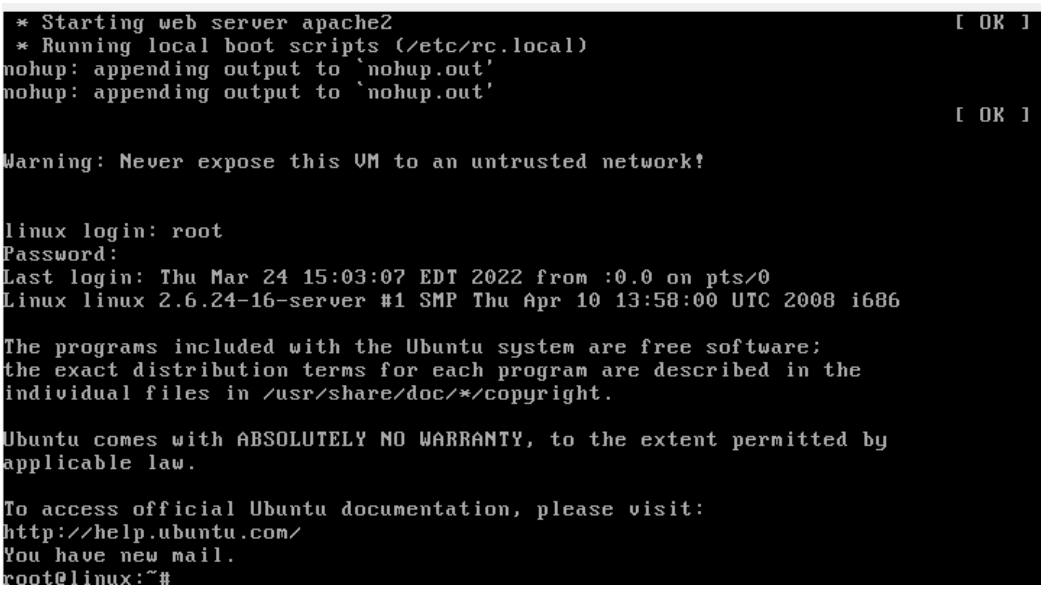
Audit

Gautham Krishna Kumar

1. Include a screenshot of a successful login once you have reset the root password.



2. Describe how you reset the password for the root account to login.

- Ubuntu 20.04 ISO file was mounted onto VirtualBox along with the live CD/DVD option enabled.
- While booting up Ubuntu, I selected “Try Ubuntu” option instead of going through the whole installation process.
- Opened the terminal and went into the root privileges.
- To look for the disk partitions, I used the lvdisplay command.
- Created a new directory to mount the partition.
- Used chroot and passwd to reset the password for the root account.

3. Is this Linux distribution Debian based or Red Hat based? Describe where you looked and how you discovered your answer.

The Linux distribution is Debian based.
The version is lenny/sid.
Reference Link: https://www.cyberciti.biz/faq/find-linux-distribution-name-version-number/
To check the version, we used the command cat /etc/debian_version

```
root@linux:~# cat /etc/debian_version
lenny/sid
root@linux:~# _
```

4. What is the exact distribution and version?

The exact distribution and version is Ubuntu 8.04 (hardy).

```
root@linux:~# cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.04
DISTRIB_CODENAME=hardy
DISTRIB_DESCRIPTION="Ubuntu 8.04"
root@linux:~#
```

5. Describe where you looked and how you discovered your answer. We have not covered how to determine this, but a Google search for “Linux get distribution and version” will show you some cool stuff.

