**Tech Challenge #4**

**Audit Your Server**

In this tech challenge, you will perform the full systems administration audit of your server. Please provide a screenshot of each successfully completed step and provide descriptive answers to each relevant question. For each step I am looking for you to determine the best method of satisfying the required audit control (Hint: Use the posted reading materials). There may be multiple methods to satisfy the control. Extra credit will be given to any control that can be satisfied using the command line interface. I am looking for you to show me that you know how to satisfy each control, how you determined this, and why it is important as an audit control. Please provide any references you used.

1. Obtain the system information and service pack version, and compare with policy requirements.
	1. Why do you think Microsoft releases service packs?
	2. Why do you think Windows 10 was offered at no cost for a while?
2. Determine whether the server is running the company provisioned firewall
	1. Are there any built-in firewall products offered by Microsoft?
3. Determine whether the server is running a company-provisioned antivirus program
	1. Explain the difference between stand-alone anti-virus and end point anti-virus protection
4. Ensure that all approved patches are installed per your server management policy
	1. Why does software constantly need to be patched?
5. Determine whether the server is running a company-provisioned patch management solution. If so, show the history of the updates.
6. Review and verify startup information
7. Determine what services are enabled on the system and validate their necessity. Are all of the services necessary?
	1. How do you think enabled services affect performance?
8. Ensure that only approved applications are installed on the system per your server management policy.
	1. Are you able to install new software on your work pc? If so, did you have to request special permission? Why would your company want to prevent you from installing software?
9. Ensure that only approved scheduled tasks are running.
	1. What is a scheduled task? What are their purpose?
10. Review and evaluate procedures for creating user accounts and ensuring that accounts are created only when there’s a legitimate business need.
	1. Explain the difference between an active directory user account and local pc user account.
11. Ensure that all users are created at the domain level and clearly annotated in the active directory. Each user should trace to a specific team.
12. Review and evaluate the use of groups and determine the restrictiveness of their use.
13. Review and evaluate the strength of system passwords.
14. Evaluate the use of password controls on the server such as password aging, length, complexity, history and lockout policies.
15. Review and evaluate the use of user rights and security options assigned to the elements in the security policy settings.
16. Review and evaluate the use and need for remote access, including RAS connections, FTP, Telnet, SSH, VPN etc.
17. Review whether a legal warning banner is displayed when users connect to the system.
18. Look for and evaluate the use of shares on the host.
19. Ensure that the server has auditing enabled.
20. Review the system administrator procedures for monitoring the state of security on the system.

**Conclusion**

Please provide a brief summary of your findings. What did you discover about the server by performing these auditing steps? Why do you feel this type of process is necessary for organizations?