**Topic: "Network configuration, system and user protection in Linux"**

Performed by students RPZ-93B group

**Team:** Бушовська О.В, Білобровенко О.С., Скворцов Д.Є.

**The purpose of the work:**

1. Familiarize yourself with the basic tools for storing system data - processes, memory, log files and kernel status messages.
2. Introduction to the Filesystem Hierarchy Standard.
3. Familiarity with the basic steps when setting up a network.

**Material support of classes**

1. Computer type IBM PC.

2. Windows family of operating systems (Windows 7).

3. Virtual machine - Virtual Box (Oracle).

4. GNU / Linux operating system - CentOS.

5. Cisco Network Academy website netacad.com and its online Linux courses

***Готував матеріал студентка Скворцов Дмитро***

**Tasks for preliminary preparation.**

1. **Read brief theoretical information about laboratory work and make a small glossary of basic English terms on the purpose of team assignments and their parameters.**

|  |  |
| --- | --- |
| Name | Description |
| Thread | is a set of sequentially executed processor instructions that use the common address space of the process. |
| Computer memory | a part of a computer, physical device, or storage medium used in computing systems over a period of time. |
| Logs (log files) | these are files that contain system information about the operation of the server or computer and certain actions of the user or program. Sometimes a Ukrainian-language analogue of the term magazine is also used. |

1. **On the basis of the considered material give answers to the following questions:**
   1. **Explain the concept of "pseudo file system", why does the system need it?**

For example – procfs - is a special file system used in UNIX-like operating systems. Allows you to access information from the kernel about system processes. Needed to run commands like ps, w, top. It is usually mounted on /proc. procfs creates a two-level representation of process spaces. At the top level, processes are directories named according to their pid (Process ID). Also at the top level is a link to the directory corresponding to the process making the request; it may have a different name on different operating systems.

* 1. **Why do users not so often go directly to the / proc directory, how can I get information from it?**

Perhaps users are reluctant to choose, because procfs almost does not perform its original function - process management. There is no interface for sending commands, the file system only provides detailed information about the processes (and in some places allows you to change some options.

* 1. **What is the purpose of the / proc / cmdline, / proc / meminfo and / proc / modules files?**
* /proc/cmdline - it is a read-only file that contains complete process information from the command line. If the process has been swapped in addition to memory, or the process is a zombie process, then this file has no content. The file ends with a null character instead of a newline character.
* /proc/meminfo -is used by to report the amount of free and used memory (both physical and swap) on the system as well as the shared memory and buffers used by the kernel.
* /proc/modules files - this file displays a list of all modules loaded into the kernel. Its contents vary based on the configuration and use of your system.
  1. **What is the purpose of the free command?**

The free command provides information about the total amount of the physical and swap memory, as well as the free and used memory.

**2.5 Why do you need log files, give examples of their use?**

Their purpose is to record the operations performed on the machine for permanent analysis by the administrator. Regular viewing of logs allows you to identify errors in the system as a whole, select a service or site (specially identified errors that do not occur when viewed in), diagnose malicious activity, and collect site visit statistics.

**2.6** **What is the purpose of the / var / log / dmesg file?**

System boot log (helps to debug the system in case it does not boot, saves the main system events (for example, hardware failures));

* 1. **What is FHS designed for?**

Organize the structure of directories and files in the GNU/Linux operating system. And the second reason that the FSH standard was created is to develop a standard that is suitable for all Unix-like operating systems. What are the basic commands in Linux for viewing and configuring the network.

* 1. **In which files is stored information about users and their groups. How to view them.**

All user information is usually stored in the /etc/passwd and /etc/group files.

***Готувала матеріал студентка Білобровенко Олександра***

* 1. Why do you need log files, give examples of their use?

System administrators, and even regular Linux users, often need to look at log files for troubleshooting. In fact, this is the first thing that any system administrator should do when any error occurs in the system.

The Linux operating system itself and running applications generate various types of messages that are logged in various log files. Linux uses special software, files and directories to store log files. Knowing in which files the logs of which programs are located will help you save time and solve the problem faster. In this article, we will look at the main parts of the Linux logging system, log files, and utilities that can be used to view Linux logs.

Most Linux log files are located in the /var/log/ folder, you can list the log files for your system with the ls command: ls -l /var/log/

To view logs on Linux, it is convenient to use several Linux command line utilities. It can be any text editor, or a special utility. Most likely, you will need superuser rights in order to view the logs in Linux. Here are the commands that are most often used for this purpose: less; more; cat; head; grep; tail; zcat; zgrep; zmore; vi; nano.