From the reference link provided in Question 3, I was able to use the following commands to get the distribution and version:
cat /etc/debian_version
cat /etc/*-release
cat /etc/lsb-release

6. Is this version of this distribution still supported? Find information on why this might be important and discuss security issues with running unsupported distributions. This is something you will need to ask Google

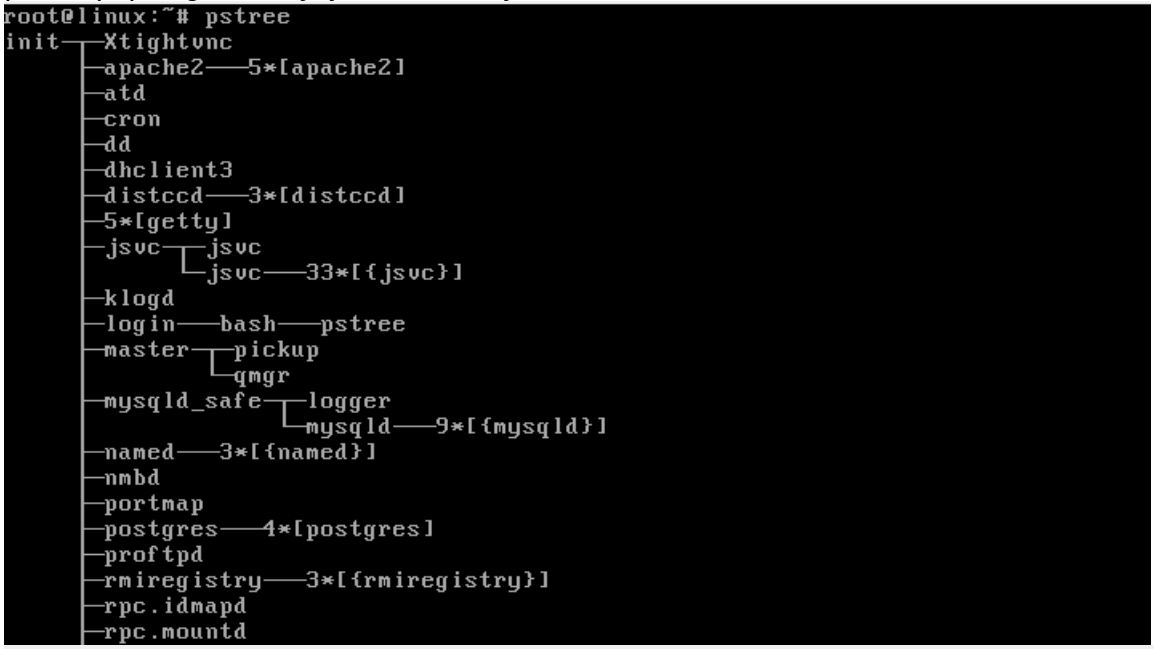
The version is no longer supported, and no further security updates and information are received in this version. The version reached the end – of – life on May 12th, 2011. The three main security issues of unsupported versions include:

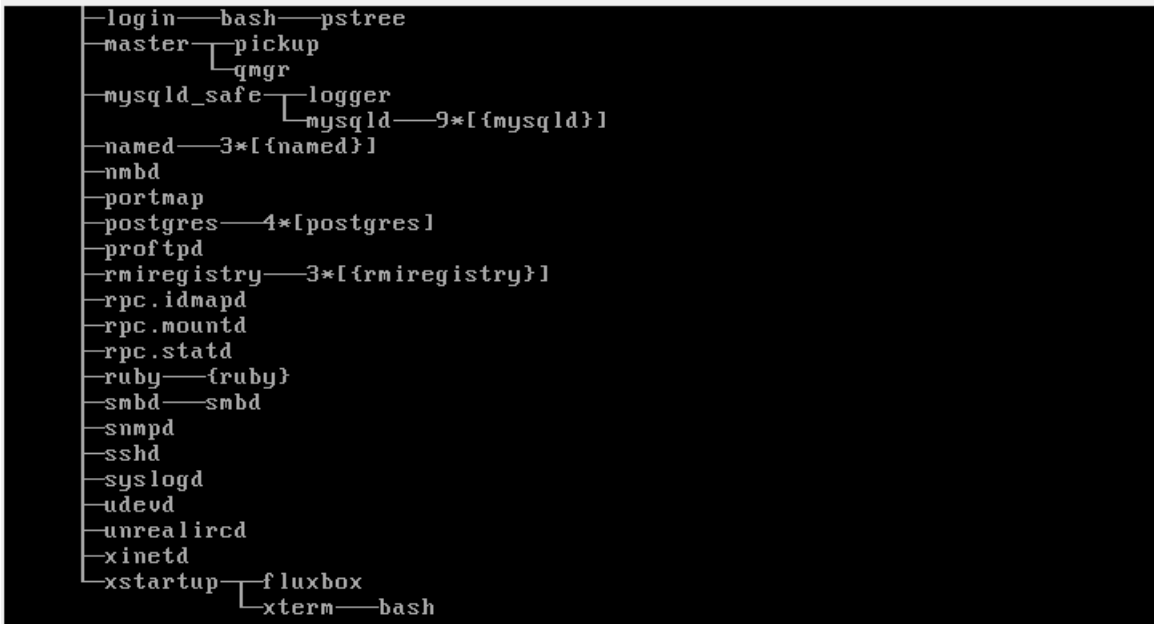
- No Security Patches: Without regular security patches, your systems get more and more vulnerable, resulting in an increased risk of being breached by malware and ransomware.
- Third-Party Software Outgrows Your Systems: Part of a good vendor-management strategy is choosing the right software for your business. Most software vendors don’t support outdated operating systems since there is little profit in doing so. In addition, if you continue to use an outdated operating system, you risk losing the ability to run third-party software.
- The Risk of Losing Customer Data: Unsupported operating systems are giant holes in your security, which put not only your data at risk, but your customers’ data too. If you handle sensitive information or personal data in your business (like medical records and credit card numbers), a breach can be extremely costly to your company, and you may even be held legally liable for resulting damages. Even without a malicious data breach, you could lose your data. Unsupported IT hardware and software could also just stop functioning without notice, and it may be impossible to recover data when it happens.

Reference Link: https://www.365tech.ca/three-dangers-of-running-an-unsupported-operating-system/

7. What services are running on the machine? Why is it important to know the services that are running on a machine? Give the installed versions of three of the services.

I ran the command pstree and some of the services which were running are: apache2, portmap, postgres, ruby, jsvc and many more.



