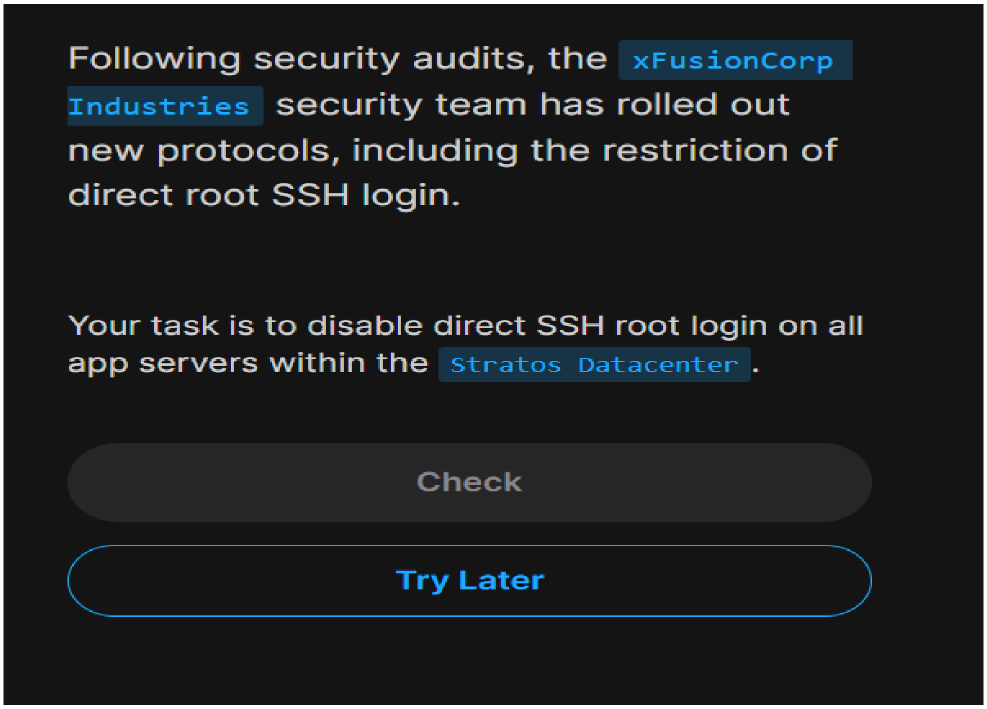
Day 3:



Following security audits, the `xFusionCorp Industries` security team has rolled out new protocols, including the restriction of direct root SSH login.

Your task is to disable direct SSH root login on all app servers within the `Stratos Datacenter`.

Step1:

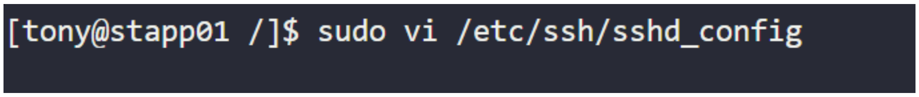
ssh onto the app server1

ssh tony@172.16.238.10

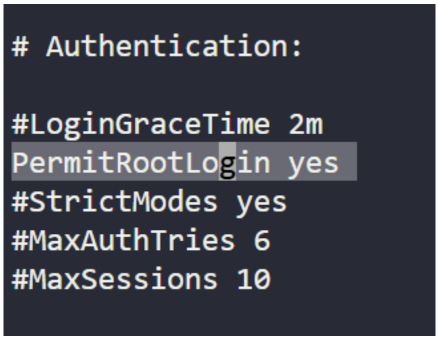
Step2:

SSH Configuration file is stored inside etc folder

Edit the configuration file and change the PermitRootLogin yes to **PermitRootLogin no**



```
[tony@stapp01 /]$ sudo vi /etc/ssh/sshd_config
```



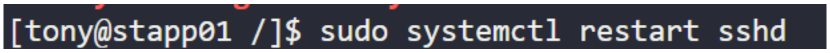
```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Change this field from yes to no

Step3:

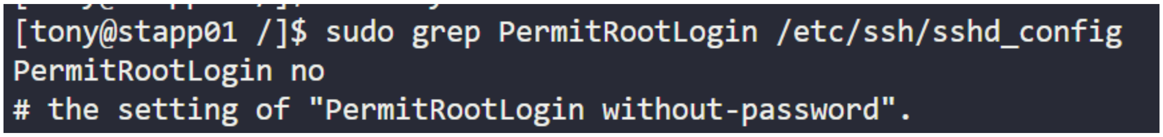
After saving the file, restart SSH for changes to take effect



```
[tony@stapp01 /]$ sudo systemctl restart sshd
```

Step 4:

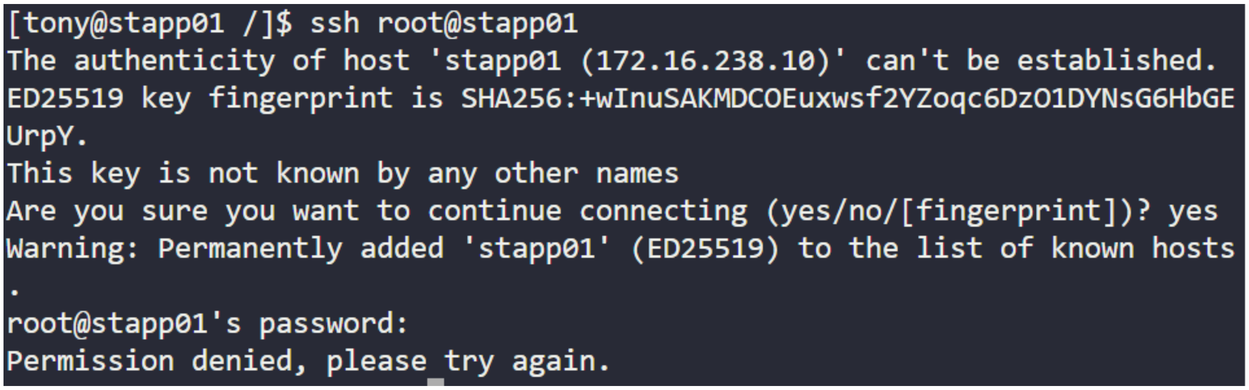
Verify the configuration



```
[tony@stapp01 /]$ sudo grep PermitRootLogin /etc/ssh/sshd_config
PermitRootLogin no
# the setting of "PermitRootLogin without-password".
```

Step5:

Try doing SSH via root



```
[tony@stapp01 /]$ ssh root@stapp01
The authenticity of host 'stapp01 (172.16.238.10)' can't be established.
ED25519 key fingerprint is SHA256:+wInuSAKMDCOEuxwsf2YZoqc6DzO1DYNsG6HbGE
UrpY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'stapp01' (ED25519) to the list of known hosts
.
root@stapp01's password:
Permission denied, please try again.
```

It gives permission denied error

Follow similar steps for appserver2 and appserver3

sshd = Secure Shell Daemon.
ssh → client command/program you run to connect to a server.

sshd → daemon/service running on the server that accepts incoming ssh connections.