

Linux. Спеціалізовані ОС (Kali, Parrot, Tails).



- Linux - операційна система, створена в 1991 році.
- Linux - це відкритий код, швидкий, надійний і невеликий, вимагає для роботи дуже мало апаратних ресурсів, і його можна легко налаштувати.
- На відміну від інших операційних систем, таких як Windows і Mac OS X, Linux було створено і в даний час підтримується спільнотою програмістів.
- Linux є частиною декількох платформ і може використовуватися на пристроях де завгодно, від «наручних годинників до суперкомп'ютерів».
- Іншим важливим аспектом Linux є те, що він розроблений для підключення до мережі, що значно спрощує написання та використання мережевих додатків.
- Оскільки Linux є відкритим кодом, будь-яка особа або компанія може отримати вихідний код ядра, перевірити його, змінити та повторно скомпілювати за власним бажанням. Їм також дозволяється розповсюджувати програму з оплатою або без.
- Дистрибутив Linux - термін, що використовується для опису пакетів, створених різними організаціями. Дистрибутиви Linux включають **ядро** Linux зі спеціальними інструментами та **програмними пакетами**. Хоча деякі з цих організацій можуть брати плату за підтримку дистрибуції Linux (орієнтовану на бізнес на базі Linux), більшість з них також пропонують розповсюдження безкоштовно без підтримки.
- **Debian, Red Hat, Ubuntu, CentOS** та **SUSE** - лише кілька прикладів дистрибутивів Linux орієнтованих на серверну інфраструктуру.

Linux часто використовують в Центрі забезпечення безпеки

(**SOC** - Security Operations Center) бо :

- Linux є **відкритим кодом** - будь-яка людина може безкоштовно придбати Linux та змінити його відповідно до конкретних потреб. Ця гнучкість дозволяє аналітикам та адміністраторам створювати операційні системи спеціально для аналізу безпеки.
- **CLI** для Linux дуже потужний - хоча графічний інтерфейс полегшує виконання багатьох завдань, він додає складності та вимагає більшої кількості комп'ютерних ресурсів. Інтерфейс командного рядка Linux (CLI) надзвичайно потужний і дозволяє аналітикам виконувати завдання не тільки безпосередньо на терміналі, але й віддалено.
- Користувач має **більший контроль** над ОС - адміністратор в Linux – root-користувач, або суперкористувач, має абсолютну владу над комп'ютером. На відміну від інших операційних систем, користувач **root** може змінити будь-який аспект комп'ютера за допомогою декількох натискань клавіш. Ця здатність особливо цінна при роботі з такими функціями низького рівня, як мережевий стек. Це дозволяє кореневому користувачеві мати повний контроль над тим, як операційна система оброблятиме мережеві пакети.
- Це дозволяє поліпшити **управління мережевим зв'язком** - управління є невід'ємною частиною Linux. Оскільки ОС можна налаштувати практично в кожному аспекті, це чудова платформа для створення мережевих додатків. Завдяки цьому багато чудових мережевих програмних засобів доступні лише для Linux.

Гнучкість, яку надає Linux, є чудовою функцією для SOC.

Вся операційна система може бути адаптована для того, щоб стати ідеальною платформою аналізу безпеки. Для прикладу, адміністратори можуть додавати в ОС лише необхідні пакети, роблячи її стрункою та ефективною. Можуть бути встановлені та налаштовані спеціальні програмні засоби, які працюють спільно, що дозволяє адміністраторам створити власний комп'ютер, який ідеально вписується в робочий процес SOC.

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2020-05-12 18:49:59 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	7	seconion-...	5.1583	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET INFO Dotted Quad Host HTA ...
RT	7	seconion-...	5.1584	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET POLICY Possible HTA Applica...
RT	1	seconion-...	5.1599	2020-05-10 21:29:13	209.165.201.17	52460	209.165.200.235	80	6	ET TROJAN Probable OneLoudner ...
RT	1	seconion-...	5.1600	2020-05-10 21:29:13	209.165.201.17	52468	209.165.200.235	80	6	ET WEB_SERVER Possible Cher...
RT	7	seconion-...	7.1896	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET INFO Dotted Quad Host HTA ...
RT	7	seconion-...	7.1897	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET POLICY Possible HTA Applica...
RT	1	seconion-...	7.1912	2020-05-10 21:29:13	209.165.201.17	52460	209.165.200.235	80	6	ET TROJAN Probable OneLoudner ...
RT	1	seconion-...	7.1913	2020-05-10 21:29:13	209.165.201.17	52468	209.165.200.235	80	6	ET WEB_SERVER Possible Cher...
RT	1	seconion-...	5.1679	2020-05-10 21:29:49	209.165.201.17	52836	209.165.200.235	80	6	ET WEB_SERVER /bin/bash In U...
RT	1	seconion-...	7.1992	2020-05-10 21:29:49	209.165.201.17	52836	209.165.200.235	80	6	ET WEB_SERVER /bin/bash In U...
RT	49	seconion-...	7.1998	2020-05-10 21:29:52	209.165.201.17	52896	209.165.200.235	80	6	ET WEB_SERVER /bin/sh In URI ...
RT	49	seconion-...	5.1701	2020-05-10 21:29:52	209.165.201.17	52896	209.165.200.235	80	6	ET WEB_SERVER /bin/sh In URI ...
RT	1	seconion-...	5.1770	2020-05-10 21:41:13	209.165.201.17	38782	209.165.200.235	3306	6	ET SCAN Suspicious inbound to ...

IP Resolution Agent Status Snort Statistics System Msgs

Sid	Net	Hostname	Type	Last
1	seconion-os...	seconion-os...	ossec	2020-05-12
2	seconion-en...	seconion-en...	pcap	2020-05-12
3	seconion-en...	seconion-en...	snort	2020-05-10
4	seconion-en...	seconion-en...	pcap	2020-05-12
5	seconion-en...	seconion-en...	snort	2020-05-10
6	seconion-en...	seconion-en...	pcap	2020-05-12
7	seconion-en...	seconion-en...	snort	2020-05-10

Update Interval (secs): 15 NOW

Show Packet Data Show Rule

alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET TROJAN Probable OneLoudner downloader (Zeus P2P)"; flow:to_server,established; content:"GET"; http_method;

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	209.165.201.17	209.165.200.235	4	5	0	172	50175	2	0	63	16900

TCP	Source Port	Dest Port	R R R C S S Y I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	52460	80	. . . X X . . .	2237277941	1593194311	8	0	501	0	30678

DATA	47 45 54 20 2F 31 31 20 48 54 54 50 2F 31 2E 31	0D 0A 48 6F 73 74 3A 20 32 30 39 2E 31 36 35 2E	32 30 30 2E 32 33 35 0D 0A 55 73 65 72 2D 41 67	65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30	20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53
	GET /11 HTTP/1.1 ..Host: 209.165. 200.235..User-Ag ent: Mozilla/4.0 (compatible; MS				

Search Packet Payload Hex Text NoCase

На малюнку показано
Sguil, який є консоллю
аналітика кібербезпеки
в спеціальній версії
Linux – **Security Onion**.

Security Onion - це набір інструментів з відкритим кодом, які працюють разом для аналізу мережевої безпеки. У таблиці перелічено кілька інструментів, які часто можна знайти у SOC.

інструмент SOC	Опис
Програмне забезпечення для захоплення мережевих пакетів	Найважливіший інструмент для аналітика SOC, оскільки він дозволяє спостерігати та розуміти кожну деталь мережевої транзакції - Wireshark - популярний інструмент захоплення та аналізу пакетів.
Інструменти аналізу шкідливого програмного забезпечення	Ці інструменти дозволяють аналітикам безпечно запускати та спостерігати за виконанням шкідливого програмного забезпечення без ризику пошкодити основну систему.
Системи виявлення вторгнень (IDS)	використовуються для моніторингу та перевірки Інтернет трафіку в режимі реального часу. Якщо будь-який аспект поточного потоку руху не відповідає будь-якому із встановлених правил, вживається заздалегідь визначена дія.
Брандмауери (firewall)	Це програмне забезпечення використовується для визначення, на основі заздалегідь визначених правил, чи дозволено трафік потрапляти в мережу чи пристрій чи виходити з неї.
Менеджери журналів (аналізатори)	Файли журналів використовуються для запису подій. Оскільки мережа може генерувати дуже велику кількість записів журналу, для полегшення моніторингу журналів використовується програмне забезпечення менеджера журналів.
Інформація про безпеку та управління подіями (SIEM - Security information and event management)	SIEM забезпечують аналіз у режимі реального часу попереджень та записів журналу, створених мережевими пристроями, такими як IDS та брандмауери.
Системи оформлення ticket (квитків)	Призначення, редагування та запис квитків виконуються через систему управління квитками. Попередження безпеки часто призначаються аналітикам через систему квитків.

