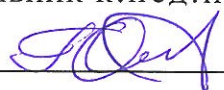


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА
до випускної кваліфікаційної роботи бакалавра
на тему:
«Проект підсистеми локального та мережного захисту робочих
станцій Linux»

Виконав студент 4-го курсу, групи КІ-3
спеціальності 123 «Комп'ютерна інженерія»

 Білошицький Р. М.
Керівник к.пед.н., доцент кафедри КІ та КБ,

 Головня О. С.

Рецензент к. т. н., доцент кафедри КІ та КБ,

 Пулеко. І. В.

Житомир 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Єфіменко А. А.

«12» квітня 2021 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента Білошицького Романа Миколайовича

Тема роботи: Проект підсистеми локального та мережного захисту робочих станцій Linux

Затверджена Наказом по університету від «12» квітня 2021 р. №133\С

Термін здачі студентом закінченої роботи – ____ 2021 р.

Вихідні дані для роботи:

1. Віртуальні робочі станції Linux(Ubuntu, Mint, Kali) та Windows XP.
2. Графічний симулятор мережевого обладнання GNS3.
3. Посібники користувача Linux Man.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються.

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Головня О. С	3.03.2021	
2	Головня О. С	23.04.2021	
3	Головня О. С	14.05.2021	

Керівник  Головня О.С.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	12.04.21	виконано
2	Розробка плану роботи	15.04.21 – 17.04.21	виконано
3	Розробка розгорнутого плану	18.04.21 – 19.04.21	виконано
4	Подача чернетки керівнику для перевірки	25.04.21	виконано
5	Доопрацювання роботи та перевірка керівником	26.04.21 – 30.05.21	виконано
6	Затвердження графічних матеріалів у керівника	01.06.21 – 04.06.21	виконано
7	Проведення попереднього захисту	05.06.21	виконано
8	Отримання відгуку керівника	16.06.21	виконано
9	Допуск завідувача кафедри	16.06.21	виконано
10	Подання роботи на рецензування	16.06.21	виконано
11	Захист	18.06.21	виконано

Студент Білошицький Р.М.

Керівник Головня О.С.

АНОТАЦІЯ

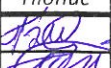
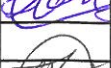
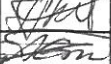
Кваліфікаційна робота складається з проекту підсистеми робочих станцій Linux та пояснювальної записки до нього. У роботі було проведено обґрунтування актуальності теми, аналіз існуючих методів захисту систем. Також було визначено основні завдання на розробку підсистеми, які образи робочих станцій Linux використовуватимуться для побудови схеми, програмне забезпечення.

Пояснювальна записка до випускної бакалаврської роботи містить 64 сторінки, 45 рисунків, 1 додаток та 13 літературних джерел.

Метою кваліфікаційної роботи є створення підсистеми локального та мережного захисту робочих станцій Linux.

У роботі було розглянуто різноманітні засоби захисту ОС Linux, проаналізовано різні команди налаштувань безпеки локального та мережного рівня, розроблено макет ddos-атак на робочу станцію, описано методи роботи з правами користувачів та атрибутами файлів,

КЛЮЧОВІ СЛОВА: ОС LINUX, USER, ID, UBUNTU, MINT, КОРИСТУВАЧ, СИСТЕМА, ЗАХИСТ, СТАНЦІЇ, ПАРОЛІ, МЕРЕЖА, ДОСТУП.

					КІ.КР.Б – 123 – 21 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми локального та мережного захисту роб. станцій Linux Пояснювальна записка	Літ.	Арк.	Аркушів	
Розроб.		Білошицький Р.М		22.06.21					
Перевір.		Головня О.С.		22.06.21			4	59	
Н. контр.						Державний університет «Житомирська політехніка», група КІ-3			
Рецензент		Нудеко І.В.							
Зав.каф.		Єфіменко А.А.		22.06.21					

ABSTRACT

The qualification work consists of a project of the Linux workstation subsystem and an explanatory note to it. The work substantiates the relevance of the topic, analyzes the existing methods of system protection. The main tasks for the development of the subsystem, which images of Linux workstations will be used to build the scheme, software were also identified.

The explanatory note to the final bachelor's thesis contains 64 pages, 45 figures, 1 appendix and 13 literary sources.

The purpose of the qualification work is to create a subsystem of local and network protection of Linux workstations.

Various means of Linux security protection were considered in the work, various commands of local and network security settings were analyzed, the layout of ddos-attacks on the workstation was developed, methods of working with user rights and file attributes were described,

KEY WORDS: OC LINUX, USER, ID, UBUNTU, MINT, USER, SYSTEM, PROTECTION, STATIONS, PASSWORDS, NETWORK, ACCESS.

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				5
	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	7
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЛОКАЛЬНОГО ТА МЕРЕЖНОГО ЗАХИСТУ ОС LINUX.....	8
1.1. Локальна безпека Linux.....	8
1.2. Користувачі системи, паролі	9
1.3. Права доступу	15
1.4. Атрибути файлів	18
1.5. Механізм квот	21
1.6. Шифрування диска	25
1.7. Шифрування домашнього каталогу Linux Mint	26
1.8. Брандмауер	27
РОЗДІЛ 2 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЛОКАЛЬНОЇ БЕЗПЕКИ ОС LINUX.	32
2.1.Робота з користувачами	32
2.2. Налаштування захищеної конфігурації web-портала	34
2.3 Налаштування комплексного захисту сервера з використанням розширених атрибутів.....	36
2.4 Розділення дискового простору між користувачами з використанням механізму квот.....	37
2.5 Утиліта CryptSetup на Linux Mint.....	39
РОЗДІЛ 3. МЕРЕЖЕВИЙ ЗАХИСТ ОС LINUX MINT	46
3.1. Міжмережний екран в Linux Mint.....	46
3.2. Захист Linux Mint від DDoS-атак.....	51
3.3. Боротьба зі flood-атаками.....	55
ВИСНОВКИ	58
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	59
ДОДАТОК	60

ВСТУП

Безпека операційних систем завжди займатиме перше місце у роботі, як і великих компаній, так і невеликих організацій, які тільки починають розвиватись. Чому саме Linux? Бо це операційна система, яка є безкоштовною і дозволяє досягти пристрою лімітів своєї продуктивності. Проблема інформаційної безпеки буде актуальною завжди як і інформація, яку необхідно захистити від стороннього ока.

У даній роботі здійснено огляд утиліт і команд терміналу, які має ОС Linux для безпечної роботи користувачів, безпечного функціонування, а також збереження конфіденційної інформації, для якої ця ОС може використовуватися.

Метою кваліфікаційної роботи є створення підсистеми локального та мережного захисту робочих станцій Linux.

Визначена мета обумовлює наступні завдання:

- Налаштування захисту інформації всередині системи
- Поділ та надання прав користувачам системи
- Налаштування захисту ОС Linux в мережі
- Організація захисту міжмережного екрану та блокування DDos-атак

Об'єктом дослідження є функціонування локального та мережного захисту ОС Linux.

Предметом дослідження є налаштування локального та мережного захисту робочих станцій Linux.

У процесі виконання кваліфікаційної роботи було розроблено проект підсистеми захисту станцій Linux, у якому зачіпаються питання локальної та мережевої безпеки, запобігання загрозам безпеки ОС Linux; безпечної роботи з персональним комп'ютером і монітором.

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				7
	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЛОКАЛЬНОГО ТА МЕРЕЖНОГО ЗАХИСТУ ОС LINUX

Linux - це мережева операційна система, але чіткої межі між локальною та мережевою безпекою немає. Комп'ютер, який використовує звичайний користувач, може виступати як в якості сервера, так і звичайного ПК, тому підключення його до мережі не гарантується. Якщо комп'ютер не підключений до мережі то і про мережну безпеку говорити недоречно, тому що мережевої загрози в принципі не існує. Отже, поділ загальної безпеки системи на дві складові цілком доцільний.

З огляду на все це, можна зробити висновок, що локальна безпека є першочерговою, і останнім рубежем до викрадення інформації, але в ситуаціях коли до комп'ютера має доступ тільки одна людина – проблем не виникатиме. Мережева ж безпека є актуальною тільки в тому випадку, коли комп'ютер зі встановленою на ньому Linux має вихід в мережу. Мережева безпека є невід'ємною ланкою локальної безпеки, які разом визначають загальну безпеку системи в цілому.

Головним завданням кваліфікаційної роботи є створення підсистеми, станції якої будуть надійно захищені найрізноманітнішими способами, всередині системи і від різних видів атак в мережі.

1.1. Локальна безпека Linux

Linux розрахована на багато користувачів, і той факт, що існує велика кількість людей, які можуть одночасно отримати доступ до системи, здається більш ніж очевидним. Чому необхідно захищати систему від локальних користувачів? Щоб відповісти на це питання, спочатку розглянемо, що може робити користувач, який має доступ до системи.

- Після входу користувачу виділяється певна частина машинних ресурсів (дисковий простір, оперативна пам'ять, час процесора і т.д.). Добре, якщо ОС спочатку налаштована на правильний розподіл ресурсів. А якщо ні? Одному користувачеві досить запустити пару «важких» програм, і час очікування інших програм навіть на потужній машині може перевищити межу допустимого.

- Є програми, які повинен запускати тільки привілейований користувач

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				8
	Арк.	№ докум.	Підпис	Дата		

(користувач root). Зазвичай ці програми використовуються для налаштування системних параметрів операційної системи, неправильна конфігурація яких може негативно позначитися на її працездатності. Випадковий запуск такої програми звичайним користувачем може мати фатальні наслідки для системи в цілому.

- "Переглядаючи" дерево каталогів на жорсткому диску, користувач може дістатися до тієї частини, якій не належить (наприклад, в директорії, де зберігаються файли інших користувачів). Особисті файли кожного користувача повинні бути доступні йому і тільки йому, якщо, звичайно, він не вирішить інакше.

Ці приклади - лише невелика частина. Іноді, навіть не усвідомлюючи цього, недосвідчений користувач може становити потенційну загрозу, якщо ви надасте йому необмежені права. Крім того, сама порядність користувача - це розкіш, яку не кожен в сучасному світі може собі дозволити.

А тепер розглянемо, які інструменти надає система Linux для локальної безпеки.

1.2. Користувачі системи, паролі

Користувач - це особа, яка використовує ресурси та можливості, надані йому певними службами. Користувач не повинен знати всіх аспектів функціонування цих служб, йому потрібно лише знати, як ними користуватися.

У Linux кожен користувач має свій унікальний числовий ідентифікатор (UID – User Identifier), за яким він визначається в системі. Для зручнішого сприйняття людиною унікальному ідентифікатору також відповідає ім'я цього користувача (логін). Деякі ідентифікатори традиційно присвоюються певним користувачам. Наприклад, нульовий ідентифікатор зарезервований для привілейованого кореневого користувача.

Усі імена користувачів Linux та відповідні ідентифікатори зберігаються у спеціальному файлі passwd. Цей файл знаходиться в каталозі etc, який, у свою чергу, знаходиться в кореневому каталозі системи. Файл має форму простого тексту.

Приклад фрагменту /etc/passwd зображений на рисунку 1.2

		Білошицький Р.М.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				9
	Арк.	№ докум.	Підпис	Дата		

```

root:x:0:0:root:/root:/bin/bash
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
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

```

Рисунок 1.2 – Файл користувацьких імен passwd

Кожен запис у цьому файлі розділений двокрапками на 7 частин:

1. Ім'я користувача(логін). Це поле містить ім'я користувача. Для операційної системи не має значення, яке ім'я має користувач, система фокусується на ідентифікаторі, і це ім'я, є лише інформаційним значенням для людини, яка працює в системі.

2. Поле пароля. Це поле в попередніх версіях Linux містило зашифрований пароль, і тепер, коли була введена технологія тіньових паролів, це поле просто x. Це поле не має практичного застосування.

3. Ідентифікатор користувача (UID). У системі Linux кожен користувач має унікальний ідентифікаційний номер, який однозначно ідентифікує його в системі. Цей номер використовується для різних цілей, наприклад, при встановленні дозволів для файлів.

4. Ідентифікатор групи, до якої належить цей користувач (GID).

5. Поле коментаря. У цьому полі можна зберігати будь-яку додаткову інформацію про користувача, наприклад, його повне ім'я.

6. Повний шлях до домашнього каталогу користувача. Linux створює домашній каталог для кожного користувача, де він може зберігати свої документи. Як правило, ці каталоги знаходяться в каталозі /home кореневого каталогу та за замовчуванням мають імена власників.

7. Шлях до командної оболонки. Останнє поле містить повний шлях до робочої оболонки користувача (за замовчуванням такою оболонкою є bash). Ця оболонка запускається, коли користувач проходить процедуру автентифікації. З

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		10

міркувань безпеки для користувачів системи, `/sbin/nologin` дуже часто використовується в цьому полі. У цьому прикладі користувач `bin` має абсолютно однакове значення в полі оболонки. Сама програма `nologin` не є оболонкою, її єдиною метою є запобігання входу в систему. Тому, коли ви намагаєтесь увійти як користувач, у якого в якості робочої оболонки встановлено `/sbin/nologin`, нічого не відбувається. Як правило, такий підхід використовується для створення користувачів, які є системними, тобто від імені яких виконуються деякі дії в системі. Оскільки таким користувачам не потрібна робоча оболонка, хорошим рішенням з точки зору безпеки буде встановлення поля оболонки в `/sbin/nologin`. Іншим поширеним рішенням у таких ситуаціях є встановлення для цього поля значення `/bin/false`. Як відомо, в Linux, як і в більшості інших операційних систем, успішне завершення програми визначається типом поверненого значення. Якщо значення повертається до нуля, виконання програми було успішним, якщо ні - нуль - в процесі виконання програми сталися помилки. На основі поверненого значення система автентифікації робить висновок про те, чи була автентифікація успішною чи "неуспішною". `false` - програма, яка, незалежно від зовнішніх факторів, завжди повертає значення, відмінне від нуля, що в даному випадку означає, що під час запуску оболонки виникають помилки, а керування повертається в систему автентифікації.

При вході в систему програма доступу зчитує інформацію про користувача з файлу `passwd`. Тільки привілейовані користувачі мають право писати в цей файл, і всі користувачі системи можуть його читати (права доступу описані в розділі «Можливості файлової системи Linux»).

Цей файл ніколи не редагується вручну, хоча в принципі це цілком допустимо. Зазвичай для редагування користувальницького файлу використовуються спеціальні команди: `useradd`, `usermod`, `userdel`, `adduser` тощо.

Команда `useradd` дозволяє вам додати нового користувача в систему. Для управління процесом створення користувача ця програма може приймати різні параметри в командному рядку. Наприклад, параметр `-s` вказує оболонку, яка використовується користувачем, а параметр `-g` вказує групу, для якої створюється

		Білошицький Р.М.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		11

користувач. Крім додавання запису користувача в файл `/etc/passwd`, `useradd` створює домашній каталог користувача, який за замовчуванням повинен бути поміщений в каталог `/home`. Шлях до каталогу користувача можна визначити за допомогою параметра `-d`, за яким слід повний шлях від кореневого каталогу до каталогу користувача.

Програма `usermod` дозволяє змінювати такі параметри, як робоча оболонка користувача, домашній каталог, група, ідентифікатор користувача і так далі.

Легко здогадатися, що робить програма `userdel`. Видаляє користувача з системи. Детальна інформація про ці команди міститься у відповідних посібниках `Man` [7].

Ім'я користувача не є секретною інформацією і може бути легко ідентифікована іншими користувачами системи. Але в цьому випадку повинен бути ризик, що один користувач увійде в систему як інший. Однак цього не відбувається. Використовується таке поняття, як аутентифікація.

Автентифікація - це встановлення автентичності користувача, тобто встановлення того факту, що користувач з таким ім'ям є саме тим, ким він назвався.

