**Name: Oscar Ynoa**

**Student Id: 00308560**

**Course: Linux Administration (CIS-245-O1A)**

**Subject: Ubuntu Server Networking**

**Professor: Adrianna Holden-Gouveia**

**Due Date: 10/17/2021**

**Network Administration Linux Ubuntu Server**

**I truly think the best option to start whit this assignment would be with the question. What we have in our servers and the dates those changes were made? Just as a starter. To see what we have installed with yum I recommend this command apt list –installed | less. We use the less if we want to see all the information. In ubuntu you can’t just scroll up.**

**Texto

Descripción generada automáticamente**

**Also, I would like to see who is logged in the server. The w command shows information about the Linux users currently on the server, and their running processes. For example: Their current time .How long the Linux server has been running How many users are currently logged on Linux. The system load averages for the past 1, 5, and 15 minutes. To be honest I considered this one of the best commands for doing checking in your network.**

**We use the w command to display the users online in our server.**

**Texto

Descripción generada automáticamente**

**Further with this there is another command called who. The who command let me see who is logged on the systems.**

**Texto

Descripción generada automáticamente**

**Who -a or who -all to display all details of current logged in user**

**Texto

Descripción generada automáticamente**

**Next the ID command. This is used** **to display user identification information. Just need to type id + the user.**

**Imagen que contiene Patrón de fondo

Descripción generada automáticamente**

**last command will give login history for a specific username. If we don’t give any argument for this command, it will list login history for all users. This command is amazing. Full control and observation about the users. Logs information. The command is last oscar**

**Texto

Descripción generada automáticamente**

**The next command works to see all the users in our network. Even if they are not connected in the moment. cat /etc/passwd | awk -F: '{print $1}' This just print their names.**

**The Awk command let me print the first field of information.**

**Texto

Descripción generada automáticamente**

**Just to finish with the users in our server for fun. Let’s try the command without awk to see where the users are allocated and do something for groups information.**

**Each line in the file has seven fields delimited by colons that contain the following information:Username.Encrypted password (x means that the password is stored in the /etc/shadow file).User ID number (UID).User’s group ID number (GID).Full name of the user (GECOS).User home directory. Login shell (defaults to /bin/bash). This is all the information we can get from the command cat /etc/passwd**

**Texto

Descripción generada automáticamente**

**Let’s find out about groups.** **/etc/group Defines the default system group entries for system groups that support some system-wide tasks, such as printing, network administration, or electronic mail. The command is cat /etc/group**

**Group name: Contains the name assigned to the group.**

**group-password (x):x in this field indicates that shadow passwords are used.**

**GID: Contains the group’s GID number.**

**username-list :List of users that are members of the group**

**Imagen que contiene Texto

Descripción generada automáticamente** **Texto

Descripción generada automáticamente**

**Let’s jump on in some basics of Networking like Knowing your Ip, DNS , Ports, and other important information.**

**Ifconfig (interface configurator) is one of the most basic and commonly used commands for finding network details. It is also used to configure network interface parameters.**

**We can use this command to get the IP address, MAC address, and MTU of available networks.**

**Texto

Descripción generada automáticamente**

**The command is cat /etc/resolv.conf**

**This allows us to find our DNS Ip Address. First difference on ubuntu server. But does the function.**

**Texto

Descripción generada automáticamente**

**Netstat -a This command is used to display the information about the tcp and udp**

**Interfaz de usuario gráfica, Texto

Descripción generada automáticamente**

**Netstat -s**  **gets all details about ports**

**Imagen de la pantalla de un celular de un mensaje en letras negras

Descripción generada automáticamente con confianza baja** **Texto

Descripción generada automáticamente**

**Whois amazon.com To display the information of a webpage. I did not need to install it surprisingly.**

**Texto

Descripción generada automáticamente**

**Texto

Descripción generada automáticamente**

**Texto

Descripción generada automáticamente**

**Texto

Descripción generada automáticamente**

**Let’s do something with the firewalls to finish this and go with the script.**

**firewall-cmd --list-all: Check for all open ports and services**

**Important notice. TO become root in ubuntu server we use sudo -i**

**Texto

Descripción generada automáticamente**

**systemctl status firewalld This allow us to see if our firewall is active and check the status of it.**

**Texto

Descripción generada automáticamente**

**Script Instructions**

**Texto

Descripción generada automáticamente**

**Read -p: This command read the user input before going into the next line.**

**tee -a** : **This command will display the output in the terminal and then append the output into a file.**

**Head and Tail -number : I used this as a combination to limit the output of information from large commands and display the information I wanted from a command. Head beginning . Tail at the end.**

