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: "Синтез та валідація засобу інформування та мінімізації впливу SYN Flood атак на поштовий сервер"

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Демчук Василь Сергійович
підпис (прізвище та ініціали)

Керівник Лечаченко Т.А
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 Демчук Василь Сергійович
(прізвище, ім'я, по батькові)

1. Тема роботи Синтез та валідація засобу інформування та мінімізації впливу SYN Flood атак на поштовий сервер

Керівник роботи Лечаченко Тарас Анатолійович
доктор філософії, старший викладач 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 12.12.2023

3. Вихідні дані до роботи Вимоги до операційної системи FreeBSD, вимоги до системи захисту від SYN Flood атак.

4. Зміст роботи (перелік питань, які потрібно розробити)
Проаналізувати роботу SMTP сервіс та технологій захисту від syn flood атак.
Відтворити лабораторне середовища для моделювання syn flood атаки
Розробити засоби для мінімізації впливу syn flood атаки
Протестувати розроблений захист
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. Місце SMTP сервера в поштовій інфраструктурі. Огляд проблем безпеки сервісу SMTP. Опис SYN flood атаки. Методи здійснення атаки SYN Flood атаки. Технології захисту від атаки. Схема тестового стенду для моделювання атаки. Поштовий сервер. Налаштування SMTP сервера Postfix. Parrot Security у ролі засобу атаки. Здійснення SYN flood атаки на SMTP сервер. Результат SYN flood атаки на SMTP сервер. Технологія проксі як механізм пом'якшення атаки. Результат захисту механізму SYNPROXY після атаки SYN flood. Розрблення додаткового програмного модуля для виявлення та блокування SYN flood атаки. Модифікація налаштувань брандмауера PF. Реалізація програмного модуля. 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 – 21.09	Виконано
2.	Підбір джерел для аналізу захисту від SYN flood атак	22.09 – 30.09	Виконано
3.	Опрацювання джерел в галузі дослідження	30.10 – 10.10	Виконано
4.	Провести аналіз технологій захисту від SYN flood атак	10.10 – 20.10	Виконано
5.	Здійснення SYN flood атак на поштовий сервер	20.10-25.10	Виконано
6.	Налаштування технології пом’якшення атаки та розроблення програмного модуля	25.10 – 30.10	Виконано
7.	Оформлення розділу «Огляд SMTP сервісу та технологій захисту від SYN flood атак»	01.11– 10.11	Виконано
8.	Оформлення розділу «Створення лабораторного середовища для моделювання SYN flood атаки»	11.11 – 20.11	Виконано
9.	Оформлення розділу «Розробка засобів для мінімізації впливу SYN flood атаки»	21.11-30.11	Виконано
10.	Виконання завдання до підрозділу «Охорона праці та безпека в надзвичайних ситуаціях»	01.12 – 05.12	Виконано
11.	Оформлення кваліфікаційної роботи	06.12 – 08.12	Виконано
12.	Нормоконтроль	08.12 – 10.12	Виконано
13.	Перевірка на плагіат	13.12 – 13.12	Виконано
14.	Попередній захист кваліфікаційної роботи	25.12 – 25.12	Виконано
15.	Захист кваліфікаційної роботи	27.12.2023	

Студент _____ Демчук В.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Лечаченко Т.А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Синтез та валідація засобу інформування та мінімізації впливу SYN Flood атак на поштовий сервер // Кваліфікаційна робота ОР «Магістр» // Демчук Василь Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-62 // Тернопіль, 2023 // С. 68 , рис. – 24, табл. – - , кресл. – 22 , додат. – 2.

КЛЮЧОВІ СЛОВА: FREEBSD, SMTP, PF, SYN FLOOD, RUBY, POSTFIX, SIGNAL.

Актуальність захисту поштових серверів зростає з кожним днем, оскільки вони стають об'єктом спрямованих атак, зокрема SYN Flood, що загрожують їх доступності.

Магістерська робота спрямована на створення та перевірку ефективності інструменту мінімізації впливу SYN Flood атак на поштові сервери. Дослідження включає аналіз існуючих методів захисту, розробку та впровадження нової системи захисту на базі операційної системи FreeBSD та брандмауера PF, а також валідацію створеного рішення.

Комплексний засіб захисту автоматично реагує на SYN Flood атаки у режимі реального часу. Після успішного блокування здійснюється повідомлення в месенджер Signal про те, що виявлена за заблокована атака SYN flood.

Результати кваліфікаційної роботи можуть бути використані для поліпшення стійкості поштових серверів що до подібних атак.

ABSTRACT

Synthesis and Validation of a Means of Informing and Minimizing the Impact of SYN Flood Attacks on a Mail Server // Thesis of educational level "Master"// Demchuk Vasyl Serhiiovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБм-62 // Ternopil, 2023 // P. 68 fig. - 24, tab. - _-_, chair. - 22 , added. – 2.

Keywords: FREEBSD, SMTP, PF, SYN FLOOD, RUBY, POSTFIX, SIGNAL.

The importance of protecting mail servers is increasing every day, as they become the object of targeted attacks, including SYN Flood, which threaten their availability.

The Master's work is aimed at creating and testing the effectiveness of a tool for minimizing the impact of SYN Flood attacks on mail servers. The research includes analysis of existing protection methods, development and implementation of a new protection system based on the FreeBSD operating system and the PF firewall, as well as validation of the created solution.

Comprehensive protection automatically reacts to SYN Flood attacks in real time. After successful blocking, a message is sent to the Signal messenger that a blocked SYN flood attack has been detected.

The results of the qualification work can be used to improve the stability of mail servers against similar attacks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 8
ВСТУП 9
1 ОГЛЯД SMTP СЕРВІСУ ТА ТЕХНОЛОГІЙ ЗАХИСТУ ВІД SYN FLOOD АТАК 11
1.1 Місце SMTP сервера в поштовій інфраструктурі 11
1.2 Огляд проблем безпеки сервісу SMTP 13
1.3 Опис SYN flood атаки 15
1.4 Методи здійснення атаки 16
1.5 Технології захисту від атаки 19
2 СТВОРЕННЯ ЛАБОРАТОРНОГО СЕРЕДОВИЩА ДЛЯ МОДЕЛЮВАННЯ SYN FLOOD АТАКИ 25
2.1 Схема тестового стенду для моделювання атаки 25
2.2 Поштовий сервер 26
2.2.1 Налаштування операційної системи FreeBSD 27
2.2.2 Налаштування SMTP сервера Postfix 29
2.3 Parrot Security у ролі засобу атаки 31
2.4 Здійснення SYN flood атаки на SMTP сервер 33
3 РОЗРОБКА ЗАСОБІВ ДЛЯ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАКИ 39
3.1 Технологія проксі як механізм пом’якшення атаки 39
3.1.1 Брандмауер PF з механізмом SYNPROXY 39
3.1.2 Налаштування та тестування механізму SYNPROXY 40
3.2 Розробка додаткового механізму захисту 44
3.2.1 Механізм виявлення та блокування атаки 44
3.2.2 Модифікація налаштувань брандмауера PF 45
3.2.3 Реалізація програмного модуля 46
3.2.4 Налаштування та запуск сервісу моніторингу 47
3.2.5 Тестування розробленого захисту 48
4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ 51