Для автентифікації в `Linux` використовується давно перевірений інструмент - пароль.

Пароль - це набір символів (секретне слово), відомий тільки його власнику, що використовується для підтвердження його автентичності.

У кожного користувача в системі свій пароль. Наявність пароля - необхідний компонент політики безпеки користувачів `Linux`. Пароль подібний пропуску користувача в систему. Без пароля, знаючи тільки ім'я користувача, неможливо увійти в систему.

Паролі зберігаються в окремому файлі `/etc/shadow`. У більш ранніх версіях `Linux` імена користувачів і паролі зберігалися в одному файлі `/etc/passwd`. Але практика показала, що для більш надійного захисту паролем необхідно створити окремий файл для їх зберігання. Таким чином, технологія виділення окремого

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				12
	Арк.	№ докум.	Підпис	Дата		

тіньового файлу для зберігання паролів отримала назву «технологія тіньових паролів».

Приклад файлу і його структура наведені нижче:

```
root!!:18664:0:99999:7:::  
daemon*:18662:0:99999:7:::  
bin*:18662:0:99999:7:::  
sys*:18662:0:99999:7:::  
sync*:18662:0:99999:7:::  
man*:18662:0:99999:7:::  
lp*:18662:0:99999:7:::
```

Рисунок 1.3 – Файл паролів користувачів

Файл shadow, як і файл passwd, розділений на кілька частин двокрапкою:

1. Ім'я користувача. Це поле просто дублюється з файлу passwd.

2. Хеш пароля. Пароль в Linux ніколи не зберігається у відкрито вигляді, на відміну від імені користувача. При встановленні пароля до збереження у файл він шифрується за спеціальним алгоритмом. За замовчуванням це алгоритм одностороннього шифрування DES (Data Encryption Standard). Використання одностороннього алгоритму шифрування виключає можливість розшифровки пароля.

Решта полів містять різну службову інформацію (Остання зміна пароля, мінімальний та максимальний термін дії пароля, періоди попередження та бездіяльності, термін зберігання, тощо.).

Файл паролів прав доступу до читачів і списками суперкористувачів (права доступу описуються в розділі «Особливості файлових системи Linux»). Його вміст є недоступним для пересічних користувачів, таким чином, виключає можливість розкриття зашифрованого пароля.

Для зміни паролів в Linux спочатку включена спеціальна програма passwd. Як параметр в командному рядку вона отримує ім'я користувача і при запуску вимагає введений пароль для цього користувача. При введенні пароля в з метою безпеки пароль не відображається на обраному моніторі - це дозволяє уникнути

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				13
	Арк.	№ докум.	Підпис	Дата		

виявлення зловмисником довжини паролю. Введення пароля здійснюється 2 рази для перевірки правильності введення. Після підтвердження пароль шифрується і зберігається в файлі `/etc/shadow`.

При вході в систему процедурою отримання імені користувача та пароля керує програма `mingetty`. `Mingetty` - це програма, яка видає запрошення на введення імені користувача та пароля на віртуальній консолі. Після його запуску на екрані монітора з'являється рядок із запрошенням на введення імені користувача та пароля. Після введення імені та пароля програма передає контроль програмі входу. `Login` - це посередницька програма, яка перевіряє наявність, правильність та відповідність імені користувача та пароля в системі. Пароль шифрується за допомогою механізмів автентифікації та порівнюється з хешем із файлу. Після успішного завершення процедури автентифікації програма входу запускає системну оболонку для взаємодії користувача з операційною системою, так звану оболонку (від англ. `Shell` - «оболонка»). Шлях до виконуваної оболонки вказаний в останньому сьомому полі запису файлу `passwd`. `Bash` (`Bourne Shell`) зазвичай використовується за замовчуванням. Вам буде запропоновано ввести команди з символом `#` або `$` в кінці (за замовчуванням символ `#` використовується в запрошенні суперкористувача, а символ `$` - у звичайному запрошенні користувача). Відтепер система готова приймати команди від користувача до виконання.

Для зручнішого управління доступом до ресурсів в `Linux` всі користувачі об'єднуються в групи. У цьому випадку група - це сукупність користувачів, об'єднаних за будь-якими критеріями.

До якої групи належить користувач, говорить 4-те поле запису про реєстрацію у файлі `passwd`. Наявність груп дозволяє створити гнучку політику безпеки на основі спільного доступу до ресурсів.

У користувача можуть бути і додаткові групи, щоб додати використовуємо наступну структуру:

```
# useradd -m -g [основна група] -G [список додаткових груп] -s [командний інтерпретатор] [ім'я користувача]
```

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				14
	Арк.	№ докум.	Підпис	Дата		

- -m - створює домашній каталог, виду /home/[ім'я користувача].
- -g - ім'я або номер основної групи користувача.
- -G - список додаткових груп, в які входить користувач.
- -s - визначає командну оболонку користувача.

Практичне застосування цієї інформації наведено у розділі 2.

1.3. Права доступу

Розглянемо ситуацію, коли деякий користувач використовує свій домашній каталог для зберігання дуже важливих документів. Інформація, що зберігається в документах, є суворо конфіденційною, тому ніхто, крім її власника, не повинен мати до неї доступу. Інший користувач просто з цікавості і, можливо, зі злим умислом спробував отримати вміст цих документів. Спроба привела до помилки з описом «відмовлено у доступі». Помилка була викликана відсутністю у другого користувача прав на читання документів, що належать першому користувачеві. З цього прикладу ми можемо зробити висновок, що права доступу дозволяють обмежити доступ до певної інформації або, простіше кажучи, захистити деяку інформацію від певних користувачів.

Концепція політики безпеки файлів Linux заснована на тому факті, що будь-яка файлова система має 3 категорії власників: фактичний власник файлу або, простіше кажучи, його творець, будь-яка група користувачів, в яку часто входить власник файлу, і всі інші. Таким чином, привілейований користувач або власник файлу, оскільки тільки він має можливість змінювати права доступу, може створити політику безпеки файлу, визначаючи права окремо для власника файлу, для групи користувачів і для всіх інших користувачів системи.

Права доступу до файлу або каталогу описуються трьома вісімковими цифрами, крайня ліва з яких - права доступу власника, середня - права доступу групи, а права доступу - права доступу для всіх інших. Кожна з цих вісімкових цифр має 3-бітну маску. Ці біти відповідають за право читання, записи і виконання файлу або каталогу. Якщо біт встановлено у 1 - операція дозволена, якщо 0 - заборонена.

Значення доступу трохи розрізняються для різних типів файлів.

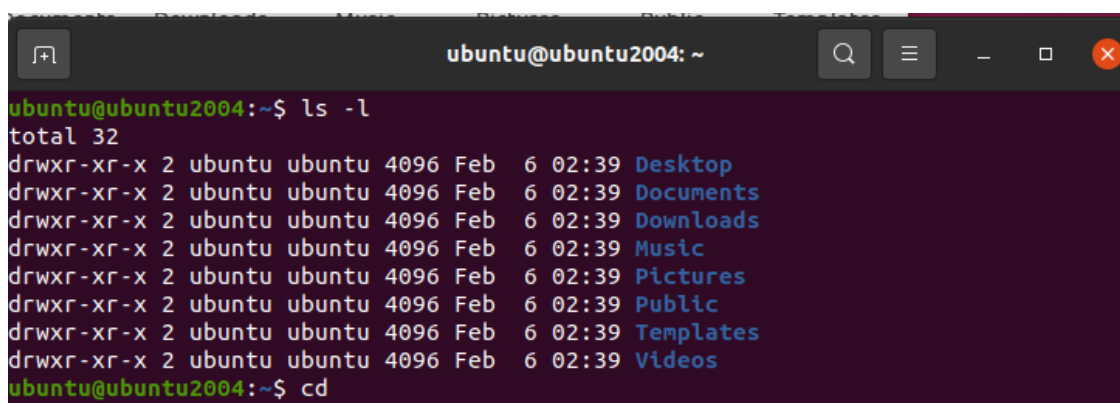
		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				15
Арк.		№ докум.	Підпис	Дата		

Право на читання файлу дозволяє користувачеві читати вміст файлу. Для каталогу встановлення дозволів на читання дозволяє вам читати файли в цьому каталозі.

Право на запис файлу дозволяє користувачеві змінювати його вміст. Для каталогу створить файли всередині каталогу.

Виконуваний файл для файлу дозволяє запускати виконуваний файл як програму. Для каталогу установка цього права дозволяє користувачеві увійти в каталог і переглянути його вміст.

Ви можете дізнатися, які права доступу визначені для кожного файлу, набравши команду `ls` в терміналі з ключем `-l`:



```
ubuntu@ubuntu2004: ~  
ubuntu@ubuntu2004:~$ ls -l  
total 32  
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Desktop  
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Documents  
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Downloads  
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Music  
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Pictures  
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Public  
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Templates  
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Videos  
ubuntu@ubuntu2004:~$ cd
```

Рисунок 1.4 – Права доступу

У першому стовпчику представлені права доступу до файлу. Цей стовпець містить 10 знаків. Перший зліва повідомляє вам, до якого типу належить файл, тобто чи є це файлом, каталогом, посиланням і т.д. Далі зліва направо знаходяться права доступу для власника, для групи і, нарешті, для всіх інших. У другому стовпці показано кількість жорстких посилань на цей файл. Третя вказує ім'я власника файлу, четверта - ім'я групи власників, п'ятий стовпець - розмір файлу, шостий - дату створення файлу, сьомий - ім'я файлу.

Як видно з прикладу, файл Desktop - це каталог, позначений буквою `d` в полі дозволів. Поле власника вказує, що власником каталогу є користувач `ubuntu`, а групою власників також - `ubuntu`. Власник має право читати файли в каталозі, записувати файли і читати вміст каталогу. Буква `r` (від слова Read) позначає

можливість даного користувача виконувати операції читання файлів каталогу, буква w (від слова Write) - можливість записувати файли в каталог, остання буква x (від слова eXecute) дає право переглядати вміст каталогу. Коли взятий окремо, x надає право “потрапляти всередину” каталогу (виконувати cd, використовувати ім'я каталогу у шляхах до підкаталогів). Дозвіл x зазвичай надається разом з дозволом r, але x працюватиме і без r (вміст саме цього каталогу подивитися не вийде, проте можна буде перейти до вкладених). Користувачі, що входять до групи власників, мають право тільки читати файли цього каталогу і отримувати його вміст (літери r і x), права на запис файлів в цей каталог у них немає. Всі інші користувачі мають ті ж права доступу, що і група власників.

Зміна прав доступу до файлу проводиться за допомогою стандартної системної команди chmod. Права доступу при виклику команди можуть бути задані як і бітовою маскою в десятковому поданні, так і за допомогою символів. Використання цієї команди детально описано на відповідній сторінці керівництва man [8].

Крім прав доступу існують так звані модифікатори доступу. Модифікатори доступу включають Sticky bit, SUID і SGID.

Sticky bit (t). Для файлів встановлення цього модифікатора в сучасних дистрибутивах втратила значення. Встановлення біта Sticky для каталогу дозволяє користувачеві записувати файли в цей каталог, але він може видаляти файли тільки з цього каталогу, який йому належить, або якщо йому явно призначені права на запис.

SUID (setgid). Якщо у файлі встановлений модифікатор доступу SUID і файл є виконуваним, то файл при запуску отримує помилку користувача, що запустив його, і права власника файлу. Ці методи використовуються для того, щоб користувач міг працювати з деякими системними файлами, які належать привілейованому користувачеві, але при цьому йому не надавалися права привілейованого користувача в усій системі. Наприклад, щоб користувач міг змінити свій пароль за допомогою програми passwd, в цій програмі, що належить

		Білошицький Р.М.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
Арк.		№ докум.	Підпис	Дата		17

користувачеві root, повинен бути встановлений біт SUID, оскільки вона працює з тіншовим файлом, який може бути змінений тільки користувачем root.

SGID (s). Якщо файл має модифікатор доступу SGID, це аналогічно установці біта SUID, за винятком того, що замість власника файлу використовується група, до якої належить файл. Якщо ви встановите SGID для каталогу, файли в цьому каталозі будуть мати ті ж налаштування групи, що і каталог.

Модифікатори доступу при правильному використанні є дуже потужним і гнучким інструментом. З іншого боку, неправильне налаштування системи з використанням цих модифікаторів може анулювати всі дії безпеки. Особливо небезпечна ситуація, коли такий же SUID встановлений на виконуваний файл, що належить привілейованому користувачеві. При виконанні запущеного файлу користувач отримує право виконувати операції, доступні тільки користувачу root. Навіть якщо файл не виконує ніяких системних операцій і не працює з системними файлами, його неправильне використання може привести до дуже неприємних наслідків.

Практичне застосування цієї інформації описано в розділі 2.

1.4. Атрибути файлів

Файлова структура операційної системи завжди містить файли, які не повинні змінюватися під час роботи системи, наприклад, виконувані файли або файли, які необхідно виправити тільки один раз під час налаштування системи і які не повинні змінюватися пізніше, наприклад, файли конфігурації. Деякі з них можуть бути доповнені, але не можуть бути видалені або перезаписані. Наявність ресурсів, що гарантують виконання цих умов, дозволяють значно підвищити безпеку файлової системи при збереженні вихідної цілісності даних для різних типів атак.

Починаючи з версії ядра 1.1 файлова система Linux підтримує розширені атрибути файлів. Останні версії ядра 2.4 підтримують наступні атрибути:

- Atime (A). Кожен раз, коли система звертається до файлу, осередок часу останнього доступу до файлу змінюється. Встановлення атрибута atime дозволяє уникнути поновлення часу останнього виклику і збільшує продуктивність файлової

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		18

системи, особливо у випадках, коли виклики файлів відбуваються дуже часто. Однак брак часу для останньої модифікації файлу загрожує зміною файлу без подальшої реєстрації цієї дії, що може бути небезпечним.

- Sync (S). Встановлення атрибута синхронізації дозволяє вам негайно записувати всі зміни, що відбуваються з файлом на жорсткому диску, синхронно з процесом, який вносить ці зміни. Це забезпечує більш безпечну роботу, але також може знизити продуктивність через прямий постійного запису на диск.

- Append (a). Цей атрибут дозволяє відкривати файл тільки для його доповнення. Усічення або перезапис файлу заборонені. Для каталогу установка цього атрибута означає, що видалення файлів, що містяться в цьому каталозі, заборонено, хоча створення нових і зміна існуючих можливо.

- Immutable (i). Файл з встановленим атрибутом immutable взагалі не може бути змінений. Якщо ви встановите цей атрибут для каталогу, процеси зможуть змінювати файли в ньому, але не зможуть створювати або видаляти файли. Для забезпечення безпеки має велике значення.

- No Dump (d). Встановлення атрибута no dump дає вказівку процесу, який здійснює створення дампа, ігнорувати цей файл і не включати його в створення резервної копії.

- Compress (c). Цей атрибут дозволяє прозора стискати файли перед їх записом на диск. Коли ви звертаєтесь до файлу, відбудеться розпакування і остаточний процес вже знаходиться в нормальній формі.

- Secure Deletion (s). Якщо цей атрибут встановлений, то при видаленні файлу всі блоки, в яких він перебував, заповнюються нулями, тобто повне видалення файлу, а не тільки його дескриптор.

- Undelete (u). Коли ви видаляєте файл з цим атрибутом, система зберігає всі блоки файлу на диск, що дозволяє при бажанні відновити видалений файл.

Останні версії ядра, починаючи з 2.4, ігнорують значення останніх трьох атрибутів: стиснення, безпечного видалення та відновлення. Розробники порахували, що їх подальше використання не має сенсу.

