Cybersecurity Problem Assignment - 1

Internship Program
Cyber Security
Hunar Intern

Task 1: Password Policy Review

Objective:

To critically evaluate and enhance the existing password policy within the organization to improve the security and protection of user accounts.

Current Password Policy Review:

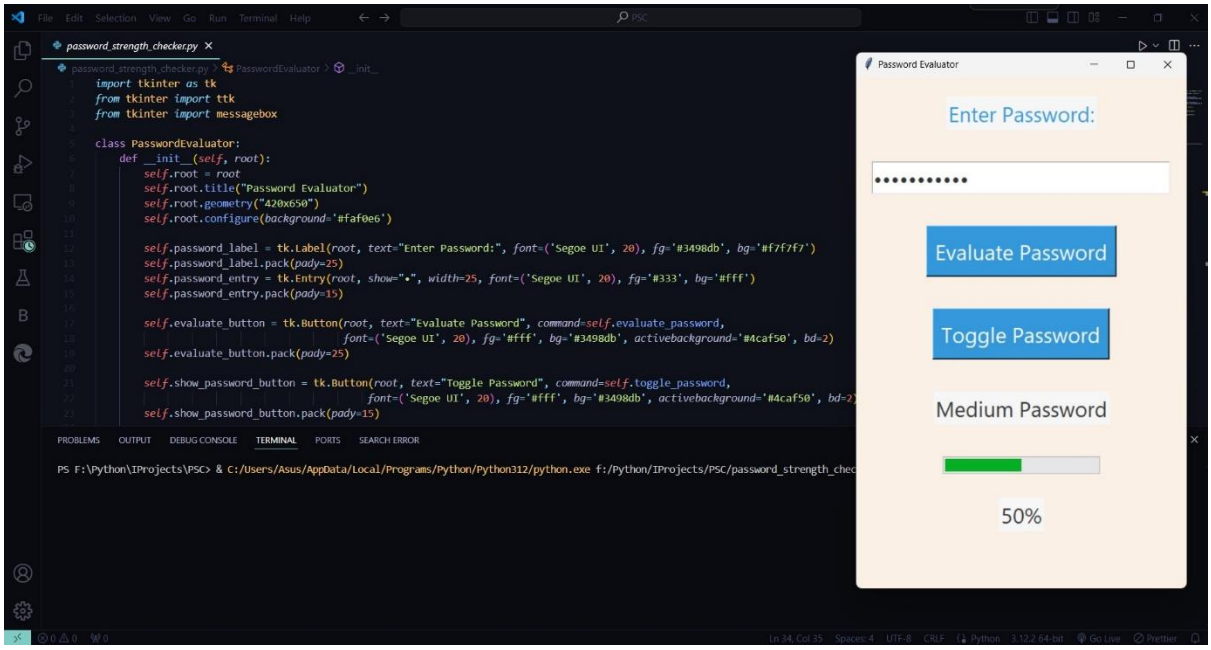
The organization currently follows a password policy that includes the following elements:

- **Minimum Password Length:** 8 characters, which is the bare minimum for password security but may not be sufficient against modern cracking techniques.
- **Complexity Requirements:** Passwords must include at least one uppercase letter, one lowercase letter, and one numeric digit. However, there is no requirement for special characters, which reduces the overall complexity.
- **Password Expiration Period:** Users are required to change their passwords every 90 days. While this policy aims to minimize the risk of password reuse, frequent changes can lead to weaker password choices if users are not adequately trained.

Strength Assessment:

To evaluate the current password strength, I conducted an analysis using the Password Meter tool. The following sample passwords were tested:

1. **Password123**:
    - **Score:** Weak
    - **Analysis:** This password is predictable and lacks complexity. It includes common patterns that are easily guessable.
2. **P@ssw0rd!**:
    - **Score:** Medium
    - **Analysis:** While this password includes a special character and a number, it follows a common pattern that attackers often target.
3. **Xy!9&hGd2***:
    - **Score:** Strong
    - **Analysis:** This password has high entropy, combining random characters, numbers, and symbols, making it difficult to crack.



Detailed Recommendations:

1. **Increase Minimum Password Length:**
    - **New Requirement:** 12-16 characters.
    - **Rationale:** Longer passwords significantly increase the time required for brute-force attacks. A 12-character password can offer sufficient security, but 16 characters provide an even higher level of protection.
2. **Enhance Complexity Requirements:**
    - **New Requirement:** Passwords must include at least one uppercase letter, one lowercase letter, one number, and one special character (e.g., !, @, #).
    - **Rationale:** Adding special characters increases the complexity, making passwords harder to guess. Consider requiring passwords to avoid common sequences (e.g., 123, abc).
3. **Implement Multi-Factor Authentication (MFA):**
    - **New Policy:** In addition to strong passwords, require MFA for accessing sensitive systems or data.
    - **Rationale:** MFA adds an extra layer of security by requiring something the user knows (password) and something they have (e.g., a mobile device with an authentication app).

