Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Розробка, інтеграція та оцінка ефективності захисту від повільних та швидких brute-force атак на IMAP сервер"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Бекер Іван Миколайович
підпис (прізвище та ініціали)

Керівник Загородна Н.В
підпис (прізвище та ініціали)

Нормоконтроль Лечаченко Т. А.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Бекеру Івану Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка, інтеграція та оцінка ефективності захисту від повільних та швидких brute-force атак на IMAP сервер

Керівник роботи Загородна Наталія Володимирівна
к.т.н., доцент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 16 » 11 2023 року № 4/7-1061

2. Термін подання студентом завершеної роботи 24.12.2023

3. Вихідні дані до роботи Вимоги до системи захисту від brute-force атак, вимоги до операційної системи FreeBSD.

4. Зміст роботи (перелік питань, які потрібно розробити)
Проаналізувати повільні та швидкі brute-force атаки.
Налаштування FreeBSD PF для захисту від швидких атак
Розробити програмний модуль для аналізу лог-файлів та захисту від повільних атак та автоматичного повідомлення адміністратору про інцидент безпеки.
Охорона праці та безпека в надзвичайних ситуаціях
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема, мета, задачі. Наукова новизна на практичне значення роботи. Методи здійснення brute-force атаки. Типи brute-force атак на сервер. IMAP сервер та проблем безпеки сервісу. Схема мережі для моделювання brute-force атаки. Налаштування операційної системи FreeBSD. Налаштування IMAP сервера Dovecot. Операційна система BackBox у ролі інструменту атаки. Розробка методів захисту від brute-force атак. Написання правил PF для захисту від швидких атак. Проведення тестування реалізованого захисту. Результати тестування захисту від швидких атак. Розробка захисту від повільних brute-force атак. Механізм виявлення та блокування brute-force атаки. Зміна налаштувань брандмауера PF. Середовище розробки програмного модуля. Автоматизація процесу виявлення та блокування атаки. Тестування розробленого захисту. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 20.09.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.09 – 23.01	Виконано
2.	Підбір джерел для аналізу повільних та швидких brute-force атак та методів захисту від них	25.09 – 10.10	Виконано
3.	Опрацювання джерел в галузі дослідження	11.10 – 15.10	Виконано
4.	Налаштування середовища для емуляції атак методом brute-force	16.10 – 25.10	Виконано
5.	Розроблення методів захисту від brute-force атак	25.10 - 30.10	Виконано
6.	Оформлення розділу «Огляд методів здійснення та технологій захисту від brute-force атак»	30.10 – 05.11	Виконано
7.	Оформлення розділу «Організація лабораторного середовища для емуляції атак методом brute-force»	06.11 – 10.11	Виконано
8.	Оформлення розділу «Розробка методів захисту від brute-force атак»	11.11 – 25.11	Виконано
9.	Виконання завдання до підрозділу «Охорона праці та безпека в надзвичайних ситуаціях»	26.11-01.12	
10.	Оформлення кваліфікаційної роботи	02.12 – 10.12	Виконано
11.	Нормоконтроль	20.12 – 21.12	Виконано
12.	Перевірка на плагіат	22.12 – 24.06	Виконано
13.	Попередній захист кваліфікаційної роботи	25.12.2023	Виконано
14.	Захист кваліфікаційної роботи	27.12.2023	

Студент _____ Бекер І.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Загородна Н.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка, інтеграція та оцінка ефективності захисту від повільних та швидких brute-force атак на IMAP сервер // Кваліфікаційна робота ОР «Магістр» // Бекер Іван Миколайович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-62 // Тернопіль, 2023 // С. 66 , рис. – 20, табл. – - , кресл. – 26 , додат. – 3.

КЛЮЧОВІ СЛОВА: FREEBSD, IMAP, PF, BRUTE-FORCE, BASH, DOVECOT.

Кваліфікаційна робота присвячена дослідженню методів захисту IMAP сервера від brute-force атак. Було проведено аналіз повільних та швидких brute-force атак та методів їх виявлення. Розроблено та застосовано політику паролів для збільшення безпеки облікових записів користувачів. Розроблено та реалізовано методику захисту від швидких brute-force атак за допомогою PF в операційній системі FreeBSD.

Також у результаті дослідження було розроблено програмний модуль для аналізу лог-файлів IMAP сервера Dovecot з метою виявлення та блокування повільних brute-force атак за допомогою PF. Було розроблено та налаштовано систему автоматичного сповіщення адміністратора про інциденти безпеки через корпоративний Jabber.

Отримані результати підтвердили, що розроблений захист працює коректно та успішно блокує спроби атак в реальному часі. Реалізація заходів захисту та автоматичного інформування адміністратора дозволяє оперативно реагувати на потенційні загрози.

ABSTRACT

Development, Integration, and Evaluation of the Effectiveness of Protection Against Slow and Fast Brute-Force Attacks on an IMAP Server// Thesis of educational level "Master"// Beker Ivan Mykolaiovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБм-62 // Ternopil, 2023 // P. 66, fig. - 20, tab. - _-_, chair. - 26 , added. – -3.

Keywords: FREEBSD, IMAP, PF, BRUTE-FORCE, BASH, DOVECOT.

The qualification work is devoted to the study of methods for protecting an IMAP server from brute-force attacks. An analysis of slow and fast brute-force attacks and methods for their detection was carried out. Developed and implemented a password policy to increase the security of user accounts. A method of protecting against fast brute-force attacks using PF in the FreeBSD operating system has been developed and implemented.

Also, as a result of the research, a software module was developed for analyzing Dovecot server IMAP log files in order to detect and block slow attacks using PF. A system for automatically notifying the administrator about security incidents via corporate Jabber was developed and configured.

The results obtained confirmed that the developed protection works correctly and successfully blocks attack attempts in real time. The implementation of protection measures and automatic notification of the administrator allows you to quickly respond to potential threats.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 8
ВСТУП 9
1 ОГЛЯД МЕТОДІВ ЗДІЙСНЕННЯ ТА ТЕХНОЛОГІЙ ЗАХИСТУ ВІД BRUTE-FORCE АТАК 11
1.1 Методи здійснення brute-force атаки 11
1.2 Типи brute-force атак на сервер 13
1.2.1 Швидка brute-force атака на сервер 13
1.2.2 Повільна brute-force атака на сервер 13
1.3 Огляд IMAP сервера та проблем безпеки сервісу 14
1.3.1 Місце IMAP сервера в поштовій інфраструктурі 14
1.3.2. Засоби захисту IMAP сервера від атак на паролі 17
2 ОРГАНІЗАЦІЯ ЛАБОРАТОРНОГО СЕРЕДОВИЩА ДЛЯ ЕМУЛЯЦІЇ АТАК МЕТОДОМ BRUTE-FORCE 20
2.1 Схема мережі для моделювання brute-force атаки 20
2.2 IMAP сервер Dovecot на базі операційної системи FreeBSD 21
2.2.1 Налаштування операційної системи FreeBSD 22
2.2.2 Налаштування IMAP сервера Dovecot 25
2.3 Операційна система BackBox у ролі інструменту атаки 28
3 РОЗРОБКА МЕТОДІВ ЗАХИСТУ ВІД BRUTE-FORCE АТАК 31
3.1 Облікові дані користувачів IMAP сервера 31
3.1.1 Налаштування політики паролів 32
3.1.2 Проведення тестування політики паролів 39
3.2 Розробка захисту від швидких brute-force атак 36
3.2.1 Написання правил PF для захисту від швидких атак 36
3.2.2 Проведення тестування реалізованого захисту 38
3.3 Розробка захисту від повільних brute-force атак 40
3.3.1 Механізм виявлення та блокування brute-force атаки 40
3.3.2 Зміна налаштувань брандмауера PF 41
3.3.3 Обрання середовища для розробки 42
3.3.4 Написання програмного модуля 43

3.3.5 Автоматизація процесу виявлення та блокування атаки 44
3.3.6 Тестування розробленого захисту 47
4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 51
4.1 Забезпечення пожежної безпеки в приміщенні ЕОМ..... 51
4.2 Підвищення стійкості роботи комп’ютеризованих систем в умовах дії ЕМІ ядерних вибухів..... 54
ВИСНОВКИ..... 56
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 57
Додаток А Публікація 59
Додаток Б Лістинг файлу bruteforcealertimap.bash 62
Додаток В Файл налаштування сервісу bruteforce_monitor 65

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IMAP	—	Internet Message Access Protocol
SSL	—	Secure Sockets Layer
TLS	—	Transport Layer Security
TCP	—	Transmission Control Protocol
PF	—	Packet Filter
POP3	—	Post Office Protocol version 3
NTP	—	Network Time Protocol.
ZFS	—	Zettabyte File System
SASL	—	Simple Authentication and Security Layer
LDAP	—	Lightweight Directory Access Protocol
SQL	—	Structured Query Language
PAM	—	Pluggable Authentication Modules
NAT	—	Network Address Translation
ALTQ	—	Alternate Queuing
Bash	—	Bourne Again Shell
XMPP	—	Extensible Messaging and Presence Protocol

ВСТУП

Актуальність теми. У цифровому світі інформаційні технології стають не лише надзвичайно важливими для підтримки різноманітних бізнес-процесів, але й піддаються постійним загрозам кібербезпеки. Зокрема, сервери електронної пошти, що працюють за протоколом IMAP, є об'єктом інтенсивних кібератак.

Захист від повільних та швидких brute-force атак на IMAP сервер є актуальною проблемою в контексті зростаючої кількості кіберзлочинності, спрямованої на сервери, що забезпечують обмін електронними листами. Існує необхідність розробки та інтеграції ефективних заходів захисту, які забезпечать надійність та безпеку обробки електронної пошти.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи є розробка, інтеграція та оцінка ефективності захисту від повільних та швидких brute-force атак на сервери, що працюють за протоколом IMAP. Задачі включають аналіз повільних та швидких brute-force атак, налаштування FreeBSD PF для захисту від швидких атак, написання програмного модуля для аналізу лог-файлів та захисту від повільних атак та автоматичного повідомлення адміністратору про інцидент безпеки.

Об’єкт дослідження. Об’єктом дослідження є сервери IMAP що піддаються атакам brute-force.

Предметом дослідження є розробка та інтеграція заходів захисту, а також перевірка їх ефективність у реальних умовах.

Наукова новизна одержаних результатів кваліфікаційної роботи. Одержані результати дослідження розкривають нові можливості захисту серверів електронної пошти від відомих повільних та швидких brute-force атак, використовуючи комбінацію FreeBSD PF та програмного модуля для аналізу лог-файлів. Розроблений захист працює в реальному часі, блокуючи спроби атак та надсилаючи повідомлення про них.

Практичне значення одержаних результатів. Отримані результати можуть бути використані адміністраторами серверів для підвищення рівня безпеки електронної пошти. Практична реалізація захисту та автоматичного

повідомлення адміністратору про інцидент безпеки сприятиме оперативному реагуванню на потенційні загрози.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: IV Всеукраїнській студентській науковій конференції «Розвиток сучасної науки: актуальні питання теорії та практики» (м.Львів, Україна), (див. Додаток А).

1 ОГЛЯД МЕТОДІВ ЗДІЙСНЕННЯ ТА ТЕХНОЛОГІЙ ЗАХИСТУ ВІД BRUTE-FORCE АТАК

1.1 Методи здійснення brute-force атаки

Brute-force атаки - це вид кібератак, де зловмисники використовують програмне забезпечення або скрипти для спроб послідовно перебрати всі можливі комбінації паролів, PIN-кодів або ключів доступу для незаконного входу в облікові записи [1].

Основні методи здійснення brute-force атак:

1) Словникові атаки (Dictionary Attacks) - це вид атак, коли зловмисники використовують попередньо складені словники або бази даних, що містять велику кількість паролів, для спроби автоматично вводити ці паролі в облікові записи або системи з метою злому. Ці атаки ґрунтуються на теорії, що багато людей використовують слабкі або загальнодоступні паролі, що можна знайти у таких словниках.

Зловмисники складають словник, включаючи загальні, популярні або потенційно слабкі паролі. Цей словник може включати слова зі словників, списки часто вживаних паролів, інформацію із різних баз даних та інші джерела. На наступному етапі зловмисники використовують програмне забезпечення або скрипти для автоматизованого введення паролів зі словника послідовно в облікові записи або системи. Це відбувається автоматично, паролі вводяться швидко та послідовно, сподіваючись знайти вірний пароль.

Якщо користувач використовує слабкий або загальнодоступний пароль, ймовірність того, що його пароль знайдуть у словнику досить висока.

Атаки можуть бути виконані відносно швидко, оскільки програми або скрипти можуть спробувати тисячі паролів за дуже короткий період часу.

Якщо пароль не міститься у словнику, атака буде неефективною.

2) Ітеративний перебір (simple brute-force attack) - це метод, що передбачає послідовну спробу всіх можливих комбінацій символів (цифри, літери, символи)

для створення паролів чи ключів доступу. Чим довший пароль або ключ, тим більше часу потрібно для повного перебору.

Ітеративний перебір, відомий також як проста brute-force атака, представляє собою метод вгадування паролю, де зловмисники пробують всі можливі комбінації символів (цифри, літери, символи тощо) для злому пароля чи ключа доступу. Цей вид атаки базується на повному переборі всіх можливих варіацій знаків для входу в систему або обліковий запис. Його особливістю є те, що він не базується на попередніх знаннях або базах даних паролів, а намагається послідовно перевірити всі можливі комбінації символів.

Зловмисники використовують програмне забезпечення або скрипти, що автоматизують генерацію всіх можливих комбінацій символів для створення паролів. Згенеровані комбінації вводяться послідовно в облікові записи або системи. Атаки можуть перевіряти усі можливі варіації символів, починаючи з одного символу і збільшуючи довжину комбінації доти, поки не буде досягнуто бажаного результату.

Час, потрібний для успішного виконання такої атаки, може бути значним, особливо при довгих або складних паролях.

Якщо пароль чи ключ доступу складається з відомих чи простих комбінацій, то ітеративна атака може бути ефективною.

3) Комбіновані атаки (Hybrid Attacks) - представляють собою комбінацію словникових та ітеративних методів, які спрямовані на злам облікових даних чи ключів доступу. Ці атаки створені для покращення ефективності та швидкості злому шляхом комбінування словникових методів (використання популярних паролів та словникових атак) з ітеративним перебором символів.

Зловмисники можуть розпочинати зі словникових методів, використовуючи відомі паролі, часто вживані слова, або дані, що були викрадені раніше.

Після спроб зі словниковими методами, атаки можуть переходити до ітеративних методів, що охоплюють більше комбінацій символів для пошуку більш складних або унікальних паролів.

Комбінація цих методів дозволяє швидше знаходити паролі, особливо у випадках, коли словникові методи виявляються неефективними.

Інтеграція словникових та ітеративних методів у комбінованих атаках дозволяє зловмисникам зламувати паролі більш ефективно, використовуючи переваги кожного з методів.

1.2 Типи brute-force атак на сервер

1.2.1 Швидка brute-force атака на сервер

Швидка brute-force атака на сервер - це тип атаки, де зловмисники використовують програмне забезпечення або скрипти для надзвичайно швидкого послідовного перебору різних комбінацій паролів або ключів доступу з метою незаконного входу в систему або облікові записи на сервері. Ці атаки влаштовуються з великою швидкістю та намагаються перевірити велику кількість можливих комбінацій паролів у короткий період часу.

Зловмисники використовують спеціалізовані програми або скрипти для автоматизованого введення паролів без інтервалів між спробами.

Ці атаки можуть перевіряти тисячі, а навіть мільйони комбінацій паролів за дуже короткий проміжок часу, використовуючи високопродуктивне програмне забезпечення та швидке підключення до сервера.

Швидкість таких атак може ускладнити виявлення атаки та призвести до успішного злому пароля, особливо якщо використовуються слабкі або прості комбінації паролів.

Запобігання швидким brute-force атакам вимагає використання комплексних заходів безпеки та обмежень, що роблять такі атаки менш успішними, складними та тривалішими.