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				19
	Арк.	№ докум.	Підпис	Дата		

Для зміни і перегляду встановлених атрибутів в стандартний пакет системи Linux входять дві програми, `chattr` і `lsattr`. Перший дозволяє змінювати атрибути, додавати або видаляти їх, другий дозволяє отримати список встановлених атрибутів. Приклад `lsattr` показаний нижче.

```
ubuntu@ubuntu2004:~$ lsattr /usr
----i-----e----- /usr/lib
-----e----- /usr/libx32
----i-----e----- /usr/include
```

Рисунок 1.5 – Права доступу

У прикладі, показаному на рис 1.5 для першого файлу встановлений атрибут `immutable` та `execute`, для другого - атрибут `execute`. Використання `lsattr` і `chattr` докладно описано у відповідних посібниках. [9], [10].

При певних умовах процеси, що виконуються від імені привілейованого користувача, можуть ігнорувати ці атрибути. З іншого боку, атрибути `ext2` враховуються деякими системними викликами, такими як `sys_open()` для відкриття файлу або `sys_truncate()` для його відключення, незалежно від ідентифікатора користувача, що викликається їх процесом, і інших умов. Наприклад, наявність незмінного прапора в файловому дескрипторі призводить до того, що системні виклики, пов'язані з модифікаціями файлів, просто перестають працювати незалежно від інших умов. Наявність цих атрибутів і спеціальних режимів роботи ядра в Linux дозволяє легко і ефективно вивчити абсолютні можливості привілейованого користувача. Метою комплексного налаштування є обмеження атрибутів всіх процесів, незалежно від їх прав доступу і рівнів привілеїв. Вони можуть служити ефективним низькорівневим захистом від атак на будь-який привілейований процес, в якому можуть бути присутніми будь-які невідомі вразливості.

Однак сама політика безпеки, заснована на налаштуванні таких атрибутів, як `immutable` і `append`, - це тільки одна сторона медалі. Хоча ці атрибути допоможуть запобігти зміні файлів, які вони захищають, навіть процесами, запущеними від імені привілейованого користувача, при нормальних обставинах користувач `root` може

		Білошицький Р.М.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
Арк.		№ докум.	Підпис	Дата		20

видалити ці прапори і продовжити роботу з файлами без цих атрибутів. Іншими словами, ніщо не заважає програмі, яка працює від імені користувача root, перевіряти файл на наявність цих атрибутів перед запуском і просто скасовувати їх.

Lcap (редактор обмежує набір можливостей ядра Linux) використовується для встановлення цих та багатьох інших параметрів ядра.

Приклад використання lcap:

```
[Ubuntu] # lcap CAP_LINUX_IMMUTABLE
```

```
[Ubuntu] # lcap CAP_SYS_RAWIO
```

Перший виклик lcap з параметром CAP_LINUX_IMMUTABLE скасовує можливість видалення immutable і append прапорів в привілейованих процесах. Другий виклик з параметром CAP_SYS_RAWIO забороняє низькорівневий доступ до блокових пристроїв, таким як диски, для запобігання прямого доступу до файлів.

Після того, як lcap був змінений для будь-якого параметра ядра, його можна буде змінити знову тільки після перезавантаження системи. Ця функція дає впевненість в тому, що система не зможе безперешкодно вносити зміни без отримання фізичного доступу і перезавантаження в режимі одного користувача.

Детальну документацію за програмою lcap можна знайти у відповідних посібниках man [11].

Практичне застосування цієї інформації описано в розділі 2.

1.5. Механізм квот

Очевидно, кожен адміністратор багатокористувацької системи знайомий з поняттям "дискової квоти". Спробуємо зрозуміти, що це таке і яке відношення має ця концепція до безпеки системи.

Дискова квота - заздалегідь визначена, фіксована кількість блоків дискового простору та кількість дескрипторів файлів, виділених кожному користувачеві або групі користувачів для роботи та зберігання даних.

Використання дискових квот дозволяє обмежити два аспекти дискового

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				21
	Арк.	№ докум.	Підпис	Дата		

простору: кількість дескрипторів файлів, іншими словами, кількість файлів, які може створити користувач або група користувачів, і частину загального дискового простору, який користувач або група може використовувати для зберігання своїх файлів. Ідея полягає у тому, щоб визначити для кожного користувача або групи певну частину загального дискового простору, щоб ні за яких обставин користувач не міг перевищити обсяг використовуваного дискового простору, який йому виділено. Це усуває проблему переповнення диска або нестачі місця на диску для інших користувачів та процесів.

Концепція поділу дискового простору оперує трьома поняттями: м'яке обмеження (soft limit), жорстке обмеження (hard limit) і період відстрочки (grace period).

М'яке обмеження визначає максимальний обсяг дискового простору, який може використовувати певний користувач або група користувачів.

Жорсткий ліміт працює лише за умови встановлення пільгового періоду.

Якщо для періоду затримки встановлено значення, відмінне від нуля, тоді, коли зайнятий обсяг перевищує м'яку межу, користувач отримує повідомлення про те, що його дискового простору мало. Якщо ви пропустите це попередження, а його квота на диск продовжує перевищувати м'який ліміт, квота на диск вважається вичерпаною після періоду відстрочки. Водночас має бути встановлено суворе обмеження. Жорстке обмеження - це абсолютне максимальне використання користувачем простору файлової системи.

Механізм квотування керується ядром операційної системи. В останніх версіях Linux підтримка квот увімкнена за замовчуванням у стандартному ядрі, що постачається з дистрибутивом. Якщо компілюється нове ядро, підтримка квот повинна бути явно включена. Увімкнення підтримки механізму квотування здійснюється шляхом встановлення параметра Quota Support (CONFIG_QUOTA) у розділі FileSystems під час налаштування ядра для процесу збірки. Якщо в ядрі немає такого параметра, це означає, що ця версія ядра не підтримує механізм квотування. У цьому випадку, щоб підтримувати квоти в ядрі, потрібно встановити

		Білошицький Р.М.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				22
	Арк.	№ докум.	Підпис	Дата		

"пакет" - спеціальне доповнення до стандартного коду ядра. Пакет можна завантажити з Інтернету.

Підтримка квот поширюється на логічний розділ диска і вказується при його монтажі. Для монтування розділу використовуйте файл `/etc/fstab`, який встановлює параметри, що вказують на використання квот. Це параметри `usrquota` та `grpquota`.

Пакет квот використовується для управління та регулювання квот на диск. У сучасних дистрибутивах Linux цей пакет входить у стандартну комплектацію, але ви можете завантажити останню версію з Інтернету.

На момент написання останнього стабільного випуску пакету квот була версія 4.03. Нижче наведено основні програми пакету `quota-4.03`, необхідні для налаштування механізму квотування:

`quota` - програма дозволяє відображати поточний стан механізму квотування. За замовчуванням відображається лише квота користувача, який запускав програму. Цю програму може запускати будь-який користувач системи.

`convertquota` – програма конвертує файли `quota.user` та `quota.group` у файли `aquota.user` та `aquota.group`. Файли `quota.user` та `quota.group` - це файли квот старого формату. Починаючи з версії ядра 2.4.0, Linux використовує новий формат квоти диску, який має, на відміну від старої версії, наступні переваги:

- підтримка 32-розрядних ідентифікаторів користувачів (UID);
- встановлення квоти для привілейованого користувача;
- встановлення дискової квоти в байтах (у старій версії одиниця дискової квоти становила кілобайт);
- підтримка дискової квоти для журнальованої файлової системи ReiserFS.

Файли `aquota.user` та `aquota.group` використовуються для налаштування нової версії механізму квотування. Простіше кажучи, програма `convertquota` дозволяє

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				23
	Арк.	№ докум.	Підпис	Дата		

конвертувати файли налаштувань квоти зі старого формату в новий, що дозволяє вам перейти на використання нової версії з мінімальною переконфігурацією системи.

edquota - програма є редактором квот користувачів. Коли ви викликаєте цю програму, запускається текстовий редактор, встановлений за замовчуванням у системі. У цьому редакторі ви можете внести необхідні зміни у файл квоти диска.

quot - програма відображає статистику в кілобайтах за квотами користувачів для певної файлової системи.

quotacheck - програма для перевірки цілісності квоти диска. Інтенсивна робота механізму квотування у файловій системі може спричинити різні неточності, пов'язані з використанням дискового простору користувача. Програма квотування перевіряє файлову систему, визначаючи обсяг вільного та зайнятого місця, буде таблиці поточного використання дискового простору та порівнює дані із записами у файлі квоти диска. Якщо є розбіжності, ці розбіжності виправляються шляхом виправлення неправильних значень у файлах квоти диска.

quotaon - програма для ввімкнення квот користувачів у зазначеній файловій системі. Перед використанням цієї програми ви повинні встановити параметр usrquota та grpquota у файлі /etc/fstab для потрібної файлової системи.

quotaoff - програма для виключення квот користувачів у зазначеній файловій системі.

repquota - програма для відображення статистичних даних про використання дискового простору для зазначеної файлової системи.

setquota - програма для редагування квот користувача в режимі командного рядка.

warnquota - програма для інформування користувачів про те, що їх дисковий простір вичерпується. Інформування здійснюється шляхом надсилання попереджувального повідомлення на електронну пошту.

Більш детальну інформацію про програми пакету квот можна отримати у

		Білошицький Р.М.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		24

відповідних посібниках map.

Практичне застосування цієї інформації наведено у розділі 2.

1.6. Шифрування диска

Одним з не менш важливих компонентів локального захисту Linux, є шифрування дисків, а саме повне шифрування диска Full Disk Encryption (FDE) - один з найбільш ефективних способів захисту даних, що зберігаються на ноутбуках, від крадіжки або втрати разом з пристроєм. Що б не сталося з пристроєм, механізм FDE дозволяє гарантувати, що вся зберігається на ньому інформація недоступна того, в чий руки потрапив даний пристрій.

FDE використовується до завантаження системи. Це означає, що застосовувана технологія починає свою роботу відразу ж після натискання кнопки живлення на пристрої. При включенні комп'ютера операційна система починає завантажуватися в зашифрованому навколишньому середовищі. Шифрування незначно уповільнює продуктивність системи, що характерно для всіх реалізацій програмного забезпечення шифрування від будь-яких постачальників. Всі операції шифрування (дешифрування) відбуваються непомітно для користувача, незалежно від використовуваного ним програмного забезпечення. При цьому зашифрована весь жорсткий диск (файл підкачки, файл глибокого сну, тимчасові файли, теж часто містять важливі дані). А в разі, якщо користувач втратить пароль до шифрованому жорсткого диска, інформація може бути розшифрована за допомогою секретного ключа, відомого тільки адміністратору продукту.

Починаючи з 14-ої версії Linux Mint використовує FDE, і як результат шифрує не тільки /home, але повністю всі розділи диска. У цьому сенсі він не відрізняється від відповідного режиму TrueCrypt. Поставивши галочку і встановивши надійний пароль, користувач отримує високий рівень захисту. Оскільки Mint є найпопулярнішим в світі дистрибутивом Linux, повне шифрування диска скоро будуть використовувати більшість користувачів.

На скріншотах показано, як виглядає реалізація FDE в інтерфейсі інсталятора Linux Mint.

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		25

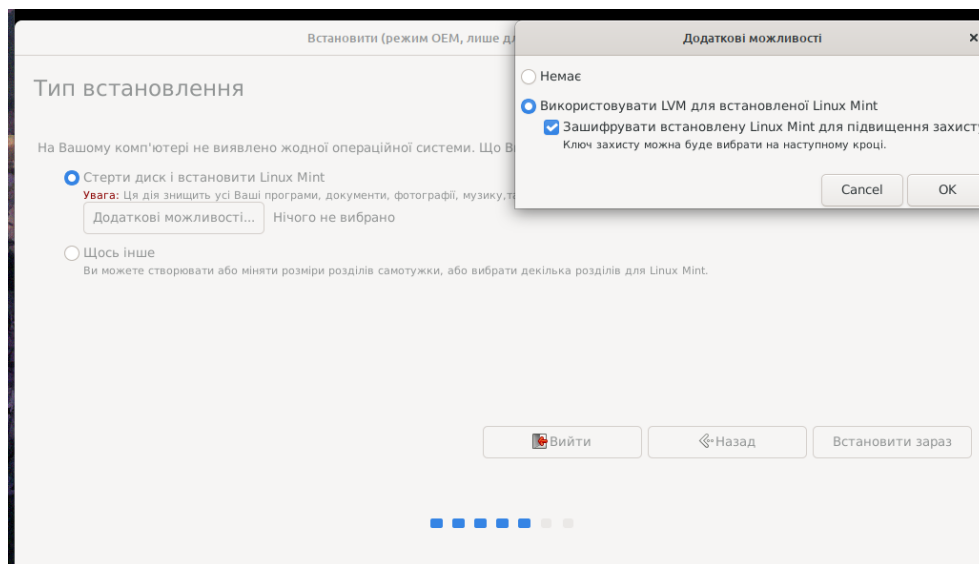


Рисунок 1.6 – Реалізація FDE в інтерфейсі інсталлятора Linux Mint

Кінцевий користувач не має можливості переналаштувати механізм шифрування. FDE запобігає несанкціонований доступ до даних за допомогою механізму аутентифікації (ім'я / пароль). При введенні правильного поєднання ім'я / пароль система витягує ключ, необхідний для розшифровки файлів на жорсткому диску. Фактично це додає додатковий рівень безпеки, оскільки зашифровані дані будуть марні для зловмисника після знищення криптографічного ключа.

Практичне застосування розглянутої інформації наводиться у розділі 2.

1.7. Шифрування домашнього каталогу Linux Mint

Шифрування домашнього каталогу забезпечує надійний захист даних, що зберігаються на жорсткому диску або іншому носії. Шифрування особливо актуально на переносних ПК, на комп'ютерах з множинним доступом, а також в будь-яких інших умовах. Шифрування домашнього каталогу пропонується при встановленні Linux Mint.

Основна проблема або хитрість при повному шифруванні домашнього каталогу полягає в тому, що необхідно «винести» каталог з зашифрованими даними за межі точки монтування.

Продуктивність знижується незначно, принаймні поки не використовується SWAP. SWAP - це спеціальний розділ на диску або файл в який операційна система переміщує окремі блоки оперативної пам'яті в разі коли її не вистачає для

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				26
Арк.	№ докум.	Підпис	Дата			

роботи додатків. SWAP теж шифрується, якщо в інсталятор вибрати шифрування домашнього каталогу, і при цьому перестає працювати сплячий режим.

Не шифрувати SWAP при зашифрованому домашньому каталозі - потенційно небезпечно, так як там можуть виявитися дані з шифрованих файлів у відкритому вигляді - весь сенс шифрування втрачається.

Починаючи з 14-ої версії Linux Mint, при установці є можливість вибрати варіант шифрування всього диска. Цей варіант найбільш підходить для збереження персональних даних на переносних пристроях (у яких, як правило, тільки один користувач).

1.8. Брандмауер

Локальна безпека є необхідною складовою загальної безпеки системи. Вона усуває загрозу локального типу. Однак, коли комп'ютер працює в мережі, існує інший тип загрози - мережа. Для усунення мережевих загроз, як і для локальних, існують інструменти та методи. Одним з таких інструментів, найважливішим і практично необхідним при побудові системи мережевої безпеки, є брандмауер.

Брандмауер, також відомий як мережевий екран, - це система або група систем, що реалізує правила контролю доступу між двома мережами. Фактичні засоби, за допомогою яких це досягається, дуже різні, але в принципі брандмауер можна розглядати як пару механізмів: один блокує передачу інформації, а інший - передає інформацію. Деякі брандмауери приділяють більше уваги блокуванню передачі інформації, інші - передачі її. Деякі брандмауери лише пропускають електронні листи, тим самим захищаючи мережу від будь-яких атак, крім атак електронної пошти. Інші брандмауери забезпечують менш жорсткий захист і блокують лише послуги, безумовно, загрожуючи безпеці. Як правило, брандмауери налаштовані на захист від несанкціонованої онлайн-реєстрації із зовнішнього світу. Це понад усе допомагає запобігти проникненню хакерів до комп'ютерів у внутрішній мережі. Досконаліші брандмауери блокують передачу інформації ззовні до захищеної мережі, дозволяючи внутрішнім користувачам вільно взаємодіяти із

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				27
	Арк.	№ докум.	Підпис	Дата		

зовнішнім світом.