* 1. **What is the purpose of the / var / log / dmesg file?**

The / var / log / dmesg file contains kernel messages that were created during system startup. You can also use the dmesg command to view the kernel ring buffer, which contains a large number of messages generated by the kernel.

* 1. **What is FHS designed for?**

Among the standards supported by the Linux Foundation is the File System Hierarchy (FHS) standard, which is located at http://www.pathname.com/fhs/.

The FHS standard classifies each system directory in several ways:

The directory can be classified as shared or not based on whether the directory can be shared online and shared by multiple machines.

The directory is placed in a category that contains static files (file contents do not change), or variable files (file contents may change).

To make this classification, it is often necessary to refer to subdirectories below the top level of directories. For example, the / var directory itself cannot be classified as shared or unavailable, but one of its subdirectories, the / var / mail directory, is shared. Conversely, the / var / lock directory should not be available.

* 1. **What are the sic commands in Linux for viewing and configuring the network.**

curl & wget - download resources from internet

ping - check host availability

tracepath and traceroute - tracing a route to a host

mtr - a combination of traceroute and ping

host - perform DNS queries

whois - search for data in the WHOIS database

ifplugstatus - determine if a network cable is connected

ifconfig - Get network configuration/configure network interface

ifdown & ifup - activate/deactivate network interface

dhclient - DHCP client management

netstat - display network information

* 1. **In which files is stored information about users and their groups. How to view them.**

The id command is used to print information about the user and group for the specified user. id [parameters] username

The who command displays a list of users who are currently logged in, where they logged in, and when they logged in. With the help of parameters, this command can also display information such as the current level of execution (a functional state of the computer) and the boot time of the system.The last command reads the entire login history from the / var / log / wtmp file and displays all login and reboot entries by default. An interesting detail about reboot records is that the version of the Linux kernel that was downloaded is displayed instead of the login location. The / var / log / wtmp file keeps a log of all logged in and logged out users.

1. **Learn Cisco Academy Online Course Materials:**

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

1. **Take the NDG Linux Essentials course on the following topics:**

* Chapter 13 Exam
* Chapter 14 Exam
* Chapter 15 Exam

1. **Prepare the initial version of the report in electronic form:**

* Title page, topic and purpose of the work
* Glossary of terms
* Answers to paragraphs 2.1-2.3 of the tasks for preliminary training

***Готувала матеріал студентка Білобровенко Олександра***

**Progress.**

* 1. Initial work in CLI mode in Linux family:
  2. Start the VirtualBox virtual machine, select CentOS, and start it. Log in under the user: CentOS, login password: reverse ***(if you are performing LR in room 401)*** and lower the terminal.
  3. Start the Ubuntu\_PC virtual machine ***(if you are performing LR tasks through the netacad academy)***
  4. Start your Linux operating system ***(if you are running your own PC and have it installed)*** and start the terminal.
  5. Study all the examples of commands presented in the laboratory work of the ***NDG Linux Essentials course:***
* ***Lab 13: Where Data is Stored***
* ***Lab 14: Network Configuration***
* ***Lab 15: System and User Security***
  1. Create a table of commands studied in paragraph 2 of the work in the following form:

|  |  |
| --- | --- |
| Command name | Its purpose and functionality |
| ps | to view a list of processes in Linux |
| top | allows you to display information about the system, as well as a list of processes dynamically updating information about the resources they consume. |
| echo | outputs a line of text to the terminal |
| cat | allows you to create, merge, and also output the contents of files on the command line or in another file |
| sysctl | utility designed to manage kernel parameters on the fly. Allows you to read and change kernel parameters. |
| ping | You can quickly find out if there is Internet on your computer using the ping utility |
| jobs | display a table of currently running jobs |
| kill | When you issue a "kill" command, you are actually sending a signal to the system and instructing it to terminate the incorrect application robot. |
| killall | is designed to "kill" all processes that have the same name. |
| pkill | is a command line utility that sends signals to the processes of a running program based on specified criteria. |
| sleep | unix utility that performs a delay for a specified time |
| free | provides information about the total amount of physical and swap memory |
| Syslogd | provides a kind of logging that many modern programs use |
| klogd | is a system daemon that intercepts and logs messages from the Linux kernel. |
| DMESG | To receive messages from a buffer core message |
| ifconfig | With it, you can enable or disable network interfaces, configure their settings, switch modes |
| route | adding and removing network routes for the system kernel, as well as viewing the contents of the routing table |
| dig | It allows you to get more information about a particular domain, in order, for example, to find out the IP addresses used by it. |
| netstat | displays data about network connections, routing table, statistics of network interfaces, masked connections. |
| su | This command replaces the shell user with the one specified. In fact, a new instance of the shell is launched with the specified parameters. |
| sudo | allows you to run programs as other users, as well as the superuser. |
| id | is a command line utility that prints real and valid user and group IDs |
| exit | A shell command to terminate the process with a success code or an error code, if one was passed as an argument. |
| grep | it enables users to sort and filter text based on complex rules. |
| head | outputs leading lines (default 10) from one or more documents |
| getent | is a Unix command that helps the user retrieve entries in a number of important text files called databases. |

**Test questions**

1. What is the difference between the *ps --forest* and *pstree commands* ?
2. In which directories are the system settings stored?

