Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Н. А. Рибачок, Я.О.Юсин

Адміністрування ОС Linux

Комп'ютерний практикум

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавра
за спеціальністю 121 Інженерія програмного забезпечення

Електронне мережеве навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2024

УДК 004.45
Р49

Автори: *Рибачок Наталія Антонівна*, канд. техн. наук
Юсин Яків Олексійович, доктор філософії

Рецензенти: *Вунтесмері Ю.В.,* канд. техн. наук, доцент, КПІ ім. Ігоря Сікорського
Ткаченко О.А., канд. фіз.-мат. наук, доцент, Державний університет інфраструктури та технологій

Відповідальний редактор Заболотня Тетяна Миколаївна, канд.техн.наук, доцент

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 2 від 08.11.2024 р.) за поданням вченої ради Факультету прикладної математики (протокол № 2 від 30.09.2024 р.)

Рибачок Н.А., Юсин Я.О.

Р49 Адміністрування ОС Linux [Електронний ресурс] : комп. практикум: навч. посіб. для здобувачів ступеня бакалавра за освіт. програмою «Інженерія програмного забезпечення мультимедійних та інформаційно-пошукових систем» спец. 121 Інженерія програмного забезпечення / Н. А. Рибачок, Я. О. Юсин; КПІ ім. Ігоря Сікорського. – Електрон. текст. дані (1 файл). – Київ : КПІ ім. Ігоря Сікорського, 2024. – 86 с.

Навчальний посібник містить приклади використання утиліт командного рядка для керування, дмініструання та супроводження операційних систем Linux. Навчальний посібник містить інструкції до виконання практичних завднь, а також вимоги до оформлення звітів. Видання призначене для здобувачів ступеня бакалавра спеціальності 121 Інженерія програмного забезпечення факультету прикладної математики КПІ ім. Ігоря Сікорського.

УДК 004.45

Реєстр. № НП 24/25-080. Обсяг 2,2 авт. арк.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Берестейський, 37, м. Київ, 03056
https://kpi.ua
Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.

ЗМІСТ

ВСТУП

Операційна система Linux, будучи відкритою та безкоштовною, є потужною альтернативою комерційним оперційним системам, таким як macOS та Windows. Вона є безпечною та надійною, гнучкою та легкою в налаштуванні. ОС Linux використовується для керування як вбудованими пристроями, так і потужними корпоративними серверами. Звичайні користувачі можуть використовувати цю ОС для роботи із своїми ПК. Уміння ефективно використовувати та керувати операційною системою є критично важливим при роботі із обчислювальною системою.

Метою вивчення дисципліни «Адміністрування ОС Linux» є формування у студентів здатностей працювати у командному рядку bash, виконуючи задачі локального та віддаленого адміністрування серверів Linux та автоматизуючи виконання таких завдань. Студенти навчаться самостійно створювати локальні та віддалені віртуальні машини, інсталювати вебсервери та керувати їх роботою, взаємодіяти із файловою системою та адмініструвати користувачів, вирішувати проблеми із завантажуваностю ОС, керувати процесами та завданнями, обробляти текстові потоки, працюватb із сервером MySQL, автоматизувати виконання завдань, використовувати протокол віддаленого доступу SSH.

Метою комп'ютерного практикуму є отримання практичних навичок керування та налаштування операційних систем. У практикумі надаються завдання, методичні вказівки щодо їх виконання, вимоги щодо оформлення звітів, питання для самоперевірки та рекомендована література. Практикум розроблений для виконання практичних завдань під час аудиторних занять та самостійної роботи.

Навчальний посібник призначений для студентів, які навчаються за спеціальністю 121 «Інженерія програмного забезпечення» факультету прикладної математики КПІ ім. Ігоря Сікорського.

ПРАКТИЧНЕ ЗАВДАННЯ 1.
СТВОРЕННЯ ТА НАЛАШТУВАННЯ ВІРТУАЛЬНОЇ МАШИНИ ІЗ ОС XUBUNTU 22.04 LTS У VIRTUALBOX

Мета роботи – набуття навичок із керування віртуальними машинами (ВМ) у середовищі Oracle Virtualbox.

Завдання

Створити ВМ із заданими параметрами. Інсталювати ОС Xubuntu. Налаштувати параметри ВМ. Налаштувати доступ за SSH із перенаправлення портів ВМ. Інсталювати сервер Nginx та виконати перенаправлення портів ВМ. Оформити звіт та вимкнути ВМ.

Підготовка до виконання завдання

1. Встановити Oracle VM VirtualBox https://www.virtualbox.org/wiki/Downloads/.
2. Завантажити дистрибутив Xubuntu 22.04.3 LTS (Jammy Jellyfish).

Для основної ОС Windows:

1. встановити MobaXterm https://mobaxterm.mobatek.net/download–home–edition.html;
2. перевірити наявність OpenSSH Client.

Для основної ОС Linux перевірити наявність графічного клієнта SSH Remmina.

Вказівки до виконання завдання

1. Створіть віртуальну машину.

1.1. ВМ повинна мати назву «Xubuntu2204_lastname», де lastname – ваше прізвище латиницею (рис. 1.1). Не обирайте Skip unattended.

1.2. Виконайте налаштування інсталяції операційної системи (ОС):

- При створенні користувача надайте йому ім’я “lastname”.
- В якості імені комп’ютера використайте КРх, де х – номер групи.
- Оберіть Guest Additions для встановлення гостьових доповнень.

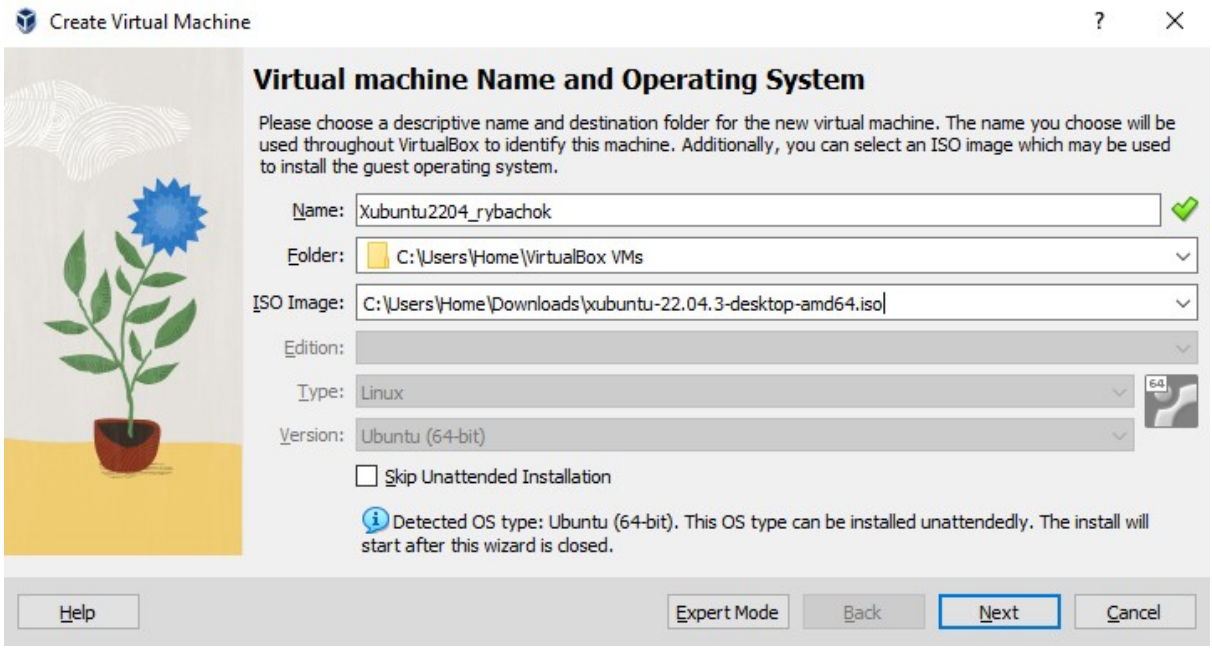


Рис. 1.1. Створення віртуальної машини

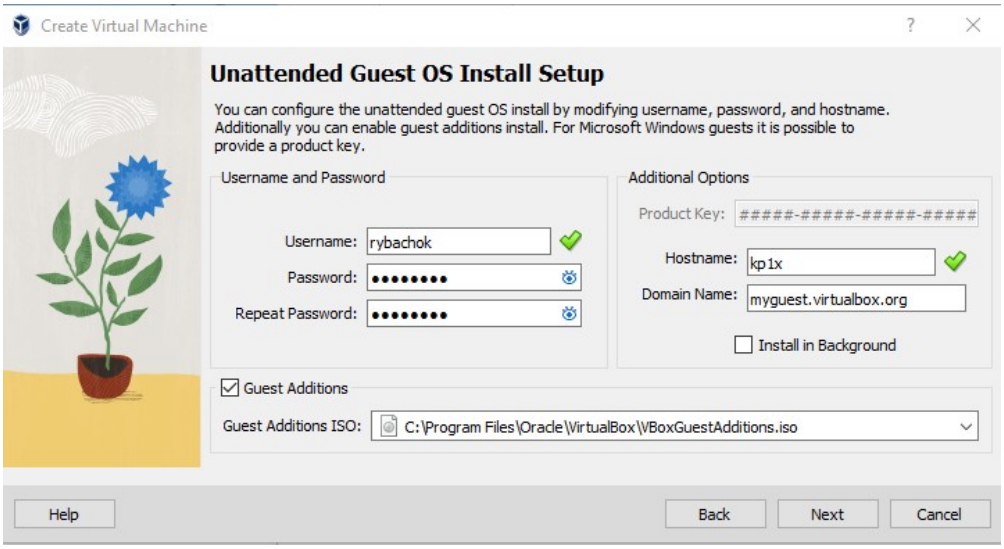


Рис.1.2. Налаштування інсталяції ОС

1.3. Виконайте налаштування параметрів ВМ. Рекомендовані параметри: пам*ять - 2 Гб, ВЖД - 25 Гб.

2. Запустіть ВМ та встановіть ОС (процес інсталяції має запуститися автоматично).

3. Після запуску налаштуйте ВМ:

- порядок завантаження ВМ:
    - жорсткий диск,
    - CD/DVD (підмонтуйте ISO-образ установочного диску);
- мережа через NAT;

- двонаправлений буфер обміну;
- drag and drop;
- спільні теки: в якості спільної теки виберіть директорію Downloads основної ОС (рис. 1.3).

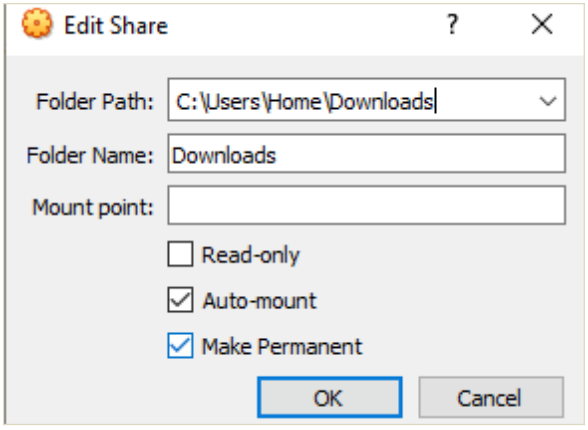


Рис.1.3. Налаштування спільної теки

Зробіть скріншот 1 головної сторінки менеджера ВМ (рис. 1.5).

4. Налаштуйте доступ за SSH із перенаправлення портів ВМ.

4.1. Дізнайтеся інтернет адресу (IP) ВМ:

ip a

Зробіть скріншот 2 результату виконання попередньої команди.

4.2. Налаштуйте перенаправлення портів ВМ відповідно до номеру варіанту (табл. 1.1), де N – номер студента в списку групи.

Таблиця 1.1. Правило перенаправлення портів ВМ

	host	guest
ip	127.0.0.N,	10.0.2.15
port	2000+N	22

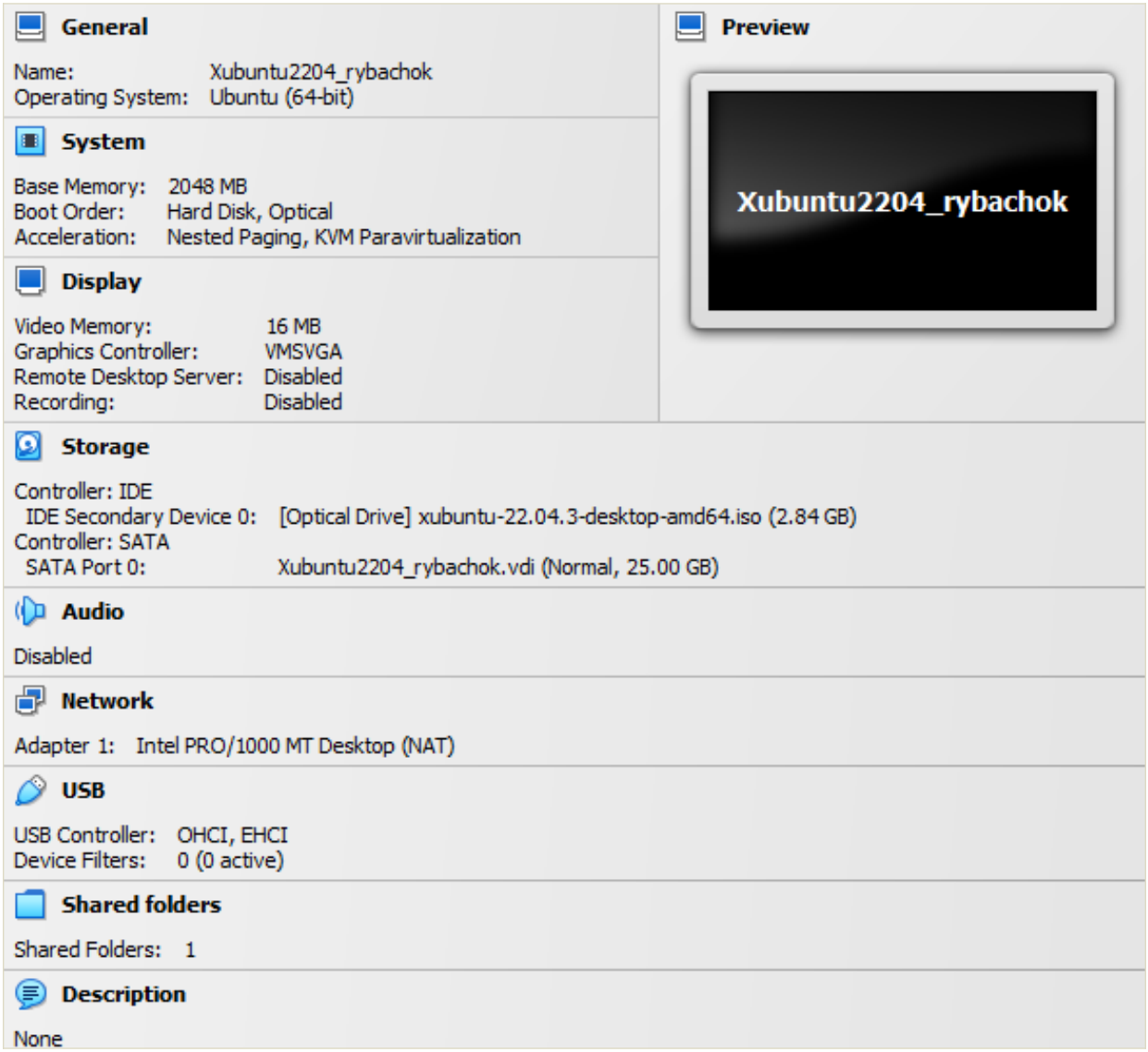


Рис.1.5. Головна сторінка менеджера ВМ. Приклад скріншоту 1

```
rybachok@kp1x:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:67:78:26 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86122sec preferred_lft 86122sec
    inet6 fe80::ca08:2e04:6b26:e1fd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Рис.1.6. Інформація про мережеві інтерфейси. Приклад скріншоту 2

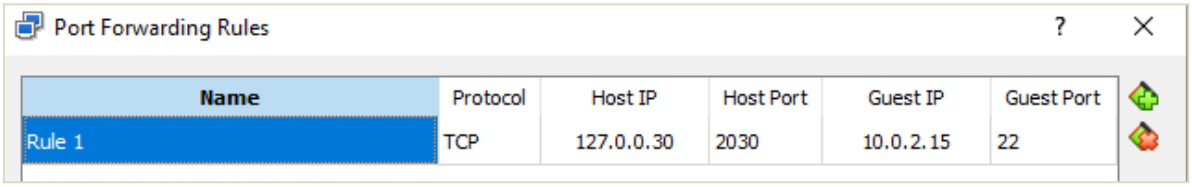


Рис. 1.7. Правило перенаправлення порту SSH. Приклад скріншоту 3

4.3. Встановіть та налаштуйте SSH Server:

sudo apt-get update

sudo apt-get install -y Openssh-server

sudo nano /etc/ssh/sshd_config

AllowTCPForwarding Yes

(для збереження змін використовуйте скорочення клавіш Ctl+S, Ctl+X)

sudo systemctrl reload sshd

4.4. Перевірте, чи входить ваш користувач до групи sudo:

id

Якщо користувач не входить до цієї групи, виконайте такі дії:

su root

usermod <lastname> -aG sudo

nano /etc/sudoers

<lastname> ALL=(ALL) ALL

4.5. Підключіться за ssh із основної ОС:

ssh <lastname>@127.0.0.N –p 2000+N

4.6. Виконайте команди:

- перегляду авторизованих користувачів:

w

- виведення рядків із файлу конфігурації:

cat /etc/ssh/sshd_config | grep -i Forwarding | grep -v \#

Зробіть скріншот 3.