1.2.2 Повільна brute-force атака на сервер

Повільна brute-force атака на сервер - це форма кібератаки, де зловмисники виконують спроби незаконного входу в систему з використанням облікових записів користувачів шляхом послідовного перебору різних комбінацій паролів або ключів доступу, проте це відбувається уповільнено для уникнення блокування облікових записів через спеціальні заходи безпеки.

Атаки відбуваються з низькою частотою спроб входу, для уникнення блокування облікового запису чи виявлення системами захисту.

Зловмисники поступово тестують різні комбінації паролів, розподіляючи спроби вводу паролів з великими інтервалами часу, щоб уникнути виявлення як атаки. Ця стратегія атаки дозволяє зменшити ризик блокування облікового запису чи виявлення спроби злому.

Повільні brute-force атаки спрямовані на те, щоб уникнути виявлення та блокування облікового запису, тому для їх запобігання важливо використовувати алгоритми моніторингу та аналізу активності, які допомагають виявляти навіть незначні аномалії, а також застосовувати додаткові методи безпеки, які ускладнюють атаки на сервер.

1.3 Огляд IMAP сервера та проблем безпеки сервісу

1.3.1 Місце IMAP сервера в поштовій інфраструктурі

IMAP сервер є ключовим компонентом поштової інфраструктури, який забезпечує доступ до електронної пошти користувачам через різні пристрої та програми для роботи з поштою, яка зберігається на віддаленому поштовому сервері [2].

IMAP дозволяє користувачам відкривати, переглядати та керувати своєю поштою через різні пристрої та поштові програми.

Основні функції IMAP сервера включають:

1) Доступ та синхронізація пошти. Користувачі можуть переглядати свою пошту у реальному часі без необхідності завантажувати всі повідомлення на свій пристрій. Поштові клієнти підтримують відображенні повідомлень та зберігають їх на сервері. IMAP сервер дозволяє користувачам отримувати доступ до своєї пошти через різні пристрої. Він зберігає поштові скриньки на сервері, що дозволяє користувачам переглядати та керувати своєю поштою з будь-якого місця. IMAP дозволяє синхронізувати поштові скриньки між сервером та пристроями користувача. Це означає, що зміни, внесені на одному пристрої

(наприклад, видалення або переміщення повідомлень), відображаються на всіх інших пристроях.

2) Організація пошти на сервері. IMAP дозволяє створювати папки, переміщати повідомлення між папками та виконувати інші дії з організацією пошти на сервері. Це дозволяє користувачам ефективно керувати своєю поштою.

3) Управління повідомленнями. Користувачі можуть видаляти, відправляти, переміщати та маркувати повідомлення, а також працювати з вкладеннями.

4) Безпека та захист даних. Шифрування з'єднання дозволяє передавати дані користувачів безпечно.

Основні порти та протоколи, які використовуються IMAP, включають [3]:

1) TCP порт 143. Використовується для встановлення з'єднання між поштовим клієнтом (наприклад, поштовою програмою на комп'ютері) та IMAP сервером. Коли клієнтський пристрій намагається підключитися до IMAP сервера, він використовує TCP порт 143 для ініціювання цього зв'язку.

IMAP працює на принципі взаємодії клієнта та сервера для отримання доступу до поштових повідомлень. Після встановлення з'єднання через TCP порт 143, клієнт може відправляти команди до сервера для отримання списку повідомлень, їхнього вмісту, керування папками та інші дії.

Інформація, яка передається через TCP порт 143, не шифрується за замовчуванням. Це означає, що дані, які передаються між поштовим клієнтом та сервером, можуть бути вразливими до перехоплення чи перегляду третіми особами. Тому для покращення безпеки передачі даних рекомендується використовувати шифровані протоколи такі як IMAPS, які забезпечують захищене з'єднання та шифрують дані, що передаються між клієнтом та сервером.

2) TCP порт 993. Це є стандартний порт, який використовується для забезпечення захищеного з'єднання з IMAP сервером за допомогою шифрування SSL/TLS. Цей порт використовується для IMAPS (IMAP over SSL) або IMAP з шифруванням, що забезпечує захищене з'єднання між поштовим клієнтом та сервером.

У зв'язку з тим, що TCP порт 993 використовує шифрування SSL/TLS, всі дані, що передаються між поштовим клієнтом і сервером IMAP будуть зашифровані. Це важливо для забезпечення конфіденційності інформації, яка пересилається і запобіганню можливим перехопленням чи прослуховуванню даних.

Зв'язок через TCP порт 993 стає можливим завдяки встановленню шифрованого з'єднання між клієнтом та сервером за допомогою протоколів шифрування, таких як SSL або його більш сучасний варіант, TLS. Під час обміну даними між поштовим клієнтом та сервером через TCP порт 993 інформація шифрується та забезпечується високий рівень захисту та конфіденційності.

Загальний рівень захисту даних у комунікації за допомогою IMAPS на TCP порті 993 забезпечує безпеку та конфіденційність обміну електронною поштою між клієнтами та серверами, що є важливим аспектом для захисту особистої інформації та попередження можливих загроз безпеці.

3) STARTTLS. Це протокол, який дозволяє створити шифроване з'єднання в рамках звичайного з'єднання IMAP через TCP порт 143. Замість використання окремого порту для шифрованого з'єднання (як в IMAPS на TCP порті 993), STARTTLS дозволяє розпочати захищене з'єднання на звичайному порті, тобто на стандартному порті для IMAP без шифрування.

Якщо цей вид з’єднання підтримується сервером і клієнтом, команда STARTTLS ініціює зміну режиму зв'язку з незашифрованого на зашифрований. Під час використання STARTTLS, спочатку встановлюється незашифроване з'єднання між клієнтом та сервером. Після цього, сервер надсилає відповідь з інструкціями для запуску захищеного з'єднання.

Після отримання команди STARTTLS, зв'язок переходить до захищеного режиму, що передбачає шифрування даних, які передаються між клієнтом та сервером. Це шифрування забезпечує конфіденційність даних, ускладнюючи можливість перехоплення чи прослуховування інформації під час її передачі.

Використання STARTTLS є важливим для безпеки передачі даних, оскільки це дозволяє здійснити шифровану комунікацію в рамках стандартного порту IMAP, забезпечуючи безпеку під час обміну електронними листами.

1.3.2. Засоби захисту IMAP сервера від атак на паролі

IMAP сервери можуть бути вразливі до різних видів атак. Ось деякі типові проблеми безпеки, що можуть виникнути на IMAP серверах:

1) Неякісне управління паролями.

Управління паролями є важливим аспектом в безпеці інформації. Використання слабких або загальних паролів у облікових записах на IMAP сервері може значно підвищити ризик злому паролів методом brute-force.

Слабкий пароль - це пароль, який легко вгадати, оскільки він короткий, використовує загальнодоступні слова, прості послідовності цифр або легко визначені особисті дані. Людина або програма для злому може використовувати ці знання, щоб виконати атаку на пароль.

Загальний пароль - це пароль, який використовується для кількох облікових записів або який легко вгадати, оскільки він широко використовується.

Слабкі або загальні паролі створюють вразливості у безпеці, оскільки зловмисники можуть використовувати програми для перебору паролів для спроб вгадування правильного пароля методом спроб та помилок. Чим простіший пароль, тим менше часу займе його відгадування.

Для покращення безпеки облікових записів на IMAP сервері рекомендується встановити:

- Складність паролів. Здійснити налаштування, які будуть вимагати від користувачів створювати лише складні паролі, які містять комбінацію великих та малих літер, цифр та символів.

- Унікальність паролів. Застосовувати політику не використання одного і того самого паролю повторно.

- Зміна паролів. Рекомендувати регулярно змінювати паролі, особливо після виявлення атак або після визначення можливого витоку інформації.

- Використання парольних фраз. Парольні фрази (наприклад, фрази з кількох слів) можуть бути більш безпечними, ніж короткі паролі.

Маючи сильні та унікальні паролі, можна значно скоротити ризики brute-force атак та підвищити безпеку облікових записів на IMAP сервері.

2) Відсутність шифрування.

Відсутнє або недостатнє шифрування з'єднання з IMAP сервером створює серйозну загрозу для конфіденційності та цілісності інформації. Коли дані (такі як листи, дані про користувачів та інша конфіденційна інформація) передаються через мережу без шифрування, існує ризик їхнього перехоплення третіми особами.

Запобігання можливості прочитати перехоплені дані шляхом використання шифрування є важливим аспектом для забезпечення безпеки облікових записів та конфіденційності інформації в IMAP сервері

3) Вразливості в програмному забезпеченні.

Вразливості в програмному забезпеченні IMAP серверів можуть бути використані зловмисниками для отримання доступу до системи, виконання небажаних команд або викрадення конфіденційної інформації.

Недоліки в реалізації протоколів аутентифікації можуть дозволити зловмисникам отримати несанкціонований доступ до системи шляхом перехоплення авторизаційних даних.

Незастосування оновлень або використання застарілих версій серверного програмного забезпечення може стати причиною вразливостей.

Залежно від типу вразливості, зловмисники можуть використовувати різноманітні методи для злому системи, отримання доступу до конфіденційної інформації або завдання шкоди.

Для запобігання цим атакам рекомендується регулярно оновлювати програмне забезпечення IMAP серверів та проводити аудит безпеки для виявлення вразливостей та слабких місць в програмному забезпеченні.

Налаштування шифрування, усунення вразливостей в програмному забезпеченні та встановлення політики паролів значно покращить безпеку сервера, але від спроб здійснення brute-force атак ці засоби не захистять. Важливо налаштувати додаткові заходи для захисту IMAP сервера від brute-force атак, які можуть бути реалізовані з використання програмних рішень.

Ці рішення можуть передбачати наступне:

1) Обмеження спроб входу. Встановлення обмежень на кількість невдалих спроб входу в систему для окремих облікових записів. Після досягнення певної кількості невдалих спроб, обліковий запис може бути тимчасово заблокований.

2) Використання двофакторної аутентифікації. Застосування додаткового кроку підтвердження, окрім введення пароля, наприклад, отримання SMS-коду або використання аутентифікаційних додатків.

3) Моніторинг активності. Використання програмного забезпечення для моніторингу активності на сервері для виявлення підозрілої поведінки, наприклад, надмірної кількості спроб входу з певних IP-адрес.

4) Блокування IP. При надмірній кількості невдалих спроб входу можна автоматично блокувати конкретні IP адреси, з яких відбуваються атаки.

Комбінація цих заходів допоможе забезпечити ефективний захист IMAP сервера від brute-force атак, роблячи його менш доступним для успішних незаконних входів.

2 ОРГАНІЗАЦІЯ ЛАБОРАТОРНОГО СЕРЕДОВИЩА ДЛЯ ЕМУЛЯЦІЇ АТАК МЕТОДОМ BRUTE-FORCE.

2.1 Схема мережі для моделювання brute-force атаки

Для моделювання атаки методом перебору паролів буде використана схема мережі наведена на рисунку 2.1.

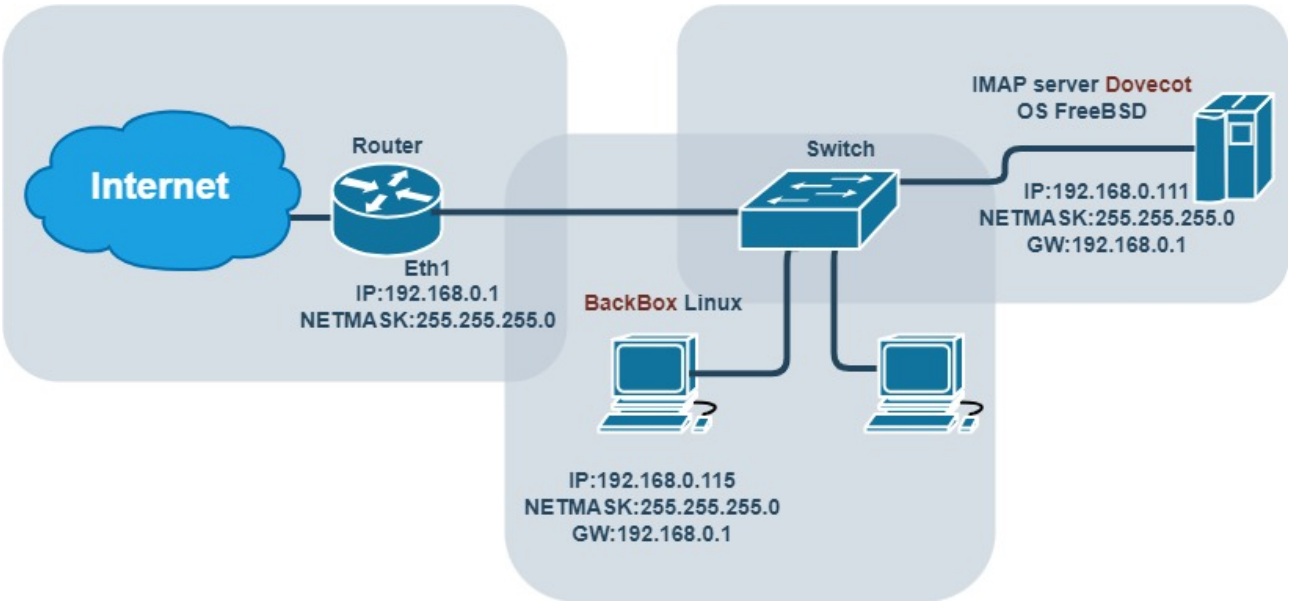


Рисунок 2.1 – Схема мережі для здійснення brute-force атаки

Схема мережі, призначена для демонстрації атаки методом перебору паролів на IMAP сервері, включає такі компоненти:

1) Стандартний мережевий комутатор, до якого підключені мережеві пристрої.

2) Комп'ютер з BackBox Linux, який буде використано для здійснення brute-force атаки.

3) Комп’ютер з операційною системою FreeBSD та встановленим та налаштованим IMAP сервером Dovecot.

У цій схемі комп'ютер з BackBox Linux та IMAP сервер підключені до комутатора, а вже комутатор підключений до маршрутизатора. Для спрощення

лабораторного середовища обидва комп'ютера знаходяться в одній мережі та використовують один і той самий шлюз для доступу до мережі Інтернет.

Ця схема мережі сприятиме набуттю навичок у виявленні, захисті та реагуванні на атаки, які базуються на методі перебору паролів, у умовах контрольованого середовища.

2.2 IMAP сервер Dovecot на базі операційної системи FreeBSD

FreeBSD є операційною системою з відкритим кодом на базі Unix, яка відома своєю стабільністю, надійністю та високою продуктивністю [4]. Основні особливості FreeBSD включають:

1) Стабільність та надійність. FreeBSD розроблений з урахуванням стабільності та надійності. Він використовує надійні механізми управління пам'яттю, взаємодії з ядром та мережевим стеком.

2) Відкритий код та спільнота. FreeBSD є проектом з відкритим кодом, що означає, що він є безкоштовним та має широку спільноту розробників та користувачів, яка активно сприяє розвитку та підтримці системи.

3) Висока продуктивність. FreeBSD відомий своєю високою продуктивністю, особливо в мережевих задачах. Це робить його відмінним вибором для серверних застосувань та великих мереж.

4) Система управління застосунками. FreeBSD має свою систему керування застосунками, відому як "pkg", що дозволяє легко встановлювати, оновлювати та видаляти програмне забезпечення.

5) Висока безпека. Операційна система розроблена з врахуванням сучасних вимог до безпеки. Команда розробників регулярно випускає оновлення для виправлення потенційних вразливостей.

5) Широкі можливості конфігурації. FreeBSD надає широкі можливості налаштування та контролю, що дозволяє користувачам налаштувати систему за власними вимогами.

Dovecot є надійним та популярним поштовим сервером, який надає підтримку для протоколів IMAP та POP3. Цей поштовий сервер часто

використовується для організації та керування електронною поштою в серверному середовищі [5].

Основні особливості Dovecot включають:

1) Підтримка IMAP та POP3. Dovecot підтримує протоколи IMAP та POP3 та дає можливість користувачам мати доступ до пошти за допомогою різних поштових клієнтів.

2) Безпека та шифрування. Dovecot надає можливості для шифрування з'єднань через SSL/TLS, що забезпечує захист під час обміну даними між поштовим клієнтом та сервером. Також він підтримує STARTTLS.

