“Київський фаховий 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»**

Виконали:

студенти групи РПЗ-93б

**Команда 1**: Усенко Б.О.,

Мельнічук М.О

Перевірив викладач

Сушанова В.С.

Київ 2022

**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.**

***Готувала матеріал студентка Усенко Б.О.***

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

|  |  |
| --- | --- |
| **Термін** | **Переклад** |
| **/proc directory** | містить інформацію про апаратне забезпечення системи та поточну конфігурацію ядра. |
| **/proc/cmdline** | Інформація, яка була передана ядру під час першого запуску, наприклад, командний рядок  параметри та спеціальні вказівки; |
| **/proc/meminfo** | Інформація про використання пам'яті ядром; |
| **the free command** | надає знімок пам'яті, яка використовується при цьому  момент. |
| **The ssh command** | дозволяє підключатися до іншого комп’ютера через мережу, входити в систему, а потім виконувати завдання  на віддаленій машині. |

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

"Псевдо" означає брехню, прикидатися. Таким чином, "псевдофайлова система" означає файлову систему, яка не має фактичних файлів - швидше вона має віртуальні записи, які сама файлова система створює на місці.

Наприклад, /proc у багатьох ОС – це procfs, що динамічно генерує каталоги для кожного процесу.

/dev може бути реальною файловою системою (просто підкаталогом /) або віртуальною псевдофайловою системою (наприклад, devfs).

/proc - це псевдо-файлова система, яка використовується як інтерфейс до структури даних в ядрі, щоб уникнути читання та запису /dev/kmem. Більшість розміщені в ній файли доступні тільки для читання, але деякі файли дозволяють змінювати змінні ядра.

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

Користува не так часто її використовують, бо Її не існує на диску або навіть в оперативній пам'яті, як це робиться /tmp. Всі піддиректорії, файли і інформація, що зберігається в них, генерується ядром на льоту, як тільки ви її запитуєте. Але працює все настільки прозоро, що ви не помітите жодної різниці між звичайною файловою системою та proc, якщо відкриєте її за допомогою файлового менеджера.

Всі файли доступні для редагування будь-яким редактором, і всі вони у простому текстовому форматі, але для того, щоб проаналізувати весь каталог вам знадобляться права суперкористувача.

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

**/proc/cmdline**

У цьому файлі ви знайдете параметри, зазначені в рядку запуску ядра завантажувачем Grub. Це може бути корисно при пошуку та усунення проблем із завантаженням ядра або якщо необхідно з'ясувати, який точно файл був використаний для завантаження.

**/proc/meminfo**

Ще один дуже відомий та широко використовуваний файл, який надає нам папка proc linux. Тут відображається вся доступна інформація про оперативну пам'ять та простір підкачки. Саме за допомогою цього файлу багато скриптів дізнаються інформацію про доступну пам'ять.

**/proc/modules**

Теж досить відомий файл. Тут міститься список усіх завантажених модулів ядра. Ту ж інформацію ми можемо побачити виконавши lsmod. Але цій утиліті також інформацію надає структура proc

* 1. *Яке призначення команди free?*

Команда free - інформація про системні ресурси

Команда free виводить інформацію про використання оперативної та віртуальної пам'яті, a df – про використання дискового простору

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

Логи (лог-файли) - це файли, що містять системну інформацію роботи сервера або комп'ютера, до яких заносяться певні дії користувача або програми.

Їхнє призначення — протоколювання операцій, що виконуються на машині, для подальшого аналізу адміністратором. Регулярний перегляд журналів дозволить визначити помилки в роботі системи в цілому, конкретного сервісу або сайту (особливо приховані помилки, які не виводяться під час перегляду в браузері), діагностувати зловмисну ​​активність, зібрати статистику відвідувань сайту

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

Лог завантаження системи - /var/log/dmesg

* 1. *Для чого розроблено FHS?*

FHS - скорочення від Filesystem Hierarchy Standard, що в перекладі з англійської означає "Стандарт ієрархії файлової системи".

Цей стандарт прийнято для уніфікації місцезнаходження файлів та директорій із загальним призначенням у файловій системі ОС UNIX. На даний момент більшість UNIX-подібних систем тією чи іншою мірою дотримуються цих правил. Наприклад, звичайна база даних користувача завжди зберігається у файлі /etc/passwd.

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

ls / sys / class / net / - список існуючих мережевих інтерфейсів

auto enp0s3 і iface enp0s3 inet dhcp - конфігурація інтерфейсу.