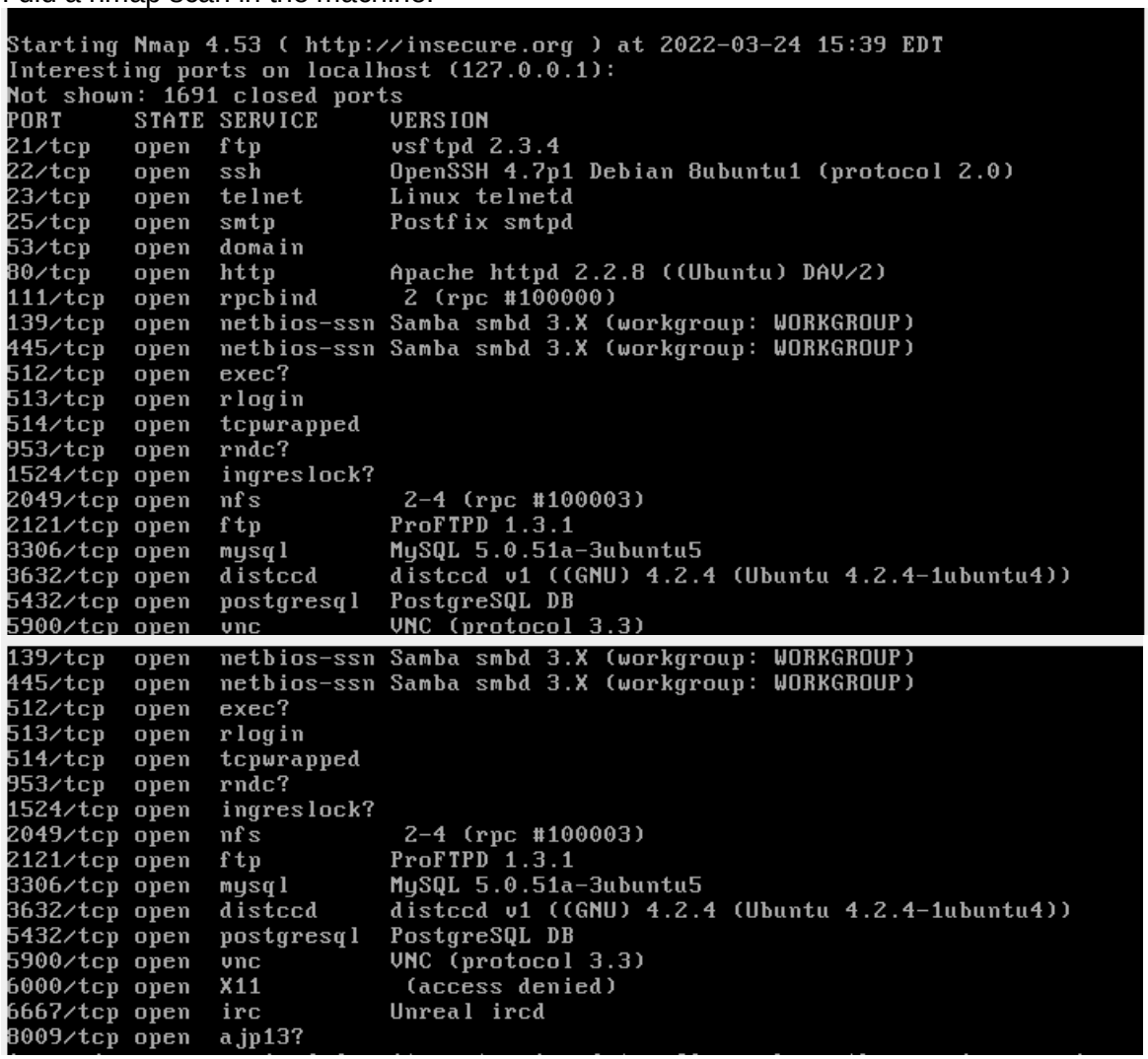


I found the versions of the services by doing a nmap scan in Question 8. Some of them are: Apache httpd 2.2.8

MySQL 5.0.51a-3ubuntu5
PostFTPD 1.3.1

8. What network ports are open and what services have opened those ports? Why is it important to know what ports are open? How might this step provide evidence of unauthorized use?

I did a nmap scan in the machine.



Knowing the open ports is important because we need to check if all the services are being executed in the designated port and not trying to allow unauthorized access and connection.

9. What run level does the system boot into? Why is it important to know what run level the system boots into?

The run level in which the system boots into is N 2. We can confirm the level by running the

command runlevel.

```
root@linux:~# who -r
         run-level 2  2022-03-24 17:12                   last=
root@linux:~# runlevel
N 2
root@linux:~# _
```

Knowing the run levels in which the system boots into is very important as they give administrators more control of the system they manage. The run levels of a system can be varied and changed. The user has the control over what system access is present at what level.

10. Is the firewall configured? You can check this using the iptables command. If so, what rule set? Discuss what these rules indicate and how this could affect system security? Note that iptables is always present. The question that you need to consider is the following: "Is iptables configured to actually do anything? You will need to read about iptables to determine how to review the rules. Google will continue to be your friend here.

