Technical Writing Prompt - Tevora

Dear Adrina,

In response to your prompt, I have listed the following vulnerabilities, the details about the risk, and their remediation steps.



After examining the above output, I have noticed three very important vulnerabilities that could cause major complications and damage to any company if left unchecked.

**Vulnerability Number 1: Use of “Root Account”**

The use of the “root” account in any environment can pose dangers for a variety of reasons. The most important reason is that although root can be used for administrative tasks and purposes, it poses the potential danger of being left open indefinitely, exposing the business to a privilege escalation attack. This allows any threat the ability to access, delete, and modify every account regardless of status. Instead of using the “root” command or account, a user account should be created using the “sudo” command, which allows users to execute their password for authentication by default. It does not give “root” privileges, rather it runs the program or command with elevated privileges. In addition to the ability of using elevated or root privileges, the ID of every “sudo”-utilizing user can be logged.

**Vulnerability Number 2: Account Password Changes**

While examining the output, I came across this string of numbers: “***15651***”. This number stands for the days that the account has been active since the password was last changed. This is very dangerous as this means the account has been active with the same password for more than 42 years! In a corporate environment, this poses a danger to the company as various users may have been in this role over the course of 40 years, and all of the prior users holding the credentials to this account still have access to the account. Failure to correct this can result in unauthorized access to databases and other data, and possibly the leakage of said data. This can be corrected by first changing the password on the account as soon as possible, within compliance of password policy. After this is completed, after each associate holding the password leaves the company or changes roles, the account needs to be locked and the password changed immediately.

**Vulnerability Number 3: Maximum Password Age**

After examining the first output string of “15651”, there was another string of numbers: “***99999***”. This number stands for the maximum number of days the password is active. This can prove to be very dangerous as the password will never expire, meaning that as soon as a threat gains access to this password (possibly by means of the “root” command and account access), he now has unlimited access to log into the system free of detection for as long as he or she needs. This can be remediated by implementing a maximum password age such as every 90 to 180 days. This prevents stored passwords from being frequently used, as well as keeps a consistent schedule of fresh passwords.