

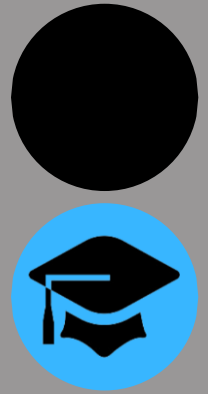


FORGE YOUR AMBITION

# HUNAR INTERN

WWW.HUNARINTERN.LIVE

LET'S GET STARTED



Name: Leburi SriRam

Date: 12/04/2024

## Cybersecurity Problem Assignment

**Objective:** The objective of this assignment is to introduce you to basic cybersecurity concepts and practical applications. This assignment is designed to be Secure-friendly.

### Task 1: Password Policy Review

#### Password Policy:

- **Password Length:** Password should be minimum length of 8 characters and, a maximum (your choice) password length. Longer passwords are generally more secure.
- **Complexity Requirements:** Require a mix of character types, such as uppercase letters(A-Z), lowercase letters(a-z), numbers(0-9), and special characters(@,#,\$,%^,&,\*).
- **Password History:** Enforce a policy that prevents users from reusing a certain number of their previous passwords. This prevents users from cycling through old passwords.
- **Expiration:** Set a maximum password age, after which users must change their passwords. Regular password changes reduce the risk of long-term compromises.
- **Multi-Factor Authentication :** Encourage or require the use of multi-factor authentication to add an extra layer of security on top of passwords.
- **Encryption:** Ensure that passwords are stored securely using strong encryption methods such as hashing with a salt.
- **Regular Reviews:** Regularly review and update the password policy to adapt to evolving security threats and best practices.

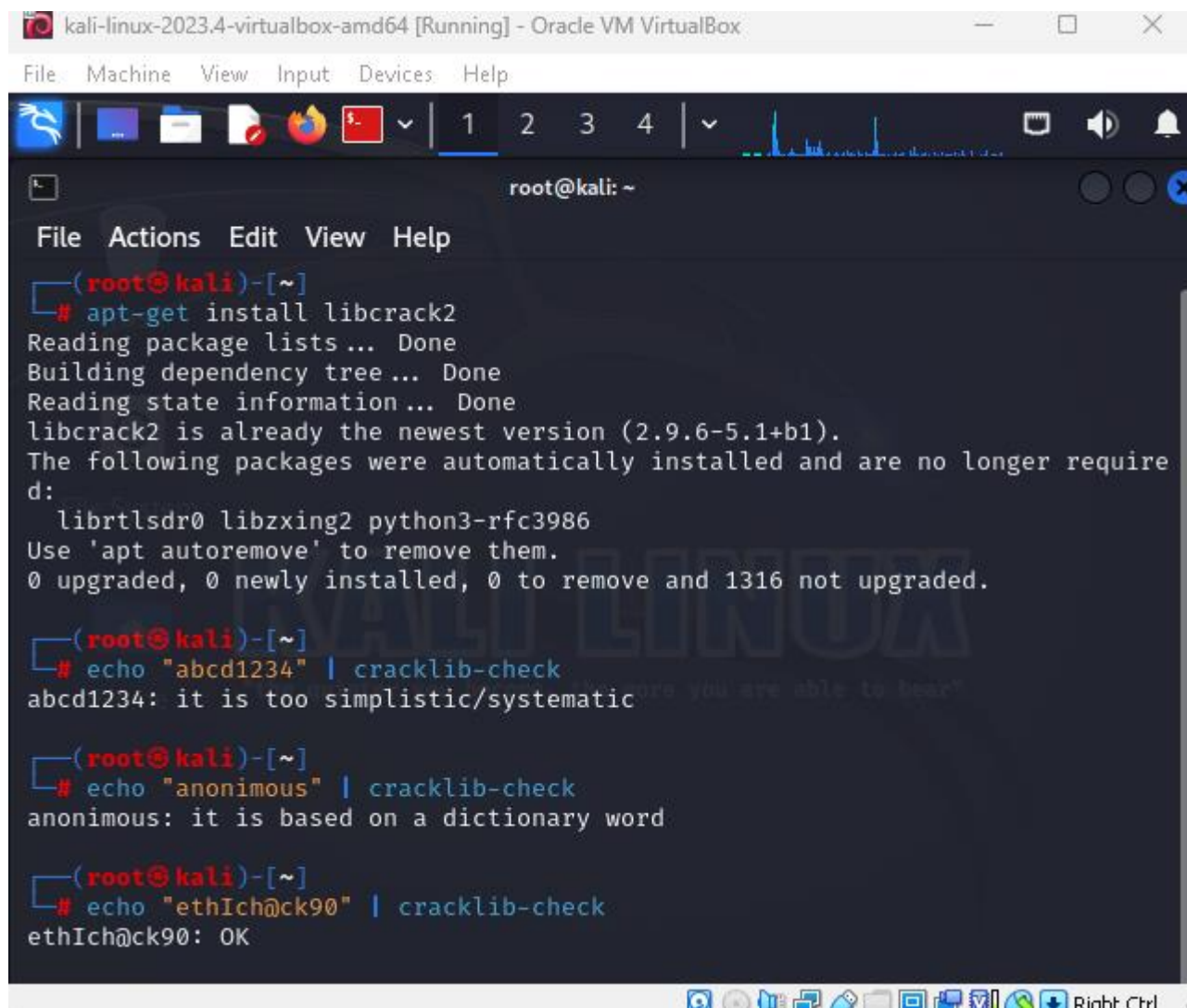
## Strength Assessment:

- Here Linux command tool “Cracklib” is used to check the strength of password

**Cracklib:** CrackLib is a library for checking the strength of passwords. It has both command-line tools and library functions. You can use the cracklib-check command to check the strength of a password.

Command to install: `$ apt-get install libcrack2`

Command to check strength of password: `$ echo “password” | cracklib-check`



```
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@kali: ~

File Actions Edit View Help








(root@kali)-[~]
# apt-get install libcrack2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libcrack2 is already the newest version (2.9.6-5.1+b1).
The following packages were automatically installed and are no longer required:
  librtlsdr0 libzxing2 python3-rfc3986
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1316 not upgraded.

(root@kali)-[~]
# echo "abcd1234" | cracklib-check
abcd1234: it is too simplistic/systematic

(root@kali)-[~]
# echo "anonymous" | cracklib-check
anonymous: it is based on a dictionary word

(root@kali)-[~]
# echo "ethIch@ck90" | cracklib-check
ethIch@ck90: OK
```

## Recommendations:

-  **Length:** Aim for a minimum of 12 characters. Longer passwords are generally more secure.
-  **Avoid Dictionary Words:** Don't use easily guessable words found in dictionaries. Hackers often use automated tools that can quickly guess common words.
-  **Randomness:** Generate passwords randomly rather than using easily guessable patterns or personal information (such as birthdays or pet names).
-  **Passphrases:** Consider using a passphrase instead of a password. Passphrases are longer combinations of words or phrases that are easier to remember and harder to crack. For example, "CorrectHorseBatteryStaple" is a strong passphrase.
-  **Unique Passwords:** Use a unique password for each account or service. Reusing passwords across multiple accounts increases the risk of a security breach if one account is compromised.
-  **Avoid Common Patterns:** Avoid using common patterns like "123456", "password", "qwerty", or keyboard patterns like "asdfghjkl".
-  **Regularly Update Passwords:** Periodically change your passwords, especially for sensitive accounts. This can help mitigate the risk of long-term compromises.

## Task 2: Device Security Basics

**Scenario:** As part of your internship, you are assigned to set up a new employee's workstation. Your manager emphasizes the importance of securing the device against common threats.

### Tasks:

#### Device Configuration:

- Enable full-disk encryption to protect data in case the device is lost or stolen. Utilize built-in encryption tools like BitLocker (Windows) or FileVault (macOS).
- Configure a strong password or passphrase for accessing the device, adhering to the recommendations mentioned earlier.
- Disable unnecessary services and features to minimize attack surface. This includes disabling unused ports, protocols, and services.
- Keep the operating system and software up to date with the latest security patches and updates. Enable automatic updates where possible to ensure timely installation of patches.

#### Antivirus Software:

- Install reputable antivirus software and keep it up to date. Ensure that real-time scanning is enabled to detect and prevent malware infections.
- Configure regular scans of the system to identify and remove any malware that may have slipped through the defenses.
- Educate the employee on the importance of not disabling or bypassing antivirus software and encourage them to report any suspicious activity immediately.

#### User Awareness:

- ❖ Provide comprehensive security training to the employee to raise awareness about common threats such as phishing attacks, social engineering, and malware.
- ❖ Emphasize the importance of practicing good password hygiene, including creating strong, unique passwords, avoiding password reuse, and not sharing passwords with anyone.
- ❖ Teach employees to recognize suspicious emails, links, and attachments, and to verify the legitimacy of requests for sensitive information.

- ❖ Encourage the use of secure communication tools and protocols for transmitting sensitive information, such as encrypted email and file transfer solutions.
- ❖ Establish clear procedures for reporting security incidents or concerns, and ensure that employees know who to contact in case of a security breach.

## **Note:**

By implementing these measures, you can help ensure that the new employee's workstation is adequately protected against common security threats and that the employee is equipped with the knowledge and tools to maintain a secure computing environment.

## **Conclusion:**

In conclusion, a robust password policy is a cornerstone of an organization's cybersecurity framework, serving as a critical line of defense against unauthorized access and data breaches. By implementing and enforcing a well-designed password policy, organizations can significantly enhance the security posture of their systems and protect sensitive information from malicious actors.

In conclusion, securing a new employee's workstation against common threats is essential for safeguarding sensitive data and maintaining a secure computing environment. By following best practices for device configuration, antivirus software deployment, and user awareness training, organizations can mitigate the risk of security breaches and unauthorized access to corporate resources.