“Київський коледж зв’язку”

Циклова комісія Комп’ютерної інженерії

**ЗВІТ ПО ВИКОНАННЮ**

**ЛАБОРАТОРНОЇ РОБОТИ №7**

з дисципліни: «Операційні системи»

**Тема:** **“Мережева конфігурація, захист системи та користувачів у Linux”**

Виконала студенток

групи РПЗ-83б

Гречаник А.Р., Німенко К.С., Гончаренко Ю.І. \_\_\_\_\_\_\_\_

Перевірив викладач

Повхліб В.С. \_\_\_\_\_\_\_

Київ 2021

Мета роботи:

1. Знайомство з базовими структурами для збереження системних даних - процеси, память, лог-файли та повідомлення про стан ядра.

2. діями при зі ствндартом Filesystem Hierarchy Standard.

3. Знайомство з базовими діями при налаштуванні мережі.

4. Знайомство з базовими діями при налаштуванні мережі

Матеріальне забезпечення занять

1. ЕОМ типу IBM PC.

2. ОС сімейства Windows (Windows 7).

3. Віртуальна машина – Virtual Box (Oracle).

4. Операційна система GNU/Linux – CentOS.

5. Сайт мережевої академії Cisco netacad.com та його онлайн курси по Linux

**Завдання для попередньої підготовки.**

1. Прочитайте короткі теоретичні відомості до лабораторної роботи та зробіть невеликий словник базових англійських термінів з питань призначення команд та їх параметрів.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

2. На базі розглянутого матеріалу дайте відповіді на наступні питання:

2.1. Розкрийте поняття “псевдо файлової системи”, для чого воно потрібно системі?

A *pseudo-file system* is a hierarchical interface to nephile objects that appear to be ordinary files in a disk or long-term file system tree. Up to now, it is possible to access non-fail objects with the same system calls and utilities as normal files and directories. The common term for both ordinary files and non-physical objects is the node.

The advantage of synthetic filesystems is that the well-known filesystem semantics can be reused for a universal and easily implementable approach of mizprocessional communication. Clients can use such a file system to perform simple filesystem operations on their nodes, and do not need to implement complex encoding and message transfer methods and other protocol engineering aspects. For most operations it is possible to use common utilities for files, so even scripts are quite easy.

2.2. Чому користувачі не так часто звертаються на пряму до каталогу /proc, яким чином з нього можна отримати інформацію?

/proc is not a real file system. It’s a virtual system. Its main task is to obtain the state of the system and partially perform the management actions. Unfortunately, not many people know what’s inside and how to use it.

2.3. Яке призначення файлів /proc/cmdline, /proc/meminfo та /proc/modules

/proc/cmdline - kernel start string information.

/proc/meminfo - system memory information.

/proc/modules - kernel modules currently loaded.

2.4. Яке призначення команди free?

Executing the free command without any options provides a snapshot of the memory being used at that moment.

2.5. Для чого потрібні лог-файли, наведіть приклади їх застосування?

Log files are useful for many reasons; they help troubleshoot problems and determine whether or not unauthorized access has been attempted. Some processes can log their own data to these files, other processes rely on a separate process (a daemon) to handle these log data files.

Although most log files contain text as their contents, which can be viewed safely with many tools, other files such as the /var/log/btmp and /var/log/wtmp files contain binary. By using the file command, users can check the file content type before they view it to make sure that it is safe to view.

2.6. Яке призначення файлу /var/log/dmesg?

/var/log/dmesg - messages generated by the kernel during system boot up.

2.7. Для чого розроблено FHS?

A standard is a set of rules or guidelines that it is recommended to follow. However, these guidelines certainly can be broken, either by entire distributions or by administrators on individual machines.

2.8. Які основні команди є у Linux для перегляду та конфігурації мережі.

The ifconfig command stands for interface configuration and is used to display network configuration information.

The ip command differs from ifconfig in several important manners, chiefly that through its increased functionality and set of options, it can almost be a one-stop shop for configuration and control of a system’s networking.

The ping command can be used to determine if another machine is reachable. If the ping command can send a network package to another machine and receive a response, then you should be able to connect to that machine.

The netstat command is a powerful tool that provides a large amount of network information. It can be used to display information about network connections as well as display the routing table similar to the route command.

The ss command is designed to show socket statistics and supports all the major packet and socket types.

The ssh command allows you to connect to another machine across the network, log in and then perform tasks on the remote machine.

2.9. У яких файлах зберігається інформація про користувачів та їх групи. Яким чином їх можна переглянути.