Ядро Linux версії 2.4 та пізніших версій має вбудований брандмауер netfilter, який має такі функції:

- дозволяє фільтрувати вхідні, вихідні та транзитні пакети на основі вмісту заголовка пакета, типу пакету, що визначає його стан у з'єднанні (перший пакет, з'єднання, пакет синхронізації, кінцевий пакет сеансу), IP-адреса відправника комп'ютера і комп'ютер-одержувач, MAC-адреса відправника та одержувача тощо.

- дозволяє передавати мережеві адреси NAT (Network Address Translation) та заміна портів NPT (переклад мережевих портів). Дія NAT полягає у підміні IP-адреси

відправника або одержувача комп'ютера на вказану. У більшості випадків ця функція використовується для обміну інформацією між двома мережами, що мають різні діапазони IP-адрес. Дія NPT подібна до NAT з тією відмінністю, що в останньому відбувається заміщення порту програми замість IP-адреси.

- дозволяє змінювати спеціальні поля заголовка пакета, такі як TOS (Type Of Service), TTL (Time To Live) тощо, що забезпечує розширені можливості управління процесом маршрутизації.

Вся логічна структура екрану netfilter базується на концепціях ланцюгів, таблиць та правил доступу.

Ланцюг - набір правил контролю доступу. Потрапивши в ланцюг, пакет проходить усі свої правила, починаючи з самого початку. Кожне правило має критерій та дію. Якщо пакет підпадає під критерій правила, тоді дія, зазначена для цього правила, виконується з пакетом.

Таблиця - це набір ланцюжків. Таблиці розділені за функціональним призначенням і визначають дії, які дозволено виконувати в правилах ланцюжків цих таблиць. Netfilter містить тільки три таблиці:

mangle - Ця таблиця використовується для внесення змін до заголовків пакунків. Прикладом є зміна поля TTL, TOS або MARK. Таблиця має п'ять

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		28

ланцюжків: PREROUTING, POSTROUTING, INPUT, OUTPUT і FORWARD. Ланцюжок PREROUTING використовується для внесення змін на вході в брандмауер перед прийняттям рішення про маршрутизацію. Ланцюжок POSTROUTING використовується для внесення змін на виході з брандмауера після прийняття рішення про маршрутизацію. Ланцюжок INPUT використовується для внесення змін до пакетів перед їх передачею до локальної програми всередині брандмауера. Ланцюжок OUTPUT використовується для внесення змін до пакетів, що надходять від програм, що знаходяться всередині брандмауера. Нарешті, ланцюжок FORWARD використовується для внесення змін до транспортних пакетів після першого рішення про маршрутизацію, але до останнього рішення про маршрутизацію. Використання таблиці для інших цілей, крім зміни заголовка пакета, заборонено.

nat - Ця таблиця використовується для перетворення мережевих адрес, які також називаються NAT, та заміни портів NPT. Через цю таблицю проходить лише перший пакет з усього потоку даних підключення. Перетворення адрес автоматично застосовується до всіх наступних пакетів. Ця таблиця містить три визначені ланцюжки. Ланцюжок PREROUTING використовується для внесення змін до пакетів біля входу в брандмауер. Ланцюжок OUTPUT використовується для перетворення адрес у пакетах, створених програмами в брандмауері, перед прийняттям рішення про маршрутизацію. І останній третій ланцюжок у цій таблиці - POSTROUTING, який використовується для перетворення пакетів перед відправкою їх до мережі. Цю таблицю слід використовувати лише для перетворення адрес та портів у пакеті.

filter - ця таблиця в основному використовується для фільтрації пакетів. Таблиця має три вбудовані ланцюжки. Перший - FORWARD, який використовується для фільтрації пакетів, які не адресовані серверу, на якому встановлений брандмауер, тобто проходять транзитом через нього. Ланцюжок INPUT передається пакетами, які присвоюються локальним серверним додаткам. А ланцюжок OUTPUT використовується для фільтрації вихідних пакетів, генерованих програмами на сервері, за допомогою брандмауера.

Для того, щоб брандмауер виконував ті функції, які на нього покладаються,

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		29

для комплексного мережевого захисту необхідно, щоб всі пакети, що приходять по мережі і йдуть в мережу, проходили через нього. Якщо ж це правило не дотримується, або дотримується частково, то всі дії, спрямовані на створення безпечного сервера з використанням брандмауера, будуть марні. Якщо існує хоча б найменша ймовірність, що брандмауер можна обійти, ця можливість обов'язково рано чи пізно буде використана злоумисниками. У Linux брандмауер є частиною ядра, а оскільки всі операції при роботі з мережею контролює ядро, гарантію того, що всі мережеві пакети пройдуть через нього, можна вважати практично стовідсотковою.

Тепер розглянемо, який шлях проходить пакет, перш ніж досягти місця призначення. Потрапляючи на сервер, пакет спочатку проходить ланцюжки PREROUTING таблиць mangle та nat. Потім, залежно від того, кому адресований пакет, його напрям може мінятися. Якщо пакет адресований локальному процесу сервера, після маршрутизації він потрапляє в ланцюжки INPUT таблиць mangle та filter. Якщо йому вдається успішно пройти ці ланцюжки, пакет досягає локального процесу. Відповідь локального процесу перед відправкою проходить спочатку ланцюжок OUTPUT всіх трьох таблиць, і, якщо пакет не був відфільтрований, він потрапляє в заключну ланцюжок POSTROUTING таблиць mangle та nat. Після цього пакет покидає сервер.

Якщо ж пакет адресований іншому комп'ютеру, тобто є транзитним, то після маршрутизації він потрапляє в ланцюжок FORWARD таблиць mangle та filter, в якій здійснюються всі необхідні дії по управлінню доступом для всіх транзитних пакетів. Далі, як і пакет локального процесу, перед відправкою в мережу транзитний пакет проходить через ланцюжки POSTROUTING таблиць mangle та nat.

Цих трьох таблиць з заздалегідь закріпленим функціональним призначенням цілком достатньо для реалізації всіх перерахованих раніше можливостей. Кількість таблиць є визначеним і не може бути змінено ні за яких умов. При налаштуванні брандмауера в таблиці можуть бути додані інші ланцюжки на додаток до вже існуючих, що дозволяє створювати більш гнучку систему управління доступом, ніж просто додавання правил в заздалегідь визначені ланцюжка. На відміну від

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		30

ланцюжків, створених адміністратором, системні ланцюжка INPUT, OUTPUT, FORWARD, PREROUTING і POSTROUTING не можуть бути видалені ні за яких умов.

Для налаштування і управління брандмауером в складі ОС Linux поставляється програмний пакет iptables. Цей пакет крім файлів документації та модулів, підвантажуваних в ядро і використовуються для здійснення фільтрації за різними критеріями, включає наступні виконувані файли:

iptables - основна програма пакету, за допомогою якої проводиться маніпулювання правилами в ланцюжках. Ця програма дозволяє здійснювати з правилами та користувацькими ланцюжками всі доступні дії.

iptables-save - програма, яка дозволяє зберігати всі поточні правила в одному файлі для подальшого їх відновлення. За замовчуванням цим файлом є /etc/sysconfig/iptables. У файлі /etc/sysconfig/iptables зберігається вся конфігурація брандмауера і з цього файлу вона зчитується при завантаженні системи.

iptables-restore - ця програма дозволяє зчитувати правила і ланцюжка, збережені раніше програмою iptables-save. За замовчуванням ця програма намагається завантажити файл /etc/sysconfig/iptables, якщо він існує.

Більш детальна інформація про програмному пакеті iptables міститься в файлах документації, а також у відповідних man-довідниках.

Практичне застосування розглянутої інформації наводиться у розділі 3.

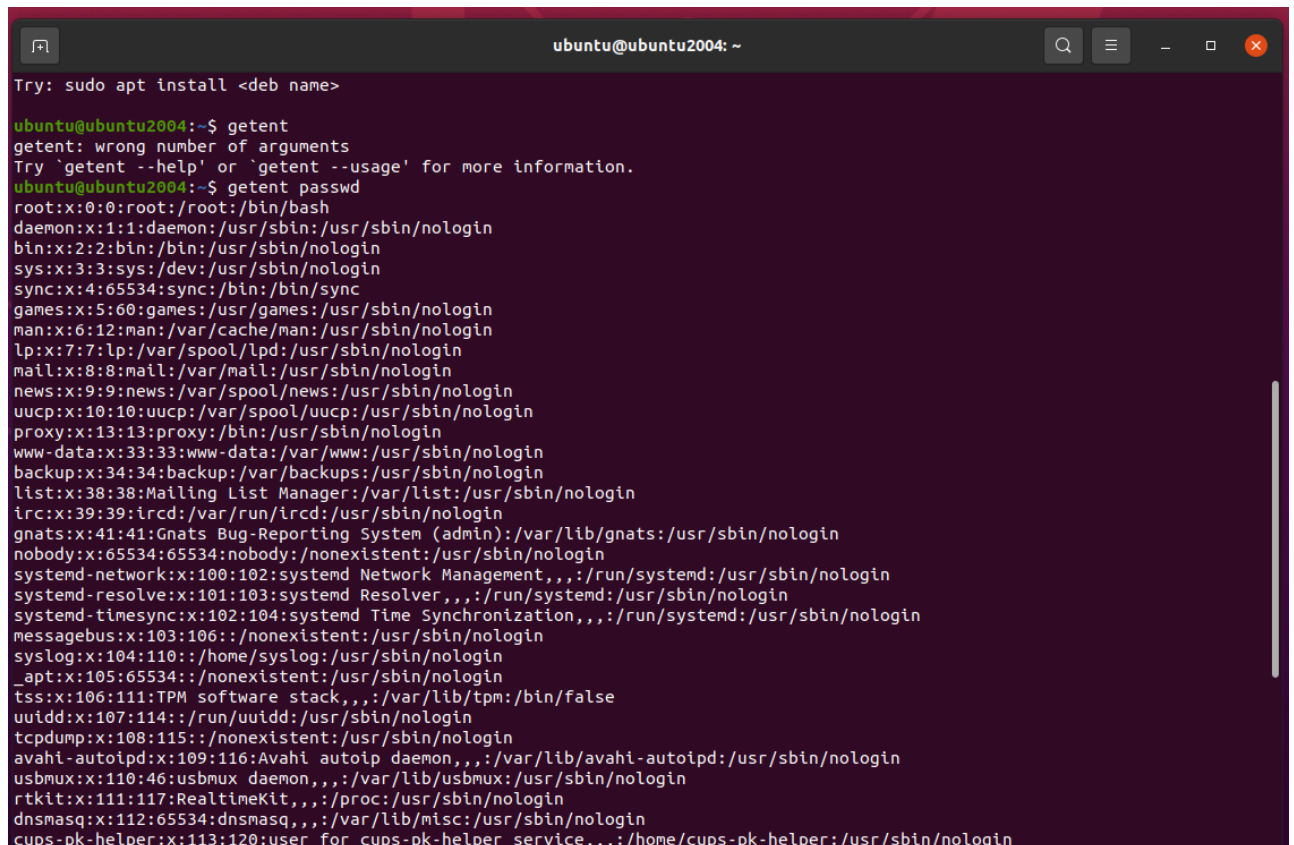
		Білошицький Р.М.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		31

РОЗДІЛ 2 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЛОКАЛЬНОЇ БЕЗПЕКИ ОС LINUX.

2.1.Робота з користувачами

Першим завданням буде видалення невикористовуваних реєстраційних записів і додаванням трьох. Необхідно додати користувачів наприклад anna і pavel , а також одного користувача з ім'ям systemuser для системних потреб.

Початково файл користувацьких реєстраційних записів може мати наступний вигляд:



```
ubuntu@ubuntu2004: ~  
Try: sudo apt install <deb name>  
ubuntu@ubuntu2004:~$ getent  
getent: wrong number of arguments  
Try 'getent --help' or 'getent --usage' for more information.  
ubuntu@ubuntu2004:~$ getent passwd  
root:x:0:0:root:/root:/bin/bash  
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:13:13: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  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin  
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin  
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin  
messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin  
syslog:x:104:110:/:/home/syslog:/usr/sbin/nologin  
_apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin  
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false  
uidd:x:107:114:/:/run/uidd:/usr/sbin/nologin  
tcpdump:x:108:115:/:/nonexistent:/usr/sbin/nologin  
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin  
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin  
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin  
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin  
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
```

Рисунок 2.1 – Результат виконання команди getent

Залежно від встановлених програм вміст цього файлу може відрізнятися від зображеного.

З міркувань безпеки варто видалити такі системні записи, які не використовуються в цій конфігурації сервера: adm, lp, shutdown, halt, news, operator, games, ftp. Запис системи lp використовується лише тоді, коли до комп'ютера підключений принтер. Налаштований комп'ютер діє як маршрутизатор, тому цей журнал зайвий. Вимкнення запису дозволяє регулярним програмам вимикати

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
Арк.		№ докум.	Підпис	Дата		32

комп'ютер, що є лише додатковим порушенням безпеки для сервера. Games використовується програмами графічного інтерфейсу, і оскільки останній відсутній на маршрутизаторі, цей обліковий запис також є зайвим.

Щоб видалити користувачів, потрібно виконати команду для кожного облікового запису:

userdel <ім'я користувача>

У реалізації це буде виглядати так:

```
ubuntu@ubuntu2004:~$ userdel games
userdel: Permission denied.
userdel: cannot lock /etc/passwd; try again later.
ubuntu@ubuntu2004:~$ sudo userdel games
ubuntu@ubuntu2004:~$ sudo userdel lp
userdel: user lp is currently used by process 697
ubuntu@ubuntu2004:~$ sudo userdel news
ubuntu@ubuntu2004:~$
```

Рисунок 2.2 – Видалення зайвих користувачів

Перша частина поставленого завдання виконано. Далі необхідно додати зазначених користувачів.

```
ubuntu@ubuntu2004:~$ sudo useradd -m -s /bin/bash -c 'Normal user' -d /home/pavel -g users pavel
ubuntu@ubuntu2004:~$ sudo useradd -m -s /bin/bash -c 'Normal user' -d /home/pavel -g users anna
useradd: warning: the home directory /home/pavel already exists.
useradd: Not copying any file from skel directory into it.
ubuntu@ubuntu2004:~$ sudo useradd -m -s /bin/bash -c 'Normal user' -d /home/anna -g users anna
useradd: user 'anna' already exists
ubuntu@ubuntu2004:~$ sudo useradd -r -s /sbin/nologin -c 'System User' -d /var/empty systemuser
ubuntu@ubuntu2004:~$
```

Рисунок 2.3 – Додавання потрібних користувачів

Наведені команди створюють в системі зазначених користувачів, проте, для входу в систему звичайним користувачем додатково до всього слід задати ще і пароль. Це виконують наведені нижче команди:

```
ubuntu@ubuntu2004:~$ sudo passwd anna
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ubuntu2004:~$ sudo passwd pavel
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ubuntu2004:~$
```

Рисунок 2.4 – Надання паролей користувачам

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
Арк.		№ докум.	Підпис	Дата		33

В результаті ми отримаємо всі необхідні системні журнали для нормальної роботи, а також двох користувачів anna та ravel, які зможуть увійти та працювати в системі.

2.2. Налаштування захищеної конфігурації web-портала

Припустимо, що всі файли об'єкта захисту, тобто веб-порталу, знаходяться в каталозі /www. У свою чергу, каталог /www містить каталоги ftp та html : перший - для зберігання та доступу до файлів через FTP, другий - для доступу до файлів через HTTP. Щоб забезпечити ефективний захист, файли в каталозі /www мають бути лише для читання користувачів ftpuser та nobody. Файли в каталозі /www/ftp повинні бути доступними для читання та запису як для ftpuser, так і користувачеві nobody. У свою чергу, файли каталогів /www/html повинні бути доступні лише користувачу nobody і з правами тільки на читання. Привілейований користувач завжди має право читати та писати, незалежно від прав доступу, встановлених для файлу.