```
rybachok@kp1x:~$ w
 11:42:57 up 12 min,  2 users,  load average: 1,51, 1,21, 0,68
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
rybachok tty7     :0               11:32   12:17   4.30s  0.31s xfce4-session
rybachok pts/2    10.0.2.2         11:39    1.00s  0.06s  0.00s w
rybachok@kp1x:~$ cat /etc/ssh/sshd_config | grep -i Forwarding | grep -v \#
AllowTcpForwarding yes
X11Forwarding yes
```

Рис. 1.7. Доступ за ssh із основної ОС із виконанням команд. Приклад скріншоту 3

5. Інсталюйте сервер Nginx та виконайте перенаправлення портів ВМ.

5.1. Інсталюйте сервер Nginx:

sudo -i

apt update -y

apt install -y nginx

systemctl enable nginx

systemctl start nginx

echo '<html><h1> Student <username> results from Xubuntu</h1></html>' > /var/www/html/index.html

де <*username*> - ваше прізвище латиницею.

/var/www/html/index.html - адреса головної сторінки вебсерверу.

5.2. Перенаправте порти ВМ (рис. 1.7). Зробіть скріншот 4.

Port Forwarding Rules

Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
Rule 1	TCP	127.0.0.30	2030	10.0.2.15	22
Rule 2	TCP	127.0.0.30	2080	10.0.2.15	80

Рис. 1.7. Правила перенаправлення портів. Приклад скріншоту 4

5.3. Зробіть скріншот 5 в основній ОС.

127.0.0.30:2080

Student Rybachok results from Xubuntu

Рис. 1.9. Головна сторінка вебсервера віртуальної машини. Приклад скріншоту 5

6. Оформіть звіт та вимкніть ВМ.

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку;
- Завдання;
- скріншоти 1-5;
- висновки.

Питання для самоперевірки

1. Яка команда використовується для визначення внутрішньої адреси ВМ?

2. Які налаштування необхідно виконати для перенаправлення порту SSH?

3. Які параметри необхідно вказати при створенні ВМ?

Література

1. Oracle® VM VirtualBox® // Електронний ресурс. Режим доступу: https://www.virtualbox.org/manual/UserManual.html

ПРАКТИЧНЕ ЗАВДАННЯ 2.
СТВОРЕННЯ ТА НАЛАШТУВАННЯ ВІРТУАЛЬНОЇ МАШИНИ UBUNTU НА ХМАРНІЙ ПЛАТФОРМІ AWS

Мета роботи – вивчення основних можливостей хмарної платформи AWS з керування віртуальними машинами.

Завдання

Ознайомитися із середовищем AWS Learner Lab. Створити ВМ Ubuntu AWS із заданими параметрами. Переглянути параметри ВМ. Визначити IP адресу. Перевірити доступність вебсторінки на Nginx сервері. Визначити дані для встановлення SSH з'єднання. Доступитися до ВМ за SSH із основної ОС. Доступитися до ВМ за SSH із ВМ Xubuntu. Вимкнути віртуальні машини.

Підготовка до виконання завдання

Для основної ОС Windows:

- завантажити інсталятор та встановити ПЗ https://mobaxterm.mobatek.net/download-home-edition.html

- встановити OpenSSH Client https://learn.microsoft.com/en-us/windows-server/administration/openssh/openssh_install_firstuse?tabs=gui

Для основної ОС Linux перевірити наявність графічного клієнта SSH Remmina.

Вказівки до виконання завдання

1. Почніть роботу із середовищем Learner Lab.

1.1. Перейдіть до сторінки курсу, *Modules - AWS Academy Learner Lab - Launch AWS Academy Learner Lab* та ознайомтеся із документацією.

1.2. Запустіть середовище, натиснувши *Start Lab* та відкрийте консоль AWS.

2. Створіть ВМ Ubuntu із заданими параметрами.

2.1. Доступіться до сервісу віртуальних машин:

Home-Services-EC2-Instances

2.2. Ініціюйте створення ВМ, натиснувши *Launch instance*.

2.3. Оберіть такі параметри ВМ:

- **Name and tags** Ubuntu with Nginx
- **Application and OS Images (Amazon Machine Image)**
  - **Quick Start -** Ubuntu (Ubuntu 22.04 LTS)
- **Instance type** t2.small
- **Key pair (login)** vockey (rsa)
- **Network Settings** As default

Firewall (security groups)

Create a new security group **(launch-wizard-1)**

- Allow SSH - Anywhere
- Allow HTTP

Щоб забезпечити більшу безпеку доступу за SSH до ВМ, можна визначити та вказати IP адреси кожного пристрою (мобільного та ноутбука, ПК)з яких відбуватиметься доступ, якщо вони різні. Для визначення IP адреси пристрою можна використати вебсервіси, наприклад: https://2ip.ua/ua/, https://ipaddress.my/.

- **Configure storage** по замовчуванню (by default)
- **Advanced details**
  - Termination protection - Enable
  - В якості User data вкажіть набір команд:

#!/bin/bash

apt update -y

apt install -y nginx

systemctl enable nginx

systemctl start nginx

echo '<html><h1> Student <username> results from Ubuntu</h1></html>' > /var/www/html/index.html

де <username> - ваше прізвище латиницею,

/var/www/html/index.html - адреса головної сторінки вебсерверу,

> - знак запису до файлу.

- **Summary** по замовчуванню (by default).

Для ініціалізації створення ВМ натисніть Launch instance.

2. Перегляньте параметри створеної ВМ.

2.1. Налаштуйте параметри відображення ВМ, як на рис. 2.1.

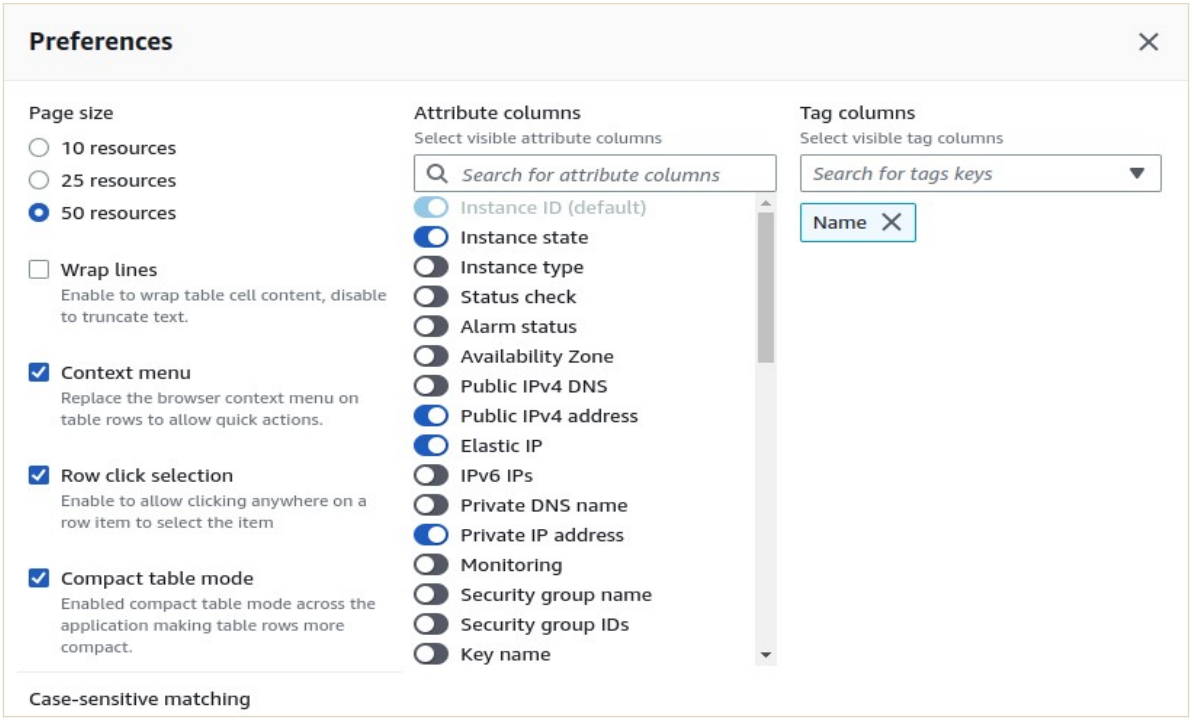


Рис.2.1. Налаштування відображення параметрів ВМ

2.2. Визначте IP адреси:

- Public IPv4 - зовнішня (для доступу з Інтернет);
- Private IP - внутрішня (для доступу в локальній мережі).

2.3. Зупиніть ВМ. Зверніть увагу, що публічна IP адреса буде звільнена.

2.4. Запустіть ВМ. Зверніть увагу, що публічна IP адреса буде надана нова.

2.5. Створіть статичну IP адресу та прив’яжіть її до ВМ:

2.5.1. Створіть статичну IP адресу:

Network & Security - Elastic IPs - Allocate Elastic IP address

(в формі залишити все без змін) - Allocate

2.5.2. Із списку оберіть створену адресу, приєднайте її до ВМ:

Action-Associate Elastic IP address

У новій формі у полі Instance обиріть створену ВМ - Associate.

2.6. Визначте IP адреси та зробіть скріншот 1.

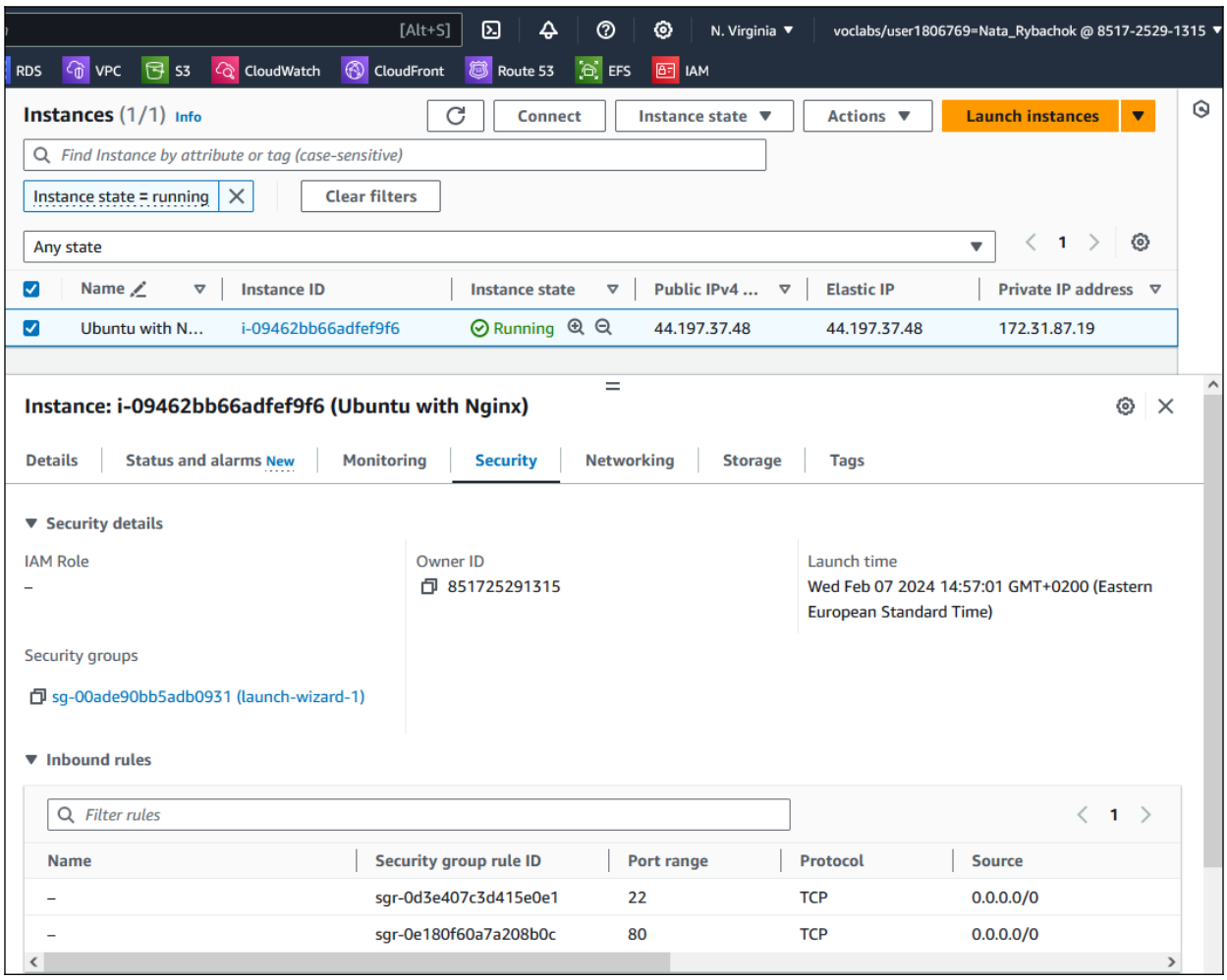


Рис. 2.2. Властивості ВМ. Приклад скріншоту 1

Зверніть увагу, що скріншот 1 обов'язково має містити назву облікового запису, саме ці поля відображення та вкладинку Security.

3. Перевірте доступність вебсторінки на Nginx сервері. Зверніть увагу, щоб у браузері було звернення до сторінки саме за протоколом http: http://Public IPv4. Зробіть скріншот 2.

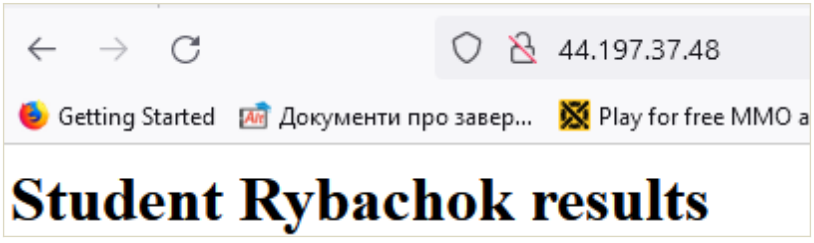


Рис. 2.3. Головна сторінка вебсерверу Nginx. Приклад скріншоту 2

Зверніть увагу, що скріншот 1 обов'язково має містити адресний рядок та ваше прізвище на сторінці.

4. Визначте дані для встановлення SSH з'єднання.

Для встановлення з'єднання використовується команда:

ssh -i private_key_name username@Public IPv4

де private_key_name - приватний ключ,

username - ім'я користувача ВМ,

Public IPv4 – публічна IP адреса.

4.1. Завантажте приватний ключ із середовища Leaner Lab (рис. 2.4):

AWS Details - Download .PEM

Про доступ за цим ключем написано у *Learner Lab - Foundational Services – Readme.*

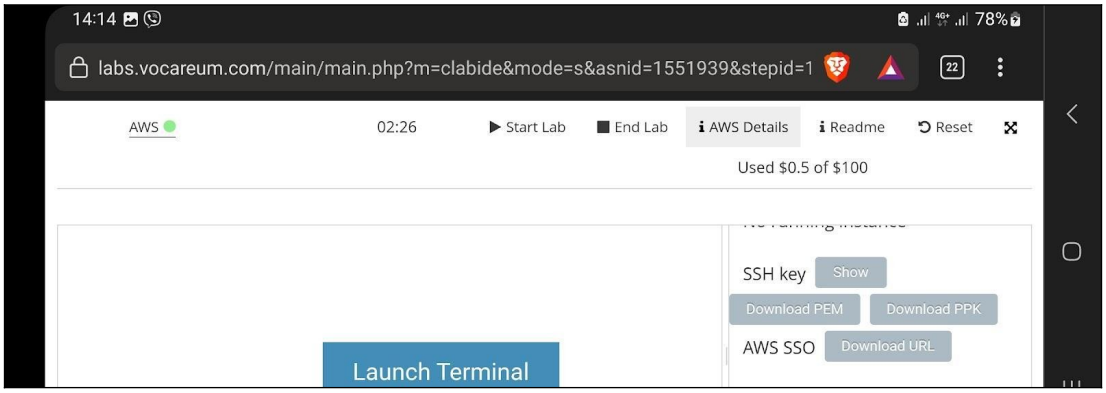


Рис.2.4. Вікно для завантаження приватного ключа

Файл матиме назву *labsuser.pem* та повинен знаходитися у папці *Downloads.*

4.2. Визначте ім'я користувача ВМ (рис.2.5):

Home-Services-EC2-Instances - обираємо Ubuntu with Nginx – Connect

Ім'я користувача за замовчуванням ubuntu.

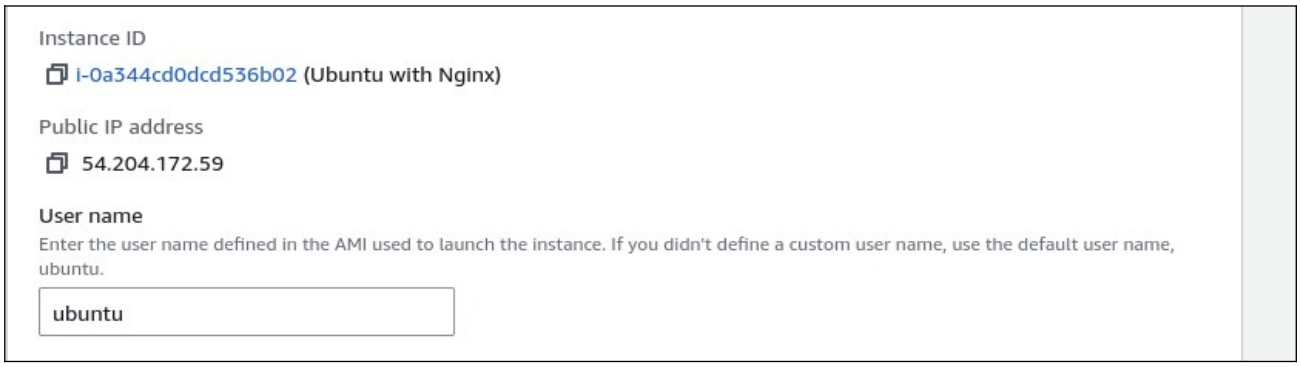


Рис.2.5. Вікно для встановлення з’єднання через браузер

5. Виконайте доступ до ВМ Ubuntu за SSH із основної ОС.

Для основної ОМС Windows

5.1. Виконайте доступ через програму з графічним інтерфейсом MobaXterm.

Змініть права на файл із приватним ключем:

Shell -> bash

cd Downloads

chmod 400 labsuser.pem

Обиріть вкладку *Session*

Підключіться до ВМ за ssh:

Remote host = Public IPv4

Specify username = username (ubuntu)

Port = 22 (SSH)

Use private key = private key name (labsuser.pem)

Зробіть скріншот 3 (вікно має містити заголовок сесії).

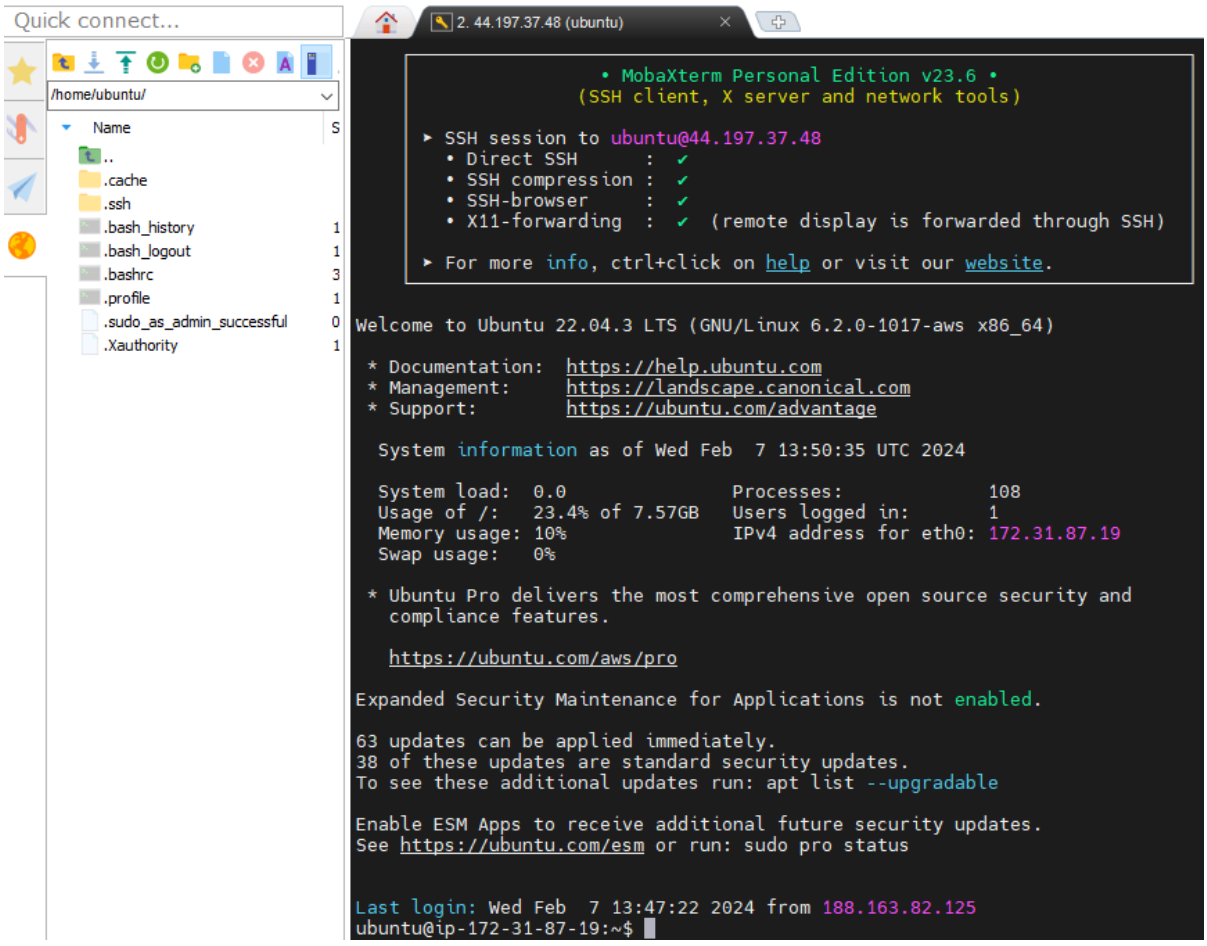


Рис. 2.6. Підключення через графічний інтерфейс. Приклад скріншоту 3

Завершіть сеанс bash - виконайте команду exit.

5.2. Виконайте підключення із командного рядка cmd чи Powershell.

Налаштуйте параметри безпеки файлу приватного ключа як на рис. 2.7 (видаліть всіх користувачів, залишіть тільки доступ на читання основному користувачу).

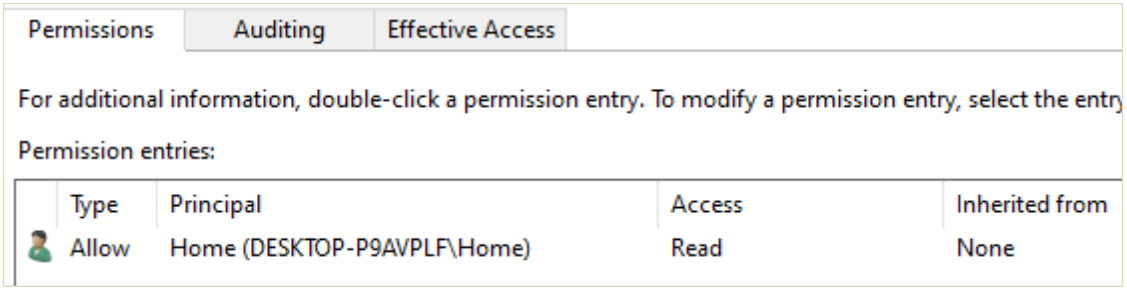


Рис. 2.7. Права доступу на файл labsuser.pem

Виконайте доступ за SSH:

ssh -i labsuser.pem ubuntu@Public IPv4

Зробіть скріншот 4 (має містити команду підключення).

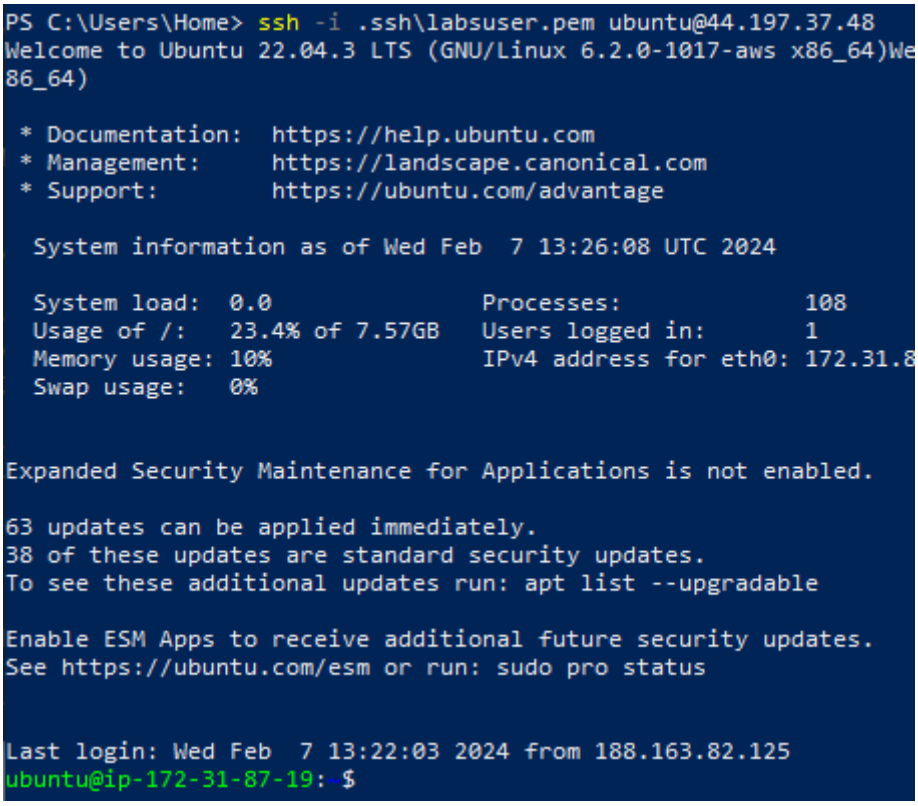


Рис. 2.8. Підключення через командний рядок. Приклад скріншоту 4

Завершіть сеанс bash, виконавши команду exit.

Для основної ОС Linux

5.1. Виконайте доступ через програму з графічним інтерфейсом.

Змініть права на файл приватного ключа в bash:

chmod 400 labsuser.pem

Підключіться до ВМ за Remmina:

Server = Public IPv4

User name = ubuntu

Identity file = labsuser.pem

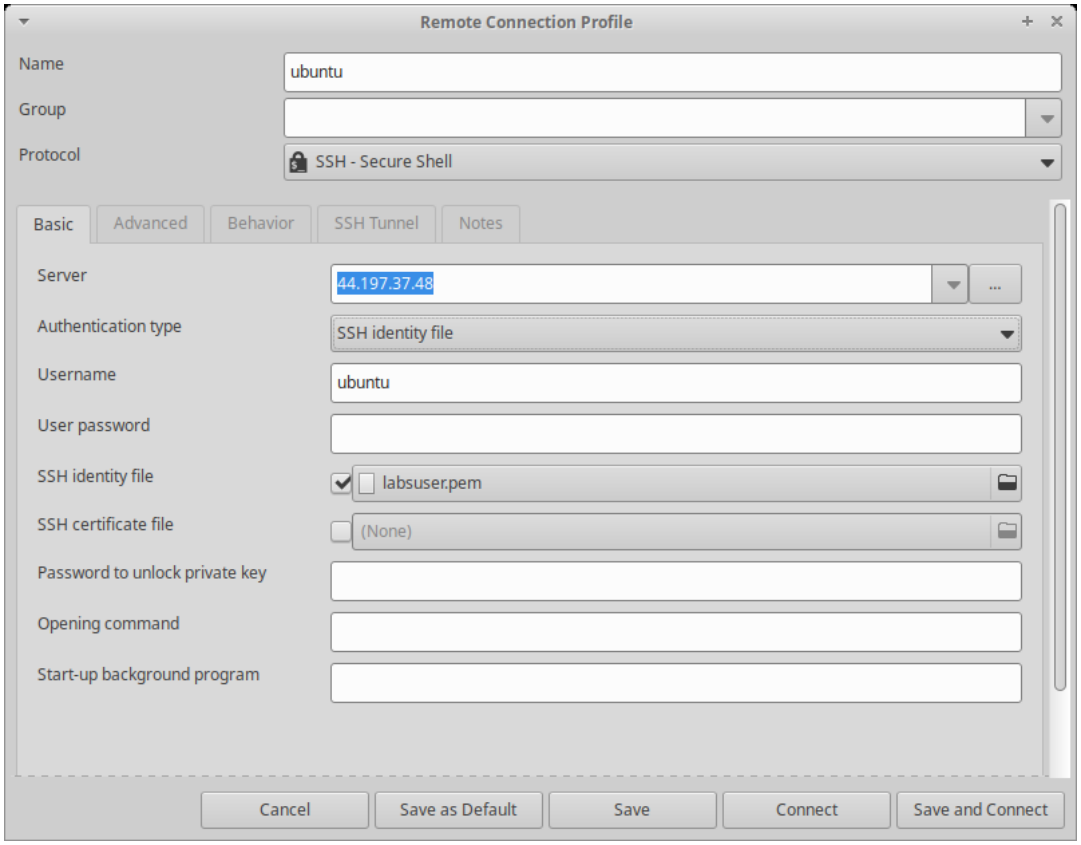


Рис. 2.9. Вікно Remmina підключення до ВМ

Зробіть скріншот 3 (вікно має містити заголовок програми).

Вийдіть із сеансу, виконавши exit.

5.2. Виконайте підключення із командного рядка bash:

ssh -i labsuser.pem ubuntu@Public IPv4

Зробіть скріншот 4 (вікно має містити команду встановлення з'єднання).

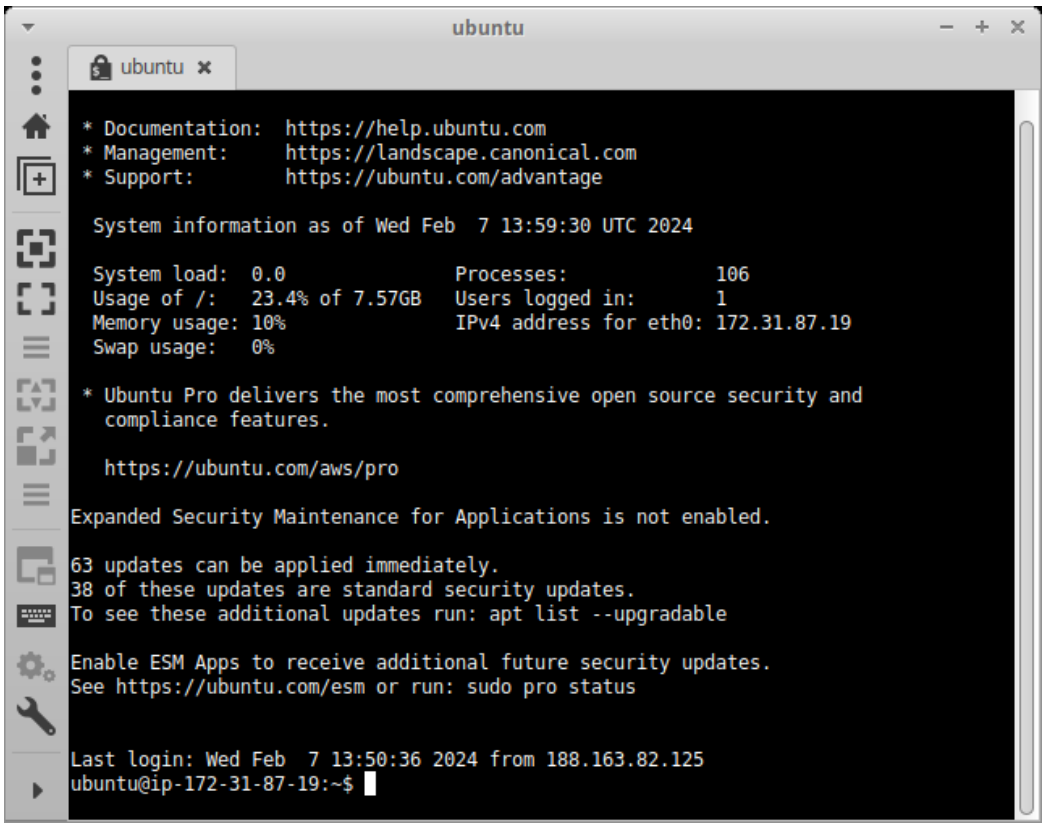


Рис. 2.10. Підключення через графічний інтерфейс. Приклад скріншоту 3

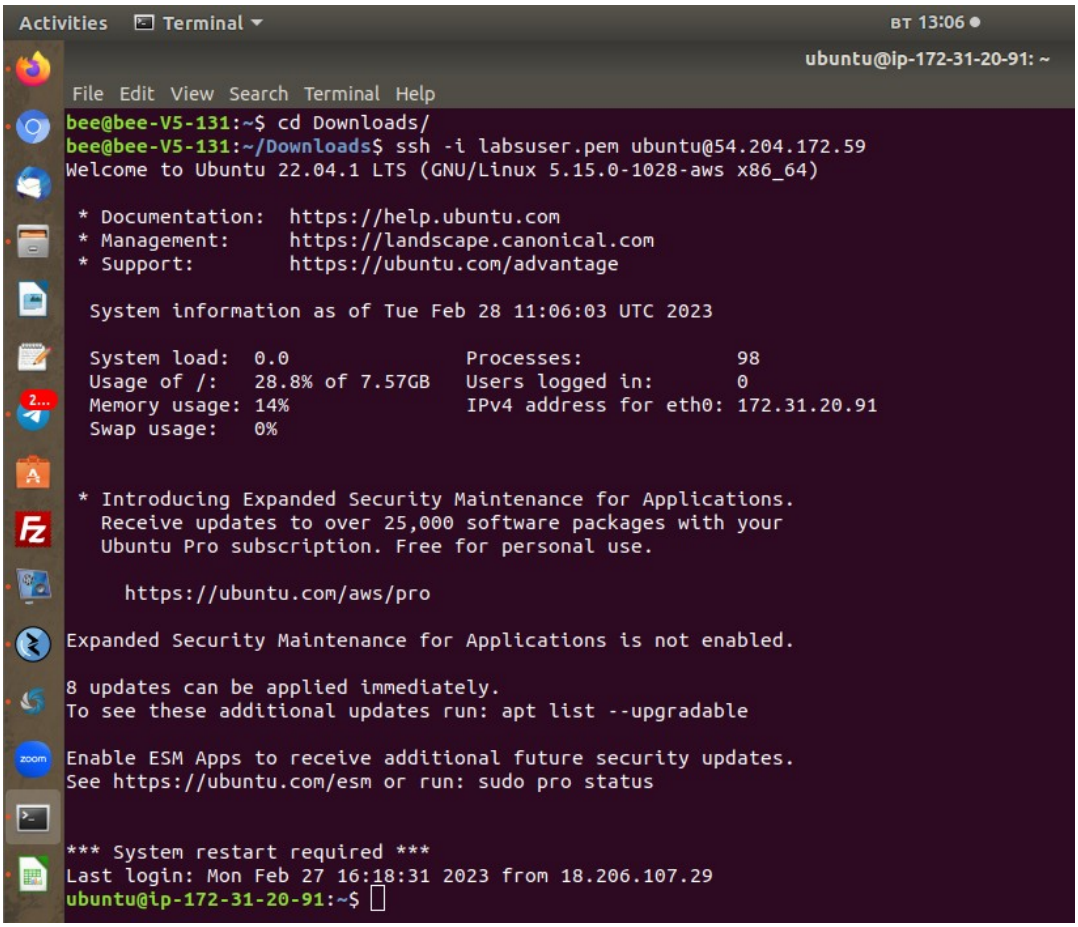


Рис. 2.10. Підключення через командний рядок. Приклад скріншоту 4

Вийдіть із сеансу, виконавши exit.

6. Доступіться до ВМ Ubuntu за SSH із ВМ Xubuntu.

6.1. Із основної ОС виконайте копіювання приватного ключа в ВМ Xubuntu в домашню директорію користувача ~ (рис. 2.11).