Популярні дистрибутиви Linux для кібербезпеки:

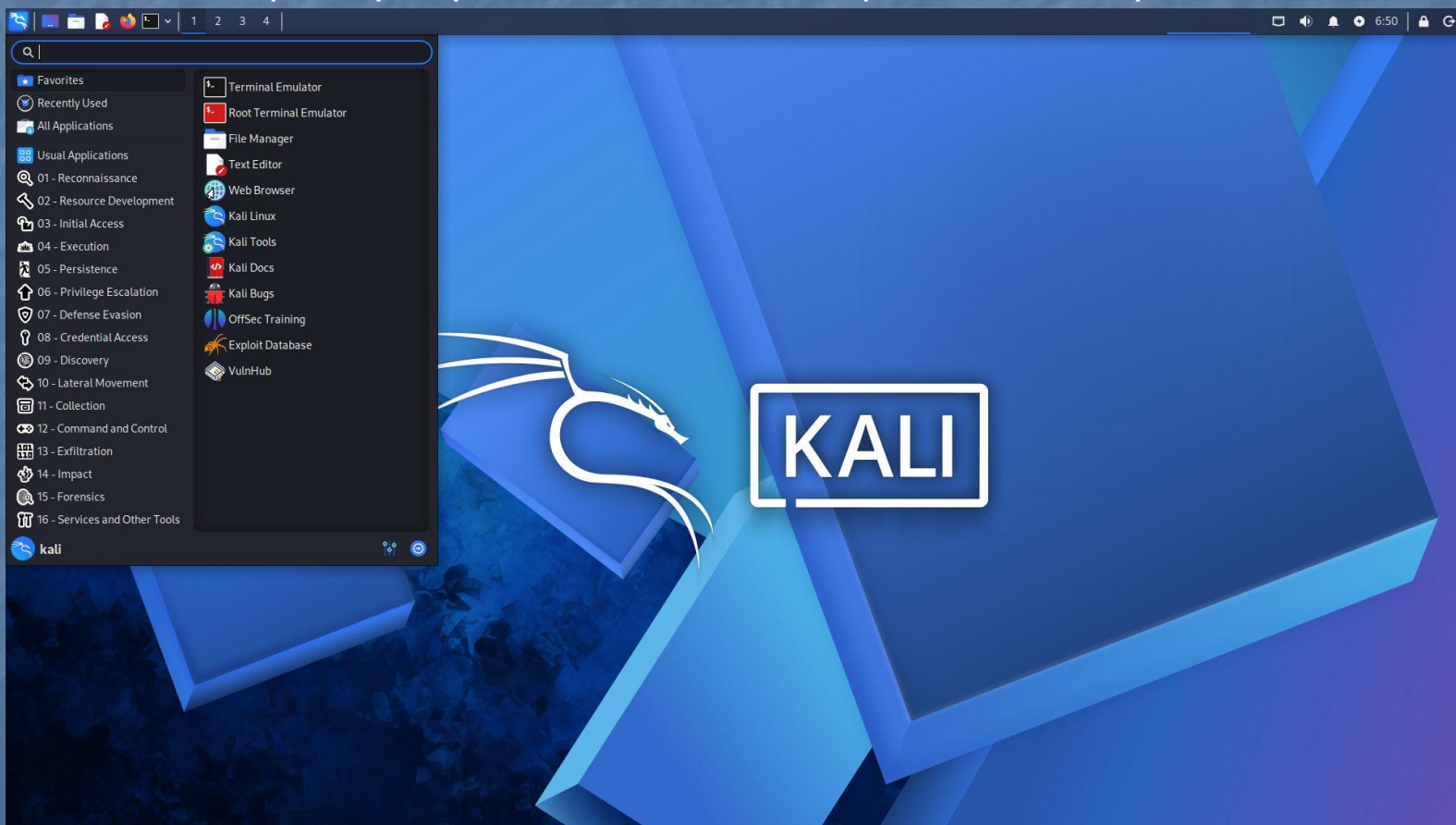
- **Kali Linux**
- **Black Arch**
- **Parrot Security OS**
- **Tails**
- **Кастомні OS на базі ядра Debian або Arch**

Окрім специфічних інструментів, комп'ютери під Linux часто містять інструменти тестування на проникнення, відомі як **PenTesting**.

Тест на проникнення - це процес пошуку вразливостей у мережі або комп'ютері шляхом їх атаки.

Генератори пакетів, сканери портів та експлойти, що підтверджують концепцію, є прикладами інструментів PenTesting.

Kali Linux – це дистрибутив Linux, який об'єднує в одній системі багато інструментів тестування на проникнення. Kali містить великий вибір інструментів. На малюнку показано знімок екрана Kali Linux. Зверніть увагу на всі основні категорії засобів тестування на проникнення.



Black Arch – це спеціалізований дистрибутив Linux на базі [Arch Linux](#), розроблений для тестування на проникнення (пентестингу), реверс-інжинірингу та дослідження кібербезпеки. Він є головним конкурентом Kali Linux, але орієнтований на більш досвідчених користувачів, які цінують гнучкість та мінімалізм.

```
root@blackarch: ~  
[ blackarch ~ ]# sploitctl -H  
usage:  
  sploitctl.sh -f <arg> | -s <arg> [options] | <misc>  
  
options:  
  -f <num>    - download and extract exploit archives from chosen  
                websites - ? to list sites  
  -s <str>    - exploit to search for using <str> pattern match  
  -w <str>    - exploit to search in web exploit site  
  -e <dir>    - exploit directory (default: /usr/share/exploits)  
  -b <url>    - give a new base url for packetstorm  
                (default: http://dl.packetstormsecurity.com/)  
  -l <file>   - give a new base path/file for website list option  
                (default: /usr/share/sploitctl/web/url.lst)  
  -c          - do not delete downloaded archive files  
  -n          - turn off colors  
  -v          - verbose mode (default: off)  
  -d          - debug mode (default: off)  
  
misc:  
  -V          - print version of packetstorm and exit  
  -H          - print this help and exit  
[ blackarch ~ ]# sploitctl -f ?  
[*] available exploit sites  
-> 0 - all exploit sites  
-> 1 - exploit-db.com  
-> 2 - packetstormsecurity.org  
-> 3 - m00-exploits (github)  
[ blackarch ~ ]#
```

applications	armitage
terminals	teamsserver
browsers	blueranger
network	cewl
	cewl-fab
blackarch	checksec
anti-forensic	checksec
automation	clusterd
backdoor	crunch
binary	dumb0
bluetooth	fstealer
code-audit	gooscan
cracker	hackersh
crypto	intersect-create
cryptography	unix-boss-autopwn
database	win-boss-autopwn
debugger	mitmap.sh
decompiler	mutator
defensive	nfspy
disassembler	nfspysh
dos	nfsshell
drone	panoptic
exploitation	regeorg
fingerprint	ramangler
firmware	sakis3g
forensic	shellme
fuzzer	simple-ducky
gpu	svcrack
hardware	svcrash
honeypot	svmap
keylogger	svreport
malware	svwar
misc	sn00p
mobile	sploitctl
network	ssl-phuck3r
networking	tiger
nfc	tigercron
packer	tigexp
proxy	getpermit
recon	md5
reversing	realpath
scanner	snefru
sniffer	testsuid
social	tissled
More...	More...

```
unix-privsc-check  
username-anarchy  
username  
veil  
voiphopper  
wnmap  
yinjector
```

Parrot Security OS – це ще один топовий дистрибутив для кібербезпеки, але на відміну від суворого хакерського BlackArch, він базується на Debian і розроблений з акцентом на конфіденційність (privacy), анонімність та повсякденну зручність. Його часто називають головною і більш «легкою» альтернативою Kali Linux.