3) Підтримка стандартів. Цей сервер дотримується багатьох стандартів та специфікацій протоколів IMAP та POP3, що робить його сумісним з різними поштовими клієнтами.

4) Висока продуктивність. Dovecot оптимізований для високої швидкості обробки запитів користувачів, що робить його популярним в серверних середовищах.

5) Розширені можливості конфігурування. Є багато параметрів конфігурації, які дозволяють налаштувати Dovecot під конкретні потреби користувача або організації.

6) Система фільтрації та управління поштою. Dovecot підтримує систему фільтрації пошти, що дозволяє налаштовувати правила обробки вхідних та вихідних повідомлень.

Поєднання Dovecot з операційною системою FreeBSD дозволяє отримати стабільне та високопродуктивне середовище для поштових послуг, забезпечуючи широкі можливості налаштування, безпеки та ефективного управління.

2.2.1 Налаштування операційної системи FreeBSD

Основні налаштування операційної системи FreeBSD може бути виконано через кілька методів та інструментів, які дозволяють змінювати параметри, налаштовувати сервіси та керувати різними аспектами системи [4].

Велика частина налаштувань здійснюється через конфігураційний файл rc.conf. Цей файли знаходяться у каталозі /etc/ та містять параметри конфігурації для різних складових системи. rc.conf є текстовим файлом конфігурації, що містить параметри налаштувань для різних сервісів та компонентів, які автоматично запускаються під час завантаження системи.

Кожен рядок у файлі rc.conf містить змінну зі значенням, де змінна представляє певний аспект конфігурації системи, а значення встановлює параметр цієї конфігурації. Ці параметри визначають, як система поводиться при запуску, встановлюючи налаштування для мережі, сервісів, журналювання та іншого.

На рисунку 2.2 показано вміст конфігураційного файлу rc.conf операційної системи FreeBSD, яка буде використовуватись в емуляції brute-force атаки.

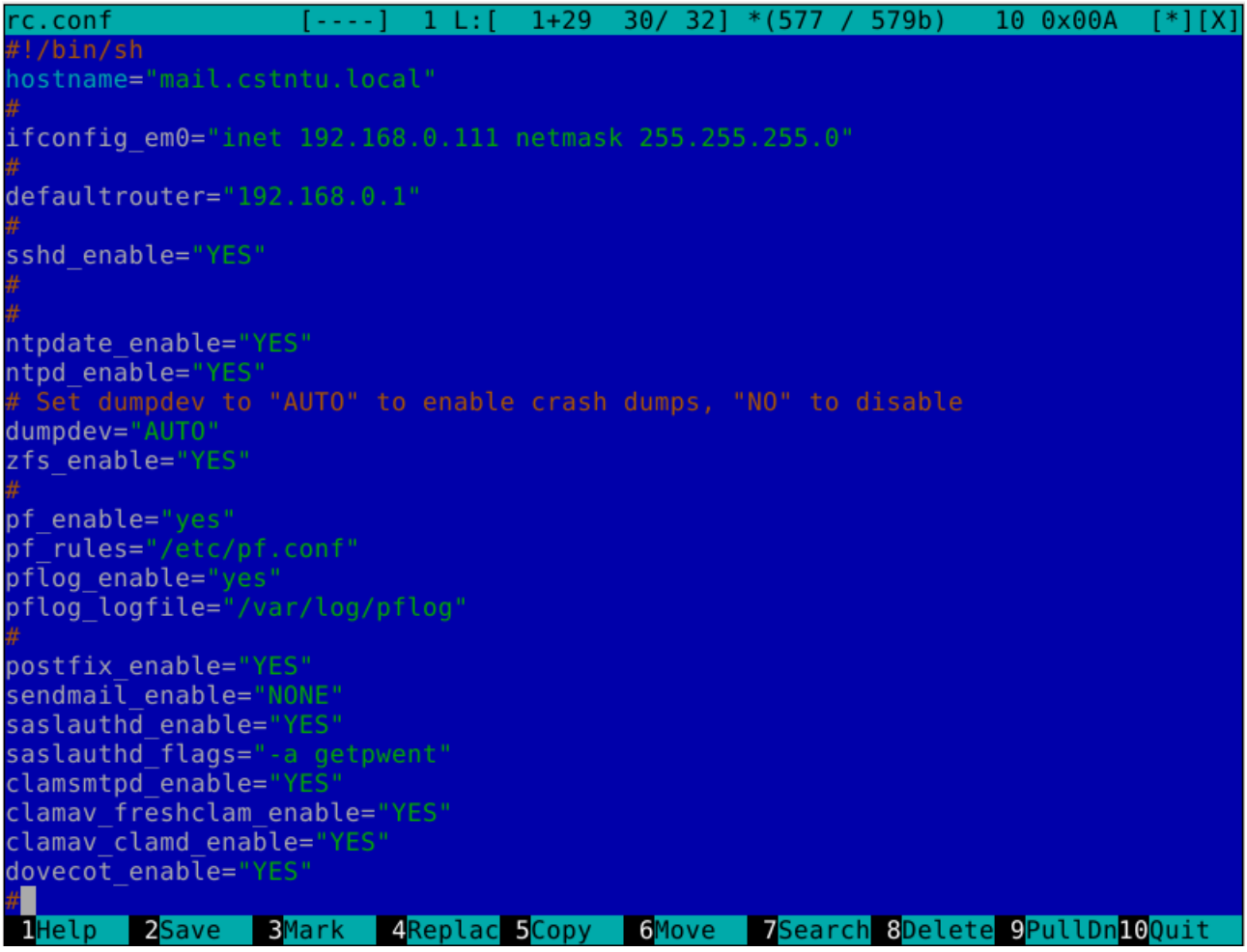


Рисунок 2.2 – Вміст конфігураційного файлу rc.conf операційної системи FreeBSD

Налаштування, які присутні в конфігураційному файлі rc.conf мають наступне значення:

1) `hostname="mail.cstntu.local"`. Вказує ім'я хоста (hostname), що використовується для ідентифікації системи у мережі;

2) `ifconfig_em0="inet 192.168.0.111 netmask 255.255.255.0"`. Налаштування мережевого інтерфейсу em0 з IP адресом 192.168.0.111 та маскою підмережі 255.255.255.0;

3) `defaultrouter="192.168.0.1"`. Вказує IP адресу шлюзу за умовчанням для вихідного трафіку;

4) `sshd_enable="YES"`. Встановлює автоматичний запуск SSH-сервера під час завантаження системи;

5) `ntpdate_enable="YES"` та `ntpd_enable="YES"`. Встановлює автоматичний запуск служби синхронізації часу (NTP) під час завантаження системи;

6) `dumpdev="AUTO"`. Налаштування для управління дампами системи під час аварій;

7) `zfs_enable="YES"`. Активація підтримки файлової системи ZFS;

8) `pf_enable="YES"`. Цей параметр вмикає брандмауер PF в операційній системі FreeBSD під час завантаження системи;

9) `pf_rules="/etc/pf.conf"`. Цей параметр вказує шлях до файлу конфігурації PF. Файл /etc/pf.conf - це місце, де зазвичай розміщуються правила брандмауера PF, в яких визначаються обмеження для мережевого трафіку;

10) `pflog_enable="YES"`. Цей параметр вмикає функцію журналювання для PF. Журнал PF (pflog) використовується для запису пакетів, які зберігаються після обробки фільтром, що дозволяє аналізувати, яким чином фільтр обробляє трафік;

11) `pflog_logfile="/var/log/pflog"`. Цей параметр вказує шлях до файлу журналу PF. В даному випадку, /var/log/pflog є шляхом до файлу, в якому зберігаються дані журналу PF;

11) `postfix_enable="YES"`. Цей параметр вмикає поштовий сервер Postfix під час завантаження операційної системи. Postfix - це поштовий агент, який призначений для передачі та прийому електронних листів;

12) `sendmail_enable="NONE"`. Цей параметр відключає стандартний поштовий агент Sendmail;

13) `saslauthd_enable="YES"`. Цей параметр вмикає агент аутентифікації SASL. SASL - це протокол для аутентифікації користувачів у різних поштових агентах та інших програмах;

14) `saslauthd_flags="-a getpwent"`. Цей параметр встановлює параметри аутентифікації для SASL. Параметр `-a getpwent` вказує SASL використовувати метод аутентифікації "getpwent", що означає отримання інформації про користувача з системних файлів;

15) `clamsmtpd_enable="YES"`. Цей параметр вмикає сервіс ClamSMTPD під час завантаження операційної системи. ClamSMTPD - це антивірусний сканер, який може використовуватися для перехоплення та сканування електронної пошти на наявність вірусів;

16) `clamav_freshclam_enable="YES"`. Цей параметр вмикає фоновий процес оновлення баз даних вірусних сигнатур для ClamAV. Freshclam - це утиліта, яка оновлює бази даних ClamAV для виявлення нових вірусів та сигнатур;

17) `clamav_clamd_enable="YES"`. Цей параметр вмикає фоновий процес ClamAV Daemon (clamd), який відповідає за фактичне сканування файлів та виявлення вірусів;

18) `dovecot_enable="YES"`. Автоматичний запуск поштового сервера Dovecot під час завантаження системи.

2.2.2 Налаштування IMAP сервера Dovecot

Конфігураційні файли Dovecot, такі як dovecot.conf, 10-master.conf та 10-ssl.conf містять налаштування IMAP сервера [6].

dovecot.conf - це основний конфігураційний файл Dovecot. Він містить глобальні налаштування. На рисунку 2.3 показано вміст конфігураційного файлу dovecot.conf.

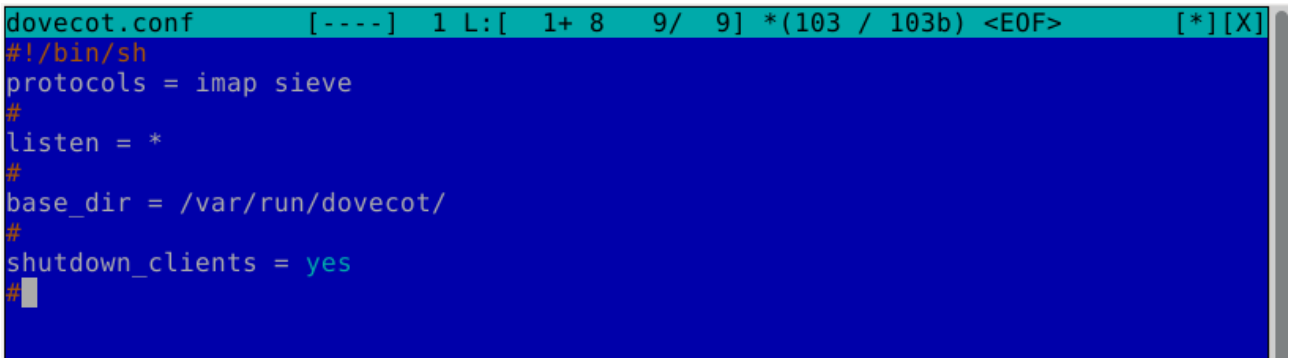


Рисунок 2.3 – Вміст конфігураційного файлу dovecot.conf

Налаштування, які присутні в конфігураційному файлі dovecot.conf мають наступне значення:

1) `protocols = imap sieve`. Цей параметр визначає, які протоколи підтримуються сервером Dovecot. У цьому випадку вказані протоколи IMAP і Sieve. Sieve – це протокол та мова скриптів для фільтрації та обробки пошти;

2) `listen = *`. Цей параметр вказує Dovecot слухати всі доступні мережеві інтерфейси (всі IP-адреси), щоб приймати з'єднання від клієнтів;

3) `base_dir = /var/run/dovecot/`. base_dir визначає каталог для тимчасових файлів та сесій Dovecot;

4) `shutdown_clients = yes`. Цей параметр вказує, що Dovecot має завершувати з'єднання клієнтів під час завершення роботи сервера (наприклад, під час перезавантаження або вимкнення). Клієнти будуть коректно завершувати роботу, коли сервер відключається.

Ці параметри визначають основні аспекти конфігурації сервера Dovecot.

10-master.conf- цей файл зазвичай містить налаштування для служб Dovecot та механізмів аутентифікації, визначаючи, які порти та механізми автентифікації використовуються для різних компонентів Dovecot.

На рисунку 2.4 показано вміст конфігураційного файлу 10-master.conf.

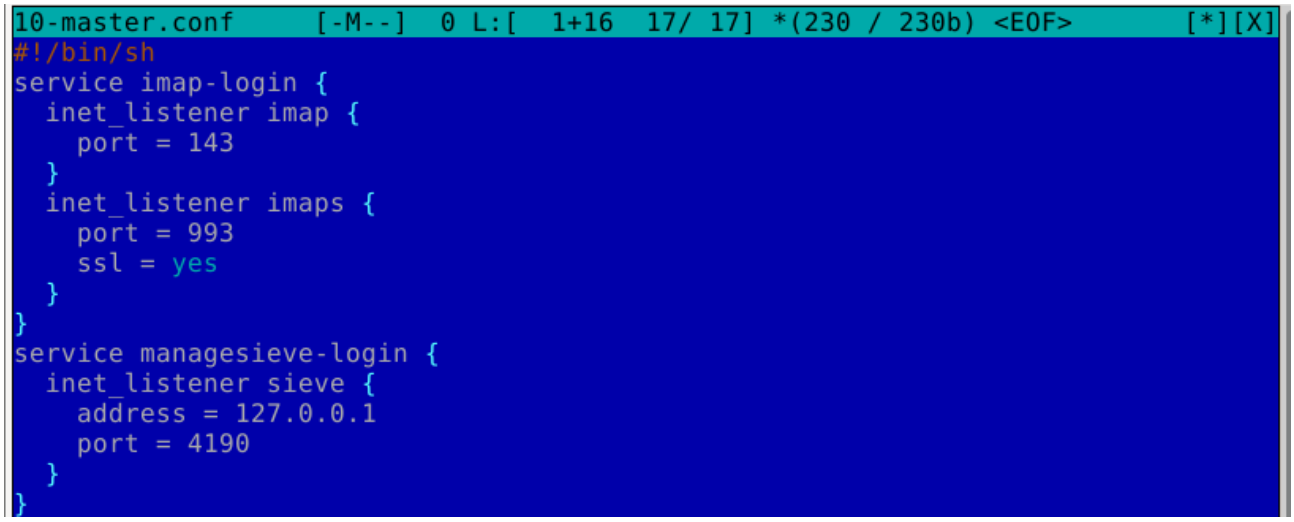


Рисунок 2.4 – Вміст конфігураційного файлу 10-master.conf

Основні налаштування, які присутні в конфігураційному файлі 10-master.conf мають наступне значення:

1) `service imap-login`. Вказує на те, що ми налаштовуємо параметри для служби imap-login. Це служба, яка відповідає за здійснення вхідних підключень для протоколу IMAP;

2) `inet_listener imap`. Налаштовує dovecot для роботи по протоколу IMAP. У цьому випадку вказано, що IMAP слухатиме на порті 143. Це стандартний незахищений порт для IMAP;

3) `inet_listener imaps`. Налаштовує dovecot для роботи по захищеному протоколу IMAP (IMAPS) за допомогою SSL/TLS. Встановлює, що IMAPS слухатиме на порті 993 та використовуватиме шифрування (SSL = yes) для захисту комунікації між клієнтом та сервером;

4) `inet_listener sieve`. Налаштовує dovecot для роботи з протоколом Sieve;

5) `address = 127.0.0.1`. Визначає IP-адресу, яка використовується для підключення. У цьому випадку є можливість лише локального з'єднання, оскільки вказано IP-адресу 127.0.0.1, що відповідає локальному інтерфейсу;

6) `port = 4190`. Визначає порт, на якому приймаються підключення для протоколу Sieve. В цьому випадку, сервіс Sieve слухає на порту 4190.

Ці налаштування визначають різні служби та їх параметри для взаємодії з різними протоколами та послугами в Dovecot сервері.

10-ssl.conf –у цьому файлі зазвичай вказані налаштування для захищеної передачі даних через SSL/TLS, включаючи налаштування сертифікатів, ключів та параметрів шифрування.

На рисунку 2.5 показано вміст конфігураційного файлу 10-ssl.conf.

