Book 9 Career simulation
Frankie Bruno

Problem:

The problem was that James edited the config file leaving the config.conf file with 777 permissions which allowed the user/group/other to have read,write and execute capabilities.

Steps taken:

1. I first located the config.conf file
2. Next I cd to the location of that config.conf file
3. Then I typed ls -l to list the permissions for that config.conf file
4. Then I inspected the hash on the file using md5sum config.conf
5. Then I inspected the file using nano config.conf and noticed the admin section didn't exist so I then went in and added the admin section along with my soc analyst 2 Alice, and me as members of this section
6. Afterwards I cp the config.conf file to my home path /home/fstack/ so I could have a copy here

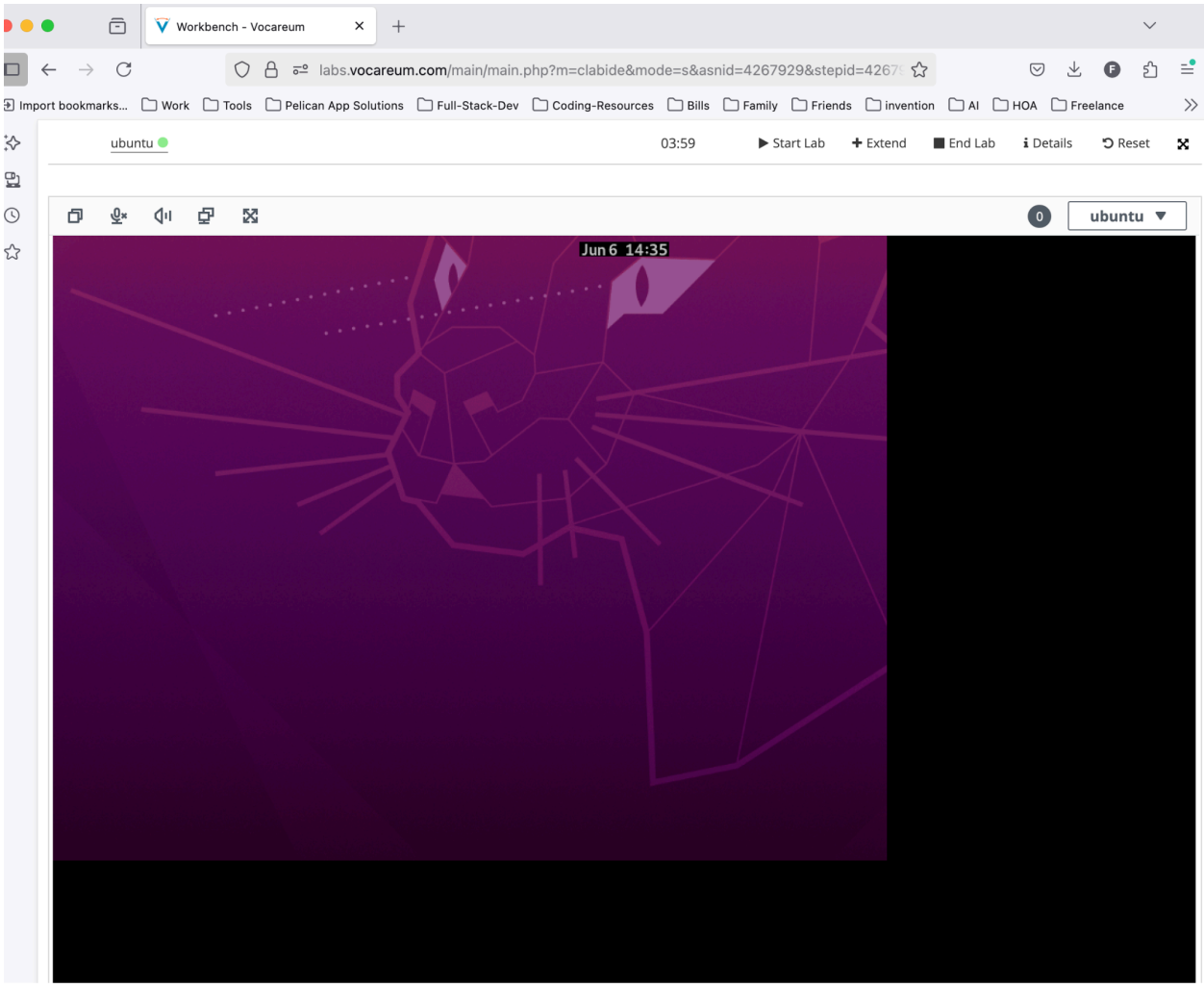
Prevention:

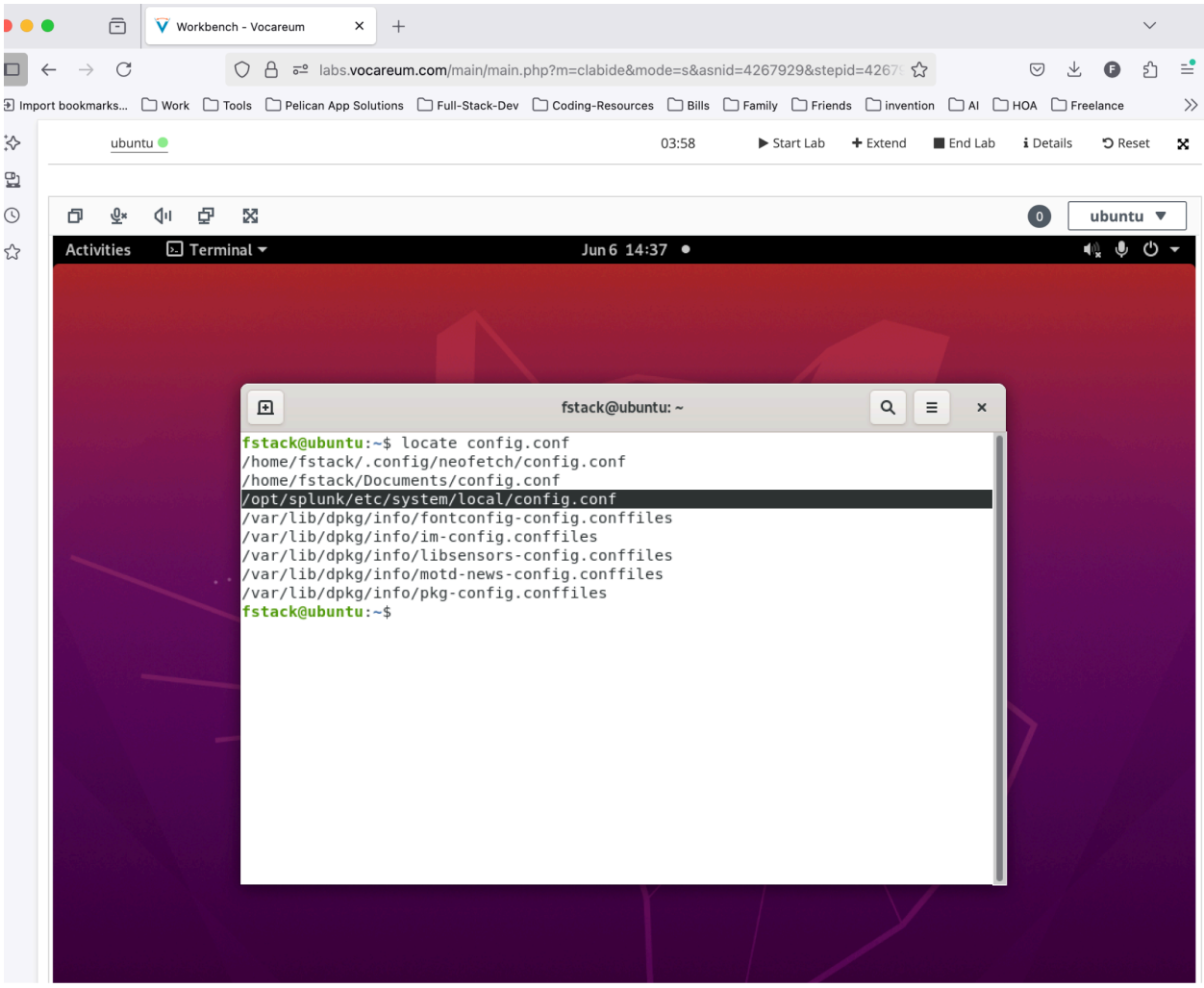
To prevent this kind of issue in the future, I would make sure the file permissions are set correctly from the start. Only the admin or high level SOC analysts should be able to make changes to important configuration files. I would use the command `sudo chmod 640` to set the right permissions, which would block anyone who isn't authorized from editing the file.