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

Переглянути права доступу на файли і каталоги у певному каталозі можна з використанням термінала. Для цього необхідно перейти у каталог (наприклад, у домашній каталог користувача) і виконати команду у терміналі ls (показати вміст каталогу), додавши опцію -l (у вигляді списку)

drwxr-xr-x - це **символьна форма запису прав доступу** у Linux

Права доступу до каталогу:

r - право на читання каталогу (можна прочитати вміст каталогу, тобто отримати список об’єктів, що знаходяться у ньому);

w - право на зміну вмісту каталогу (можна створювати і видаляти об’єкти в цьому каталозі, причому, якщо ви маєте право на запис, то видаляти ви зможете навіть ті файли, які вам не належать);

x - право на виконання, яке дозволяє увійти в каталог (це право завжди перевіряється в першу чергу, і навіть якщо ви маєте усі потрібні права на об’єкт, який знаходиться глибоко в ланцюжку каталогів, але не маєте **права на виконання** для доступу хоча б до одного каталогу на шляху до цього файла, то до нього ви так і *не проб’єтеся*).

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

**Хід роботи.**

***Готувала матеріал студентка Мельнічук М.О.***

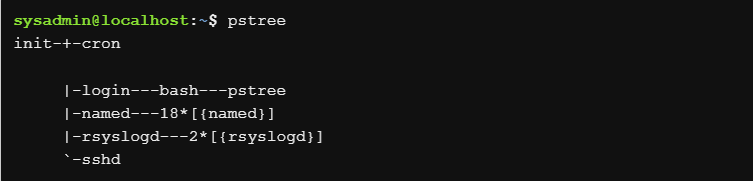
* 1. Початкова робота в CLI-режимі в Linux ОС сімейства Linux:
  2. Запустіть віртуальну машину Ubuntu\_PC ***(якщо виконуєте завдання ЛР через академію netacad)***
  3. Опрацюйте всі приклади команд, що представлені у лабораторних роботах курсу ***NDG Linux Essentials:***
* ***Lab 13: Where Data is 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 |
| 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. |

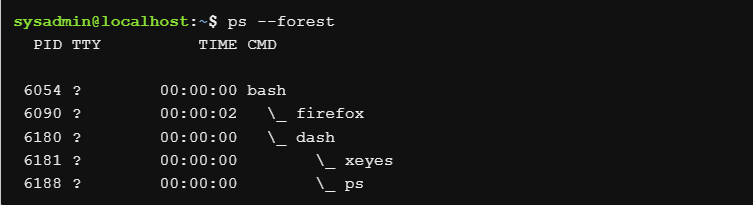
**Відповіді на контрольні запитання:**

***Готували матеріал студентки Мельнічук М.О, Усенко Б.О.***

*1.*Процеси можна «відобразити» в генеалогічне дерево батьківських і дочірніх зв’язків. Якщо ви хочете переглянути це дерево, команда *pstree* відобразить його:



Якщо ви запустите ps з опцією *--forest*, то, подібно до команди *pstree*, він покаже рядки, що вказують батьківський і дочірній зв’язок:

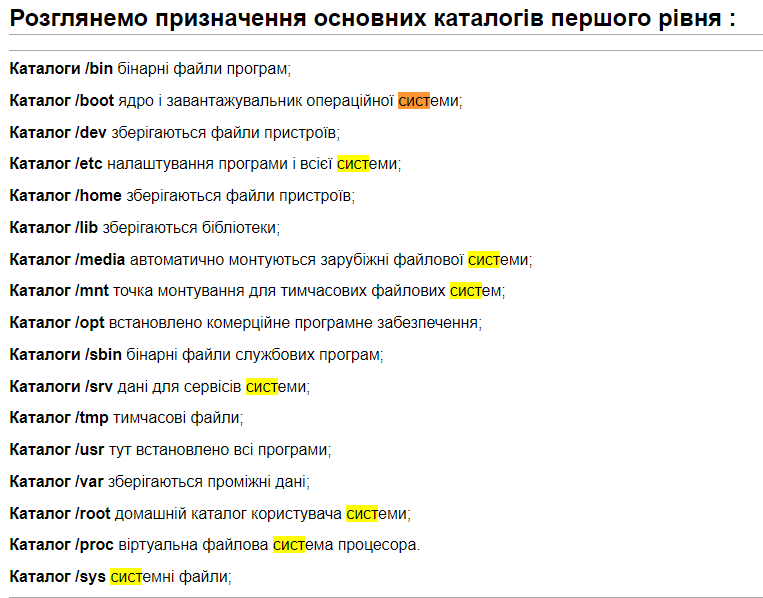


***2***. Каталог /etc налаштування програми і всієї системи;

Найважливіший каталог HKEY\_LOCAL\_MACHINE. Саме ці ключи відповідають фізичним даним реєстру. Ключ HKLM містить інформацію про всю систему

