices agree on the authentication protocol to use, the login credentials are exchanged and login is allowed or denied.
- 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.

Accounting is an activity that tracks or logs the use of the remote access connection. Accounting is used to keep track of resource use but is not typically used to control resource use. If access is allowed or denied based on time limits, information provided by accounting might be used by authorization rules to allow or deny access.

Identification is the initial process of confirming the identity of a user requesting credentials and occurs when a user types in a user ID to log on.

Identity proofing occurs during the identification phase as the user proves that they are who they say they are in order to obtain credentials.

**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\_acct\_ctrl\_authentication\_01\_secp7.question.fex

**Question 30:** ✓ Correct

Which of the following commands removes a user from all secondary group memberships?

- usermod -g**
- usermod -G ""**
- usermod -G**
- usermod -aG**

**EXPLANATION**

**usermod - G ""** removes the user from all secondary group memberships. Do not include a space between the quotes.

**usermod -g** assigns a user to a primary group.

**usermod -G** assigns a user to a secondary group.

**usermod -aG** assigns a user to a secondary group (or groups) by appending the group to any which the user already belongs to. Follow the command with a comma-separated list of groups.

**REFERENCES**

-  [6.8.2 Linux Group Commands](#)

q\_linux\_grps\_cmds\_remove\_secp7.question.fex

**Question 31:** ✓ Correct

Which of the following terms is used to describe an event in which a person who should be allowed access is denied access to a system?

- False positive
- False acceptance
- False negative
- Error rate

**EXPLANATION**

A false negative occurs when a person who should be allowed access is denied access.

A false positive occurs when a person who should be denied access is allowed access.

The processing rate, or system throughput, identifies the number of subjects or authentication attempts that can be validated.

The crossover error rate, also called the equal error rate, is the point where the number of false positives matches the number of false negatives in a biometric system.

**REFERENCES**

-  6.2.7 Biometrics and Authentication Technologies Facts

q\_sso\_false\_rej\_secp7.question.fex

**Question 32:** ✓ Correct

Which of the following is used for identification?

- PIN
- Cognitive question
- Password
- Username

**EXPLANATION**

Identification is the initial process of confirming the identity of a user requesting credentials and occurs when a user types in a user ID to log on. The username is used for identification, while a password, PIN, or some other cognitive information is used for authentication.

Authentication is the verification of the issued identification credentials. It is usually the second step after identification and establishes the user's identity, ensuring that users are who they say they are.

**REFERENCES**

-  6.1.3 Access Control Facts

q\_acct\_ctrl\_identification\_secp7.question.fex

**Question 33:**

✓ 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 34:** ✓ Correct

You manage a single domain named widgets.com.

Organizational units (OUs) have been created for each company department. User and computer accounts have been moved into their corresponding OUs. Members of the Directors OU want to enforce longer passwords than are required for the rest of the users.

You define a new granular password policy with the required settings. All users in the Directors OU are currently members of the DirectorsGG group, which is a global security group in that OU. You apply the new password policy to that group. Matt Barnes is the chief financial officer, and he would like his account to have even more strict password policies than are required for other members in the Directors OU.

What should you do?

- Create a granular password policy for Matt. Apply the new policy directly to Matt's user account.
- Create a granular password policy for Matt. Apply the new policy directly to Matt's user account. Remove Matt from the DirectorsGG group.
- Create a granular password policy for Matt. Create a new group, make Matt a member of the group, and then apply the new policy directly to the new group. Make sure the new policy has a higher precedence value than the value for the existing policy.
- Edit the existing password policy. Define exceptions for the required settings. Apply the exceptions to Matt's user account.

**EXPLANATION**

To use a different set of policies for a specific user, create a Password Settings Object (PSO) for the user and apply it directly to the user account. If a PSO has been applied directly to a user, that PSO is in effect regardless of the precedence value.

You could create a second group only for Matt's account and password policy. However, this policy must have a lower precedence value than the value set for the policy applied to the DirectorsGG group. Removing Matt's account from the DirectorsGG group is unnecessary and would probably affect his permissions to network resources.