To check whether the firewall is configured or not, we use the iptables command to view the rules.

```
root@linux:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@linux:~#
root@linux:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

We can see that that the table is empty which means the packets are allowed through all the tables. Hence, the firewall is NOT configured.

11. What SUID and SGID files exist on the system? List a few of these and explain why is it important to know these files exist? How does that relate to system security? The find on this machine may not support the –perm /6000 format. In that case, use the obsolete –perm +6000 instead.

I ran the command find . perm /6000 to view both the SUID and SGID files.

Some of the files include:
./etc/chatscripts
./var/mail
./etc/bind
./var/local
./usr/bin/nmap
./usr/bin/crontab

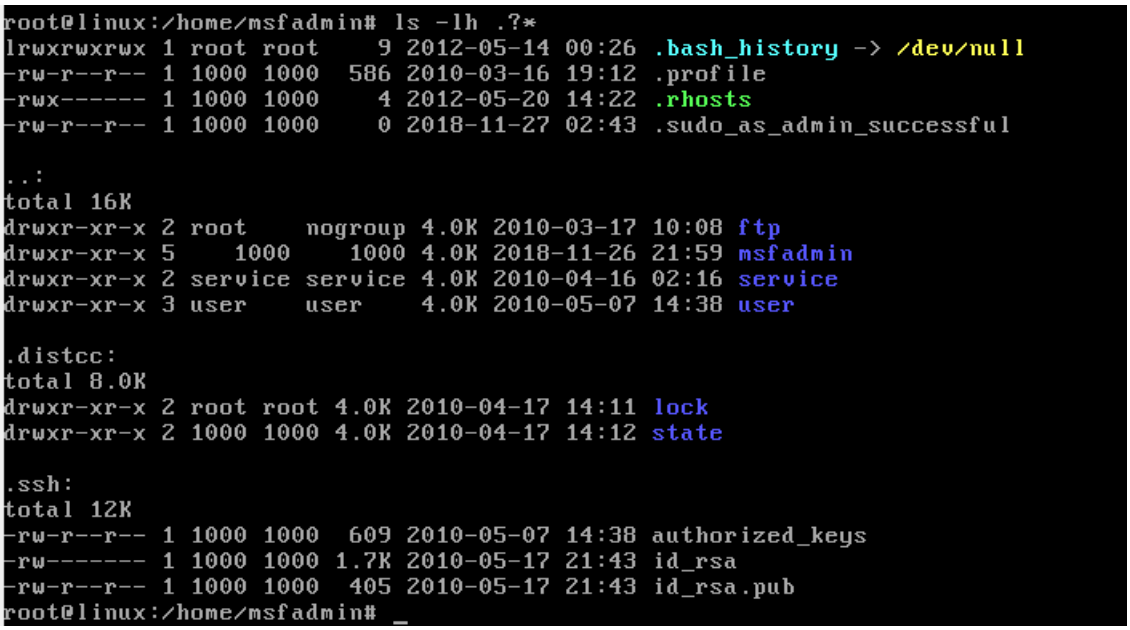
Any unauthorized user can enter the system and modify the system level permissions by setting the SUID and SGID bits. We can monitor these bits to make sure that no unauthorized users can enter the system and get system privileges.

12. Are there any files on the system that do not have an owner or group? List a few of these and explain why this might be important information.

There are quite a few files in the /home/msfadmin directory which do not have an owner or a group. Some of the files are:
./home/msfadmin/.ssh
./home/msfadmin/.profile

Whenever a new user is created in Linux, the unowned files are automatically owned by the new user making it more dangerous depending on what type of user is the new user.

