**CYBR 450 – Access Control Assignment**

NAME: \_\_\_Abby Gopal\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ DATE:\_\_\_09-20-2024\_\_\_\_\_\_\_\_\_\_\_\_

Fully complete all of the following using complete sentences and proper English grammar, punctuation, and spelling. *You need to complete all parts*.

Please include your name, class number, and assignment number on your paper.

Part 1

Let’s evaluate the strength of one of your current passwords. Just because an attacker steals your password database does not mean he automatically knows your password. He still has to crack it. Creating a strong password can make it impractical for an attacker to crack your password.

These tools can help you understand the differences between strong and weak passwords.

1. Go to my1login at <https://www.my1login.com/resources/password-strength-test/>
2. Enter a password of a similar construction to one you use on a regular basis
3. Take a screenshot.

A screenshot of a computer screen

Description automatically generated

1. Take note of the problems with your password (e.g. a number sequence and a dictionary word). Make sure you understand all of the characteristics evaluated for passwords with this tool.

The problem with my password is that it is weak because it contains 2 dictionary words.

1. Try entering a password you might actually use and you think is strong.

A12@#weak!\*

1. How long does the web tool say it would take to break?

4 years

1. Take a screenshot of the results.

A screenshot of a computer

Description automatically generated

1. Go to Norton Identity Safe Password Generator: https://my.norton.com/extspa/idsafe?path=pwd-gen
2. Try different combinations of the settings at the right side of the page, generate several passwords. Are the passwords you generated examples of good passwords?

After generating several passwords using various combinations of settings (letters, mixed case, punctuation, and numbers), the results illustrate a range of password strengths. One example of a strong password generated was "b\_0AqeWet5+" it effectively combines uppercase and lowercase letters, numbers, and special characters, providing the necessary complexity to resist brute force or dictionary attacks. This password meets the criteria for a good password as it uses multiple character types and has a sufficient length of 11 characters, making it more secure.

On the other hand, shorter passwords, such as "!9EFr" and "6#vizeNitr," were flagged as weak or bad by the password generator. These passwords are either too short or lack the sufficient complexity that would make them resistant to attacks. For instance, "!9EFr" contains fewer characters and, while it incorporates some complexity with punctuation and numbers, it does not meet length recommendations for strong passwords.

In conclusion, passwords that integrate a combination of uppercase and lowercase letters, numbers, punctuation, and meet or exceed a length of at least 12 characters are generally classified as strong passwords.

1. Take a screenshot.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

1. Provide a 2-3 paragraph description of your analysis of this activity.
   1. Do you agree with the tool results? Why or why not?
   2. Include an authoritative source

The Norton Password Generator offers users a reliable way to create secure passwords by allowing customization based on length and complexity. As seen in the images, the tool categorizes passwords below 5 characters as “bad,” 5-10 characters as “weak,” and 11-64 characters as “strong.” This aligns with password security guidelines, such as those from NIST, which emphasize that longer passwords, combined with mixed case, numbers, and symbols, significantly reduce vulnerability to brute-force and dictionary attacks.

I agree with these results because password complexity and length are critical in securing accounts, especially against modern threats. As an authoritative source, the National Institute of Standards and Technology (NIST) highlights those longer passwords, even without strict complexity rules, offer stronger protection against attacks like brute-forcing. The Norton tool adheres to these principles by not only measuring length but also incorporating complexity (i.e., mixed case, punctuation, and numbers), ensuring comprehensive password strength.

NIST's Special Publication 800-63B provides a valuable resource for understanding password management best practices.

References:

NIST. (2020). *NIST Special Publication 800-63B*. Nist.gov; NIST. <https://pages.nist.gov/800-63-3/sp800-63b.html>

Part 2

Multifactor Authentication (MFA) (aka Two-Factor Authentication (TFA)) is often used to supplement a PIN/password or to replace them. In 2-3 paragraphs, explain how it works using real-world examples. Include applications or programs used for MFA/TFA.

Multifactor Authentication (MFA), also known as Two-Factor Authentication (TFA), adds an extra layer of security by requiring users to present two or more forms of identification to gain access to an account. It typically involves something the user knows (password or PIN), something they have (smartphone, hardware token, etc.), and something they are (biometric data like fingerprints or facial recognition). This ensures that even if a hacker obtains a user’s password, they still cannot access the account without the second authentication factor.

Common programs that provide MFA or TFA include Google Authenticator and Microsoft Authenticator, which generate time-based one-time passwords (TOTP). Users link their accounts to the app, and when prompted, provide a password along with a verification code displayed on the app. Other widely used MFA tools include Duo Security (commonly used by universities and corporations), Authy, and hardware tokens like YubiKey. For instance, users of platforms like Facebook or Twitter may be prompted to verify their identity via text message or an authenticator app when logging in. Similarly, online banking services like Chase and Bank of America use MFA to prompt customers for a code received on their mobile devices after they enter their username and password, enhancing security.

Part 3

On Windows systems that are networked as part of a domain, access control policies are set as part of Group Policy Objects (GPOs). The Local Security Policy is used when it acts as a standalone system. Together, they provide the security standards in place for the computer. For this exercise, you are to view the Group and Local Policies on a Windows 10 computer and report on your findings and recommendations.

You may do this on your own Windows system or use the Virtual Cybersecurity Desktop provided by the University.

See the separate instructions to access the BU Virtual Desktop environment.

Group Policies

* To access the Windows Local Group Policies, you can either search for “edit group Policy” or type gpedit.msc on the Windows Run bar.
* In the Local Group Policy Editor window, find the “Account Policies” and “Local Policies.” Take a screenshot of its contents and include it here.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Local Policies

* To access the Windows Local Security Policy, you can either search for “local security policy” or type secpol.msc on the Windows Run bar.
* In the Local Security Policy Window, find the “Account Policies” and “Local Policies.” Take a screenshot of its contents and include it here.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Explain the password and account lockout policies you find.

The password and account lockout policies you’ve outlined offer a structured approach to securing user accounts on a Windows 10 system. Currently, the password policies enforce a solid security framework. With 5 passwords remembered, the system ensures that users cannot reuse their last five passwords, which encourages them to select new ones. Passwords must be changed every 90 days, helping to limit the exposure of any single password. Users must wait at least 1 day before they can change their password again, which prevents them from quickly rotating through passwords to bypass the history requirement. The minimum password length is set to 8 characters, which is a basic but effective requirement for preventing easy-to-guess passwords. The password complexity requirements are enabled, meaning passwords must include a mix of uppercase and lowercase letters, numbers, and symbols, making them more resistant to guessing and brute-force attacks. The settings for minimum password length audit and relax minimum password length limits are not defined, meaning there is no specific auditing for password length compliance and no temporary relaxation of length requirements. The store passwords using reversible encryption setting is disabled, which is good practice because reversible encryption could potentially allow passwords to be decrypted if compromised.

On the other hand, the account lockout policies are not configured, as indicated by several settings being marked as "Not Applicable." This means that currently, the system does not lock out accounts after a certain number of failed login attempts. Specifically, the account lockout threshold is set to 0 invalid logon attempts, so accounts are not locked out regardless of how many failed attempts occur. There is no defined account lockout duration or reset account lockout counter after time, further confirming that account lockout policies are not in effect. The allow administrator account lockout setting is also marked as "Not Applicable," indicating that the lockout policy does not extend to the Administrator account either. Overall, while the password policies in place help secure user accounts by enforcing strong passwords and complexity requirements, enabling and configuring account lockout policies would further enhance security by protecting against brute-force attacks and unauthorized access.