|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | | **System Server Administration**  **Lab Practice 10** | | | |  |  | | | **Topic:** | Security Management on a  Linux Debian 8.0 Server | | |  |  | | |  |  | | |  | | **ID Number** | **Name** | | | **E-mail** | |  |  | | |  | |

1. Introduction

Learn about the configuration files used to manage a Linux Debian 8.0 server’s security. Write down on a paper the answers to the questions asked in this lab.

1. Desarrollo
2. Open your Virtual Box software installed on your host Operating System.
3. Select the **Linux Debian 8.0**  VM and click on the button **“🡪 Start”**
4. Try logging in as root to your VM using the graphic interface (directly through the VM, don’t use SSH).
5. Could you enter to GNOME as root? No
6. Analyze the code in the file:

**/etc/pam.d/gdm-password**

1. Which line of the code do you have to erase or comment to be able to log in as root to GNOME? #auth required pam\_succeed\_if.so user != root quiet\_success
2. Try commenting the line you chose by adding a # symbol to the beginning and restart the gdm3 service with the following command:

**service gdm3 restart**

1. Could you enter now to GNOME as root? Yes
2. Open a ssh remote session via PuTTY from your host machine to your Linux Server and log in as root.
3. Open another ssh remote session via PuTTY from your host machine to your Linux Server and log in as AXXXXXXXX.
4. Type the command “**su”** in both sessions
5. What was the difference between these sessions?

On the AXXXXXX it took me to ‘/home/a01231278’ and password was required.

1. In which path/file does this security is specified and what instruction (**PAM** module) causes this behavior? /etc/pam.d/su
2. Configure **PAM** so that only the root user can log in through SSH. Don’t forget to back up the original configuration file by renaming it, so that you can recover the original configuration when this lab practice is finished. Once you have modified the PAM configuration file for the SSH, restart the service or SSH demon with this command:

**service ssh restart**

1. Now open two ssh sessions, one of them as root and the other as AXXXXXXXX.
2. Could you enter to both sessions? No, I could only do it with root
3. Which PAM configuration file did you modify? (Include the path)

/etc/ssh/sshd

Which command did you add to this file? auth required pam\_succeed\_if.so user = root quiet\_success

1. Restore the original file deleting the one you modified and renaming the original file with the name it had.
2. Try again to enter to the ssh sessions as root and as AXXXXXXXX.
3. Could you enter to both sessions? Why? Yes, the original configuration was necessary this time.
4. Using the TCP Wrapper files, what files (include path) would you modify in order to allow the following situations and what content would each file have?
   1. That only your Host Machine IP address might connect with a ssh session to your Server (As we use Virtual Box, the IP address of your server won’t be the same, look for it within the SSH open session using the command **who --ips**)

/etc/host.allow

sshd: 10.0.2.2

/etc/host.deny

ALL: ALL

* 1. Try logging in from a classmate’s laptop.

1. Now, configure with IPTables a rule that doesn’t allow you to ping your server, by blocking the ICMP packets.
   1. Use the command **iptables -L** to display a list of chains and rules. As the packet filter table hasn’t been manipulated, this command will return the three basic chains, without any rules.
   2. Type the following command to see how the ping command responds:

**ping -c1 127.0.0.1**

* 1. Does the ping respond? Copy the result in the answer sheet.

root@A01231278debian:~# ping -c1 127.0.0.1

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

64 bytes from 127.0.0.1: icmp\_seq=1 ttl=64 time=0.014 ms

--- 127.0.0.1 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 0.045/0.045/0.045/0.000 ms

* 1. Let’s add (-A) a rule to the INPUT chain that test all packets from the ICMP protocol (-p), coming from 127.0.0.1 (source, -s) and then make them jump (-j) to the DROP target with the following command:

**iptables -A INPUT -p ICMP -s 127.0.0.1 -j DROP**

* 1. Verify the creation of this rule with the command **iptables -L**
  2. Try again to see how the ping responds:

**ping -c1 127.0.0.1**

* 1. Does the ping respond? Copy the result in the answer sheet.

root@A01231278debian:~# ping -c1 127.0.0.1

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

* 1. Erase the recently created rule using this command:

**iptables -D INPUT -p ICMP -s 127.0.0.1 -j DROP**

* 1. Check that the rule has actually been deleted with the command **iptables -L**

1. Type **exit**  to end the **PuTTY**  sessions
2. Shutdown your Debian server clicking on the arrow in the upper right corner the **Power Button**
3. Review

Hand in to your teacher your paper with the answers to the questions of this lab practice.