4.1 Охорона праці 51
4.2 Забезпечення захисту працівників суб’єкта господарювання від іонізуючих випромінювань 53
ВИСНОВКИ 58
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 59
Додаток А Публікація 60
Додаток Б Лістинг файлу synflood_check.rb 62
Додаток В Файл сервісу synflood_check_service 66

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

SMTP	—	Simple Mail Transfer Protocol
SSL	—	Secure Sockets Layer
TLS	—	Transport Layer Security
RBL	—	Real-time Blackhole List
MITM	—	Man-in-the-Middle
POP3	—	Post Office Protocol version 3
DoS	—	Denial of Service
IMAP	—	Internet Message Access Protocol
TCP	—	Transmission Control Protocol
MSS	—	Maximum Segment Size
TCB	—	Transmission Control Block
BSD	—	Berkeley Software Distribution
CPU	—	Central Processing Unit
PF	—	Packet Filter

ВСТУП

Актуальність теми. Інформаційні технології відіграють ключову роль у різних аспектах нашого життя, забезпечення кібербезпеки стає надзвичайно важливим завданням. Зокрема, поштові сервери, які володіють великою кількістю конфіденційної інформації, стають об'єктом спеціально спрямованих атак, таких як SYN Flood, які можуть призвести до серйозних наслідків.

Актуальність обраної теми обумовлена необхідністю ефективного захисту поштових серверів від атак, спрямованих на виснаження їхніх ресурсів. SYN Flood атаки залишаються однією з потужних загроз, враховуючи їхню спроможність викликати відмову в обслуговуванні та негативний вплив на доступність інтернет-сервісів.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи є синтез та валідація засобу мінімізації впливу SYN Flood атак на поштовий сервер. Задачі дослідження включають аналіз існуючих методів захисту, розробку системи захисту на базі операційної системи FreeBSD та брандмауера PF, валідацію та дослідження ефективності розробленого рішення.

Об’єкт дослідження. Об'єктом дослідження є поштовий сервер, який є ключовим елементом інфраструктури для обміну електронною поштою та зберігання користувацьких даних.

Предмет дослідження. Предметом дослідження є створення та впровадження заходів захисту, а також оцінка їх ефективності в реальних умовах.

Наукова новизна одержаних результатів кваліфікаційної роботи. Науковою новизною є вдосконалення існуючих методів та розробка нового комплексного засобу захисту, який поєднує в собі ефективні технології та механізми реагування на SYN Flood атаки. Розроблений механізм захисту функціонує у режимі реального часу, автоматично блокуючи спроби атак та відправляючи повідомлення про їх виявлення.

Практичне значення одержаних результатів. Результати дослідження можуть бути використані адміністраторами систем безпеки для поліпшення стійкості поштових серверів до атак та підвищення рівня їхньої безпеки.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: IV Internatinal scientific and theoretical conference «Theory and practice of modern science» (Krakow, Republic of Poland), 24.11.2023.

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

1 ОГЛЯД SMTP СЕРВІСУ ТА ТЕХНОЛОГІЙ ЗАХИСТУ ВІД SYN FLOOD АТАК

1.1 Місце SMTP сервера в поштовій інфраструктурі

SMTP є стандартним протоколом, який використовується для надсилання та приймання електронної пошти в мережах [1]. Основна функція SMTP сервера полягає в обробці та відправці електронних листів до призначених отримувачів.

Основні ролі та місце SMTP сервера в поштовій інфраструктурі включають:

1) Надсилання та отримання листів. SMTP сервер використовується для прийому електронних листів від клієнтів (наприклад, від користувачів поштових програм), а потім відправляє ці листи до серверів призначення. Це може бути поштовий сервер отримувача або інший проміжний SMTP сервер. Також сервер може отримувати листи призначені для своїх користувачів, які були надіслані з інших SMTP серверів.

2) Резервний сервер. Це додатковий поштовий сервер, який призначений для забезпечення неперервної роботи електронної пошти в умовах можливих відмов чи відключень основного сервера. Він використовується як частина стратегії відновлення в разі аварійної ситуації з основним сервером.

Резервний SMTP сервер призначений для того, щоб у разі відмови або недоступності основного сервера продовжувати обробку та відправку електронних листів. Він готовий приймати та передавати повідомлення, якщо основний сервер виявиться недоступним. У багатьох випадках, резервний SMTP сервер має механізми автоматичного включення у дію в разі відмови основного сервера. Це може бути реалізовано через механізми перенаправлення трафіку на резервний сервер в разі виявлення проблем із основним. Метою резервного SMTP сервера є забезпечення неперервності роботи електронної пошти, щоб уникнути перерв у комунікаціях через можливі відмови, технічні проблеми або інші непередбачувані обставини.

3) Зберігання черги листів. Зберігання черги листів (mail queue) є важливою функцією поштових серверів, яка дозволяє тимчасово зберігати листи, які

очікують відправки або доставки, в разі тимчасових проблем з мережею, сервером або отримувачем. Коли поштовий сервер отримує лист для відправки, але не може надіслати його відразу (наприклад, через проблеми мережі або недоступність отримувача), він поміщає цей лист у чергу. Це дозволяє серверу зберегти лист тимчасово до моменту, коли він може бути відправлений.

Поштові сервери можуть мати механізми управління чергою, включаючи пріоритетність листів. Наприклад, важливі листи можуть мати вищий пріоритет для надання пріоритетного доступу до відправки. Якщо лист не може бути відправлений з першої спроби через проблеми з доставкою, поштовий сервер автоматично спробує відправити його пізніше. Це включає механізми повторної відправки через певні інтервали часу. Незважаючи на механізми зберігання черги листів, в окремих випадках листи можуть бути втрачені, особливо при тривалих проблемах з мережею або сервером.

Зберігання черги листів є важливою функцією для забезпечення надійності електронної пошти.