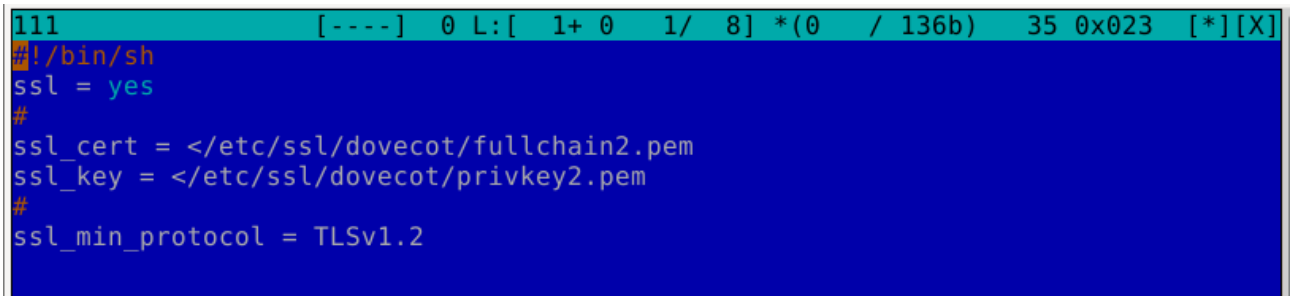


Рисунок 2.5 – Вміст конфігураційного файлу 10-ssl.conf

Основні налаштування, які присутні в конфігураційному файлі 10-ssl.conf мають наступне значення:

1) `ssl = yes`. Цей параметр позначає активацію SSL/TLS шифрування для забезпечення захищеності підключень до сервера Dovecot;

2) `ssl_cert = </etc/ssl/dovecot/fullchain2.pem`. Вказує шлях до файлу сертифіката для шифрування;

3) `ssl_key = </etc/ssl/dovecot/privkey2.pem`. Вказує шлях до файлу з приватним ключем, який використовується разом з сертифікатом для забезпечення шифрування;

4) `ssl_min_protocol = TLSv1.2`. Визначає мінімальну версію протоколу SSL/TLS, яку підтримує сервер. У цьому випадку, вказано, що мінімальною допустимою версією є TLSv1.2, що є більш сучасною та безпечною версією протоколу шифрування.

Кожен файл містить специфічні параметри налаштувань, які впливають на певні моменти роботи IMAP сервера Dovecot.

2.3 Операційна система BackBox у ролі інструменту атаки

BackBox - це операційна система на основі Ubuntu Linux, яка спеціально створена для проведення тестів на проникнення та аудиту безпеки. Вона має вбудований набір інструментів для виявлення вразливостей, сканування мережі та виконання кібератак. BackBox є популярним вибором серед спеціалістів з кібербезпеки та етичних хакерів завдяки своїй зручності, легкості використання та ефективності [7].

Операційна система BackBox містить набір програмних засобів, спрямованих на виявлення та експлуатацію вразливостей в мережах та програмах. З її допомогою можна проводити сканування портів, тестування на проникнення, аналіз безпеки мереж та застосунків, злам паролів, перехоплення пакетів тощо.

Крім того, BackBox забезпечує можливість проведення кібератак у контрольованому середовищі для виявлення слабких місць і застосування відповідних заходів безпеки для їх усунення. Ця операційна система дозволяє спеціалістам з кібербезпеки та етичним хакерам відтворювати різні види атак для підвищення рівня захищеності мереж та систем.

На рисунку 2.6 можна побачити параметри налаштування мережі в операційної системи BackBox Linux.

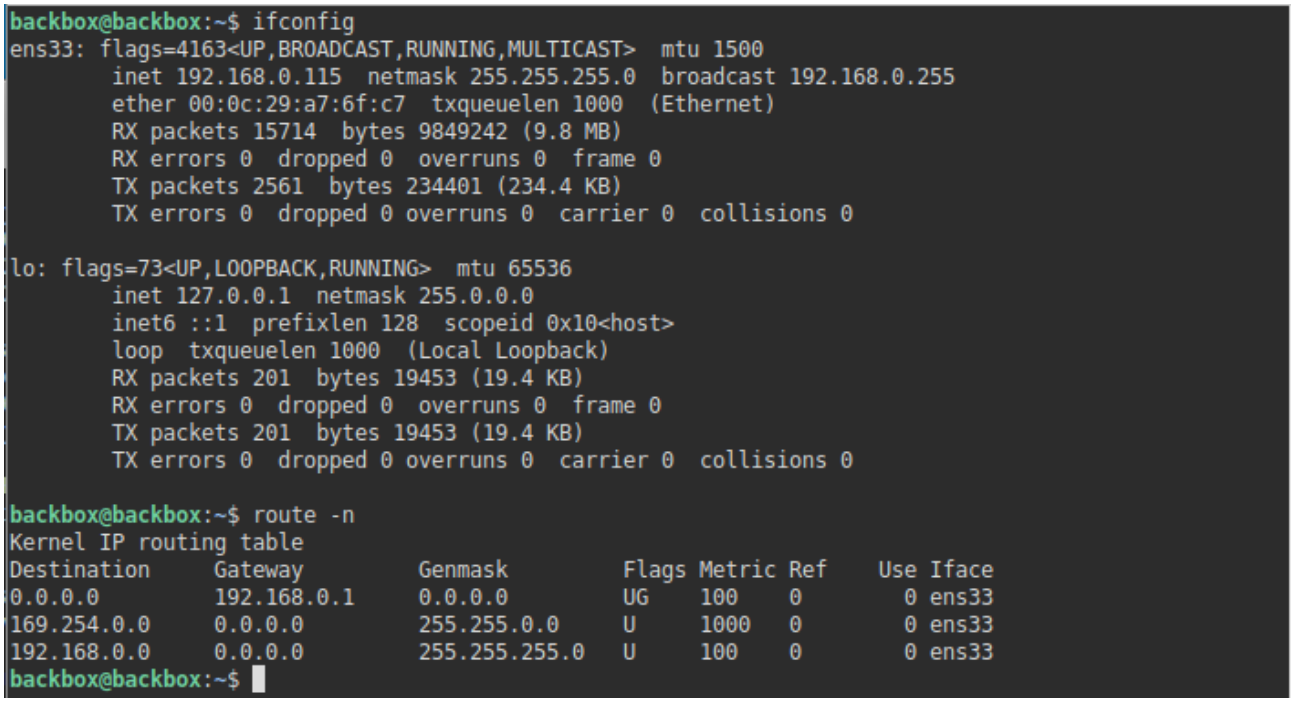


Рисунок 2.6 – Мережеві налаштування операційної системи BackBox Linux

Для здійснення атаки методом перебору паролів буде використано програму Hydra в операційній системі BackBox:

Hydra - це популярний інструмент для тестування на проникнення, що використовується для brute-force атак на різноманітні протоколи. Це дозволяє здійснювати паралельні атаки методом перебору паролів. Програмне забезпечення може використовувати словникові або ітеративні методи для перевірки можливих паролів і імен користувачів [8].

Hydra підтримує численні протоколи, такі як SSH, FTP, HTTP, IMAP, POP3, RDP та багато інших. Інструмент дозволяє швидко перевіряти облікові дані за допомогою списків імен користувачів та паролів для спроби авторизації на конкретних службах. Також надає можливість налаштовувати різні параметри для атаки, включаючи словник паролів, список імен користувачів, метод аутентифікації, та багато інших. Використовуючи цей інструмент у BackBox, експерти з кібербезпеки можуть ефективно та швидко проводити тестування на проникнення та виявлення вразливостей, що допомагає підвищити рівень безпеки систем і мереж.

3 РОЗРОБКА МЕТОДІВ ЗАХИСТУ ВІД BRUTE-FORCE АТАК

3.1 Облікові дані користувачів IMAP сервера

Збереження інформації про користувачів та їх облікових даних є критично важливим для безпеки будь-якої інформаційної системи. Вибір оптимального та надійного методу розміщення облікових даних має вирішальне значення для забезпечення безпеки та ефективного управління доступом до системи.

Сервер IMAP Dovecot має декілька можливих варіантів розміщення користувачів та паролів [6]:

1) Локальні файли. У цьому варіанті, інформація про користувачів (ім'я користувача, пароль тощо) зберігається локально на сервері в текстових файлах. Зазвичай це файли типу /etc/passwd та /etc/master.passwd. Це може бути швидкий і простий спосіб для невеликих обсягів користувачів.

2) LDAP/Active Directory. Цей метод дозволяє використовувати вже існуючі бази даних користувачів з інших систем, таких як LDAP або Active Directory. Він спрощує управління користувачами, оскільки вони уже існують у цих каталогах. Аутентифікація Dovecot відбувається через ці джерела.

3) SQL бази даних. Dovecot підтримує різні типи баз даних, які можна використовувати для зберігання облікових даних користувачів. Це дозволяє більшу гнучкість та контроль над даними, оскільки управління користувачами може бути реалізовано через SQL-запити. Проте цей підхід вимагає налаштування та керування базою даних, що може бути складним.

4) Kerberos. Якщо у системі використовується аутентифікація Kerberos, Dovecot може бути налаштований для використання цієї системи аутентифікації для зберігання та перевірки облікових даних користувачів.

Вибір методу залежить від потреб, обсягу користувачів, рівня безпеки та доступних ресурсів. Кожен метод має свої переваги та обмеження, тому важливо обрати той, що найкраще відповідає вимогам.

Всі методи мають свої можливості налаштування політики паролів. Перший метод в базовій конфігурації за замовчування в операційній системі FreeBSD не

використовує політику паролів. Для покращення захисту від brute-force атак здійснимо налаштування та застосування політики паролів в операційній системі FreeBSD за допомогою PAM [9].

3.1.1 Налаштування політики паролів

Забезпечення безпеки локальних облікових записів шляхом застосування вимог щодо довжини, складності та надійності паролів є ключовою складовою захисту від brute-force атак. Ці вимоги можна налаштувати за допомогою PAM, що дозволяє контролювати стійкість паролів та їх складність для підвищення рівня безпеки системи [9].

Модулі аутентифікації PAM є стандартним механізмом в багатьох сучасних операційних системах, включаючи FreeBSD, які забезпечують гнучкість управління процесом аутентифікації користувачів. PAM дозволяє адміністраторам системи налаштовувати та контролювати процес аутентифікації, забезпечуючи високий рівень безпеки.

Основні функції PAM включають наступне:

1) Гнучкість управління аутентифікацією. PAM дозволяє використовувати різні методи аутентифікації, такі як паролі, ключі, біометричні дані тощо. Це дозволяє налаштувати різні способи аутентифікації для різних користувачів або груп користувачів.

2) Розширення функціональності. PAM може бути розширений шляхом використання додаткових модулів. Це дозволяє розширювати функціонал аутентифікації шляхом включення нових модулів без зміни основного коду системи.

3) Безпека. Використання PAM дозволяє встановлювати правила та політики безпеки для аутентифікації. Можливість використання складних паролів, періодичної зміни паролів та інші аспекти безпеки можуть бути легко налаштовані через PAM.

4) Системна аудит. PAM дозволяє забезпечити системну безпеку та можливість аудиту процесу аутентифікації, включаючи ведення журналів дій користувачів для подальшого аналізу.

Модуль pam_passwdqc.so є одним із модулів, які використовуються в PAM для керування аутентифікацією та політиками паролів у системах UNIX-подібних операційних систем, таких як FreeBSD [10].

Модуль реалізує ряд строгих правил щодо встановлення паролів, що допомагає підвищити рівень безпеки в системі. Ці правила можуть включати обмеження на довжину пароля, складність пароля та інші стандарти безпеки.

Основні характеристики pam_passwdqc.so включають:

1) Складність пароля. Модуль може вимагати від користувачів використання паролів, які містять різні типи символів (цифри, великі та малі літери, спеціальні символи). Це підвищує складність пароля та ускладнює завдання зламу.

2) Мінімальна та максимальна довжина пароля: Можливість налаштування мінімальної та максимальної довжини пароля, що покращує надійності пароля.

Для налаштування модуля pam_passwdqc.so у FreeBSD відредагуємо файл /etc/pam.d/passwd (Рисунок 3.1).

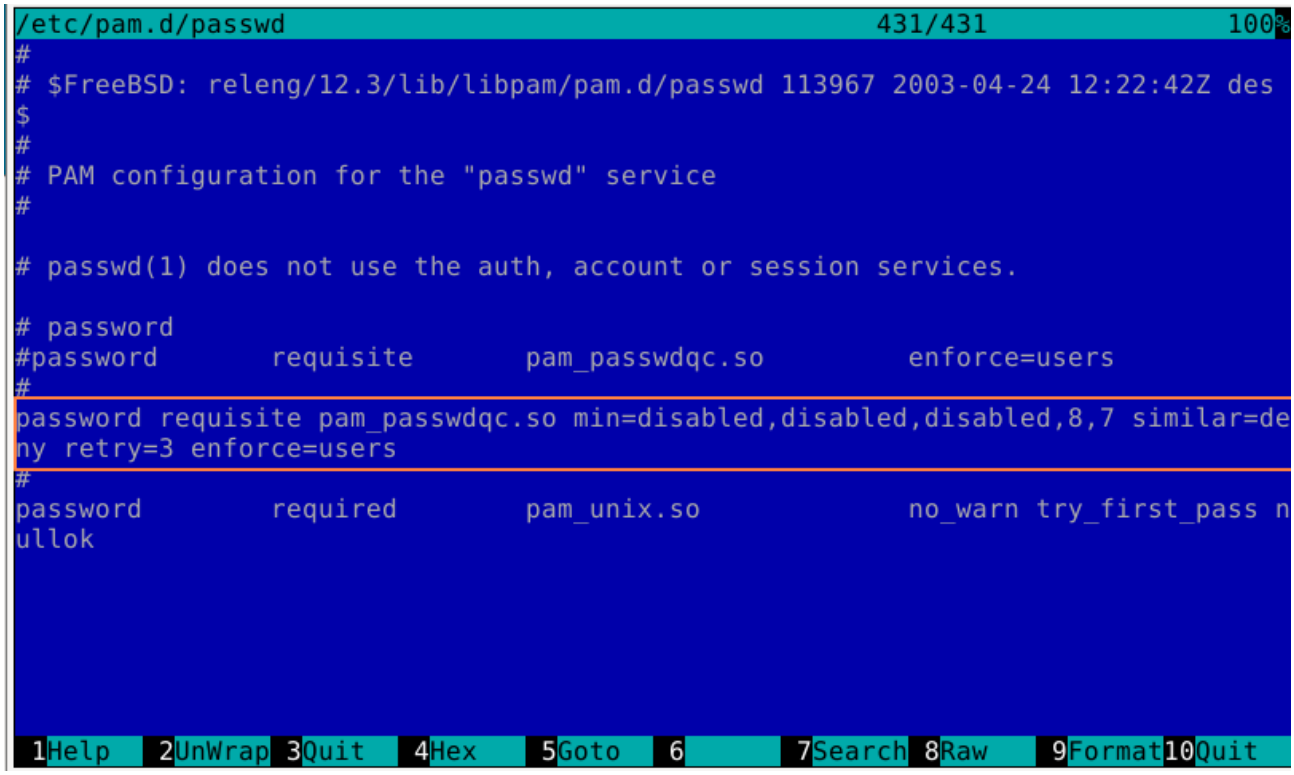


Рисунок 3.1 – Налаштування модуля pam_passwdqc.so у FreeBSD

Налаштування, які присутні в конфігураційному файлі мають наступне значення:

1) `min=disabled,disabled,disabled,8,7`. Ця опція визначає мінімальну довжину пароля для різних класів паролів. Класифікація базується на складності пароля (кількість використовуваних різних типів символів: великі букви, малі букви, цифри, інші символи). Кожна позиція в цій опції відповідає класу, починаючи з найбільш простого (тільки один тип символів) і закінчуючи найбільш складним (всі чотири типи символів);

У вашому випадку:

- перші три disabled означають, що для паролів, що складаються тільки з одного типу символів (наприклад, тільки літери або тільки цифри), не встановлено мінімальної довжини, тому що такі паролі не дозволені;
- 8 вказує, що паролі з трьома типами символів повинні бути довжиною не менше 8 символів;
- 7 вказує, що паролі, які містять чотири типи символів, повинні мати мінімум 7 символів;

2) `similar=deny`. Це означає, що новий пароль не повинен бути занадто схожим на старий. Ця опція допомагає запобігти використанню паролів, які змінюються лише незначною мірою;

3) `retry=3`. Це вказує на кількість спроб, які користувач може зробити, коли вводить новий пароль. Якщо користувач не вводить прийнятний пароль після вказаної кількості спроб, процедура зміни пароля закінчується невдало;

4) `enforce=users`. Ця опція змушує правила застосовуватися до всіх користувачів системи.