```
C:\Users\Home\.ssh>scp -P 2030 labsuser.pem rybachok@127.0.0.30:
rybachok@127.0.0.30's password:
labsuser.pem                                  100% 1674   416.7KB/s   00:00
```

Рис. 2.11. Копіювання приватного ключа

6.2. У віртуальній машині перемістіть ключ в директорію .ssh та надайте приватному ключу права 400:

mv labsuser.pem .ssh/

chmod 400 .ssh/labsuser.pem

6.3. Встановіть з'єднання із сервером:

ssh -i .ssh/labsuser.pem ubuntu@IP_address

Зробіть скріншот 5 (вікно має містити команду підключення).

```
rybachok@kp1x:~$ ssh -i .ssh/labsuser.pem ubuntu@44.197.37.48
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1017-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Feb  7 14:04:17 UTC 2024

  System load:  0.0               Processes:             102
  Usage of /:   23.4% of 7.57GB   Users logged in:       1
  Memory usage: 10%               IPv4 address for eth0: 172.31.87.19
  Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

63 updates can be applied immediately.
38 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Wed Feb  7 13:59:30 2024 from 188.163.82.125
ubuntu@ip-172-31-87-19:~$
```

Рис. 2.12. Доступ за SSH із ВМ Xubuntu. приклад Скріншоту 5

7. Зупиніть віртуальні машини.

Щоб завершити роботу із середовищем AWS Learner Lab, виконайте Sing out із консолі, закрийте сторінку, виконаємо End Lab. Віртуальна машина при цьому автоматично вимкнеться. Можна вручну вимкнути ВМ, обравши її та виконавши операцію Stop Instance.

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку,
- Завдання;
- скріншоти 1-5,
- висновки.

Питання для самоперевірки

1. Як визначити внутіршню та зовнішню IP адреси ВМ?

2. Як відкрити порти для вхідного трафіку ВМ?

3. Як завантажити приватний ключ SSH та які права він повинен мати?

3. Як визначити ім’я користувача ВМ?

5. Синтаксис та призначення команди ssh.

6. Синтаксис та призначення команди scp.

Література

1. User Guide for Linux Instances // Електронний ресурс. Режим доступу: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EC2_GetStarted.html

ПРАКТИЧНЕ ЗАВДАННЯ 3.
ОТРИМАННЯ ДОВІДКИ У BASH

Мета роботи – набуття навичок із отримання довідки у командному рядку bash.

Завдання

Запустити ВМ Xubuntu. Знайти характеристики користувача, операційної системи, апаратного забезпечення у ВМ Xubuntu та створити файл із результатами. Передати вміст файлу для розміщення на вебсервер. Вимкнути ВМ.

Знайти характеристики користувача, операційної системи, апаратного забезпечення у середовищі AWS Leaner Lab. Створити файл із результатами та передати його на розміщення у ВМ Ubuntu AWS. Оформити звіт та завершити роботу із середовищем.

Вказівки до виконання завдання

1. Запустіть ВМ Xubuntu.

2. Знайдіть характеристики користувача, операційної системи, апаратного забезпечення у ВМ Xubuntu.

2.1. В домашній папці користувача створіть директорію OS/result та зайдіть до неї:

- визначте тип та отримайте довідку для команди mkdir;
- визначте тип та отримайте довідку для команди cd;
- створіть директорії OS та OS/result, зайдіть до OS/result.

2.2. За допомогою команди env, використовуючи команду grep, виведіть інформацію про змінні середовища:

- визначте тип та отримайте довідку для команди env;
- визначте тип та отримайте довідку для команди grep;
- за допомогою grep із виведення команди env виберіть дані, які стосуються USER;
- допишіть дані в кінець файлу task3.txt (див. рис. 3.1).

Приклад команди:

command | grep string >> task3.txt

2.3. За допомогою команди hostnamectl, використовуючи команду grep, виведіть дані про назву хоста, операційну систему, ядро ОС:

- визначте тип та отримайте довідку для команди hostnamectl;
- за допомогою grep із виведення команди hostnamectl виберіть дані, які стосуються назви хоста, операційної системи, ядра ОС;
- допишіть дані в кінець файлу task3.txt

2.4. За допомогою команди cat прочитайте створений файл:

- визначте тип та отримайте довідку для команди cat;
- виконайте команду cat без опцій (отримане від користувача введення виводиться у рядок);
- прочитайте створений файл;
- прочитайте файли /etc/issue, /etc/hostname.

2.5. За допомогою команди free виведіть інформацію про об'єм ОП:

- визначте тип та отримайте довідку для команди free;
- визначити опцію, яка використовується для відображення в форматі, зручному для людини (show human-readable output);
- допишіть дані в кінець файлу task3.txt

2.6. За допомогою команди df виведіть інформацію про об'єм жорсткого диску:

- визначте тип та отримайте довідку для команди df;
- визначте опцію, яка використовується для відображення в форматі, зручному для людини (show human-readable output);
- за допомогою grep виберіть дані, які стосуються тільки кореневого розділу /;
- допишіть дані в кінець файлу task3.txt

2.7. За допомогою команди lscpu виведіть інформацію про кількість процесорів:

- визначте тип та отримайте довідку для команди lscpu;
- за допомогою grep виберіть дані, які стосуються кількості ЦП:

lscpu | grep ^CPU'('s')':

- допишіть дані в кінець файлу task3.txt

2.8. За допомогою команди timedatectl установіть часову зону на сервері Europe/Kyiv:

- визначте тип та отримайте довідку для команд timedatectl;
- виведіть список часових зон;
- установіть часову зону Europe/Kyiv (використайте sudo);
- використовуючи команду grep, виведіть дані про часову зону та запишіть у файл task3.txt

2.9. Призначте псевдонім для команди встановлення ssh з'єднання із ВМ Ubuntu на хмарній платформі:

- визначте тип та отримайте довідку для команди alias;
- встановіть псевдонім у поточній сесії, переконайтеся, що він працює коректно;
- відкрийте нову оболонку:

bash

- переконайтеся, що псевдонім відсутній у новій оболонці;
- допишіть команду встановлення псевдоніму у файл ~/.bashrc:

nano ~/.bashrc

- відкрийте нову оболонку:

bash

- перегляньте всі псевдоніми;
- допишіть створений псевдонім до файлу task3.txt

2.10. Відредагуйте файл task3.txt таким чином, щоб між блоками результатів завдань був пустий рядок і вони починалися з початку рядка (рис. 3.1).

2.11. Додайте використані команди із відповідними опціями (п. 1.2-1.8) до task3.txt.

```
rybachok@kp1x:~/OS/result$ cat task3.txt
USER=rybachok

Static hostname: kp1x
Operating System: Ubuntu 22.04.3 LTS
Kernel: Linux 6.2.0-32-generic

               total        used        free      shared  buff/cache   available
Mem:           1,9Gi       275Mi       738Mi        15Mi       944Mi       1,5Gi
Swap:          2,6Gi          0B       2,6Gi

/dev/sda3        24G   12G   11G  53% /

CPU(s):                             1

Time zone: Europe/Kiev (EET, +0200)

alias ssha='ssh -i /home/rybachok/.ssh/labsuser.pem ubuntu@44.197.37.48'
```

Рис. 3.1. Вміст файлу task3.txt. Приклад скріншоту 1

2.12. Створіть файл /var/www/html/task3.html та запишіть у нього теги і вміст файлу task3.txt (рис. 3.2).

sudo -i

```
root@kp1x:~# echo '<html><pre>'> /var/www/html/task3.html
root@kp1x:~# cat /home/rybachok/OS/result/task3.txt >> /var/www/html/task3.html
root@kp1x:~# echo '</pre></html>' >> /var/www/html/task3.html
```

Рис. 3.2. Створення файлу /var/www/html/task3.html

2.13. Відкрийте файл на сервері та зробіть скріншот 2 (має містити результат виконання п.1.2-1.8 та відповідні команди).

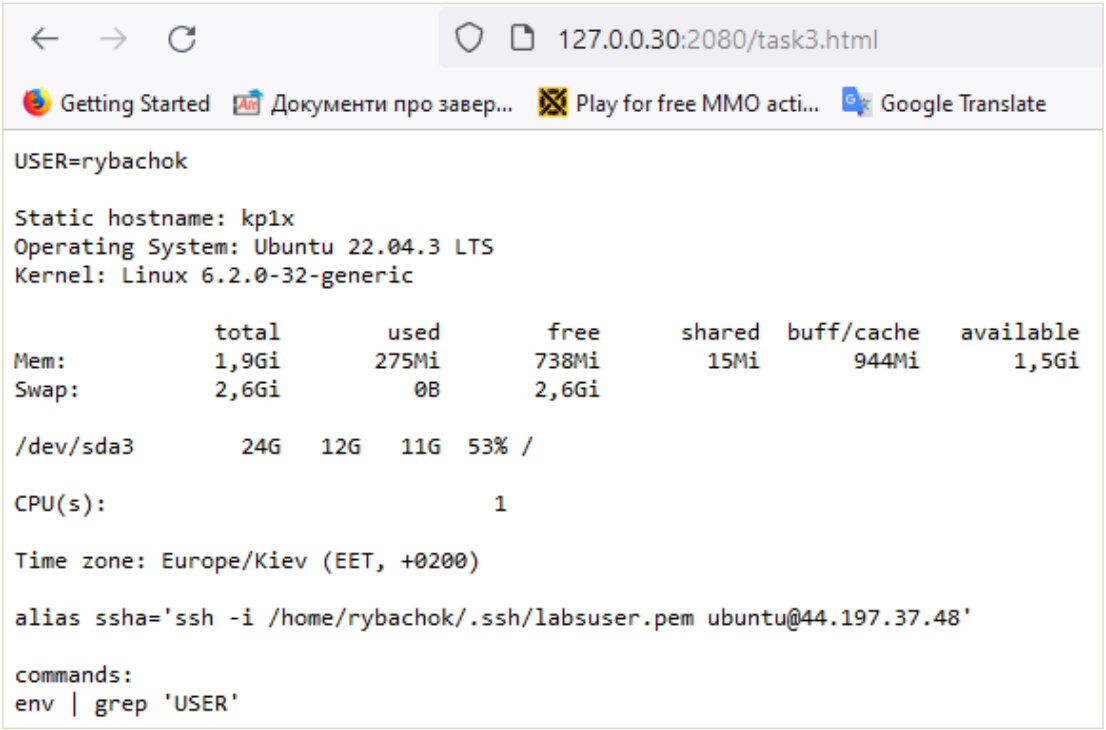


Рис. 3.3. Вміст файлу /var/www/html/task3.html. Приклад скріншоту 2

2.14. Завершіть сеанс bash командою exit.

2.15. Вимкніть віртуальну машину.

3. Знайдіть характеристики користувача, операційної системи, апаратного забезпечення у середовищі AWS Leaner Lab.

3.1. Запустіть середовище AWS Leaner Lab. Роботу виконуйте у Терміналі середовища (рис. 3.4).

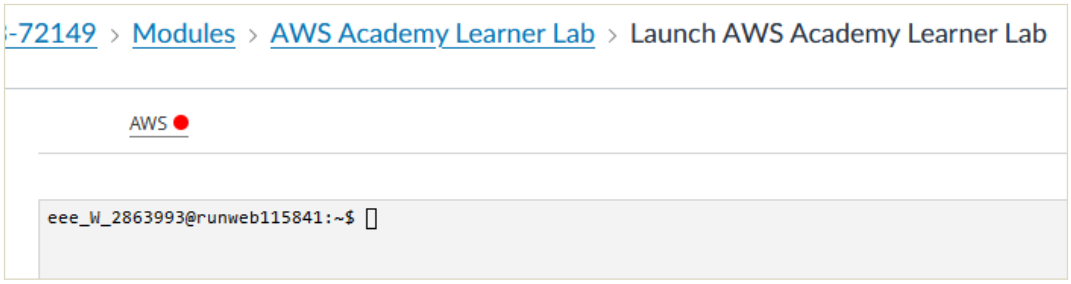


Рис. 3.4. Темінал середовища Leaner Lab

3.2. Створіть файл із даними <lastname>3.html та додайте в нього початкові обрамляючі теги <html><pre>, <lastname> - ваше прізвище латиницею.

3.3. Визначте параметри середовища Leaner Lab та додайте їх у файл <lastname>3.html:

- ім’я поточного користувача;
- налаштування хосту:
    - назва;
    - операційна система;
    - ядро;
- інформацію про об'єм ОП;
- інформацію про об'єм жорсткого диску (розділу /);
- інформацію про кількість процесорів;
- часову зону.

3.4. Відредагуйте файл <lastname>3.html таким чином, щоб між блоками результатів завдань був пустий рядок і вони починалися з початку рядка.

3.5. Додайте до файлу <lastname>3.html закриваючі обрамляючі теги </pre></html>.

3.6. Передайте файл <lastname>3.html у віртуальну машину AWS Ubuntu:

scp <lastname>3.htm -i .ssh/labsuser.pem ubuntu@Public_IPv4:

Використовується приватний ключ labsuser.pem, який знаходиться в директорії .ssh.

3.7. Відкрийте сеанс із віртуальною машиною AWS Ubuntu та перемістіть файл із директорії домашнього користувача в директорію вебсервера:

ssh -i .ssh/labuser.pem ubuntu@Public_IPv4

sudo mv <lastname>3.htm /var/www/html/

3.8. Відкрийте вебсторінку у браузері та зробіть скріншот 2. Зверніть увагу, що результат знаходиться на сервері Nginx віртуальної машини Ubuntu.

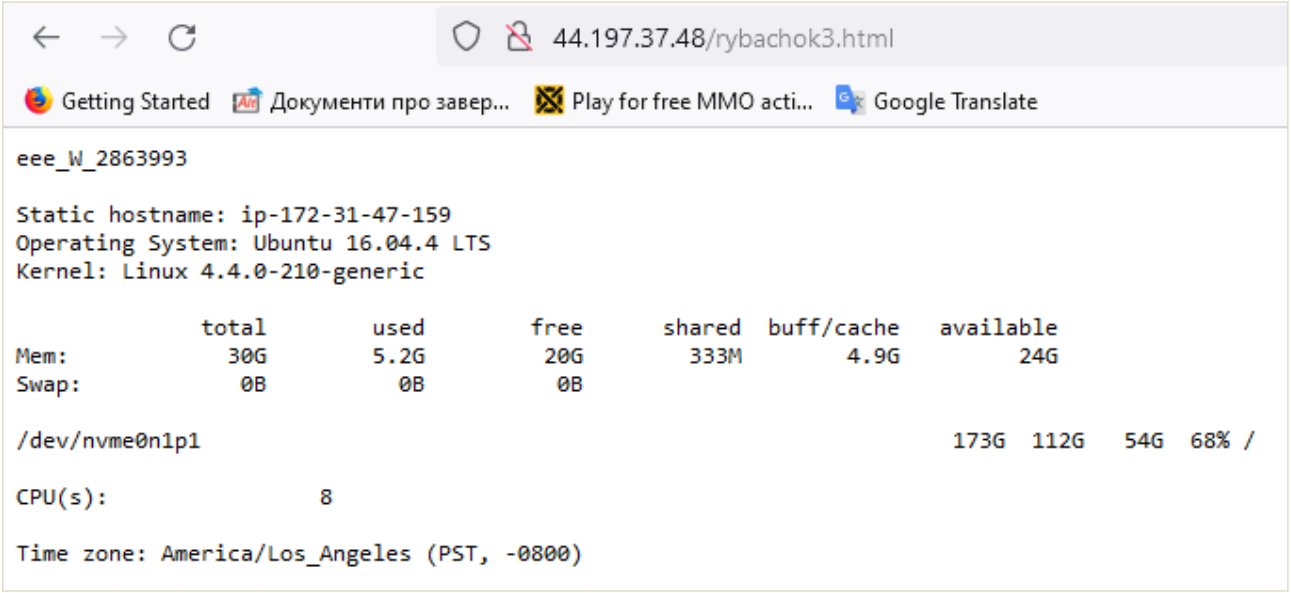


Рис. 4. Вміст файлу /var/www/html/<lastname>3.html. Приклад скріншоту 2

3.9. Закрийте з'єднання із сервером:

exit

3.10. Заверште сеанс роботи з середовищем AWS Leaner Lab.

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку,
- Завдання;

- скріншоти 1, 2;
- висновки.

Питання для самоперевірки

1. Чим відрізняються внутрішні та зовнішні команди bash?
2. Які є типи обробників внутрішніх команд bash?
3. Розділи man та їх призначення.
4. Використання псевдонімів у bash.

Література

1. linuxcommand.org // Електронний ресурс. Режим доступу: https://linuxcommand.org/

ПРАКТИЧНЕ ЗАВДАННЯ 4.
РОБОТА В КОМАНДНОМУ РЯДКУ BASH

Мета роботи – набуття навичок із роботи в командному рядку bash.

Завдання

Запустити ВМ Ubuntu AWS та під'єднатися до неї за SSH. Внести зміни в налаштування ОС Ubuntu. Написати скрипт для виведення інформації про систему. Створити файли результатів та розмістити їх на вебсервері. Оформити звіт та вимкнути ВМ.

Вказівки до виконання завдання

1. Запустіть ВМ Ubuntu AWS та під'єднайтеся до неї за SSH.

2. Внесіть зміни в налаштування системи:

1.1. установіть часову зону – Europe/Kiev;

1.2. змініть назву хоста на <lastname>,

де lastname – ваше прізвище латиницею.

2. Напишіть скрипт для виведення інформації про систему.

2.1. Скрипт має знаходитися в файлі ~<username>/script/script4.sh.

2.2. Скрипт має містити функцію, яка показує параметри системи:

- назву хоста ;
- назву ОС;
- версію ядра;
- дані про ОП;
- дані про кореневий розділ /;
- дані про ЦП;
- часову зону;
- дату.

3. Виведіть результати у файл результатів ~<username>/result/task4.html та на екран, обрамляючи тегами для відображення сторінки в браузері (рис. 4.1).

```
(echo '<html><pre>';./script4.sh;echo '</pre></html>') | tee ../result/task4.html
```

Рис.4.1. Створення файлу ~<username>/result/task4.html

4. Таким же чином підготуйте файл script4.sh для розміщення на сервері як файл script4.html з відповідним форматуванням (рис. 4.2).

```
(echo '<html><pre>'; cat script/script4.sh;echo '</pre></html>') | tee result/script4.html
```

Рис.4.2. Створення файлу ~<username>/result/script4.html

5. Розмістіть результати на сервері: скопіюйте файл task4.html та script4.html в директорію /var/www/html (рис. 4.3).