The screenshot shows a terminal window titled "Parrot Terminal". The user has executed the command `$neofetch`. The output consists of two columns of ASCII art. The left column features a stylized cat face made of symbols like `@`, `#`, and `%`. The right column displays system information:

```

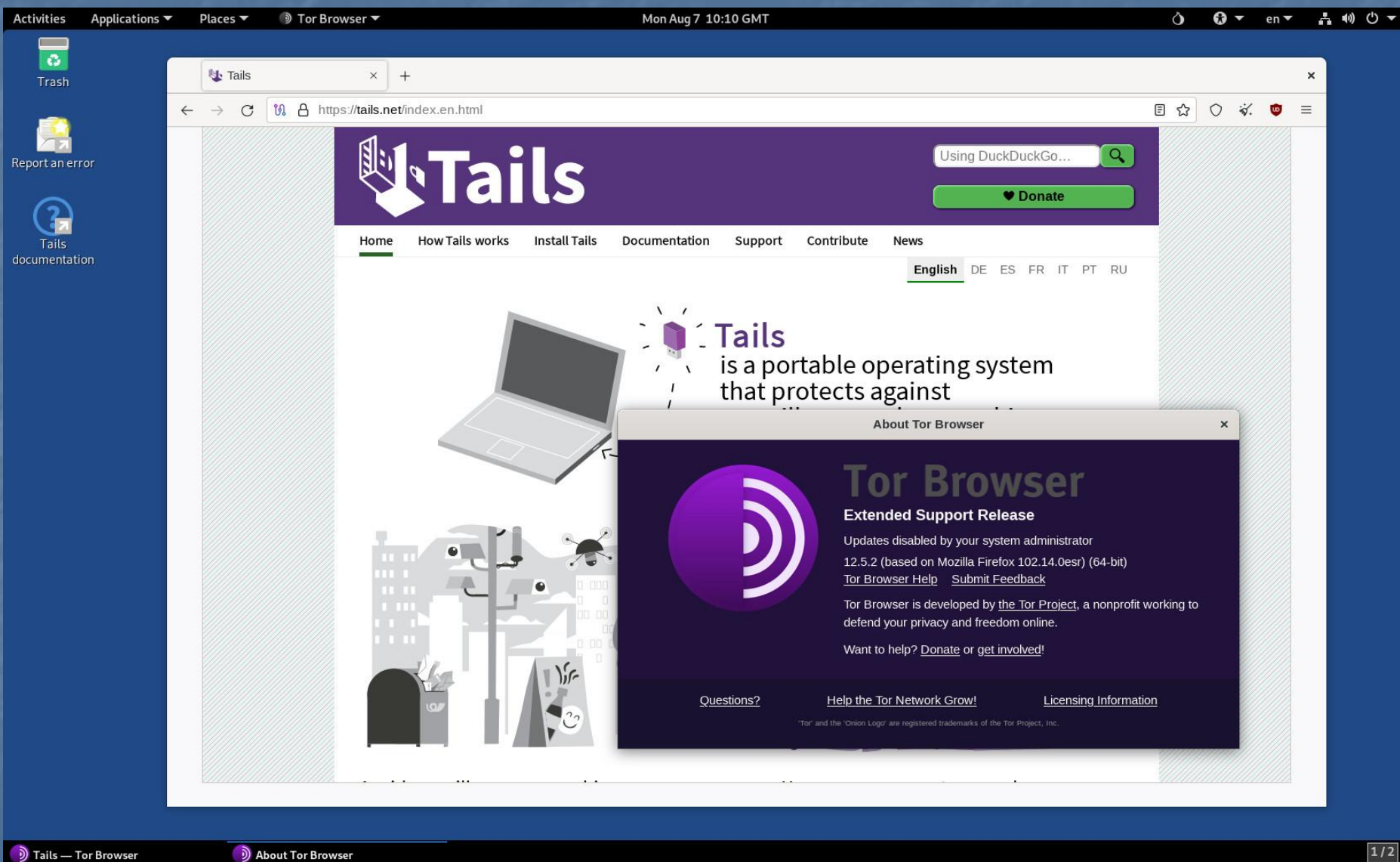
palinuro@parrot /~$ neofetch
      ,ohh/-'
      |
      |#####kandhy-
      |#####ns'
+MMsohh#####n/
.My .+c#####Mh.
+ :#####No
    'y#####:
      /N#####y'
      .h#####+
          '-N#####d-
              /N#####s'
                  r#####yNM/
                      +#####o :sNh.
                          N##### -o/
                              o#####.
                                  'N#####+
                                      -NMd/NM+
                                          mMa -m\
                                              /NM `h:
                                                  dM'
                                                      :M-
                                                          d:
                                                              +-
                                                                  -

OS: Parrot Security 6.2 (lorikeet) x86_64
Host: Laptop 13 (AMD Ryzen 7840Series) A7
Kernel: 6.11.5+bpo-amd64
Uptime: 2 hours, 29 mins
Packages: 4661 (dpkg), 42 (flatpak)
Shell: bash 5.2.15
Resolution: 2256x1504
DE: MATE 1.26.0
WM: Metacity (Marco)
Theme: ARK-Dark [GTK2/3]
Icons: ara [GTK2/3]
Terminal: mate-terminal
Terminal Font: Monospace 13
CPU: AMD Ryzen 7 7840U w/ Radeon 780M Graphics {16} @ 5.132GHz
GPU: AMD ATI c1:00.0 Phoenix1
Memory: 4726MiB / 31401MiB
  
```

At the bottom of the terminal, there is a color calibration bar with nine squares: black, red, green, yellow, cyan, blue, magenta, white, and grey.



Tails (The Amnesic Incognito Live System) — це абсолютно унікальний дистрибутив Linux на базі Debian, який кардинально відрізняється від BlackArch чи Parrot OS. Його головна мета — **не хакінг чи пентест, а відносна анонімність, захист від стеження та цензури.**



У Linux користувач спілкується з ОС за допомогою **CLI** (Command-line interface) або **GUI** (Graphical user interface).

Linux часто запускається в графічному інтерфейсі за замовчуванням.

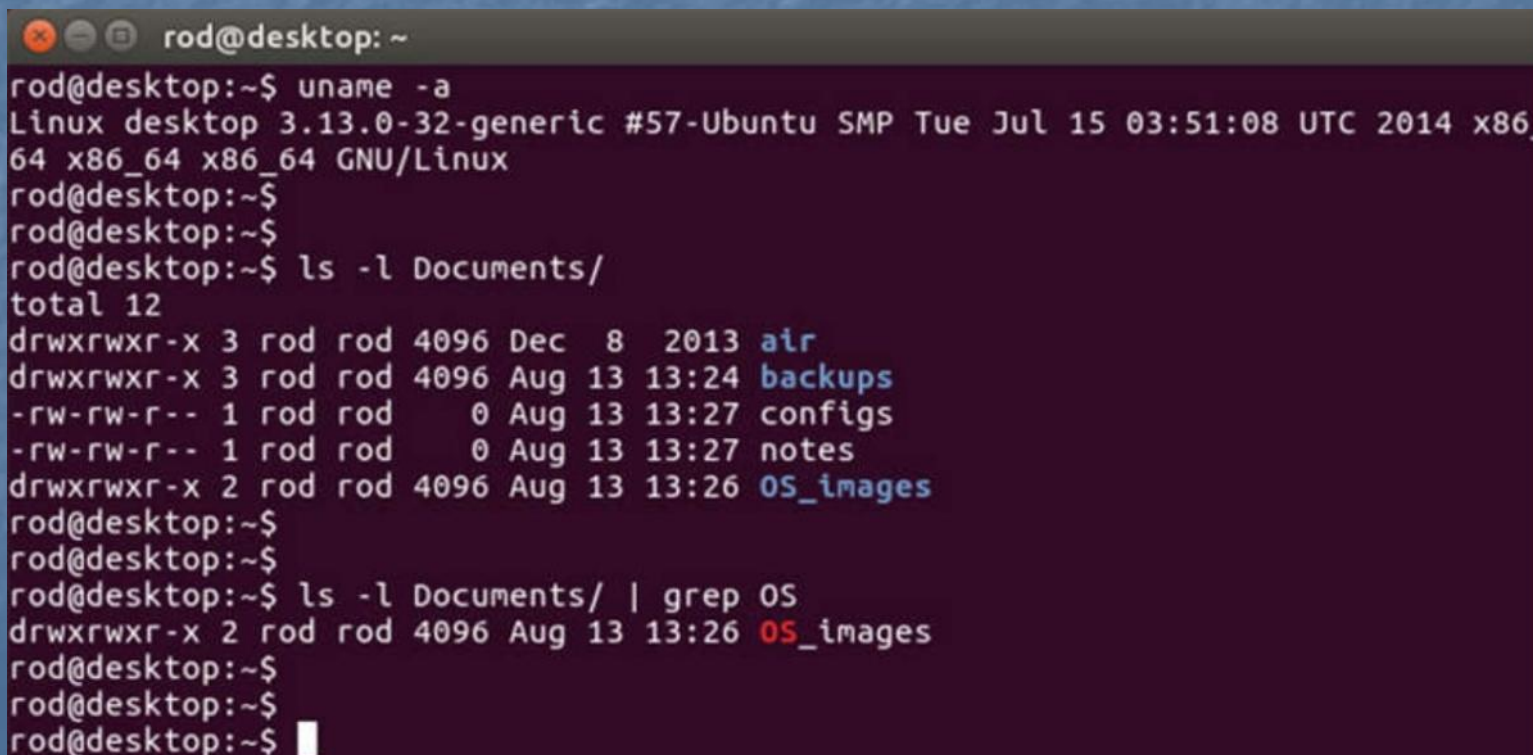
Це приховує CLI від користувача.

Один із способів отримати доступ до CLI із графічного інтерфейсу - це програма емулятора терміналу [terminal emulator application](#).

Ці програми надають користувачеві доступ до CLI і часто називаються якимсь різновидом слова "термінал".

