lab assessment questions and answers

1. Define why change control management is relevant to security operations in an organization.

Change control is a precision arrangement of managing every change made to a system. This is to ensure that no unneeded changes are done, that every change is documented, and that no service is disrupted unless absolutely necessary, and that all resources efficiently used.

2. What type of access control system uses security labels?

A LBA C Label Base Access Control

3. Describe two options you would enable in a Windows Domain password policy.

Password must meet complexity requirements Minimum Password length

4. Where would patch management and software updates fall under in security operations and management?

Procedures/ The SA or other personnel to be the responsible authority in informing all local authorities about patches that are related to software packages included on the entire inventory of the organizations software.

Also in Procedures/ Additionally, any post-patch update distributions to the Database/Management Configuration Plan will be executed immediately after any patching has been done.

5. Is there a setting in your GPO to specify how many logon attempts will lock out an account?

Yes, The Account Lockout Threshold can be set, this policy determines the number of failed attempts to logon, before the users' account becomes locked. Once locked, it can not be used unless it is reset by an Administrator, or until the accounts lockout duration expires. A value of up to 999 failed logon attempts can be set, or you may set the value to zero, to allow the account to never be locked out.

Name two parameters that you can set to enhance the access control to the system.

Account Policies/ Password must meet Complexity Requirements. Also in Account Policies/ Account Lockout Threshold

6. What are some password policy parameter options you can define for GPOs that can enhance the CIA for system access?

Account Policies/Password Policies/ Enforce Password History. Also in Account Policies/Password Policies/ Maximum Password Age. Also in Account Policies/Password Policies/ Minimum Password Age. Also in Account Policies/Password Policies/ Minimum Password Length. Also in Account Policies/Password Policies/ Password Must Meet Complexity Requirements

7. What sources could you use as a source to perform the MBSA security state?

You can direct the MBSA either to use the Microsoft Update Live Service, a Windows Server Update Services (WSUS) server, or an Offline catalogue as the missing security updates source instead.

8. What does WSUS stand for, The WSUS or Windows Server Update is a free management tool for patches, and available to all Administrators of Window’s Servers.

The WSUS allows these administrators to authorize, publish & distribute updates throughout their networks. And what does it do?

It is imperative that Administrators keep their Networks safe & Secure. Instead of each and every workstation manually connecting to Microsoft updates, Administrators can employ WSUS to download updates centrally to an internal server in their network. Once the WSUS authorizes them, they are deployed to their internal locations. Then, Reporting tools assist and keep the Administrators informed about the progresses of their patch(s). This is an extremely efficient technique of establishing full control on all controls concerning network workstations.

9. What is the difference between MBSA and Microsoft® Update?

Microsoft Update is a site on the Internet that scans a lone computer and then will display updates that are missing or needed, then will install them a group, just as long as the computer has internet access, and can access the Microsoft site on the web of webs.

Adversely, the MBSA allows the scanning of multiple computers for missing or needed updates, all at one time by a remote scan. This is regardless if the target computers have Internet access and/or can reach the Microsoft Update site on the web.