**Group 3**

**11/22/2017**

**IT 310 – 41**

**10 – 1 Case Project**

As shown by the audit, the lack of standardized password policies has opened the bank to many avenues of password security vulnerability. Before the password security and account lockout policies can be set, proper site, domain, OU, or local computer groups must be established. Assuming that the groups has been constructed properly to link new Account policy, we can proceed with opening Group Policy to enact the proper fixes to ensure audit compliance. I will break down the corrections by found discrepancies below (All changes will be performed by opening the Under the Group Policy Management Editor for the specific group that requires the change)

* Some bank employees have used the same user account password for years:
  + Setting the maximum password age. Configure the maximum time allowed until a password expires.
  + Recommended settings: Around 30-45 days or depending on company needs.
* Many of the existing passwords are only four or five characters in length:
  + Setting the minimum password length. Sets a minimum amount of characters required for a user to make a “good” password.
  + Recommend settings: 8+ characters are fine, and use of complexity requirements available in GPME.
* Several bank employees regularly change their passwords but rotate between the same three or four passwords with each change
  + Setting the Enforce password history. Requires users to choose new passwords when a password change is made. The system remembers old passwords and rejects the same, or similar password if it’s been used before.
* An employee who has forgotten a password can keep trying different combinations for as long as they like, until they hit upon the password or give up trying.
  + - Like the Password Policy, Account Lockout Policies can be set under the Account Policies sub settings. An administrator can set the following:
* Account lockout duration. Specifies in minutes how long the system will keep the account locked out after the set number of unsuccessful attempts.
* Recommended settings: 30 minutes.
* Account lockout threshold. Used in conjunction with Duration, this sets a limit of unsuccessful attempts to sign in to an account.
* Recommended settings: Three attempts.
* Reset account lockout count after. Specifies the number of minutes to wait after EVERY single unsuccessful login before the logon counter is reinitialized.

Recommended settings: Per Microsoft “Determine the treat level of your organization and balance that against the cost of your Help Desk support for password resets. Each organization will have specific requirements” (Technet – Reset account lockout count after)

**Case Project 11-3**

The monitor that we would use to monitor the activity of users in the inventory department to identify the gaming players would be the performance monitor. We would use the performance monitor because it monitors the CPU load and how long the CPU is at that load. It can also monitor how much memory the system is using, and along with monitoring the network bandwidth. If there is too much bandwidth going out of the network, or the CPU usage is too high for too long, or even too much memory is being used, a system administrator could be alerted to find out the outliers in the inventory network. The company could conduct several tests to set a baseline for expected bandwidth, CPU usage, and memory prior to running the monitors. These baselines once triggered would send the alerts to the system administrator.

Additionally, the Users tab in the Task Manager provides a comprehensive list of A, current users logged in, and B, the programs that are opened. The tab also displays CPU and memory usage by each program, divided into expanding and collapsible lists. You can also sign out users manually by clicking the Disconnect button, ensuring that open files are closed before the user is signed out.

**Case Project 12 - 1**

Troubleshooting Strategy

* Know how the network works by creating a diagram of the network
* Get as much information as possible about the problem
* Record the error message at the time it appears or when a user reports it to you
* Gather benchmarks
* Set up alerts when there is a security problem
* Have monitoring software for the network
* Keep logs of problems and solutions (Windows Server 2016 Event logs)
* Use Performance Monitor, Data Collector Sets, Task Manager, Server Manager, and the Computer Management tool to help troubleshoot the problem
* Define the problem
* Check for power interruptions
* Have a centralized way of detecting and alerting problems instead of looking at every event
* Determine possible solutions for the issue
* Define whether the best or most likely solution and which may be simple ones
* Determine negative user experience
* Once issue is corrected and a solution implemented, continue to monitor to ensure there is no further issues
* Train users to help detect problems

**Case Project 12 – 2**

Where would you look first for a clue about what happened?

The first place to look would be the event viewer after the server crashed. The event viewer is a storehouse of logs from which one can monitor a system and diagnose problems.

How would you explain the steps and tools you would use in handling the crash?

I would explain that I used the repair my computer options on the advanced boot options to access the recovery system and after looking through the event logs that I determined that this would be the best course of action.

Expanding on the above, the issue may be a result in software or driver reconfiguring. Using advanced options for booting (F8 on boot), you can access Safe Mode. This provides a generic environment to troubleshoot the server and possibly restoring the original page file or remove the component that adversely affected the server. If the problem isn’t found or can be repaired, the Last Known Good Configuration option can be used to restore the server to the last known point of successful startup. If this setting is used, be mindful that the probability of this issue returning is high unless divers issues were repaired or component conflicts corrected.

If it is truly a system disk crash, how can you restore the system?

If it truly was a system disk crash we can use image backups, which includes everything from when you made the backup. This would simply rollback anything that had happened back unto when the backup was made, if you make frequent image backups this shouldn’t be a problem.