4) Забезпечення автентифікації та безпеки. SMTP сервери можуть також вимагати автентифікації для надання доступу до відправки листів, а також здійснювати заходи безпеки, такі як шифрування з'єднань (SSL/TLS) для захисту конфіденційності даних.

Аутентифікація - це процес перевірки ідентичності користувача перед наданням доступу до поштової скриньки. Вона може використовувати різні методи, такі як паролі, двофакторна аутентифікація, біометричні дані тощо.

Усі дані, які передаються між поштовими серверами та клієнтами, повинні бути зашифровані. TLS часто використовується для шифрування трафіку поштових протоколів, таких як SMTP, POP3, IMAP, що дозволяє захистити дані від несанкціонованого доступу під час передачі через мережу. Поштові сервери використовують антивірусні та антиспам фільтри для виявлення та блокування небажаної пошти та шкідливих вкладень, що допомагає захистити користувачів від шкідливих програм та шахрайства.

Отже, SMTP-сервер відіграє ключову роль у відправці електронної пошти, забезпечуючи її надійну передачу від відправника до отримувача в рамках поштової інфраструктури.

1.2 Огляд проблем безпеки сервісу SMTP

Сервіс SMTP може мати декілька проблем безпеки, які потребують уваги для забезпечення безпеки електронної пошти.

Ось деякі з них:

1) Ретрансляція спаму (open relay).

Сервери, які відкриті та доступні для надсилання листів всім без винятку (open relays) дозволяють невідомим користувачам використовувати SMTP сервер для відправки спаму. Це може призвести до блокування IP-адрес сервера через спам-фільтри.

Open relay є проблемою безпеки, оскільки відкритий доступ до сервера SMTP може призвести до:

- Спаму. Зловмисники можуть використовувати open relay для масової відправки небажаної пошти до великої кількості адрес електронної пошти.
- Поширення шкідливих вкладень. Крім відправки спаму, open relay може бути використаний для поширення шкідливих вкладень.
- Блокування сервера: Якщо сервер стає джерелом значної кількості спаму, його IP адреса може потрапити в чорний список різних сервісів, що призведе до неможливості або ускладнення доставки легітимної електронної пошти. RBL - це механізм, що використовується для ідентифікації потенційно небажаних або шкідливих IP адрес або доменів, які відправляють спам, містять віруси або представляють загрозу для безпеки мережі. Ці чорні списки підтримуються або керуються різними організаціями чи спільнотами, які визначають IP адреси або домени, які вони вважають небажаними чи шкідливими. Інші поштові сервери та системи безпеки можуть використовувати ці списки для блокування або маркування вхідних листів, що походять від цих небажаних джерел.

Для запобігання проблемам open relay, адміністраторам поштових серверів зазвичай достатньо здійснити коректне налаштування сервера. Налаштувати SMTP сервера для вимоги аутентифікації перед тим, як дозволити відправку повідомлень через нього. Обмежити доступу до сервера без потреби аутентифікації тільки для внутрішніх користувачів або для тих, хто має відповідний доступ.

Ці заходи допомагають запобігти використанню сервера SMTP для надсилання небажаної пошти та забезпечити більшу безпеку поштових систем.

2) Вразливості програмного забезпечення.

В деяких випадках, програмне забезпечення SMTP сервера може мати вразливості, які можуть бути використані для виконання зловмисного коду або витоку конфіденційної інформації. Щоб уникнути цих вразливостей, важливо регулярно оновлювати програмне забезпечення, слідкувати за оновленнями безпеки а також проводити аудит безпеки для виявлення та виправлення потенційних проблем.

3) Нешифрований трафік.

Нешифрований трафік SMTP може стати потенційною загрозою для безпеки, оскільки дані, що передаються через незахищені канали, можуть бути перехоплені зловмисниками.

Основні ризики, пов'язані з нешифрованим трафіком SMTP, включають:

– Перехоплення конфіденційної інформації. Якщо трафік SMTP не зашифрований, логіни, паролі, а також вміст електронних листів можуть бути легко перехоплені.

– Можливість маніпуляції даними: Незахищений трафік може бути вразливим до атак MITM, де зловмисники можуть змінювати вміст листів або навіть відправляти фальшиві листи від імені користувачів.

– Витік конфіденційної інформації: Якщо в незахищеному трафіку міститься конфіденційна інформація, така як паролі або особисті дані, це може призвести до їх витоку та небезпеки для конфіденційності.

Для захисту від цих загроз рекомендується встановлення захищеного TLS з'єднання для шифрування трафіку між поштовими серверами. Це дозволить

захистити дані, що передаються, від перехоплення та зміни. Налаштування поштового сервера для вимоги шифрованого зв'язку з клієнтами, що зменшить ризик передачі незахищених даних.

Використання шифрування для трафіку SMTP важливо для забезпечення конфіденційності даних у електронній пошті.

4) Атаки на доступність (DoS). Сервіс SMTP може бути підданий DoS атакам, коли атакуючі намагаються перевантажити сервер запитами, що призводить до відмови в обслуговуванні для легітимних користувачів. Атака SYN Flood є однією з найпоширеніших форм атак на доступність (DoS), спрямованих на SMTP сервер і не тільки [2].

1.3 Опис SYN flood атаки

SYN Flood атака є формою атаки на протокол TCP, спрямованою на переповнення та виснаження ресурсів цільового сервера. Перед початком комунікації пристрої, що взаємодіють через TCP, виконують процедуру three way TCP handshake. Клієнт надсилає пакет SYN (синхронізації) серверу, сервер відповідає пакетом SYN-ACK (синхронізації-підтвердження), а клієнт завершує процес, надсилаючи пакет ACK (підтвердження). Після цього відбувається встановлення з'єднання (Рисунок 1.1).