***3.*** /opt Каталог, в який встановлюються додаткові компоненти системи або програми

***4***. sudo - надає можливість користувачам виконувати команди від імені суперкористувача root, або інших користувачів;



[*https://wiki.cuspu.edu.ua/index.php/%D0%9A%D0%B0%D1%82%D0%B0%D0%BB%D0%BE%D0%B3%D0%B8*](https://wiki.cuspu.edu.ua/index.php/%D0%9A%D0%B0%D1%82%D0%B0%D0%BB%D0%BE%D0%B3%D0%B8)*. ??*

*5.*Утиліта *ping* – це дуже простий інструмент для діагностики мережі. Вона дозволяє перевірити доступний віддалений хост чи ні. Для цього утиліта перевіряє, чи хост може відповідати на мережеві запити за допомогою протоколу ICMP.

*ifconfig* (налаштування інтерфейсу) – це інструмент управління мережею. Він використовується для настроювання та перегляду стану мережевих інтерфейсів в операційних системах Linux. За допомогою *ifconfig* ви можете призначати IP-адреси, включати або вимикати інтерфейси, керувати кешем ARP, маршрутами тощо.

*traceroute* — це утиліта, яка дозволяє простежити маршрут проходження даних до віддаленого адресата в мережах TCP/IP.

*6.**Мережевий інтерфейс*— це системний (програмний та/або апаратний) інтерфейс між двома частинами устаткування або шарами протоколів у комп'ютерній мережі. Мережеві інтерфейси забезпечують стандартизовані функції, такі як передавання повідомлень, підключення та відключення тощо.

*Ifconfig* - команда UNIX і UNIX-подібних операційних систем що використовується для налаштування мережевих інтерфейсів.

***7.*** Команда *ifconfig* використовується для конфігурування мережевих інтерфейсів ядра. Вона використовується на етапі завантаження операційної системи при необхідності налаштування інтерфейсів. Після цього вона зазвичай використовується тільки при налагодженні або налаштуванні продуктивності системи.

Якщо аргументи не передані, ifconfig видає інформацію про стан активних інтерфейсів. Якщо вказаний один аргумент інтерфейс, видається інформація тільки про стан цього інтерфейсу; якщо вказаний один аргумент, видається інформація про стан всіх інтерфейсів, навіть відключених. Інакше команда конфігурує вказаний інтерфейс.

У ядрі Linux також є утиліта [IP](https://uk.wikipedia.org/wiki/IP), яка дозволяє керувати великою кількістю налаштувань мережевого інтерфейсу.

Команда ifconfig повинна використовуватися при завантаженні системи для задання адреси кожному інтерфейсу системи. Вона також може використовуватися в подальшому для перевизначення адреси інтерфейсу та інших параметрів його роботи.

ifconfig вимагає вказати існуючий мережевий пристрій (інтерфейс) або -a як перший аргумент. При використанні аргументу -a вибираються всі проініціалізовані мережеві карти. При виклику без опцій ifconfig видає повідомлення про використання. Якщо вказано сімейство протоколів (наприклад, inet), ifconfig буде повідомляти тільки деталі, пов'язані з даними сімейством протоколів. Тільки привілейований користувач може змінювати конфігурацію мережного інтерфейсу.

*8.* Зберігання паролів у прикладних системах (зокрема, в [операційних системах](https://uk.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0)) у відкритому вигляді є *неприпустимим*, оскільки у випадку зламу паролі усіх користувачів стають надбанням порушника.

У явному вигляді паролі ніде в системі не зберігаються, а зберігаються їхні образи – результат виконання над рядком пароля деякої функції. Образи паролів і ідентифікатори користувачів разом з деякою додатковою інформацією зберігаються у файлі **/etc/master.passwd** (в деяких системах – **/etc/shadow**), доступ на читання і запис до якого має тільки суперкористувач (**root**).

*9.*Постійно використовувати обліковий запис root не рекомендується, оскільки, маючи абсолютні права доступу, можна абсолютно випадково нанести системі непоправної шкоди. Тому в системі існує команда su, що дозволяє звичайному користувачеві отримувати root-права в будь-який момент.

*10.*Команда *su* дозволяє запускати оболонку від іншого користувача.

Команда *sudo* дозволяє користувачам виконувати команди як інший користувач.

**Висновок:**

Під час виконання лабораторної роботи ми ознайомилися з базовими структурами для збереження системних, дізналися про стандарт Filesystem Hierarchy Standard та про базові дії при налаштування системи.