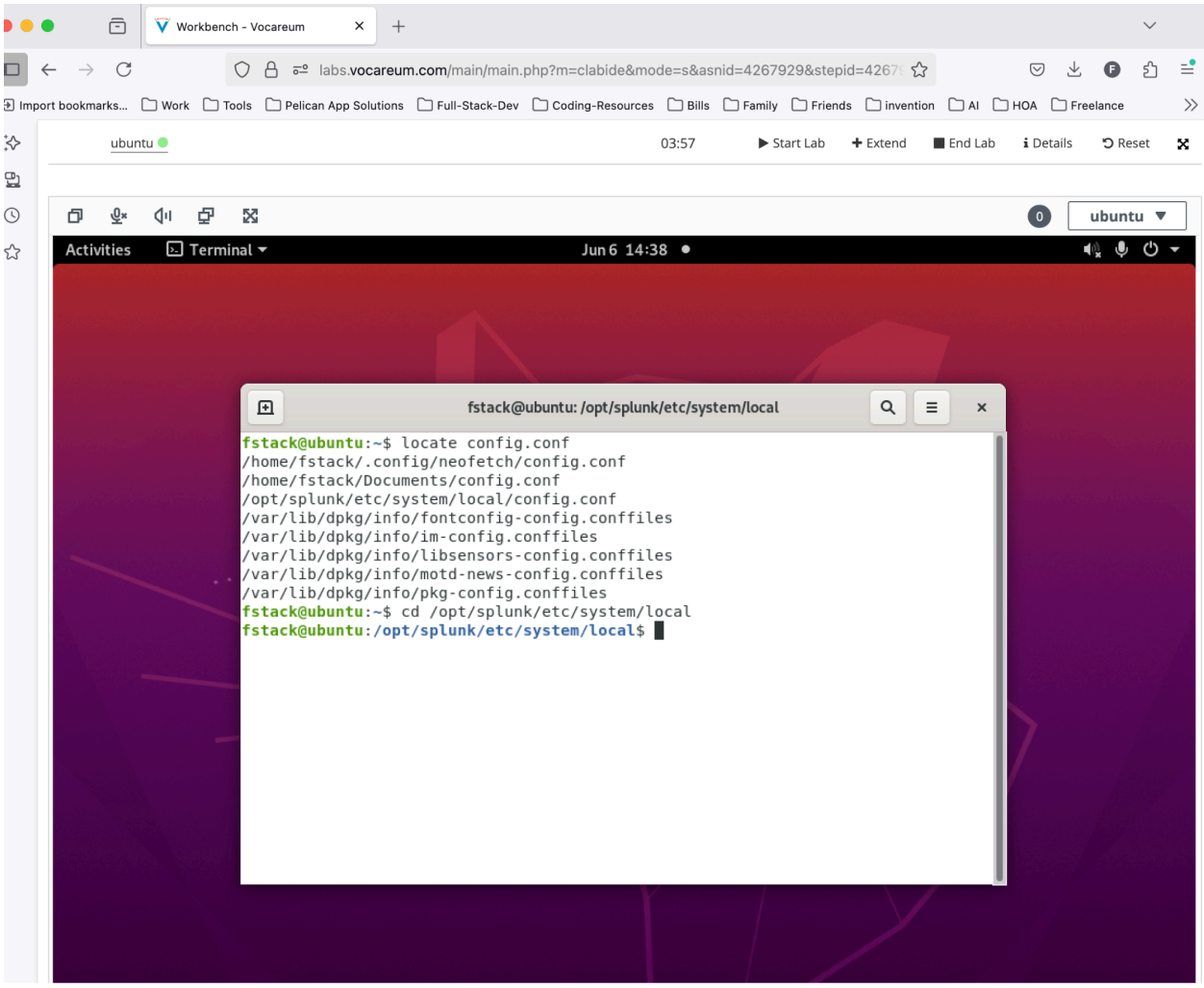
Monitor Integrity:

To monitor integrity with the md5sum hash I would check to see if there are any changes to the hash, if so this would tell me someone made an edit. I would then open and look in the file with nano to see what's been done