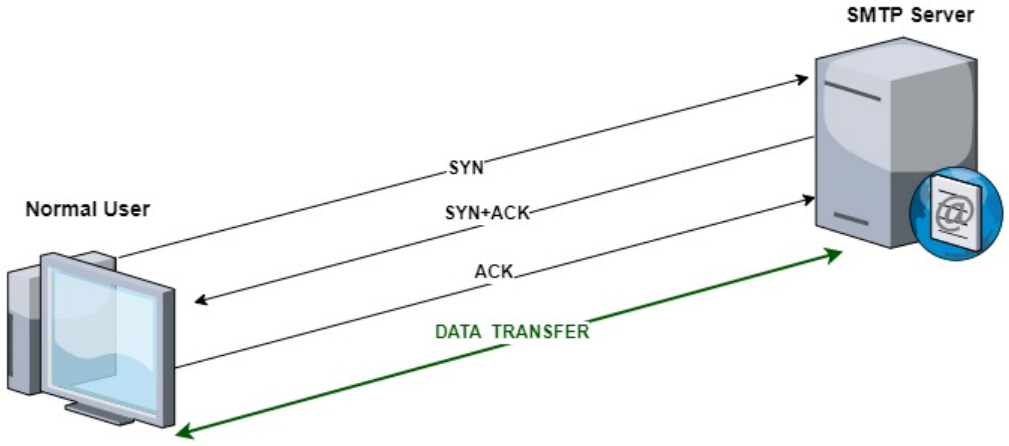


Рисунок 1.1 – Етапи взаємодії при three way TCP handshake

Цей тип атаки використовує недолік у процесі встановлення з'єднання між клієнтом і сервером за допомогою SYN, SYN-ACK, ACK. Зловмисник надсилає

велику кількість підроблених SYN-пакетів пробуючи переповнити буфер пам'яті на сервері та викликати відмову в обслуговуванні (DoS). Основна ідея полягає в тому, що зловмисник починає процес з'єднання, але не завершує його, залишаючи сервер чекати на відповідь і витрачати ресурси [2].

Сервер отримує велику кількість запитів на встановлення з'єднання, але через те, що вони не завершуються (не відбувається фактичний обмін даними), це спричиняє виснаження ресурсів сервера та призводить до затримок чи відмови в обслуговуванні для легітимних запитань.

1.4 Методи здійснення атаки

SYN Flood атака, як одна з найбільш ефективних атак на мережевий протокол TCP, використовує різноманітні методи для перевантаження ресурсів сервера.

Основні методи, які зловмисники використовують для здійснення SYN Flood атак:

1) Відправка фальшивих запитів SYN за допомогою ботнет мережі.

Один із найбільш ефективних методів здійснення SYN Flood атаки включає використання ботнет мережі. Цей підхід дозволяє зловмисникам координувати і синхронізувати великий обсяг фальшивих запитів SYN від різних джерел, зменшуючи ймовірність виявлення та підвищуючи ефективність атаки.

Зловмисники формують ботнет, що складається з великої кількості комп'ютерів. Ці комп'ютери можуть бути розташовані в різних географічних місцях та мати різні IP-адреси, що ускладнює виявлення окремого джерела атаки [3]. Зловмисники активують механізм відправки фальшивих запитів SYN. Ця відправка здійснюється синхронізовано з багатьох джерел, спрямовуючи велику кількість запитів на один або кілька цільових серверів (Рисунок 1.2).

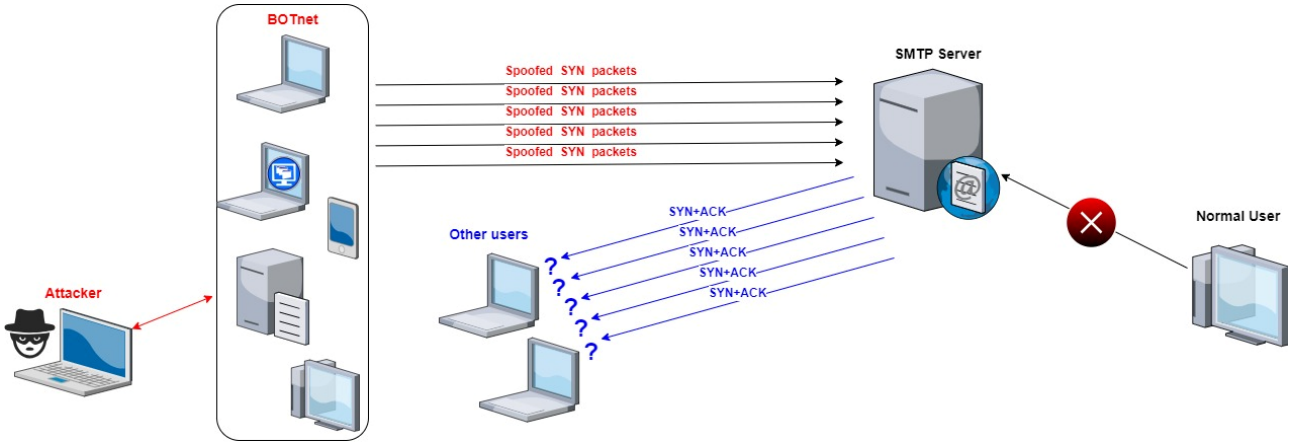


Рисунок 1.2 – Схема здійснення SYN flood атаки

Використання розподіленої мережі комп'ютерів у ботнеті дозволяє зловмисникам уникнути блокування IP-адрес, оскільки атака здійснюється з різних джерел. Це ускладнює завчасне виявлення та блокування атаки.

За допомогою ботнет мережі, зловмисники можуть динамічно збільшувати обсяг атаки, мобілізуючи більше ресурсів і збільшуючи потужність атаки, коли це необхідно.

Керівництво ботнетом може включати інтелектуальні алгоритми, які аналізують ефективність атаки та можливості виявлення, дозволяючи адаптувати стратегію атаки для максимальної ефективності.

Використання ботнет мережі для відправки фальшивих запитів SYN виконується з ефективною координацією дій, що робить цей метод одним із основних для здійснення складних та потужних SYN Flood атак.

2) Використання збільшеної швидкості відправки запитів.

Збільшена швидкість відправки запитів SYN є одним із ефективних методів здійснення SYN Flood атак. Зловмисники активно використовують цей підхід для спричинення перевантаження сервера шляхом швидкого та постійного відправлення великої кількості фальшивих запитів SYN.

У цьому методі атаки використовуються спеціально налаштовані інструменти для штучного збільшення частоти відправки пакетів SYN. Це може бути досягнуто зміною параметрів відправки, таких як час затримки між пакетами, або використання потужних ресурсів для автоматичної генерації та відправки пакетів. Зловмисники можуть створювати пакети так, щоб вони

виглядали, як реальний мережевий трафік. Це дозволяє їм уникати виявлення за допомогою систем виявлення вторгнень, які можуть аналізувати аномалії у структурі пакетів.

Використання оптимізованих та швидких алгоритмів генерації пакетів дозволяє зловмисникам ефективно та миттєво створювати та відправляти велику кількість запитів SYN, збільшуючи обсяг атаки.

Зловмисники можуть регулювати швидкість відправки запитів, збільшуючи або зменшуючи її в ході атаки. Це може бути використано для уникнення виявлення та адаптації до захисту.