**echo** : **the echo command output the strings of the written argument.**

**read <variable>:** **The read command will read the user input and stored as a variable.**

**How to run the script**

**Explanation: We need to use the root command because we want to see user’s inputs. We need admin permission here.**

**The command is su -i**

**A reminder before running the script: The script needs permissions to be executable.**

**To make the script executable we use** **chmod 755 + Filename**

**Texto

Descripción generada automáticamente**

**To run the script, we use the command ./Filename to run the script. In my case it would be ./user.sh**

**The script starts showing the active users in the serve or who is connected right now.**

**Texto

Descripción generada automáticamente**

**It will ask for a user to see the last 10 logins it has made so. We type a user.**

**Texto

Descripción generada automáticamente con confianza media**

**Here it will ask to type a user to see the last 10 commands performed in the console. So, we type a username. I created one as an example just to see if it worked and it did.**

**Texto

Descripción generada automáticamente**

**Later it will ask to press enter to show network information. I set a limit in the script command to show just this part. This can be changed.**

**Texto

Descripción generada automáticamente**

**We press enter again to see the Ip of the net .**

**Texto

Descripción generada automáticamente**

**Later It will ask you to type a domain to do an observation in a webpage. The thing is that I made it use whois. We will try with the college webpage to see what we found.**

**Texto

Descripción generada automáticamente**

**We press enter to display information about the firewall ports.**

**Texto

Descripción generada automáticamente**

**And Press enter again to display if the firewall is active.**

**Texto

Descripción generada automáticamente**

**And that is all. Thank you!**

**Why did I choose These commands?**

**With this I hope to cover most of the essentials and the importance of the user’s and groups about how to look for who is connected and when it was their last connection and what kind of power that the users have. I truly think that knowing who is in your server and what it does and the kind of power it has is vital information at the moment of analyzing and maintain your network. I will display the w command to see who is active in the server. In this way I will know who is connected. From the user’s I will use the last command to display the last 10 loggings from a user. This command works as long as the user has made a connection. Next, I would like to see the last things they were doing. I used the command cat /home/$users/.bash\_history to see their last 10 inputs in the command line.**

**Furthermore, with the Network itself. I would like to explain why I want to use the next commands in my script I will use netstat and ifconfig to display the network information to monitor and analyze what is on my net at that current moment. If there is somebody like accessing a webpage that I have no knowledge about it. The script let me use an option called whois to just type the domain of the webpage and I can see a lot of information there from it.**

**Lastly, I would like to check my firewall ports in the server and the status available of the firewall. Just in case to be careful. I thought too much about what commands to use just as an overview of the net. At the beginning I wasn’t thinking of adding any information about user’s or the firewall. But as I was doing my research. That information caught my attention and I decided to add something with user plus firewalls. Just as a measure to check the server. It truly was a challenge to display the last 10 commands of a user used in the server, but it was fun.**

**Sources**

[**https://linux.die.net/man/8/ping**](https://linux.die.net/man/8/ping)

[**https://www.javatpoint.com/linux-networking-commands**](https://www.javatpoint.com/linux-networking-commands)

[**https://www.redhat.com/sysadmin/7-great-network-commands**](https://www.redhat.com/sysadmin/7-great-network-commands)

[**https://www.networkworld.com/article/3233306/more-ways-to-examine-network-connections-on-linux.html**](https://www.networkworld.com/article/3233306/more-ways-to-examine-network-connections-on-linux.html)

[**https://www.networkworld.com/article/3228127/getting-linux-to-ignore-pings.html**](https://www.networkworld.com/article/3228127/getting-linux-to-ignore-pings.html)

[**https://www.fosslinux.com/42935/linux-networking-commands.htm**](https://www.fosslinux.com/42935/linux-networking-commands.htm)

[**https://www.educba.com/networking-commands/**](https://www.educba.com/networking-commands/)

[**https://javarevisited.blogspot.com/2010/10/basic-networking-commands-in-linuxunix.html#axzz79npqnTcH**](https://javarevisited.blogspot.com/2010/10/basic-networking-commands-in-linuxunix.html#axzz79npqnTcH)

[**https://linuxconfig.org/redhat-8-stop-start-firewall**](https://linuxconfig.org/redhat-8-stop-start-firewall)

[**https://www.configserverfirewall.com/ufw-ubuntu-firewall/ubuntu-check-firewall-status-ufw/**](https://www.configserverfirewall.com/ufw-ubuntu-firewall/ubuntu-check-firewall-status-ufw/)

**GitHub Link:**

[**https://github.com/OscarYnoa/Linux-Admin**](https://github.com/OscarYnoa/Linux-Admin)