У Linux популярними емуляторами терміналів є **Terminator**, **eterm**, **xterm**, **konsole** та **gnome-terminal**, **xfce4-terminal**, **parrot-terminal** та інші.

Фабріс Беллард створив **JSLinux**, що дозволяє емульованій версії Linux працювати в браузері. У вільному доступі в Інтернеті.



```
rod@desktop:~$ uname -a
Linux desktop 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_
64 x86_64 x86_64 GNU/Linux
rod@desktop:~$
rod@desktop:~$
rod@desktop:~$ ls -l Documents/
total 12
drwxrwxr-x 3 rod rod 4096 Dec  8  2013 air
drwxrwxr-x 3 rod rod 4096 Aug 13 13:24 backups
-rw-rw-r-- 1 rod rod   0 Aug 13 13:27 configs
-rw-rw-r-- 1 rod rod   0 Aug 13 13:27 notes
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images
rod@desktop:~$
rod@desktop:~$
rod@desktop:~$ ls -l Documents/ | grep OS
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images
rod@desktop:~$
rod@desktop:~$
rod@desktop:~$
```

На малюнку
показано
**gnome-
terminal**,
популярний
емулятор
терміналу
Linux

Основні команди

команда **man** (скорочення від [manual](#)), щоб отримати документацію про команди.

Як приклад, [man ls](#) надає документацію про команду ls з посібника користувача.

Оскільки команди - це програми, що зберігаються на диску, коли користувач вводить команду, оболонка повинна знайти її на диску, перш ніж її можна буде виконати.

Оболонка буде шукати команди, що вводяться користувачем, у конкретних каталогах і намагатись їх виконати. Список каталогів, які перевіряє оболонка, називається шляхом. Шлях містить багато каталогів, які зазвичай використовуються для зберігання команд. Якщо команди немає в шляху, користувач повинен вказати її розташування, інакше оболонка не зможе її знайти. Користувачі можуть легко додавати каталоги до шляху, якщо це необхідно. Нижче наведено деякі команди Linux і функції.

mv	Переміщує або перейменовує файли та каталоги
chmod	Змінює дозволи файлу
chown	Змінює право власності на файл
dd	Копіює дані з входу на вихід
pwd	Відображає ім'я поточного каталогу
ps	Перераховує процеси, які в даний час працюють у системі
sudo	Запускає команду як суперкористувач за замовчуванням або як інший іменований користувач
grep	Використовується для пошуку певних рядків символів у файлі або інших командних результатах. Для пошуку результатів попередньої команди grep повинен бути розміщений в кінці попередньої команди.
apt-get / apt	Використовується для встановлення, налаштування та видалення пакетів на Debian та його похідних.
iwconfig	Використовується для відображення або налаштування інформації, пов'язаної з бездротовою мережевою картою. Подібно до ifconfig , iwconfig відображатиме інформацію про бездротові мережі, коли видаватиметься без параметрів.
Shutdown	Вимикає систему, після завершення роботи може бути доручено виконати ряд завдань, пов'язаних із вимкненням, включаючи перезавпуск, зупинку, переведення в режим сну або вимкнення всіх підключених користувачів.
passwd	Використовується для зміни пароля. Якщо параметри не вказані, passwd змінює пароль поточного користувача.
cat	Використовується для переліку вмісту файлу і в якості параметра очікує ім'я файлу. Команда cat зазвичай використовується для текстових файлів.
man	Використовується для відображення документації для певної команди.

файлові команди та каталогів

Багато інструментів командного рядка включені в Linux за замовчуванням. Щоб відрегулювати командну операцію, користувачі можуть передавати параметри та перемикачі разом із командою.

команди	Опис
ls	Відображає файли всередині каталогу
cd	Змінює поточний каталог
mkdir	Створює каталог у поточному каталозі
cp	Копіює файли від джерела до місця призначення
mv	Переміщує файли в інший каталог
rm	Видаляє файли
grep	Шукає певні рядки символів у файлі або на виході інших команд
cat	Перераховує вміст файлу та очікує ім'я файлу як параметр

Linux має безліч різних текстових редакторів з різними функціями. Деякі текстові редактори включають графічні інтерфейси, тоді як інші є інструментами лише командного рядка. Кожен текстовий редактор включає набір функцій, призначений для підтримки певного типу завдань. Деякі текстові редактори призначені для програмістів та включають такі функції, як підсвічування синтаксису, дужки та перевірка дужок та інші функції, орієнтовані на програмування. Хоча графічні текстові редактори зручні та прості у використанні, текстові редактори на основі командного рядка дуже важливі для користувачів Linux. Головна перевага текстових редакторів на основі командного рядка полягає в тому, що вони дозволяють редагувати текстові файли з віддаленого комп'ютера. **Nano** - популярний текстовий редактор командного рядка.

Сервери та клієнти Linux.

Сервери - це комп'ютери з встановленим програмним забезпеченням, яке дозволяє їм надавати послуги клієнтам по всій мережі.

Існує безліч видів послуг. Деякі надають клієнтам за запитом зовнішні ресурси, такі як файли, повідомлення електронної пошти або веб-сторінки. Інші служби виконують такі завдання технічного обслуговування, як управління журналами, управління пам'яттю, сканування дисків

Кожна послуга вимагає окремого серверного програмного забезпечення.

Для того, щоб комп'ютер міг бути сервером для кількох служб, використовуються порти.

Порт - це зарезервований мережевий ресурс, який використовується службою.

Кажуть, що сервер «прослуховує» порт, коли він приєднався до цього порту.

Хоча адміністратор може вирішити, який порт використовувати з будь-якою службою, багато клієнтів налаштовані на використання певного порту за замовчуванням.

У таблиці перелічено кілька часто використовуваних портів та їхні послуги.

20/21	(FTP) Протокол передачі файлів
22	захищена оболонка (SSH)
23	Служба віддаленого входу в Telnet
25	Простий протокол пересилання пошти (SMTP)
53	Система доменних імен (DNS)
67/68	Протокол динамічної конфігурації хосту (DHCP)
69	Тривіальний протокол передачі файлів (TFTP)
80	Протокол передачі гіпертексту (HTTP)
110	Протокол поштового відділення, версія 3 (POP3)
123	Мережевий протокол часу (NTP)
143	Протокол доступу до Інтернет-повідомлень (IMAP)
161/162	Простий протокол управління мережею (SNMP)
443	HTTP Secure (HTTPS)

Клієнти - це програми або прикладення, призначені для спілкування з певним типом сервера. Також відомі як клієнтські програми, клієнти використовують чітко визначений протокол для зв'язку з сервером.

Веб-браузери - це веб-клієнти, які використовуються для зв'язку з веб-серверами через протокол передачі гіпертексту (HTTP) на порту 80.

Клієнт протоколу передачі файлів (FTP) - це програмне забезпечення, що використовується для зв'язку з сервером FTP.

Основи адміністрування сервера

У Linux службами керують за допомогою файлів конфігурації.

Загальними параметрами у файлах конфігурації є номер порту, розташування розміщених ресурсів та деталі авторизації клієнта.

Коли служба запускається, вона шукає свої конфігураційні файли, завантажує їх у пам'ять та налаштовує відповідно до налаштувань у файлах.

Зміни файлів конфігурації часто вимагають перезапуску служби до того, як зміни набудуть чинності.

Оскільки для запуску служб часто потрібні привілеї суперкористувача, відповідно це необхідно і для редагування файлів конфігурації служб.

Немає правил щодо формату файлу конфігурації – це вибір розробника послуги.

Однак часто використовується формат `option = value.`

Захист пристрою передбачає впровадження перевірених методів захисту пристрою та захисту його адміністративного доступу.

Деякі з цих методів включають підтримку паролів, налаштування розширених функцій віддаленого входу та впровадження безпечного входу за допомогою SSH.

Визначення адміністративних ролей з точки зору доступу є ще одним важливим аспектом захисту пристроїв інфраструктури, оскільки не всі працівники повинні мати однаковий рівень доступу до пристроїв інфраструктури.

Залежно від дистрибутива Linux, багато служб увімкнено за замовчуванням.

Зупинка таких служб та забезпечення того, щоб вони не запускались автоматично під час завантаження - ще одна техніка зміцнення пристрою.

Оновлення ОС також надзвичайно важливі для підтримки безпеки пристрою. Щодня виявляються нові вразливості. Розробники ОС регулярно створюють та видають виправлення. Оновлене ПЗ комп'ютера менш схильне до компрометації.

Нижче наведено основні найкращі методи укріплення пристрою.

- Забезпечити фізичну безпеку
- Мінімізувати встановлені пакети
- Вимкнути невикористовувані послуги
- Використовувати SSH та відключіть вхід до кореневого облікового запису через SSH
- Систематично оновлювати систему
- Вимкнути автоматичне виявлення USB
- Застосовуйте надійні паролі
- Примусово періодично змінюйте пароль
- Не дайте користувачам повторно використовувати старі паролі

Існує багато інших кроків, які часто залежать від послуг чи програм.

