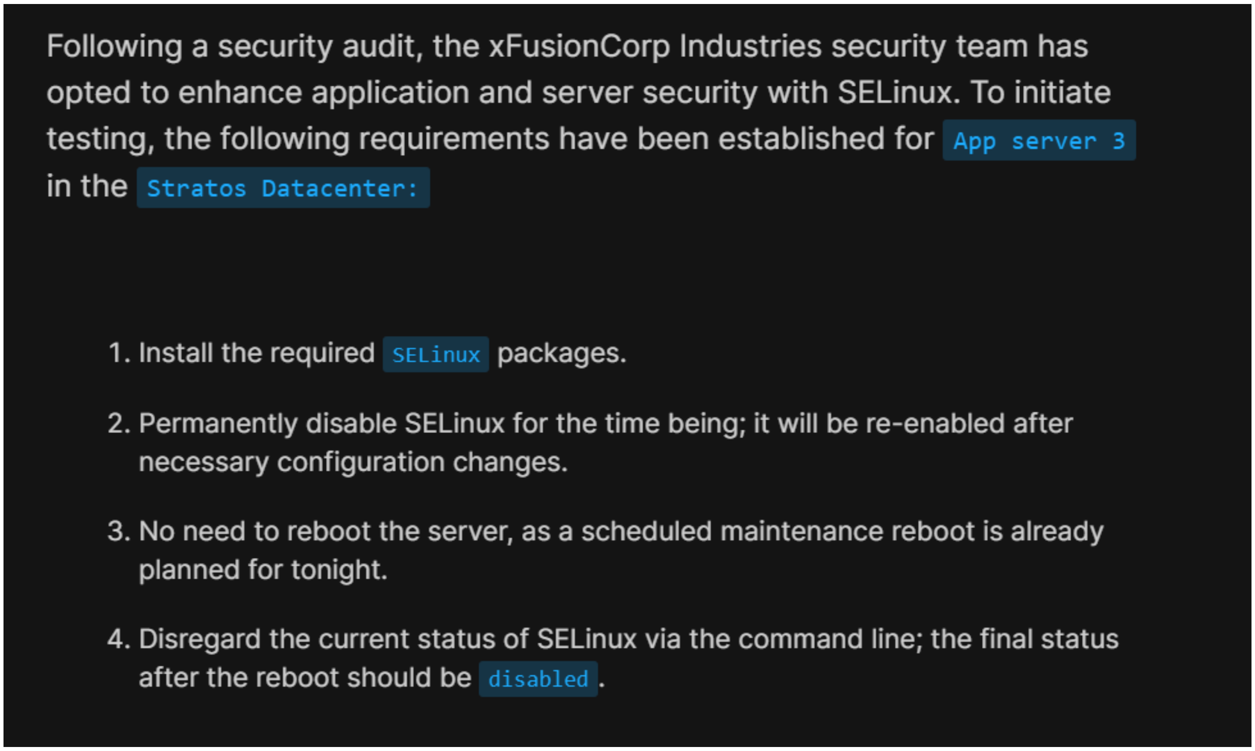
Day 5:



Following a security audit, the xFusionCorp Industries security team has opted to enhance application and server security with SELinux. To initiate testing, the following requirements have been established for `App server 3` in the `Stratos Datacenter:`

1. Install the required `SELinux` packages.
2. Permanently disable SELinux for the time being; it will be re-enabled after necessary configuration changes.
3. No need to reboot the server, as a scheduled maintenance reboot is already planned for tonight.
4. Disregard the current status of SELinux via the command line; the final status after the reboot should be `disabled`.

**SELinux (Security-Enhanced Linux)** is a **security layer** built into Linux.

- It controls **what users and processes can do** on a system

**Modes of SELinux**

1. **Enforcing** → SELinux is active and blocking violations.
2. **Permissive** → SELinux only logs violations but doesn't block.
3. **Disabled** → SELinux is turned off.

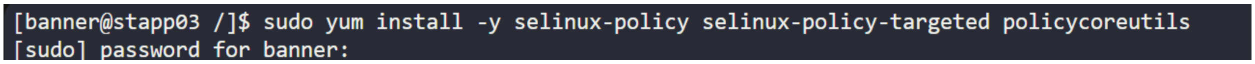
Step 1:

ssh onto the appserver3

ssh banner@172.16.238.12

Step2:

Install the required  SELinux packages



```
[banner@stapp03 /]$ sudo yum install -y selinux-policy selinux-policy-targeted policycoreutils
[sudo] password for banner:
```

-selinux-policy: This is the **base SELinux policy package**. Its like a "rulebook" for SELinux.

-selinux-policy-targeted: This is the **default policy used in most systems**.

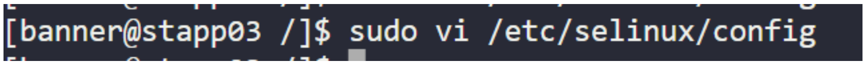
-policycoreutils: Provides the **core SELinux utilities** (commands).

You can check if SELinux is already installed onto the system
yum list installed | grep selinux

getenforce: Shows the **current mode** of SELinux.
setenforce 0 or setenforce 1: Temporarily **switches SELinux mode** (without reboot).

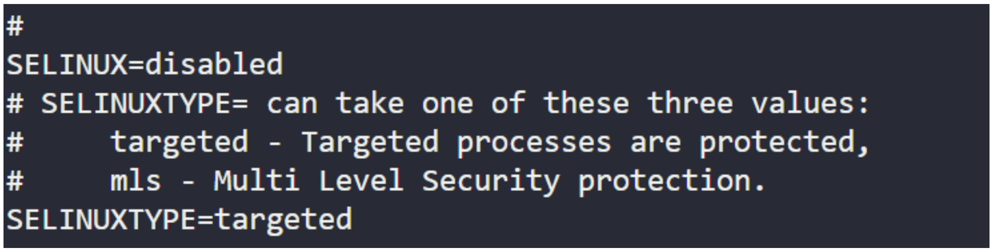
Step3:

/etc/selinux/config controls the **permanent state** of SELinux after reboot.



```
[banner@stapp03 /]$ sudo vi /etc/selinux/config
```

Step 4:Change SELINUX=enforcing to SELINUX=disabled



```
#
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```