“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-93а

Команда 1:

Складаний Я.О.,

Яницький О.А.

Перевірив викладач

Сушанова В.С.

Робота студентів групи РПЗ-93а Команда 1: Складаний Я.О., Яницький О.А.

**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

**Готував матеріал студент Складаний Ярослав**

**2.1 Розкрийте поняття “псевдофайлової системи”, для чого воно потрібно системі?**

"Псевдо" означає брехню, прикидатися. Таким чином, "псевдофайлова система" означає файлову систему, яка немає 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 під каталогом /) 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.

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

Користувачі 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 нальоту, як тільки ви її запитуєте. Але працює все настільки прозоро, що ви непомітите жодної різниці міжз вичайною 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.

**2.3.Якепризначенняфайлів /proc/cmdline, /proc/meminfoта /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. Туж інформацію ми можемо побачити виконавши lsmod. Але цій утиліті також інформацію надає структура proc

**2.4.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

**2.5.Для чого потрібніло г-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

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

Лог завантаження системи - /var/log/dmesg

**2.7.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.

**2.8.Якіосновнікоманди є у Linux для перегляду та конфігурації мережі.**

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

auto enp0s3 іiface enp0s3 inetdhcp - конфігурація інтерфейсу.

**2.9. 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);

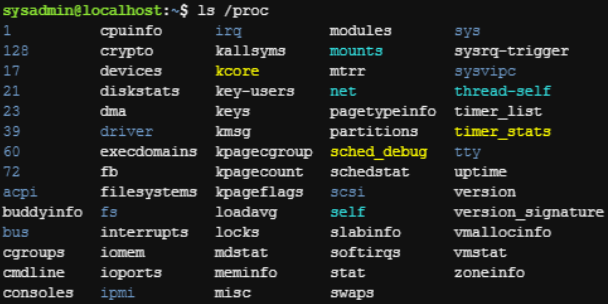
• w – право на зміну вмісту каталогу (можна створювати і видаляти об’єкти в цьому каталозі, причому, якщо ви маєте право на запис, то видаляти ви зможете навіть ті файли, які вам не належать);

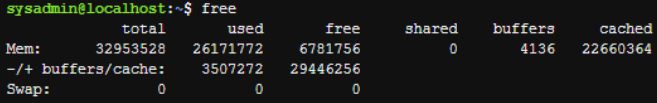
• x – право на виконання, яке дозволяє увійти в каталог (це право завжди перевіряється в першу чергу, і навіть якщо ви маєте усі потрібні права на об’єкт, який знаходиться глибоко в ланцюжку каталогів, але немаєте права на виконання для доступу хоча б до одного каталогу на шляху до цього файла, то до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

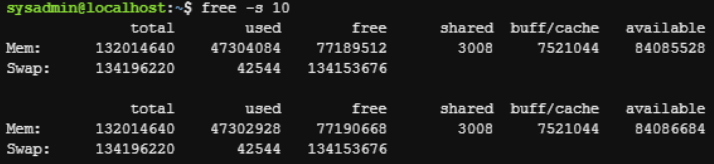
**Готував матеріал студент Складаний Ярослав**