Використання збільшеної швидкості відправки запитів SYN є ефективним методом для створення великого обсягу трафіку та спричинення відмови в обслуговуванні, призводячи до виснаження ресурсів сервера та зниження його пропускної здатності.

3) Зміна IP-адреси відправника (IP address spoofing).

Зміна IP-адреси відправника, відома як IP address spoofing, є ефективним методом, шо погіршує можливості виявлення та блокування SYN Flood атак (Рисунок 1.2). Зловмисники використовують цей підхід щоб запобігти розпізнаванню атаки.

Зловмисники можуть використовувати спеціалізовані інструменти для IP spoofing, які автоматично маніпулюють IP-адресами в пакетах, відправлених під час атаки. Ці інструменти можуть бути легко налаштовані для зміни адрес при кожному відправленні пакету, ускладнюючи виявлення.

Зміна IP-адреси відправника це також спроба уникнути виявлення за допомогою систем виявлення вторгнень, які можуть спостерігати за звичайними IP-адресами та виявляти аномалії. Зміна IP-адреси відправника ускладнює завчасне виявлення та реагування на атаку.

Зміна IP-адреси відправника є важливим елементом для здійснення успішних SYN Flood атак, оскільки вона створює додатковий шар анонімності та унеможливлює виявлення зловмисників.

Ці методи підкреслюють хитрість та гнучкість SYN Flood атак, роблячи їх важкими для виявлення та запобігання. У подальших розділах дослідження буде розглянуто розробку та валідацію захисту від таких атак.

1.5 Технології захисту від атаки

Існує кілька технологій та підходів, які використовуються для захисту від атак SYN Flood та пом'якшення їх впливу на поштовий сервер [2]:

1) SYN Cookies.

Ця техніка дозволяє серверам залишатися доступними для легітимних клієнтів, ігноруючи непідтверджені SYN-запити генеруючи унікальні хеш-ключі на основі інформації в SYN-пакеті, такі як IP-адреса та порт. Замість того, щоб зберігати об'ємні таблиці з'єднань, сервер використовує ці хеш-ключі для генерації тимчасових SYN Cookies, які включають інформацію, необхідну для підтвердження з'єднання.

Якщо клієнт із правильно згенерованим SYN Cookie надсилає свій наступний пакет, сервер може використати інформацію з цього SYN Cookie для відновлення стану з'єднання, замість зберігання контексту з'єднання. SYN Cookies дозволяють серверам витримувати атаки SYN Flood, зберігаючи їх доступними для легітимних користувачів, тим самим сприяючи збереженню доступності мережевих ресурсів.

Але SYN Cookies має певну кількість недоліків, на які потрібно звернути увагу. Використання SYN Cookies може вплинути на деякі параметри TCP-з’єднань, оскільки інформація з початкового SYN-запиту не зберігається в традиційний спосіб. Це може призвести до деякої обмеженості функціональності, так як певні параметри, такі як масштаб вікна, мітки часу (timestamps) або точний розмір MSS, можуть бути втрачені або недоступні для з'єднання.

Одним з наслідків застосування SYN Cookies є те, що обробка SYN-запитів та встановлення з'єднання відбувається на вищому рівні абстракції без

збереження повної інформації про з'єднання, що може призвести до обмеження доступних параметрів TCP.

Оскільки ACK, що повертається, встановлює з’єднання, зловмисник може надіслати на сервер велику кількість ACK пакетів, намагаючись створити з’єднання. Якщо брандмауери фільтрують вхідні сегменти з установленим бітом SYN, атаки, спрямовані на створення з'єднання за допомогою ACK, можуть бути одним із способів обхідної атаки.

2) Збільшення резервів системи.

Збільшення резерву (backlog) відноситься до спроби підвищити параметр backlog в TCP як потенційного заходу захисту від атак, таких як SYN Flood. Параметр backlog визначає максимальну довжину черги з'єднань, які очікують на прийняття сервером.

Ідея збільшення backlog полягає в тому щоб дозволити серверу обробляти більше вхідних запитів на з'єднання, припускаючи, що це може допомогти поглинути або пом'якшити вплив потоку запитів SYN. Однак цей підхід може мати обмеження та недоліки.

Однією з можливих проблем цієї стратегії є те, що значне збільшення backlog може споживати більше системних ресурсів, зокрема пам'яті, що може вплинути на загальну продуктивність системи. Крім того, це може не бути дуже ефективним рішенням проти масштабних атак, оскільки воно не запобігає перевантаженню сервера від початкових запитів SYN.

Важливо зазначити, що атаки SYN Flood зазвичай переповнюють сервер великою кількістю запитів SYN, не завершуючи повного TCP-рукостискання, що призводить до вичерпання ресурсів через велику кількість напіввідкритих з'єднань. Збільшення backlog може забезпечити обмежену буферизацію, але це може не бути повноцінним рішенням для пом'якшення всієї атаки.

У кінцевому підсумку, хоча збільшення backlog може потенційно мати певні переваги, це може бути недостатнім як самостійний механізм захисту від складних чи великомасштабних атак SYN Flood.

3) Зменшення таймера.

Зменшення таймера "SYN-RECEIVED" полягає в зміні часу, протягом якого система утримує з'єднання в стані "SYN-RECEIVED" під час взаємодії за протоколом TCP.

Стан "SYN-RECEIVED" виникає, коли сервер отримує пакет SYN від клієнта для встановлення TCP-з'єднання. Зменшення таймера, пов'язаного з цим станом, означає зменшення тривалості часу, протягом якого сервер очікує завершення three way TCP handshake.

Зменшення таймера "SYN-RECEIVED" може розглядатися як спроба обмежити час, протягом якого сервер очікує завершення процесу TCP-рукостискання, перш ніж перенести з'єднання в інший стан або припинити його, якщо TCP-рукостискання не завершиться протягом встановленого проміжку часу. Це може допомогти звільнити ресурси та зменшити вплив потенційної атаки типу SYN Flood шляхом швидкого відкидання неповних з'єднань.

Проте ця стратегія може мати як позитивні, так і негативні аспекти. Хоча вона потенційно може допомогти у зменшенні наслідків атак типу SYN Flood шляхом швидкого припинення неповних з'єднань, вона також може збільшити ймовірність передчасного завершення легітимних з'єднань, які займають більше часу, ніж налаштований таймер для завершення рукостискання.

Необхідно обережно налаштовувати та оптимізувати таймер "SYN-RECEIVED", щоб він забезпечував баланс між ефективною протидією потенційним атакам та збереженням функціональності легітимних з'єднань.