Файли журналів - це записи, які комп'ютер зберігає для відстеження важливих подій.

Ядро, служби та події додатків записуються у файли журналів. Для адміністратора дуже важливо періодично переглядати журнали комп'ютера, щоб підтримувати його дієздатність. Відстежуючи файли журналів Linux, адміністратор отримує чітке уявлення про продуктивність комп'ютера, стан безпеки та всі основні проблеми.

Аналіз файлів журналів дозволяє адміністратору захищатися від майбутніх проблем до їх виникнення.

У Linux файли журналів можна класифікувати як:

- Журнали програм
- Журнали подій
- Журнали обслуговування
- Системні журнали

Деякі журнали містять інформацію про демони, які працюють у системі Linux.

Демон - це фоновий процес, який працює без необхідності взаємодії з користувачем.

Наприклад, демон системних служб безпеки (SSSD - System Security Services Daemon) керує віддаленим доступом та автентифікацією для можливостей єдиного входу.

У таблиці нижче перелічено кілька популярних файлів журналів Linux та їх функції

Захист пристрою передбачає [впровадження перевірених методів захисту](#). Вихідні дані команди відображають частину файлу журналу `/var/log/messages`. Кожен рядок представляє зареєстровану подію.

Мітки часу на початку рядків позначають момент, коли відбулася подія.

Linux Log File	Опис файлу
<code>/var / log / messages</code>	• Цей каталог містить загальні журнали діяльності комп'ютера. • В основному використовується для зберігання інформаційних та некритичних системних повідомлень. • На комп'ютерах, що базуються на Debian, каталог <code>/var / log / syslog</code> виконує ті ж цілі.
<code>/var/log/auth.log</code>	• файл зберігає всі події, пов'язані з автентифікацією, на комп'ютерах Debian та Ubuntu. • У цьому файлі можна знайти все, що стосується механізму авторизації користувачів.
<code>/var / log / secure</code>	• Цей каталог використовується комп'ютерами RedHat та CentOS замість <code>/var/log/auth.log</code>. • Він також відстежує sudo логіни, SSH логіни та інші помилки, зареєстровані SSSD.
<code>/var/log/boot.log</code>	• Цей файл зберігає інформацію, пов'язану із завантаженням, та повідомлення, записані під час запуску комп'ютера.
<code>/var / log / dmesg</code>	• Цей каталог містить повідомлення буфера ядра. • Тут записана інформація, що стосується апаратних пристроїв та їх драйверів. • Це дуже важливо, оскільки через свою низькорівневу природу системи реєстрації, такі як syslog, не працюють, коли відбуваються ці події, а тому часто недоступні адміністратору в режимі реального часу.
<code>/var/log/kern.log</code>	• Цей файл містить інформацію, записану ядром.
<code>/var / log / cron</code>	• Cron - це служба, яка використовується для планування автоматизованих завдань у Linux, і цей каталог зберігає свої події. • Щоразу, коли виконується заплановане завдання (яке також називається завданням cron), тут зберігається вся його відповідна інформація, включаючи стан виконання та повідомлення про помилки.
<code>/var/log/mysqld.log</code> Або <code>/var/log/mysql.log</code>	• Це файл журналу MySQL. • Усі повідомлення про налагодження, помилки та успіх, пов'язані з процесом mysqld та демоном mysqld_safe, реєструються тут. • Дистрибутиви RedHat, CentOS та Fedora Linux зберігають журнали MySQL у розділі <code>/var/log/mysqld.log</code>, тоді як Debian та Ubuntu підтримують файл входу <code>/var/log/mysql.log</code>.

Файлова система Linux

файлова система Linux	Опис
Ext2	- ext2 була файловою системою за замовчуванням у кількох основних дистрибутивах Linux, поки ext3 не витіснила її. - Практично повністю сумісна з ext3 також підтримує ведення журналів . - ext2 все ще залишається обраною файловою системою для носіїв даних на базі флеш-пам'яті, оскільки відсутність журналу підвищує продуктивність та мінімізує кількість записів. - Оскільки пристрої флеш-пам'яті мають обмежену кількість операцій запису, мінімізація операцій запису збільшує термін служби пристрою. • Однак сучасні ядра Linux також підтримують ext4, ще більш сучасну файлову систему, з кращою продуктивністю, яка також може працювати в режимі без журналу.
Ext3	- ext3 - це журнальна файлова система, призначена для вдосконалення існуючої файлової системи ext2. - Журнал, головна особливість яка додається до ext3, - це методика, що використовується для мінімізації ризику пошкодження файлової системи у разі раптової втрати енергії. - Файлові системи ведуть журнал усіх змін файлової системи, які мають бути зроблені. • Якщо комп'ютер аварійно завершує роботу до завершення змін, журнал може бути використаний для відновлення або виправлення будь-яких можливих проблем, створених аварією. • Максимальний розмір файлу у файлових системах ext3 становить 32 ТБ.
ext4	- Розроблена як наступниця ext3, ext4 була створена на основі серії розширень до ext3. - Хоча розширення покращують продуктивність ext3 та збільшують підтримувані розміри файлів, розробники ядра Linux були стурбовані проблемами стабільності і виступали проти додавання розширень до стабільного ext3. Проект ext3 був розділений на дві частини; один зберігається як ext3 та його нормальний розвиток, а інший, названий ext4, включає згадані розширення.
NFS (мережева файлова система)	- NFS - це мережева файлова система, що забезпечує доступ до файлів через мережу. - З точки зору користувача, немає різниці між доступом до файлу, що зберігається локально або на іншому комп'ютері в мережі. • NFS - це відкритий стандарт, який дозволяє будь-кому впровадити його.
CDFS (компакт-дискова файлова система)	CDFS була створена спеціально для оптичних дискових носіїв.
Файлова система підкачки	- Файлова система підкачки використовується Linux, коли у неї закінчується оперативна пам'ять. - Технічно це розділ підкачки, який не має певної файлової системи, але він має відношення до обговорення файлової системи. - Коли це трапляється, ядро переміщує неактивний вміст оперативної пам'яті до розділу підкачки на диску. - Незважаючи на те, що розділи підкачки (також відомі як простір підкачки) можуть бути корисними для комп'ютерів Linux з обмеженим обсягом пам'яті, їх не слід розглядати як основне рішення. - Розділ підкачки зберігається на диску, який має набагато нижчу швидкість доступу, ніж оперативна пам'ять.
HFS Plus або HFS + (ієрархічна файлова система Plus)	- Файлова система, що використовується Apple на комп'ютерах Macintosh. - Ядро Linux включає модуль для монтажу HFS + для операцій читання-запису.
APFS (Apple File System)	- Оновлена файлова система, яка використовується пристроями Apple. - Вона забезпечує надійне шифрування та оптимізована для флеш-накопичувачів та твердотільних накопичувачів.
Основний завантажувальний запис Master Boot Record (MBR)	Розташований у першому секторі розділеного комп'ютера, MBR зберігає всю інформацію про спосіб організації файлової системи. • MBR швидко передає контроль функції завантаження, яка завантажує ОС.

Існує багато різних типів файлових систем, які відрізняються за швидкістю, гнучкістю, безпекою, розміром, структурою, логікою

Адміністратор повинен вирішити, який тип файлової системи найкраще відповідає операційній системі та файлам, які він буде зберігати.

У таблиці вище перелічено кілька типів файлових систем, якими зазвичай користуються і підтримують Linux

Монтування - термін, яким називають процес присвоєння каталогу розділу. Після успішної операції монтування файлова система, що міститься в розділі, доступна через вказаний каталог.

У цьому контексті каталог називається точкою монтування для цієї файлової системи. Для користувачів Windows аналогія – буква диска.

Команда **mount**.

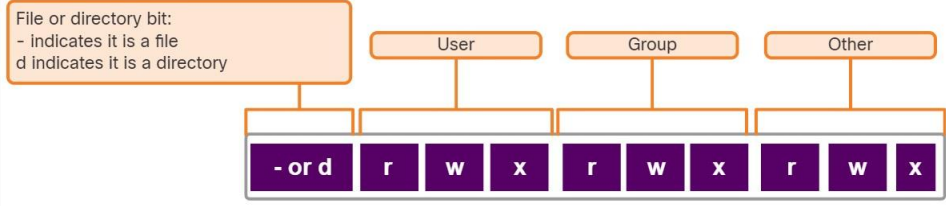
У разі задання без опцій, **mount** повертає список файлових систем, наразі змонтованих на комп'ютері Linux.

Коренева файлова система представлена символом “/” і за замовчуванням містить усі файли на комп'ютері.

коренева файлова система часто відформатована як **ext4** і займає перший розділ першого диска (**/ dev / sda1**).

