Audit

Name	Sahil Yuvraj Bhirud

1. Upload 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.

I used a LiveCD method to reset the Linux Machine's password and performed the following steps while doing so:

1. Downloaded and mounted Ubuntu 16.04 desktop iso file through the CDROM of the Linux System.
2. From the boot menu, I chose the "Try Ubuntu" option and opened Terminal.
3. Next, I used the fdisk command to check the disk partitions.
4. Created and mounted a directory to the disk which contained the Linux Machine.
5. Used the **chroot** command to open up the shell of the Linux machine.
6. Next, used **passwd** command to enter a new password for the machine.

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.

And Version is **lenny/sid.**

I Googled my query and found it on https://unix.stackexchange.com/questions/6345/how-can-i-get-distribution-name-and-version-number-in-a-simple-shell-script

4. What is the exact distribution and version?

Ubuntu 8.04 (hardy) with Linux Version is 2.6.24

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.

I Google searched how to get the Linux distribution and version. There were a lot of commands which would display the Linux distribution viz. **/etc/os-release, /etc/lsb-release, lsb_release -a, /etc/issue, /etc/redhat-release, /etc/debian_version, etc.**

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

This version is not supported now and has been archived since 2012. It receives no new security updates since then too.

The security issues with unsupported distributions are:

1. **No More Security Patches or Updates Leaves the System at Risk** – Adversaries can dissect the update and reverse engineer the fix to find the security hole that was patched and then try to exploit that vulnerability in the unsupported distribution.
2. **Loss of Functionality** – 3rd party applications may not work as efficiently as they do on the updated versions of the system. Daily tasks can consume more time than necessary.
3. **Customer Data at Risk** – The damage to the reputation due to this will be detrimental (fusetg).

   Other risks of running a unsupported software are Ransomware, Business Disruptions, Third Party Risk, etc. (bitsight)

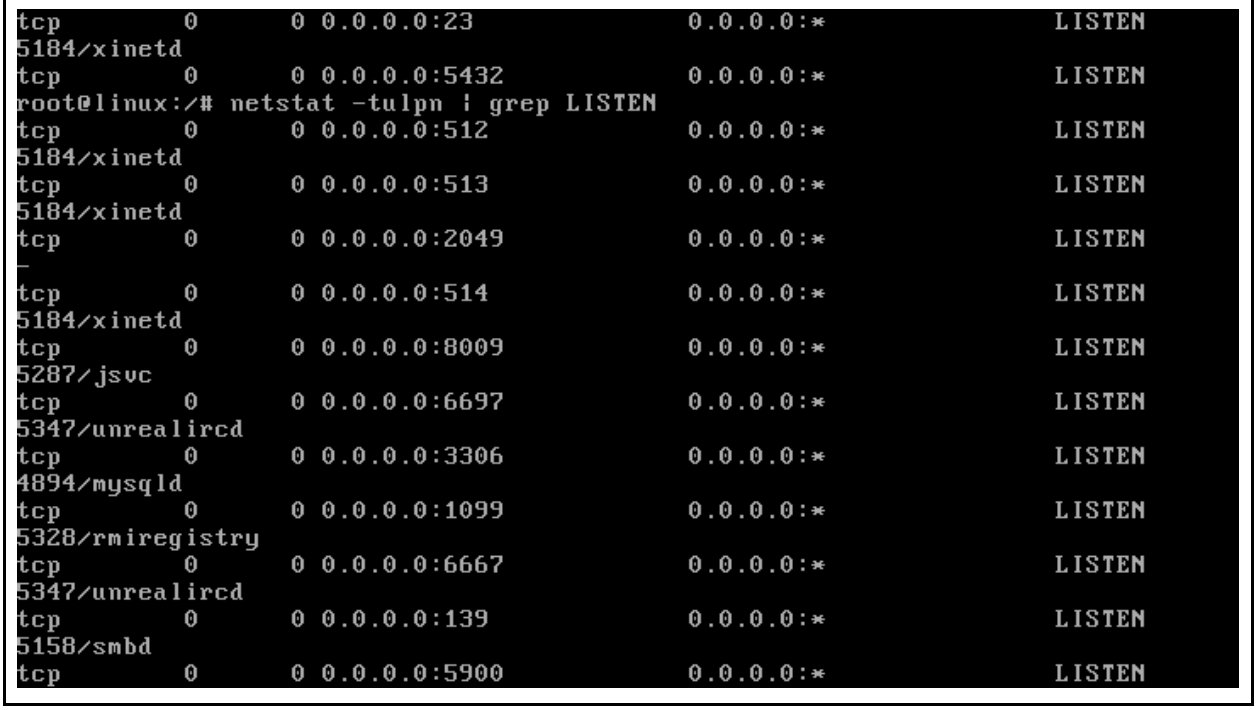
7. What services are running on the machine? Why is it important to know the services that are running on a machine? Give the installed versions of three of the services.