Налаштування параметрів TCP, таких як таймер "SYN-RECEIVED", часто потребує конфігурації на рівні системи та потребує обережного підходу, оскільки неправильні налаштування можуть негативно вплинути на продуктивність або стабільність системи.

3) Видалення найстарішого напіввідкритого TCB [4].

Видалення найстарішого напіввідкритого TCB означає операцію у TCP, де найстаріше напіввідкритий блок управління з'єднанням (TCB) забирається для відновлення пам'яті або ресурсів.

Коли атака типу SYN Flood створює багато напіввідкритих з'єднань, вони можуть споживати пам'ять та ресурси сервера. Щоб захиститися, деякі системи

можуть використовувати стратегію видалення напіввідкритих TCB. Ця стратегія полягає у видаленні або переробці (закритті) найстаріших напіввідкритих з'єднань у TCB, які не були завершені після певного періоду часу.

Однак потрібно зауважити, що використання цієї стратегії може мати певні обмеження. Наприклад, видалення найстаріших напіввідкритих з'єднань може призвести до припинення легітимних з'єднань, які довго утримуються в стані SYN-RECEIVED, що може негативно вплинути на роботу системи та послуг для легітимних користувачів.

Важливо налаштовувати ці параметри обережно, з урахуванням специфіки мережевого навантаження та потреб користувачів, для забезпечення балансу між ефективністю захисту від атак і надійною роботою системи.

4) SYN Cache.

SYN Cache є механізмом захисту від атак типу SYN Flood у TCP/IP-протоколі. Він використовується для тимчасового зберігання інформації про напіввідкриті з'єднання TCB, які ще не завершили процедуру three way TCP handshake.

SYN Cache зберігає інформацію про напіввідкриті з'єднання на відміну від того, щоб негайно включити їх у активний стан обробки з'єднань (SYN-RECEIVED). Це дозволяє серверу зберігати певну кількість напіввідкритих з'єднань в кеші, перш ніж додати їх до активних оброблювачів з'єднань.

Основна перевага SYN Cache полягає в тому, що він дозволяє серверу ефективно керувати тимчасовим зберіганням напіввідкритих з'єднань, не навантажуючи ресурси сервера. Це дозволяє впоратися зі значним обсягом SYN-пакетів під час атаки, відділивши потенційно небезпечні напіввідкриті з'єднання від основного потоку обробки з'єднань.

Проте важливо пам'ятати, що параметри та ефективність SYN Cache можуть відрізнятися в залежності від конфігурації сервера та властивостей мережі. Налаштування SYN Cache потребує уважного аналізу та належного узгодження для забезпечення оптимального захисту проти атак SYN Flood.

В разі масштабних атак, коли SYN Cache переповнюється, може виникнути значне навантаження на обробники з'єднань при спробі управління великою кількістю напіввідкритих з'єднань.

5) Брандмауери та проксі сервера.

Брандмауери та проксі можуть бути використані для захисту від атак типу SYN flood, однак це супроводжується певними важливими моментами та можливими наслідками.

У цьому контексті одним із підходів є використання стратегій на основі брандмауерів для захисту кінцевих вузлів від атак SYN flood. Основна ідея полягає в тому, щоб перекласти на брандмауер або проксі відповідальність за процедури встановлення з'єднання, які вони контролюють до того моменту, поки вони успішно завершуються. Після цього ці з'єднання повертаються або перенаправляються до захищених кінцевих вузлів.

За допомогою цього підходу відбувається перенесення відповідальності за процес встановлення з'єднання від кінцевих вузлів до брандмауера чи проксі. Однак цей підхід може викликати проблеми, пов'язані зі зміною очікуваних кінцевих семантик TCP, що може вплинути на надійність та очікувану поведінку TCP-з'єднань.

Зазвичай брандмауери та проксі використовують техніки, подібні до тих, що використовуються кінцевими вузлами для протидії атакам SYN flood. Вони відстежують вхідні SYN-пакети, які надсилаються клієнту та серверу на різних етапах TCP-рукостискання. Цей процес дозволяє брандмауеру або проксі перевіряти та відсіювати вхідні з'єднання без їх повного встановлення, допомагаючи зменшити вплив атак типу SYN flood на кінцеві вузли.

Хоча такі тактики можуть розподіляти навантаження обробки вхідних з'єднань та захищати кінцеві вузли від атак SYN flood, вони можуть внести складнощі у керування TCP-з'єднаннями та змінити стандартну поведінку, очікувану від кінцевих комунікацій. Обережне налаштування необхідне для забезпечення ефективної протидії атакам SYN flood за допомогою брандмауера чи проксі, без негативного впливу на загальну продуктивність мережі чи виникнення неочікуваних проблем з підключенням TCP.

Брандмауер PF в FreeBSD може бути потужним інструментом для виявлення та захисту від SYN flood атак.

В загальному всі ці технології можуть використовуватися окремо або в комбінації для забезпечення більш ефективного захисту проти атак SYN flood та підвищення доступності та безпеки поштового сервера.

2 СТВОРЕННЯ ЛАБОРАТОРНОГО СЕРЕДОВИЩА ДЛЯ МОДЕЛЮВАННЯ SYN FLOOD АТАКИ.

2.1 Схема тестового стенду для моделювання атаки

Для моделювання SYN Flood атаки буде використано тестове середовище, схема якого представлена на рисунку 2.1.