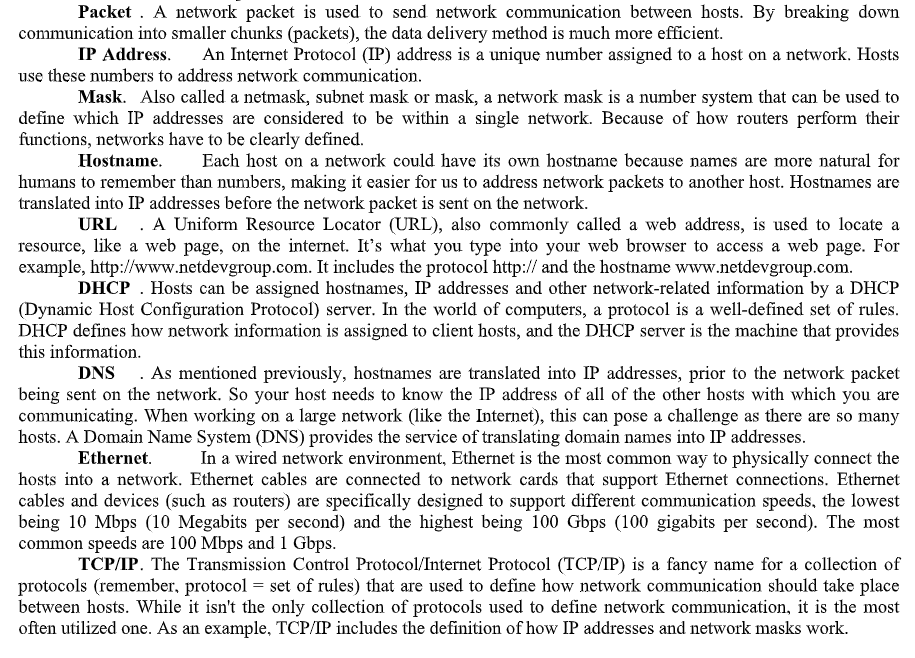
**Хід роботи.**

**Документація з матеріалу роботи.**

****

****

****

****

**Готував матеріал студент Яницький Олександр**

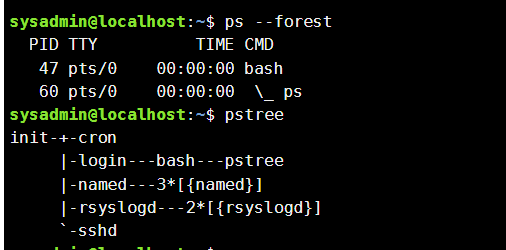
**3. Створіть таблицю команд вивчених у п.2 ходу роботи у наступному вигляді:**

|  |  |
| --- | --- |
| **Назва команди** | **Її призначення та функціональність** |
| free | показує загальне використання системної пам'яті |
| dmesg | дозволяє переглядати поточні повідомлення ядра |
| ifconfig | визначити свою адресу Інтернет-протоколу (IP). |
| route | переглянути таблицю маршрутної інформації |
| dig | використовується для збору інформації DNS. |
| netstat | використовується для усунення несправностей та налаштування |
| ss | переглянути, які з’єднання в даний момент встановлені між локальною машиною та віддаленими машинами, статистику цих з’єднань тощо |
| su | змінити ідентифікатор користувача або стати суперкористувачем |
| sudo | виконати команду від імені іншого користувача |
| id | Роздрукувати ідентифікатор користувача |
| exit | викликати нормальне припинення процесу |
| grep | друкує рядки, які містять відповідність шаблону. |
| getent | отримати записи з бібліотек перемикачів служби імен |
| last | показати список останніх користувачів, які ввійшли в систем |

**Готував матеріал студент Яницький Олександр**

**Відповіді на контрольні питання**

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



*2. У яких каталогах зберігаються налаштування системи?*

Майже завжди файли на дисках об'єднуються в *каталоги*. У найпростішому випадку всі файли на цьому диску зберігаються в одному каталозі. Така *однорівнева* схема використовувалася в CP/M та у першій версії MS-DOS 1.0. *Ієрархічна файлова система* з вкладеними один в одного каталогами вперше з'явилася в Multics'і , потім - в UNIX'і .В даний час однорівневі файлові системи використовуються дуже рідко, за винятком пристроїв з малою обчислювальною потужністю та об'ємом пам'яті, наприклад, [мікроконтролера](https://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BA%D1%80%D0%BE%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D0%BB%D0%B5%D1%80)ESP8266 , що використовує у власній флеш-пам'яті (до 16 Мб) власну файлову систему SPIFFS.

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

Інтерпретатор команд для DOS працює, коли не запущено жодних прикладних програм. Якщо при виході з програми перехідна частина командного інтерпретатора в пам'яті була переписана, DOS перезавантажить його з диска. Деякі команди є внутрішніми, вони вбудовані в COMMAND.COM; інші зовнішні команди, збережені на диску. Коли користувач друкує символи в командний рядок операційної системи, COMMAND.COM буде намагатись розібрати рядок і знайти відповідність між введеною та вбудованою командами або з іменем виконуваного файлу програми, або пакетного файлу на диску. Якщо збіг не знайдено, з'являється повідомлення про помилку, друкується і командний рядок оновлюється. Зовнішні команди були занадто великі, щоб тримати їх в командному процесорі або рідко використовувались. Такі допоміжні програми зберігатимуться на диску і будуть завантажуватись як звичайні програми, але розширені операційною системою. Копії цих програмних команд повинні бути на поточному або доступному диску, або в шлясі команди, що встановлений в командний інтерпретатор.