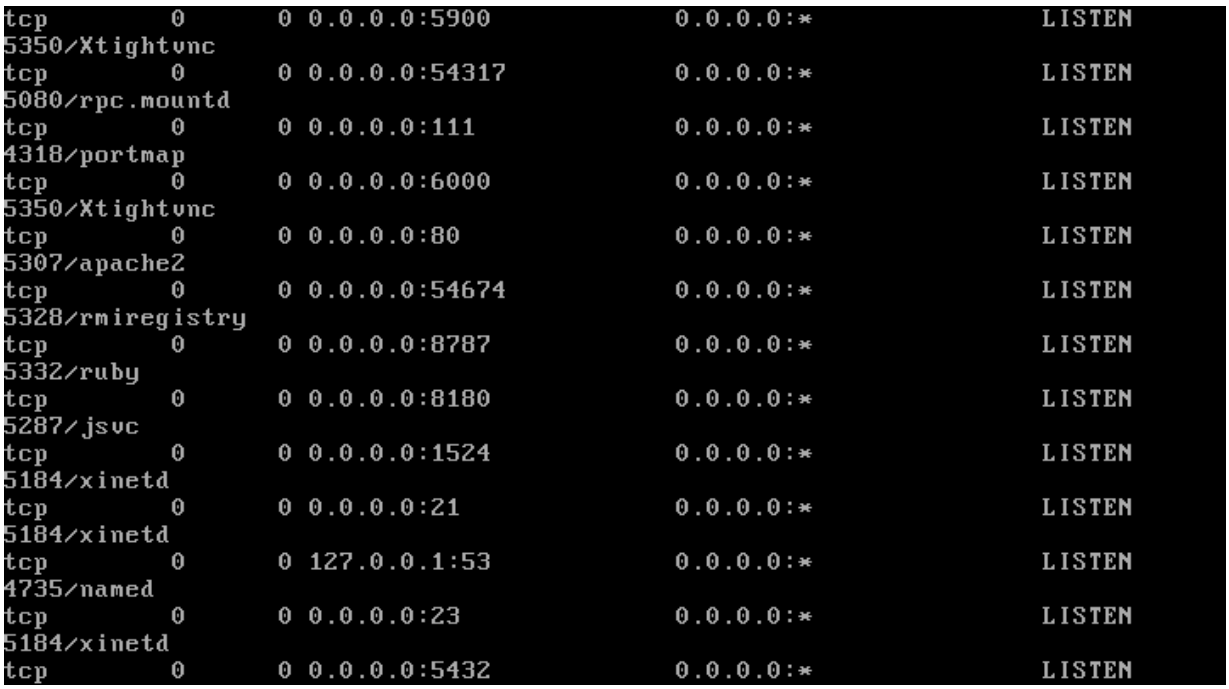
Running services: xinetd, rmiregistry, jsvc, unrealircd, mysqld, smbd, Xtightvnc, rpc.mountd, portmap, apache2, ruby, named, sshd, postgres, master, rpc.statd, distccd and nmbd

