Test – Learning Design

This evaluation contains 2 parts:

1. Review the following script and suggest improvements with respect to:

Content flow: Identify content flow issues, redundancies

Language: Spelling and grammar, rephrase/rewrite sentences for clarity and brevity, where required

Any other changes

(You can turn on TRACK CHANGES option before you begin).

* **Introduction:**

Let’s recall the basic concept covered in the previous lesson, wherein users need to reveal their identity along with the proof for being authenticated to access a network as well as being authorized to access the desired resources.

However, I would like to ask a small question here: Is this all we have to do to ensure complete security?

Is your answer ‘yes’? Apparently, your answer might be ‘yes’. I have some counter statements that would actually question your confident answer.

* What about security if the user cannot login just because she or he has forgotten the password? Don’t you think that security shall be breached if the solution to this issue is to write down passwords on paper? Even if you try the ‘forgot password option’, what if users try one of the previously used passwords or some very easy to remember secret phrase such as birth date or name?
* Then, what about security if a user sticks to only a single password for months? Doesn’t this increase the risk of password cracking?
* Next, what about security if anyone else other than the genuine user tries to login by entering username and password repeatedly and succeed in doing so?
* Similarly, what about security if an administrator performs both administrative and reviewing tasks using just a single set of credentials?
* Further, what about security if two or more users are sharing a single guest account for accessing common resources such as a network printer?
* Finally, what about security if the credentials of a user who has left the company is still being accepted for logging onto the internal network?

Well, these questions simply tell us that authentication and authorization are not enough to ensure 100% security. As a system administrator, you will have to take more actions by managing user accounts or credentials. This is perhaps in the form of user account policies dictating credential or account usage rules for best practices. Regular updating of the same is mandatory.

The access levels of a user have a direct impact on the level of network protection. Although it may sound a bit odd that the network needs protection from its own users, it is also a fact that these internal users have maximum rights and privileges, sufficient to disrupt deliberately or misuse it’s resources even accidentally. Upon logon, revealing a rule or statement that the access is granted if a few conditions are fulfilled or that your activities are monitored which helps following security policy protocols or policies and obtain legal ramifications.

So, let us begin this lesson by discussing these best practices or policies for managing user accounts which all users must agree upon after a fair discussion and understanding of their benefits.

* **Learning Outcome:**

After completing this lesson, you will be able to:

* Mitigate issues associated with users with multiple accounts/roles and/or shared accounts.
* Enforce different account policy settings for securing the system.
* Apply privileges to groups and individual users for access control monitoring.
* Describe the significance of reviewing and continuous monitoring what the user actually accesses through the system.

**Topic – 1:**

In the first topic, we will discuss the issues associated with users with multiple accounts or roles, and/or shared accounts.

In most organizations, it is common to have several users operating with several capacities. The most common example is of an administrator who usually has two accounts namely, administrator and standard. So, what is the issue here? Well, the issue can be the administrator, intentionally or unintentionally, may use the administrative account when it is not supposed to be used, for example, for browsing the Internet.

Therefore, the best practice is to use the standard account for daily mundane tasks, while the administrator’s account having special privileges must be used for special administrator functions. Doing so forces the user to use the right account for doing the related task. It also restricts the time for which a highly privileged account is in use as well as prevents from using it at the time of higher security breach or data loss such as while browsing the Internet or doing general file transfers.

* **Conclusion:**

In short, such distinction limits the span of operation for each of their accounts and reduce security breach. A good real-life example of such use of accounts are the pseudo or superuser-do-command that Linux users use to perform administrative tasks from their session account.