***Готувала матеріал студентка Бушовська Ольга***

1. In which directories can you find the programs installed in the system available to the user?

/ opt A directory in which additional system or program components are installed

1. In which directories can you find installed system programs and programs designed to run by superuser?

sudo - allows users to execute commands on behalf of the root superuser or other users;

The / bin and / sbin directories. These directories contain: system utilities and binary (ie executable) files, shells, files of many external commands, editors, etc. The main difference between the programs stored in the mentioned directories is that the programs from the / sbin directory can be executed only by the superuser.

Catalog / lib. This directory contains general system libraries. One of the subdirectories of the / lib directory contains the Linux kernel.

Catalog / dev. Here are the files that represent system devices (terminals, printers, hard drives, etc.).

1. Explain the purpose of the ping, ifconfig, traceroute commands.

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

information. Not all network settings are covered in this course, but it is important to note from the output below that

the IP address of the primary network device eth0 is 192.168.1.2 and that the device is currently active UP:

The ifconfig command is becoming obsolete in some Linux distributions (deprecated) and is being replaced

with a form of the ip command, specifically ip addr show.

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.

By default, the ping command continues sending packages endlessly. To limit how many pings to send, use

the -c option followed by a number indicating how many iterations you desire. The following examples show ping

being limited to 4 iterations.

Traceroute – The traceroute command is used to determine the path between two connections. Often a connection to another device will have to go through multiple routers. The traceroute command will return the names or IP addresses of all the routers between two devices.

1. What are the network interfaces in Linux called?

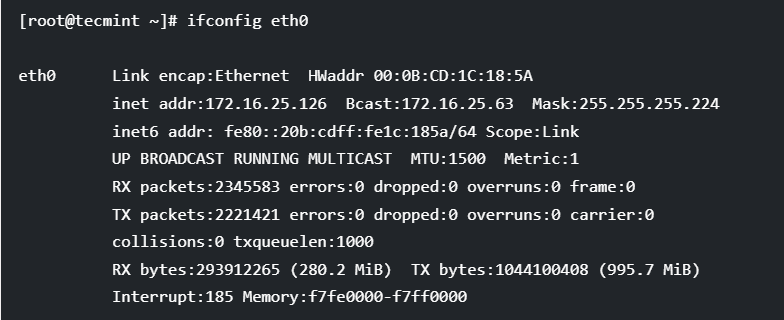
[ip command](https://www.cyberciti.biz/faq/linux-ip-command-examples-usage-syntax/) – It is used to show or manipulate routing, devices, policy routing and tunnels.

netstat command – It is used to display network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

ifconfig command – It is used to display or configure a network interface.

nmcli command – A command to show or configure a network interface on Linux.

1. How to use the ifconfig command to display the parameters of only one network interface (for example, eth1) and not all?



1. Why aren't passwords explicitly stored in configuration files?

They are encrypted to ensure the security of the user's system.

1. Why is it not recommended to perform daily operations using a root account?

Because it is possible to pick up a virus or modify important system files that will disrupt the system.

1. What is the difference between the mechanisms for obtaining special privileges su and sudo?

The su command allows you to run a shell from another user. Although the command is most often used to switch to a user, it can also switch to other root.su users

su [parameters] [username]

It is recommended that you use the login shell option when switching users, as the login shell completely configures the new shell with the new user settings, ensuring that any commands are executed correctly. If this option is omitted, the new shell changes the UID, but is not fully logged in

The sudo command allows users to execute commands as another user. Like the subcommand, the root user is considered the default.

sudo command [parameters].

In distributions that do not allow the root user to log in directly or with the sucom command, the installation process automatically configures one user account to be able to use the sudo command to execute commands as if the root user were executing them.

***Готувала матеріал студентка Білобровенко Олександра***

**Conclusion:** I got acquainted with the basic structures for saving system data - processes, memory, log files and kernel status messages, I got acquainted with the Filesystem Hierarchy Standard and the basic actions for setting up a network.