Модуль pam_passwdqc.so є важливим інструментом для підвищення безпеки облікових записів користувачів у системах, що базуються на UNIX, дозволяючи адміністраторам налаштовувати політики безпеки паролів згідно поточних вимог та стандартів безпеки.

Для встановлення терміну дії пароля у FreeBSD, налаштуємо параметр passwordtime для класу входу користувача у файлі /etc/login.conf (Рисунок 3.2). Це допоможе визначити строк дії пароля згідно потреб безпеки.

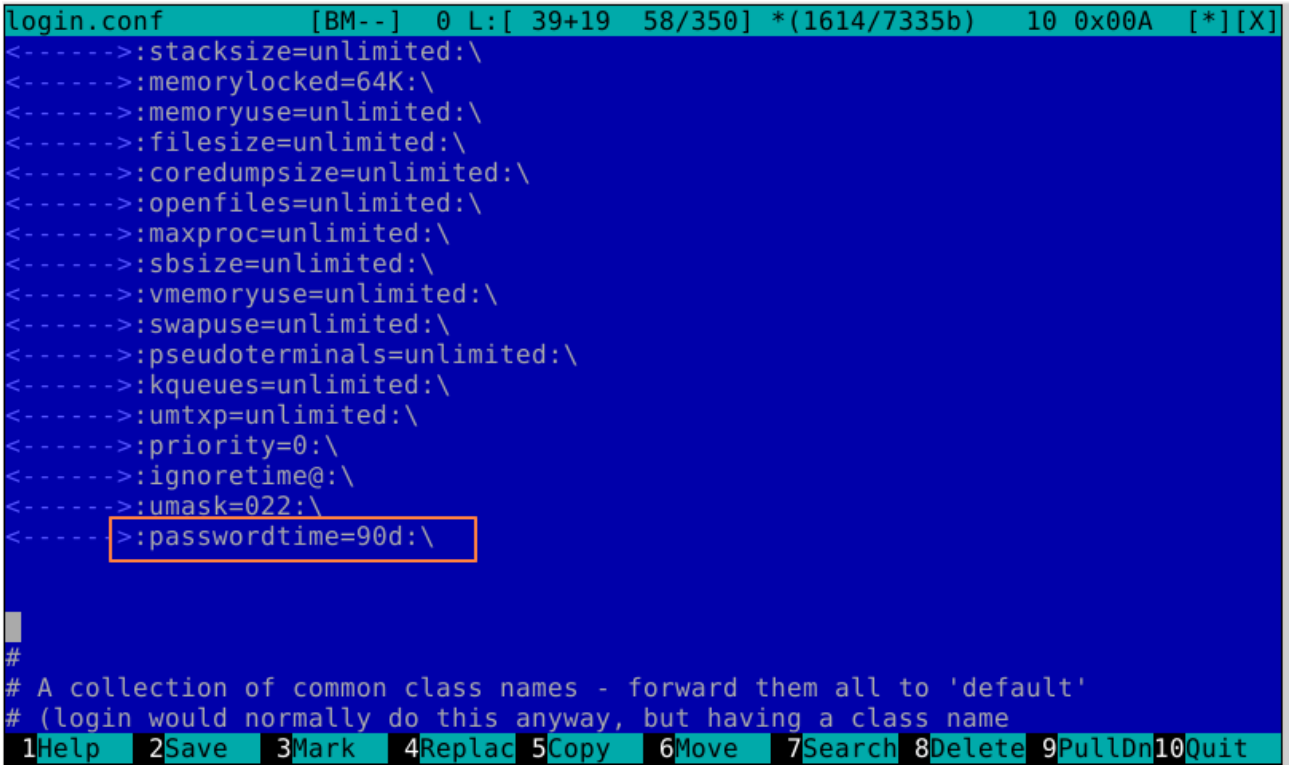


Рисунок 3.2 – Налаштування параметр passwordtime для класу входу користувача у файлі /etc/login.conf

В нашому налаштуванні встановлено термінів дії пароля 90 днів. Отже користувачеві потрібно буде змінювати свій пароль кожних 90 днів.

3.1.2 Проведення тестування політики паролів

Проведемо тестування коректності застосування політики паролів. Спробуємо змінити пароль користувача `admin`. Як можна побачити з рисунку 3.3 система видає попередження про вимоги що до складності паролів та не дозволить встановити простий пароль.

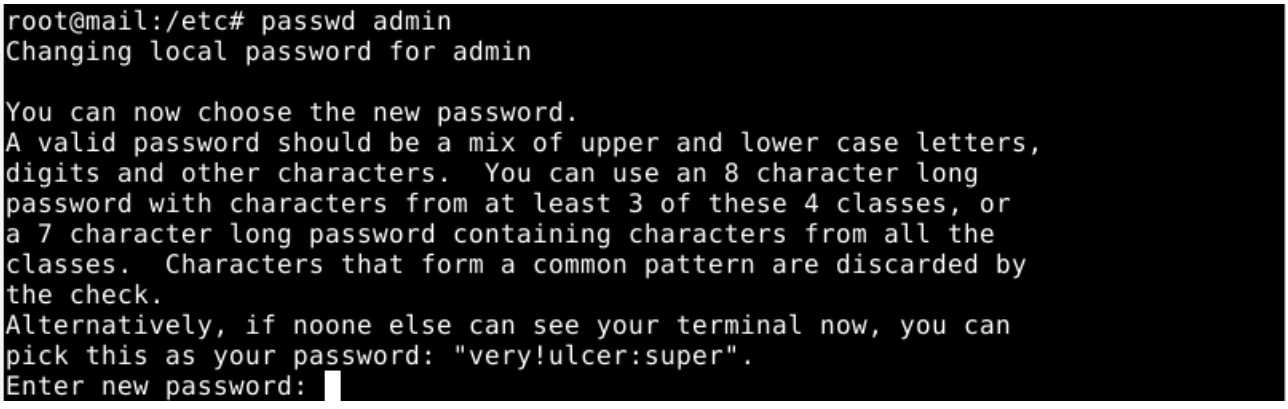


Рисунок 3.3 – Попередження при зміні паролю користувача

Система пропонує пароль "`very!ulcer:super`" як приклад прийнятного пароля, який задовольняє вказані вимоги. Користувачу пропонується ввести новий пароль, відповідно до вказаних правил безпеки.

3.2 Розробка захисту від швидких brute-force атак

3.2.1 Написання правил PF для захисту від швидких атак

PF - це відома в багатьох операційних системах, включаючи FreeBSD, OpenBSD і NetBSD, система фільтрації пакетів [4]. Вона використовується для керування мережевим трафіком, брандмауером і NAT. PF надає розширені засоби для керування мережевим трафіком та керування брандмауером.

Основні характеристики та можливості PF:

1) Фільтрація пакетів. PF може використовуватися для фільтрації вхідних і вихідних мережевих пакетів на основі різних критеріїв, таких як IP-адреси, порти, протоколи, стани тощо. Це дозволяє створити політику безпеки і обмежити доступ до ресурсів мережі.

2) NAT. PF підтримує NAT, що дозволяє приховати внутрішні IP-адреси в мережі і надавати їм доступ до мережі Інтернет через одну або декілька зовнішніх IP-адрес.

3) Застосування відстеження стану. PF підтримує відстеження стану, що дозволяє обробляти пакети на основі їх взаємодії з попередніми пакетами в мережі.

4) Черги ALTQ. Він також підтримує функцію очікування черги, яка дозволяє керувати пропускною здатністю мережі, встановлюючи пріоритети та обмеження швидкості для різних видів трафіку.

5) Логування трафіку. PF може логувати мережевий трафік для аналізу та відлагодження.

6) Можливість зміни конфігурації в реальному часі: Можливо змінювати правила PF без перезапуску служби.

PF є потужним інструментом у сфері мережевої безпеки, оскільки надає великий спектр можливостей для фільтрації та керування мережевим трафіком.

Файл pf.conf використовується для налаштування PF - брандмауеру, що є частиною операційної системи FreeBSD.

На рисунку 3.4 наведений конфігураційний файлу pf.conf з налаштуваннями для захисту від швидких brute-force атак.

```
pf.conf            [----]  0 L:[  1+14  15/ 15] *(337 / 337b) <EOF>        [*][X]
#!/bin/sh
ext_if = "em0".
#
#FOR IMAP brute force
#fast
table <fastbruteforceimap> persist
block drop in quick from <fastbruteforceimap>
#
pass in quick on $ext_if proto tcp from any to $ext_if port {imaps, imap} \
<------>flags S/SA keep state  \
<------>(max-src-conn 15, max-src-conn-rate 20/120,  \
<------>overload <fastbruteforceimap> flush global)
#
```

Рисунок 3.4 – Конфігураційний файлу pf.conf з налаштуваннями для захисту від швидких brute-force атак

Налаштування, які наведені в конфігураційному файлі pf.conf мають наступне значення:

1) `ext_if = "em0"`. Ця змінна визначає ім'я зовнішнього інтерфейсу. В цьому випадку ім'я інтерфейсу встановлено як "em0";

2) `table <fastbruteforceimap> persist`. Тут створюється таблиця PF з іменем "fastbruteforceimap" та позначається як постійну. Ця таблиця буде використовуватися для відстеження адрес, з яких відбуваються спроби brute-force атак;

3) `block drop in quick from <fastbruteforceimap>`. Це правило вказує PF блокувати всі вхідні пакети з IP адрес, які знаходяться в таблиці "fastbruteforceimap";

4) `pass in quick on $ext_if proto tcp from any to $ext_if port {imaps, imap}`. Це правило дозволяє вхідний мережевий трафік на інтерфейс `$ext_if` з будь-якої адреси на порт 993 або 143 по протоколу TCP;

5) `flags S/SA keep state`. Це вказує PF відстежувати стан пакетів і дозволяти тільки пакети, які відповідають встановленим станам (S - початок з'єднання, SA - відповідь на початок з'єднання);

6) `max-src-conn 15`. Це правило обмежує максимальну кількість одночасних з'єднань з одного джерела до 15;

7) `max-src-conn-rate 20/120`. Це обмеження максимальної швидкості з'єднань з одного джерела до 20 з'єднань за хвилину;

8) `overload <fastbruteforceimap> flush global`. Якщо обмеження спрацює, то IP адреса, з якої надходять спроби brute-force атаки, буде додана до таблиці "fastbruteforceimap" та відбудеться видалення заблокованих пакетів з загальної черги згідно з правилом "flush global".

Представлена конфігурації PF призначена для захисту сервера IMAP від швидких brute-force атак.

3.2.2 Проведення тестування реалізованого захисту

Для проведення тестування налаштованого захисту здійснимо швидку brute-force атаку за допомогою інструменту Hydra з операційно системи BackBox Linux. На рисунку 3.5 показано параметри запуску Hydra.

```
backbox@backbox:/usr/share/john$
backbox@backbox:/usr/share/john$ sudo hydra -l admin -P /usr/share/john/password.lst  -s 993 -t 64
192.168.0.111 imaps
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
vice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics a
nyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-04 18:00:41
[INFO] several providers have implemented cracking protection, check with a small wordlist first - a
nd stay legal!
[DATA] max 64 tasks per 1 server, overall 64 tasks, 3559 login tries (l:1/p:3559), ~56 tries per tas
k
[DATA] attacking imaps://192.168.0.111:993/
```

Рисунок 3.5 – Швидка brute-force атака за допомогою інструменту Hydra

Параметри команди, яка показана на рисунку 3.5 мають наступне значення:

1) `-l admin`. Задає логін, який буде використовуватися для аутентифікації;

2) `-P /usr/share/john/password.lst`. Вказує шлях до файлу, який містить словник паролів для спроб входу;

3) `-s 993`. Вказує порт, на якому працює IMAPS;

4) `-t 64`. Вказує кількість одночасних задач, які виконуватимуться;

5) `-I 192.168.0.111`. Вказує IP адресу цілі атаки;

6) `imaps`. Вказує на протокол, який використовується для атаки (в даному випадку IMAPS).

Початок тестової атаки можна відслідкувати в файлі `/var/log/dovecot.log`. Файл dovecot.log є файлом журналу, який містить інформацію про події та помилки, пов'язані з роботою IMAP сервера Dovecot.

Файл містить успішні та неуспішні спроби входу користувачів в систему IMAP. Інформацію про підключення користувачів до їхніх поштових скриньок через протокол IMAP. Дані про будь-які помилки, що виникають під час роботи IMAP сервера. Це може включати помилки аутентифікації, помилки при зверненні до бази даних або конфлікти на рівні системи.

На рисунку 3.6 показано записи в файлі dovecot.log під час виконання атаки.

```
Nov 04 19:00:42 imap-login: Debug: SSL: where=0x2002, ret=-1: before SSL initial
ization
Nov 04 19:02:01 imap-login: Debug: SSL: where=0x2002, ret=-1: TLSv1.3 early data
Nov 04 19:02:01 imap-login: Debug: SSL error: read(size=509) failed: Operation t
imed out
Nov 04 19:02:01 imap-login: Info: Disconnected: Connection closed: read(size=509
) failed: Operation timed out (no auth attempts in 80 secs): user=<>, rip=192.16
8.0.115, lip=192.168.0.111, TLS handshaking: read(size=509) failed: Operation ti
med out, session=<27xjlFYJoILAqABz>
Nov 04 19:02:01 imap-login: Debug: SSL: where=0x2002, ret=-1: TLSv1.3 early data
Nov 04 19:02:01 imap-login: Debug: SSL error: read(size=509) failed: Operation t
imed out
```

Рисунок 3.6 – Записи в файлі dovecot.log при швидкій brute-force атаці

В файлі dovecot.log можна побачити що спроб надіслати логін та пароль для вгадування паролю користувача `admin` не було, лише було здійснено підключення до IMAP сервера багатьма одночасними встановленими сесіями. Це пов’язано з тим що при швидкій brute-force атаці захист за допомогою PF

спрацював швидше чим Hydra встигла надіслати логін та пароль для спроби входу.

На рисунку 3.7 можна побачити що IP BackBox Linux заблокована.

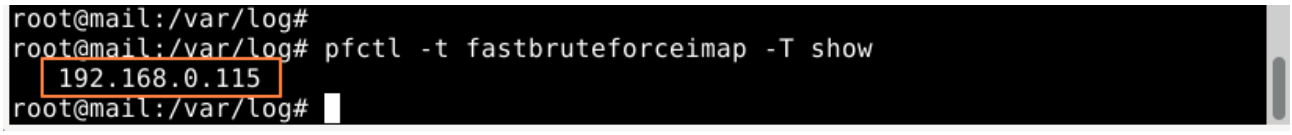


Рисунок 3.7 – Вивід вмісту таблиці `fastbruteforceimap`

Отже захист за допомогою PF від швидких brute-force є ефективним та надійним. Його налаштування надає можливість ефективно блокувати IP адреси, які пробують здійснювати атаку. Це дозволяє ефективно контролювати доступ та мінімізувати ризики швидких атак на систему IMAP сервера.

3.3 Розробка захисту від повільних brute-force атак

Захист від повільних brute-force атак буде реалізовано за допомогою програмного модуля написаного на bash. Створення програмного модуля для захисту від brute-force атак передбачає послідовні кроки і заходи для виявлення та зменшення можливостей проведення таких атак.

Модуль буде аналізувати лог файл dovecot.log та при виявленні атаки буде блокування IP зловмисників за допомогою брандмауер PF.

Також програмний модуль буде повідомляти про спроби здійснення brute-force атаки в корпоративний Jabber сервер.