У Linux, nobody - ім'я користувача, який не є власником жодного файлу, який не перебуває ні в одній привілейованій групі, і не має ніяких повноважень, крім стандартних для звичайних користувачів. Nogroup є груповим аналогом nobody користувача. Він використовується для непривілейованих процесів, так що навіть якщо щось піде не так, у процесу не буде дозволу завдати серйозної шкоди важливому користувачеві або групі.

Оскільки nobody і ftpuser належать до однієї групи nogroup, права на каталог /www можна встановити наступним чином:

```
ubuntu@ubuntu2004:~$ sudo chmod 050 www
ubuntu@ubuntu2004:~$ sudo chown root:nogroup www
ubuntu@ubuntu2004:~$ ls -l
total 36
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Desktop
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Documents
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Downloads
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Music
drwxr-xr-x 2 ubuntu ubuntu 4096 Jun 11 00:53 Pictures
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Public
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Templates
drwxr-xr-x 2 ubuntu ubuntu 4096 Feb  6 02:39 Videos
d---r-x--- 2 root  nogroup 4096 Jun 11 01:02 www
ubuntu@ubuntu2004:~$
```

Рисунок 2.5 – Встановлення прав на каталоги

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
Арк.		№ докум.	Підпис	Дата		34

Перша команда встановлює права на читання та права входу для користувачів групи власників каталогів. Друга команда змінює групу власників каталогів на групу nogroup. Третя команда дозволяє переглянути внесені зміни. Як видно з результату третьої команди, каталог www тепер має права доступу лише для читання та входу в систему для групи, жодних прав для власника користувача та всіх інших.

Тепер, коли обидва користувачі системи мають доступ до каталогу www, необхідно розмежувати права на внутрішні каталоги www.

```
ubuntu@ubuntu2004:~$ sudo chown -R ftpuser:nogroup www/ftp
ubuntu@ubuntu2004:~$ sudo chmod -R o-rwx www/ftp
ubuntu@ubuntu2004:~$ sudo chmod -R ug+rw www/ftp
ubuntu@ubuntu2004:~$ sudo chown -R nobody:root www/html
ubuntu@ubuntu2004:~$ sudo chmod -R go-rwx www/html
ubuntu@ubuntu2004:~$ sudo chmod -R u+r www/html
ubuntu@ubuntu2004:~$ ls -l www
ls: Terminal: can't open directory 'www': Permission denied
ubuntu@ubuntu2004:~$ sudo ls -l www
total 0
-rw-rw---- 1 ftpuser nogroup 0 Jun 11 01:02 ftp
-rw----- 1 nobody root 0 Jun 11 01:02 html
ubuntu@ubuntu2004:~$
```

Рисунок 2.6 – Доступ до каталогів веб портала

Перша команда змінює групу-власника і користувача-власника для каталогу ftp, друга - скасовує всі права на операції з файлами для всіх інших, третя - додає права на читання і запис для користувача-власника і групи-власника. Ключ -R дозволяє рекурсивно змінити параметри у поточного каталогу і всіх підкаталогів і файлів, що зберігаються в ньому. Наступна команда "chown -R nobody: root /www/html" дозволяє змінити користувача-власника для каталогу html і всіх його підкаталогів і файлів на користувача nobody. Команда "chmod -R go-rwx /www/html" скасовує всі права для групи-власника і всіх інших. Далі команда "chmod -R u + r /www/html" встановлює права тільки на читання для користувача-власника. Остання команда виводить результат виконаних операцій на екран. Задача виконана.

2.3 Налаштування комплексного захисту сервера з використанням розширених атрибутів.

Для реалізації поставленого завдання необхідно спочатку визначити, які файли в процесі роботи можуть бути змінені, а які можуть бути змінені тільки у спеціальному режимі, наприклад, тільки в режимі профілактики або оновленні програмного забезпечення. В даному випадку спеціальний режим передбачає переведення системи в одного користувача режиму роботи.

У загальному випадку при нормальних умовах вміст наступних каталогів не повинен змінюватися або може змінюватися, але досить рідко:

`/boot/etc` - в доопрацьованій системі вміст цих каталогів не повинен змінюватися. За рідкісними винятками вміст каталогу `/etc` може змінитися при зміні конфігурації будь-яких програм або служб.

`/bin` - каталог містить виконувані файли, які можна змінювати, видаляти або додавати тільки при оновленні програмного забезпечення.

`/sbin` - в цьому каталозі зберігаються виконувані файли системних програм, більшість з яких можуть виконуватися тільки привілейованим користувачем і також не повинні змінюватися під час роботи системи.

`/lib` - це каталог системних бібліотек, який також можна змінити тільки при оновленні програмних продуктів.

Наступні команди дозволяють встановити незмінний атрибут для зазначених вище каталогів і для всіх файлів в них.

```
ubuntu@ubuntu2004:~$ sudo chattr -R +i /boot /etc /bin /sbin /lib
```

Рисунок 2.7 –Встановлення атрибуту immutable

Параметр `-R` як і в попередніх прикладах використовується для рекурсивної установки атрибута для всіх файлів і каталогів, розташованих нижче в ієрархії.

Каталог `/usr` має свою власну ієрархію. У цій ієрархії такі каталоги повинні

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		36

мати встановлений прапор immutable:

/usr/bin/usr/sbin/usr/lib/usr/local/bin/usr/local/sbin/usr/local/lib - перераховані каталоги мають те ж значення, що і однойменні каталоги кореневої ієрархії.

/usr/include/usr/local/include - обидва каталоги містить головні файли для компільованих програм. Заголовки не повинні змінюватися ні за яких умов, ну хіба тільки тоді, коли комп'ютер використовується для розробки програмного забезпечення і в заголовки вносяться зміни.

```
ubuntu@ubuntu2004:~$ sudo chattr -R +i /usr/bin /usr/sbin /usr/lib /usr/include
```

Рисунок 2.8 –Встановлення атрибуту immutable

```
ubuntu@ubuntu2004:~$ lsattr /usr
---i-----e----- /usr/lib
-----e----- /usr/libx32
---i-----e----- /usr/include
---i-----I--e----- /usr/bin
-----e----- /usr/src
-----I--e----- /usr/share
-----e----- /usr/local
---i-----I--e----- /usr/sbin
-----e----- /usr/libexec
-----e----- /usr/lib64
-----e----- /usr/lib32
-----e----- /usr/games
```

Рисунок 2.9 – Результати виконання команди lsattr /usr

2.4 Розділення дискового простору між користувачами з використанням механізму квот.

Призначені для користувача квоти поширюються на окремий розділ жорсткого диска і активізуються при завантаженні системи. Для включення підтримки квот необхідно в файлі /etc/fstab для розділу /home додати параметр usrquota або grpquota, або обидва цих параметра, якщо потрібна підтримка квоти для користувачів і груп одночасно. В даному випадку для реалізації поставленого завдання необхідний тільки параметр usrquota.

Рядок файлу /etc/fstab, що відноситься до розділу /home, після зміни може мати наступний вигляд:

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				37
Арк.		№ докум.	Підпис	Дата		

/Dev/hda3/home ext2 default, usrquota 1 2

Оскільки версії ядер починаючи з гілки 2.4 підтримують новий формат користувальницьких квот, який має деякі переваги перед старою версією, використання нової версії буде набагато доцільніше. Вся подальша настройка проводиться за цим обліком.

Для активації користувача квот необхідно перезавантажити систему. При завантаженні необхідно виконати перевірку квоти розділу, що можна зробити запуском програми `quotacheck`, а також включити механізм квот виконанням програми `quotaon`. Ці обидві програми мають безліч параметрів командного рядка, про які можна дізнатися з man-посібників, що входять в пакет `quota`.

Стандартний рядок запуску цих програм, яка підходить для більшості систем, може мати вигляд:

`quotacheck -aug`

`quotaon -aug`

Параметр командного рядка `-a` повідомляє програмі, що необхідно виконати перевірку всіх файлових систем, перерахованих у файлі `fstab`, на яких включена підтримка квот, і які не є файловими системами NFS. Параметр `-u` вказує виконати перевірку квот для користувачів на розділах, перерахованих у файлі `/etc/mtab`. Файл `/etc/mtab` модифікується при монтуванні і размонтированні будь-якої файлової системи і містить всі файлові системи, змонтовані на поточний момент. Параметр `-g` виконує ту ж функцію, що і параметр `-u`, але тільки для груп. Останній параметр не має значення, якщо квота включена тільки для користувачів, але, щоб в подальшому при зміні конфігурації не виникало проблем, рекомендую додавати цей параметр.

Бажано зробити так, щоб механізм квот активувався відразу після монтування файлових систем. Монтування файлових систем при запуску Linux Ubuntu виконується в файлі `/etc/rc.d/init.d/rc.sysinit`. У тому ж файлі відразу після монтування слід код, який запускає програми `quotacheck` і `quotaon` з зазначеними параметрами, якщо вони присутні в системі. Отже, для Linux Ubuntu додавати код запуску програм не потрібно, оскільки він вже присутній за замовчуванням. Для інших версій ОС Linux цей код, можливо, доведеться додавати вручну.

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		38

Під час завантаження системи програма quotacheck виконає перевірку файлових систем з включеними квотами на наявність файлів квот і, якщо файли відсутні, quotacheck створить їх в кореневому каталозі цієї файлової системи. В даному випадку в каталозі /home з'явиться файл aquota.user, в якому буде зберігатися інформація про користувача квоти.

Далі, використовуючи програму setquota, необхідно виконати настройку квот для кожного користувача, що має домашній каталог в розділі /home. Це можна зробити командою:

```
[root@app /]# setquota -u <ім'я_користувача> 10240 0 1000 0 /dev/hda3
```

Наведена команда встановить обмеження дискового простору в 10 Мбайт з максимальною кількістю можливих файлів - 1000 для зазначеного користувача. Для користувача anna ця команда буде мати вигляд:

```
[Root @ app /] # setquota -u anna 10240 0 1000 0 /dev/hda3
```

Якщо квота інших користувачів повинна бути ідентична наведеної, що як раз і потрібно для реалізації, квоту користувача anna можна використовувати як шаблон. Далі при створенні квоти для користувача igor параметри квотування користувача anna просто копіюються:

```
[Root @ app /] # setquota -u -p anna igor /dev/hda3
```

В результаті виконання команди користувач igor отримує ті ж налаштування квоти, що і користувач anna, в даному випадку йому виділяється 10 Мбайт на зберігання 1 000 файлів. Вищенаведену команду необхідно виконати для всіх користувачів системи.

Перегляд зроблених налаштувань дозволяє виконати програма repquota. Виклик цієї програми з параметрами -a виводить досить чіткий детальний звіт по всім файловим системам з підтримкою квот.

2.5 Утиліта CryptSetup на Linux Mint

Утиліта Cryptsetup дозволяє полегшити шифрування розділу Linux за допомогою модуля dm-crypt. Давайте спочатку її встановимо.

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				39
	Арк.	№ докум.	Підпис	Дата		

В Mint або Ubuntu, для цього використовуйте таку команду:

`sudo apt install cryptsetup`

```
oem@BRM-VirtualBox:~$ sudo apt install cryptsetup
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей
Зчитування інформації про стан... Виконано
cryptsetup вже є новою версією (2:2.2.2-3ubuntu2.3).
оновлено 0, встановлено 0 нових, 0 відмічено для видалення і 96 не оновлено.
oem@BRM-VirtualBox:~$
```

Рисунок 2.10 – Встановлення утиліти cryptsetup

Синтаксис запуску команд такий:

\$ Cryptsetup опції операція параметри_операції

Розглянемо основні операції, які можна зробити за допомогою цієї утиліти:

```
oem@BRM-VirtualBox:~$ cryptsetup luksAddKey
Використання: cryptsetup [-?Vvyrq] [-?|--help] [--usage] [-V|--version]
[-v|--verbose] [--debug] [--debug-json] [-c|--cipher=STRING]
[-h|--hash=STRING] [-y|--verify-passphrase] [-d|--key-file=STRING]
[--master-key-file=STRING] [--dump-master-key] [-s|--key-size=БІТИ]
[-l|--keyfile-size=байти] [--keyfile-offset=байти]
[--new-keyfile-size=байти] [--new-keyfile-offset=байти]
[-S|--key-slot=INT] [-b|--size=СЕКТОРИ] [--device-size=байти]
[-o|--offset=СЕКТОРИ] [-p|--skip=СЕКТОРИ] [-r|--readonly]
[-q|--batch-mode] [-t|--timeout=секунди]
[--progress-frequency=секунди] [-T|--tries=INT]
[--align-payload=СЕКТОРИ] [--header-backup-file=STRING]
[--use-random] [--use-urandom] [--shared] [--uuid=STRING]
[--allow-discards] [--header=STRING] [--test-passphrase]
[--tcrypt-hidden] [--tcrypt-system] [--tcrypt-backup] [--veracrypt]
[--veracrypt-pim=INT] [--veracrypt-query-pim] [-M|--type=STRING]
[--force-password] [--perf-same-cpu-crypt]
[--perf-submit-from-crypt-cpus] [--deferred]
[--serialize-memory-hard-pbkdf] [-i|--iter-time=mc] [--pbkdf=STRING]
[--pbkdf-memory=кілобайти] [--pbkdf-parallel=threads]
[--pbkdf-force-iterations=LONG] [--priority=STRING] [--disable-locks]
[--disable-keyring] [-I|--integrity=STRING] [--integrity-no-journal]
[--integrity-no-wipe] [--token-only] [--token-id=INT]
[--key-description=STRING] [--sector-size=INT] [--persistent]
[--label=STRING] [--subsystem=STRING] [--unbound]
[--json-file=STRING] [--luks2-metadata-size=байти]
[--luks2-keyslots-size=байти] [--refresh] [--keyslot-key-size=БІТИ]
[--keyslot-cipher=STRING] [--encrypt] [--decrypt] [--init-only]
```

Рисунок 2.11 – Перелік операцій утиліти cryptsetup

Параметри операції залежать від самої операції, зазвичай це або фізичний пристрій, з яким потрібно провести дію, або віртуальний або і те й інше.

Давайте оберемо диск для шифрування.

Команда `fdisk` дозволить перевірити які диски існують і доступні для шифрування.

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				40
Арк.		№ докум.	Підпис	Дата		

```

oem@BRM-VirtualBox:~$ sudo fdisk -l
Диск /dev/sda: 13 GiB, 13958643712 байтів, 27262976 секторів
Модель диска: VBOX HARDDISK
Одиниці: секторів з 1 * 512 = 512 байтів
Розмір сектора (логічного/фізичного): 512 байтів / 512 байтів
Розмір введення-виведення (мінімальний/оптимальний): 512 байтів / 512 байтів
Тип мітки диска: dos
Ідентифікатор диска: 0xec4b4836

Пристрій   Заван.  Початок   Кінець   Сектори  Розмір  Ід Тип
/dev/sda1  *       2048      1050623  1048576   512M    b W95 FAT32
/dev/sda2              1052670  27260927 26208258  12,5G    5 Extended
/dev/sda5              1052672  2549759  1497088   731M    83 Linux
/dev/sda6              2551808  27260927 24709120  11,8G    83 Linux

Диск /dev/mapper/sda6_crypt: 11,79 GiB, 12634292224 байтів, 24676352 секторів
Одиниці: секторів з 1 * 512 = 512 байтів
Розмір сектора (логічного/фізичного): 512 байтів / 512 байтів
Розмір введення-виведення (мінімальний/оптимальний): 512 байтів / 512 байтів

Диск /dev/mapper/vgmint-root: 10,8 GiB, 11572084736 байтів, 22601728 секторів
Одиниці: секторів з 1 * 512 = 512 байтів
Розмір сектора (логічного/фізичного): 512 байтів / 512 байтів
Розмір введення-виведення (мінімальний/оптимальний): 512 байтів / 512 байтів

Диск /dev/mapper/vgmint-swap_1: 976 MiB, 1023410176 байтів, 1998848 секторів
Одиниці: секторів з 1 * 512 = 512 байтів

```

Рисунок 2.12 – Перевірка дисків для шифрування

Для прикладу використаємо пристрій /dev/mapper/sda6_crypt. Включимо утиліту parted і вкажемо роді аргумента ім'я диску.