13. What hidden files exist on the system? Again, list only a few of these and discuss how an attacker might use hidden files while compromising a system. The patterns you want to search for are '.??*' and '.[^.]'. The quotes around the patterns are important



Some of the hidden files are:
/home/msfadmin/.ssh/authorized_keys
/home/msfadmin/.ssh/id_rsa

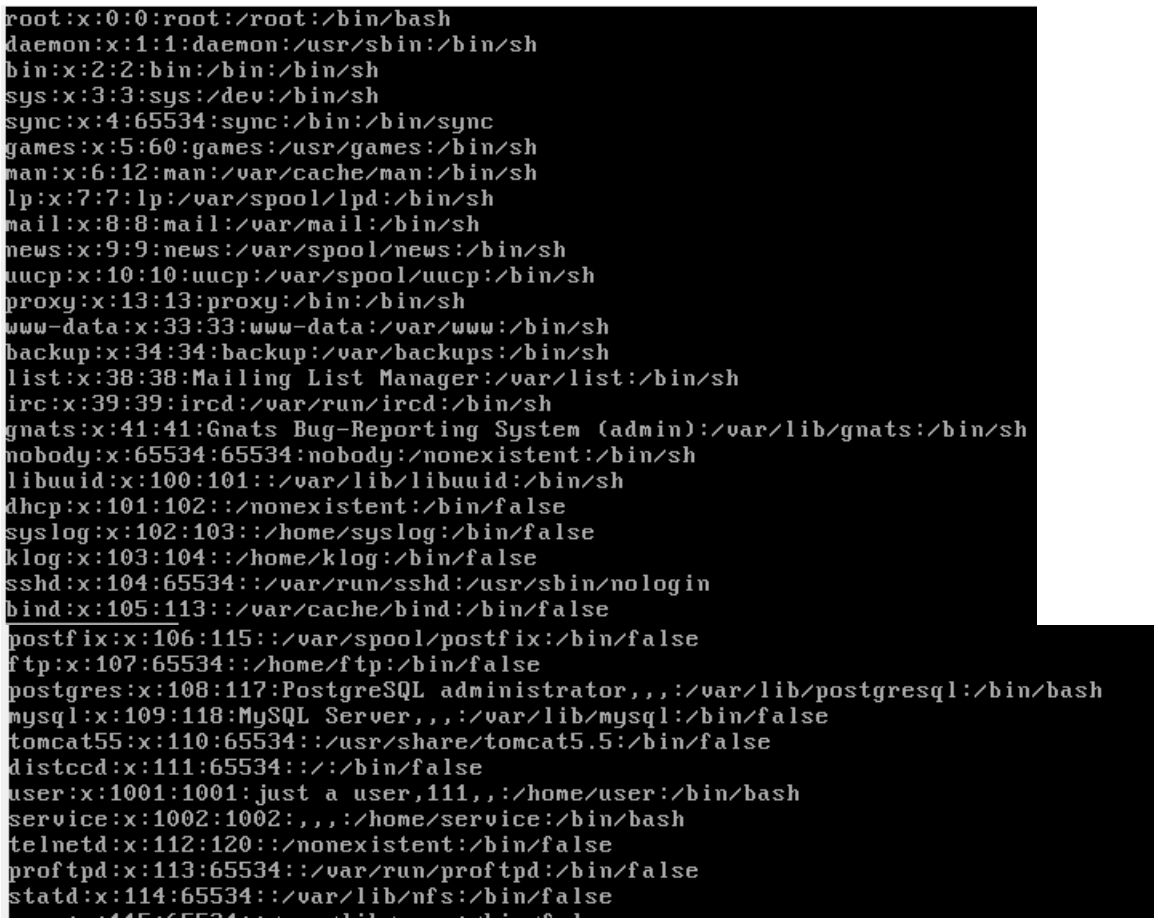
The attacker will take advantage on these hidden files such as the ssh keys and id in order to gain root access into the system.

14. Does this system use an external authentication source? Why would it be important to know if the system is using an external authentication source? How to do this was only hinted at in the videos. Try asking Google but do not spend too much time trying to figure it out.

It is important to know whether the system is using external authentication and whether it should be given access or not. If provided access, the system level should be determined too. Here, the system is using LDAP as an external authentication source.

Reference Link: https://help.ubuntu.com/community/OpenLDAPServer

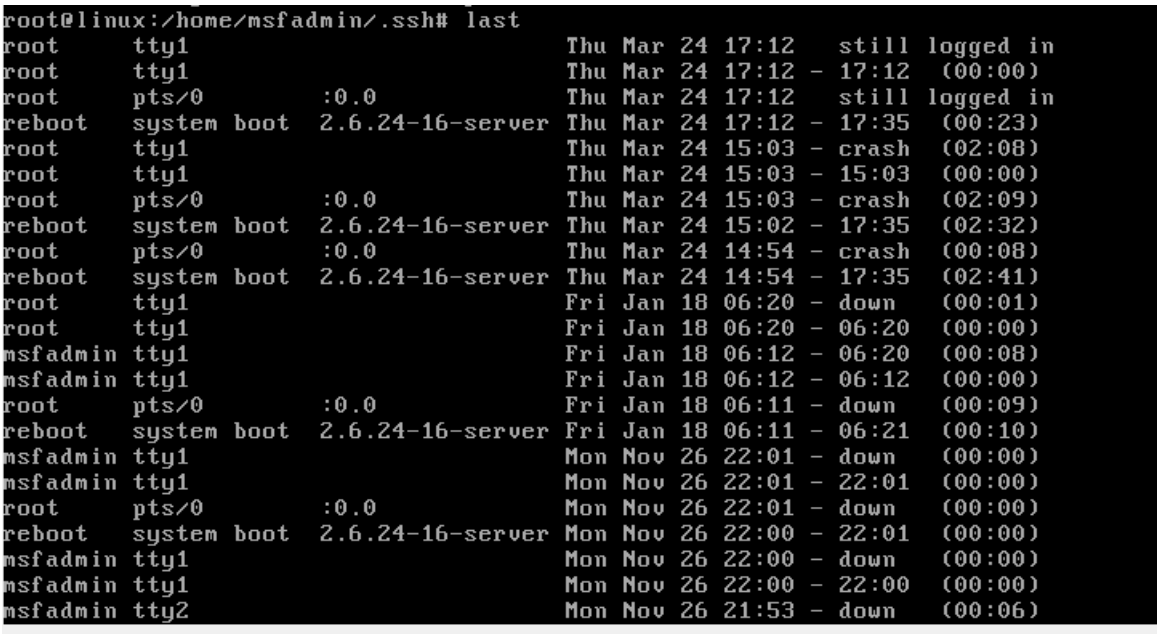
15. What local users are on the system? Do any users look suspicious? Discuss why these look suspicious.



Some of the local users include:
sshd
mail
proxy
user

In my opinion, I feel the local user named “user” looks suspicious.

16. What users have logged into the machine recently? From where? Why is it important to check this frequently? What are a couple indications if you check and find that nobody has logged on recently (especially if this a heavily used machine)?



