

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра кібербезпеки

Звіт до лабораторної роботи № 4
на тему “ Підготовка тестового середовища. Встановлення дистрибутиву Kali
Linux на віртуальну машину ”

Виконав студент(ка)

Борщ Дмитро

Група

КБ-01

Перевірила

Лаврик Т.В

Суми 2023

ЗВІТ

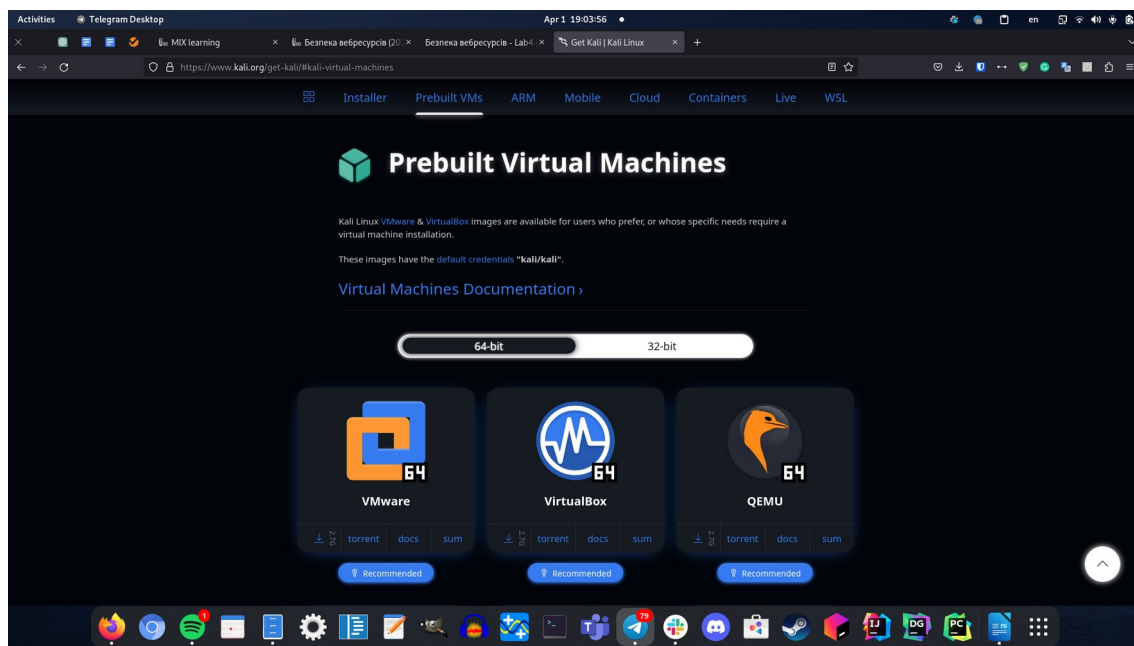
про виконану роботу

Частина I

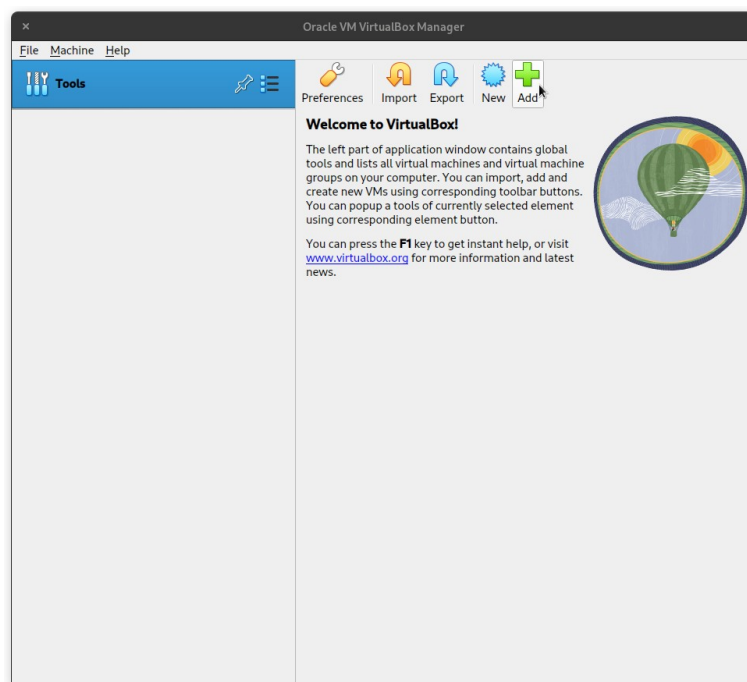
Спосіб № 2

Зберегти скріншоти, що відображають процес встановлення Kali Linux.

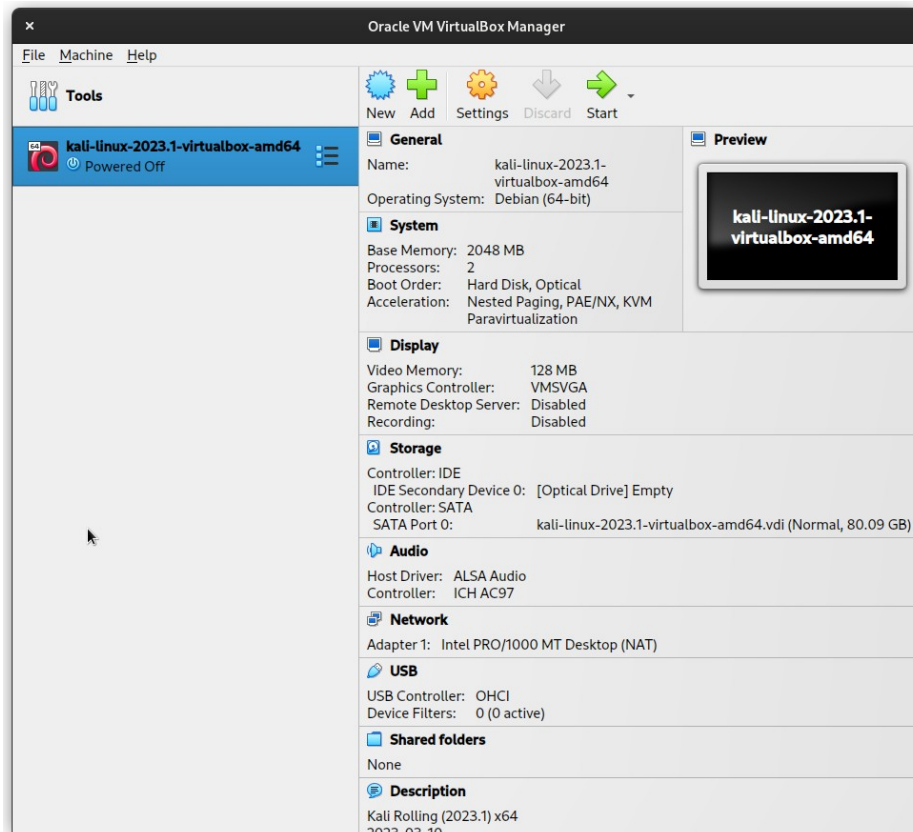
Для виконання лабораторних робіт я завантажув prebuilt віртуальну машину з Kali Linux:



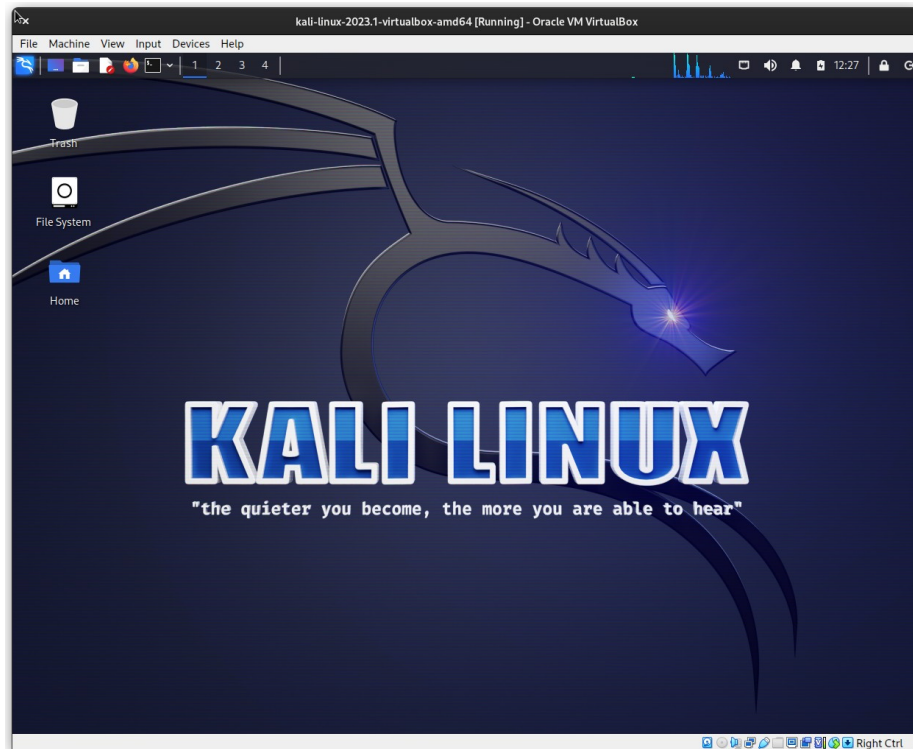
Додаємо готову віртуальну машину:



Імпортована ВМ:



Запустимо й перевіримо працездатність:

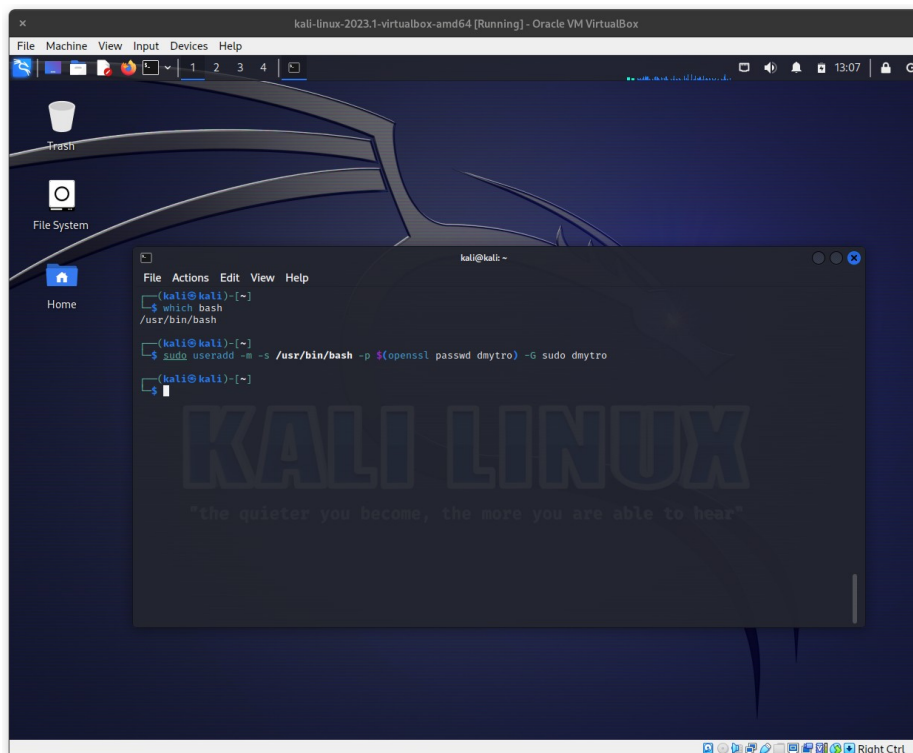


Частина II

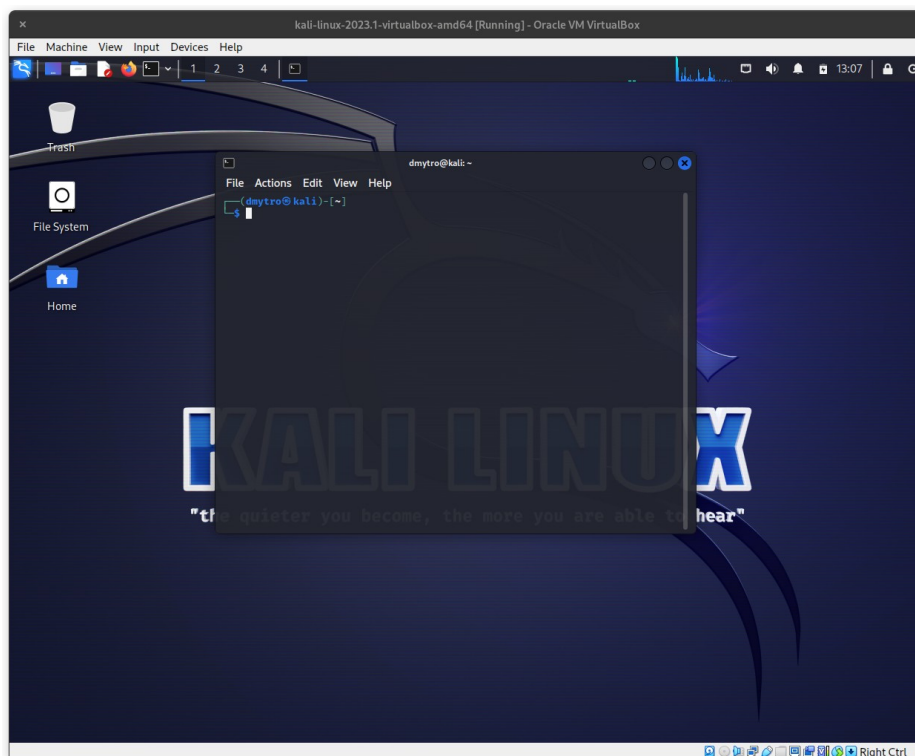
Налаштування віртуальної машини Kali Linux

2.1 Зберегти скріншоти, що відображають створення власного облікового запису в Kali Linux.

Створення користувача з потрібним паролем, шелом та групою sudo:



Спробуємо залогінитися:



Робота з терміналом

2.2 Відкрийте термінал. Запишіть у таблицю відповіді на питання.


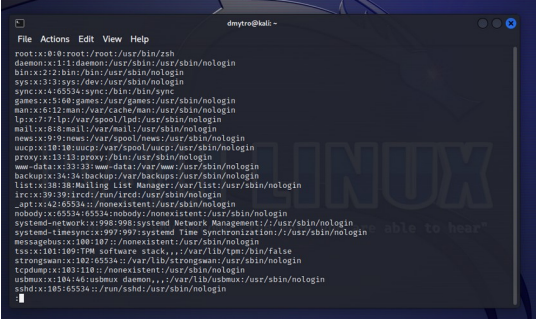
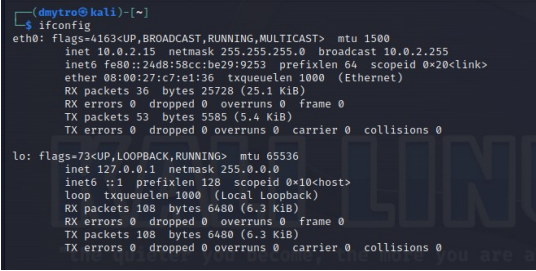
Яке запрошення у командному рядку?	<code>(dmytro kali)-[~]</code> <code>\$</code>
Що означає символ # перед областю введення команд?	Що даний шелл відкритий від імені root
Що означає символ \$ перед областю введення команд?	Що даний шелл відкритий від імені звичайного користувача
Як перейти з одного режиму в інший?	Відкрити шелл від імені потрібного користувача.

2.3 Для чого використовуються команди **su** і **sudo**?