```
sudo cp result/script4.html /var/www/html/
sudo cp result/task4.html /var/www/html/
```

Рис. 4.3. Розміщення файлів результатів на сервері

6. Оновіть головну сторінку сервера, додавши посилання на файли (рис. 4.4).

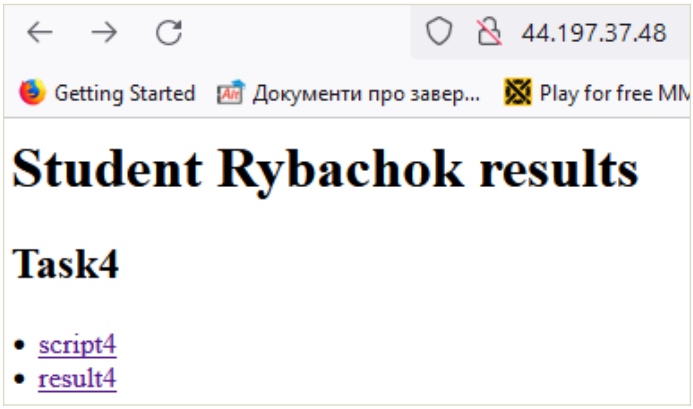


Рис. 4.4. Головна сторінка вебсервера

7. Зробіть скріншоти сторінок зі скриптом та результатами його виконання (скрипт має бути видно повністю).

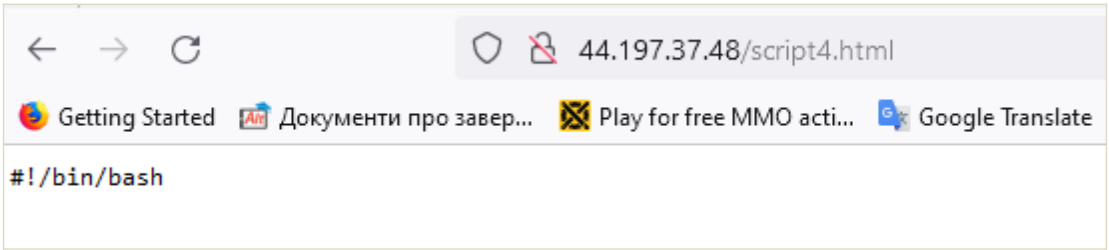


Рис. 4.5. Вміст файлу зі скриптом script4.html. Приклад скріншоту 1

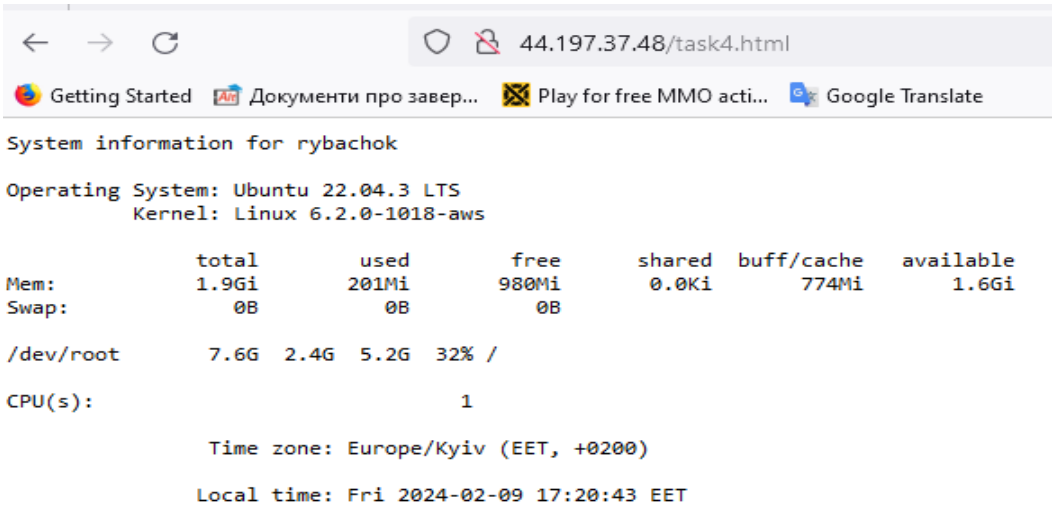


Рис. 4.6. Вміст файлу з результатом task4.html. Приклад скріншоту 2

8. Завершіть сеанс SSH, виконавши команду exit.

9. Завершіть роботу із середовищем AWS.

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку,
- Завдання;
- скріншоти 1, 2;
- висновки.

Питання для самоперевірки

1. Використання спецсимволів (екранування, лапки).
2. Використання операторів керування (послідовності).
3. Використання операторів керування (перенаправлення).
4. Використання змінних оточення.
5. Використання підстановки команд.

Література

1. Перетворення команд у скрипт // Електронний ресурс. Режим доступу: https://learning.lpi.org/uk/learning-materials/010-160/3/3.3/

ПРАКТИЧНЕ ЗАВДАННЯ 5.
НАПИСАННЯ ІНТЕРАКТИВНИХ BASH СКРИПТІВ

Мета роботи – набуття навичок із написання інтерактивних скриптів у командному рядку bash.

Завдання

Запустити ВМ Ubuntu AWS та під'єднатися до неї за SSH. Створити файл скрипта із трьома функціями.

Створити файл із результатами та передати його на розміщення у ВМ Ubuntu AWS. Оформити звіт та завершити роботу із середовищем.

Вказівки до виконання завдання

1. Запустіть ВМ Ubuntu AWS та під'єднайтеся до неї за SSH.
2. Створіть файл з функціями /home/ubuntu/script/script5.sh.
3. Зробіть функції доступними для всіх користувачів, зчитавши файл /home/ubuntu/script/script5.sh у /etc/profile.
4. Напишіть першу функцію (рис. 5.1):

- створює index.html файл, куди виводить список файлів у директорії і посилання на них, обрамляючи цей вміст html тегами;
- на початок списку файлів додається посилання на батьківську директорію.

```
ubuntu@rybachok:~$ cat index.html
<html><pre>
<li><a href=..>..</a>
<li><a href=index.html>index.html</a>
<li><a href=ls.html>ls.html</a>
<li><a href=result>result</a>
<li><a href=script>script</a>
</pre></html>
```

Рис. 5.1. Результат роботи функції 1

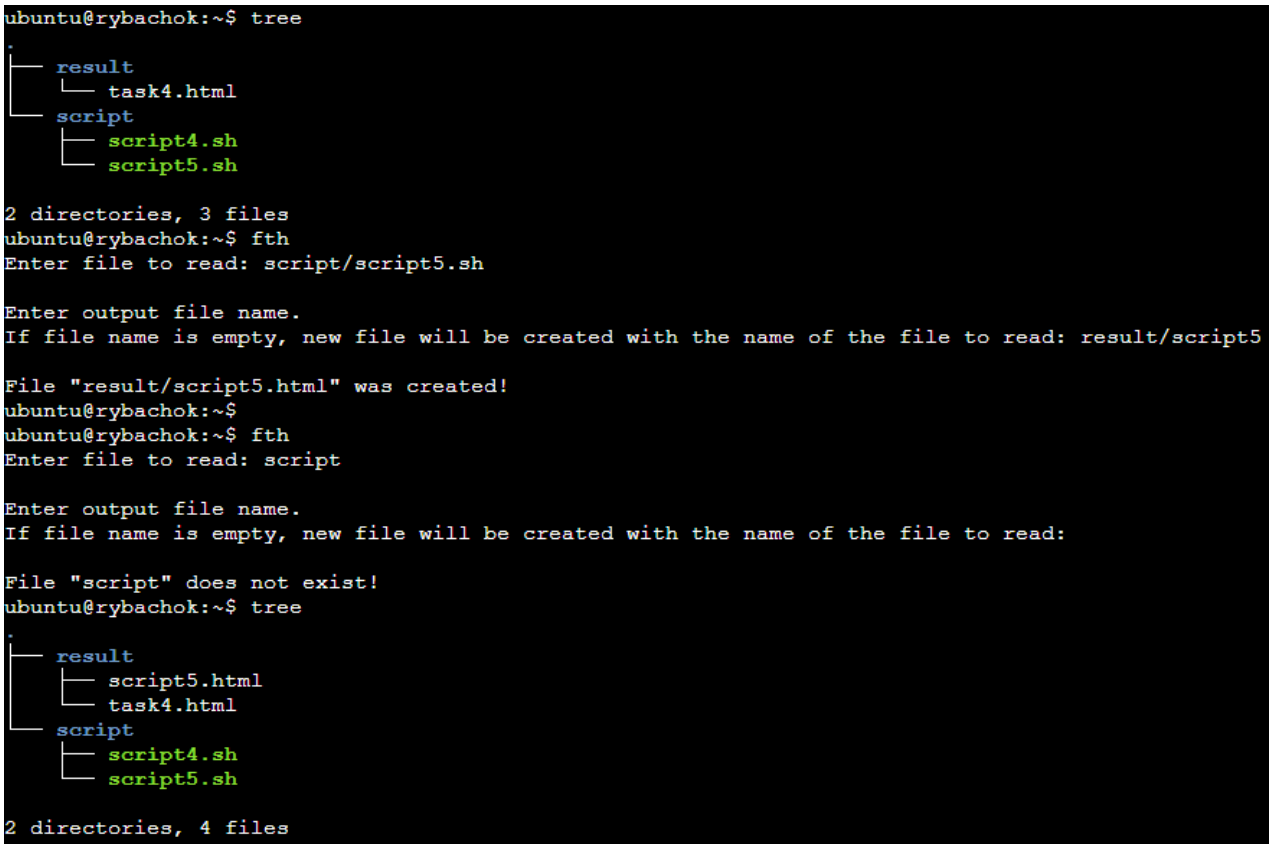
5. Напишіть другу функцію (рис. 5.2):

- обрамляє тегами вміст початкового файлу;
- формує файл із розширенням html, запитуючи у користувача ім'я результуючого файлу. Якщо ім'я файлу не задається, то використовується

ім'я початкового файлу (наприклад, task5.txt перетворюється в task5.txt.html);

- якщо початкового файлу не існує, то виводить помилку;
- при успішному виконанні функції виводиться повідомлення про створення відповідного файлу.

-



- Рис. 5.2. Виконання функції, яка перетворює файл у файл html (успішне виконання та помилка). Приклад скріншоту 1

6. Напишіть **третю** функцію (рис. 5.3):

- формує файл із розширенням html, куди записує результат виконання команди, яку вводить користувач;
- запитує ім'я кінцевого файлу. якщо ім'я не вказується, то в якості імені використовує команду (наприклад, ls перетворюється в ls.html);
- якщо команди не існує, то виводить помилку;
- при успішному виконанні функції виводиться повідомлення про створення відповідного файлу.

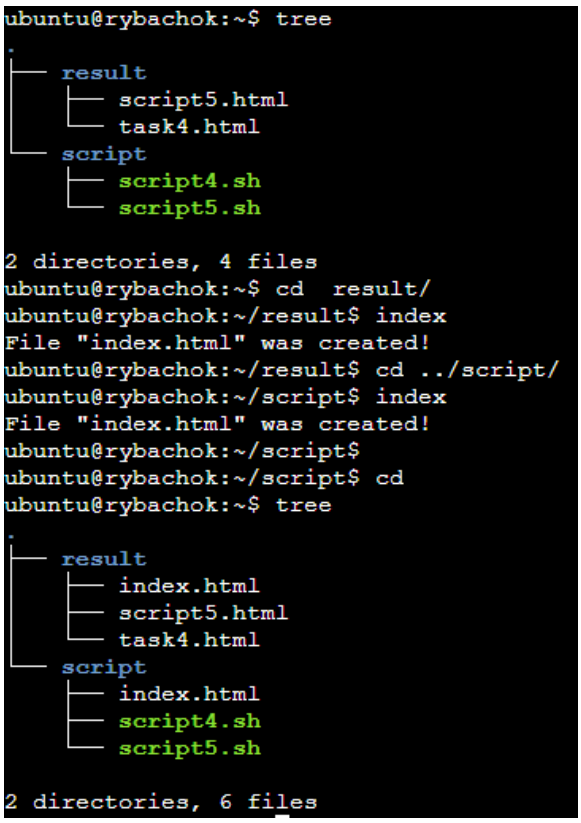


Рис. 5.3. Створення індексних файлів в директоріях result та script

7. За допомогою другої функції створити файл result/script5.html, що містить вміст файлу script/script5.sh. Зробити скріншот 1 виконання скрипта з успішним створенням файлу та помилкою.

9. За допомогою першої із функції створити індексні html файли в директоріях result та script, що містить перелік файлових об'єктів із посиланням на них .

10. Запишіть виведення команди ls -lR в домашньому каталозі користувача у файл html за допомогою третьої функції. Спробуйте виконати функцію із командою, яка не існує. Зробіть скріншот 2.

11. За допомогою першої функції створіть список файлових об'єктів домашньої директорії користувача ubuntu.

12. Зв'яжіть піддомен ubuntu із домашньою директорією користувача ubuntu, створивши символічне посилання та змінивши дозволи:

sudo ln -s /home/ubuntu /var/www/html/ubuntu

chmod o+rx /home/ubuntu

```
ubuntu@rybachok:~$ cth
Enter command: ls -lR

Enter file name. If file name is emply, new file will be created with the name of command.
Name:

File "ls.html" was created!
ubuntu@rybachok:~$ cth
Enter command: goto

Enter file name. If file name is emply, new file will be created with the name of command.
Name:
Command 'goto' not found, did you mean:
  command 'toto' from snap toto (giant-quarter)
  command 'goo' from deb goo (0.155+ds-4)
  command 'wgoto' from deb wily (0.13.41-10)
  command 'gyoto' from deb gyoto-bin (1.4.4-7build1)
  command 'gotox' from deb dvb-apps (1.1.1+rev1500-1.4)
See 'snap info <snapname>' for additional versions.
```

Рис. 5.4. Виконання функції, який записує результат виконання команди у файл html (успішне виконання та помилка). Приклад скріншоту 2

13. На головну сторінку вебсерверу додайте посилання на піддомен ubuntu (рис. 5.5).

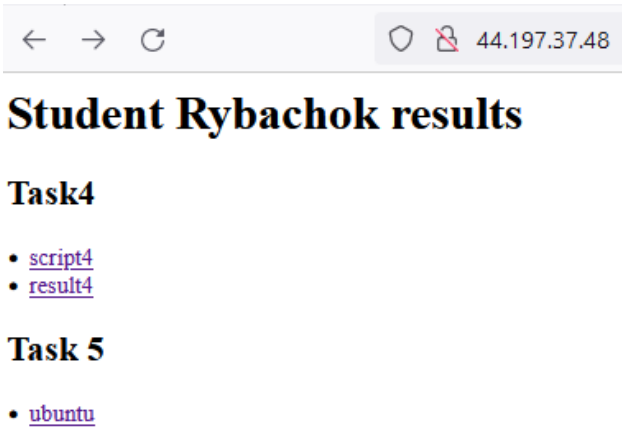


Рис. 5.6. Головна сторінка сервера

14. Перейдіть за посиланнями та зробіть скріншоти:

- головної сторінки піддомена ubuntu (рис. 5.7),
- файлу і списком файлових обєктів (рис. 5.8),
- файлу із функціями (рис. 5.9), всі функції мають бути видно.

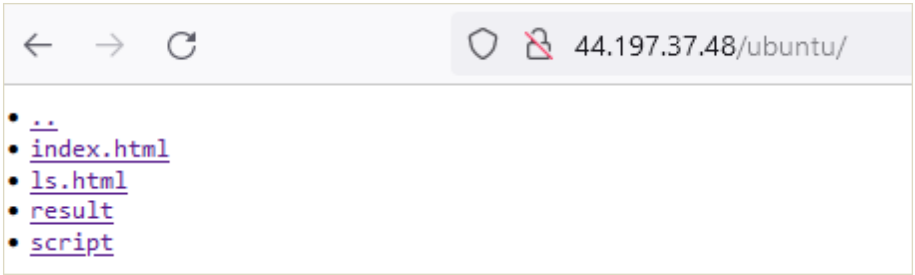


Рис. 5.7. Головна сторінка піддомена ubuntu. Приклад скріншоту 3

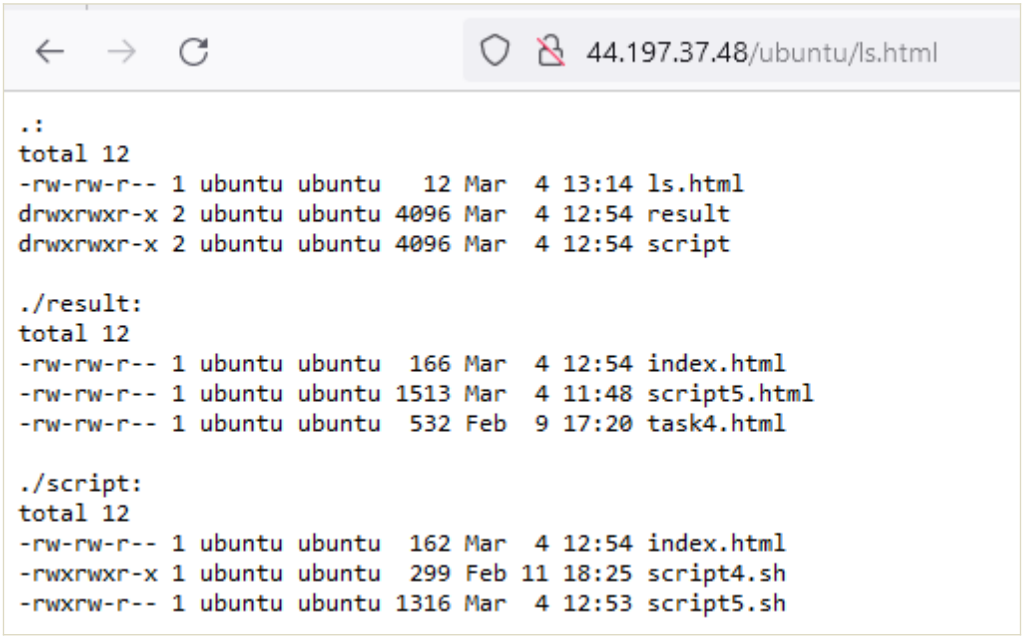


Рис. 5.8. Результат виконання третьої функції. Приклад скріншоту 4

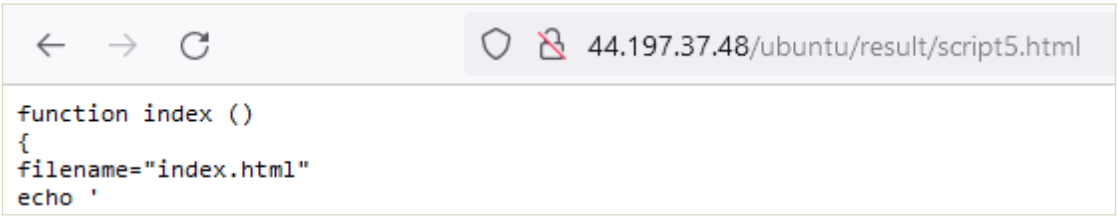


Рис. 5.9. Файл із функціями. Приклад скріншоту 5

15. Завершіть роботу із віртуальною машиною.

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку;
- завдання до лабораторної роботи;
- скріншоти 1-5;
- висновки.

Питання для самоперевірки

1. Які мають бути права на файл скрипта та що таке шебанг?

2. Які команди використовуються для читання введення від користувача?

3. Синтаксис та призначення команд if, for, while, case.

Література

1. Advanced Bash-Scripting Guide // Електронний ресурс. Режим доступу: https://tldp.org/LDP/abs/html/index.html

2. Bash scripting cheatsheet // Електронний ресурс. Режим доступу: https://devhints.io/bash

ПРАКТИЧНЕ ЗАВДАННЯ 6. ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ФАЙЛОВИХ ОБ'ЄКТІВ ТА ПРАВ ДОСТУПУ В ОС LINUX

Мета роботи - одержання практичних навичок роботи із файловою системою ОС Linux.

Завдання

У ВМ Ubuntu створити ресурс для підтримки навчального процесу. Структура (рис. 6.1):

drwxr-x--- teacher OS **/home/OS** - домашня директорія користувача teacher групи OS з правами 750

├── task

├── student

│ └── <lastname> (ваше прізвище латиницею)

└── share

drwxr-x--- teacher OS **task** - директорія із завданнями, містить файли 640 teacher OS (наповнити із файлу)

dr-xrwx--- teacher OS **student** - директорія містить домашні директорії студентів

drwxr-x--- lastname OS **<lastname>** - домашня директорія студента lastname, містить файли 640 **lastname** OS

drwxrwxrwt root root **share** - директорія містить файли користувачів

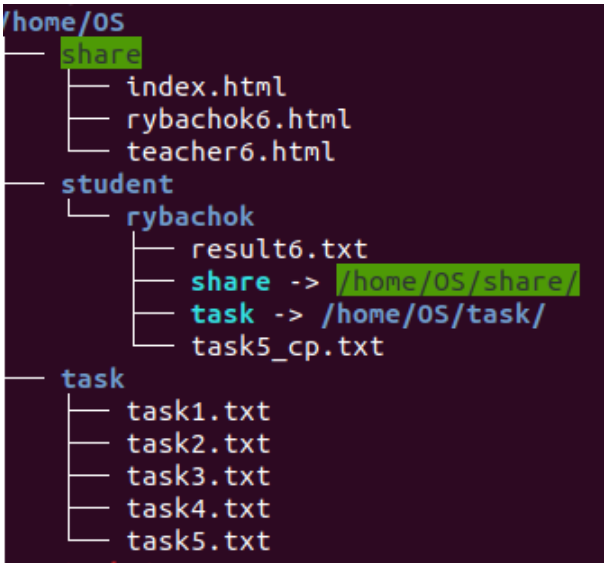


Рис. 6.1. Структура директорій

Вказівки до виконання завдання

1. Від імені root

1.1. Створіть групу OS:

groupadd OS

Перевірка: cat /etc/group – перегляд файлу існуючих груп

1.2. Створіть користувача teacher з групою OS та домашньою директорією:

useradd -m -g OS teacher

Перевірка: id teacher – перегляд облікового запису teacher

1.3. Перейменуйте домашню директорію в OS:

mv ~teacher /home/OS

або

mv /home/teacher /home/OS

Перевірка: tree /home

1.4. Внесіть зміни в файл /etc/passwd (замініть назву домашньої директорії користувача teacher на /home/OS оболонку на /bin/bash*)*

nano /etc/passwd

Ctlr+O, Ctrl+X, Ctr+S

Перевірка: рядок у файлі /etc/passwd повинен мати вигляд:

teacher:x:1001:1001::/home/OS:/bin/bash

1.5. Задайте пароль teacher

passwd teacher

1.6. В директорії OS створіть директорію share із правами доступу 1777 (всі користувачі мають право створювати, редагувати, видаляти директорії та файли, але тільки свої):

mkdir -m 1777 ~teacher/share

або

mkdir -m 1777 /home/OS/share

Перевірка: ls -l ~teacher

```
root@rybachok:~# ls -l  ~teacher/
total 4
drwxrwxrwt 2 root root 4096 Mar 22 09:02 share
```

2. Від імені користувача teacher в іншому терміналі наповніть директорію OS.

2.1. Відкрийте нову ssh сесію з основної ОС.

2.2. Відкрийте сесію від імені користувача teacher:

sudo login teacher

Переконайтеся, що директорія не містить файлів, створених по замовчуванню. При наявності їх необхідно видалити (крім прихованих, бо вони містять файли профілю).

ls -l

```
teacher@rybachok:~$ ls -l
total 4
drwxrwxrwt 2 root root 4096 Mar 22 09:02 share
```

2.3. Встановіть umask 027. Це дозволить при створенні нових директорій та файлів встановлювати права, які є інвертованими до маски (якщо маска 027, то права на директорії 777 - 027 =750, права на файли 666 - 027 = 640).

Перегляд поточної маски: **umask**

Встановлення нового значення: **umask 027**

2.4. Завантажте файл за посиланням та розпакуйте його (назву файлу потрібно екранувати одинарними лапками, оскільки використовується знак &).

Перед виконанням команди ще раз перевірте її правильність, бо редактори замінюють лапки!

wget --no-check-certificate 'https://docs.google.com/uc?export=download&id=1HaYwNpOJoDtj_3ohZeiyQi_s1POmM_KB' -O task.tar

tar -xf task.tar

Перевірка:

ls -l

tree

```
teacher@rybachok:~$ tar -xf task.tar
teacher@rybachok:~$ tree
.
├── share
├── task
│   ├── task1.txt
│   ├── task2.txt
│   ├── task3.txt
│   ├── task4.txt
│   └── task5.txt
└── task.tar

2 directories, 6 files
```

2.3. Перегляньте даємо права на файли, у разі необхідності змініть їх на 640 (chmod 640 task/*):

ls -lR

```
teacher@rybachok:~$ ls -lR
.:
total 20
drwxrwxrwt 2 root    root  4096 Mar 21 14:44 share
drwxr-x--- 2 teacher OS    4096 Mar 21 14:11 task
-rw-r----- 1 teacher OS   10240 Mar 21 14:47 task.tar

./share:
total 0

./task:
total 20
-rw-r----- 1 teacher OS 3422 Mar 21 14:07 task1.txt
-rw-r----- 1 teacher OS  235 Mar 21 14:08 task2.txt
-rw-r----- 1 teacher OS  517 Mar 21 14:09 task3.txt
-rw-r----- 1 teacher OS  410 Mar 21 14:10 task4.txt
-rw-r----- 1 teacher OS  365 Mar 21 14:10 task5.txt
```

2.4. Створіть директорію *student* з правами 570:

mkdir -m 570 student

3. Від імені root (в першому терміналі) створіть користувача <lastname>, де <lastname> - ваше прізвище латиницею.

3.1. Створіть користувача <lastname>, із базовою директорією /home/OS/student групою OS, власною директорією <lastname>:

useradd -b /home/OS/student -m -g OS <lastname>

Перевірка: id <lastname>

3.2 Встановіть оболонку по замовчуванню /bin/bash:

nano /etc/passwd

3.3. Задайте пароль:

passwd <lastname>

4. Від імені користувача <lastname> наповніть директорію.

4.1. Відкрийте нову (третю) SSH сесію з основної ОС.

4.2. Відкрийте сесію від імені користувача <lastname>:

sudo login <lastname>

Переконайтеся, що директорія не містить файлів, створених по замовчуванню. При наявності їх необхідно видалити, крім прихованих.

4.3. Змініть маску**:**

umask 027

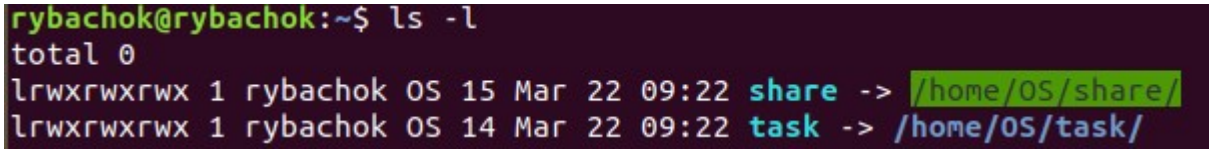
4.4. В домашній директорії створіть символічні посилання на директорії *task, share:*

ln -s /home/OS/task/ task

ln -s /home/OS/share/ share

Зверніть увагу:

- розмір такого файлу – довжина адреси відповідного файлового об’єкту;
- файл символічного посилання має права 777;
- спроба виконання операції над посиланням відповідає спробі виконання операції над відповідним об’єктом ФС, на який вказує це посилання.



4.4. Використовуючи створені символічні посилання, зробіть копію файлу task6.txt:

cp task/task6.txt task6_cp.txt

Якби ми не мали символічного посилання, довелося б використовувати повний шлях до файлу /home/OS/task/task6.txt. Отже, символічне посилання діє як псевдонім.

Зверніть увагу:

- власником файлу-копії є поточний користувач, права доступу до новоствореного файлу залежать від встановленої раніше маски.