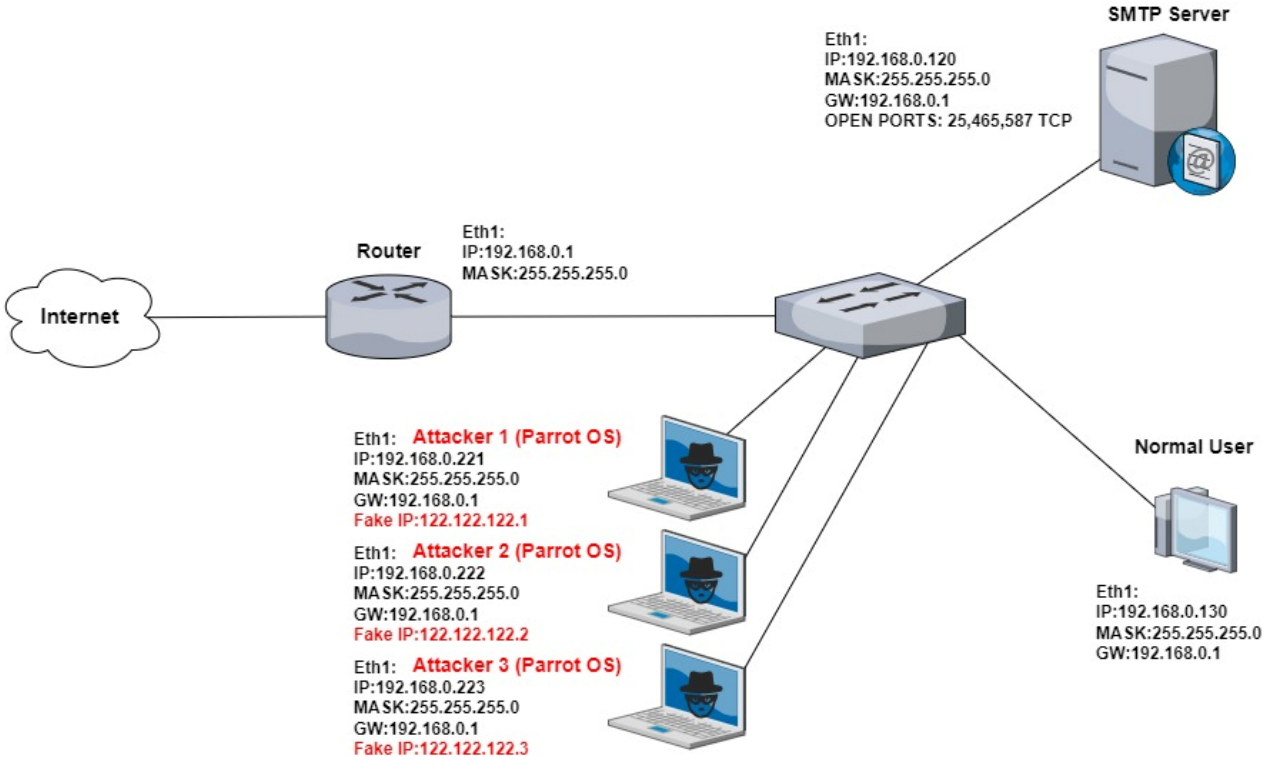


Рисунок 2.1 – Схема мережі для моделювання SYN flood атаки

Схема мережі призначена для моделювання SYN flood атаки. SYN flood атака є типом атаки DoS, в ході якої атакуючий надсилає безперервний потік SYN запитів до цілі, з метою вичерпати ресурси сервера до рівня, при якому система стає нечутливою до легітимного трафіку.

Опис налаштування мережі згідно схеми наступний:

1) Маршрутизатор (Router). Має два з’єднання. Перше використовується для підключення до мережі Інтернет. Друге (Eth1) з IP-адресою 192.168.0.1 та маскою підмережі 255.255.255.0 для підключення до локальної мережі.

2) Атакуючі хости (Attacker 1, Attacker 2 та Attacker 3). Працюють на операційній системі Parrot OS, налаштовані з IP-адресами 192.168.0.221, 192.168.0.222 та 192.168.0.223, маскою підмережі 255.255.255.0 та шлюзом за замовчуванням 192.168.0.1. Дані хости використовують фальшиві IP-адреси 122.122.122.1, 122.122.122.2 та 122.122.122.3 відповідно.

3) Звичайний користувач (Normal user). Операційна система Oracle Linux з IP-адресою 192.168.0.130, маскою підмережі 255.255.255.0 та шлюзом 192.168.0.1. Дана операційна система буде використовуватись для перевірки доступності SMTP сервісу під час здійснення атаки.

4) SMTP сервер: У правому верхньому кутку зображено SMTP сервер з IP-адресою 192.168.0.120, маскою підмережі 255.255.255.0, а також переліком відкритих портів 25, 465, 587 TCP, які є типовими для SMTP сервісів. Це є цільовим сервером для SYN flood атаки.

Налаштування виконано так, що атакуючі хости знаходяться в одній локальній мережі з SMTP сервером і звичайним користувачем. Для моделювання атаки це є оптимальна схема, яка не вимагає ускладнених налаштувань та засобів реалізації. Використання фальшивих IP адрес дає можливість атакуючим хостам маскувати свої IP адреси для уникнення виявлення і також це створює враження, що потік запитів надходить з інших джерел.

Ця конфігурація мережі сприятиме набуттю практичних навичок у виявленні, захисті та реагуванні на атаки типу SYN Flood в умовах лабораторного середовища.

2.2 Поштовий сервер

Поштовий сервер на базі операційної системи FreeBSD та Postfix - це комплексне рішення, призначене для обробки, надсилання та отримання електронних листів у мережі. FreeBSD виступає як операційна система, а Postfix - як поштовий сервер, що забезпечує обробку пошти в мережі з високою продуктивністю, безпекою та надійністю.

2.2.1 Налаштування операційної системи FreeBSD

FreeBSD - це відкрита операційна система на базі UNIX, яка володіє високою стабільністю, надійністю та безпекою [5]. Вона розробляється та підтримується волонтерами і компаніями з усього світу. FreeBSD є одним з різновидів системи BSD, яка включає в себе розширені функції, оптимізовані для роботи на серверах та інших пристроях.

Операційна система FreeBSD відома своєю ефективністю та стабільністю у роботі з мережевими пристроями, серверами та вебхостингом. Вона має високу швидкодію, включає в себе багато можливостей, таких як підтримку мережевих протоколів, а також широкий спектр програмного забезпечення, яке може бути легко встановлене за допомогою системи керування пакунками.

Завдяки своїй безпеці та високій продуктивності, FreeBSD часто використовується як операційна система для серверів, маршрутизаторів, брандмауерів та інших мережевих пристроїв. Вона надійно працює як у великих підприємствах, так і в особистих системах, де вимагається надійність та висока ефективність операційної системи.

Файл rc.conf в операційній системі FreeBSD - це текстовий файл, який містить налаштування та параметри запуску системи, служб і різноманітних компонентів операційної системи. Він знаходиться у каталозі /etc і відповідає за встановлення значень змінних середовища, активацію служб і додаткові конфігураційні налаштування.

На рисунку 2.2 наведено вміст файлу налаштувань rc.conf для операційної системи FreeBSD.