<p>su — запустити команду зі зміненими UID або GID.</p> <p>sudo — скорочення від superuser do, запустити команду від імені root.</p>
--

2.4 У командному рядку терміналу введіть послідовно такі команди *pwd*, *cd ...*, *cd kali*, *mkdir Reports*, *ls*, *clear*, *man*, *whoami*, *passwd*, *less /etc/passwd*, *ifconfig* і результати виконання команд занесіть у таблицю:

Команда	Результат (скріншот)	Характеристика команди
pwd		Виводить на екран шлях до поточної директорії.
cd ..		Перехід в директорію .. “..” в файловій системі Лінукс це жорстке посилання на директорію вищого рівня. Всі директорії його мають, включно з /, тільки там вона вказує саму на себе.
cd kali		Перехід в директорію “kali”, так як це директорія іншого користувача, у нас немає права це робити.
mkdir Reports		Створення директорії “Reports”
ls		Продивитися вміст директорії
clear		Очищає термінал
man		Скорочення від manual, отримання довідки
whoami		Отримати ім'я поточного користувача

<p>passwd</p>	 <pre>(dmytro@kali)-[~] \$ passwd Changing password for dmytro. Current password: New password: Retype new password: The password has not been changed. New password: Password change has been aborted. passwd: Authentication token manipulation error passwd: password unchanged (dmytro@kali)-[~] \$</pre>	<p>Зміна паролю для поточного користувача</p>
<p>less /etc/passwd</p>	 <pre>dmytro@kali - File Actions Edit View Help root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:11:11:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mail list Manager:/var/list:/usr/sbin/nologin ircd:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-networkd:x:990:990:systemd Network Management:/:/usr/sbin/nologin systemd-timesyncd:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin messagebus:x:180:187:/nonexistent:/usr/sbin/nologin tss:x:181:189:TPM software stack,,:/var/lib/tpm:/bin/false strongswan:x:182:65534:/:/var/lib/strongswan:/usr/sbin/nologin cpufreq:x:183:118:/nonexistent:/usr/sbin/nologin usbmux:x:184:66:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin sshd:x:185:65534:/:/run/sshd:/usr/sbin/nologin</pre>	<p>Відкриває файл /etc/passwd в пейджері less</p>
<p>ifconfig</p>	 <pre>(dmytro@kali)-[~] \$ ifconfig eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255 inet6 fe80::248:158c:be29:9253 prefixlen 64 scopeid 0<link> ether 08:00:27:c7:e1:36 txqueuelen 1000 (Ethernet) RX packets 36 bytes 25728 (25.1 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 53 bytes 5585 (5.4 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0<host> loop txqueuelen 1000 (Local Loopback) RX packets 108 bytes 6480 (6.3 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 108 bytes 6480 (6.3 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0</pre>	<p>Утиліта для конфігурації мережевих інтерфейсів</p>

2.5 Більшість команд використовують опції. Щоб дізнатися про опції для даної команди в командному рядку терміналу необхідно ввести:

команда `--help`.

Скористайтесь цією командою і дізнайтеся інформацію про опції таких команд: `passwd`, `sudo`, `ping`, `usermod`. Результати занесіть у таблицю.

Команда	Опція та її характеристика (розглянути 2-3 опції)
passwd	-a, --all — подивитися статус паролів для всіх користувачів -d, --delete — видалити пароль для вказаного юзера -e, --expire — примусово помітити пароль як той, у якого вийшов термін дії.
sudo	-g, --group=group — виконати команду з потрібною групою користувача -R, --chroot=directory — зробити chroot перед виконанням у потрібну директорію -S, --stdin — прочитати пароль зі стандартного потоку вводу.
ping	-i N — інтервал між пакетами в секундах -n — не проводити пошук по DNS -c N — зупинити ping після N пакетів
usermod	-a, --append — використовується разом з прапором -G, для того, щоб вказати, що ми хочемо додати вказані групи до вже вказаних у користувача. -l, --login — змінити ім'я користувача -p, --password — змінити пароль користувача, приймає строку, що містить зашифрований пароль.