**REFERENCES**

-  [6.6.12 Smart Card Authentication Facts](#)

q\_smartcard\_auth\_complex\_02\_secp7.question.fex

**Question 35:** ✓ Correct

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

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

**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 36:**  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 37:** ✓ 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 38:** ✓ Correct

Which networking model is based on peer-to-peer networking?

- None
- Client-server
- Workgroup
- Standalone

**EXPLANATION**

A workgroup model is based on peer-to-peer networking. In the workgroup model:

- No hosts in a workgroup have a specific role.
  - All hosts can function as both workstation and server.
  - All hosts in a workgroup can provide network services or consume network services.
- Hosts are linked together by some type of local network connection.
- Hosts in the same workgroup can access shared resources on other hosts.
- No specialized software is required.

In a standalone model, each Windows system functions independently of other systems.

In the client-server model, each host has a specific role in the network. Servers provide services such as file storage, user management, security configuration, and printing. Clients request services from servers.

**REFERENCES**

-  6.4.2 Windows Operating System Roles Facts

q\_win\_osroles\_peer\_secp7.question.fex

**Question 39:**

✓ Correct

You are consulting a small startup company that needs to know which kind of Windows computer network model they should implement.

The company intends to start small with only 12 employees, but they plan to double or triple in size within 12 months. The company founders want to make sure they are prepared for growth.

Which networking model should they implement?

- Standalone
- Wireless
- Workgroup
- Client-server
- Public
- Wired

**EXPLANATION**

This startup company should invest in a client-server network if they want to be prepared to double or triple in size within 12 months. A client-server network that uses Active Directory as a centralized database to manage network resources is the most scalable networking model.

The workgroup (peer-to-peer) networking model would be less expensive and easier to set up for a dozen employees, but it would become too difficult to manage when the company increases in size.

The standalone networking model would not connect the company's computers to each other. Employees would not be able to share any resources, such as printers or data storage.

Wired and wireless networks are not networking models. These network configurations provide connectivity between computers and can be used for any of the networking models.

A public network, such as the internet, would be the only way computers using the standalone networking model could communicate with each other.

**REFERENCES**

-  6.4.2 Windows Operating System Roles Facts

q\_win\_osroles\_client\_secp7.question.fex

**Question 40:**

✓ Correct

You have performed an audit and found an active account for an employee with the username *joer*. This user no longer works for the company.

Which command can you use to disable this account?

- usermod -d joer**
- usermod -l joer**
- usermod -u joer**
- usermod -L joer**

**EXPLANATION**

Use **usermod -L joer** to lock the user's password. Doing so disables the account.

The **usermod -l joer** command changes the account's login name.

The **-d** flag is used for changing the account's home directory.

The **-u** flag is used for changing the account's numeric ID.

**REFERENCES**

-  6.7.3 Linux User Commands and Files

q\_linux\_usr\_cmds\_audit\_secp7.question.fex

**Question 41:** ✓ Correct

What is the primary purpose of separation of duties?

- ➡  Prevent conflicts of interest
- Increase the difficulty of performing administrative duties
- Inform managers that they are not trusted
- Grant a greater range of control to senior management

**EXPLANATION**

The primary purpose of separation of duties is to prevent conflicts of interest by dividing administrative powers between several trusted administrators. This prevents a single person from having all of the privileges over an environment, which would create a primary target for attack and a single point of failure.

Increasing administrative difficulty, informing managers that they are not trusted, or granting a greater range of control to senior management are not the primary purposes of separation of duties. Separation of duties might seem to increase administrative difficulty, but this separation provides significant security benefits. A manager is informed they are not trusted when they are not given any responsibility as opposed to a reasonable portion of responsibility. Senior management already has full control over their organization.

**REFERENCES**

-  6.1.4 Access Control Best Practices

q\_acct\_bstpract\_separate\_03\_secp7.question.fex