```
rybachok@rybachok:~$ ls -l
total 4
lrwxrwxrwx 1 rybachok OS  15 Mar 21 15:06 share -> /home/OS/share/
lrwxrwxrwx 1 rybachok OS  14 Mar 21 15:06 task -> /home/OS/task/
-rw-r----- 1 rybachok OS 365 Mar 21 15:08 task5_cp.txt
```

4.5. Виконайте дозапис у файл task6_cp.txt:

whoami >> task6_cp.txt

4.6. Спробуйте виконати дозапис у файл task/task6.txt. Вам це не вдасться. Помилка виникає через те, що у вас немає прав на запис у файл.

4.7. Прочитайте довідку по команді diff. Порівняйте два файли task6_cp.txt та task/task6.txt. Відмінність запишіть у файл ~/result6.txt.

```
rybachok@rybachok:~$ cat result6.txt
Refresh the webpage and take a screenshot 1. File name webpag   Refresh the webpage and take a screenshot 1. File name webpag

Run the tree command and take screenshot 2 of the contents of   Run the tree command and take screenshot 2 of the contents of

https://learning.lpi.org/uk/learning-materials/010-160/         https://learning.lpi.org/uk/learning-materials/010-160/
rybachok                                                      <
```

4.7. Використовуючи написану у попередній роботі функцію, сформуйте <lastname>6.html файл у директорії share, який містить вміст файлу result6.txt, обрамлений html тегами.

5. Від імені користувача **teacher** в другому терміналі виконайте дії.

5.1. Спробуйте видалити файл share/<lastname>6.html

```
teacher@rybachok:~$ rm share/rybachok6.html
rm: remove write-protected regular file 'share/rybachok6.html'? y
rm: cannot remove 'share/rybachok6.html': Operation not permitted
```

Зверніть увагу, що використання біта-липучки не дозволяє видаляти чужі файли із директорії;

5.2. Виконайте функцію, яка виводить у html файл результати виконання команди ls –lR /home/OS (рис. 6.1):

5.3. Виконайте функцію, який в файл share/index.html виводить список файлових об’єктів /home/OS і посилання на них (рис. 6.2).

6. Від імені користувача root створіть піддомен OS_share на основі директорії /home/OS/share.

6.1. Створіть символічний зв’язок та надайте права на директорії, що входять в шлях для перегляду іншим користувачам:

sudo ln -s /home/OS/share /var/www/html/OS_share

chmod o+x /home/OS

6.2. Надамо права на файли, які будуть видно на сервері, для перегляду іншим користувачам:

chmod o+r /home/OS/share/*

8. Заверште сеанси всіх користувачів командою **exit.**

9. Для оформлення звіту зробіть 4 скріншоти:

- головної сторінку серверу;
- головної сторінки піддомену OS;
- вмісту файлу ls.html
- вмісту файлу <lastname>6.html

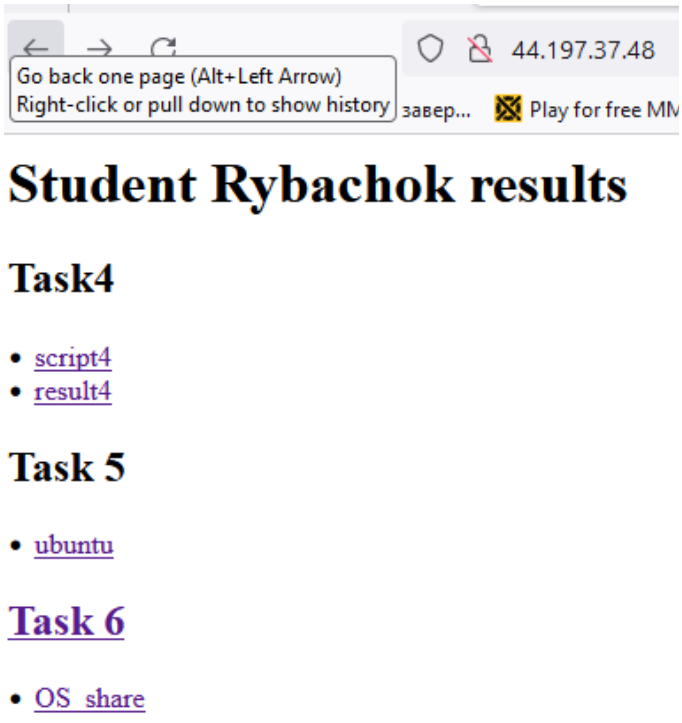


Рис. 6.1. Головна сторінка серверу. Приклад скріншоту 1

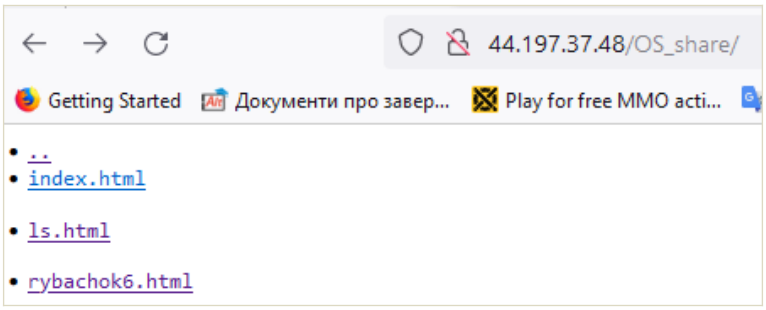


Рис. 6.2. Головна сторінка піддомену OS. Приклад скріншоту 2

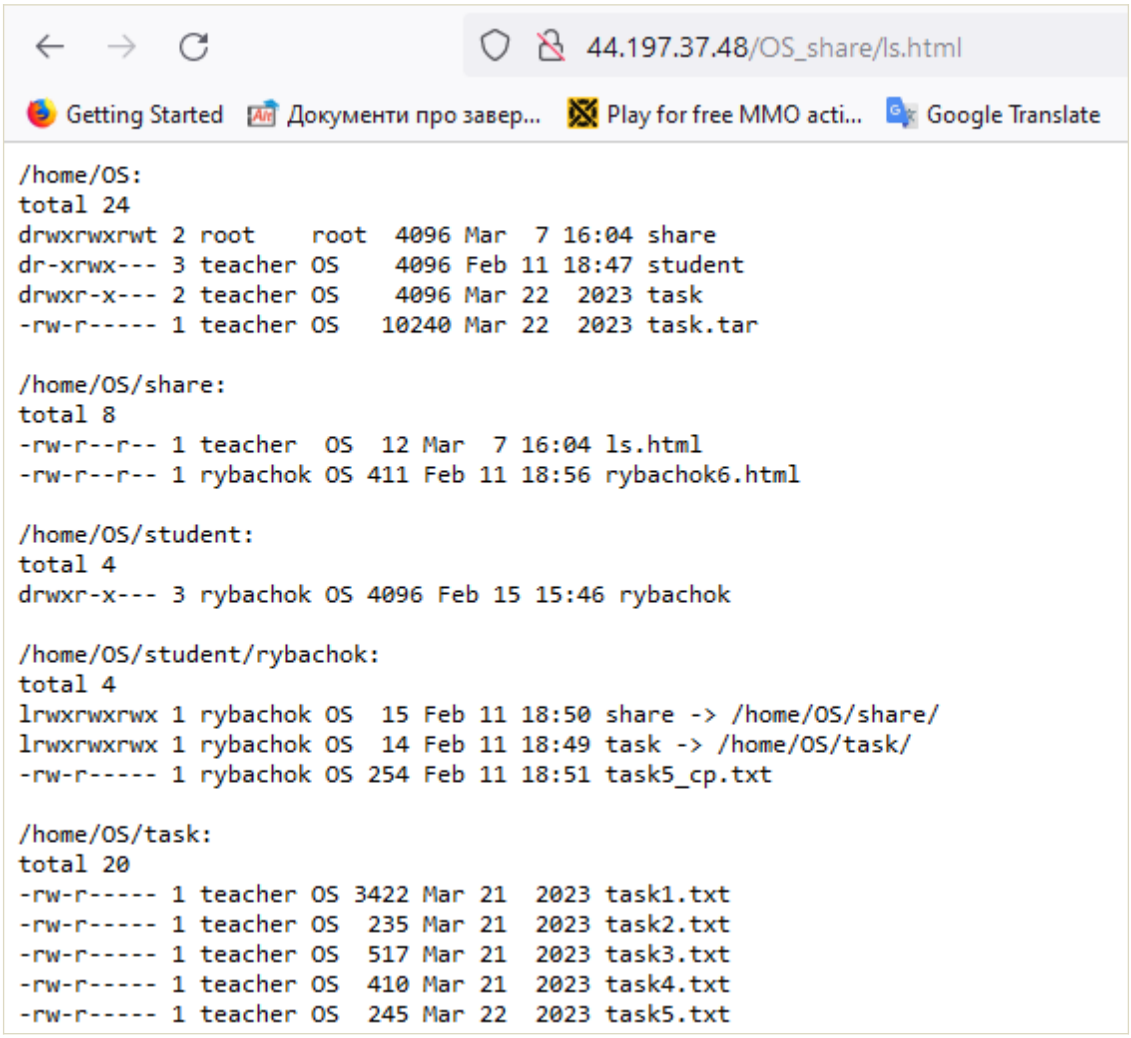


Рис. 6.3. Вміст файлу ls.html. Приклад скрішоту 3

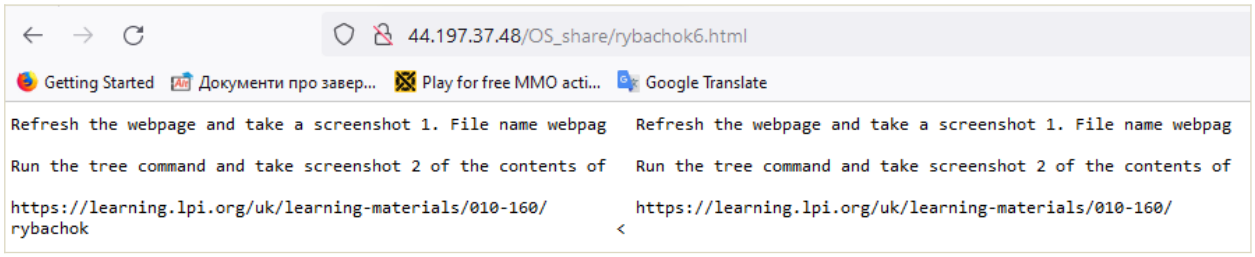


Рис. 6.4. Вміст файлу <lastname>6.html. Приклад скріншоту 4

11. Завершіть роботу із середовищем AWS.

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку;
- завдання до лабораторної роботи;
- скріншоти 1-4;
- висновки.

Питання для самоперевірки

1. Права доступу до файлів.
2. Використання додаткових бітів S, T.
3. Використання жорсткх посилань.
4. Використання додаткових атрибутів файлів.

Література

1. Використання папок та перегляд списку файлів // Електронний ресурс. Режим доступу: https://learning.lpi.org/uk/learning-materials/010-160/2/2.3/

2. Створення, переміщення та видалення файлів // Електронний ресурс. Режим доступу: https://learning.lpi.org/uk/learning-materials/010-160/2/2.4/

ПРАКТИЧНЕ ЗАВДАННЯ 7.

НАДАННЯ ДОСТУПУ ЗА SSH КОРИСТУВАЧАМ В ОС LINUX

Мета роботи - одержання практичних навичок роботи із файловою системою ОС Linux та протоколом SSH.

Завдання

У ВМ Xubuntu згенерувати 2 набори ключів для користувачів teacher, <lastname> Налаштувати доступ за ключами для користувачів teacher, <lastname> із ВМ Xubuntu у ВМ Ubuntu AWS.

Налаштувати SSH доступ із основної ОС до ВМ Xubuntu з використанням ключів.

Вказівки до виконання завдання

1. Налаштування доступу за ключами користувачів teacher, <lastname> у ВМ Ubuntu.

1.1. У ВМ Xubuntu, використовуючи команду ssh-keygen, згенеруйте 2 пари ключів для користувачів teacher, <lastname> (залиште парольну фразу пустою, просто натисніть Enter):

ssh-keygen -t rsa -f <username> <username>

<username> =teacher, <lastname>

Буде згенеровано 2 файли:

.pub – public key ;

<username> - private key .

1.2. Використовуючи команду scp, передайте на сервер у директорію ~ubuntu/.ssh створені публічні ключі:

scp -i labsuser.pem <username>.pub ubuntu@Public_IPv4:~/.ssh/

<username> =teacher, <lastname>

1.3. У ВМ Ubuntu від імені основного користувача ubuntu, використовуючи sudo та mkdir створити 2 директорії ~/.ssh для teacher, <lastname>. Зверніть увагу, що назва директорії починається з крапки, тому вона є прихованою.

1.4. Використовуючи команди chmod, chown, змініть:

- права доступу до обох директорій на 711;

- власника директорії на <username>:OS.

Перевірка:

sudo ls -la ~<username>

sudo ls -ld ~<username>/.ssh

```
ubuntu@rybachok:~$ sudo ls -ld ~teacher/.ssh
drwx--x--x 2 teacher OS 4096 Mar 28 21:22 /home/OS/.ssh
```

1.5. Використовуючи команду mv, перемістіть для teacher, <lastname> pub-ключі в папку ~<username>/.ssh.

1.6. Використовуючи команди chmod, chown, mv змініть для файлів публічних ключів:

- права на 600;

- власника файлу на <username>:OS;

- назву файлу на ~<username>/.ssh/authorized_keys.

Перевірка:

sudo ls -l ~<username>/.ssh

```
ubuntu@rybachok:~$ sudo ls -l ~teacher/.ssh
total 4
-rw------- 2 teacher OS 390 Mar 28 21:14 authorized_keys
```

1.7. Додайте користувача teacher до групи sudo:

sudo usermod -G -a sudo teacher

1.8. У віртуальній машині Xubuntu спочатку від імені користувачів teacher, потім від імені користувача <lastname> виконайте кроки 1.8.1-1.8.3.

1.8.1. Використовуючи команду ssh, приєднайтеся за приватним ключем. Зробіть скріншот 1 та скріншот 2.

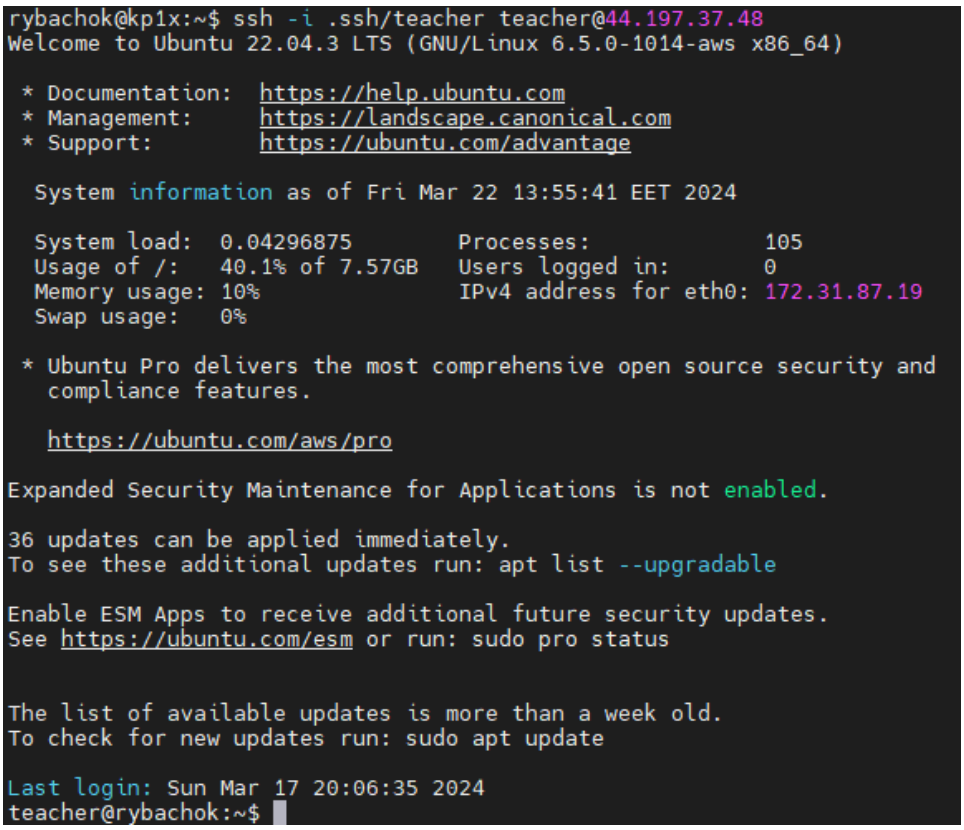


Рис.7.1. SSH сесія для користувача teacher ВМ Ubuntu. Приклад скріншоту 1

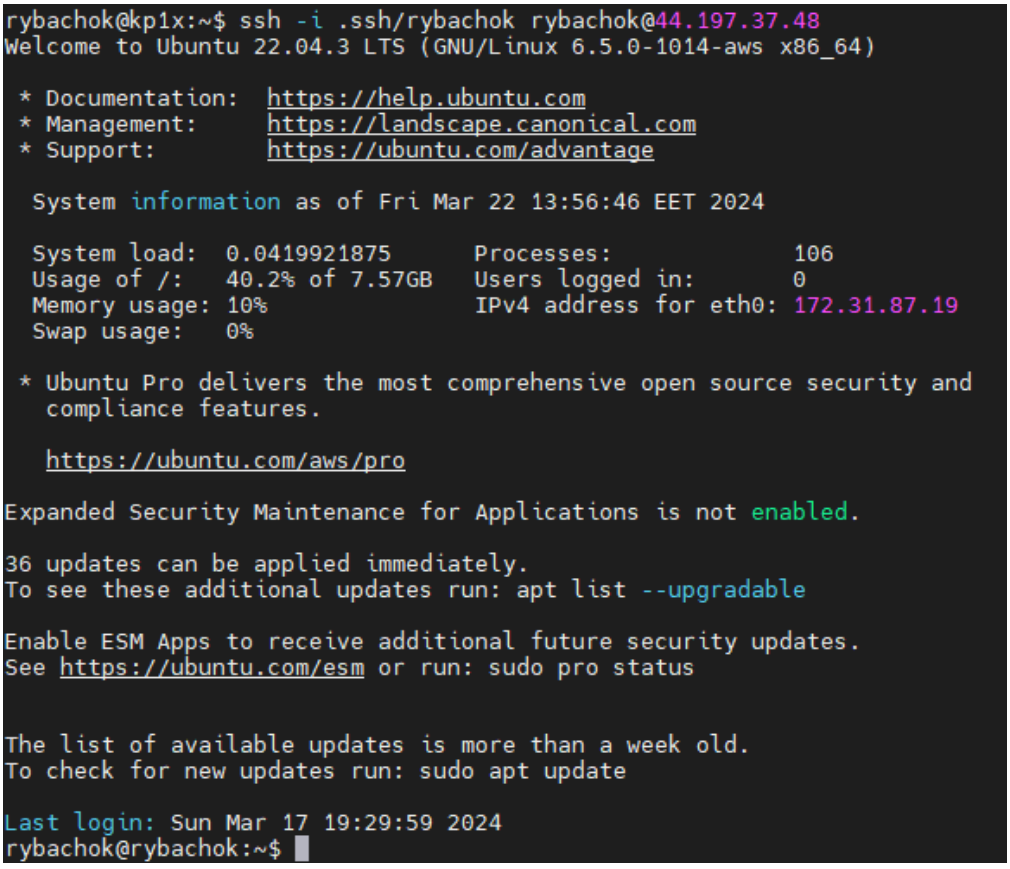


Рис.7.2. SSH сесія для користувача <lastname> ВМ Ubuntu. Приклад скріншоту 2

1.8.2. Використовуючи команду mkdir, створіть директорію ~<username>/.bak з правами 751.

1.8.3. Використовуючи команду ln, створіть жорсткий зв'язок на файл ~<username>/.ssh/authorized_keys із іменем ~<username>/.bak/authorized_keys.bak для обох користувачів.

Перевірка:

ls -l .bak

Властивості файлу мають показати наявність 2 жорстких зв'язків (2 поле в ярлику файла).

```
teacher@rybachok:~$ ls -l .bak
total 4
-rw------- 2 teacher OS 390 Mar 28 21:14 authorized_keys.bak
```

1.9. Підготовка звіту. Від імені користувача teacher виконайте дії.

1.9.1. Використовуючи команду

ls -li .bak <lastname>/.bak

створіть файл share/task7, який містить вміст директорії .bak (перенаправити вивід команди). Створіть файл share/task7.html, який містить вміст файлу share/task7, обрамлений тегами.

1.9.2. Оновіть файл share/index.html.

1.9.3. Змініть файл /var/www/html//index.html, розмістивши посилання на файл share/task7.html.

Task 7

- task7.html

1.9.4. Перегляньте файл share/task7.html.Зробити скріншот 3.

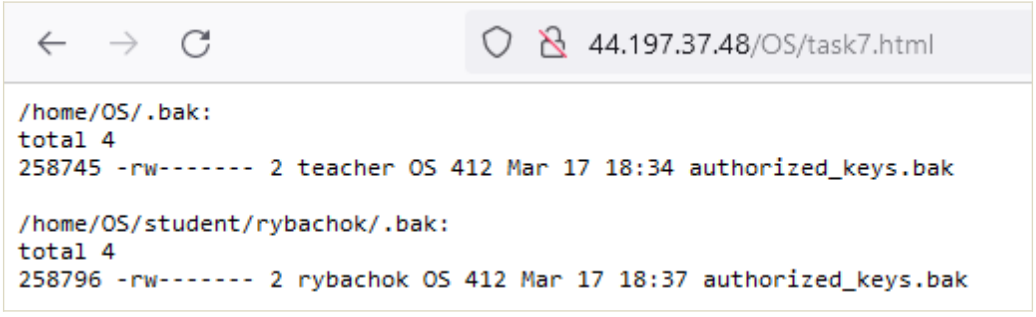


Рис. 7.3. Файл із результатами завдання ВМ Ubuntu. Приклад скріншоту 3

1.10. Закрийте сеанси всіх користувачів командою exit та завершіть роботу із середовищем.

2. Налаштування доступу за SSH ключами у ВМ Xubuntu

2.1. У основній ОС:

- за допомогою команди ssh-keygen згенеруйте ключ з іменем xubuntu;

- перевірте, що права на приватний ключ мають значення 400;

- за допомогою команди scp передайте публічний ключ у ~/.ssh директорію користувача та перейменувати його у authorized_keys.

2.2. У ВМ Xubuntu виконати наступні дії:

- За допомогою команди chmod встановіть права на файл authorized_keys 600.

- Внесіть правки у файл /etc/ssh/sshd_config:

PubkeyAuthentication yes

PasswordAuthentication no

- Перечитайте конфігурацію сервісу sshd:

sudo systemctl reload sshd

- Створіть директорію ~/.bak .

- Зробіть жорсткі копії файлів приватних ключів teacher, <lastname>, labsuser.pem та файлу публічного ключа authorized_keys в директорію ~/.bak з іменами *.bak.

- Перегляньте вміст директорії ~/.bak та зробіть скріншот 4.