BELOW ARE THE PHOTOS IN ORDER FOR THE STEPS ABOVE (1-6)


Workbench - Vocareum
labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=4267929&stepid=4267
Import bookmarks...
Work
Tools
Pelican App Solutions
Full-Stack-Dev
Coding-Resources
Bills
Family
Friends
invention
AI
HOA
Freelance
ubuntu
03:59
Start Lab
Extend
End Lab
Details
Reset
0
ubuntu
Jun 6 14:35


Workbench - Vocareum
labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=4267929&stepid=4267
Import bookmarks... Work Tools Pelican App Solutions Full-Stack-Dev Coding-Resources Bills Family Friends invention AI HOA Freelance
ubuntu
03:58
Start Lab
Extend
End Lab
Details
Reset
ubuntu
Activities
Terminal
Jun 6 14:37
fstack@ubuntu: ~
fstack@ubuntu:~$ locate config.conf
/home/fstack/.config/neofetch/config.conf
/home/fstack/Documents/config.conf
/opt/splunk/etc/system/local/config.conf
/var/lib/dpkg/info/fontconfig-config.conffiles
/var/lib/dpkg/info/im-config.conffiles
/var/lib/dpkg/info/libsensors-config.conffiles
/var/lib/dpkg/info/motd-news-config.conffiles
/var/lib/dpkg/info/pkg-config.conffiles
fstack@ubuntu:~$


Workbench - Vocareum
labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=4267929&stepid=4267
Import bookmarks... Work Tools Pelican App Solutions Full-Stack-Dev Coding-Resources Bills Family Friends invention AI HOA Freelance
ubuntu
03:57
Start Lab
Extend
End Lab
Details
Reset
ubuntu
Activities
Terminal
Jun 6 14:38
fstack@ubuntu: /opt/splunk/etc/system/local
fstack@ubuntu:~$ locate config.conf
/home/fstack/.config/neofetch/config.conf
/home/fstack/Documents/config.conf
/opt/splunk/etc/system/local/config.conf
/var/lib/dpkg/info/fontconfig-config.conffiles
/var/lib/dpkg/info/im-config.conffiles
/var/lib/dpkg/info/libsensors-config.conffiles
/var/lib/dpkg/info/motd-news-config.conffiles
/var/lib/dpkg/info/pkg-config.conffiles
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$

Workbench - Vocareum

labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=4267929&stepid=4267

Import bookmarks... Work Tools Pelican App Solutions Full-Stack-Dev Coding-Resources Bills Family Friends invention AI HOA Freelance

ubuntu 03:53 Start Lab Extend End Lab Details Reset

Activities Terminal Jun 6 14:41 ubuntu

fstack@ubuntu: /opt/splunk/etc/system/local

```
fstack@ubuntu:~$ locate config.conf
/home/fstack/.config/neofetch/config.conf
/home/fstack/Documents/config.conf
/opt/splunk/etc/system/local/config.conf
/var/lib/dpkg/info/fontconfig-config.conffiles
/var/lib/dpkg/info/im-config.conffiles
/var/lib/dpkg/info/libsensors-config.conffiles
/var/lib/dpkg/info/motd-news-config.conffiles
/var/lib/dpkg/info/pkg-config.conffiles
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l config.conf
-rwxrwxrwx 1 root root 185 Sep 29  2022 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$
```

Workbench - Vocareum

labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=4267929&stepid=4267

Import bookmarks... Work Tools Pelican App Solutions Full-Stack-Dev Coding-Resources Bills Family Friends invention AI HOA Freelance

ubuntu 03:52 Start Lab Extend End Lab Details Reset

Activities Terminal Jun 6 14:42 ubuntu

fstack@ubuntu: /opt/splunk/etc/system/local

```
fstack@ubuntu:~$ locate config.conf
/home/fstack/.config/neofetch/config.conf
/home/fstack/Documents/config.conf
/opt/splunk/etc/system/local/config.conf
/var/lib/dpkg/info/fontconfig-config.conffiles
/var/lib/dpkg/info/im-config.conffiles
/var/lib/dpkg/info/libsensors-config.conffiles
/var/lib/dpkg/info/motd-news-config.conffiles
/var/lib/dpkg/info/pkg-config.conffiles
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l config.conf
-rwxrwxrwx 1 root root 185 Sep 29  2022 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$
```

