Report on Disabling Password-Based Authentication in SSH:

Objective:

The objective is to enhance the security of the Ubuntu Server by disabling password-based authentication in SSH and enabling SSH key-based authentication.

Steps Taken:

a. Generate SSH Key Pair:

The user is instructed to generate an SSH key pair using the ssh-keygen command if they haven't already done so. This command generates a public and private key pair.

Command:

(ssh-keygen -t rsa)

b. Copy Public Key to Server:

The ssh-copy-id command is provided as a method to copy the local SSH public key to the Ubuntu Server. This command appends the public key to the authorized_keys file on the server, allowing key-based authentication.

An example command is provided for copying the SSH public key to the server, replacing placeholders with actual username and server IP address.

Command:

(ssh-copy-id username@server_ip_address)

c. Disable Password Authentication:

The PasswordAuthentication option in the SSH server configuration file (sshd_config) is explained as the control for enabling or disabling password-based authentication.

Instructions are given to edit the sshd_config file using a text editor with root privileges (nano), locate the PasswordAuthentication option, and set it to no to disable password-based authentication.

An alternative is provided to add the PasswordAuthentication no line at the end of the sshd_config file if the option does not exist.

After making the changes, users are instructed to restart the SSH service for the changes to take effect.

Commands:

(sudo nano /etc/ssh/sshd_config)

Locate **PasswordAuthentication** and set it to **no** or add **PasswordAuthentication no** at the end of the file.

(PasswordAuthentication no)

Restart SSH service:

(sudo service ssh restart)

Conclusion:

By following the provided steps, users can enhance the security of their Ubuntu Server by disabling password-based authentication in SSH and relying solely on SSH key-based authentication. This helps mitigate the risk of unauthorized access via brute-force attacks on weak passwords.