1) Create three user accounts: 20 Points

- Create a user account called SJ-Student and make it a general user account
- Create a user account called SJ-Parent and make it an Administrator
- Create an account called Deacon and make it an Administrator account

2) Create an Administrator Group, with administrator privileges (If needed, this may already be set by the system): 10 Points

- Make the account called Deacon a member of the Administrator group
- Make the account called SJ-Parent a member of the Administrator group

3) Create a Student Group, with general user privileges :10 Points

- Make the account called SJ-Student a member of the Student group

4) All user accounts are password protected: 10 pts.

- How do I find this problem?

  Password protecting all user accounts is good cybersecurity practice in general.

- How do I solve this problem?

- Why is fixing this problem important?

  Not having a password on an account makes it extremely vulnerable to attacks by outside individuals. Without a password, an attacker can access the user account easily. Secure passwords are highly recommended as a deterrent to potential attackers.

5) A password of at least 10 characters is required: 10 pts.

- How do I find this problem?

  Enforcing use of longer passwords is a good cybersecurity practice in general.

- How do I solve this problem?

- Why is fixing this problem important?

  Setting a password policy ensures that all users on the system must set a secure password. By setting a password minimum length, IT administrators force users to create more secure passwords.

- Ensure Password Complexity is enabled

6) Administrator account has been changed to User: 10 pts.

- How do I solve this problem?

Change the SJ Parent Account to a User account and remove it from the Administrator Group and place it in the Student Group

- Why is fixing this problem important?

  Ensuring account types are set correctly is very important. A Standard user given administrative permissions can accidentally or purposefully cause significant damage to a system because they would have unrestricted full read and write access to all files on the system, not just their own.

9) Enforce a password history policy: 10 pts.

- How do I find this problem?

  Enforcing a password history policy is a good cyber security practice that administrators should implement.

- How do I solve this problem?

- Why is fixing this problem important?

  It is important to enforce a password history policy, so users won't reuse the same passwords again. Reusing a password gives the malicious user more time to obtain the users password via a brute force method.

10) Set a maximum password age policy: 10 pts.

- How do I find this problem?

  Enforcing a maximum password age policy is a good cyber security practice that administrators should implement.

- How do I solve this problem?

- Why is fixing this problem important?

  It is important to set a maximum password age policy because the system will require the user to change their passwords when the set time has been met. As there is much work to be done throughout the day, the user may forget to change their passwords periodically. It is good practice to have the user change their passwords in case a malicious agent is trying to brute force their way into the system.

Bonus Question: 30 Points

Translate the following to ASCII text:

4d 61 72 63 68 20 63 6f 6d 65 73 20 69 6e 20 6c 69 6b 65 20 61 20 6c 69 6f 6e 2c 20 61 6e 64 20 67 6f 65 73 20 6f 75 74 20 6c 69 6b 65 20 61 20 6c 61 6d 62 21

01001001 01101110 01100100 01101001 01110110 01101001 01100100 01110101 01100001 01101100 01101100 01111001 00101100 00100000 01110111 01100101 00100000 01100001 01110010 01100101 00100000 01101111 01101110 01100101 00100000 01100100 01110010 01101111 01110000 00101110 00100000 01010100 01101111 01100111 01100101 01110100 01101000 01100101 01110010 00101100 00100000 01110111 01100101 00100000 01100001 01110010 01100101 00100000 01100001 01101110 00100000 01101111 01100011 01100101 01100001 01101110 00101110