ZULNOORAIN WAQAR

TASK 2

Digital Empowerment Pakistan

Contents

[Implementation of MFA 2](#_Toc177575610)

[Monitoring MFA Adoption: 6](#_Toc177575611)

[Addressing MFA Issues: 6](#_Toc177575612)

[Maintaining MFA Configurations: 6](#_Toc177575613)

# Implementation of MFA

To install Google Authenticator on Kali Linux running on VMware, follow these steps:

**Step 1: Update Your System**

First, ensure your Kali Linux system is up to date:

**sudo apt update && sudo apt upgrade -y**

****

**Step 2: Install Google Authenticator**

The package is part of the libpam-google-authenticator module, which integrates with PAM (Pluggable Authentication Modules).

To install Google Authenticator, run the following command:

**sudo apt install libpam-google-authenticator**

****

**Step 3: Set Up Google Authenticator**

Once installed, set up Google Authenticator by running the command below:

**google-authenticator**

During the setup, you’ll be prompted with a series of questions:

1. **Do you want authentication tokens to be time-based?** Type y for time-based tokens.
2. **Secret Key, QR Code, and Emergency Codes**: You'll see a secret key and a QR code. You can either scan the QR code with the Google Authenticator app on your mobile device or manually enter the secret key. Keep the emergency codes in a safe place as they can be used if you lose access to your phone.
3. **Update .google\_authenticator file**: Type y to save the configuration.
4. **Disallow multiple uses of the same token**: Type y to prevent token reuse.
5. **Increase the time window**: Type y if needed, although default settings work for most.
6. **Enable rate-limiting to prevent brute force attacks**: Type y to enable rate limiting.

**Step 4: Configure PAM for Google Authenticator**

Now, you need to integrate Google Authenticator with PAM to enable two-factor authentication (2FA). Open the PAM configuration file using a text editor:

**sudo nano /etc/pam.d/sshd**

Add the following line at the top:

**auth required pam\_google\_authenticator.so**

A screenshot of a computer

Description automatically generated

**Step 5: Configure SSH for Google Authenticator (Optional)**

If you want to use Google Authenticator with SSH, you need to edit the SSH configuration file:

**sudo nano /etc/ssh/sshd\_config**

Find the line:

**ChallengeResponseAuthentication no**

Change it to:

**ChallengeResponseAuthentication yes**

Save and exit the file.

A screenshot of a computer program

Description automatically generated

**Step 6: Restart SSH Service**

After modifying the SSH configuration, restart the SSH service to apply the changes:

**sudo systemctl restart ssh**

**Step 7: Install Google Authenticator App**

Download and install the **Google Authenticator** app on your mobile phone from the app store (Google Play Store for Android or the Apple App Store for iOS).

**Step 8: Test Google Authenticator**

You can test Google Authenticator by attempting to log in. It will prompt for your regular password and a verification code from the app.

A qr code on a computer screen

Description automatically generated

That's it! You've successfully installed and configured Google Authenticator on Kali Linux running on VMware.

# Monitoring MFA Adoption:

* **Track MFA Enrollment:** Use identity provider reports to monitor how many users have enabled MFA.
* **Analyze Logs:** Check authentication logs for failed/successful MFA attempts and set alerts for anomalies.
* **User Feedback:** Collect and address MFA issues reported via help desk tickets.

# Addressing MFA Issues:

* **Troubleshooting:** Identify common MFA failures (e.g., token issues) and provide backup methods.
* **User Education:** Offer training materials and guides for MFA setup.
* **Security Audits:** Ensure privileged accounts use MFA and remove any exemptions.

# Maintaining MFA Configurations:

* **Regular Updates:** Keep MFA software updated and review policies periodically.
* **Time Sync:** Ensure TOTP tokens are synced and use NTP for time accuracy.
* **Recovery Planning:** Implement and back up MFA recovery processes.