Lesson 6

Security Planning and Administrative Delegation

Matching

Match the following definitions with the appropriate term.

a. Active Directory Migration Tool f. password-cracking

b. Delegation of Control Wizard g. personal identification number (PIN)

c. dictionary attack h. runas

d. drag-and-drop i. Secondary Logon

e. dsmove j. strong password

\_\_\_\_\_\_\_ 1. This service is required to use the runas feature. I P129

\_\_\_\_\_\_\_ 2. This command-line tool can be used to move an object from one OU to another. [e] P135

\_\_\_\_\_\_\_ 3. This tool is used to move objects from one domain to another. [a] P134

\_\_\_\_\_\_\_ 4. Hackers will use this attack to identify a user's password by trying numerous words and word combinations until they find a match. [c] P127

\_\_\_\_\_\_\_ 5. When you create this item do not use words from the dictionary. [j] P127

\_\_\_\_\_\_\_ 6. This can be used to run a single command using administrative privileges while logging onto a workstation or server using a Domain User account. [h] P129

\_\_\_\_\_\_\_ 7. This can be used for authentication in lieu of a password when used with an ATM or a smart card. [g] P127

\_\_\_\_\_\_\_ 8. Use this tool to grant authority to a user or group of users over a portion of the Active Directory tree. [b] P131

\_\_\_\_\_\_\_ 9. This method of moving objects from one OU to another was introduced in Windows Server 2003. [d] P134

\_\_\_\_\_\_\_ 10. A dictionary attack is one type of this attack. [f] P127

Multiple Choice

1. Which interface allows you to grant limited permissions within Active Directory to individual users or groups to adhere to a principle of least privilege in administering Active Directory?

a. Delegation of Authority Wizard

b. Delegation of Control Wizard

c. Control Wizard

d. Authority Wizard

The Delegation of Control Wizard within the Active Directory Users and Computers MMC snap-in allows you to delegate permissions to perform a number of preconfigured tasks, as well as create custom tasks to be delegated. P134

2. Which program allows you to use the Secondary Logon service to launch individual programs and utilities using administrative privileges?

a. Runas

b. Wscript

c. Cscript

d. Secwiz

You can run a program using alternate credentials from the GUI by using the right-click context menu or from the command line by using runas.exe. P129

3. Which command-line utility can be used to move an Active Directory object from one container to another?

a. Dsget

b. Dsrm

c. Dsmove

d. Admt

Use the dsmove.exe utility to quickly and efficiently move Active Directory objects from a command prompt or within a script. P135

4. What is a numeric or alphanumeric character sequence that you enter with a smart card to access a server or other Active Directory resource?

a. Personal Identification Number (PIN)

b. Password Identification Number (PIN)

c. Smart card password

d. Smart card identifier

When the necessary PKI infrastructure has been deployed, you can deploy smart card devices that can be used with a PIN to enable two-factor authentication in an Active Directory environment. P127

5. What is a password that has sufficient length and complexity that it is difficult for a hacker or other malicious user to hack?

a. Long password

b. Smart card password

c. Strong password

d. Personal identification password

A strong password is one that is created adhering to a minimum password length and is of a sufficient complexity that it is resistant to password-cracking attacks. P127

6. Which service enables you to use the runas command-line utility?

a. Secondary Service

b. Secondary Logon

c. Runas Service

d. Alternate Credentials Service

The Secondary Logon service in Windows allows you to use runas or the Run as administrator GUI option to launch individual executables using alternate credentials. P129

7. What is the recommended method for moving Active Directory objects from one domain to another?

a. Movetree.exe

b. Dsmove

c. Active Directory Migration Tool (ADMT)

d. Drag-and-drop

When moving objects from one Active Directory domain to another, the supported mechanism is the Active Directory Migration Tool (ADMT), a free download from the Microsoft Website. P134

8. Which password-cracking attack functions by attempting every possible combination of alphanumeric characters until it finds a match?

a. Trojan horse

b. Dictionary attack

c. Rootkit

d. Boot virus

A dictionary attack is an automated password-cracking tool. Its effectiveness can be minimized by the use of strong passwords that are changed on a regular basis. P127

9. What is a new GUI option in Windows Server 2008 and Windows Vista that allows you to launch a specific application using elevated privileges?

a. Delegation of Control Wizard

b. Active Directory Administrative Credentials

c. Run as Administrator

d. Delegation of Privilege Wizard

Windows Server 2008 and Windows Vista gives you the ability to right-click a particular program and select Run as administrator, which allows you to log on to a computer as a non-administrative user and elevate your privileges only when it is specifically required. P129

10. With a username, what is needed to access network resources in a default Active Directory environment?

a. Password

b. Access Token

c. Smart card

d. PIN

In a default Active Directory environment, logons are processed using a username and password combination. In an environment where smart card authentication has been enabled, this can be supplemented or replaced by the use of smart cards and PINs, but this capability is not present in an out-of-the-box Active Directory installation. P127

Case Scenarios

Case Scenario 6-1: Planning Active Directory for Contoso Pharmaceuticals

You are a consultant working with Contoso Pharmaceuticals to assist them in planning their Active Directory infrastructure. Contoso Pharmaceuticals is a medical research and experimental drug company that participates in government projects. The information on the company's network is very sensitive and, therefore, security is the CEO's primary concern. The plan that is implemented should have the strongest precautions against attacks from the outside.

The company currently is using a Microsoft Windows 2000 domain and will be transitioning to Active Directory with the migration of their network to Windows Server 2008. The company has a single domain and will be expanding to include a single forest and one domain for each of its five locations when the new network is installed. An administrator has been designated for each location. In addition, the accounting and human resource departments, which are located at the main site, want to be able to manage their own containers.

a. Based on this scenario, should administration be centralized or decentralized? Explain.

Decentralized administration is called for in this scenario, because each location has a dedicated administrator and each site is configured as a separate domain.

b. How will you achieve the goal set forth by the accounting and human resource departments?

Use the Delegation of Control wizard to grant control of the containers in question to the HR and Accounting departments.

c. What will you propose for a secure logon method?

Implement two-factor authentication such as smart cards to protect access to sensitive data.