4. **Enforce Password History and Reuse Restrictions:**
    - **New Policy:** Users cannot reuse their last 5-10 passwords.
    - **Rationale:** This policy prevents users from cycling through the same passwords, which can weaken security if old passwords were compromised.
5. **Conduct Regular Security Training:**
    - **New Policy:** Regular training sessions on password security should be conducted.
    - **Rationale:** Users should be educated on the importance of strong passwords, recognizing phishing attempts, and using password managers to avoid password fatigue.
6. **Consider Password Managers:**
    - **Recommendation:** Encourage or provide access to password managers (e.g., LastPass, 1Password).
    - **Rationale:** Password managers help users generate and store complex passwords securely, reducing the temptation to use easily memorable (and thus weak) passwords.

Conclusion:
The existing password policy provides a basic level of security but can be significantly improved by adopting longer, more complex passwords, implementing MFA, and educating users. These measures will bolster the organization's defenses against unauthorized access.

Task 2: Device Security Basics

Objective:

To ensure that a new employee's workstation is secured against common cybersecurity threats by implementing essential security settings, educating the user, and installing necessary protection software.

Device Configuration:

1. **Enable Automatic Updates:**
    - **Configuration:** Automatic updates were enabled for the operating system and all installed applications.
    - **Rationale:** Keeping software up to date is crucial for protecting the workstation from known vulnerabilities that attackers could exploit.

2. **Configure a Screensaver Lock:**
    - **Configuration:** A screensaver lock was configured to activate after 5 minutes of inactivity, requiring the user to re-enter their password to resume work.
    - **Rationale:** This prevents unauthorized access if the workstation is left unattended.
3. **Set Up a Guest Account:**
    - **Configuration:** A guest account was created with limited privileges, preventing unauthorized users from installing software or changing system settings.
    - **Rationale:** This reduces the risk of malware installation or accidental system changes by users without administrative access.
4. **Implement Device Encryption:**
    - **Configuration:** Full-disk encryption was enabled to protect sensitive data on the workstation.
    - **Rationale:** Even if the device is stolen, the data remains protected and inaccessible without the decryption key.

User Awareness Guide:

To further enhance security, I prepared a comprehensive guide for the new employee that covers critical cybersecurity practices:

1. **Recognizing Phishing Emails:**
    - **Guidance:** Look for signs of phishing, such as unfamiliar sender addresses, generic greetings (e.g., "Dear User"), urgent requests for personal information, or suspicious attachments and links.
    - **Recommendation:** Always verify the sender's identity before clicking on links or downloading attachments. When in doubt, contact the IT department.
2. **Using Strong and Unique Passwords:**
    - **Guidance:** Create passwords that are at least 12-16 characters long, combining uppercase and lowercase letters, numbers, and special characters.
    - **Recommendation:** Avoid using the same password for multiple accounts. Use a password manager to generate and store strong passwords securely.
3. **Avoiding Suspicious Websites and Downloads:**
    - **Guidance:** Only visit trusted websites, and avoid clicking on pop-up ads or downloading software from unknown sources.
    - **Recommendation:** Install browser extensions like HTTPS Everywhere to ensure a secure connection and ad blockers to minimize exposure to potentially malicious content.

4. **Understanding the Importance of Software Updates:**
    - **Guidance:** Ensure that all software, especially antivirus and operating systems, are kept up to date.
    - **Recommendation:** Enable automatic updates for all critical software to protect against vulnerabilities.
5. **Secure Use of Public Wi-Fi:**
    - **Guidance:** Avoid accessing sensitive information (e.g., online banking) over public Wi-Fi networks.
    - **Recommendation:** Use a Virtual Private Network (VPN) when connecting to public Wi-Fi to encrypt your internet traffic.

Antivirus Software Installation:

1. **Software Used:** Avast Free Antivirus was installed on the workstation.
2. **Full System Scan:**
    - **Action:** A full system scan was performed immediately after installation to check for any pre-existing threats.
    - **Results:** The scan detected no threats, confirming that the workstation was clean.
3. **Scheduled Scans and Updates:**

- **Configuration:** The antivirus software was set to perform weekly scans and update virus definitions automatically.
- **Rationale:** Regular scans and updates ensure ongoing protection against new threats.

Conclusion:

The workstation has been configured with essential security settings, and the new employee has been provided with comprehensive cybersecurity guidance. These proactive measures will help protect the device and the organization's data from common threats, reducing the risk of security breaches.