“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”**

Виконали студенти

групи КСМ-93а

Коваль О.М.

Карпенко І.В.

Перевірив викладач

Повхліб В.С.

Київ 2021

***Коваль Олексій***

**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.**

|  |  |
| --- | --- |
| Log Files | Файли журналу |
| Kernel Messages | Повідомлення ядра |
| Filesystem Hierarchy Standard | Стандарт ієрархії файлової системи |
| Basic Network Terminology | Основна мережева термінологія |
| System and User Security | Захист системи та користувача |

2.

2.1 Файлова система — спосіб організації даних, який використовується операційною системою для збереження інформації у вигляді файлів на носіях інформації. Також цим поняттям позначають сукупність файлів та директорій, які розміщуються на логічному або фізичному пристрої. Створення файлової системи відбувається в процесі форматування.

2.2 З цих папок можна отримати будь-яку інформацію про вашу систему. Наприклад, скільки пам'яті підкачування зараз використовується, наскільки великий розмір кешу процесора, які модулі ядра завантажені, скільки дисків або розділів доступно і т.д. Все це можна отримати у звичайному текстовому вигляді з папки proc linux.

2.3 У /proc/cmdline ви знайдете параметри, зазначені в рядку запуску ядра завантажувачем Grub. Це допомагає при пошуку та усунення проблем за завантаженням ядра або якщо необхідно з'ясувати, який точно файл був використаний для завантаження.

/proc/meminfo - дуже відомий та широко використовуваний файл, який надає нам папка proc. У ньому відображається вся доступна інформація про оперативну пам'ять та простір підкачки. Саме за допомогою цього файлу скрипти дізнаються інформацію про доступну пам'ять.

/proc/modules - містить список усіх завантажених модулів ядра. Ту ж саму інформацію ми можемо побачити виконавши команду «lsmod». Але цій команді також інформацію надає структура proc.

2.4 free - виводить інформацію про використання оперативної та віртуальної пам'яті

df – про використання дискового простору.

2.5 Лог-файл – це документ із послідовним записом усіх подій, що відбуваються на веб-сайті або віддаленому сервері. Оскільки фіксується все, що відбувається, вивчення лога дозволяє використовувати накопичені дані в різних важливих для просування та обслуговування сайтів цілях.

* При виникненні технічних проблем, недоступності сайту, вірусному зараженні, хакерських атаках, DDoS-атаках адміністратор ресурсу може за зафіксованими у файлі логу відомостями з'ясувати причину, що полегшить та прискорить усунення небажаних наслідків.
* За допомогою відомостей з лога, SMM’щик може вивчати поведінку відвідувачів на сайті, оцінювати якість цільового трафіку, формувати рекомендації щодо покращення, вибирати оптимальні стратегії просування та розкрутки сайту.

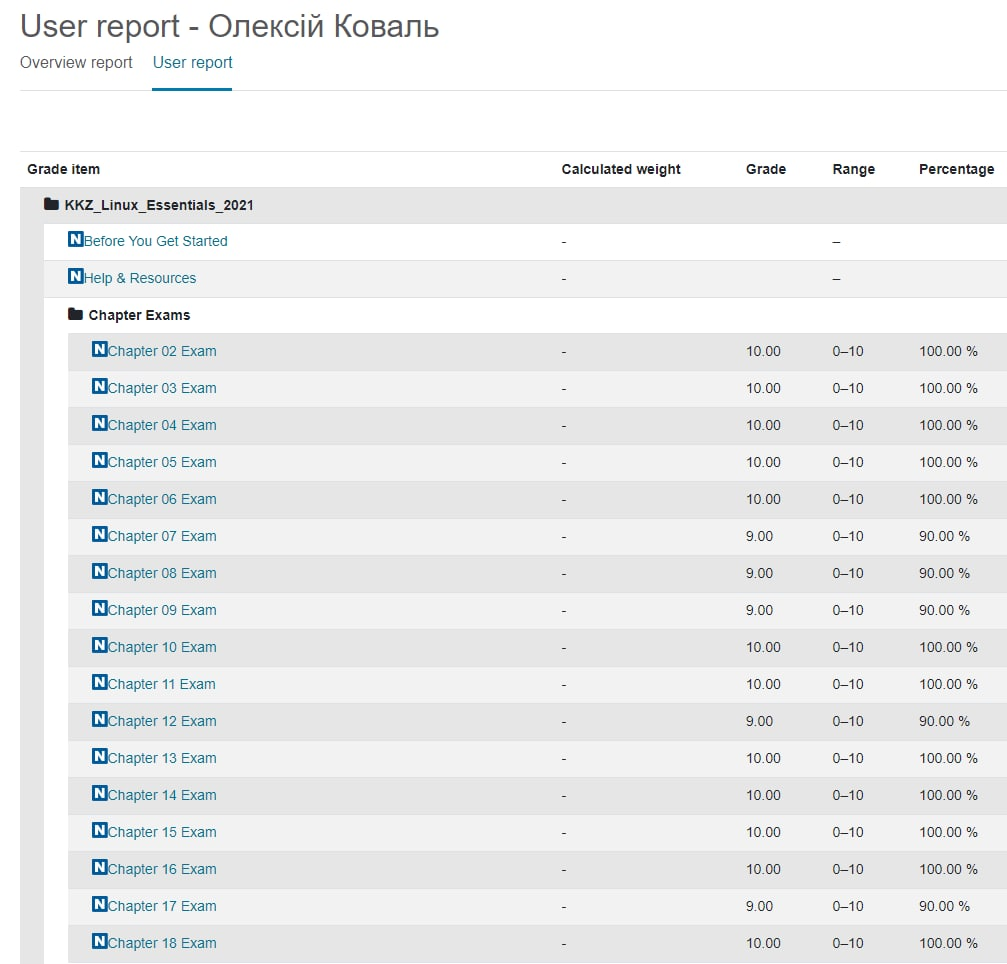
2.6 /var/log/dmesg- драйвера пристроїв. Командою dmesg можна переглянути висновок вмісту файлу. Розмір журналу обмежений, коли файл досягне своєї межі, старі повідомлення будуть перезаписані новішими.