3.3.1 Механізм виявлення та блокування brute-force атаки

Механізм виявлення та припинення brute-force атак буде реалізований в такий спосіб:

1) Створення додаткової таблиці в PF. До конфігураційного файлу pf.conf добавимо таблицю, яка буде використана для блокування IP адрес, які здійснюють повільні brute-force атаки.

2) Аналіз файлу dovecot.log. Аналізуємо вміст файлу /var/log/dovecot.log на наявність помилок автентифікації "auth failed" за останні 10 хв.

3) Виявлення атаки. Після обробки всіх рядків журналу перевіряємо кількість невдалих спроб автентифікації для кожної IP-адреси. Якщо кількість спроб більше або дорівнює 3, то IP адреса блокується за допомогою PF.

4) Генерація повідомлення. Додатково, генерується повідомлення про атаку на IMAP сервер, яке буде надіслане через протокол XMPP на корпоративний Jabber сервер адміністратору системи.

3.3.2 Зміна налаштувань брандмауера PF

Для забезпечення функціонування механізму, який був описаний в розділі 3.3.1, проведемо зміни в файл конфігурації pf.conf шляхом додавання наступних рядків налаштувань:

1) `table <bruteforceip> persist file "/etc/bruteforceip"`. Цей рядок визначає та ініціалізує таблицю з назвою <bruteforceip>, що зберігатиме адреси IP, які будуть заблококовані. Ця таблиця буде постійно зберігатися у файлі "/etc/bruteforceip".

2) `block drop in quick from <bruteforceip>`. Цей рядок встановлює правило, що блокує вхідні пакети з IP адресам, які містяться в таблиці <bruteforceip>. Це захистить систему від вхідних з'єднань з цих адрес, запобігаючи атакам з цих джерел.

3) `table <slowbruteforceimap> persist`. Ця частина визначає та ініціалізує іншу таблицю під назвою <slowbruteforceimap> для обробки повільних brute-force атак.

4) `block drop in quick from <slowbruteforceimap>`. Аналогічно першій таблиці, цей рядок встановлює правило для блокування вхідних пакетів з IP адрес, які зберігаються в таблиці <slowbruteforceimap>. Це захистить систему від повільних атак brute-force з цих джерел.

На рисунку 3.8 показано оновлений вмісти файлу pf.conf.

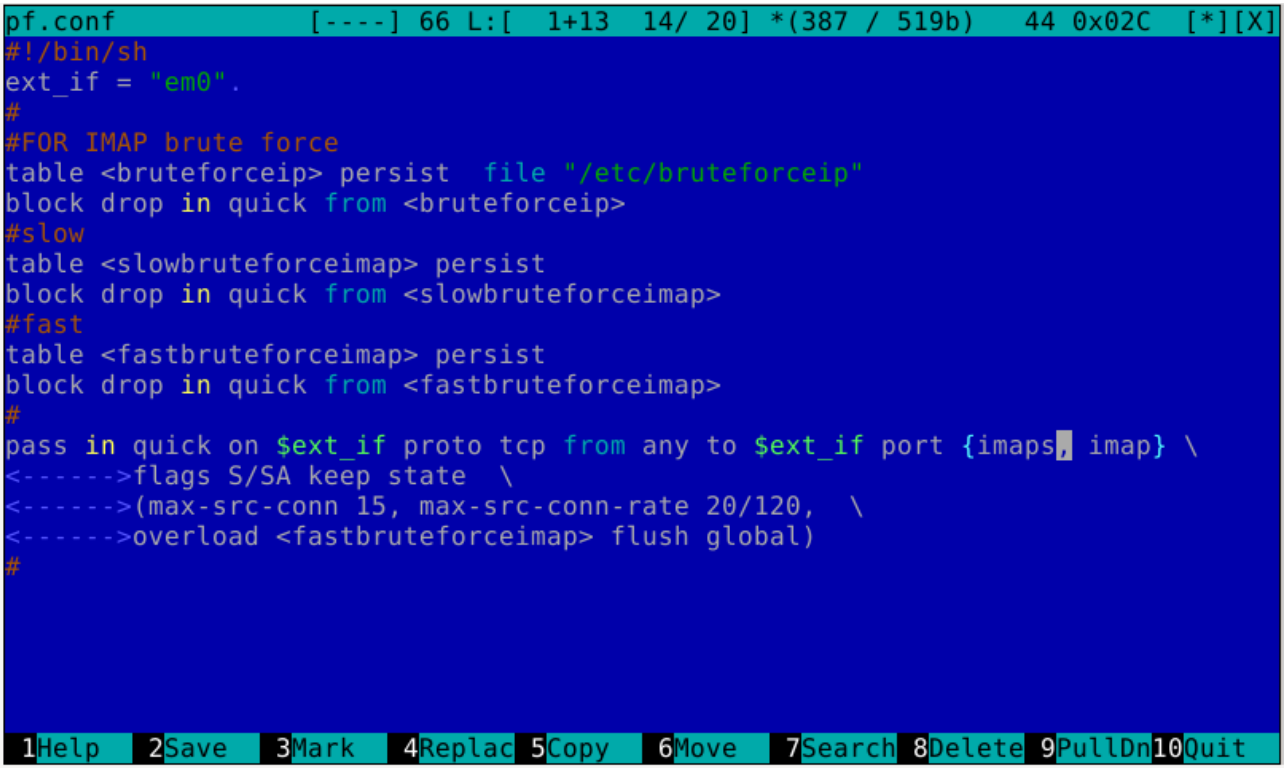


Рисунок 3.8 – Оновлений конфігураційний файл pf.conf

Цей набір налаштувань PF є частиною механізму для виявлення та блокування як повільних, так і швидких brute-force атак на IMAP сервері.

3.3.3 Обрання середовища для розробки

Для створення програмного модуля, який автоматично блокуватиме IP-адреси зловмисників, буде використана мова програмування оболонку bash [11].

Bash є широко використовуваною командною оболонкою та мовою сценаріїв у системах Unix та Unix-подібних операційних системах, таких як Linux та macOS. Це дозволяє виконувати команди, робити сценарії для автоматизації завдань та обробки файлів, керувати процесами, змінювати системні налаштування та багато іншого. Bash підтримує введення та виведення даних, роботу з текстовими рядками, умовні вирази, цикли, функції та багато інших можливостей програмування, що дозволяє створювати скрипти для автоматизації різноманітних завдань на командному рядку операційної системи.

3.3.4 Написання програмного модуля

Програмний модуль, розроблений на мові програмування оболонки bash та призначений для виявлення та реагування на brute-force атаки на IMAP сервер. В додатку Б подано лістинг цього сценарію.

Логіка роботи сценарію наступна:

1) Оголошуються глобальні змінні та асоціативний масив для відстеження кількості невдалих спроб входу за кожною унікальною IP-адресою.

Значення змінних:

а) `log_file="/var/log/dovecot.log"`. Це змінна, яка містить шлях до журналу Dovecot - файлу журналу, в якому записуються події, пов'язані з роботою поштового сервера Dovecot;

б) `subj="IMAP Server date "+DATE: %Y-%m-%d TIME: %H:%M:%S""`. Ця змінна створює тему для повідомлення. Використано команду date для вставки поточної дати та часу;

в) `declare -A ip_counts`. Це оголошення асоціативного масиву bash. Тут створюється порожній асоціативний масив з ім'ям ip_counts, який буде використовуватися для збереження та підрахунку кількості невдалих спроб входу за кожним унікальним IP адресом, які були зафіксовані в журналі Dovecot.

2) Визначаються дві функції `get_current_time()` та `get_x_minutes_ago()` Які призначені для отримання поточного часу у форматі години:хвилини:секунди. Та отримання час, який був 10 хвилин тому.

3) Визначається функція `is_ip_blocked()` призначена для перевірки того, чи IP-адреса вже заблокована у файлі /etc/bruteforceip.

4) Функція `handle_ip_blocking()` відповідає за блокування IP-адреси зловмисників.

Рядки коду в даній функції виконують наступні завдання:

а) `local ip=$1` та `local count=$2`. Створення локальних змінних ip і count, які отримують значення IP-адреси і лічильника спроб, що передаються функції як аргументи;

б) `if [ "$count" -ge 3 ]; then`. Перевірка, чи лічильник спроб (count) перевищує або дорівнює 3. Якщо умова справджується то виконується код, що розміщений всередині цього блоку;

в) `printf "$ip\n" >> /etc/bruteforceip`. Додає IP-адресу до файлу /etc/bruteforceip. Цей файл використовується для зберігання списку заблокованих IP-адрес;

г) `pfctl -t slowbruteforceimap -T add $ip >> /root/bruteforceimap/addtablebrute 2>&1`. Додає IP-адресу до таблиці блокування PF. Дія цього рядка полягає в блокуванні IP адрес в реальному часі на рівні мережевого стеку;

д) `printf "Added IP to PF block table: $ip (count: $count)\n"`. Виводить повідомлення про успішне додавання IP-адреси до файлу та таблиці блокування;

е) `body="BRUTE FORCE Attack IMAP Alert: IP -$ip; IP count -$count"`. Підготовка повідомлення для надсилання адміністратору про спробу атаки;

є) `echo "$body" | sendxmpp -d -s "$subj" admin@xmpp.cstntu.local` Надсилає сповіщення про спробу атаки через протокол XMPP на корпоративний Jabber сервер адміністратору системи [12].

Сценарій дозволяє автоматизувати процес виявлення та блокування IP-адрес, які здійснюють повільну brute-force атаку на сервер IMAP.

3.3.5 Автоматизація процесу виявлення та блокування атаки

У FreeBSD для автоматизації процесу виявлення атак і блокування IP-адрес зловмисників буде використано механізм запуску сценарію `bruteforcealertimap.bash` як сервісу з використання інструментів системи для управління сервісами.

Для цього створимо в каталозі `/usr/local/etc/rc.d` файл `bruteforce_monitor` та встановимо біт виконання. В додатку В показано вміст файлу для налаштування сервісу `bruteforce_monitor`.

Основні налаштування сервісу `bruteforce_monitor` мають наступне занчення:

1) `PROVIDE, REQUIRE, KEYWORD`. Ці параметри визначають, як сервіс взаємодіє з іншими службами під час завантаження чи вимкнення системи.

2) Завантаження системних функцій. `./etc/rc.subr` - ця команда включає системні функції, необхідні для коректної роботи сервісу.

3) `name="bruteforce_monitor"`. Це змінна, яка містить назву сервісу, яку цей скрипт представляє. В даному випадку, назва служби - `bruteforce_monitor`.

4) `rcvar=bruteforce_monitor_enable`. Ця змінна представляє конфігураційну змінну, яка визначає, чи ввімкнена чи вимкнена ця служба. Під час завантаження системи це значення визначає, чи буде служба автоматично запущена чи ні.

5) `extra_commands="status restart"`. Це змінна, яка містить додаткові команди, які служба може виконувати. В цьому випадку, ця служба має команди status та restart, які дозволяють перевіряти стан служби та перезапускати її відповідно.

6) `start_cmd="${name}_start"`. Ця змінна визначає команду, яка буде виконана при запуску служби. Значення цієї змінної буде ${name}_start (де ${name} - назва служби), що співвідноситься зі створеною командою запуску служби.

7) `stop_cmd="${name}_stop"`. Ця змінна визначає команду, яка буде виконана при зупинці служби.

8) `status_cmd="${name}_status"`. Ця змінна визначає команду, яка буде викликана для отримання статусу служби.

9) `restart_cmd="${name}_restart"`. Ця змінна визначає команду, яка буде виконана для перезапуску служби.

10) Функція `bruteforce_monitor_start` відповідає за запуск сценарію `bruteforcealertimap.bash` для відслідковування та обробки лог-файлів щодо спроб атаки. Основна дія полягає в безкінечному циклі, який виконується кожні 5 секунд, забезпечуючи постійний процес слідкування за лог-файлом dovecot.log. Вміст логів аналізується сценарієм `bruteforcealertimap.bash`, який визначає,

чи спостерігаються спроби атаки. У разі знаходження спроби атаки, сценарій `bruteforcealertimap.bash` реагує на це та оновлює свій власний лог-файл `bruteforce_monitor.log`, вказуючи час та інформацію щодо виявлення потенційної атаки. Крім цього, під час роботи ця функція реєструє PID процесу, що відповідає за моніторинг, в файлі `/var/run/bruteforce_monitor.pid`, забезпечуючи можливість подальшого контролю за процесам.

11) Функція `bruteforce_monitor_stop` відповідає за припинення процесу моніторингу. Вона знаходить ідентифікатор процесу (PID), який зберігаїться у файлі `/var/run/bruteforce_monitor.pid` та припиняє роботу сценарію, викликаючи сигнал на зупинку процесу, після чого видаляє файл з PID.

12) Функція `bruteforce_monitor_status` використовується для перевірки поточного стану процесу моніторингу. Вона перевіряє наявність файлу `/var/run/bruteforce_monitor.pid`, який зберігає ідентифікатор процесу. Якщо файл існує, це свідчить про те, що процес моніторингу працює, та виводить інформацію про його роботу разом з ідентифікатором процесу. У випадку відсутності файлу, виводиться повідомлення, що процес моніторингу не запущено.

13) Функція `bruteforce_monitor_restart` відповідає за перезапуск процесу моніторингу при зміні його налаштувань чи інших обставинах, які вимагають його повторного запуску. Для цього спершу викликається функція `bruteforce_monitor_stop` для зупинки поточного процесу моніторингу. Після зупинки процесу відбувається пауза тривалістю 2 секунди, після чого запускається процес моніторингу знову за допомогою функції `bruteforce_monitor_start`.

Встановимо в конфігураційному файлі rc.conf значення змінній bruteforce_monitor_enable на "YES" (`bruteforce_monitor_enable="YES"`). Це означає, що сервіс bruteforce_monitor буде запущений автоматично при завантаженні операційної системи.

Запустимо за допомогою команди `service bruteforce_monitor start`, наш сервіс та перевіримо його статус (Рисунок 3.9).

```
root@mail:~/bruteforceimap/conf# service bruteforce_monitor start
root@mail:~/bruteforceimap/conf# service bruteforce_monitor status
bruteforce_monitor is running with PID 34987.
root@mail:~/bruteforceimap/conf#
```

Рисунок 3.9 – Вивід команди `service bruteforce_monitor status`

Для управління запущеним сервісом можна також використовувати команди stop та restart.

Отже сценарій bruteforcealertimap.bash налаштовано як сервіс в операційній системі FreeBSD, що дозволяє автоматично виявляти та блокувати IP-адреси під час brute-force атак на сервер IMAP.

3.3.6 Тестування розробленого захисту

Для проведення тестування налаштованого захисту здійснимо повільну brute-force атаку за допомогою інструменту Hydra з операційно системи BackBox Linux. На рисунку 3.10 показано параметри запуску Hydra.

```
backbox@backbox:/usr/share/john$
backbox@backbox:/usr/share/john$ sudo hydra -l admin -P /usr/share/john/password.lst  -s 993 -t 3
 192.168.0.111 imaps
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
ervice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethi
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-05 03:09:18
[INFO] several providers have implemented cracking protection, check with a small wordlist first -
 and stay legal!
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3559 login tries (l:1/p:3559), ~1187 tries per t
ask
[DATA] attacking imaps://192.168.0.111:993/
```

Рисунок 3.10 – Повільна brute-force атака за допомогою інструменту Hydra

Параметр `-t` вказує кількість одночасних задач, які виконуватимуться. Для моделювання повільної атаки було встановлено лише 3 одночасних сесії.

Переглядаючи інформацію, яка фіксується у файлі журналу /var/log/dovecot.log можна відслідковувати початок тестової атаки.

На рисунку 3.11 показано записи в файлі dovecot.log під час виконання повільної brute-force атаки.