```
rybachok@kp1x:~$ ls -li .bak
total 16
524435 -rw------- 2 rybachok rybachok 1426 бер 22 13:47 authorized_keys.bak
524365 -r-------- 2 rybachok rybachok 1674 лют  7 15:38 labsuser.pem.bak
524479 -r-------- 2 rybachok rybachok 1679 бер 22 13:54 rybachok.bak
524476 -r-------- 2 rybachok rybachok 1675 бер 22 13:53 teacher.bak
```

Рис. 7.4. Вміст папки із бекапами на ВМ Xubuntu. Приклад скріншоту 4

3.2. Завершіть сеанс користувача та вимкніть віртуальну машину.

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку;

- завдання до лабораторної роботи;
- скріншоти 1-4;
- висновки.

Питання для самоперевірки

1. Синтаксис команди ssh-keygen.
2. Права файлів приватних та публічних ключів SSH та їх розташування.
3. Головний конфігурційний файл SSH.
4. Властивості жорстких посилань.

Література

1. openssh.com // Електронний ресурс. Режим доступу: https://www.openssh.com/

ПРАКТИЧНЕ ЗАВДАННЯ 8.

ВІДНОВЛЕННЯ ЗАВАНТАЖУВАНОСТІ ВМ ІЗ ОС XUBUNTU

Мета роботи - одержання практичних навичок відновлення завантажуваності ОС Linux.

Завдання

Виконати пошкодження, а потім відновлення першого сектору диску з бекапа. Виконати пошкодження, а потім відновлення GRUB2 з LiveCD. Виконати запуск ОС через команди консолі GRUB. Виконати пошкодження, а потім відновлення файлу /etc/fstab. Виконати відновлення налаштування GRUB.

Підготовка до виконання завдання

1. Створіть знімок стану ВМ Xubuntu.

2. Приєднайте до ВМ iso-образ диску, з якого встановлено ОС.

3. Увімкніть ВМ.

Вказівки до виконання завдання

1. Відновлення першого сектору диску з бекапа

1.1. Створіть бекап першого сектору завантажувального диску:

sudo dd if=/dev/sda of=~/.bak/first.bak bs=512 count=1

1.2. Пошкодьте перший сектор завантажувального диску:

sudo dd if=/dev/zero of=/dev/sda bs=440 count=1

1.3. Перезавантажтеся:

sudo reboot

Система не завантажиться. Завантажтеся із iso-образу (оберіть Try Xubuntu).

1.4. В Терміналі виконайте команди відновлення першого сектору із бекап файлу:

sudo mount /dev/sda3 /mnt

sudo dd if=/mnt/home/<lastname>/.bak/first.bak of=/dev/sda conv=notrunc

sudo umount /mnt

Зробіть скріншот 1.

```
xubuntu@xubuntu:~$ sudo mount /dev/sda3 /mnt
xubuntu@xubuntu:~$ sudo dd if=/mnt/home/rybachok/.bak/first.bak of=/dev/sda conv=notrunc
1+0 records in
1+0 records out
512 bytes copied, 0.00691176 s, 74.1 kB/s
xubuntu@xubuntu:~$ sudo umount /mnt
```

Рис. 8.1. Відновлення першого сектору диску із бекапу. Приклад скріншоту 1

1.5. Перезавантажтеся.

2. Відновлення GRUB2 з LiveCD (chroot)

2.1. Пошкодьте перший сектор завантажувального диску:

sudo dd if=/dev/zero of=/dev/sda bs=440 count=1

2.2. Перезавантажтеся. Система не завантажиться.

2.3. Завантажтеся із iso-образу.

2.4. В Терміналі виконайте команди відновлення:

- підмонтуйте кореневий розділ та тимчасові файлові системи:

sudo -i

mount /dev/sda3 /mnt

mount --bind /dev /mnt/dev

mount --bind /proc /mnt/proc

mount --bind /sys /mnt/sys

- змініть кореневу директорію на директорію /mnt.

chroot /mnt

- перевстановіть Grub на диск /dev/sda:

grub-install /dev/sda

(використайте опцію –recheck, якщо виникла помилка)

ls -l /home

- зробіть скріншот 2.

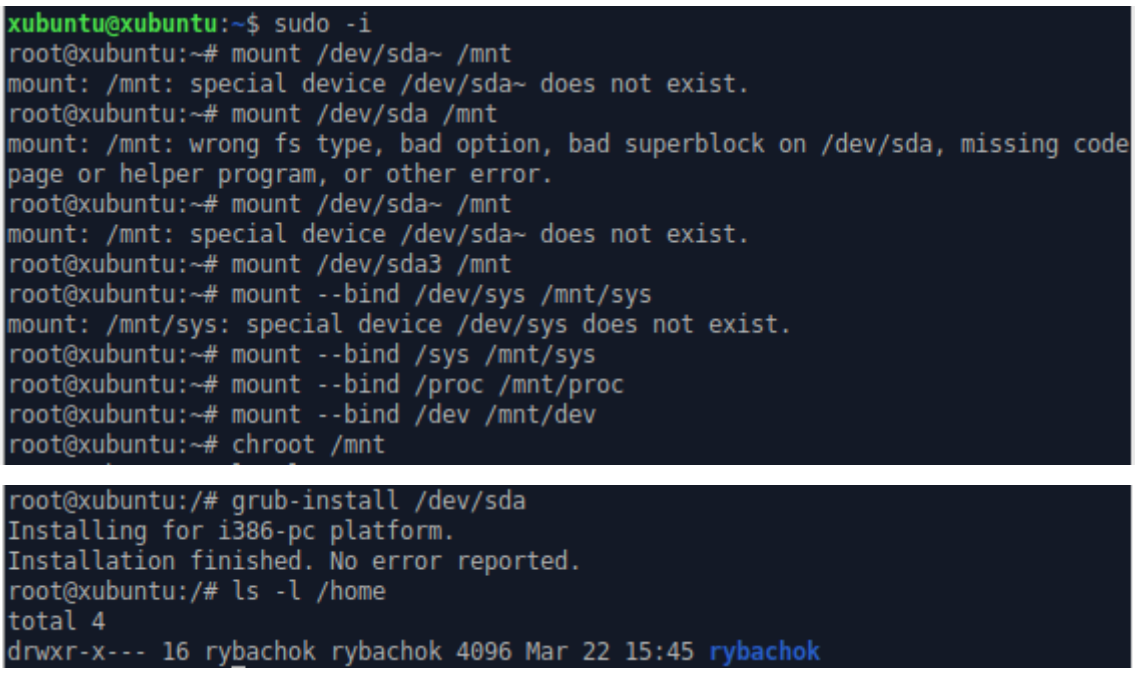


Рис. 8.2. Перевстановлення Grub. Приклад скріншоту 2

- заверште сеанс root командою exit.

- відмонтуйте раніше монтовані ФС та перезавантажтеся:

umount /mnt/dev

umount /mnt/proc

umount /mnt/sys

umount /mnt

sudo reboot

3. Запуск ОС через команди консолі GRUB

3.1. Виконайте правку налаштувань Grub:

sudo nano /etc/default/grub

GRUB_TIMEOUT=-1

sudo grub-mkconfig -o /boot/grub/grub.cfg

sudo reboot

3.2. Перезавантажтеся і виконайте вхід в консоль (для входу використайте клавішу c).

3.3. Перегляньте доступні команди та пристрої:

help

ls

3.4. Знайдіть пристрій на якому розташовано конфігурацію Grub:

search -f /boot/grub/grub.cfg

(результат hd0,gpt3)

3.5. Встановіть цей пристрій як кореневий:

set root=(hd0,3)

ls /home

ls -l /boot

Зробіть скріншот 3.

```
grub> ls
(proc) (hd0) (hd0,gpt3) (hd0,gpt2) (hd0,gpt1)
grub> set root=(hd0,3)
grub> ls -l /home
DIR          20240322125340 rybachok/

grub> ls -l /boot
DIR          20230911102640 efi/
DIR          20240322130554 grub/
7963097      20230713132242 System.map-6.2.0-26-generic
275465       20230713132242 config-6.2.0-26-generic
13791304     20230911103846 vmlinuz
76427371     20230911102704 initrd.img.old
182800       20220206203543 memtest86+.bin
184476       20220206203543 memtest86+.elf
184980       20220206203543 memtest86+_multiboot.bin
69436381     20230911103846 initrd.img
13770312     20230807153612 vmlinuz-6.2.0-26-generic
13791304     20230818094010 vmlinuz-6.2.0-32-generic
76427371     20230911103705 initrd.img-6.2.0-26-generic
275587       20230818093855 config-6.2.0-32-generic
7969006      20230818093855 System.map-6.2.0-32-generic
13770312     20230911103846 vmlinuz.old
69436381     20230925140509 initrd.img-6.2.0-32-generic

grub> _
```

Рис. 8.3. Робота в консолі Grub. Приклад скріншоту 3

3.6. Розмістіть ядро ОС, початковий диск в пам'ять та виконайте команду завантаження ОС:

linux /boot/vmlinuz-6.2.0-32-generic root=/dev/sda3

(6.2.0-32-generic – версія ядра ОС)

initrd /boot/initrd.img-6.2.0-32-generic

boot

4. Відновлення файлу /etc/fstab

4.1. Зробіть бекап файлу /etc/fstab в директорію ~.bak:

cp /etc/fstab ~/.bak/fstab.bak

4.2. Встановіть невірний UUID для розділу, що монтується в /boot/efi (наприклад, вкажіть пустий UUID=):

sudo nano /etc/fstab

4.3. Перезавантажтеся:

sudo reboot

4.4. Через помилку у файлі /etc/fstab система має не завантажитися, необхідно ввести пароль і працювати в консолі.

4.5. Перевірте, чи монтовано розділ /boot/efi:

mount | grep boot

4.6. Відновіть /etc/fstab:

cp /home/<lastname>/.bak/fstab.bak /etc/fstab

4.7. Виконайте монтування:

mount /boot/efi

Зробіть скріншот 4.

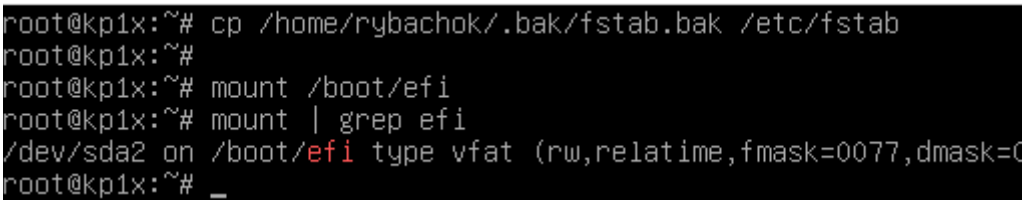


Рис. 8.4. Відновлення файлу /etc/fstab. Приклад скріншоту 4

4.8. Перезавантажтеся:

reboot

5. Виконайте відновлення налаштування GRUB:

sudo nano /etc/default/grub

GRUB_TIMEOUT=0

sudo grub-mkconfig -o /boot/grub/grub.cfg

sudo reboot

6. Вимкніть ВМ.

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку;
- завдання до лабораторної роботи;
- скріншоти 1-4;
- висновки.

Питання для самоперевірки

1. Синтаксис утиліти dd.
2. Послідовність дій при відновленні першого сектору із бекап файлу.
3. Послідовність дій при відновленні GRUB2 з LiveCD.
4. Послідовність дій при запуску ОС через команди консолі GRUB.
5. Послідовність дій при відновленні файлу /etc/fstab із консолі.

Література

1. GNU GRUB Manual 2.12 // Електронний ресурс. Режим доступу: https://www.gnu.org/software/grub/manual/grub/html_node/index.html

ПРАКТИЧНЕ ЗАВДАННЯ 9.
УПРАВЛІННЯ ПРОЦЕСАМИ І ЗАВДАННЯМИ В ОБОЛОНЦІ BASH

Мета роботи: — одержання практичних навичок створення, моніторингу, зміни пріоритетів процесів і завдань та надсилання їм сигналів в оболонці bash.

Завдання

Виконати спостереження за процесами та побудову ієрархії процесів. Створити фонові процеси та змінити їх пріоритет. Виконати моніторинг процесів, надсилання сигналів, зміну пріоритетів з допомогою команди top.

Вказівки до виконання завдання

1. Запустіть ВМ Ubuntu AWS. Приєднайтеся за SSH.

2. Виконайте спостереження за процесами та побудову ієрархії процесів.

2.1. Відкрийте сесію від імені користувача із вашим прізвищем, запустіть додатково 4 рази інтерпретатор bash.

2.2. Запишіть у файл результатів share/ps.txt логін користувача, PID поточної оболонки (див. рис. 9.3).

Для визначення *PID* поточного процесу використовується змінна середовища $.

2.3. Перегляньте список процесів вашого користувача у повному форматі і з використанням опції forest, допишіть їх у файл ps.txt (див. рис. 9.3).

2.4. Через команду ps та поля PID та PPID простежте всю ієрархію процесів поточної оболонки. Побудуйте дерево процесів, які визначені у попередньому пункті. Результат виконання допишіть в файл share/ps.txt.

Для виконання цього завдання необхідно використовувати опції –p для вказування PID процесу, який нас цікавить, та –o для вказування стовпчиків, які необхідно вивести (рис. 9.1).

```
rybachok@rybachok:~$ ps -p 12243  -o pid,ppid,cmd
    PID    PPID CMD
  12243   12236 bash
rybachok@rybachok:~$ ps -p 12236  -o pid,ppid,cmd
    PID    PPID CMD
  12236   12229 bash
rybachok@rybachok:~$ ps -p 12229  -o pid,ppid,cmd
    PID    PPID CMD
  12229   12222 bash
rybachok@rybachok:~$ ps -p 12222  -o pid,ppid,cmd
    PID    PPID CMD
  12222   12203 bash
rybachok@rybachok:~$ ps -p 12203  -o pid,ppid,cmd
    PID    PPID CMD
  12203   12149 -bash
rybachok@rybachok:~$ ps -p 12149  -o pid,ppid,cmd
    PID    PPID CMD
  12149   12148 login
rybachok@rybachok:~$ ps -p 12148  -o pid,ppid,cmd
    PID    PPID CMD
  12148   12147 sudo login rybachok
rybachok@rybachok:~$ ps -p 12147  -o pid,ppid,cmd
    PID    PPID CMD
  12147   12132 sudo login rybachok
rybachok@rybachok:~$ ps -p 12132  -o pid,ppid,cmd
    PID    PPID CMD
  12132   12131 -bash
rybachok@rybachok:~$ ps -p 12131  -o pid,ppid,cmd
    PID    PPID CMD
  12131   12045 sshd: ubuntu@pts/0
rybachok@rybachok:~$ ps -p 12045  -o pid,ppid,cmd
    PID    PPID CMD
  12045     594 sshd: ubuntu [priv]
rybachok@rybachok:~$ ps -p 594  -o pid,ppid,cmd
    PID    PPID CMD
    594       1 sshd: /usr/sbin/sshd -D -o AuthorizedKeysCommand
rybachok@rybachok:~$ ps -p 1  -o pid,ppid,cmd
    PID    PPID CMD
      1       0 /sbin/init
```

Рис.9.1. Перегляд процесів

2.5. Побудуйте дерево процесів, які визначено у попередньому пункті, та розмістіть його у файл звіту share/ps.txt.

```
rybachok@rybachok:~$ ps -p 1,594,12045,12131,12132,12147,12149,12203,12222,12229,12236,12243 -f --forest
UID          PID    PPID  C STIME TTY          TIME CMD
root       12149   12148  0 20:19 pts/1    00:00:00 login
rybachok   12203   12149  0 20:19 pts/1    00:00:00  \_ -bash
rybachok   12222   12203  0 20:20 pts/1    00:00:00      \_ bash
rybachok   12229   12222  0 20:20 pts/1    00:00:00          \_ bash
rybachok   12236   12229  0 20:20 pts/1    00:00:00              \_ bash
rybachok   12243   12236  0 20:20 pts/1    00:00:00                  \_ bash
root           1       0  0 18:06 ?        00:00:05 /sbin/init
root         594       1  0 18:06 ?        00:00:00 sshd: /usr/sbin/sshd -D -o AuthorizedKeysCommand /usr/s
root       12045     594  0 20:18 ?        00:00:00  \_ sshd: ubuntu [priv]
ubuntu     12131   12045  0 20:18 ?        00:00:00      \_ sshd: ubuntu@pts/0
ubuntu     12132   12131  0 20:18 pts/0    00:00:00          \_ -bash
root       12147   12132  0 20:19 pts/0    00:00:00              \_ sudo login rybachok
```

Рис.9.1. Побудова дерева процесів

2.6. Виведіть список процесів у вигляді дерева (команда pstree) та допишіть у файл share/ps.txt.

2.7. Перегляньте файл у браузері. Зробіть скріншот 1.

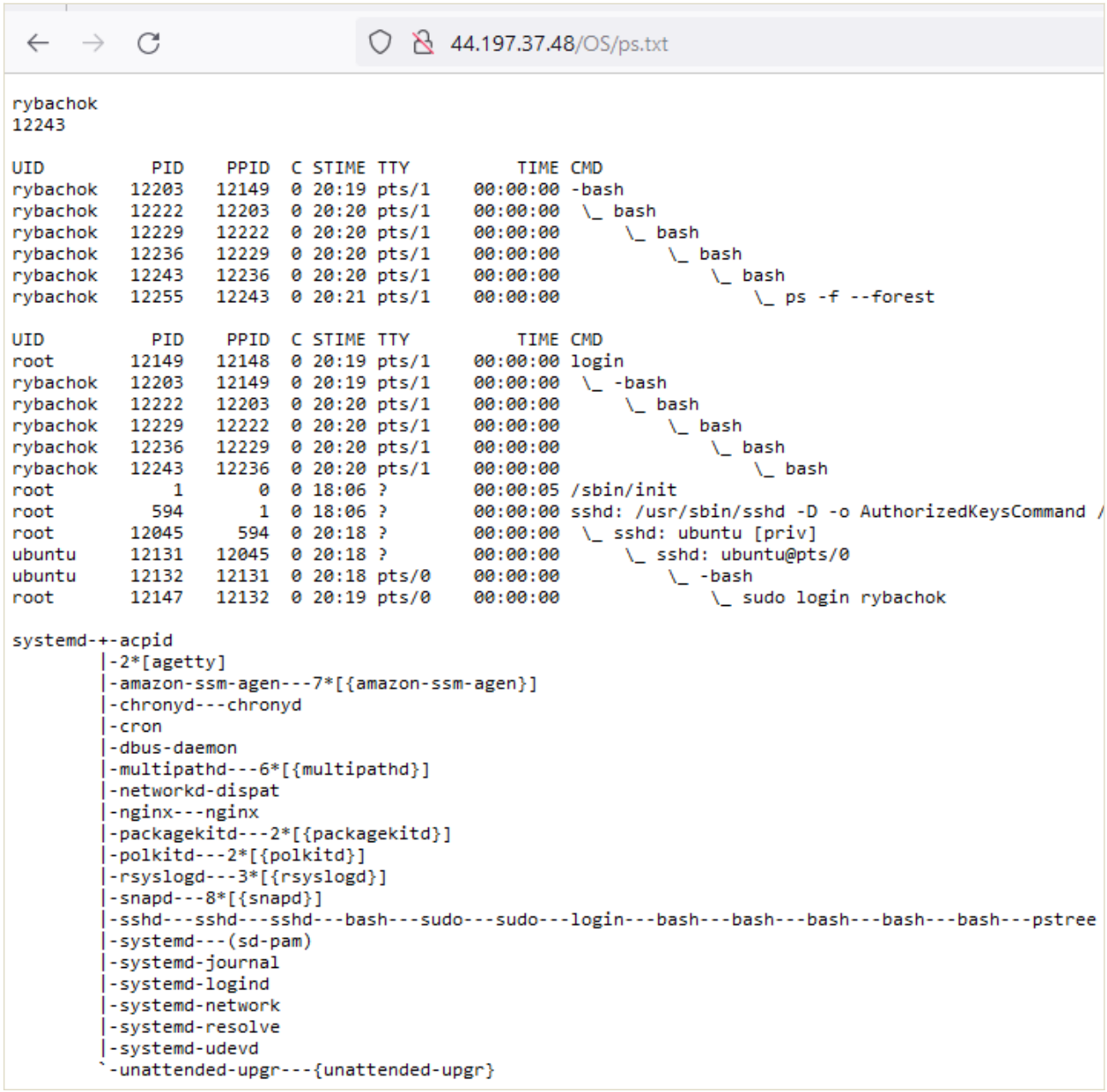


Рис.9.3. Файл результатів share/ps.txt. Приклад скріншоту 1

2. Керування фоновими процесами та наданням процесам пріоритету

Від імені користувача teacher

2.1. Запустіть у фоні виконання 3 завдань із вказаними пріоритетами:

- yes fg (пріоритет 10);
- yes bg (пріоритет 10);
- yes nice (пріоритет 0).

2.1.1. Запустіть три фонові завдання.

- Запустіть команду, яка буде працювати «вічно» та перенаправте її виведення у файл поглинач:

```
teacher@rybachok:~$ yes bg  >  /dev/null
^Z
```

- Зупиніть виконання команди, натиснувши поєднання клавіш Ctrl + Z — призупинення виконання процесу.