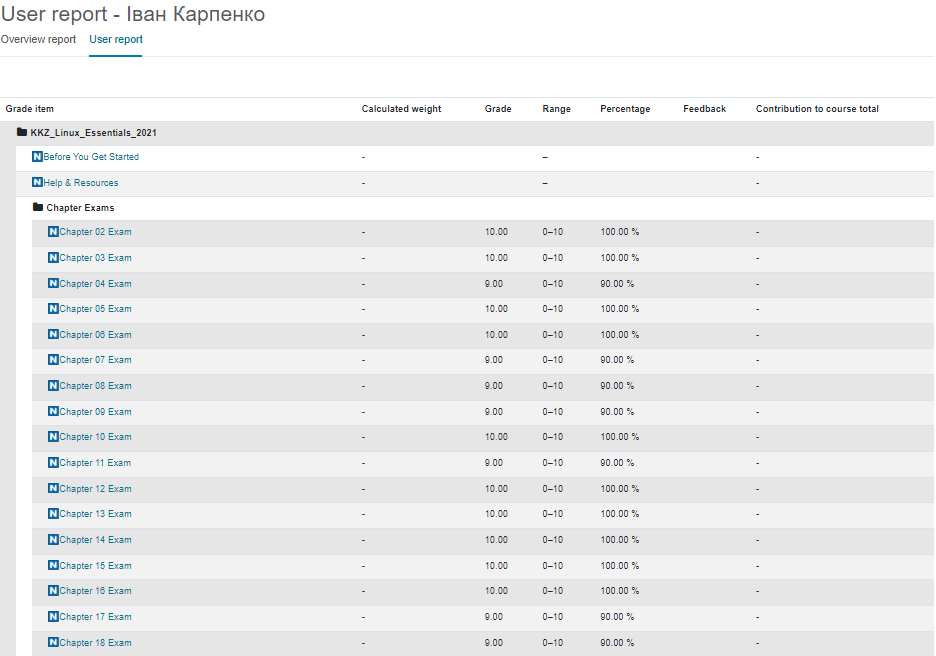
2.7 Filesystem Hierarchy Standard - стандарт прийнятий для уніфікації розташування файлів і каталогів загального призначення у файловій системі ОС UNIX. Сьогодні більшість UNIX-подібних систем в тій або іншій мірі слідують цим правилам. Наприклад, типова база даних про користувачів завжди зберігається у файлі /etc/passwd.

2.8

* Команда find
* Команди whereis і which
* Команда less
* Команди head і tail
* Команди cat і tac
* Команда wc

2.9 У системі існує файл, що зберігає облікові записи груп, у якому зазначені імена груп та відповідні їм числові ідентифікатори. Зазвичай цей файл називається /etc/group. На додачу до групи, ідентифікатор якої зазначений у файлі паролів, ОС Linux дозволяє користувачу бути членом інших груп.

4. 



**Хід роботи.**

1. Початкова робота в CLI-режимі в Linux ОС сімейства Linux:

1.1. 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.

1.2. Запустіть віртуальну машину Ubuntu\_PC (якщо виконуєте завдання ЛР через академію netacad)

1.3. Запустіть свою операційну систему сімейства Linux (якщо працюєте на власному ПК та її встановили) та запустіть термінал.