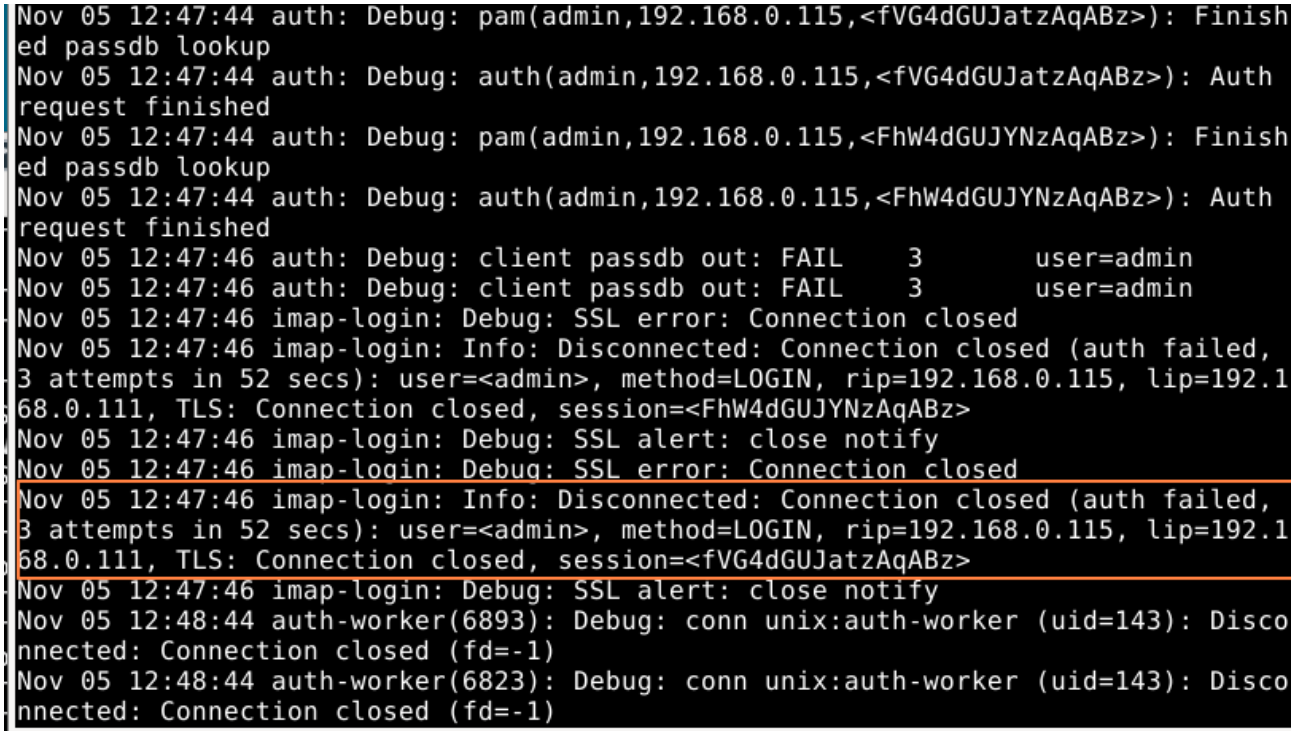


Рисунок 3.11 – Записи в файлі dovecot.log при повільній brute-force атаці

Інформація з цього запису в журналі показує, що спроба аутентифікації для користувача "admin" була неуспішною. Клієнт з IP-адресою "192.168.0.115" спробував увійти, але не пройшов перевірку, зробивши три спроби за 52 секунди. TLS-з'єднання також було закрито.

З рисунку 3.12 можна побачити що спрацював саме захист від повільних brute-force атак.

Рисунок 3.12 – Вивід вмісту таблиці `slowbruteforceimap`

Захист від швидких brute-force атак не зміг виявити та заблокувати атаку, але це було очікувано.

Лог файл сервісу `bruteforce_monitor` також містить інформацію про виявлену атаку (Рисунок 3.13).

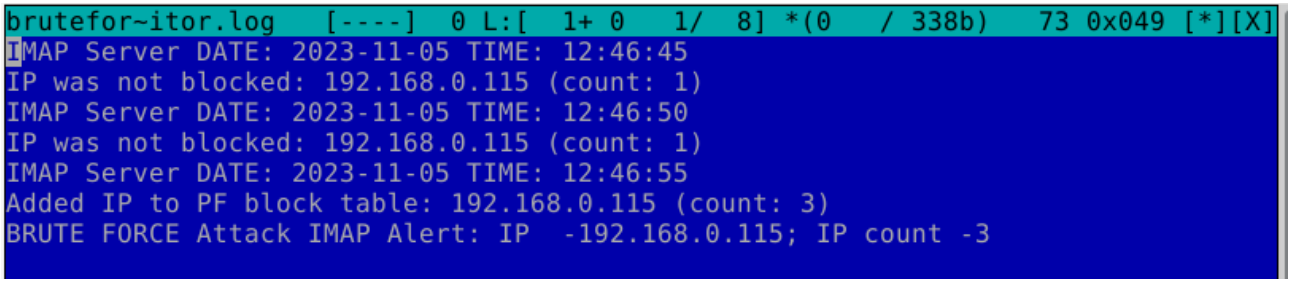


Рисунок 3.13– Вміст файлу `bruteforce_monitor.log`

Перші дві події показують, що IP-адреса 192.168.0.115 не була заблокована та кількість спроб доступу становить 1. Третя подія вказує, що після третьої спроби доступу з тієї самої IP-адреси, вона була додана до таблиці блокування PF.

Останній рядок файлу містить копію повідомлення про brute-force атаку, яке було надіслано по протоколу XMPP на корпоративний Jabber сервер адміністратору системи (Рисунок 3.14).

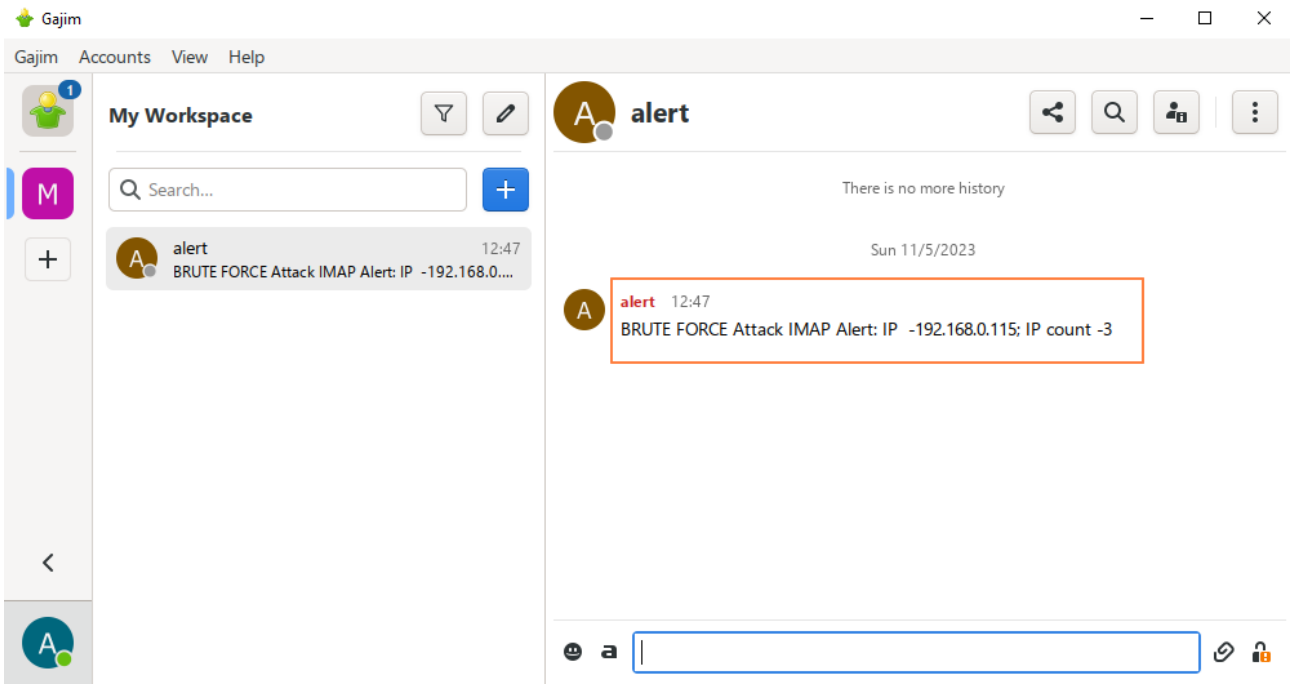


Рисунок 3.14– Повідомлення про brute-force атаку

Це повідомлення інформує про атаку типу "brute-force" на сервері IMAP, яка була здійснена з IP 192.168.0.115 та була заблокована за три невдалі спроби входу.

Отже розроблений механізм захисту від повільних brute-force атак функціонує коректно та успішно виявляє та блокує IP адреси зловмисників.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Забезпечення пожежної безпеки в приміщенні ЕОМ

Метою даної кваліфікаційної роботи є розробка, інтеграція та оцінка ефективності захисту від повільних та швидких brute-force атак на сервери, що працюють за протоколом IMAP. Дані системи встановлюються на серверному обладнанні, яке розміщене в приміщення спеціального типу. Пожежна безпека в серверних кімнатах є важливим завдання збереження матеріальних цінностей та життя людей.

Небезпечними чинниками, які впливають на людей під час пожежі, може бути відкритий вогонь чи іскри, підвищена температура повітря, предметів, токсичні продукти горіння, дим, знижена концентрація кисню. Тому пожежну безпеку вважають за невід'ємну частину охорони праці.

Пожежна безпека – це стан об'єкта, за якого із встановленою ймовірністю виключається можливість виникнення та розвитку пожежі, а також забезпечується захист матеріальних цінностей. У сучасних ЕОМ дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості один від одного розташовуються різні елементи, дроти, комутаційні кабелі. При протіканні електричного струму відходить значна кількість теплоти, що може призвести до підвищення температури окремих вузлів до 80-100°С. З іншого боку, робоча температура силових транзисторів сягає 120°С. Все це може викликати оплавлення ізоляції з'єднувальних дротів, їх оголення і, як наслідок, коротке замикання, що супроводжується іскрінням, веде до неприпустимих температурних навантажень елементів схем, їх згоряння з виділенням диму [13].

Будівлі і ті їх частини, в яких розташовуються ЕОМ, повинні мати не нижче II ступень вогнестійкості. Приміщення для обслуговування, ремонту та налагодження ЕОМ повинні належати до категорії В за безпекою що до пожеж та вибухів, а за класом приміщення - до П за ПБЕ.

Неприпустимим є розташування приміщень категорій А і Б, а також виробництв з мокрими технологічними процесами поряд з приміщеннями, де

розташовуються ЕОМ, виконується їх обслуговування, налагодження і ремонт, а також над такими приміщеннями або під ними.

Стіни кабін мають бути виготовлені з негорючих матеріалів. Дозволяється виготовляти їх зі скла та металевих конструкцій. У кабіні мусить бути оглядове вікно (вікна). Висота оглядового вікна має бути не менше 1,5 м, а відстань від підлоги не більше 0,8 м.

Приміщення з ЕОМ повинні бути оснащені системою автоматичної пожежної сигналізації з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог правил пожежної безпеки в Україні. В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі.

Приміщення, в яких розміщуються великі ЕОМ загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до правил пожежної безпеки в Україні та вимог нормативно-технічної та експлуатаційної документації заводу-виробника [13].

Підходи до засобів пожежогасіння повинні бути вільними. Будівлі та приміщення, в яких експлуатуються ПК та виконується їх обслуговування, налагодження і ремонт, повинні відповідати вимогам пожежної безпеки об'єктів будівництва, експлуатаційної документації заводу-виробника ПК, чинним санітарним нормам у сфері охорони праці.

Не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки.

Приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до вимог, в інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі.

Приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення, мають бути оснащені вогнегасниками.

Приміщення, в яких розміщуються робочі місця операторів великих ЕОМ загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння

Система вентиляції обчислювальних центрів та приміщень з ЕОМ повинна бути обладнана блокувальним пристроєм, який забезпечує її відключення на випадок пожежі.

Пожежна безпека приміщень забезпечується такими засобами:

- справність електропроводки;
- наявність засобів пожежогасіння;
- наявність пожежної сигналізації.

До первинних засобів пожежогасіння у приміщеннях з ЕОМ відносяться різні вуглекислотні, аерозольні, порошкові вогнегасники, призначені для гасіння загорянь та пожеж у початковій стадії їх розвитку.

Вуглекислотні вогнегасники (ВВ-2, ВВ-5, ВВ-8) призначені для гасіння невеликих вогнищ горіння речовин, матеріалів та електроустановок під напругою. Дані вогнегасники містять вуглекислоту, яка при відкритті крана розширюється та викидається через розтруб у вигляді вуглекислого снігу температурою -55°С. Тривалість роботи вогнегасників 25-40 секунд, довжина струменя, що викидається, 1,5-2 м (ВВ-2, ВВ-5).

Аерозольні вогнегасники закачувального типу містять або тільки вогнегасний засіб, або ще й додатковий (робочий) газ (наприклад, азот, хладон). Вони призначені для гасіння невеликих вогнищ горіння речовин, матеріалів та електроустановок під напругою. Дані вогнегасники малогабаритні, спрощені (з об'ємом заряду від 0,25 до 1,0 літра).

Порошкові вогнегасники (ВП-1, Момент, ВП-2А, ВП-10А) застосовуються для гасіння лужних металів, що горять, горючих рідин, а також обладнання з напругою до 5000 В. Дані вогнегасники містять вогнегасний порошок і балон з газом. Порошок з корпусу вогнегасника виштовхується стисненим газом (азот, повітря) приблизно за 30 секунд.

Автоматичні засоби пожежогасіння розраховані на подачу вогнегасної речовини у разі виникнення пожежі незалежно від того, перебувають у

приміщенні люди або відсутні. Останнім часом знаходять широке застосування автономних автоматичних установок порошкового пожежогасіння.

Проведені дослідження в кваліфікаційній роботі вимагали взаємодії людини з серверним обладнанням. Тому важливим є забезпечити безпечні умови праці інженерів комп'ютерних систем при встановленні, налаштуванні та подальшому обслуговуванні систем захисту сервісів.

4.2 Підвищення стійкості роботи комп'ютеризованих систем в умовах дії ЕМІ ядерних вибухів

Інтенсивний сучасний технічний розвиток несе комфорт і процвітання в усі сфери людської діяльності, проте поряд з цим зростає ймовірність техногенної небезпеки. Техногенні небезпеки можуть носити механічний, енергетичний та хімічний характер. Однією з найпотужніших енергетичних небезпек є ядерний вибух. Ядерний вибух – це вибух, який утворюється при виділенні внутрішньої енергії при розпаді важких ядер урану-235, 233, 238, плутонію-239 та ін.

Внаслідок дії своїх вражаючих факторів ядерні вибухи призводять до масштабних небезпек та таких негативних наслідків як загибель людей, тварин і рослин, потрапляння радіоактивних речовин в навколишнє середовище, руйнування будівель, затоплення територій, пожеж.

Електромагнітне поле – це особлива форма матерії, яка виникає в результаті виробничої діяльності людей. Електромагнітні хвилі можуть існувати у вигляді випромінювань, що переміщуються в просторі зі швидкістю світла (с).

Вплив ЕМП на здоровий організм людини досліджений ще в наш час недостатньо. Існує ймовірність, що ЕМП призводить до розщеплення атомів і молекул організму на іони, а це може бути причиною утворення іонних струмів, які в результаті сприяють підвищенню температури тіла людини. Дослідження показали, що ЕМП може призводити до гальмування рефлексів, гіпотонії, збільшення лейкоцитів в крові людини, погіршення зору та ін. Певну небезпеку представляють для людини лінії електропередачі, поблизу яких визначається дуже значна напруженість електричного поля (до 15 КВ/м) [14].

При ядерному вибуху утворюється сильне електромагнітне випромінювання в широкому діапазоні хвиль з максимумом спектральної щільності в області 15-30 кГц. Це випромінювання триває кілька мікросекунд, тому його прийнято називати електромагнітним імпульсом.

ЕМІ характеризується великою напруженістю електричного та магнітного полів. Ці параметри є основним вражаючим фактором для струмопровідних елементів, хоча значного впливу на людину не мають. Імпульс струму, що з'являється на момент вибуху і високий потенціал можуть вивести з ладу трансформатор, пошкодити напівпровідникові елементи в приладах, розплавити ізоляційний матеріал на кабелях, спричинити вигорання запобіжників та розрядників. Особливу увагу слід приділити пунктам управління, де працюють люди, оскільки існує загроза ураження персоналу внаслідок виведення з ладу техніки та розгортання аварійної ситуації.

