**Assaignment 2:**

**Assignment: Disable SSH Root Login on Linux and Verify**

**Objective**

The objective of this assignment is to disable remote SSH login for the root user on a Linux system, restart the SSH service to apply changes, and verify that root login is effectively disabled by testing remote SSH access.

**Environment**

* Linux distribution (Ubuntu, Debian, CentOS, etc.) with sudo/root access
* SSH server installed and running

**Procedure**

**Step 1: Edit SSH Configuration File**

* Open the SSH daemon configuration file with a text editor:

sudo nano /etc/ssh/sshd\_config

* Locate the line containing *PermitRootLogin.*
* Change its value to no to disable root login remotely:

*text*

PermitRootLogin no

* Save and exit the editor.

**Step 2: Restart SSH Service**

* Apply changes by restarting the SSH service:

*bash*

sudo systemctl restart sshd

(On some distributions, use sudo service ssh restart or sudo service sshd restart.)

**Step 3: Verify the Configuration**

* *Try to login remotely as root user:*

*bash*

ssh root@<server-ip-address>

* The connection should be refused or denied due to disabled root login.

**Results**

* Root login over SSH was successfully disabled.
* Remote root login attempts were denied, enhancing system security by preventing direct root access.

**Conclusion**

Disabling SSH root login is a critical security measure that minimizes risk exposure by forcing administrators to log in as a non-root user and escalate privileges only when necessary. This approach improves accountability and reduces the attack surface.

**Commands Summary**

| **Command** | **Purpose** |
| --- | --- |
| sudo nano /etc/ssh/sshd\_config | Edit SSH daemon configuration |
| *PermitRootLogin no* | Disable remote root login |
| *sudo systemctl restart sshd* | Restart SSH service to apply changes |
|  |  |

This report provides a complete overview of the process to disable SSH root login, restart the service, and verify the security configuration through testing.