Наприклад:

```

oem@BRM-VirtualBox:~$ sudo parted /dev/mapper/sda6_crypt
GNU Parted 3.3
Використовується /dev/mapper/sda6_crypt
Ласкаво просимо до GNU Parted! Перелік команд виводиться командою 'help'.
(parted) █

```

Рисунок 2.13 – Використання утиліти parted

Тепер треба розмітити таблицю розділів як GPT:

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		41

```

(parted) sudo mktable gpt
align-check ТИП N                перевірити розділ N щодо ТИПу(min|opt) вирівнювання
help [КОМАНДА]                   вивести загальну довідку, або довідку про КОМАНДА
mklabel,mktable ТИП ЕТИКЕТКИ     створити нову позначку диска (таблицю розділів)
mkpart ТИП-РОЗДІЛУ [ТИП-ФС] ПОЧАТОК КІНЕЦЬ створити розділ
name НОМЕР НАЗВА                 призначити назву НАЗВА розділу НОМЕР
print [devices|free|list,all|ЧИСЛО] відображає таблицю розділів, наявні пристрої, вільний
                                простір, всі знайдені розділи, або певний розділ
quit                             вихід з програми
rescue ПОЧАТОК КІНЕЦЬ           знайти втрачені розділи між ПОЧАТОК та КІНЕЦЬ
resizepart НОМЕР КІНЕЦЬ        змінити розмір розділу з номером НОМЕР
rm НОМЕР                        видалити розділ з номером НОМЕР
select ПРИСТРІЙ                вибирати пристрій для роботи
disk_set ПРАПОРЕЦЬ СТАН        змінити значення ПРАПОРЦЯ для вибраного пристрою
disk_toggle [ПРАПОРЕЦЬ]        перемкнути стан ПРАПОРЦЯ на вибраному пристрої
set НОМЕР ОЗНАКА СТАН          змінити ознаку розділу з номером НОМЕР
toggle [НОМЕР [ОЗНАКА]]        перемикнути ознаку ОЗНАКА розділу з номером НОМЕР
unit БЛОК                      встановити для типового блоку значення БЛОК
version                         вивести поточну версію GNU Parted та інформацію про авторське
                                право
Попередження: Існуюча позначка диска на /dev/mapper/sda6_crypt буде знищена разом з усіма даними
на ній. Продовжити?
Так/Yes/Hi/No? yes

```

Рисунок 2.14 – Розмітка таблиці розділів

Створюємо один основний розділ з номером 1 на весь диск:

```

(parted) mkpart primary 1 -1
(parted) quit
Інформація: Не забудьте оновити /etc/fstab, якщо це необхідно.

```

Рисунок 2.15 – Створення розділу

Для створення 2048-бітного ключа потрібно вказати його розташування:

```

oem@BRM-VirtualBox:~$ sudo dd if=/dev/urandom of=/dev/secret.key bs=1024 count=2
2+0 записів прочитано
2+0 записів записано
скопійовано 2048 байтів (2,0 kB, 2,0 KiB), 0,00211405 s, 969 kB/s
oem@BRM-VirtualBox:~$

```

Рисунок 2.16 – Створення секретного ключа

Коригуємо права файлу, дозвіл тільки на читання:

```

oem@BRM-VirtualBox:~$ sudo chmod 0400 /dev/secret.key
oem@BRM-VirtualBox:~$

```

Рисунок 2.17 – Дозвіл тільки на читання

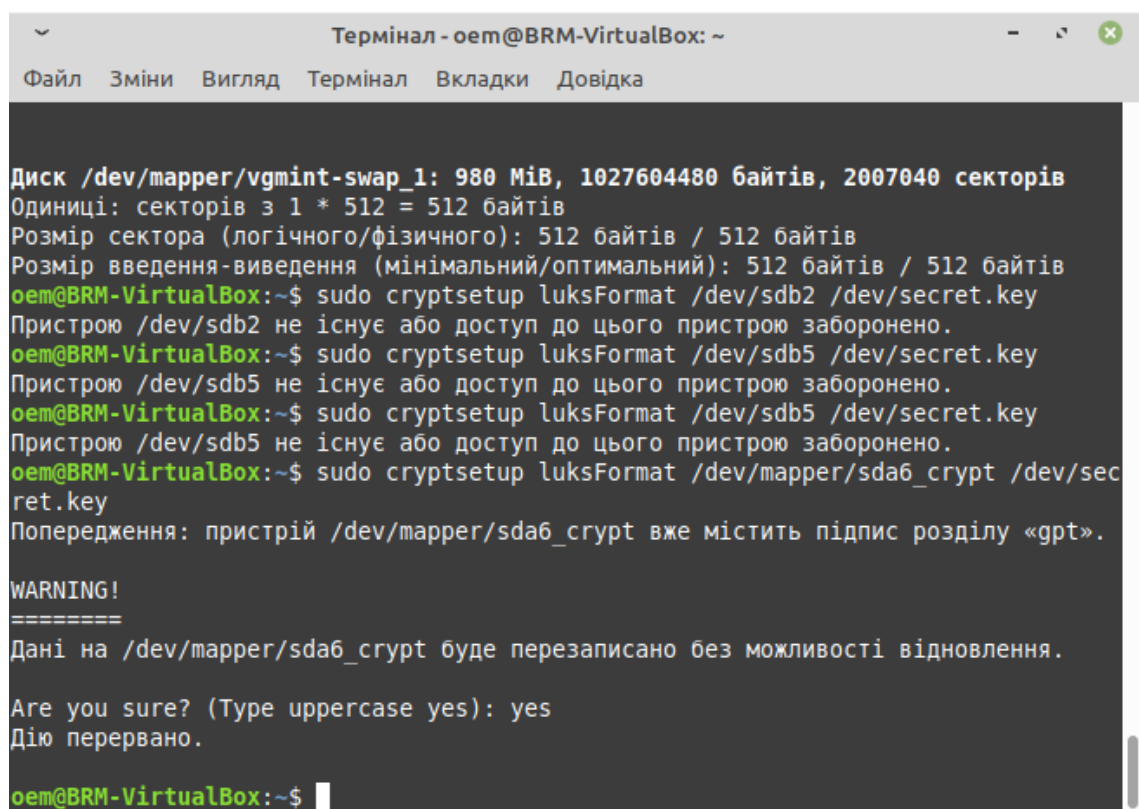
		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		42

У разі спроби несанкціонованого доступу до вашого диску, третім особам буде необхідно мати ключ для розшифрування даних на диску. Не слід повідомляти шлях до ключа нікому!

За допомогою створеного ключа створимо LUKS-розділ.

Це приклад з використанням ключа, також актуальний спосіб з ключовою фразою.

cryptsetup luksFormat /dev/secret.key



```
Термінал - oem@BRM-VirtualBox: ~
Файл  Зміни  Вигляд  Термінал  Вкладки  Довідка

Диск /dev/mapper/vgmint-swap_1: 980 MiB, 1027604480 байтів, 2007040 секторів
Одиниці: секторів з 1 * 512 = 512 байтів
Розмір сектора (логічного/фізичного): 512 байтів / 512 байтів
Розмір введення-виведення (мінімальний/оптимальний): 512 байтів / 512 байтів
oem@BRM-VirtualBox:~$ sudo cryptsetup luksFormat /dev/sdb2 /dev/secret.key
Пристрою /dev/sdb2 не існує або доступ до цього пристрою заборонено.
oem@BRM-VirtualBox:~$ sudo cryptsetup luksFormat /dev/sdb5 /dev/secret.key
Пристрою /dev/sdb5 не існує або доступ до цього пристрою заборонено.
oem@BRM-VirtualBox:~$ sudo cryptsetup luksFormat /dev/sdb5 /dev/secret.key
Пристрою /dev/sdb5 не існує або доступ до цього пристрою заборонено.
oem@BRM-VirtualBox:~$ sudo cryptsetup luksFormat /dev/mapper/sda6_crypt /dev/secret.key
Попередження: пристрій /dev/mapper/sda6_crypt вже містить підпис розділу «gpt».

WARNING!
=====
Дані на /dev/mapper/sda6_crypt буде перезаписано без можливості відновлення.

Are you sure? (Type uppercase yes): yes
Дію перервано.

oem@BRM-VirtualBox:~$
```

Рисунок 2.18 – LUKS-розділ

Зв'яжемо ключ до розділу, що згодом дозволить його авторизувати і приховати підказку пароля:

cryptsetup luksAddKey /dev/secret.key --key-file = /root/secret.key

До початку використання LUKS-розділу його слід коректно відобразити і відформатувати. Використаємо опцію luksOpen для створення пристрою введення-виведення і взаємодії з розділом:

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		43

```
cryptsetup luksOpen /dev secret --key-file = /root/secret.key
```

Пристрій введення-виведення LUKS буде доступним в /dev/mapper/secret.

Тепер вкажемо розмір розділу LUKS:

```
cryptsetup resize secret
```

Використання опції `resize` без додаткових змінних передбачає, що розмір базового розділу буде зайнятий максимальний.

Створимо файлову систему, наприклад `ext4`:

```
mkfs.ext4 /dev/mapper/secret
```

Тепер проконтролюймо стан пристрою за допомогою такої команди:

```
cryptsetup -v status secret
```

Для перегляду інформації заголовку LUKS:

```
cryptsetup luksDump /dev
```

Як монтувати LUKS-розділ:

Створимо оптимальну для нас точку монтування та встановимо права:

```
sudo chmod 755 /secret
```

Монтуємо пристрій LUKS:

```
mount /dev/mapper/secret/secret
```

Для перевірки коректності монтування диска використаємо команду команду:

```
df -h
```

Не рекомендується автоматичне монтування шифрованого розділу, тому що при завантаженні системи дані також автоматично будуть розшифровані.

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				44
	Арк.	№ докум.	Підпис	Дата		

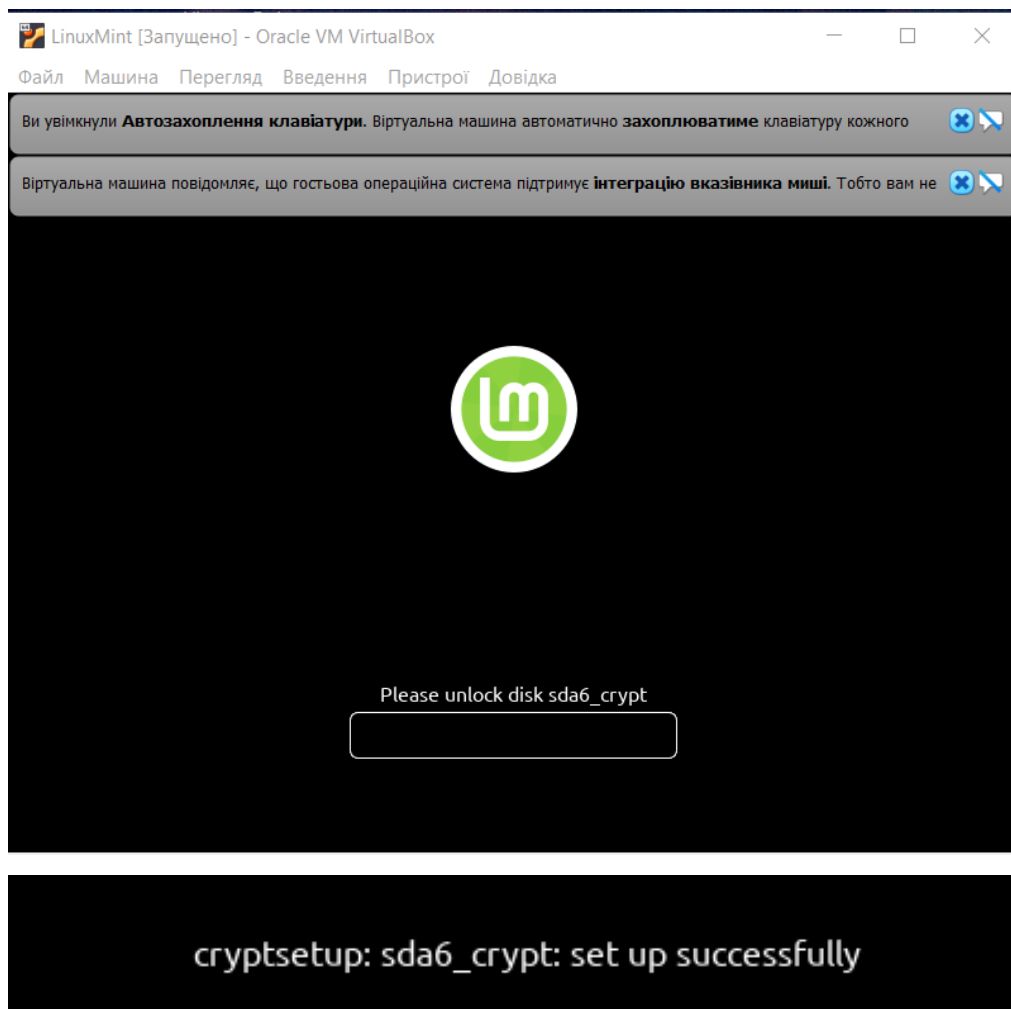


Рисунок 2.19-20 – Результат шифрування та монтування диску(розділу)

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				45
Арк.	№ докум.	Підпис	Дата			

РОЗДІЛ 3. МЕРЕЖЕВИЙ ЗАХИСТ ОС LINUX MINT

3.1. Міжмережний екран в Linux Mint

В операційній системі Linux Mint як фільтр пакетів використовується Netfilter, який входить до складу ядра і розробляється групою Netfilter Core Team. Для управління його налаштуваннями використовується утиліта командного рядка iptables, що розробляється паралельно цим же проектом. Процес налаштування вимагає деякого розуміння протоколів, використовуваних при обміні інформації в Інтернеті, і назвати його простим можна. Хоча тема налаштування netfilter / iptables вже не є новою, в глобальній мережі можна знайти не один десяток документів, що описують як його пристрій, так і самі команди.

За замовчуванням UFW завжди відключений, і перед запуском демона його необхідно активувати, замінивши в файлі /etc/ufw/ufw.conf рядок

ENABLED = no

ENABLED = yes

```
roman@roman-VirtualBox:~$ sudo cat /etc/ufw/ufw.conf
[sudo] пароль до roman:
# /etc/ufw/ufw.conf
#
# Set to yes to start on boot. If setting this remotely, be sure to add a rule
# to allow your remote connection before starting ufw. Eg: 'ufw allow 22/tcp'
ENABLED=yes
# Please use the 'ufw' command to set the loglevel. Eg: 'ufw logging medium'.
# See 'man ufw' for details.
LOGLEVEL=low
roman@roman-VirtualBox:~$
```

Рисунок 3.1 – Увімкнення утиліти UFW

Інакше при спробі його запуску командою `sudo /etc/init.d/ufw start` буде отримано відмову.