У Linux більшість системних сутностей розглядаються як файли. Для того, щоб організувати систему та накласти обмеження на комп'ютер, Linux використовує дозволи на використання файлів. Файлові дозволи вбудовані в структуру файлової системи та забезпечують механізм визначення дозволів для кожного файлу. Кожен файл у Linux має свої дозволи, які визначають дії, які власник, група та інші можуть виконувати з файлом. Можливими правами дозволу є "Читати, писати та виконувати". Команда `ls -l` містить додаткову інформацію про файл. Розглянемо вихід команди `ls -l`

```
[analyst@secOps ~]$ ls -l space.txt
-rwxrw-r-- 1 analyst staff 253 May 20 12:49 space.txt
(1)(2)(3)(4)(5)(6)(7)
[analyst@secOps ~]$
```



Вихідні дані містять багато інформації про файл `space.txt`. Перше поле вихідних даних відображає дозволи, пов'язані з `space.txt` (`-rwxrw-r--`). Файлові дозволи завжди відображаються в порядку користувача, групи та іншого.

Файл `space.txt` має такі дозволи:

- Тире (-) означає, що це файл. Для каталогів першим символом буде `d`.
- Перший набір символів призначений для дозволу користувача (`rw`x). Користувач, аналітик, якому належить файл, може читати, писати та виконувати файл.
- Другий набір символів призначений для групових дозволів (`rw`-). Група, персонал, якому належить файл, може читати та записувати у файл.
- Третій набір символів призначений для будь-яких інших дозволів користувача або групи (`r--`). Будь-який інший користувач або група на комп'ютері може лише прочитати файл.

Друге поле визначає кількість жорстких посилань на файл (число 1 після дозволів). Жорстке посилання створює інший файл з іншим ім'ям, пов'язаний з тим самим місцем у файловій системі (так званий **inode**).

У третьому та четвертому полі відображаються відповідно користувач (**аналітик**) та група (**персонал**), яким належить файл.

П'яте поле відображає розмір файлу в байтах. Файл space.txt має **253** байти.

Шосте поле відображає дату та час останньої модифікації.

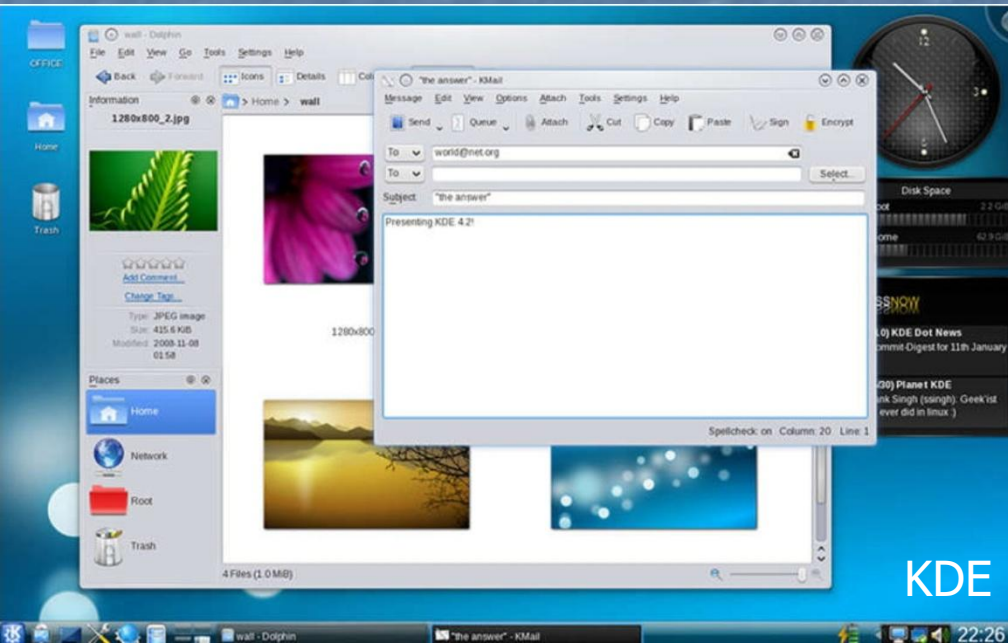
Сьоме поле відображає ім'я файлу.

```
[analyst@secOps ~]$ ls -l space.txt
-rwxrw-r-- 1 analyst staff 253 May 20 12:49 space.txt
(1)(2)(3)(4)(5)(6)(7)
[analyst@secOps ~]$
```

- Файлові дозволи є основною частиною Linux і не можуть бути порушені.
- Користувач має лише права на файл, дозволені цим дозволом.
- Єдиним користувачем, який може перевизначити дозвіл файлів на комп'ютері Linux, є користувач **root**.
- Оскільки кореневий користувач має можливість перевизначити дозволи файлів, він може писати в будь-який файл.
- Оскільки все обробляється як файл, користувач **root** має повний контроль над комп'ютером Linux.
- Кореневий доступ часто потрібен перед виконанням технічних та адміністративних завдань.
- Завдяки потужності кореневого користувача, кореневі облікові дані повинні використовувати надійні паролі і не передаватися нікому, крім системних адміністраторів та інших користувачів високого рівня.

Робота з графічним інтерфейсом Linux

Графічний інтерфейс, присутній у більшості комп'ютерів Linux, базується на системі X Window. Також відомий як X або X11. **X Window** - це система вікон, призначена для забезпечення базової основи графічного інтерфейсу. X включає функції для малювання та переміщення вікон на пристрої відображення та взаємодії з мишею та клавіатурою. X працює як сервер, що дозволяє віддаленому користувачеві використовувати мережу для підключення, запуску графічного додатка та відкриття графічного вікна на віддаленому терміналі. Поки сама програма працює на сервері, графічний аспект її надсилається X через мережу та відображається на віддаленому комп'ютері.



Зверніть увагу, що X не вказує користувальницький інтерфейс, залишаючи його іншим програмам, таким як менеджери вікон, для визначення всіх графічних компонентів. Ця абстракція забезпечує велику гнучкість та налаштування, оскільки графічні компоненти, такі як кнопки, шрифти, піктограми, межі вікон та кольорові схеми, визначаються програмою користувача. Через це розділення графічний інтерфейс Linux сильно відрізняється від розподілу до розподілу. Прикладами менеджерів вікон є **Gnome** та **KDE**. Хоча зовнішній вигляд менеджерів вікон різний, основні компоненти все ще присутні.

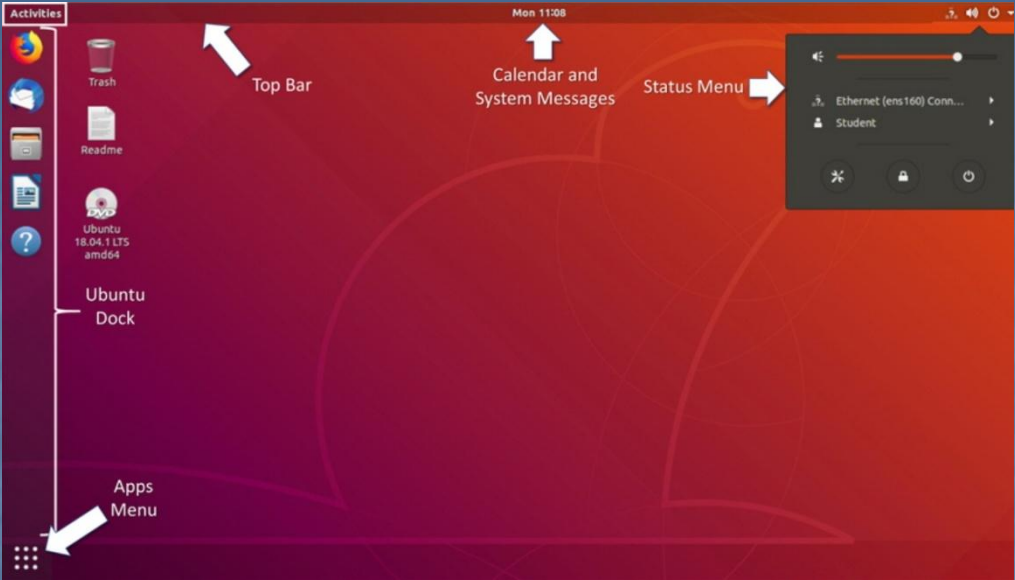
Хоча операційна система не потребує графічного інтерфейсу для функціонування, графічні інтерфейси вважаються більш зручними для користувача, ніж **CLI**.

Графічний інтерфейс Linux в цілому може бути легко замінений користувачем до прикладу на Xfce4, LXDE, Mate, LXQT, OpenBox, KDE.

Ubuntu Linux використовує **Gnome** як стандартний графічний інтерфейс.

Мета **Gnome** - зробити Ubuntu ще зручнішим для користувачів. У таблиці перелічені основні компоненти інтерфейсу користувача.