2. 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

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

|  |  |
| --- | --- |
| free | Найзручніша команда Linux для перевірки використання пам'яті в linux. |
| vmstat | Дозволяє вивести інформацію щодо використання пам’яті, дисків, процесору. |
| top command | Команда top зазвичай використовується для перевірки використання пам'яті та завантаження процесора для кожного процесу. Однак він також повідомляє про спільне використання пам'яті та може використовуватися для контролю загального використання пам'яті. Верхня область містить потрібну інформацію. |
| htop | Подібно до команди top, команда htop також показує використання пам'яті та іншу інформацію. |

***Карпенко Іван***

**Контрольні запитання:**

1. Як і багато утиліт UNIX, ps має масу опцій, найбільш поширені з них це: a - показує процеси, запущені іншими користувачами

x - показує процеси, що не мають контролюючого терміналу (або запущені з іншого терміналу)

u - виводить ім'я користувача, який запустив процес, та час запуску для кожного з процесів.

Команда pstree виводить процеси у вигляді дерева. Так ви зможете відразу бачити, який процес є батьківським якого, що буде дуже корисним коли вам потрібно буде зняти цілу низку процесів, а ви зможете усе зняти просто виключивши батьківський процес.

У той час, коли ps –forest вважається менш зрозумілішою за pstree.

2. Специфічні налаштування Linux зазвичай зберігаються у /eth

3. У більшості випадків програми зберігаються у /usr, а там вже діляться на частини:

/usr/bin – виконуючі файли програми.

/usr/sbin – виконуючі файли програми, що використовують права адміністратора.

4. Дистрибутив зазвичай містить програми для початкової ініціалізації системи (у випадку дистрибутиву операційної системи — ініціалізація апаратної частини, завантаження урізаної версії системи і запуск програми-встановлювача), програму-встановлювач (для вибору режимів і параметрів встановлення) і набір спеціальних файлів, що містять окремі частини системи (так звані пакети).

Наявність дистрибутивів — наслідок того, що форма програмного забезпечення, яка використовується для його розповсюдження, майже ніколи не збігається з формою програмного забезпечення на працюючій системі.

5. Команда ping – спеціальна програма для перевірки доступності мережевих ресурсів. Фахівці з мережевих технологій використовують команду ping частіше за будь-яку іншу команду, хоча дія, що виконується цією командою - найпростіша. Команда ping посилає вказаний хост пакет заданого розміру, який потім повертається назад.

Команда tracert (traceroute)

Дуже часто користувачі запитують, з чим пов'язана різниця в написанні tracert і traceroute? Насправді команда tracert застосовується в операційних системах Windows, а traceroute - в операційних системах Linux і в операційній системі маршрутизаторів Cisco.

Найпростіший і найпоширеніший приклад використання команди tracert - tracert ya.ru. При використанні команди tracert з літерною адресою хоста, що перевіряється, автоматично перевіряється ще й працездатність і доступність DNS - сервера. Адже для того, щоб почати процес трасування, команда tracert повинна спочатку зв'язатися з сервером DNS і отримати IP-адресу хоста, що перевіряється.

Команда ifconfig використовується для конфігурування мережевих інтерфейсів ядра. Вона використовується на етапі завантаження операційної системи при необхідності налаштування інтерфейсів.

6. Налаштування мережевих інтерфейсів в UNIX / Linux-системах зазвичай виконується за допомогою команди ifconfig, а в Linux ще й за допомогою команди ip.

7. Це можна зробити за допомогою уточнювання куди ми звертаємося, тобто:

sudo ifconfig eth1 або до будь-якого потрібного вам

8. Для того, щоб запобігти його перехвату. Якщо б наші паролі не шифрувалися, то при перехваті їх було б дуже легко дізнатися. Тому зазвичай при шифруванні інший ком’ютер (або, наприклад, сервер) мають ключ дешифрування. А також якщо хтось отримає доступ до файлів серверу то не зможе дешифрувати паролі.

9. Зазвичай використовується для запобігання якихось неприємних подій, бо користувач з root правами має необмежений доступ та можливості, ти можеш видалити кореневу папку та прийдеться відновлювати систему з backup’у

10. Sudo і su є двома різними способами отримання привілеїв root, до того ж кожен функціонує по-різному.

Команда su перемикається на користувача root. Вам потрібно буде ввести пароль кореневого облікового запису. Це не все, що виконує команда su, також ви можете використовувати її для перемикання на будь-який обліковий запис користувача. Якщо виконати su User2 (у випадку коли такий юзер є) вам буде запропоновано ввести пароль до його кореневого облікового запису, а оболонка перейде на користувача User2.

Після виконання команд у кореневій оболонці слід ввести “exit”, залишити кореневу оболонку і повернутися до режиму обмежених привілеїв.

Sudo запускає лише одну команду з привілеями root. При використанні команди sudo, система запросить пароль поточного облікового запису користувача команду як кореневий користувач. Метод їх роботи – і є ключова відмінність між su та sudo.

**Висновок:** Ми ознайомилися з базовими структурами для збереження системних даних, зі стандартом Filesystem Hierarchy Standard, з базовими діями при налаштуванні мережі.