Для захисту необхідно здійснити екранування ліній зв'язку, пунктів управління, окремих вузлів та блоків, електро та радіоапаратури, використовувати спеціальні захисні пристрої [15].

Поряд з цим слід зазначити, оскільки час ЕМІ в кілька мільярдних часток секунд настільки мізерний, що його зовсім недостатньо, щоб спрацювали більшість електронних систем захисту. Тому чутливе комп'ютерне обладнання не завжди зможе уникнути потужного перенавантаження. Комп'ютерні системи містять багато напівпровідникових елементів (цифрові процесори, діоди, транзистори, випрямлячі та ін.), які є дуже вразливими до дії ЕМІ.

У випадку, коли ядерний вибух відбувся неподалік лінії електропостачання, то наведені в них напруги можуть проходити через провідники впродовж багатьох кілометрів, а також псувати апаратуру та становити загрозу людям, які перебувають на безпечній відстані від вибуху.

Отже, основні критерії, які слід враховувати під час підвищення стійкості роботи електричних та комп'ютеризованих систем при дії ЕМІ - це максимальна напруга та максимальна енергія. Зокрема напруга, що наводиться у струмопровідних елементах та кабельних лініях передач, при якій ще не виходять з ладу системи.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи освітнього рівня "Магістр" було проведено комплексне дослідження аспектів захисту IMAP сервера від brute-force атак.

В ході дослідження було розроблено, інтегровано та підтверджено ефективність заходів захисту від повільних та швидких brute-force атак.

Це включало:

1) Аналіз характеристик повільних та швидких brute-force атак на сервери електронної пошти, що працюють за протоколом IMAP.

2) Розробка та застосування політики паролів з метою підвищення безпеки облікових записів користувачів.

3) Налаштування систему захисту в операційній системі FreeBSD для блокування швидких brute-force за допомогою PF.

4) Написання програмного модуля для аналізу лог-файлів IMAP сервера Dovecot з метою виявлення повільних brute-force атак та блокування за допомогою PF.

5) Реалізацію надсилання автоматичних повідомлень адміністратору через корпоративний Jabber про події безпеки.

Результати дослідження показали, що розроблений захист ефективно працює в реальному часі та блокує спроби атак. Практична реалізація заходів захисту та автоматичного інформування адміністратора про інциденти забезпечує оперативну реакцію на потенційні загрози, що в свою чергу сприяє підвищенню рівня безпеки електронної пошти.

Отримані результати можуть бути корисні адміністраторам серверів електронної пошти для підвищення безпеки обміну електронними повідомленнями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Brute force attack [Електронний ресурс]. — URL: https://us.norton.com/blog/emerging-threats/brute-force-attack (дата звернення: 05.11.2023).

2. What is IMAP Server [Електронний ресурс]. — URL: https://www.systoolsgroup.com/imap/ (дата звернення: 05.11.2023).

3. Internet Message Access Protocol [Електронний ресурс]. — URL: https://www.networxsecurity.org/members-area/glossary/i/imap.html (дата звернення: 05.11.2023).

4. FreeBSD Documentation [Електронний ресурс]. — URL: https://docs.freebsd.org/en/ (дата звернення: 05.11.2023).

5. DOVECOT. The Secure IMAP server [Електронний ресурс]. — URL: https://www.dovecot.org/ (дата звернення: 05.11.2023).

6. Dovecot manual [Електронний ресурс]. — URL: https://doc.dovecot.org/ (дата звернення: 05.11.2023).

7. BACKBOX LINUX. Penetration Testing Distribution [Електронний ресурс]. — URL: https://linux.backbox.org/ (дата звернення: 05.11.2023).

8. HYDRA [Електронний ресурс]. — URL: https://github.com/vanhauser-thc/thc-hydra (дата звернення: 05.11.2023).

9. Pluggable Authentication Modules [Електронний ресурс]. — URL: https://docs.freebsd.org/en/articles/pam/ (дата звернення: 05.11.2023).

10. pam_passwdqc -- Password quality-control PAM module [Електронний ресурс]. — URL: https://man.freebsd.org/cgi/man.cgi?query=pam_passwdqc &sektion=8&format=html (дата звернення: 05.11.2023).

11. Bash Reference Manual [Електронний ресурс]. — URL: https://www.gnu.org/software/bash/manual/bash.html (дата звернення: 05.11.2023).

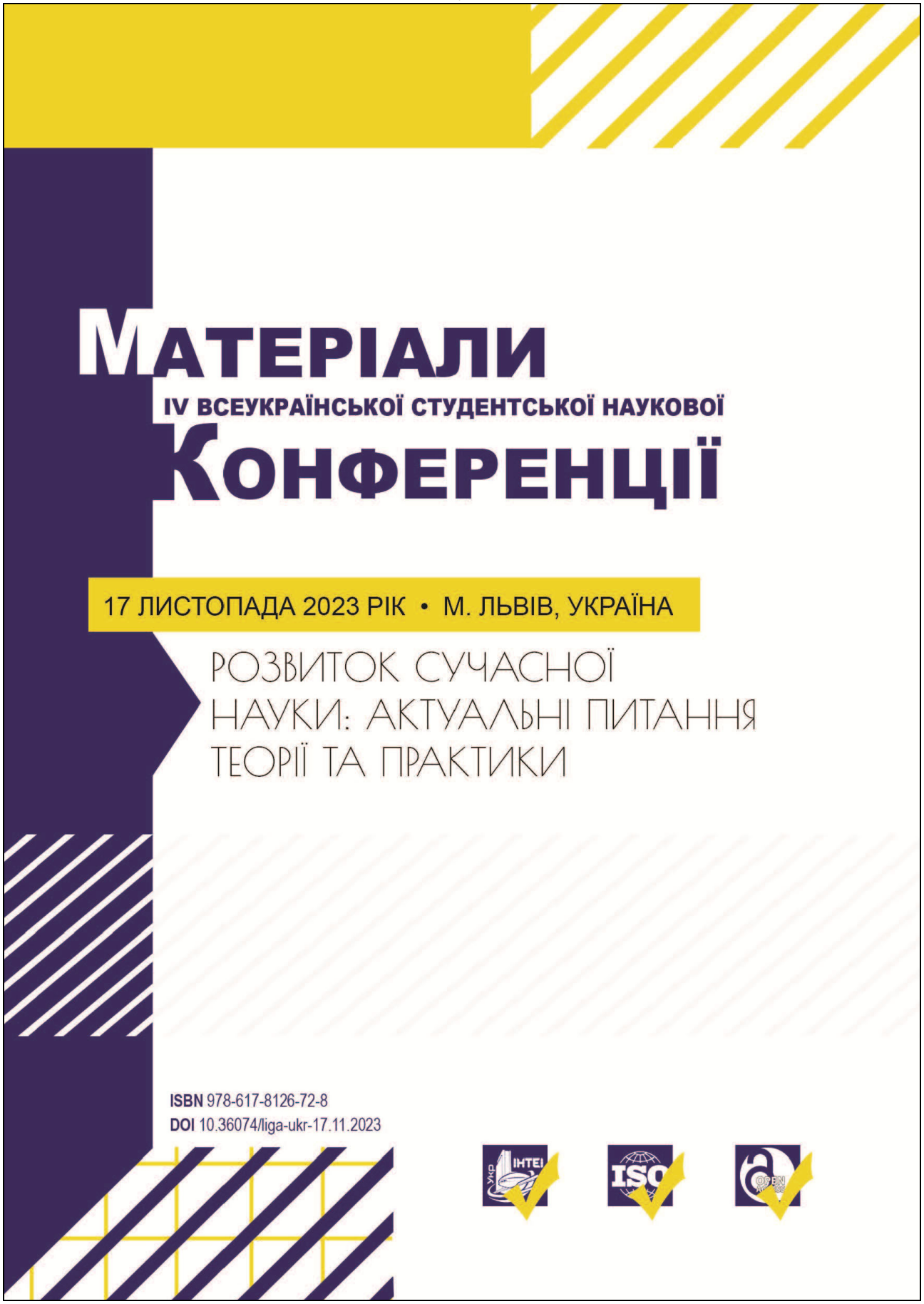
12. sendxmpp - Linux Manuals [Електронний ресурс]. — URL: https://www.systutorials.com/docs/linux/man/1-sendxmpp/ (дата звернення: 05.11.2023).

13. Основи охорони праці: навчальний посібник / М. П. Купчі та ін. Київ: Основа, 2000. 416 с.

14. В.В.Зацарний, Н.А.Праховнік, О.В.Землянська Безпека життєдіяльності: Конспект лекцій для студентів усіх спеціальностей за освітньокваліфікаційним рівнем «бакалавр» . Київ: НТУУ «КПІ», 2016. 92 с.

15. Техноекологія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник / В.С. Стручок, – Тернопіль: ТНТУ ім. І.Пулюя, 2022. – 150 с.

Додаток А – Публікація



Бекер Іван Миколайович, здобувач другого (магістерського) рівня вищої освіти факультету комп'ютерно-інформаційних систем і програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Тимощук Віталій Дмитрович, здобувач першого (бакалаврського) рівня вищої освіти факультету прикладних інформаційних технологій та електроінженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Маслянка Тарас Володимирович, здобувач першого (бакалаврського) рівня вищої освіти факультету комп'ютерно-інформаційних систем і програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Науковий керівник: Тимощук Дмитро Іванович, старший викладач кафедри кібербезпеки
Тернопільський національний технічний університет імені Івана Пулюя, Україна

МЕТОДИКА ЗАХИСТУ ВІД ПОВІЛЬНИХ ТА ШВИДКИХ BRUTE-FORCE АТАК НА IMAP СЕРВЕР

У сучасній епосі цифрових технологій безпека інформації стає ключовим завданням для захисту даних у всіх сферах, починаючи від особистих комунікацій і закінчуючи корпоративними та урядовими системами. Це набуває ще більшої вагомості через зростання кількості кіберзагроз, які ставлять під загрозу інформаційну безпеку та можуть мати серйозні наслідки для суспільства та бізнесу.

Одним з ключових елементів інформаційної інфраструктури компаній є сервери електронної пошти, що використовують IMAP протокол для доступу та управління електронною поштою [1]. Сервери часто стають об'єктом brute-force атак [2]. Такі атаки можуть бути повільними та відбуватись протягом тривалого часу для уникнення виявлення, або швидкими, що намагаються здобути несанкціонований доступ до системи за дуже короткий період.

Дослідження було спрямоване на розроблення комплексної методики захисту від обох типів brute-force атак. Було проаналізовано методику здійснення та поведінку таких атак, вивчались їх характеристики та шаблони, які в подальшому були використані для їх виявлення. За результатами дослідження було розроблено та застосовано політику паролів. Також був розроблений та впроваджений захисний механізм, що дозволяє блокувати швидкі атаки за допомогою брандмауера в операційній системі типу BSD [3].

Для протидії повільним атакам був розроблений програмний модуль, який аналізує журнали подій сервера для виявлення аномалій та характерних шаблонів цих атак. Даний модуль був інтегрований з брандмауером операційної системи для блокування зловмисників та системою сповіщень, що забезпечує автоматичне повідомлення адміністраторів через корпоративний месенджер. Такий підхід не тільки покращує реагування на інциденти, але й допомагає у формуванні даних для подальшого аналізу та удосконалення систем безпеки.

Результати дослідження підтверджують, що комбінований підхід, який об'єднує різні засоби та методи, значно підвищує захищеність IMAP серверів від відомих видів

brute-force атак. Такий підхід може стати важливою частиною комплексної стратегії захисту інформаційних систем від поширених загроз і виступити як ефективний засіб для забезпечення безпеки корпоративних поштових ресурсів. Ця методика може бути адаптована та використана адміністраторами серверів у різних організаціях для покращення рівня безпеки та стійкості перед сучасними кіберзагрозами.

Список використаних джерел:

1. Internet Message Access Protocol [Електронний ресурс]. — URL: https://www.networxsecurity.org/members-area/glossary/i/imap.html (дата звернення: 05.11.2023).
2. Brute force attack [Електронний ресурс]. — URL: https://us.norton.com/blog/emerging-threats/brute-force-attack (дата звернення: 05.11.2023).
3. FreeBSD Documentation [Електронний ресурс]. — URL: https://docs.freebsd.org/en/ (дата звернення: 05.11.2023).

Додаток Б – Лістинг файлу bruteforcealertimap.bash

```
#!/bin/bash

# Global variables
log_file="/var/log/dovecot.log"
subj="IMAP Server `date "+DATE: %Y-%m-%d TIME: %H:%M:%S"`"
declare -A ip_counts

# Function to get the current time
get_current_time() {
    current_time="`date "+%H:%M:%S"`"
    echo "$current_time"
}

# Function to get the time from 10 minutes ago
get_x_minutes_ago() {
    x_minutes_ago=$(date -v-10M "+%H:%M:%S")
    echo "$x_minutes_ago"
}

# Function to check if IP is already blocked
is_ip_blocked() {
    local ip=$1
    grep -q "$ip" /etc/bruteforceip
}

# Function to process each line of the log
process_log_line() {
    local line=$1
    local x_minutes_ago=$2

    words=($line)
    time=${words[2]}

    if [[ $line == *"auth failed"* && $time > $x_minutes_ago ]];
then
```

```
        for word in "${words[@]}"; do
            if [[ "$word" == rip=* ]]; then
                ip=${word#rip=}
                ip=${ip%,}

                if ! is_ip_blocked $ip; then
                    ((ip_counts["$ip"]++))
                fi
            fi
        done
    fi
}

# Function to handle IP blocking
handle_ip_blocking() {
    local ip=$1
    local count=$2

    if [ "$count" -ge 3 ]; then
        # Add IP to block file
        printf "$ip\n" >> /etc/bruteforceip

        # Add IP to PF block table
        pfctl -t slowbruteforceimap -T add $ip >>
/root/bruteforceimap/addtablebrute 2>&1
        printf "$subj\n"
        printf "Added IP to PF block table: $ip (count: $count)\n"
        echo "BRUTE FORCE Attack IMAP Alert: IP  -$ip; IP count -
$count"
        body="BRUTE FORCE Attack IMAP Alert: IP  -$ip; IP count -
$count"
        # Uncomment the line below to send an alert message
        echo "$body" | sendxmpp -d -s "$subj"
admin@xmpp.cstntu.local
    else
        printf "IP was not blocked: $ip (count: $count)\n"
    fi
```

```
}

# Main execution starts here
x_minutes_ago=$(get_x_minutes_ago)

while IFS= read -r line; do
    process_log_line "$line" "$x_minutes_ago"
done < "$log_file"

for ip in "${!ip_counts[@]}"; do
    handle_ip_blocking $ip "${ip_counts[$ip]}"
done
```

Додаток В – Файл налаштування сервісу bruteforce_monitor

```
#!/bin/sh

# PROVIDE: bruteforce_monitor
# REQUIRE: LOGIN
# KEYWORD: shutdown

. /etc/rc.subr

name="bruteforce_monitor"
rcvar=bruteforce_monitor_enable

extra_commands="status restart"

start_cmd="${name}_start"
stop_cmd="${name}_stop"
status_cmd="${name}_status"
restart_cmd="${name}_restart"


bruteforce_monitor_start()
{
    while :; do
     /usr/local/bin/bash
/root/bruteforceimap/bruteforcealertimap.bash     >>     /var/log/
bruteforce_monitor.log
     sleep 5
    done &
     echo $! > /var/run/${name}.pid
}

bruteforce_monitor_stop()
{
     kill `cat /var/run/${name}.pid`
        rm /var/run/${name}.pid
}
```

```
bruteforce_monitor_status()
{
    if [ -e "/var/run/${name}.pid" ]; then
     echo   "bruteforce_monitor   is   running   with   PID   `cat
/var/run/${name}.pid`."
    else
     echo "bruteforce_monitor is not running."
    fi
    exit 0
}


bruteforce_monitor_restart()
{
    bruteforce_monitor_stop
        sleep 2
    bruteforce_monitor_start
}


load_rc_config $name
: ${bruteforce_monitor_enable="NO"}
run_rc_command "$1"
```