На малюнку показано розташування деяких функцій робочого столу Ubuntu Gnome 3.



компонент	інтерфейсу користувача	Опис
Меню програм		• У меню програм відображаються піктограми програм, які встановлені в системі. • Меню, клік правою кнопкою миші, містить ярлики, що дозволяють запускати або налаштовувати програми. • Вікно пошуку в системі доступне у вікні дій.
Док-станція Ubuntu		• Це док-станція в лівій частині екрана, яка служить панеллю запуску програм та перемикачем для вибраних програм. • Клацніть, щоб запустити програму, а коли програма працює, натисніть ще раз, щоб переключитися між запущеними програмами. • Якщо запущено кілька екземплярів програми, Launcher відображатиме всі екземпляри. • Клацніть правою кнопкою миші будь-яку програму, розміщену на панелі запуску, щоб переглянути деталі про цю програму.
Верхній рядок		• Цей багатофункціональний рядок меню містить меню програми, яка в даний у фокусі. • Він відображає поточний час і вказує, чи є нові системні повідомлення. • Він також надає доступ до перегляду робочого столу Activity та меню стану системи.
Календар та системна панель повідомлень		• Клацніть день та час, щоб переглянути повний календар зустрічей та будь-які поточні системні повідомлення. • Доступ до календаря зустрічей звідси, щоб створити нові зустрічі.
Діяльність		• Переключитись на режим перегляду програм, щоб перейти або закрити запущені програми. • Тут доступний потужний інструмент пошуку, який дозволяє знаходити програми, файли та значення у файлах. • Дозволяє перемикатися між робочими областями.
Меню стану		• Дозволяє конфігурувати мережевий адаптер та інші запущені пристрої. • Поточний користувач може вийти з системи або змінити свої налаштування. • Тут можна внести зміни в конфігурацію системи. • Звідси робочу станцію можна заблокувати або вимкнути.

Робота на хості Linux

Багато програм для кінцевих користувачів - це складні програми, написані компільованими мовами. Для полегшення процесу встановлення Linux часто включає програми, які називаються менеджерами пакетів.

Пакет - це термін, який використовується для позначення програми та всіх допоміжних файлів.

За допомогою диспетчера пакетів для встановлення пакету всі необхідні файли розміщуються у правильному розташуванні файлової системи.

Менеджери пакетів різняться залежно від дистрибутивів Linux. Наприклад, **pacman** використовується Arch Linux, **yum** використовується в CentOS тоді як **dpkg** (пакет Debian) та **apt** (Advanced Packaging Tool) використовуються в дистрибутивах Debian та Ubuntu Linux.

Постійне оновлення системи. Також відомі як виправлення, оновлення ОС періодично випускаються компаніями ОС для усунення будь-яких відомих вразливостей їх операційних систем. Поки компанії мають графіки оновлення, випуск позапланових оновлень ОС може відбуватися, коли в коді ОС виявляється критична вразливість. Сучасні операційні системи попереджатимуть користувача, коли оновлення доступні для завантаження та встановлення, але користувач може перевірити наявність оновлень у будь-який час. У наступній таблиці порівнюються команди розподілу Arch Linux та Debian / Ubuntu Linux для виконання основних операцій системи пакетів.

Завдання	Arch	Debian / Ubuntu
Встановіть пакет за назвою	<code>pacman -S</code>	<code>apt install</code>
Видаліть пакет за назвою	<code>pacman -Rs</code>	<code>apt remove</code>
Оновіть локальний пакет	<code>pacman -Syy</code>	<code>apt-get update</code>
Оновіть усі встановлені на даний момент пакети	<code>pacman -Syu</code>	<code>apt-get upgrade</code>

Processes and Forks

Процес - це запущений примірник комп'ютерної програми.
Багатозадачність операційних систем дозволяє виконувати багато процесів одночасно.
Форкінг - це метод, який ядро використовує, щоб дозволити процесу створити свою копію.
Процесам потрібен спосіб створення нових процесів у багатозадачних операційних системах.
Операція форкінгу - це єдиний спосіб зробити це в Linux.
Розгалуження важливо з багатьох причин. Один із них стосується масштабованості процесів.
Хорошим прикладом є популярний веб-сервер Apache. Форк-уючи себе, Apache може обслуговувати велику кількість запитів із меншою кількістю системних ресурсів, ніж сервер на основі одного процесу.
Коли процес викликає **fork**, він стає батьківським процесом, а нещодавно створений процес називається його дочірнім процесом. Після **forks**-у процеси є певною мірою незалежними процесами; вони мають різні ідентифікатори процесів, але запускають однаковий програмний код.
У таблиці перелічено три команди, які використовуються для управління процесами.

команди	опис
ps	- Використовується для переліку процесів, що працюють на комп'ютері під час його виклику. - Можна доручити відображати запущені процеси, що належать поточному користувачеві чи іншим користувачам. - Хоча перелік процесів не вимагає привілеїв root, виключення або зміна процесів інших користувачів вимагає.
top	Використовується для переліку запущених процесів, але на відміну від ps, top продовжує відображати запущені процеси динамічно.
kill	- Використовується для модифікації поведінки певного процесу. - Залежно від параметрів, kill може видалити, перезапустити або призупинити процес. - У багатьох випадках користувач запускає ps або top перед запуском kill. - Це робиться для того, щоб користувач міг вивчити PID процесу перед запуском kill.

Шкідливе програмне забезпечення (malware) на хості Linux

До шкідливих програм Linux належать **віруси**, **троянські коні**, **хробаки** та інші типи шкідливих програм, які можуть впливати на операційну систему.

Через низку компонентів дизайну, таких як структура файлової системи, дозволи на файли та обмеження облікових записів користувачів, операційні системи Linux, як правило, вважаються краще захищеними від шкідливих програм.

Але Linux не абсолютно захищений від шкідливих програм.

У Linux виявлено та використано багато вразливих місць.

Вони варіюються від серверного програмного забезпечення до вразливостей ядра.

Зловмисники здатні використовувати ці вразливості і компрометувати ціль.

Оскільки Linux є відкритим кодом, виправлення та оновлення часто стають доступними протягом декількох годин після виявлення таких проблем.

Якщо шкідлива програма буде виконана, це спричинить шкоду, незалежно від платформи.

Загальним вектором атак Linux є його послуги та процеси.

Вразливості часто зустрічаються в сервері та коді процесу, що працює на комп'ютерах, підключених до мережі.

Застаріла версія веб-сервера Apache може містити невиправлену вразливість, яку може використати зловмисник.

Наприклад, зловмисники часто перевіряють відкриті порти, щоб оцінити версію та характер сервера, що працює на цьому порту.

Маючи ці знання, зловмисники можуть дослідити, чи є якісь відомі проблеми з цією конкретною версією цього конкретного сервера для підтримки атаки.

Як і для більшості вразливостей, оновлення комп'ютера та закриття будь-яких невикористаних служб та портів є хорошим способом зменшити можливості для атак на комп'ютері Linux.

Перевірка руткіт-ів (Rootkit)

Руткіт - це тип шкідливого програмного забезпечення, призначений для збільшення привілеїв несанкціонованого користувача або надання доступу до частин програмного забезпечення, які зазвичай не повинні бути дозволені.

Руткіти також часто використовуються для захисту "задніх дверей" до скомпрометованого комп'ютера. Встановлення руткіта може бути автоматизовано (зроблено в рамках зараження) або зловмисник може встановити його вручну після компрометації комп'ютера.

Руткіт руйнівний, оскільки він змінює код ядра та його модулі, змінюючи найважливіші операції самої ОС. Завдяки такому глибокому рівню компромісу, руткіти можуть приховати вторгнення, видалити будь-які доріжки встановлення і навіть втрутитися в засоби усунення несправностей та діагностики, так що їх результати тепер приховують наявність руткіта.

Хоча кілька вразливостей Linux через історію дозволяли встановлювати руткіт за допомогою звичайних облікових записів користувачів, переважна більшість зламів руткітом вимагає доступу root або адміністратора.

Оскільки сама природа комп'ютера порушена, виявлення руткітів може бути дуже складним.

Типові методи виявлення часто включають завантаження комп'ютера з надійних носіїв, таких як діагностичний операційний центр із компакт-диска.

Зламаний диск встановлено, і з набору надійних системних інструментів можна запустити надійні засоби діагностики для перевірки пошкодженої файлової системи.

Методи перевірки включають поведінкові методи, сканування підписів, сканування різниць та аналіз дампа пам'яті.

Видалення руткітів може бути складним і часто неможливим, особливо у випадках, коли руткіт знаходиться в ядрі; **перевстановлення операційної системи**, як правило, є єдиним реальним рішенням проблеми.