Workbench - Vocareum

labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=4267929&stepid=4267

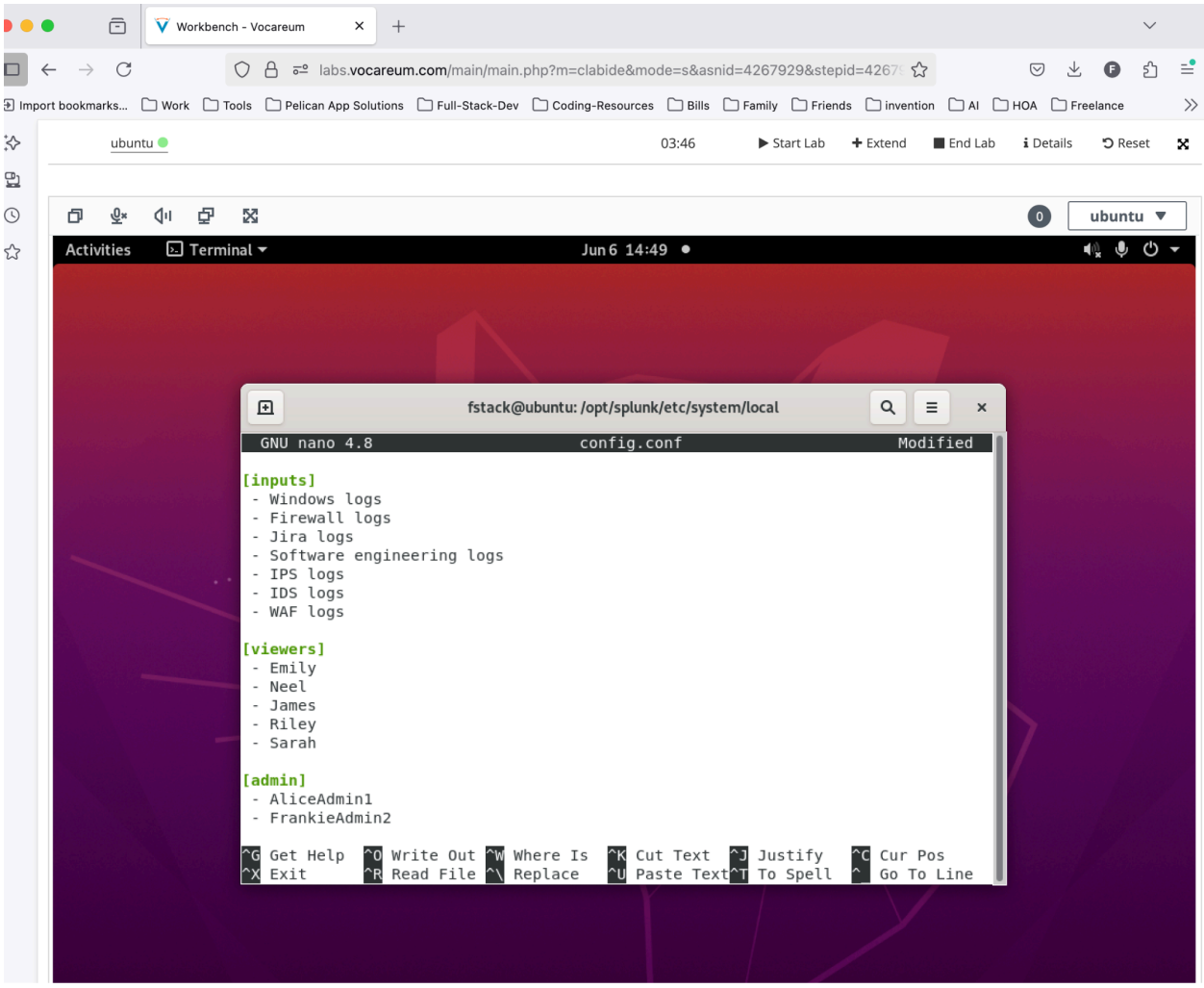
Import bookmarks... Work Tools Pelican App Solutions Full-Stack-Dev Coding-Resources Bills Family Friends invention AI HOA Freelance