The /etc/passwd file defines some of the account information for user accounts. Each line contains information pertaining to a single user. The data is separated into fields by colon characters. The /etc/passwd file defines the primary group membership for a user. Supplemental group membership (or secondary group membership) and the groups themselves are defined in the /etc/group file.

3. Вивчіть матеріали онлайн-курсів академії Cisco:

- NDG Linux Essentials (Chapter 13-15 all Topics)

4. Пройдіть тестування у курсі NDG Linux Essentials за такими темами:

- Chapter 13 Exam

- Chapter 14 Exam

- Chapter 15 Exam

5. Підготувати в електронному вигляді початковий варіант звіту:

- Титульний аркуш, тема та мета роботи

- Словник термінів

- Відповіді на п.2.1-2.3 з завдань для попередньої підготовки

**Хід роботи.**

1. Початкова робота в CLI-режимі в Linux ОС сімейства Linux:
2. Запустіть віртуальну машину VirtualBox, оберіть CentOS та запустіть її. Виконайте вхід в систему під користувачем: CentOS, пароль для входу: reverse ***(якщо виконуєте ЛР у 401 ауд.)*** та зпустіть термінал.
3. Запустіть віртуальну машину Ubuntu\_PC ***(якщо виконуєте завдання ЛР через академію netacad)***
4. Запустіть свою операційну систему сімейства Linux ***(якщо працюєте на власному ПК та її встановили)*** та запустіть термінал.
5. Опрацюйте всі приклади команд, що представлені у лабораторних роботах курсу ***NDG Linux Essentials:***

* ***Lab 13: Where Data is Stored***
* ***Lab 14: Network Configuration***
* ***Lab 15: System and User Security***

1. Створіть таблицю команд вивчених у п.2 ходу роботи у наступному вигляді:

|  |  |
| --- | --- |
| Назва команди | Її призначення та функціональність |
| ls /proc | The /proc directory contains a subdirectory for each running process on the system. Programs such as ps and top read the information about running processes from these directories. The /proc directory also contains information about the operating system and its hardware in files like /proc/cpuinfo, /proc/meminfo and /proc/devices. |
| cat /proc/1/cmdline; echo | Use cat then ps to view information about the /sbin/init process (Process IDentifier (PID) of 1) The other files in the /proc directory contain information about the operating system. |
| ping localhost > /dev/null | The output of the ping is being redirected to the /dev/null file (which is commonly known as the bit bucket). The system will continue to ping until the process is terminated or suspended by the user. |
| ping localhost > /dev/null & | To start the same process in the background. By adding the ampersand & to the end of the command, the process is started in the background, allowing the user to maintain control of the terminal. |
| jobs | To see which commands are running in the current terminal |
| fg %1 | Once you have verified that two ping commands are running, bring the first command to the foreground |
| **Ctrl**-**Z** | To suspend (pause) the process and regain control of the terminal |
| bg %1 | To have this process continue executing in the background |
| kill %3 | Using the job number, stop the last ping command with the kill command |
| killall ping | you can stop all of the ping commands with the killall command. After executing the killall command, wait a few moments |
| top | The output of the top command changes every 2 seconds. The top command is an interactive program, which means that you can issue commands within the program. You will use the top command to kill the ping processes. First type the letter **k**. At the PID to kill: prompt, type the PID of the first running ping process, then press **Enter**. At the Kill PID with signal [15]: prompt, enter the signal to send to this process. In this case, just press the **Enter** key to use the default signal. Notice that the first ping command is removed and only one ping command remains in the listing (you may need to wait a few seconds as the top command refreshes) Type **q** to exit the top command. |
| sleep 888888 & | The sleep command is typically used to pause a program (shell script) for a specific period of time. In this case it is used just to provide a command that will take a long time to run. |
| pkill -15 sleep | use the pkill command to terminate the remaining sleep command, using the name of the program rather than the PID |
| ps -o pid,tty,time,%cpu,cmd | Use the ps command with the -o option to specify which columns to output. |
| ps -o pid,tty,time,%mem,cmd --sort %mem | Use the --sort option to specify which column(s) to sort by. By default, a column specified for sorting will be in ascending order, this can be forced with placing a plus + symbol in front of the column name. To specify a descending sort, use the minus - symbol in front of the column name. |
| free | While the ps command can show the percentage of memory that a process is using, the free command will show overall system memory usage |
| ls /var/log | System logs are stored in the /var/log directory. |
| ssh localhost  {At the first prompt, type yes}  {At the second prompt, type abc}  {At the third prompt, type abc}  {At the fourth prompt, type abc}  tail -5 /var/log/auth.log | Each log file represents a service or feature. For example, the auth.log file displays information regarding authorization or authentication, such as user login attempts. New data is stored at the bottom of the file. The ssh command was used to generated data in the /var/log/auth.log file. |
| ifconfig | In order to determine your Internet Protocol (IP) address, execute the ifconfig command. The output shows two main blocks of information. The first block, indented by eth0, reflects information about your first Ethernet network card. The second block, indented by lo, reflects information about the loopback or internal network interface.  The second line in each block contains the pertinent information for version 4 of the Internet Protocol (called IPv4) while the third line has the information for version 6 of the Internet Protocol (IPv6). IPv4 is an older method of identifying machines with a series of numbers. It is still widely used today despite the fact that the improved IPv6 method has been available for many years.  The IPv4 addresses are displayed as four decimal numbers ranging from 0 to 255 separated by periods.  The IPv6 addresses are 128-bit numbers which are displayed as hexadecimal digits ranging from 0 to f. The hexadecimal digits are generally organized into groups of four digits separated by colons. If a number of consecutive hexadecimal digits have the value of zero, then they are replaced with two colons. |
| route | Having an IP address will allow your system to communicate with other systems on the same network. With routing devices, you are able to communicate with systems on other networks. To view the table of routing information, use the route command |
| ping -c4 localhost | Unlike the ping command that is available in the Microsoft Windows operating system, the Linux ping command does not stop making requests by default. If you forget to specify the -c option, then you will have to manually stop the command by holding the **Control** key and pressing **C** (**CTRL**+**C**). |
| cat /etc/resolv.conf | View the /etc/resolv.conf file to see if any nameserver entries exists |
| dig localhost.localdomain | Use the dig command to resolve the localhost.localdomain name to an IP address |
| dig cserver.example.com | You can use the dig command to resolve other fully-qualified domain names. Use the dig command to resolve the cserver.example.com hostname to an IP address |
| dig -x 192.168.1.2 | Use the dig command to resolve the IP address 192.168.1.2 to a hostname |
| netstat --help | The netstat command performs a large variety of tasks related to networking. To get an idea of some of its capabilities, execute the command with the --help option. One of the common uses of netstat is to determine which services are listening to or waiting for an incoming connection. For example, a service that is used to allow users to perform remote or network logins is called Secure SHell or SSH. SSH normally will listen to TCP port 22.  Well-known ports are the port numbers in the range of 0-1023, typically used by system processes to provide network services. A list of service names and associated port numbers can be found in the /etc/services file.  The -t option to the netstat command limits the listing to TCP ports; the -l option limits the output to ports with listening services; the -n shows the network addresses numerically. |
| start\_webserver | A more modern approach is to use the ss command to view which connections are currently established between the local machine and remote machines, statistics about those connections, etc.  Similar to the netstat command, you can get a great deal of useful information from the ss command by itself, as shown in the example below.  The script started a webserver and created the traffic which is displayed by the ss command. This is one way the ss command can be used for troubleshooting. |
| su - | To access the root user account, the su or sudo commands are normally used.  The su command is usually used to switch users and start a new shell as another user, with the default being the root user. The su command is often used when a series of commands need to be executed as the root user.  The sudo command is typically used to execute a single command as the root user by prefixing that command with sudo. The sudo command must be configured by the root user before an ordinary user can use it. By default, the sudo command stays in effect for 15 minutes on Ubuntu systems where the root account is not enabled by default. Root access has been enabled on the virtual machine used in this lab allowing the su command to be used.  When executed without arguments, the su command opens a new shell as the root user. There is some confusion as to what the initials “su” stand for (substitute user, switch user, and superuser are all often referenced) , but the main thing to note is that it allows an administrator to change their login to any user on the system.  When entering this command without a username, the system will assume the root user. Most systems will display the current user at the command prompt, but it can be helpful to confirm what user is logged in with the id command as shown below. This step will ensure changes required for specific users (such as service accounts) are executed properly.  Switch users to the root user and provide the root password of netlab123 when prompted |
| id | Confirm the new user identity using the id command |
| exit  id | After using the shell started by the su command to perform the necessary administrative tasks, return to your original shell (and original user account) by using the exit command. Confirm the user identity change using the id command. |
| grep sysadmin /etc/passwd | Use the grep command to view the record for your sysadmin account. By using the grep command, the output only includes the account information for that one username. |
| head -3 /etc/shadow | Try to view the first few lines of /etc/shadow file, a file that contains users' encrypted passwords and information about aging them |
| getent passwd sysadmin | Another way to retrieve the account information for a user is by running the following command: getent passwd username. The getent command has the advantage over the grep command as it is also able to access user accounts that are not defined locally. In other words, the getent command is able to get user information for users who may be defined on network directory servers such as LDAP, NIS, Windows Domain, or Active Directory Domain servers. |
| man 5 passwd | You can view the documentation of the fields in the /etc/passwd file with the following command |
| who | Use the who command to get the current list of users on the system |
| w | Use the w command to get a more detailed view of the users who are currently on your system |
| last | Use the last command to view the /var/log/wtmp file which keeps a log of all users who have logged in and out the system. |

**Контрольні запитання**

1. В чому відмінність між командами ps --forest та pstree?