```
root@linux:/home/msfadmin/.ssh# last
root     tty1                         Thu Mar 24 17:12   still logged in
root     tty1                         Thu Mar 24 17:12 - 17:12  (00:00)
root     pts/0        :0.0            Thu Mar 24 17:12   still logged in
reboot   system boot  2.6.24-16-server Thu Mar 24 17:12 - 17:35  (00:23)
root     tty1                         Thu Mar 24 15:03 - crash  (02:08)
root     tty1                         Thu Mar 24 15:03 - 15:03  (00:00)
root     pts/0        :0.0            Thu Mar 24 15:03 - crash  (02:09)
reboot   system boot  2.6.24-16-server Thu Mar 24 15:02 - 17:35  (02:32)
root     pts/0        :0.0            Thu Mar 24 14:54 - crash  (00:08)
reboot   system boot  2.6.24-16-server Thu Mar 24 14:54 - 17:35  (02:41)
root     tty1                         Fri Jan 18 06:20 - down   (00:01)
root     tty1                         Fri Jan 18 06:20 - 06:20  (00:00)
msfadmin tty1                         Fri Jan 18 06:12 - 06:20  (00:08)
msfadmin tty1                         Fri Jan 18 06:12 - 06:12  (00:00)
root     pts/0        :0.0            Fri Jan 18 06:11 - down   (00:09)
reboot   system boot  2.6.24-16-server Fri Jan 18 06:11 - 06:21  (00:10)
msfadmin tty1                         Mon Nov 26 22:01 - down   (00:00)
msfadmin tty1                         Mon Nov 26 22:01 - 22:01  (00:00)
root     pts/0        :0.0            Mon Nov 26 22:01 - down   (00:00)
reboot   system boot  2.6.24-16-server Mon Nov 26 22:00 - 22:01  (00:00)
msfadmin tty1                         Mon Nov 26 22:00 - down   (00:00)
msfadmin tty1                         Mon Nov 26 22:00 - 22:00  (00:00)
msfadmin tty2                         Mon Nov 26 21:53 - down   (00:06)
```

Msfadmin was the user who had logged in recently into the system.
Checking system logs is very important as we can monitor who is logging into the system and when. Unauthorized users can also be detected in the logs. Some people delete the logs, making it difficult to monitor the user's login.