```
^Z
[1]+  Stopped                 yes bg > /dev/null
```

- Продовжіть виконання цієї команди в фоновому режимі:

```
teacher@rybachok:~$ bg
[1]+ yes bg > /dev/null &
```

З’явиться напис на зразок наступного: [1] (в квадратних дужках вказано номер завдання).

- Перегляньте пріоритет процесу (атрибут NI):

```
teacher@rybachok:~$ ps -C yes -l -f
F S UID          PID    PPID  C PRI  NI ADDR SZ WCHAN  STIME TTY          TIME CMD
0 R teacher    12976   12956 46  80   0 -  1547 -      20:54 pts/2    00:00:38 yes bg
```

- Переконайтеся за допомогою команди jobs, що в фоні працює одна задача:

```
teacher@rybachok:~$ jobs
[1]+  Running                 yes bg > /dev/null &
```

- Запустіть ще одну задачу з пріоритетом 0:

```
teacher@rybachok:~$ yes bg > /dev/null &
[2] 12988
```

- За допомогою команди nice запустіть ще один фоновий процес з пріоритетом по замовчуванню (10):

```
teacher@rybachok:~$ nice yes nice >  /dev/null &
[3] 12991
```

Перевірка:

```
teacher@rybachok:~$ ps -C yes -l -f
F S UID          PID    PPID  C PRI  NI ADDR SZ WCHAN  STIME TTY          TIME CMD
0 R teacher    12976   12956 58  80   0 -  1547 -      20:54 pts/2    00:02:07 yes bg
0 R teacher    12988   12956 49  80   0 -  1547 -      20:56 pts/2    00:00:45 yes bg
0 R teacher    12991   12956  4  90  10 -  1547 -      20:57 pts/2    00:00:00 yes nice
```

2.2. Змініть пріоритети завдань:

- yes fg — пріоритет 10,

- yes nice — пріоритет –10.

- Змініть пріоритет першого процесу на 10 (уповільнить виконання команди):

```
teacher@rybachok:~$ renice -n 10 12976
12976 (process ID) old priority 0, new priority 10
teacher@rybachok:~$ ps -C yes -l -f
F S UID          PID    PPID  C PRI  NI ADDR SZ WCHAN  STIME TTY          TIME CMD
0 R teacher    12976   12956 55  90  10 -  1547 -      20:54 pts/2    00:02:37 yes bg
0 R teacher    12988   12956 49  80   0 -  1547 -      20:56 pts/2    00:01:17 yes bg
0 R teacher    12991   12956  5  90  10 -  1547 -      20:57 pts/2    00:00:03 yes nice
```

- Збільште пріоритет процесу yes nice (від імені root) до –10:

```
teacher@rybachok:~$ sudo renice -n -10 12991
12991 (process ID) old priority 10, new priority -10
teacher@rybachok:~$ ps -C yes -l -f
F S UID          PID    PPID  C PRI  NI ADDR SZ WCHAN  STIME TTY          TIME CMD
0 R teacher    12976   12956 49  90  10 -  1547 -      20:54 pts/2    00:02:41 yes bg
0 R teacher    12988   12956 55  80   0 -  1547 -      20:56 pts/2    00:01:49 yes bg
0 R teacher    12991   12956  8  70 -10 -  1547 -      20:57 pts/2    00:00:09 yes nice
```

- Визначте номер вашого варіанта (остання цифра в номері за списком групи). Допишіть цю інформацію у файл share/jobs.txt (рис. 9.4). Далі наводиться приклад для номера варіанту 0.

2.3. Виведіть на екран та у файл share/jobs.txt інформацію про процеси, породжені за допомогою команди yes та сортовані за параметром із таблиці 9.1, який відповідає номеру варіанту.

2.4. Оновіть вміст файлу share/index.html.

2.5. Перегляньте файл share/jobs.txt у браузері. Зробіть скріншот 2.

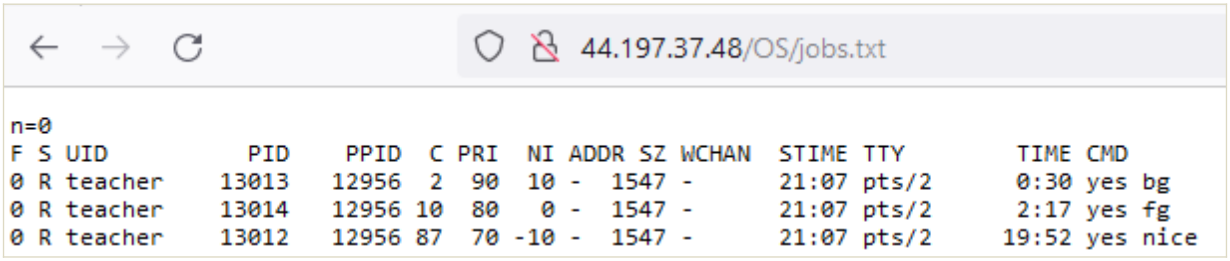


Рис. 9.2. Файл результатів share/jobs.txt. Приклад скріншоту 2

3. Моніторинг процесів, надсилання сигналів, зміна пріоритетів з допомогою команди top

3.1. Налаштуйте відображення команди top відповідно до номеру варіанту:

- 6 полів: S, PID, UID, NI, параметр сортування, CMD (параметр сортування взяти із табл. 9.1 відповідно до номера варіанта);
- команда повинна бути записана у повному форматі;
- кількість процесів у виведенні — n+3;

Зробіть скріншот 3.

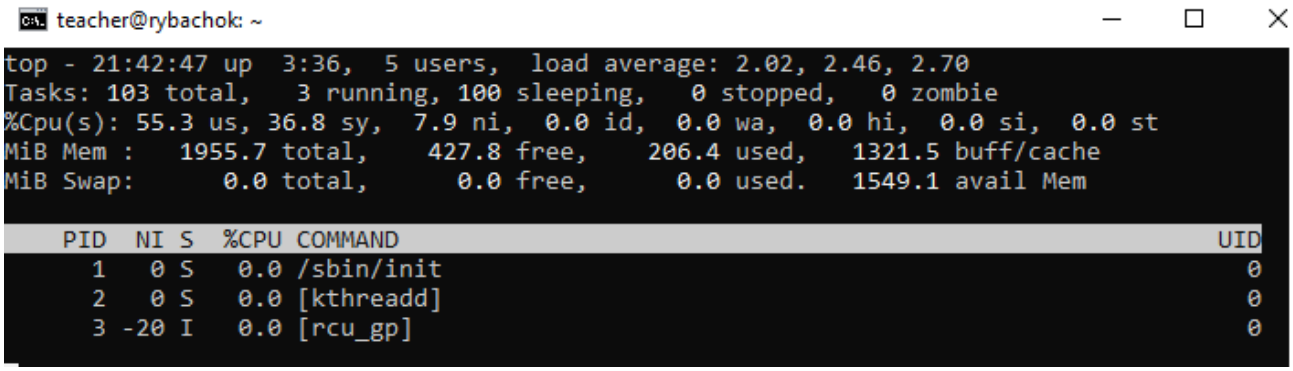


Рис. 9.3. Фільтрація результатів команди top. Приклад скріншоту 3

Завершіть top.

3.2. Виконайте зміну пріоритетів та надсилання сигналів процесам.

- Відкрийте top від імені sudo.

- Відсортуйте процеси за назвою команди (команда повинна бути показна повністю).

- Змініть пріоритет процесу “yes nice” на -20.

- Зупиніть процес “yes fg”, надіславши йому сигнал SIGSTOP (19).

- Зробіть скріншот 4.

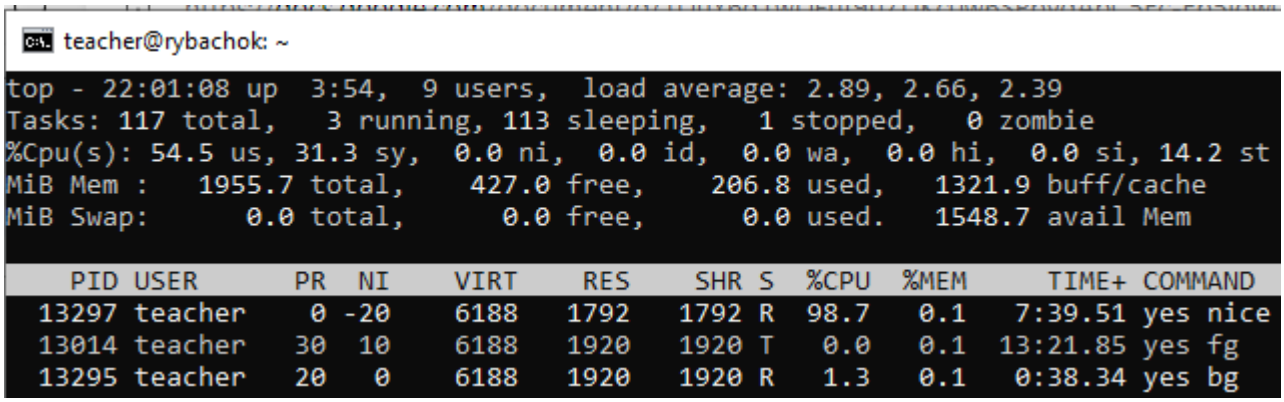


Рис. 9.4. Фонові завдання в команді top. Приклад скріншоту 4

3.3. Надішліть сигнал завершення процесу login користувача <username>

- Додайте у виведення top стовпчик PPID, відсортуйте процеси за USER.

- Визначте PID процесу login для користувача <username>. Команда повинна бути записана у повному форматі.

- Зробіть скріншот 5.

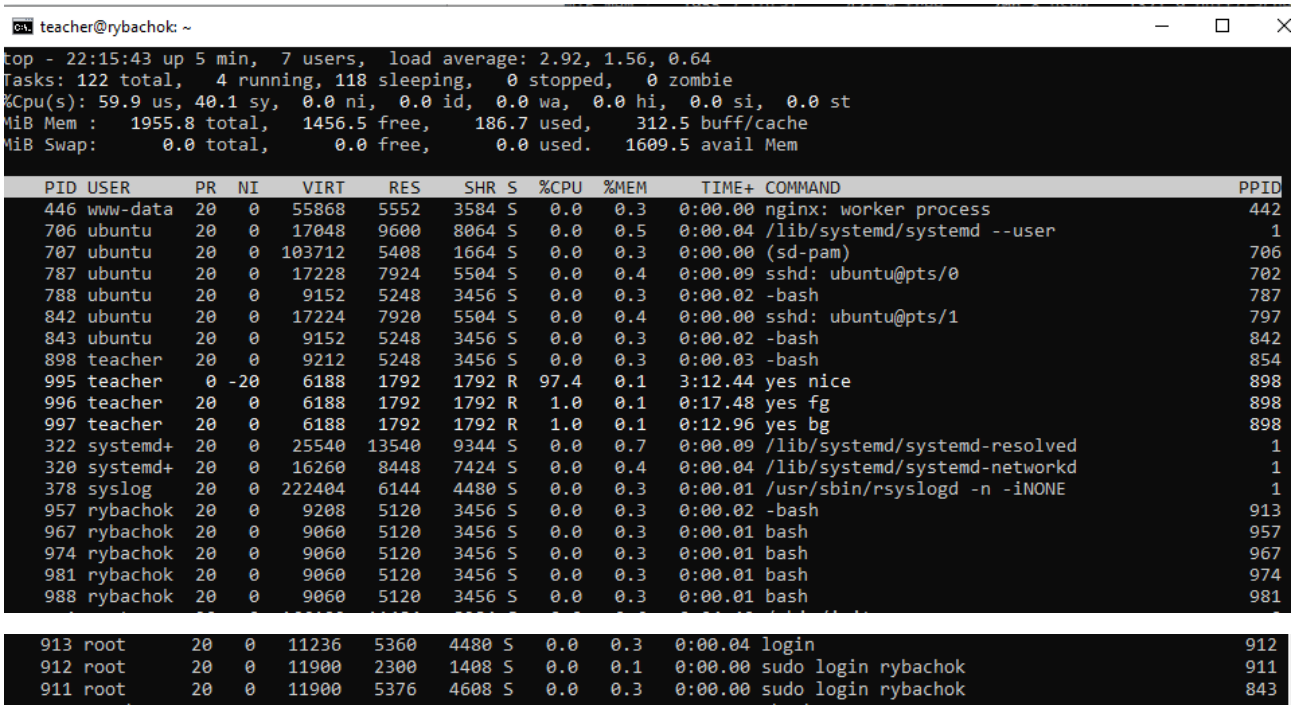


Рис. 9.5. Процеси користувача <username> в top. Приклад скріншоту 5

- Знищіть процес login (має закритися сеанс користувача <username>).

4. Знищіть фонові процеси, скориставшись утилітою killall.

5. Завершіть всі сеанси та вимкніть ВМ.

Варіанти завдання

Таблиця 9.1. Параметри сортування для команди ps , top

Остання цифра №варіанту, n	*стовпчик для відображення*		*порядок сортування*
	ps	*top*	
0	C	%cpu	за зростанням
1	C	%cpu	за спаданням
2	TIME	time+	за зростанням
3	TIME	time+	за спаданням
4	PRI	PR	за зростанням

Продовження таблиці 9.1

5	PRI	PR	за спаданням
6	NI	VIRT	за зростанням
7	NI	VIRT	за спаданням
8	SZ	nTH	за зростанням
9	SZ	nTH	за спаданням

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку;
- завдання до лабораторної роботи;
- скріншоти 1-5;
- висновки.

Питання для самоперевірки

1. Стани процесів у Linux.
2. Які команди призначені для управління завданнями?
3. Яка команда дозволяє переглянути список процесів? Призначення опцій та колонок виведення команди.
4. Яка команда дозволяє переглянути динамічну інформацію про процеси? Призначення опцій та колонок виведення команди.
5. Як дізнатися та змінити пріоритет виконання процесів?
6. Які команди призначені для надсилання сигналів процесам?
7. В чому відмінність між обробкою сигналів SIGKILL та SIGTERM? Який із них завершує роботу процесу більш дипломатично?

Рекомендована література

1. Створення, моніторинг та зупинка процесів. Урок 1https://learning.lpi.org/uk/learning-materials/101-500/103/103.5/103.5_01/

ПРАКТИЧНЕ ЗАВДАННЯ 10.

ОСНОВИ АДМІНІСТРУВАННЯ КОРИСТУВАЧІВ ТА ГРУП

Мета роботи - одержання практичних навичок адміністрування користувачів та груп в операційній системі Linux.

Завдання

Сформувати шаблонну директорію від імені користувача teacher. Створи ти скрипти для додавання групи та окремого користувача, видалення групи та окремого користувача. Створити групу, додати до неї окремого користувача, створити файли користувача, видалити користувача. Вивести результати виконання завдань на сервер.

Вказівки до виконання завдання

1. Запустіть ВМ Ubuntu AWS. Приєднайтеся за SSH.

2. Сформуйте шаблонну директорію від імені користувача teacher.

2.1. Сформуйте шаблонну директорію /home/OS/skel з символічними посиланнями:

mkdir skel; cd skel

ln -s /home/OS/task task

ln -s /home/OS/share share

2.2. Скопіюйте файли профілю в директорію-шаблон:

sudo cp /etc/skel/.???* /home/OS/skel/

2.3. Встановіть маску на створення нових файлів у файлі /home/OS/skel/.bashrc

UMASK 0022

3.Напишіть скрипти, які будуть виконувати:

- створення групи або нового користувача у групі,

- видалення групи або видалення користувача групи,

- генерацію файлу результатів для групи.

3.1. Скрипт створення групи або нового користувача у групі (рис. 10.1, 10.2) приймає на вхід параметри:

- назву групи (group);

- файл зі списком групи (file) або ПІ користувача (first, last);

- дату блокування облікових записів (e_date).

Скрипт виконує дії:

- створює користувачів studentKgroup, K=1,N ;

- із домашньою піддиректорією в /home/OS/student;

- використовується шаблон /home/OS/skel;

- в якості оболонки використовується /bin/bash;

- користувач додається в основну групу OS;

- в якості паролю встановлюється пароль studentKgroup;

- дата блокування облікових записів e_date;

- надає права 755 на домашні директорії.

sudo useradd -b /home/OS/student -e $e_date -f -1 -g OS -N -k /home/OS/skel -m -s /bin/bash -c comment -p $pass studentKgroup

При додаванні окремого користувача у групу додатково виводиться запис про нього із файлів /etc/passwd та /etc/shadow.

3.2. При видаленні скрипт запитує (рис. 10.4):

- назву групи;

- видаляється вся група чи окремий користувач;

- чи потрібно видаляти файли, створені у спільній директорії share;

- чи потрібно видаляти домашню директорію користувачів.

3.3. При генерації результів (рис. 10.3) скрипт запитує назву групи group, генерує файл/home/OS/share/$group.html, який містить ПІ студента (поле файлу /etc/passwd) та посилання на файл ~studentK/taski.html, i=1..12, якщо такий файл існує.

3.4. Після створення скриптів розмістити їх у папку /home/OS/script, створити жорсткі посилання на файли скриптів у папці .bak.

4. Оформіть звіт.

4.1. Створіть групу до якої ви належите, використавши файл зі списком групи. Зробіть скріншот 1.

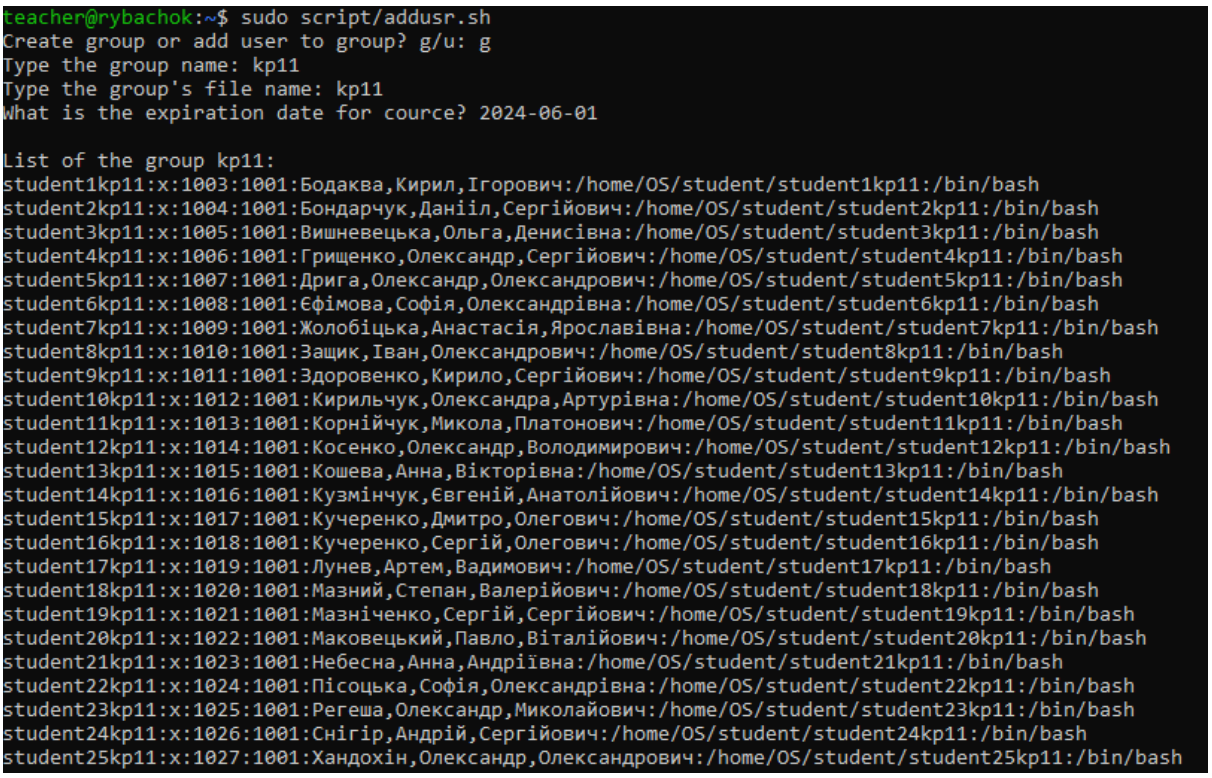


Рис. 10.1. Створення групи. Приклад скріншоту 1

4.2. До групи додайте нового користувача Іваненко Іван. Зробіть скріншот 2.

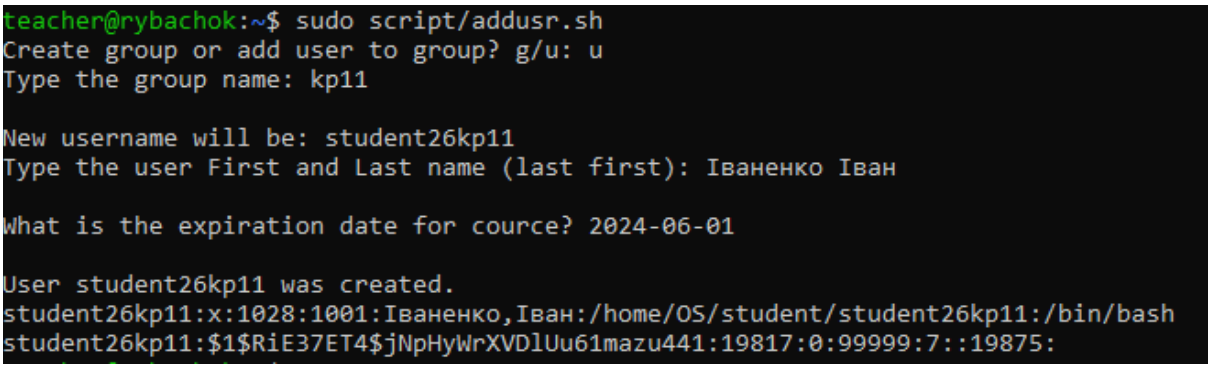


Рис. 10.2. Створення окремого користувача групи. Приклад скріншоту 2

Зверніть увагу, що пароль має бути хешованим.

4.3. Від імені користувача із вашим логіном за списком групи створити файли /home/OS/student/studentK/taski.html, i=1-10 .

4.4. Від імені teacher згенерувати файл результатів по групі $group.html та оновіть /home/OS/share/index.html. Зробіть скріншот 3.

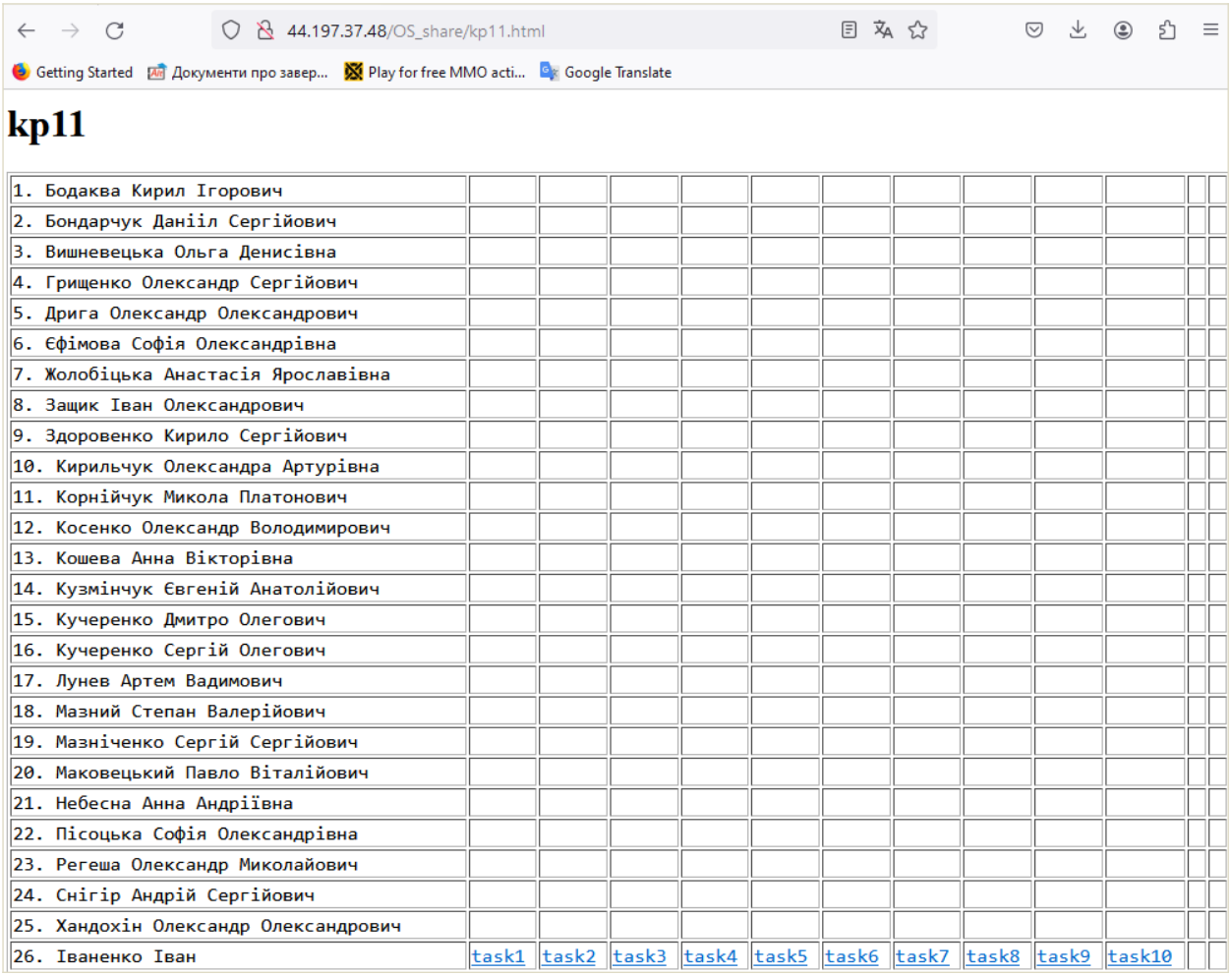


Рис. 10.3. Файл результатів групи. Приклад скріншоту 3

5.5. В спільній папці share від користувача Іваненко створіть файл ivanenko.html, видаліть користувача Іваненко, спільний файл і домашню директорію користувача. Зробіть скріншот 4.

6. Заверште всі сеанси та вимкніть ВМ.

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку;
- завдання до лабораторної роботи;
- скріншоти 1-4;
- висновки.

