You have been asked to select the proper type of protocol to implement in order to grant access to remote users. The protocol should use separate and multiple challenges and responses for each of the authentication, authorization, and auditing functions. Which of the following should you select?

RADIUS

TACACS+

LDAP

Active Directory

Answer: B

Explanation: TACACS+ is the only one listed that supports separate functions for authentication and authorization of remote users.

Which authentication technology utilizes a key distribution center (KDC)?

EAP

RADIUS

Kerberos

TACACS+

Answer: C

Explanation: The Domain Controller in a Windows network serves as the key distribution center. This is the device that will issue the tickets to clients once they are authenticated using the Kerberos protocol.

During a recent vulnerability scan, you found that your domain controller is not transmitting its information over a secure port since SSL was not enabled. You have just enabled SSL and need to open the port in the server’s host-based firewall to allow communications to occur over the newly-created secure path. Which port should you open on the firewall?

636

443

3389

389

Answer: A

Explanation: A domain controller or directory service (such as Active Directory in Windows and LDAP in Linux) utilizes port 389 when transmitting without an SSL (Secure) connection. When SSL is enabled, you should use port 636 for a secure LDAP connection by default.