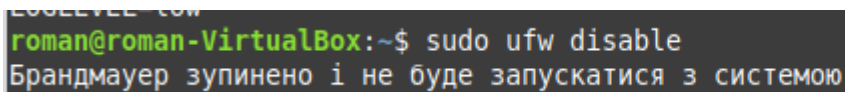
Крім безпосереднього редагування конфігураційних файлів настройки можна проводити за допомогою консольної утиліти `ufw`. Наприклад, щоб активувати `ufw` і дозволити її завантаження, при старті системи можна зробити наступним чином:

		Білошицький Р.М.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				46
	Арк.	№ докум.	Підпис	Дата		

```
sudo ufw enable
```

Відключити також просто:

```
sudo ufw disable
```

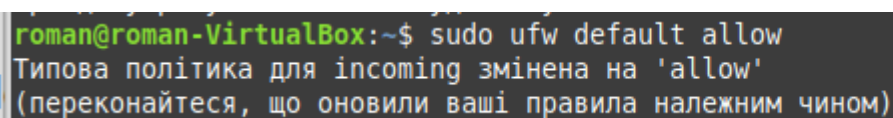


```
roman@roman-VirtualBox:~$ sudo ufw disable
Брандмауер зупинено і не буде запускатися з системою
```

Рисунок 3.2 - Відключення утиліти UFW

Існує дві глобальні політики: все дозволено і все заборонено. Перша активується за допомогою команди

```
sudo ufw default allow
```



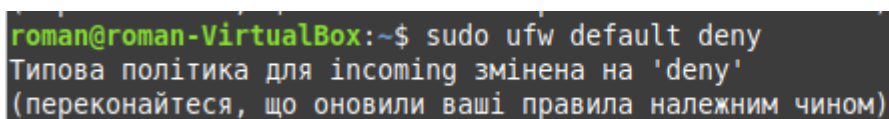
```
roman@roman-VirtualBox:~$ sudo ufw default allow
Типова політика для incoming змінена на 'allow'
(переконайтеся, що оновили ваші правила належним чином)
```

Рисунок 3.3 – Зміна політики incoming на allow

Політика за замовчуванням incoming змінена на allow.

Щоб заборонити всі підключення, використовується команда

```
sudo ufw default deny
```



```
roman@roman-VirtualBox:~$ sudo ufw default deny
Типова політика для incoming змінена на 'deny'
(переконайтеся, що оновили ваші правила належним чином)
```

Рисунок 3.4 – Зміна політики incoming на allow

За допомогою ufw дуже просто дозволити або заборонити вхідні з'єднання для сервісу, описаного в /etc/services, або конкретного порту / протоколу.

У загальному випадку команда виглядає так:

```
ufw allow | deny [service]
```

Іншими словами, щоб дозволити підключення до веб-сервера, що працює на 80-му порту, необхідно зробити в такий спосіб:

```
sudo ufw allow 80 /tcp
```

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				47
	Арк.	№ докум.	Підпис	Дата		

```
roman@roman-VirtualBox:~$ sudo ufw allow 80/tcp
Правила оновлено
Правила оновлено (v6)
```

Рисунок 3.5 – Оновлення підключень

Щоб переглянути правила iptables без їх активації, необхідно додати в команду параметр - --dry-run. Параметр status дозволить дізнатися поточні настройки UFW без заглядання всередину iptables:

```
sudo ufw status
```

Видалити дозвіл на підключення до вибраного порту можна так само просто:

```
sudo ufw delete allow 80 /tcp
```

Що забороняє правило створюється аналогічно яке дозволяє, тільки замість allow використовується deny:

```
sudo ufw deny 53
```

Тепер був блокований доступ до 53-му порту. При цьому якщо раніше було створено, наприклад, дозволяє правило, яке тепер потрібно замінити на блокуючу, то це краще робити в два етапи. Спочатку відключається перше правило, а потім встановлюється друге.

Замість номера порту можна назвати сервіс по імені. Необхідно дізнатися як називається потрібний сервіс:

```
cat /etc/services | less
```

```
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
#
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux      1/tcp                                # TCP port service multiplexer
echo        7/tcp
echo        7/udp
discard     9/tcp      sink null
discard     9/udp      sink null
sysstat     11/tcp      users
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
qotd        17/tcp      quote
chargen     19/tcp      ttytst source
chargen     19/udp      ttytst source
ftp-data    20/tcp
ftp         21/tcp
fsp         21/udp      fspd
ssh         22/tcp                                # SSH Remote Login Protocol
telnet      23/tcp
```

Рисунок 3.6 – Перегляд сервісів

і включити його в правило:

```
sudo ufw allow ssh
```

```
roman@roman-VirtualBox:~$ sudo ufw allow ssh
Правила оновлено
Правила оновлено (v6)
roman@roman-VirtualBox:~$
```

Рисунок 3.7 – Включення ssh

У правилах UFW можна задавати IP-адреси (джерела і призначення). Наприклад, щоб дозволити з'єднання з внутрішньою мережі 192.168.1.0/24, використовується:

```
sudo ufw allow 191.3.1.0/24
```

або забороняє правило:

```
sudo ufw deny from 10.20.30.40
```

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				49
	Арк.	№ докум.	Підпис	Дата		

Опціонально можна вказати порт і протокол. Для того щоб дозволити підключення по SSH тільки з однієї IP-адреси слід ввести наступну команду:

sudo ufw allow from 192.168.0.20 to any port 22

```
roman@roman-VirtualBox:~$ sudo ufw allow from 191.3.1.5 to any port 22
[sudo] пароль до roman:
Правила оновлено
```

Рисунок 3.8 – Дозвіл на підключення

Для включення / відключення реєстрації використовується команда logging.

sudo ufw logging on

Файл `/etc/ufw/sysctl.conf` задає деякі системні змінні (аналог загальносистемного `/etc/sysctl.conf`). Наприклад, щоб дозволити перенаправлення пакетів, знімається коментар з рядка

net/ipv4/ip_forward = 1

До складу Linux Mint включений і графічний інтерфейс UFW - GUFW

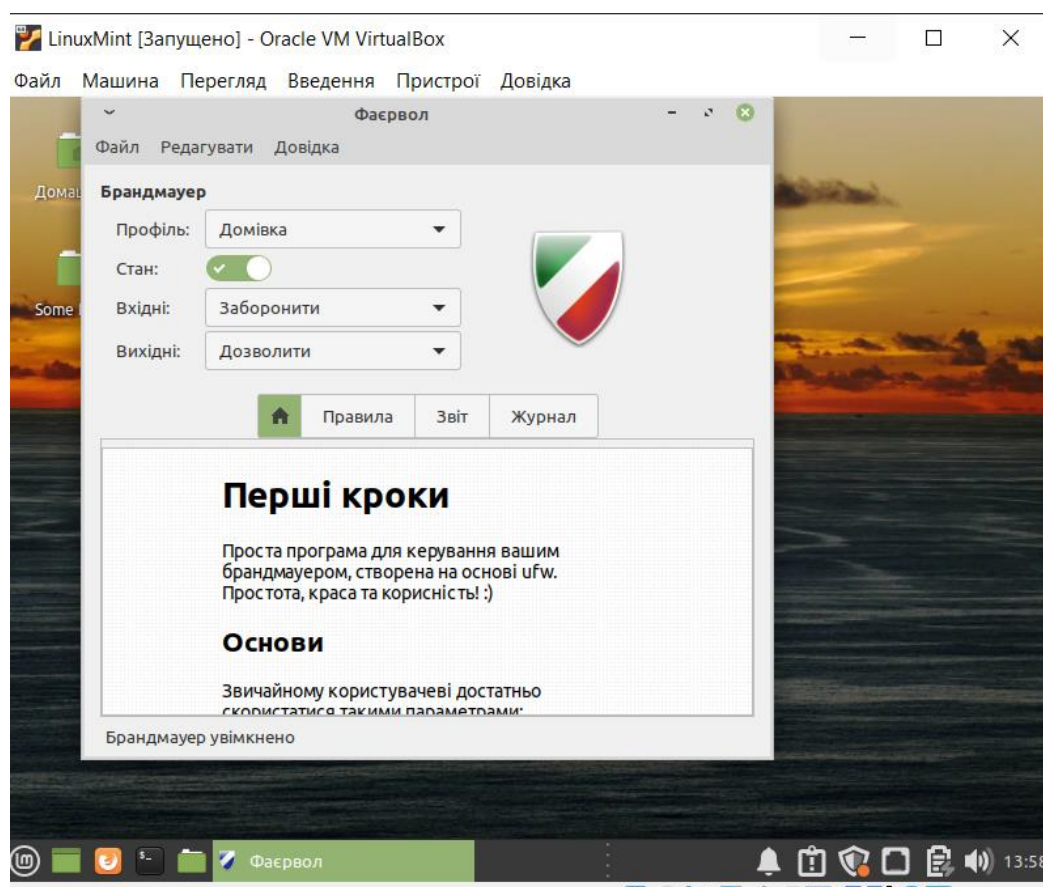


Рисунок 3.9 – Графічна оболонка GUFW

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				50
Арк.		№ докум.	Підпис	Дата		

Для запуску GFW використовується команда:

```
sudo gfw
```

Насамперед слід змінити статус роботи фаєрвола на «Включено». Але слід врахувати: на дефолтних настройках входить інформація з інтернету заборонена, а виходить перевіряється. Таким чином, весь трафік стане нагадувати вулицю з одностороннім рухом.

Також можна створити розгорнуті правила, наприклад, для специфічних завдань. Слід звернути увагу на першу з трьох вкладок «Правила». У ній задаються правила всебічного інтернет руху для додатків на зразок torrent і Skype. На жаль, не всі труднощі долаються шляхом фіксації розпоряджень для списку встановлених додатків. Крім вищезгаданого, можна залишити цінні цільові вказівки цілому переліку хостів і IP адрес, а також напрямків з'єднань.

Якщо після всіх подорожей з налагодження безпеки системи через фаєрвол, можна зробити висновок, що все можливе вже зроблено, залишиться останній сервісний штрих - прописати UFW в автозавантаження. Потрібно запустити в терміналі команду:

```
sudo update-rc.d ufw defaults
```

3.2. Захист Linux Mint від DDoS-атак

Для прикладу створимо невелику схему з декількома робочими станціями, і продемонструємо, як захистити станцію Linux Mint. Атаки проводитимуться з відомої всім Kali Linux в якій неважко організувати атаки на мережу.

Для початку створимо проект у GNS3 та додамо станції з Virtual Box до схеми.

		Білошицький Р.М.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				
	Арк.	№ докум.	Підпис	Дата		51

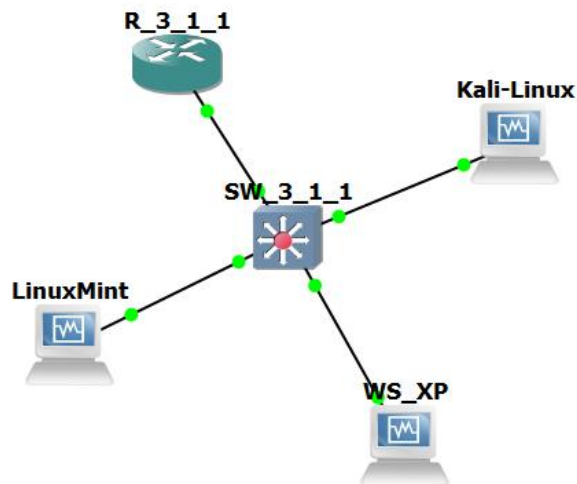


Рисунок 3.10 – Проект мережі

Тепер ми маємо провести базові налаштування пристроїв мережі.

```

SW_3_1_1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
SW_3_1_1(config)#int vlan 1
SW_3_1_1(config-if)#ip address 195.1.1.250 255.255.255.0
SW_3_1_1(config-if)#no shu
SW_3_1_1(config-if)#exit
SW_3_1_1(config)#
*Jan 27 12:16:37.180: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Jan 27 12:16:38.180: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SW_3_1_1(config)#
  
```

Рисунок 3.11 – Базові налаштування комутатора SW_3_1_1

```

R_3_1_1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R_3_1_1(config)#int fa0/0
R_3_1_1(config-if)#desc LINK_TO_SW_3_1_1
R_3_1_1(config-if)#ip address 195.1.1.254 255.255.255.0
R_3_1_1(config-if)#no shu exit
^
% Invalid input detected at '^' marker.

R_3_1_1(config-if)#
R_3_1_1(config-if)#no shu
R_3_1_1(config-if)#
*Mar 1 00:29:18.583: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:29:19.583: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R_3_1_1(config-if)#exit
R_3_1_1(config)#ip dhcp excluded address 195.1.1.250
^
% Invalid input detected at '^' marker.

R_3_1_1(config)#ip dhcp excluded-address 195.1.1.250
R_3_1_1(config)#ip dhcp excluded-address 195.1.1.254
R_3_1_1(config)#ip dhcp pool LAN-A
R_3_1_1(dhcp-config)#network 195.1.1.0 255.255.255.0
R_3_1_1(dhcp-config)#default-router 195.1.1.1
R_3_1_1(dhcp-config)#dns-server 195.1.1.1
R_3_1_1(dhcp-config)#domain-name my.net
R_3_1_1(dhcp-config)#exit
R_3_1_1(config)#

```

Рисунок 3.12 – Базові налаштування маршрутизатора R_3_1_1 та DHCP

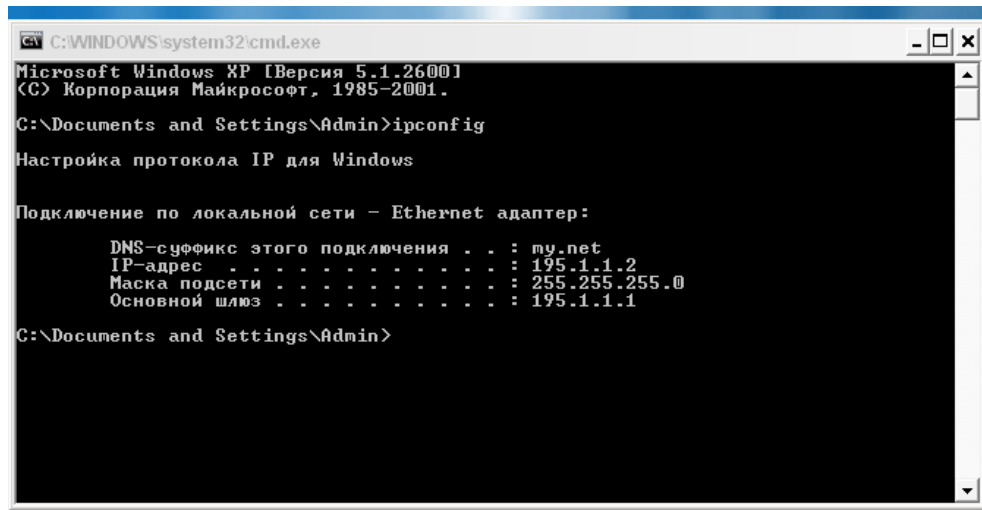


Рисунок 3.13 – Отримання DHCP адреси на Windows XP

```

kali@kali:~$ ip route
default via 195.1.1.1 dev eth0 proto dhcp metric 100
195.1.1.0/24 dev eth0 proto kernel scope link src 195.1.1.1 metric 100

```

Рисунок 3.14 – Отримання DHCP адреси на Kali Linux

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				53
Арк.		№ докум.	Підпис	Дата		

```
roman@roman-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 195.1.1.3 netmask 255.255.255.0 broadcast 195.1.1.255
inet6 fe80::3611:33da:fec2:5cff prefixlen 64 scopeid 0x20<link>
ether 08:00:27:45:8d:20 txqueuelen 1000 (Ethernet)
RX packets 505 bytes 37195 (37.1 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 620 bytes 52441 (52.4 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 19 base 0xd020
```

Рисунок 3.15 – Отримання DHCP адреси на Linux Mint

```
kali@kali:~$ sudo hping3 -S --flood -V -p 80 195.1.1.3
using eth0, addr: 195.1.1.1, MTU: 1500
HPING 195.1.1.3 (eth0 195.1.1.3): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 195.1.1.3 hping statistic ---
586175 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Рисунок 3.16 – DDos атака з Kali linux на Linux Mint