Руткіти мікропрограми зазвичай вимагають заміни обладнання.

chkrootkit - це популярна програма на базі Linux, призначена для перевірки комп'ютера на наявність відомих руткітів. Це сценарій оболонки, який використовує загальні інструменти Linux, такі як рядки та **grep**, для порівняння підписів основних програм. Він також шукає розбіжності, коли проходить файлову систему, порівнюючи знайдені там підписи з результатом **ps**.

Хоча це корисно, майте на увазі, що програми для перевірки руткітів не є надійними на 100%.

Хоча інструменти командного рядка зазвичай призначені для виконання конкретного, чітко визначеного завдання, багато команд можуть поєднуватися для виконання більш складних завдань за допомогою техніки, відомої як **piping**.

Названа на честь його визначального символу, **pipe (|)**, **piping commands** складаються з ланцюгових команд, що подають результат (вихід) однієї команди на вхід іншої.

Наприклад, команда **ls** використовується для відображення всіх файлів і каталогів даного каталогу.

Команда **grep** порівнює пошук у файлі або тексті, шукаючи вказаний рядок.

Якщо знайдено, **grep** відображає весь вміст папки, де був знайдений рядок.

Дві команди, **ls** і **grep**, можна об'єднати в **piping**, щоб відфільтрувати вихідні дані **ls**.

Приклад **ls -l | grep host** та **ls -l | grep file**.

Висновки

Linux - це швидка, надійна та невелика операційна система з відкритим кодом.

Для його запуску потрібно небагато апаратних ресурсів, і його можна легко налаштувати.

Він призначений для використання в мережах.

Ядро Linux поширюється різними організаціями з різними інструментами та програмними пакетами.

Індивідуальна версія Linux, яка називається **Security Onion**, містить програмне забезпечення та інструменти, призначені для моніторингу безпеки мережі аналітиками кібербезпеки.

Kali Linux - це ще один налаштований дистрибутив Linux, який має безліч інструментів, призначених для тестування на проникнення мережевої безпеки.

У Linux користувач спілкується з операційною системою через графічний інтерфейс (**GUI**) або інтерфейс командного рядка (**CLI**).

Якщо графічний інтерфейс запущений, оболонка доступна через додаток терміналу, такий як термінал **xterm** або **gnome**.

Команди Linux - це програми, що виконують певне завдання.

Команда **man**, за якою слідує конкретна опція, забезпечує документацію для цієї команди.

Важливо знати принаймні основні команди Linux, команди файлів і каталогів, а також команди для роботи з текстовими файлами.

У Linux все обробляється так, якби це був файл, включаючи пам'ять, диски, монітор та каталоги.

Сервери - це комп'ютери, на яких встановлено програмне забезпечення, що дозволяє їм надавати послуги клієнтським комп'ютерам у всій мережі.

Деякі служби надають клієнтам доступ до зовнішніх ресурсів, таких як файли, електронна пошта та веб-сторінки, за запитом.

Інші служби працюють внутрішньо і виконують такі завдання, як управління журналами, керування пам'яттю або сканування диска.

Щоб комп'ютер міг надавати кілька служб, використовуються порти.

Порт - це зарезервований мережевий ресурс, який "прослуховує" запити клієнтів.

Хоча номер порту, який використовується службою, можна налаштувати, більшість служб слухають за замовчуванням "добре відомі" порти.

Клієнтські програми призначені для зв'язку з певними типами серверів.

Веб-браузери призначені для зв'язку з веб-серверами за допомогою протоколу HTTP на порту 80.

FTP-клієнти спілкуються з FTP-серверами для передачі файлів.

У Linux сервери управляються за допомогою **файлів конфігурації**.

Різні параметри можна змінювати та зберігати у файлах конфігурації.

Коли служба запущена, вона переглядає її конфігураційний файл (файли), щоб знати, як вона повинна працювати.

Немає правила написання конфігураційних файлів.

Формат файлу конфігурації залежить від творця серверного програмного забезпечення.

Пристрої Linux слід захищати за допомогою перевірених методів захисту пристрою та адміністративного доступу. Це називають укріплення пристроїв.

Одним із способів зміцнення пристрою є :

- підтримка паролів,
- налаштування розширених функцій входу та
- впровадження безпечного віддаленого входу за допомогою SSH.
- також дуже важливо постійно оновлювати операційну систему.

Інші способи зміцнення пристрою - це

- примусові періодичні зміни паролів,
- забезпечення надійних паролів та
- запобігання повторному використанню паролів.

Нарешті, клієнти та сервери Linux використовують журнали для запису роботи системи та важливих подій.

Ведеться ряд різних журналів, включаючи:

- журнали програм,
- журнали подій,
- журнали обслуговування та
- системні журнали.

Журнали сервера записують дії, які проводяться віддаленими користувачами, які отримують доступ до системних служб.

Важливо знати розташування різних журналів у файловій системі Linux, щоб вони могли отримувати доступ та контролювати наявність проблем.

Linux підтримує низку різних файлових систем, які відрізняються

- швидкістю,
- гнучкістю,
- безпекою,
- розміром,
- структурою,
- логікою тощо.

Деякі файлові системи, які підтримуються Linux, це ext2, ext3, ext4, NFS та CDFS.

Файлові системи монтуються як розділи та отримують доступ через точки монтування або як каталоги.

Букви диска Windows є прикладами точок монтування.

Команда **mount** може використовуватися для відображення деталей файлових систем, які в даний час встановлені на комп'ютері Linux.

Коренева файлова система представлена символом **"/**".

Він містить усі файли на комп'ютері за замовчуванням.

Linux використовує дозволи на файли, щоб контролювати, кому дозволено мати різні типи доступу до файлів і каталогів.

Дозволи включають читання (**r**), запис (**w**) та виконання (**x**).

Файли та каталоги мають дозволи, призначені для користувачів, груп та інших.

Дозволи на файли та папки відображаються за допомогою команди **ls -l**.

Ця команда також відображає посилання на файл.

Жорсткі посилання створюють ще один файл з іншим ім'ям, який пов'язаний з тим самим місцем у файловій системі.

Власник файлу та група файлу також відображаються разом із датою та часом останньої модифікації файлу.

Дозволи на файли є потужними функціями файлової системи Linux і не можуть бути порушені.

Тільки користувач **root** може змінити дозволи файлів.

Через потужність кореневого користувача доступ до нього слід ретельно контролювати.

Система X Windows, або X11, є базовим програмним забезпеченням, яке включає функції для створення, керування та налаштування графічного інтерфейсу користувача Windows в інтерфейсі "наведи і клацни".

Різні постачальники використовують систему X Windows для створення різних графічних інтерфейсів менеджера вікон для Linux.

Прикладами менеджерів вікон є **Gnome** та **KDE**.

У дистрибутиві **Ubuntu** Linux за замовчуванням використовується **Gnome 3**.

Робочий стіл **Gnome 3** складається з меню додатків, док-станції Ubuntu, верхньої панелі, календаря та панелі системних повідомлень, області діяльності та меню стану.

Для встановлення додатків на хости Linux використовуються програми, які називаються менеджерами пакетів.

Пакети - це **software applications** та всі допоміжні файли.

Менеджери пакетів надзвичайно корисні для встановлення складних програм із централізованих сховищ пакетів, доступних через Інтернет.

У різних дистрибутивах Linux використовуються різні менеджери пакетів.

Наприклад, **Arch Linux** використовує **pacman**, **Debian** використовує **dpkg** як основний менеджер пакетів.

Ubuntu також використовує **apt**.

Команди **CLI** менеджера пакетів використовуються для встановлення, видалення та оновлення програмних пакетів.

Управління пакетами також можна виконувати в графічному інтерфейсі.

Програмні процеси - це екземпляри запущених комп'ютерних програм.
Багатозадачні операційні системи можуть одночасно запускати багато процесів.

Форкінг - це метод, який ядро використовує, щоб дозволити запущеному процесу самокопіюватися.

Команда **ps** перелічує запущені процеси, **top** відображає інформацію про запущені процеси динамічно, а **kill** використовується для видалення, перезапуску або призупинення запущених процесів.

Хоча Linux вважається краще захищеним від шкідливого (зловмисного) програмного забезпечення, ніж інші операційні системи, він все ще сприйнятливий до дії троянських коней, хробаків та інших видів шкідливих програм.

Зазвичай Linux атакують через його служби та процеси.

Застаріле програмне забезпечення часто вразливе до атак.

Актори загроз (зловмисники) можуть перевірити пристрій на відкриті порти, які пов'язані із застарілими серверними процесами.

Завдяки цим знанням можна запускати атаки.

Важливо постійно оновлювати операційну систему та її компоненти та програми.

Програма **chkrootkit** призначена для виявлення шкідливих **rootkit-ів**.

Руткіти - це шкідливі програми глибокого рівня, які дуже важко виявити та видалити.

Вони можуть змінити фундаментально роботу самої операційної системи і можуть використовуватися для створення несанкціонованого доступу до систем.