

# **ITAS 181 Lab Chapter 12**

## **Disabling SSH Root Login on Fedora Linux**

Raj Singh

04 November 2023

## Project Overview

For enhanced security, it's a best practice to disable direct root logins via SSH. This document outlines the steps required to modify the SSH configuration to prevent root login attempts over a network.

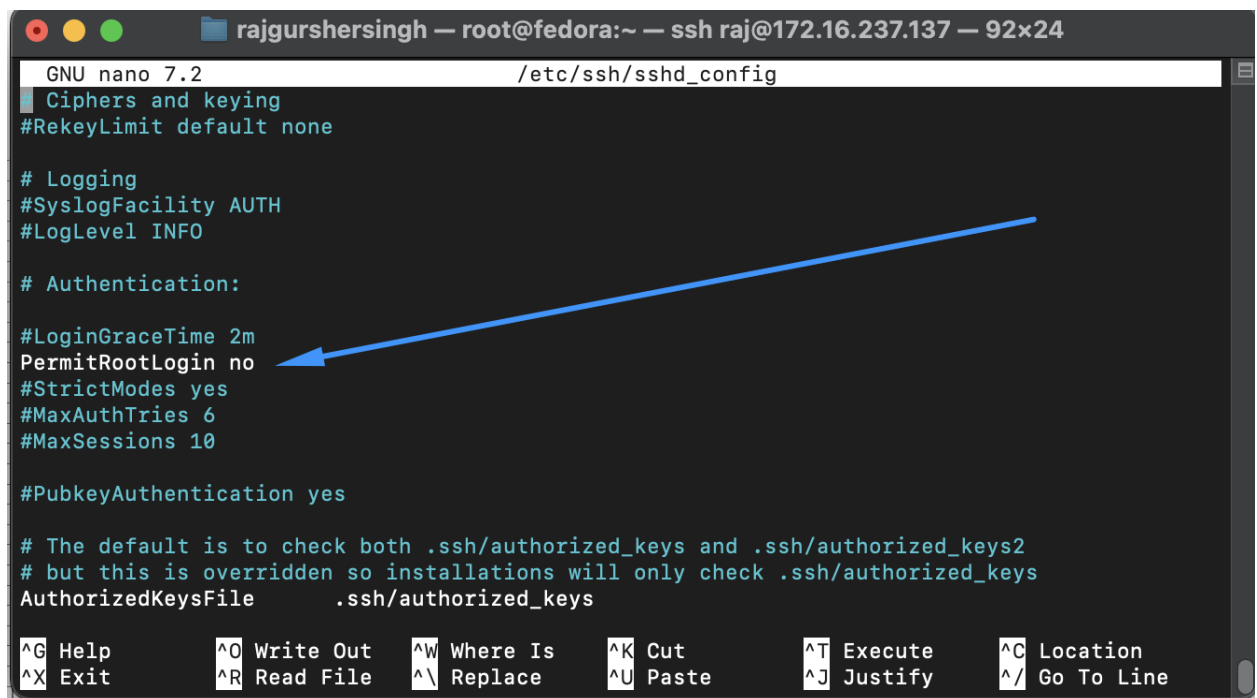
## Configuration Steps

### 1. Modify SSH Configuration:

- Open the SSH daemon's configuration file located at `/etc/ssh/sshd_config` with a text editor.

```
[[root@fedora ~]# nano /etc/ssh/sshd_config
```

- Locate the line that starts with `#PermitRootLogin` and uncomment it (remove the `#` sign) and then change it to `"PermitRootLogin"` as shown in the screenshot below:



```
GNU nano 7.2 /etc/ssh/sshd_config
#Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

- Save and exit out of the editor.

## 2. Restart SSH service

→ Apply the new configuration by restarting the SSH service with the following command:

```
[root@fedora ~]# sudo systemctl restart sshd.service
```

## 3. Verify Configuration

→ Attempt to SSH into the server as the root user to ensure that the configuration change is effective using the `ssh root@<server-ip>` command

```
rajgurshersingh@Rajgurshers-MacBook-Air ~ % ssh root@172.16.237.137
root@172.16.237.137's password:
Permission denied, please try again.
```

## Conclusion

This document, authored by Raj Singh for the ITAS 181 Lab on 04 November 2023, confirms the successful disablement of SSH root login on our Fedora Linux server. The outlined steps enhance our server's security by mitigating the risks associated with root access over the network.

The applied changes have been verified, ensuring our system adheres to industry-standard security practices. Future maintenance and security operations can build upon the foundation established by this procedure.

**Note:** *While the measures we've implemented do provide added security, they are foundational. A determined individual with sudo access could potentially alter the sshd\_config file.*

```
rajgurshersingh@Rajgurshers-MacBook-Air ~ % ssh raj@172.16.237.137
raj@172.16.237.137's password:
Last login: Fri Nov  3 22:12:26 2023 from 172.16.237.1
[[raj@fedora ~]$ su -
Password:
[[root@fedora ~]# echo "I have breached"
I have breached
[root@fedora ~]#
```

Terminal showing user 'raj' escalating to root and echoing 'I have breached'—a simulated security breach scenario.

To fortify our defenses, it is prudent to supplement these steps with a robust logging system. Such a system would monitor file modifications, enabling us to track any changes made to critical configuration files and trace them back to individual users.

We have now bolstered our server's defenses, demonstrating our ongoing commitment to robust cybersecurity measures.