```
roman@roman-VirtualBox:~$ ping 195.1.1.2
ЛУНА-ІМПУЛЬС 195.1.1.2 (195.1.1.2) 56(84) байтів даних.
64 байтів з 195.1.1.2: icmp_seq=2 ttl=128 час=92.0 мс
64 байтів з 195.1.1.2: icmp_seq=3 ttl=128 час=270 мс
64 байтів з 195.1.1.2: icmp_seq=5 ttl=128 час=146 мс
64 байтів з 195.1.1.2: icmp_seq=6 ttl=128 час=1.77 мс
64 байтів з 195.1.1.2: icmp_seq=8 ttl=128 час=96.6 мс
^C
--- Статистика луна-імпульсів 195.1.1.2 ---
Передано 9 пакетів, отримано 5, втрачено 44,4444% пакетів, час 8048 мс
rtt мін/сер/макс/мdev = 1.765/121.372/270.301/87.841 мс
roman@roman-VirtualBox:~$ ping 195.1.1.2
ЛУНА-ІМПУЛЬС 195.1.1.2 (195.1.1.2) 56(84) байтів даних.
64 байтів з 195.1.1.2: icmp_seq=1 ttl=128 час=2.52 мс
64 байтів з 195.1.1.2: icmp_seq=2 ttl=128 час=1.91 мс
64 байтів з 195.1.1.2: icmp_seq=3 ttl=128 час=1.93 мс
64 байтів з 195.1.1.2: icmp_seq=4 ttl=128 час=2.21 мс
64 байтів з 195.1.1.2: icmp_seq=5 ttl=128 час=1.74 мс
^C
--- Статистика луна-імпульсів 195.1.1.2 ---
Передано 5 пакетів, отримано 5, втрачено 0% пакетів, час 4008 мс
rtt мін/сер/макс/мdev = 1.741/2.062/2.521/0.274 мс
```

Рисунок 3.17 – Результат атаки

```
roman@roman-VirtualBox:~$ sudo iptables -A INPUT -i eth0 -m conntrack --ctstate INVALID -j DROP
roman@roman-VirtualBox:~$ sudo iptables -A INPUT -i eth0 -p tcp
roman@roman-VirtualBox:~$ sudo iptables -A INPUT -i eth0 -p tcp ! --syn -m conntrack --ctstate NEW -j DROP
```

Рисунок 3.18 – Захист за використанням iptables

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				54
Арк.		№ докум.	Підпис	Дата		

Блокування INVALID-пакетів

```
iptables -A INPUT -i eth0 -m conntrack --ctstate INVALID -j DROP
```

Блокування нових пакетів, які не мають прапора SYN

```
iptables -A INPUT -i eth0 -p tcp! --syn -m conntrack --ctstate NEW -j DROP
```

Блокування нестандартних значень MSS

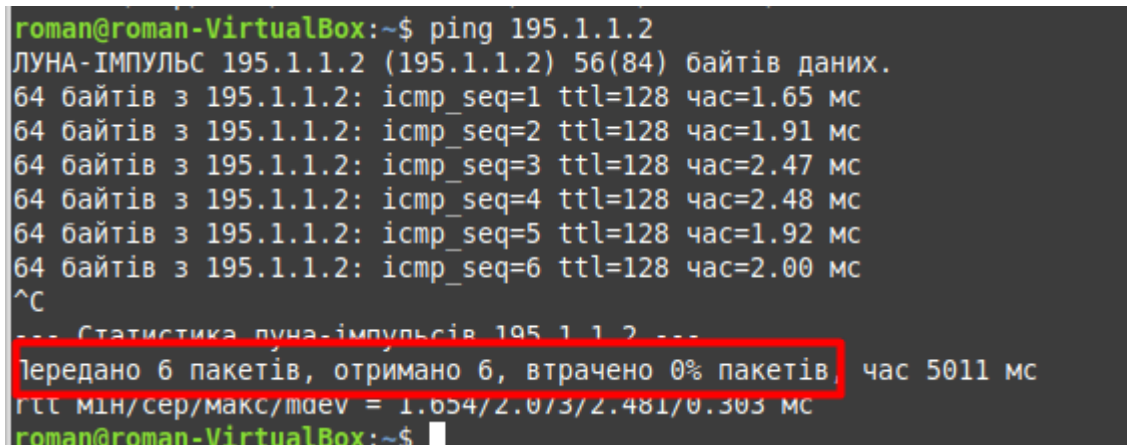
```
iptables -A INPUT -i eth0 -p tcp -m conntrack --ctstate NEW -m tcpmss! --mss 536:65535 -j DROP
```

Блокування фрагментованих пакетів

```
iptables -A INPUT -i eth0 -f -j DROP
```

Блокування пакетів з невірними TCP прапорами

```
iptables -A INPUT -i eth0 -p tcp --tcp-flags FIN, SYN, RST, PSH, ACK, URG NONE -j DROP
```



```
roman@roman-VirtualBox:~$ ping 195.1.1.2
ЛУНА-ІМПУЛЬС 195.1.1.2 (195.1.1.2) 56(84) байтів даних.
64 байтів з 195.1.1.2: icmp_seq=1 ttl=128 час=1.65 мс
64 байтів з 195.1.1.2: icmp_seq=2 ttl=128 час=1.91 мс
64 байтів з 195.1.1.2: icmp_seq=3 ttl=128 час=2.47 мс
64 байтів з 195.1.1.2: icmp_seq=4 ttl=128 час=2.48 мс
64 байтів з 195.1.1.2: icmp_seq=5 ttl=128 час=1.92 мс
64 байтів з 195.1.1.2: icmp_seq=6 ttl=128 час=2.00 мс
^C
--- Статистика луна-імпульсів 195.1.1.2 ---
Передано 6 пакетів, отримано 6, втрачено 0% пакетів, час 5011 мс
rtt мін/сер/макс/маєв = 1.654/2.073/2.481/0.303 мс
roman@roman-VirtualBox:~$
```

Рисунок 3.19 – Результати блокувань

3.3. Боротьба зі flood-атаками

Наведу кілька команд, які можуть допомогти при флуді нашого хоста.

Підрахунок кількості з'єднань на певний порт:

```
$ Netstat -na | grep ": nopr" | wc -l
```

```

roman@roman-VirtualBox:~$ netstat -na | grep 80
unix 2      [ ACC ]     STREAM    LISTENING   25380      /run/user/1000/pulse/native
unix 3      [  ]       STREAM    CONNECTED   28003
unix 3      [  ]       STREAM    CONNECTED   26080
unix 3      [  ]       STREAM    CONNECTED   28004      /run/user/1000/bus
unix 3      [  ]       STREAM    CONNECTED   28044
unix 3      [  ]       STREAM    CONNECTED   28045      /run/systemd/journal/stdout
unix 3      [  ]       STREAM    CONNECTED   25805
unix 3      [  ]       STREAM    CONNECTED   25580      /run/dbus/system_bus_socket
unix 3      [  ]       STREAM    CONNECTED   25806      /run/systemd/journal/stdout
unix 3      [  ]       STREAM    CONNECTED   28081
unix 3      [  ]       STREAM    CONNECTED   28082      @/tmp/dbus-zHYcdTdZqZ
unix 3      [  ]       STREAM    CONNECTED   26280      @/tmp/.X11-unix/X0
unix 3      [  ]       STREAM    CONNECTED   28380
unix 3      [  ]       STREAM    CONNECTED   27080      /run/dbus/system_bus_socket
roman@roman-VirtualBox:~$ netstat -na | grep 80 | wc -l
14
roman@roman-VirtualBox:~$

```

Рисунок 3.20 – Перевірка з'єднань порта

Підрахунок числа «напіввідкритих» TCP-з'єднань:

\$ Netstat -na | grep ": nopr" | grep SYN_RCVD | wc -l

```

14
roman@roman-VirtualBox:~$ netstat -na | grep 80 | grep SYN_RCVD | wc -l
0
roman@roman-VirtualBox:~$

```

Рисунок 3.21 – Перевірка напіввідкритих TCP-з'єднань

Перегляд списку IP-адрес, з яких йдуть запити на підключення:

\$ Netstat -na | grep ": nopr" | sort | uniq -c | sort -nr | less

Аналіз підозрілих пакетів за допомогою tcpdump:

Tcpdump -n -i eth0 -s 0 -w output.txt dst port nopr and host IP-сервера

Скидаємо підключення атакуючого:

Iptables -A INPUT -s IP-атакуючого -p tcp --destination-port nopr -j DROP

Обмежуємо максимальну кількість "напіввідкритих" з'єднань з однієї IP до конкретного порту:

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				56
	Арк.	№ докум.	Підпис	Дата		

Iptables -I INPUT -p tcp --syn --dport nopr -m iptlimit --iptlimit-above 10 -j DROP

Відключаємо відповіді на запити ICMP ECHO:

Iptables -A INPUT -p icmp -j DROP --icmp-type 8

		Білошицький Р.М.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				57
	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У пояснювальній записці був виконаний огляд засобів безпеки, якими володіє операційна система Linux для безпечного функціонування як в якості користувальницької системи, так і в якості сервера, а також, було розроблено підсистему локального та мережного захисту робочих станцій Linux.

У роботі було розглянуто:

- Основні поняття комп'ютерної безпеки, елементів захисту, вразливостей, основних видів атак;
- Користувальницькі записи в Linux, додавання і видалення користувачів, зміна реєстраційних записів, структура файлу користувальницьких реєстраційних записів passwd, структура файлу паролів shadow, програми управління призначеними для користувача записами useradd, usermod і userdel, програма установки пароля користувача passwd, приклад безпечного налаштування системи шляхом видалення непотрібних реєстраційних записів;
- Можливості файлової системи ext2, права доступу, програми зміни прав доступу та власника файлу chmod і chown, атрибути файлів, програми роботи з атрибутами chattr і lsattr, пакет lcap, призначені для користувача дискові квоти, пакет для роботи з дисковими квотами quota, приклад безпечного налаштування системи за допомогою прав доступу, розширених атрибутів і дискових квот;

Крім теоретичної частини до кожного підрозділу в другому та третьому розділі наводяться приклади практичного застосування розглянутого матеріалу. Всі приклади, наведені в роботі, були випробувані в реальних умовах і успішно реалізовані на станції Linux Ubuntu та Linux Mint.

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				58
	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Офіційна документація Ubuntu [Електронний ресурс] - Режим доступу до ресурсу: <https://ubuntu.com/tutorials?topic=server>
2. Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting Ubuntu Server, 3rd Edition. – 2020. – №3 – 702с.
3. Daniel J. Barret. Linux Pocket Guide, 3rd Edition - класика видавництва O'Relly про командний рядок Linux. - 2016. - №3 – 274с.
4. Корисні статті по Ubuntu/ Linux [Електронний ресурс] - Режим доступу до ресурсу: <https://linuxrussia.com/guides>
5. Ман-посібник [Електронний ресурс] - Режим доступу до ресурсу: <https://man7.org/linux/man-pages/>
6. Офіційна документація Ubuntu (російською мовою) - [Електронний ресурс] - Режим доступу до ресурсу: <https://help.ubuntu.ru/wiki>
7. Ман-посібник (userdel) - [Електронний ресурс] - Режим доступу до ресурсу: <https://man7.org/linux/man-pages/man8/userdel.8.html>
8. Ман-посібник (chmod) - [Електронний ресурс] - Режим доступу до ресурсу: <https://man7.org/linux/man-pages/man1/chmod.1.html>
9. Ман-посібник (lsattr) - [Електронний ресурс] - Режим доступу до ресурсу: <https://man7.org/linux/man-pages/man1/lsattr.1.html>
10. Ман-посібник (chattr) - [Електронний ресурс] - Режим доступу до ресурсу: <https://man7.org/linux/man-pages/man1/chattr.1.html>
11. Ман-посібник (lcap) - [Електронний ресурс] - Режим доступу до ресурсу: <https://linux.die.net/man/8/lcap>
12. Защита сайта от DDoS-атак средствами iptables и nginx [Електронний ресурс]. Режим доступу: <https://defcon.ru/web-security/2860/>
13. Простая защита от DDos-атаки [Електронний ресурс]. Режим доступу: <https://itdraft.ru/2019/08/07/prostaya-zashhita-ot-ddos-ataki>

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				59
Арк.		№ докум.	Підпис	Дата		

ДОДАТОК

		Білошицький Р.М.			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				60
	Арк.	№ докум.	Підпис	Дата		

Роутер R_3_1_1

```

R_3_1#show run
!
Building configuration...

ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3

Current configuration : 942 bytes
!
!
version 12.4
!
service timestamps debug datetime msec
!
service timestamps log datetime msec
!
no service password-encryption
!
!
hostname R_3_1
!
!
boot-start-marker
!
boot-end-marker
!
!
!
no aaa new-model
!
memory-size iomem 5
!
ip cef
!
!
!
no ip dhcp use vrf connected
!
ip dhcp excluded-address 195.1.1.254
!
ip dhcp excluded-address 195.1.1.250
!
!
!
ip dhcp pool lan-A
!
    network 195.1.1.0 255.255.255.0
!
    default-router 195.1.1.254
!
interface FastEthernet0/0

```

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				61
	Арк.	№ докум.	Підпис	Дата		

```

ip address 195.1.1.254 255.255.255.0
!
duplex auto
!
speed auto
!
!
control-plane
interface FastEthernet0/1
!
no ip address
!
shutdown
!
duplex auto
!
speed auto
!
!
!
interface FastEthernet1/0
!
no ip address
!
shutdown
!
duplex auto
!
speed auto
line con 0
!
line aux 0
ip forward-protocol nd
line vty 0 4
!
login
!
!
ip http server
!
no ip http secure-server
end
!
!

Комутатор SW_3_1_1
version 15.1
SW_3_1_1#show run
service timestamps debug datetime msec
Building configuration...
service timestamps log datetime msec
no service password-encryption
Current configuration : 1238 bytes
service compress-config
!
!
! Last configuration change at 12:54:03 UTC Tue Jun
22 2021
hostname SW_3_1_1
!

```

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				62
	Арк.	№ докум.	Підпис	Дата		

```

boot-start-marker                                !
boot-end-marker                                !
!                                                !
!                                                !
!                                                !
no aaa new-model                                !
!                                                !
ip cef                                           interface Ethernet0/0
!                                                duplex auto
!                                                !
no ipv6 cef                                     interface Ethernet0/1
ipv6 multicast rpf use-bgp                     duplex auto
!                                                !
!                                                interface Ethernet0/2
!                                                duplex auto
!                                                !
!                                                interface Ethernet0/3
!                                                duplex auto
!                                                !
!                                                interface Ethernet1/0
spanning-tree mode pvst                       duplex auto
spanning-tree extend system-id                 !
!                                                !
!                                                interface Ethernet1/1
!                                                duplex auto
!                                                !
vlan internal allocation policy ascending       interface Ethernet1/2
!                                                duplex auto
!                                                !
!                                                interface Ethernet1/3

```

		Білошицький Р.М			КІ.КР.Б – 123 – 21 – ПЗ	Арк.
		Головня О.С.				63
	Арк.	№ докум.	Підпис	Дата		

duplex auto

!

interface Ethernet2/0

duplex auto

!

interface Ethernet2/1

duplex auto

!

interface Ethernet2/2

duplex auto

!

interface Ethernet2/3

duplex auto

!

interface Ethernet3/0

duplex auto

!

interface Ethernet3/1

duplex auto

!

interface Ethernet3/2

duplex auto

!

interface Ethernet3/3

duplex auto

!

interface Vlan1

ip address 195.1.1.250 255.255.255.0

!

!

no ip http server

!

!

!

!

!

control-plane

!

!

line con 0

logging synchronous

line aux 0

line vty 0 4

!

end

Білошицький Р.М

Головня О.С.

Арк.

№ докум.

Підпис

Дата

КІ.КР.Б – 123 – 21 – ПЗ

Арк.

64