```
teacher@rybachok:~$ ls -l `find share -user student26kp11`
-rw-r--r-- 1 student26kp11 OS 0 Apr  4 15:49 share/ivanenko.html
teacher@rybachok:~$ ls -ld /home/OS/student/student26kp11/
drwxr-x--- 3 student26kp11 OS 4096 Apr  4 15:49 /home/OS/student/student26kp11/
teacher@rybachok:~$ sudo script/delgrp.sh
Delete group or user? g/u: u
Type group name: kp11
 Students of group  kp11
student1kp11:x:1003:1001:Бодаква,Кирил,Ігорович:/home/OS/student/student1kp11:/bin/bash
student2kp11:x:1004:1001:Бондарчук,Даніїл,Сергійович:/home/OS/student/student2kp11:/bin/bash
student3kp11:x:1005:1001:Вишневецька,Ольга,Денисівна:/home/OS/student/student3kp11:/bin/bash
student4kp11:x:1006:1001:Грищенко,Олександр,Сергійович:/home/OS/student/student4kp11:/bin/bash
student5kp11:x:1007:1001:Дрига,Олександр,Олександрович:/home/OS/student/student5kp11:/bin/bash
student6kp11:x:1008:1001:Єфімова,Софія,Олександрівна:/home/OS/student/student6kp11:/bin/bash
student7kp11:x:1009:1001:Жолобіцька,Анастасія,Ярославівна:/home/OS/student/student7kp11:/bin/bash
student8kp11:x:1010:1001:Защик,Іван,Олександрович:/home/OS/student/student8kp11:/bin/bash
student9kp11:x:1011:1001:Здоровенко,Кирило,Сергійович:/home/OS/student/student9kp11:/bin/bash
student10kp11:x:1012:1001:Кирильчук,Олександра,Артурівна:/home/OS/student/student10kp11:/bin/bash
student11kp11:x:1013:1001:Корнійчук,Микола,Платонович:/home/OS/student/student11kp11:/bin/bash
student12kp11:x:1014:1001:Косенко,Олександр,Володимирович:/home/OS/student/student12kp11:/bin/bash
student13kp11:x:1015:1001:Кошева,Анна,Вікторівна:/home/OS/student/student13kp11:/bin/bash
student14kp11:x:1016:1001:Кузмінчук,Євгеній,Анатолійович:/home/OS/student/student14kp11:/bin/bash
student15kp11:x:1017:1001:Кучеренко,Дмитро,Олегович:/home/OS/student/student15kp11:/bin/bash
student16kp11:x:1018:1001:Кучеренко,Сергій,Олегович:/home/OS/student/student16kp11:/bin/bash
student17kp11:x:1019:1001:Лунев,Артем,Вадимович:/home/OS/student/student17kp11:/bin/bash
student18kp11:x:1020:1001:Мазний,Степан,Валерійович:/home/OS/student/student18kp11:/bin/bash
student19kp11:x:1021:1001:Мазніченко,Сергій,Сергійович:/home/OS/student/student19kp11:/bin/bash
student20kp11:x:1022:1001:Маковецький,Павло,Віталійович:/home/OS/student/student20kp11:/bin/bash
student21kp11:x:1023:1001:Небесна,Анна,Андріївна:/home/OS/student/student21kp11:/bin/bash
student22kp11:x:1024:1001:Пісоцька,Софія,Олександрівна:/home/OS/student/student22kp11:/bin/bash
student23kp11:x:1025:1001:Регеша,Олександр,Миколайович:/home/OS/student/student23kp11:/bin/bash
student24kp11:x:1026:1001:Снігір,Андрій,Сергійович:/home/OS/student/student24kp11:/bin/bash
student25kp11:x:1027:1001:Хандохін,Олександр,Олександрович:/home/OS/student/student25kp11:/bin/bash
student26kp11:x:1028:1001:Іваненко,Іван:/home/OS/student/student26kp11:/bin/bash

Type student login: student26kp11
Delete share files? y/n: y
Delete home directory? y/n: y
userdel: student26kp11 mail spool (/var/mail/student26kp11) not found
teacher@rybachok:~$ ls -ld /home/OS/student/student26kp11/
ls: cannot access '/home/OS/student/student26kp11/': No such file or directory
teacher@rybachok:~$ ls -l `find share -user student26kp11`
find: ‘student26kp11’ is not the name of a known user
teacher@rybachok:~$ find share -user 1028 2> /dev/null
```

Рис. 10.4. Видалення користувача. Приклад скріншоту 4

Питання для самоперевірки

1. Структура файлу /etc/passwd.
2. Структура файлу /etc/shadow.
3. Структура файлу /etc/group.

Рекомендована література

1. Creating Users and Groups. Lesson 1 // Електронний ресурс. Режим доступу: https://learning.lpi.org/en/learning-materials/010-160/5/5.1/5.1_01/

ПРАКТИЧНЕ ЗАВДАННЯ 11.
РОБОТА ІЗ ТЕКСТОВИМИ ДАНИМИ ТА НАДСИЛАННЯ ПОШТИ ЗА ДОПОМОГОЮ GMAIL

Мета роботи - отримання навиків практичної роботи із текстовими даними та надсилання пошти за допомогою Gmail.

Завдання

Налаштувати відправлення пошти із командного рядка, використовуючи сервер Gmail. Написати скрипт, який обробляє текстові файли та надсилає повідомлення на пошту. Передресувати SSH трафік на порт 222.

Вказівки до виконання завдання

1. Налаштуйте Google Account.

1.1. Створіть або використайте вже існуючий Google Account. Необхідно налаштувати двоетапну перевірку.

1.2. Після налаштувань двоетапної перевірки, необхідно в розділі *Безпека/Вхід в обліковий запис Google/Паролі додатків* створити та зберегти окремий пароль для пошти, котрий надалі буде необхідний при налаштуваннях.

2. Встановіть агент передачі пошти Postfix.

2.1. Під’єднайтеся до ВМ Ubuntu AWS.

2.2. Оновіть пакети:

sudo apt-get update && sudo apt-get upgrade

2.3. Встановіть агент передачі пошти Postfix:

sudo apt install postfix

Для реконфігурації Postfix можна використати команду:

sudo dpkg-reconfigure postfix

Першою частиною інсталяції Postfix є текстовий інтерфейс користувача. За допомогою клавіатури виберіть *Інтернет-сайт* для типу конфігурації пошти. На наступному екрані введіть доменне ім’я вашого сервера. Зауважте, що це ніяк не впливає на вашу здатність надсилати пошту з Gmail, тож якщо у вас немає доменного імені, це нормально.

3. Налаштуйте SASL за допомогою своїх облікових даних Gmail.

3.1. Створіть файл /etc/postfix/sasl/sasl_passwd і додайте до нього свою адресу Gmail і пароль програми:

sudo nano /etc/postfix/sasl/sasl_passwd

[smtp.gmail.com]:587 microdomainz@gmail.com:password

3.2. Далі створіть файл хеш-бази даних за допомогою такої команди postmap:

sudo postmap /etc/postfix/sasl/sasl_passwd

3.3. Щоб захистити простий текстовий пароль, змініть власника та дозвіл на файли SASL наступним чином:

sudo chown root:root /etc/postfix/sasl/sasl_passwd /etc/postfix/sasl/sasl_passwd.db

sudo chmod 0600 /etc/postfix/sasl/sasl_passwd /etc/postfix/sasl/sasl_passwd.db

3.4. Щоб наказати Postfix використовувати сервери Gmail для надсилання пошти, відредагуйте /etc/postfix/main.cf:

sudo nano /etc/postfix/main.cf

relayhost = [smtp.gmail.com]:587

3.5. Також додайте наступне в кінець /etc/postfix/main.cf, щоб увімкнути автентифікацію SASL для Postfix:

 # Enable SASL authentication

smtp_sasl_auth_enable = yes

smtp_sasl_security_options = noanonymous

smtp_sasl_password_maps = hash:/etc/postfix/sasl/sasl_passwd

smtp_tls_security_level = encrypt

smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt

3.6. Перезапустіть Postfix:

sudo systemctl restart postfix

4. Протестуйте надсилання повідомлень (в даному варіанті надсилань повідомлень, для відправки необхідно натиснути Ctrl+D).

```
ubuntu@rybachok:~$ mail rybachoknata@gmail.com
Cc:
Subject: From Ubuntu
This letter is from Ubuntu VM
```

Рис. 11.1. Приклад відправлення листа із командного рядка bash

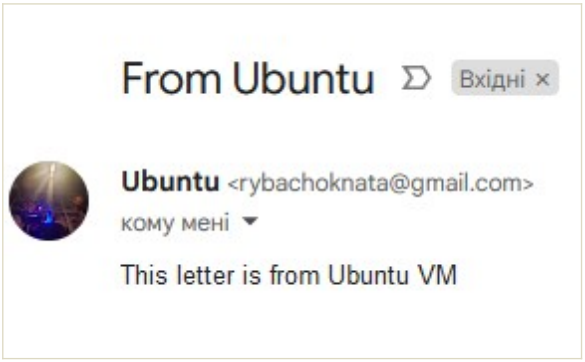


Рис. 11.2. Приклад отриманого листа

5. Напишіть скрипт, який містить 3 функції, що обробляють текстові файли. Реультати записуються результат у файл, який надсилається на пошту rybachok.nataliia@lll.kpi.ua та виводиться на екран.

5.1. Файл /var/log/auth.log

Файл містить вдалі та невдалі спроби входу в систему, а також задіяні механізми аутентифікації.

- Ознайомтеся зі структурою файлу.

- Створіть першу функцію, яка для файлу /var/log/auth.log визначає записи, що стосуються невдалих спроб входу в систему за sshd (містять рядок Invalid), а якщо записи відсутні, то видає відповідне повідомлення (рис. 11.2). Запишіть результати виконання фільтрації до файлу та виведіть на екран.

Невдалі спроби авторизації за sshd до хосту <назва хоста> за sshd за <IP адреса> станом на ДД/ММ/РР ГГ:ХХ

```
Невдалі спроби авторизації до хосту  rybachok за sshd з 44.197.37.48 станом на  02/06/24 16:03
відсутні
```

Рис. 11.3. Приклад виведення функції 1

- Додатково перевірте файли /var/log/auth.log.1, /var/log/auth.log.*.gz. Виведіть результати пошуку, зробіть скріншот 1.

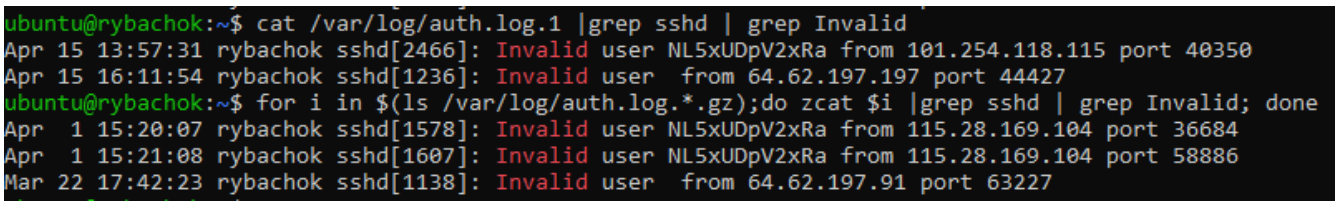


Рис. 11.4. Невдалі спроби авторизації . Приклад скріншоту 1

5.2. Файл /var/log/nginx/access.log

Містить інформацію про запити до сервера за поточний день.

- Ознайомтеся зі структурою файлу.

- За допомогою другої функції скрипта визначте записи, які стосуються “шкідливих” запитів. Приймемо гіпотезу, що запити, які генерують 4xx помилку – шкідливі. Запишіть результати виконання фільтрації до файлу та виведіть на екран.

Згенеруйте повідомлення, яке містить текст та записи про отримання 404 помилки (унікальні IP адреси та кількість запитів із адреси, сортовані за спаданням) та виведіть відповідне повідомлення у файл та на екран. Якщо такі записи відсутні, то надайте відповідне повідомлення.

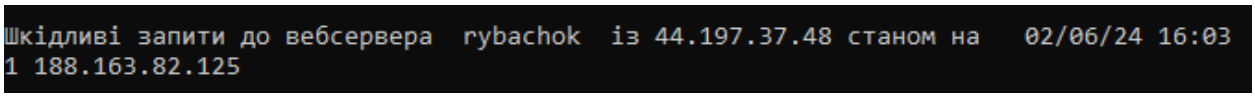


Рис. 11.5. Приклад виведення функції 2

- Додатково перевірте файли /var/log/nginx/access.log.1, /var/log/nginx/access.log.gz.

- Виведіть дату модифікації файлу та кількість унікальних адрес, із яких були здійснені шкідливі запити, зробіть скріншот 2.

Рис. 11.6. Шкідливі запити до вебсервера. Приклад скріншота 2

5.3. Команда netstat -ntu

Ця команда показує інтернет-з'єднання з певних адрес.

- Напишіть третю функцію, яка генерує повідомлення, що містить текст та записи про список унікальних IP-адрес і портів та вкажіть кількість підключень із IP адрес, сортованих за спаданням. Повідомлення вивести у файл та на екран.

```
Кількість підключень за різними портами до сервера  rybachok  з 44.197.37.48 станом на 02/06/24 16:03
      3 34.117.118.44:80
      1 188.163.82.125:30199
```

Рис. 11.6. Приклад виведення функції 3

5.4. Додайте у файл скрипта команду для надсилання згенерованого файлу:

```
cat $file | mail -s "From $(hostname)"  rybachok.nataliia@lll.kpi.ua
```

5.5. Зробіть скріншот файлу скрипта.

```
ubuntu@rybachok:~/script$ cat filter.sh
#!/bin/bash
ip=`curl ifconfig.me 1>/dev/null 2>&1`
```

Рис. 11.6. Створений скрипт. Приклад скріншота 3

6. Переадресуйте ssh трафік на 222 порт та налаштувати відповідне вхідне правило NSG.

6.1. Відредагуйте файл */etc/ssh/sshd_config:*

Port 222

4.2. Перезапустіть сервіс:

sudo systemctl reload sshd

6.3. Налаштуйте відповідне вхідне правило NSG на порталі AWS:

Protocol TCP

Port range 222

Source 0.0.0.0/0

Зробіть скріншот 4.

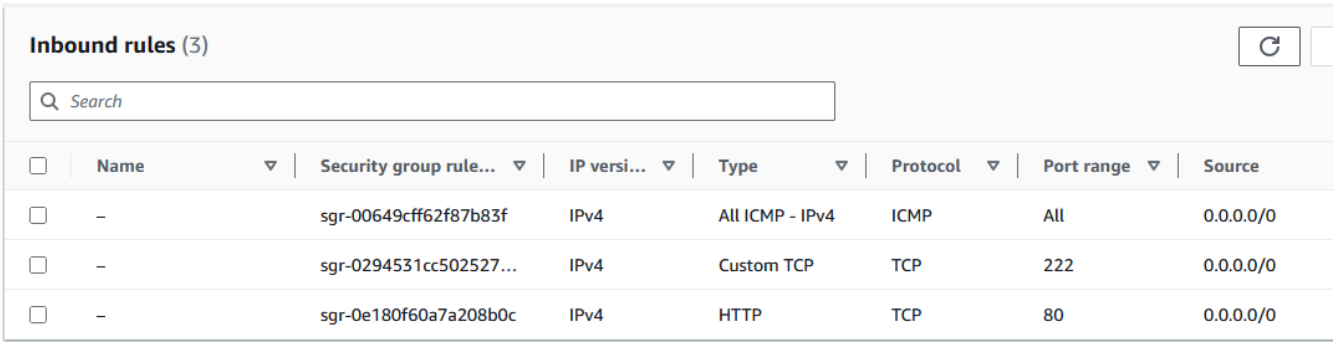


Рис. 11.7. Правило NSG. Приклад скріншота 4

6.4. Закрийте ssh сеанс та відкрийте його знову із використанням нового порта.

```
C:\Users\Home>ssh -i .ssh\labsuser.pem ubuntu@44.197.37.48 -p 222
```

4.5. Зробіть скріншот 5 статусу сервісу sshd:

sudo systemctl status sshd

```
ubuntu@rybachok:~$ sudo systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
    Drop-In: /usr/lib/systemd/system/ssh.service.d
             └─ec2-instance-connect.conf
     Active: active (running) since Mon 2024-04-22 14:21:47 EEST; 44min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 601 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Process: 1387 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Process: 1388 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
   Main PID: 606 (sshd)
      Tasks: 1 (limit: 2329)
     Memory: 5.5M
        CPU: 103ms
     CGroup: /system.slice/ssh.service
             └─606 "sshd: /usr/sbin/sshd -D -o AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized

Apr 22 14:21:47 rybachok systemd[1]: Started OpenBSD Secure Shell server.
Apr 22 14:30:40 rybachok sshd[803]: Accepted publickey for ubuntu from 188.163.82.125 port 30553 ssh2: RSA SHA256:3Oxqe
Apr 22 14:30:40 rybachok sshd[803]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by (uid=0)
Apr 22 14:57:10 rybachok systemd[1]: Reloading OpenBSD Secure Shell server...
Apr 22 14:57:10 rybachok sshd[606]: Received SIGHUP; restarting.
Apr 22 14:57:10 rybachok systemd[1]: Reloaded OpenBSD Secure Shell server.
Apr 22 14:57:10 rybachok sshd[606]: Server listening on 0.0.0.0 port 222.
Apr 22 14:57:10 rybachok sshd[606]: Server listening on :: port 222.
Apr 22 14:58:08 rybachok sshd[1396]: Accepted publickey for ubuntu from 188.163.82.125 port 30412 ssh2: RSA SHA256:3Oxq
Apr 22 14:58:08 rybachok sshd[1396]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by (uid=0)
```

Рис. 11.8. Статус сервісу sshd. Приклад скріншота 5

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку;
- завдання до лабораторної роботи;
- скріншоти 1-5;
- висновки.

Питання для самоперевірки

1. Яку конфігурацію повинен мати Postfix для роботи із інтернет-серверами?

2. Синтаксис та призначення команди mail.

3. Синтаксис та призначення команд tail, head, sort, grep, uniq, cut, wc, cat, tac.

4. Структура та призначення файлів /var/log/auth.log, /var/log/nginx/access.log.

5. Синтаксис та призначення команди netstat.

Рекомендована література

1. Обробка текстових потоків за допомогою фільтрів. Урок 1 // Електронний ресурс. Режим доступу: https://learning.lpi.org/uk/learning-materials/101-500/103/103.2/103.2_01/

2. Configure Postfix with Gmail on Ubuntu // Електронний ресурс. Режим доступу: https://www.tutorialspoint.com/configure-postfix-with-gmail-on-ubuntu

ПРАКТИЧНЕ ЗАВДАННЯ 12.
РОБОТА ІЗ БАЗОЮ ДАНИХ MYSQL

Мета роботи - отримання навичків практичної роботи із базою даних MYSQL в командному рядку bash.

Завдання

Встановити MySQL server на ВМ Xubuntu. Створити базу даних (БД) та заповнити її таблицю із файлу. Створити користувача зі своїм прізвищем та надати йому права на читання БД. Зробити вибірку даних у файл. Створити скрипт, який робить бекап БД та за допомогою команди rsync синхронізує вміст директорії на серверах Xubuntu та Ubuntu AWS. Створити завдання для anacron, яке запускає створений раніше скрипт.

Вказівки до виконання завдання

1. Встановіть MySQL server на ВМ Xubuntu.

1.1. Виконайте оновлення списку пакетів на сервері:

sudo apt update

1.2. Встановіть пакет MySQL сервер:

sudo apt install mysql-server

Перевірка:

systemctl status mysql.service

2. Створіть базу даних (БД) cource та заповніть її таблицю із наданого файлу, що відповідає вашій групі.

2.1. Підключіться до БД від імені користуваача root:

sudo mysql -u root -p

2.2. Створіть БД cource:

CREATE DATABASE cource;

Перевірка:

SHOW DATABASES;

2.3. Виберіть для використання базу даних:

USE course;

2.4. Перемістіть файл group.txt, що відповідає вашій групі, у директорію /var/lib/mysql-files/. Зробіть власником та групою для файлу користувача mysql та групу mysql:

mv /var/lib/mysql-files/

chown mysql:mysql /var/lib/mysql-files/group.txt

Примітка

MySQL читає файли із директорії, шлях до якої визначається системною змінною secure_file_priv. Прочитати її вміст можна наступною командою:

select @@secure_file_priv;

2.5. Створіть таблицю cource.group з 3 стовпцями даних VARCHAR(20) та заповніть її із файлу group.txt:

create table group (surname VARCHAR(20),firstname VARCHAR(20),secondname VARCHAR(20));

Перевірка:

SHOW TABLES;

DESCRIBE group;

LOAD DATA INFILE "/var/lib/mysql-files/group.txt" INTO TABLE course.group;

Перевірка:

SELECT * FROM group;

3. Створіть користувача зі своїм прізвищем та надайте йому права на читання БД. Зробіть вибірку даних у файл, який розмістіть на сервер.

3.1. Створіть користувача зі своїм прізвищем та надайте йому права на читання БД. Зробіть скріншот 1.

CREATE USER 'username'@'localhost' IDENTIFIED BY 'password';

де 'username'– логін користувача, password- його пароль.

GRANT SELECT ON course.froup TO 'username'@'localhost';

FLUSH PRIVILEGES;

SHOW GRANTS FOR 'username'@'localhost';

```
mysql> SHOW GRANTS FOR 'rybachok'@'localhost';
+-----------------------------------------------------------+
| Grants for rybachok@localhost                             |
+-----------------------------------------------------------+
| GRANT USAGE ON *.* TO `rybachok`@`localhost`              |
| GRANT SELECT ON `course`.`KP11` TO `rybachok`@`localhost` |
+-----------------------------------------------------------+
2 rows in set (0,00 sec)

mysql>
```

Рис. 12.1. Права користувача username.Приклад скріншоту 1

3.2. Змініть в БД запис зі своїм прізвищем, щоб від починався із *:

UPDATE group SET surname = '*lastname' WHERE surname = 'lastname';

3.3. Зробіть вибірку всіх даних у файл.

```
rybachok@kp1x:~$ sudo mysql -u rybachok --password -vv -se "select * from course.KP11;" >KP11.txt
Enter password:
rybachok@kp1x:~$ cat KP11.txt
--------------
select * from course.KP11
--------------

Bodakva Kyryl   Ihorovych
Bondarchuk      Daniil  Serhiiovych
```

3.4. Файл розмістіть на локальному сервері. Зробіть скріншот 2.

mv KP11.txt /var/www/html

Рис. 12.2. Файл із вмістом таблиці БД.Приклад скріншоту 2

4. На ВМ Xubuntu створіть скрипт, який робить бекап БД (у назві файлу використати поточну дату) та за допомогою команди rsync синхронізує вміст директорії на серверах Xubuntu та Ubuntu AWS. Зробіть скріншот 3.

```
rybachok@kp1x:~$ cat task12.sh
#!/bin/bash
file=course-bak_`date +%d%m%y`.sql
sudo mysqldump course > /home/rybachok/database/$file
rsync -avzhe "ssh -i /home/rybachok/.ssh/labsuser.pem -p 222" /home/rybachok/database/
 ubuntu@44.197.37.48:/home/ubuntu/.bak/

if [ $? != 0  ];  then  echo  "Server is not available!!!"
fi
```

Рис. 12.3. Файл із вмістом скрипта. Приклад скріншоту 3

5. На ВМ Xubuntu створіть завдання для anacron, яке запускає створений раніше скрипт. Зробіть скріншот 4.

```
rybachok@kp1x:~$ cat /etc/anacrontab
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
HOME=/root
LOGNAME=root

# These replace cron's entries
1       5       cron.daily      run-parts --report /etc/cron.daily
7       10      cron.weekly     run-parts --report /etc/cron.weekly
@monthly        15      cron.monthly    run-parts --report /etc/cron.monthly
1       2       database_copy   sudo /home/rybachok/task12.sh
```

Рис. 12.4. Файл із завданням anacron. Приклад скріншоту 4

6. Декілька днів включайте віртуальні машини, забезпечуючи створення бекапів.

7. На сервері AWS за допомогою скрипта із завдання 5 створіть сторінку, яка містить список файлових об'єктів директорії .bak. Напишіть завдання для планувальника anacron на створення такої сторінки. Зробіть скріншот 5.

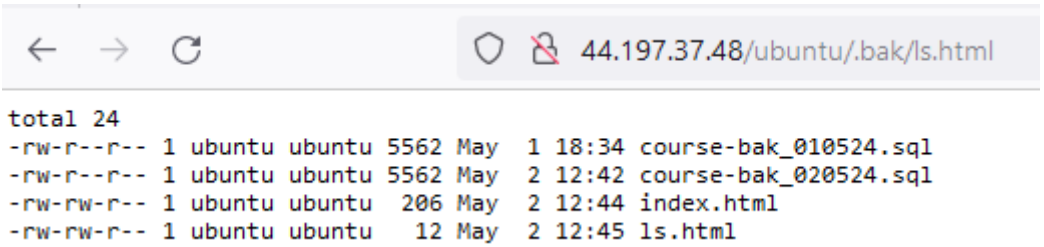


Рис.12.5. Список файлових об'єктів директорії .bak сервера Ubuntu AWS. Приклад скріншоту 4

Вимоги до звіту

Звіт із роботи має бути розміщений у Класрум і містити:

- титульну сторінку;
- завдання до лабораторної роботи;
- скріншоти 1-5;
- висновки.

Питання для самоперевірки

1. Команди MySQL.
2. Синтаксис та призначення команди mysql.
3. Структура та призначення файлу /etc/anacron.
4. Синтаксис та призначення команди rsync.

Рекомендована література

1. MySQL :: MySQL 8.0 Reference Manual :: 15.2.9 LOAD DATA Statement // Електронний ресурс. Режим доступу: https://dev.mysql.com/doc/refman/8.0/en/load-data.html
2. bash - How to redirect mysql output to file? - Stack Overflow // Електронний ресурс. Режим доступу: https://stackoverflow.com/questions/52477206/how-to-redirect-mysql-output-to-file
3. Cron Vs Anacron: как планировать выполнение задач с Anacron в Linux (sedicomm.com) // Електронний ресурс. Режим доступу: https://blog.sedicomm.com/2020/04/11/cron-ili-anacron-kak-planirovat-vypolnenie-zadach-s-pomoshhyu-anacron-v-linux/