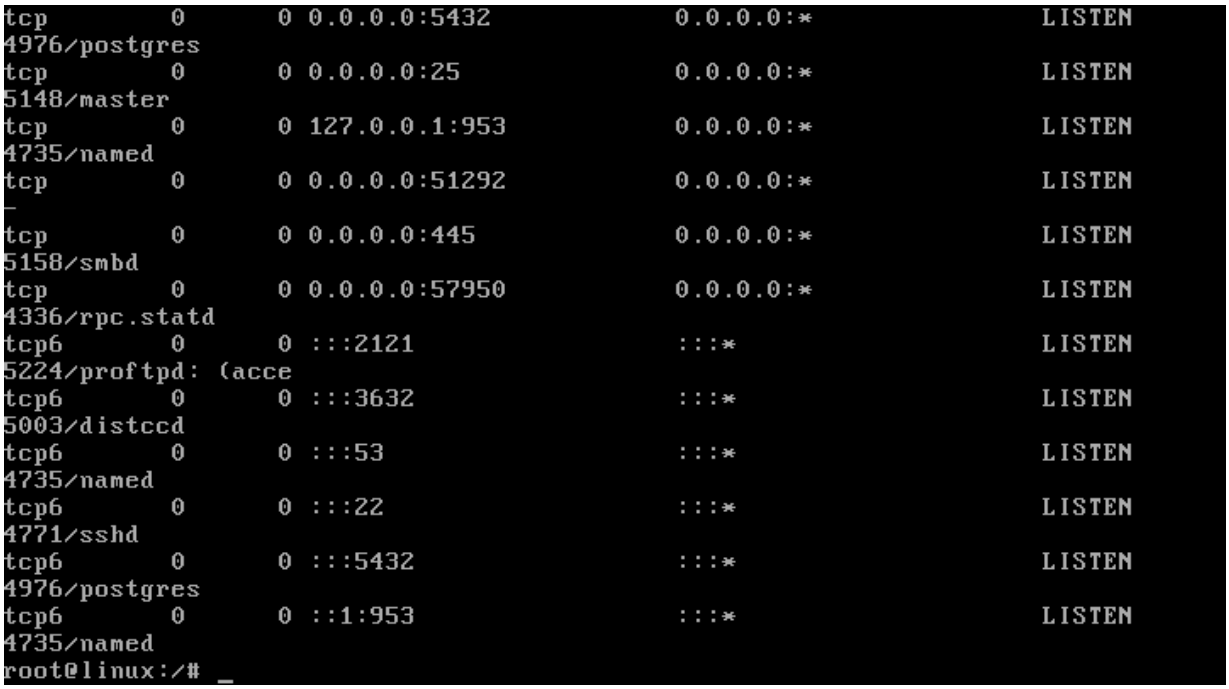
Knowing which services are running helps us to know which unwanted services are running which are harming the performance of the system. We also come to know if there are some suspicious services running on our system.

Installed versions of services:
Apache2 – 2.2.8
Mysqld – 5.0.51a-3ubuntu5
Postgres – 8.3.1

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?







Mysql is using port 3306
Apache is using port 80
Jsvc is using port 8009

It is important to know which ports are open because we need to know if all the running services are using only the designated ports and are not trying to open a remote connection with some unauthorized system.

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

N 2
Runlevels give administrators increased control of the system they manage. System's runlevel can be changed, as can the services which run inside the runlevels. This gives the user complete control over what services the system has access to at any given time.

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.

The firewall is not configured. When we check it using the iptables command, we see a table which is said to be an empty table which means that all the packets are allowed through each table.

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.

Some of the many SUID and SGID files are:
./usr/bin/sudo
./usr/sbin/pppd
./var/mail
./etc/chatscripts

Setting the SUID and SGID bits can provide a non-root user to modify the system level permissions. By monitoring these bits, we can make sure that no non-root user is getting elevated 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.

Yes, there are many such files and apparently all these files are in the **./home/msfadmin/** directory. Some of them are:
./home/msfadmin/.ssh
./home/msfadmin/.profile
./home/msfadmin/.distcc

In Linux if a new user is created then all the unowned files are automatically owned by the new user. This will become dangerous if the new user is an adversary.

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
/home/msfadmin/.ssh/authorized_keys
/home/msfadmin/.ssh/id_rsa

The hidden files contain sensitive information about the ssh keys. So, if an attacker gets his hands on these files then it would be a piece of cake for him to get a root access for the targeted 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.

Yes, it uses LDAP server as an external authentication source. It would be important to know if the system is using external authentication source as it decides whether an user should be granted access to the system or no and if yes then, level of access is also decided by it.

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

Some of the many local users are:
Sshd
Klog
Mail
Proxy

It is difficult to find a suspicious one in a long list, but I think that the local user ‘user’ could be a malicious one.

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)?

The most recent login was done by **msfadmin** from group **audio, dip, admin** and also from

shadow groups ‘adm’, ‘dip’.

It is important to check login logs because there might be an unauthorized user trying to log into the system and he could be caught if we check this log. It is also a problem if we see that not a lot of the users are logging into the machine because maybe there is someone who is clearing the logs after performing modifications on the system.

References:

1. Fusetg - https://fusetg.com/dangers-running-unsupported-operating-system/
2. Bitsight - https://www.bitsight.com/blog/outdated-software-issues