If information can be presented in a graphical form, it becomes easy to comprehend and remember. If you agree with this, you'll be glad to know that's possible with the ps command as well, as the tool is capable of showing processes in a hierarchical format.

The feature in question can be accessed using the *--forest* command-line option. Here's an example for it:

ps -ae –forest

**pstree** is a Linux command that shows running processes as a tree. It is used as a more obvious alternative to the ps command. The root of a tree is either an initi or a process with a given hearth.

1. У яких каталогах зберігаються налаштування системи?

Generally system/global **config** is **stored** somewhere under /etc. **User**-specific **config** is **stored** in the **user's** home directory, often as a hidden **file**, sometimes as a hidden directory containing non-hidden files (and possibly more subdirectories).

1. У яких каталогах можна знайти встановлені в системі програми, доступні для користувача?

The /etc/passwd file defines some of the account information for user accounts. Each line contains information

pertaining to a single user. The data is separated into fields by colon characters.

1. У яких каталогах можна знайти встановлені системні програми і програми призначені для виконання суперкористувачем?

Users log into the system using regular user accounts. Typically, these accounts have UID values of greater than 500 (on some systems 1,000). The root user has special access to the system. This access is provided to the account with a UID of 0.

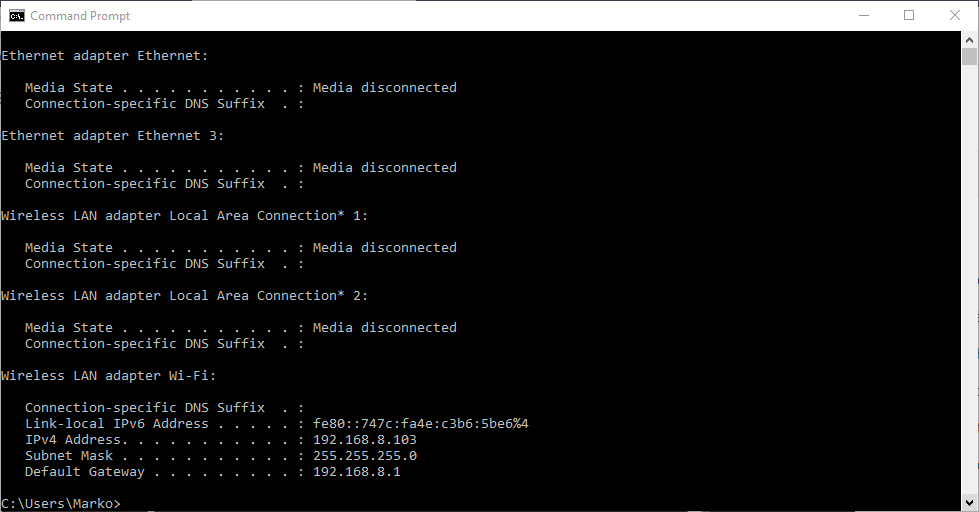
There are additional accounts that are not designed for users to log into. These accounts, typically from UID 1 to UID 499, are called system accounts, and they are designed to provide accounts for services that are running on the

system.

System accounts have some fields in the /etc/passwd and /etc/shadow files that are different than other accounts. For example, system accounts rarely have home directories as they typically are not used to create or store files.

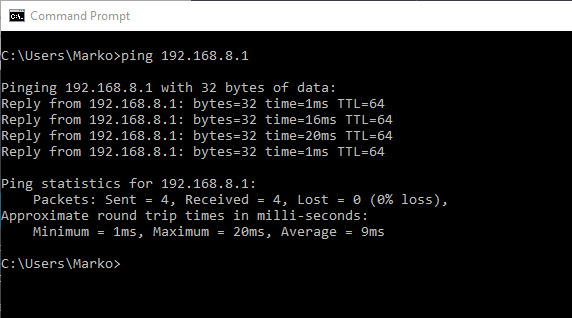
1. Поясніть призначення команд ping, ifconfig, traceroute.

he “ipconfig” displays the current information about your network such as your your IP and MAC address, and the IP address of your [router](https://www.utilizewindows.com/difference-between-hub-switch-router-explained/). It can also display information about your DHCP and DNS servers. Let’s see the basic output of “ipconfig”:

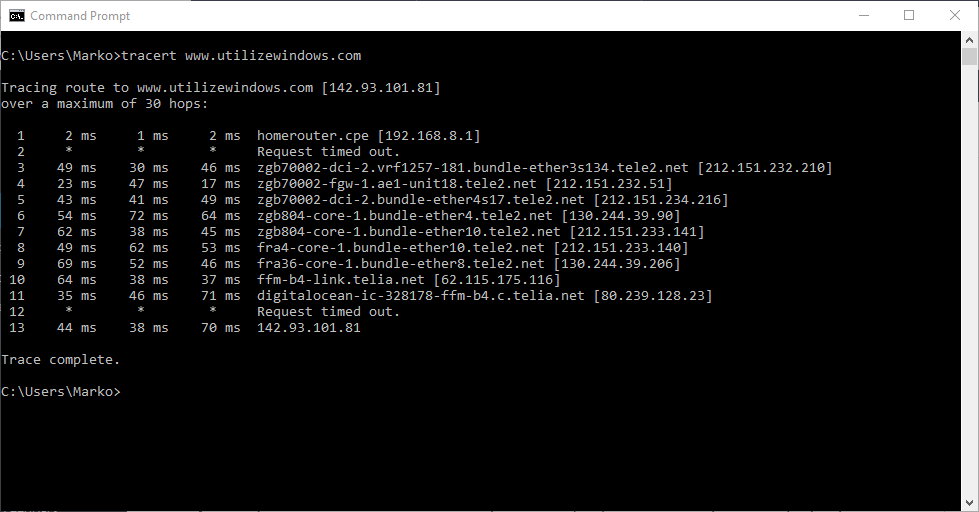


The “ping” command ping command allows you to send a signal to another device, and if that device is active, it will send a response back to the sender. The “ping” command is a subset of the ICMP (Internet Control Message Protocol), and it uses what is called an “echo request”. So, when you ping a device you send out an echo request, and if the device you pinged is active or online, you get an echo response.

For example, if your local computer has Internet connectivity issues, you can try to ping your router. If you get no response then you know that the router is what is giving you problems. Let’s ping our router IP, which is 192.168.8.1 in our example, and let’s analyze the the printout.



traceroute command lets you see all steps a packet takes to the destination. For example, if we send a packet to www.google.com, it actually goes through a couple of routers to reach the destination. The packet will first go to your router, and then it will go to all kinds of different routers before it reaches Google servers. We can also use the term “hops” instead of routers. Let’s run the command and see what kind of results we get.



1. Як називаються мережеві інтерфейси в Linux?

lo

Feedback loop interface.

eth

Network interface to Ethernet card or WaveLan (Radio Ethernet) cards.

tr

Network interface to Token Ring card.

ppp

Network interface to the PPP (Point-to-Point Protocol) channel.

fig

Network interface to the SLIP (Serial Line IP) channel.

plip

Network interface to the PLIP channel (Parallel Line IP). Used to organize network communication using a parallel port.

ax

Network interface to AX.25 amateur radio devices.

fddi

Network interface to the FDDI Line IP card).

1. Як за допомогою команди ifconfig вивести параметри тільки одного мережевого інтерфейсу (наприклад, eth1), а не всіх?

 sudo ifconfig eth1

1. Чому в конфігураційних файлах паролі не зберігається в явному вигляді?

Initially, the / etc / passwd file was used to store passwords. But this file is readable by all users. Therefore, for security reasons, user passwords have been moved to the / etc / shadow file. This file is read-only by the root user.

It is important to note that the passwords in this file are not stored in an open form, but in a hashed one.

1. Чому не рекомендується виконувати повсякденні операції, використовуючи обліковий запис root?

Strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks. To view the tasks that require you to sign in as the root user, see AWS Tasks That Require Root User. For a tutorial on how to set up an administrator for daily use, see Creating your first IAM admin user and user group.

1. У чому відмінність механізмів отримання особливих привілеїв su і sudo?

Both **su** and **sudo** elevate privileges assigned to the current user.

The main difference between the two is that **su** requires the password of the target account, while **sudo** requires the password of the current user. Therefore, it is much safer to use **sudo** since it doesn’t include exchanging sensitive information.

Additionally, it is advisable to stick to **sudo** when performing tasks that require root privileges. By doing so, the current user is only granted privileged for the specified command. On the other hand, **su** switches to the root user completely, exposing the entire system to potential accidental modification.

**Висновок:** Ми ознайомились з базовими структурами для збереження системних даних - процеси, память, лог-файли та повідомлення про стан ядра.