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

**Мета роботи:**

1. Знайомство з базовими структурами для збереження системних даних - процеси, память, лог-файли та повідомлення про стан ядра.
2. Знайомство зі стандартом Filesystem Hierarchy Standard.
3. 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.** (Ilya)

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

|  |  |
| --- | --- |
| troubleshoot | усунення несправностей |
| daemon process | процес демона |
| regularly-scheduled basis | на регулярній основі |
| network interfaces | мережеві інтерфейси |
| **Packet** | Пакет |
| The Transmission Control | Контроль трансмісії |
| technical limit | технічний ліміт |
| Porting | Перенесення |
| chiefly | головним чином |
| socket statistics | статистика сокетів |

1. На базі розглянутого матеріалу дайте відповіді на наступні питання:
   1. Розкрийте поняття “псевдо файлової системи”, для чого воно потрібно системі?

A virtual file system (VFS) or virtual filesystem switch is an abstract layer on top of a more concrete file system. The purpose of a VFS is to allow client applications to access different types of concrete file systems in a uniform way. A VFS can, for example, be used to access local and network storage devices transparently without the client application noticing the difference.

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

The /proc directory is read, and its information utilized by many different commands on the system, including but not limited to top, free, mount, umount and many others. It is rarely necessary for a user to mine the /proc directory directly—it’s easier to use the commands that utilize its information.

* 1. Яке призначення файлів /proc/cmdline, /proc/meminfo та /proc/modules?

|  |  |
| --- | --- |
| /proc/cmdline | Information that was passed to the kernel when it was first started, such as command line parameters and special instructions |
| /proc/meminfo | Information about the use of memory by the kernel |
| /proc/modules | A list of modules currently loaded into the kernel to add extra functionality |

* 1. Яке призначення команди free?

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

* 1. 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.

* 1. Яке призначення файлу /var/log/dmesg?

The /var/log/dmesg file contains the kernel messages that were produced during system startup.

* 1. Для чого розроблено FHS?

A Filesystem Hierarchy 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.

The FHS standard categorizes each system directory in a couple of ways:

* A directory can be categorized as either *shareable* or not, referring to whether the directory can be shared on a network and used by multiple machines.
* The directory is put into a category of having either *static* files (file contents won't change) or *variable* files (file contents can change).
  1. Які основні команди є у Linux для перегляду та конфігурації мережі.

**host -** Command that works with DNS to associate a hostname with an IP address.

**ifconfig -** Command used to display network configuration information, depreciated and being replaced by the ip addr show command.

**ip addr show -** Command used to display and manipulate network configuration information, replacing the depreciated ifconfig command.

**ip route show -** Command that displays IP routing table, replacing the depreciated route command.

**netstat -** Command used to display information about network connections as well as display the routing table.

**ping -** Command used to determine if another machine is reachable by sending a network package to another machine and checking for a response.

**route -** Command that displays IP routing table, depreciated and being replaced by the ip route show command

**ss -** Command designed to display socket statistics and supports all major socket types, similar to but more verbose than the netstat command.

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

**/etc/group** File that contains group configuration information.  
To view information about a specific group, either the grep or getent commands can be used.

**/etc/passwd** File that defines some of the account information for user accounts.  
An efficient way to check if a specific user has been defined on a system is to search the /etc/passwd file using the grep command.

**/etc/shadow** File that contains account information related to the user's password.

1. Вивчіть матеріали онлайн-курсів академії Cisco:

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

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

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

1. 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.(Andrii)**

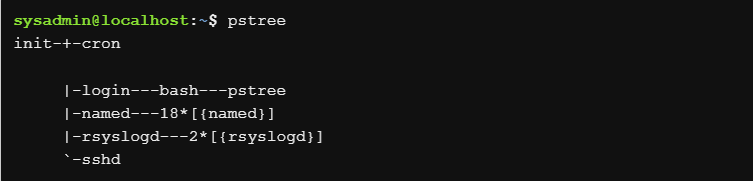
* 1. Опрацюйте всі приклади команд, що представлені у лабораторних роботах курсу ***NDG Linux Essentials:***
* ***Lab 13: Where Data is Stored***
* ***Lab 14: Network Configuration***
* ***Lab 15: System and User Security***
  1. Створіть таблицю команд вивчених у п.2 ходу роботи у наступному вигляді:

|  |  |
| --- | --- |
| Назва команди | Її призначення та функціональність |
| cat /proc/cmdline | View the /proc/cmdline file to see what arguments were passed to the kernel at boot time. |
| ping local > /dev/null & | To start process in the background. |
| jobs | To see which commands are running in the current terminal. |
| bg % 1 | To have current process continue executing in the background. |
| kill | To stop the process. |
| killall | To stop all the processes. |
| top | To sort the processes in descending order of percentage of CPU usage |
| sleep | Is used to pause a program (shell script) for a specific period of time. |
| ps -e | To view all processes are displayed. |
| free | To show overall system memory usage. |
| ls /var/log | To view list of the system logs. |
| ifconfig | To determine your Internet Protocol (IP) address. |
| route | To view the table of routing information, use the route command |
| grep 127.0.0.1 /etc/host | To verify that the IP address 127.0.0.1 has an entry in the /etc/hosts file |
| dig localhost.localdomain | To resolse the localhost.localdomain name to an IP address |
| netstat -tln | 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 |
| ss | To view which connections are currently established between the local machine and remote machines, statistics about those connections, etc. |
| su | Is usually used to switch users and start a new shell as another user, with the default being the root user. |
| sudo | Is typically used to execute a single command as the root user. |
| exit | To return to your original shell (and original user account). |
| grep sysadmin /etc/passwd | To view the record for current sysadmin account. |
| sudo head -4 /etc/shadow | To view the first few lines of the /etc/shadow file. |
| getent passwd sysadmin | Another way to retrieve the account information for a user. |
| id | To view account information for currect account. |
| who | To get the current list of users on the system. |
| w | To get a more detailed view of the users who are currently on system. |
| last | To view the /var/log/wtmp file which keeps a log of all users who have logged in and out the system. |

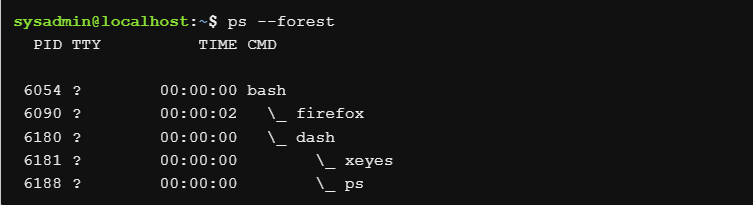
**Контрольні запитання(Andrii, Ilya)**

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

Processes can be "mapped" to the family tree of parent and child relationships. If you want to view this tree, the *pstree* command will display it:



If you run *ps* with the *--forest* option, it will, like the pstree command, show lines that indicate the parent and child relationship:



1. У яких каталогах зберігаються налаштування системи?

**/etc:** Program settings and the settings of whole system.

The most important directory is HKEY\_LOCAL\_MACHINE. These keys correspond to the physical data of the register. The HKLM key contains information about the entire system.

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

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

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

**/bin**, **/sbin:** 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.

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

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

1. Поясніть призначення команд ping, ifconfig, traceroute.

**ping** - is a very simple tool for network diagnostics. It allows you to check the available remote host or not. To do this, the utility checks whether the host can respond to network requests using ICMP.

**ifconfig**(interface settings) - is a network management tool. It is used to configure and view the status of network interfaces in Linux operating systems. With **ifconfig**, you can assign IP addresses, enable or disable interfaces, manage ARP cache, routes, and more.

**traceroute** - is a utility that allows you to trace the route of data to a remote destination on TCP / IP networks.

1. Як називаються мережеві інтерфейси в Linux?

**em[1234]** - for integrated,

**pci<slot>#<port>\_<vf>** - for mounted.

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

If no arguments are passed, **ifconfig** provides information about the status of the active interfaces. If one interface argument is specified, only the status of that interface is displayed; if one argument is specified, information about the status of all interfaces, even disabled ones, is displayed. Otherwise, the command configures the specified interface.

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

Storing passwords in application systems (in particular, in operating systems) in the open is not allowed, because in case of hacking passwords of all users become the property of the infringer.

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

It is not recommended to use the root account all the time, because if you have absolute access rights, you can accidentally cause irreparable damage to the system. Therefore, the system has a **su** command that allows the average user to obtain root privileges at any time.

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

The **su** command allows to run the shell from another user.

The **sudo** command allows users to execute commands like another user.

**Conclusion:**

During the laboratory work, we got acquainted with the basic structures for saving systems, learned about the Filesystem Hierarchy Standard and the basic actions for setting up the system.