ubuntu 03:49 Start Lab Extend End Lab Details Reset

Activities Terminal Jun 6 14:45 ubuntu

fstack@ubuntu: /opt/splunk/etc/system/local

```
fstack@ubuntu:~$ locate config.conf
/home/fstack/.config/neofetch/config.conf
/home/fstack/Documents/config.conf
/opt/splunk/etc/system/local/config.conf
/var/lib/dpkg/info/fontconfig-config.conffiles
/var/lib/dpkg/info/im-config.conffiles
/var/lib/dpkg/info/libsensors-config.conffiles
/var/lib/dpkg/info/motd-news-config.conffiles
/var/lib/dpkg/info/pkg-config.conffiles
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l config.conf
-rwxrwxrwx 1 root root 185 Sep 29  2022 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
c70754d9c7bab08a8c441f90c37f27eb  config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$
```


Workbench - Vocareum
labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=4267929&stepid=4267
Import bookmarks... Work Tools Pelican App Solutions Full-Stack-Dev Coding-Resources Bills Family Friends invention AI HOA Freelance
ubuntu
03:46
Start Lab
Extend
End Lab
Details
Reset
ubuntu
Activities
Terminal
Jun 6 14:49
fstack@ubuntu: /opt/splunk/etc/system/local
GNU nano 4.8 config.conf Modified
[inputs]
- Windows logs
- Firewall logs
- Jira logs
- Software engineering logs
- IPS logs
- IDS logs
- WAF logs
[viewers]
- Emily
- Neel
- James
- Riley
- Sarah
[admin]
- AliceAdmin1
- FrankieAdmin2
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line

Workbench - Vocareum

labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=4267929&stepid=4267

Import bookmarks... Work Tools Pelican App Solutions Full-Stack-Dev Coding-Resources Bills Family Friends invention AI HOA Freelance

ubuntu 03:44 Start Lab Extend End Lab Details Reset

Activities Terminal Jun 6 14:50 ubuntu

fstack@ubuntu: /opt/splunk/etc/system/local

```
fstack@ubuntu:~$ locate config.conf
/home/fstack/.config/neofetch/config.conf
/home/fstack/Documents/config.conf
/opt/splunk/etc/system/local/config.conf
/var/lib/dpkg/info/fontconfig-config.conffiles
/var/lib/dpkg/info/im-config.conffiles
/var/lib/dpkg/info/libsensors-config.conffiles
/var/lib/dpkg/info/motd-news-config.conffiles
/var/lib/dpkg/info/pkg-config.conffiles
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l config.conf
-rwxrwxrwx 1 root root 185 Sep 29  2022 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
c70754d9c7bab08a8c441f90c37f27eb  config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ nano config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ nano config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
22040081e75a89f945ad73f8e7ba9e70  config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$
```

Workbench - Vocareum

labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=4267929&stepid=4267

Import bookmarks... Work Tools Pelican App Solutions Full-Stack-Dev Coding-Resources Bills Family Friends invention AI HOA Freelance

ubuntu 03:43 Start Lab Extend End Lab Details Reset

Activities Terminal Jun 6 14:51 ubuntu

fstack@ubuntu: /opt/splunk/etc/system/local

```
fstack@ubuntu:~$ locate config.conf
/home/fstack/.config/neofetch/config.conf
/home/fstack/Documents/config.conf
/opt/splunk/etc/system/local/config.conf
/var/lib/dpkg/info/fontconfig-config.conffiles
/var/lib/dpkg/info/im-config.conffiles
/var/lib/dpkg/info/libsensors-config.conffiles
/var/lib/dpkg/info/motd-news-config.conffiles
/var/lib/dpkg/info/pkg-config.conffiles
fstack@ubuntu:~$ cd /opt/splunk/etc/system/local
fstack@ubuntu:/opt/splunk/etc/system/local$ ls -l config.conf
-rwxrwxrwx 1 root root 185 Sep 29  2022 config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
c70754d9c7bab08a8c441f90c37f27eb  config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ nano config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ nano config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ md5sum config.conf
22040081e75a89f945ad73f8e7ba9e70  config.conf
fstack@ubuntu:/opt/splunk/etc/system/local$ cp config.conf /home/fstack/
fstack@ubuntu:/opt/splunk/etc/system/local$
```