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

Суперкористувач (також зустрічається під назвами root, supervisor, адміністратор, адмін тощо) — спеціальний [аккаунт](https://uk.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BB%D1%96%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81) в [UNIX-подібних системах](https://uk.wikipedia.org/wiki/UNIX-%D0%BF%D0%BE%D0%B4%D1%96%D0%B1%D0%BD%D1%96_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8) з ідентифікатором (UID, User IDentifier), власник якого має право на виконання всіх без винятку операцій. Суперкористувач UNIX-систем має логін «root» тільки за замовчуванням і легко перейменовується при необхідності.

*5. Поясніть призначення команд ping, ifconfig, traceroute.*

**Ping**  – [утиліта](https://ru.wikipedia.org/wiki/%D0%A3%D1%82%D0%B8%D0%BB%D0%B8%D1%82%D0%B0) для перевірки цілісності та якості з'єднань у [мережах](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) на основі [TCP/IP](https://ru.wikipedia.org/wiki/TCP/IP) , а також звичайне найменування самого запиту.

Команда **ifconfig** - аналог IPconfig Windows, з іншими ключовими параметрами та ширшим функціоналом.

**Traceroute**  — це службова [комп'ютерна програма](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0) , призначена для визначення маршрутів даних у [мережах](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C)[TCP/IP](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%BA_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%BE%D0%B2_TCP/IP) .

*6. Як називаються мережеві інтерфейси в Linux?*

lo – інтерфейс зворотного зв’язку.

eth0 –У сучасних дистрибутивах Linux eth0 можна перейменувати на enp0s31f6 залежно від вашого драйвера.

wlan0 – інтерфейс бездротової мережі в Linux. Знову ж таки, пристрій WiFi може бути перейменовано в wlp82s0 залежно від вашого драйвера.

ppp0 – мережевий інтерфейс Point to Point Protocol, який може використовуватися модемом комутованого зв'язку, підключенням PPTP vpn або бездротовим USB-модемом 3G.

vboxnet0, vmnet1, vmnet8 – Інтерфейс віртуальної машини, що працює в режимі мосту або режимі NAT в Linux.

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

Якщо аргументи не вказано, ifconfig відображає статус активних інтерфейсів системи. Якщо вказано один аргумент інтерфейсу, він відображає статус лише даного інтерфейсу.

*8. Чому в конфігураційних файлах паролі не зберігається в явному вигляді?*

Через особливості конфігурації користувацьких даних. Паролі мають інший тип конфігурації інформації, через що їх вигляд може змінитися.

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

Бо обліковий запис rood має права адміністративного корпусу, через що може змінювати дані які бажано залишати стаоими.

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

**Команда su** (від англ. **s***ubstitute***u***ser - замінити користувача* ) застосовується в основному для перемикання з одного користувача на іншого. При цьому вона може запустити оболонку входу в умовах поточного каталогу і оточення ( su), так і повністю змінити налаштування, замінивши їх оточенням цільового користувача ( su -).

**Команда sudo** (від англ. *"***Substitute U***ser  and***do***"* -  *"підмінити користувача і виконати"* ) використовується як префікс до [**команд Linux**](https://ravesli.com/spisok-vseh-komand-v-linux/) , дозволяючи користувачеві, що увійшов до системи, виконувати команди, що вимагають привілеїв *root* . На відміну від su, команда sudo вимагає введення пароля поточного користувача (котрий виконує цю команду).

**Висновок**

Ознайомились з базовими структурами для збереження системних даних - процеси, память, лог-файли та повідомлення про стан ядра. Ознайомились зі стандартом Filesystem Hierarchy Standard. Ознайомились з базовими діями при налаштуванні мережі.