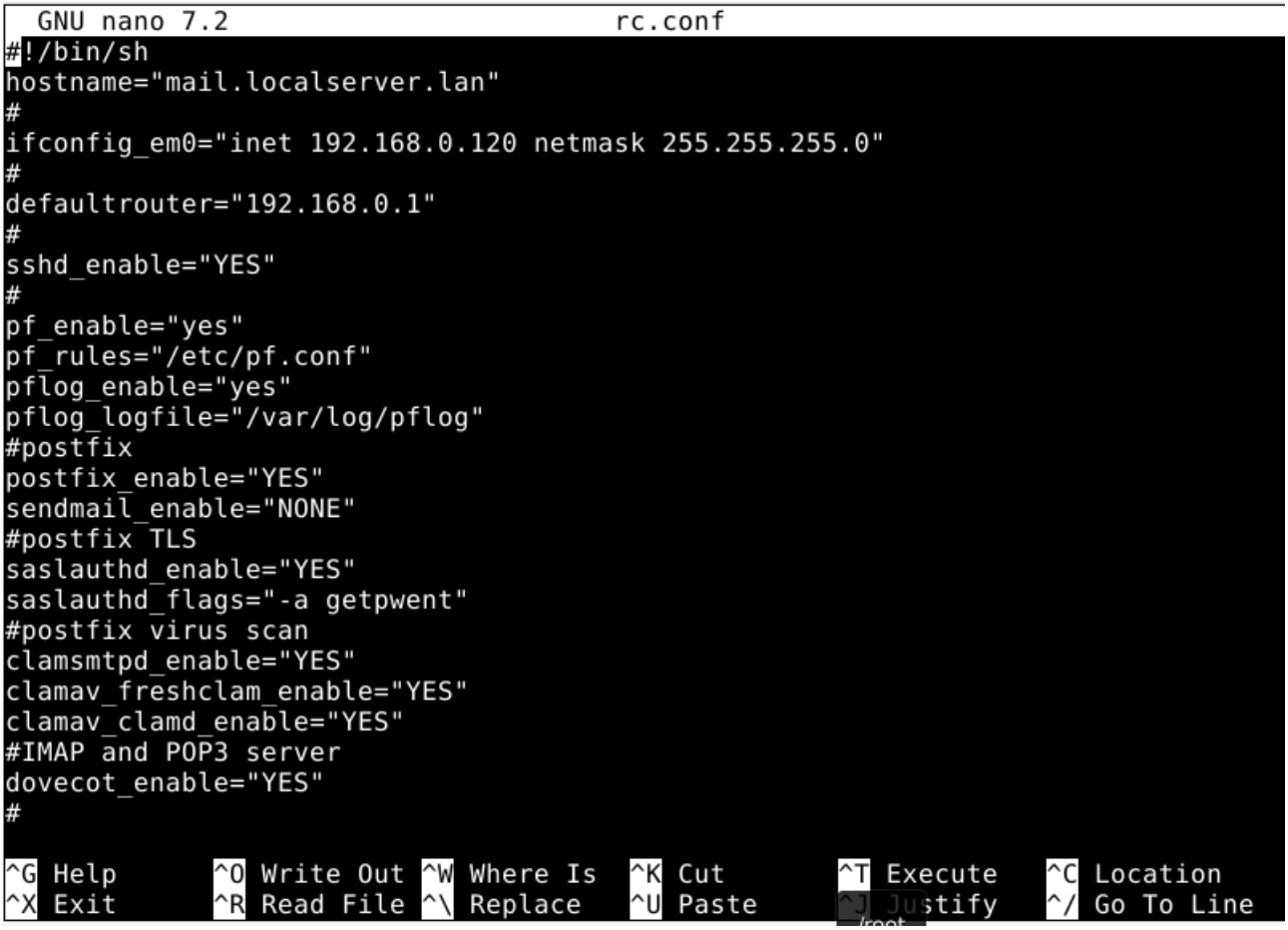


Рисунок 2.2 – Вміст конфігураційного файлу rc.conf

Короткий опис конфігураційних параметрів файлу rc.conf:

1) `hostname="mail.localserver.lan"`. Встановлює ім'я хоста системи.

2) `ifconfig_em0="inet 192.168.0.120 netmask 255.255.255.0"`. Налаштовує мережевий інтерфейс em0 з IP-адресою 192.168.0.120 та мережевою маскою 255.255.255.0.

3) `defaultrouter="192.168.0.1"`. Вказує IP-адресу шлюзу за замовчуванням.

4) `sshd_enable="YES"`. Активує службу SSH для віддаленого з'єднання з системою за допомогою SSH-клієнта.

5) `pf_enable="yes"`. Увімкнення служби брандмауера PF.

6) `pf_rules="/etc/pf.conf"`. Вказує шлях до файлу з правилами брандмауера PF.

7) `pflog_enable="yes"`. Увімкнення логування пакетів брандмауера PF.

8) `pflog_logfile="/var/log/pflog"`. Вказує шлях до файлу журналу логування пакетів брандмауера PF.

9) `postfix_enable="YES"`. Активує службу поштового сервера Postfix.

10) `sendmail_enable="NONE"`. Відключає стандартний поштовий сервер Sendmail.

11) `saslauthd_enable="YES"`. Активує службу аутентифікації SASL.

12) `clamsmtpd_enable="YES"`. Активує службу антивірусного проксі-сервера ClamSMTP.

13) `clamav_clamd_enable="YES"`. Активує службу демона антивірусного сканування ClamAV.

14) `dovecot_enable="YES"`. Активує службу IMAP nta POP3 сервера Dovecot.

Цей файл містить налаштування різних служб та компонентів системи, що дозволяє системі працювати як поштовий сервер.

2.2.2 Налаштування SMTP сервера Postfix

Налаштування SMTP сервера Postfix включає ряд параметрів та конфігураційних файлів для забезпечення коректної роботи сервера [6]. Основні файли конфігурації Postfix зазвичай знаходяться в каталозі /etc/postfix/.

Деякі основні файли налаштування:

1) Файл main.cf - це головний файл конфігурації, де встановлюються основні параметри і налаштування SMTP сервера. В цьому файлі містяться різні параметри, які визначають поведінку сервера, його обмеження, зовнішні та внутрішні налаштування.

Налаштування залежать від конкретних потреб і вимог сервера електронної пошти. Для моделювання SYN flood атаки даний файл не потребує додаткових специфічних налаштувань.

2) Файл master.cf в поштовому сервері Postfix містить конфігураційні дані для керування різними процесами та службами, що виконуються на сервері. Цей файл дозволяє налаштовувати параметри роботи окремих компонентів Postfix, таких як SMTP сервер, фільтри повідомлень, TLS налаштування та інші опції.

Кожен рядок у файлі master.cf містить конфігурацію окремого сервісу або процесу, які відповідають за різні аспекти роботи Postfix.

Редагування файлу master.cf потребує обережності, оскільки невірна конфігурація може призвести до неправильної роботи сервера електронної пошти.

На рисунку 2.3 показано підтвердження коректного запуску Postfix.

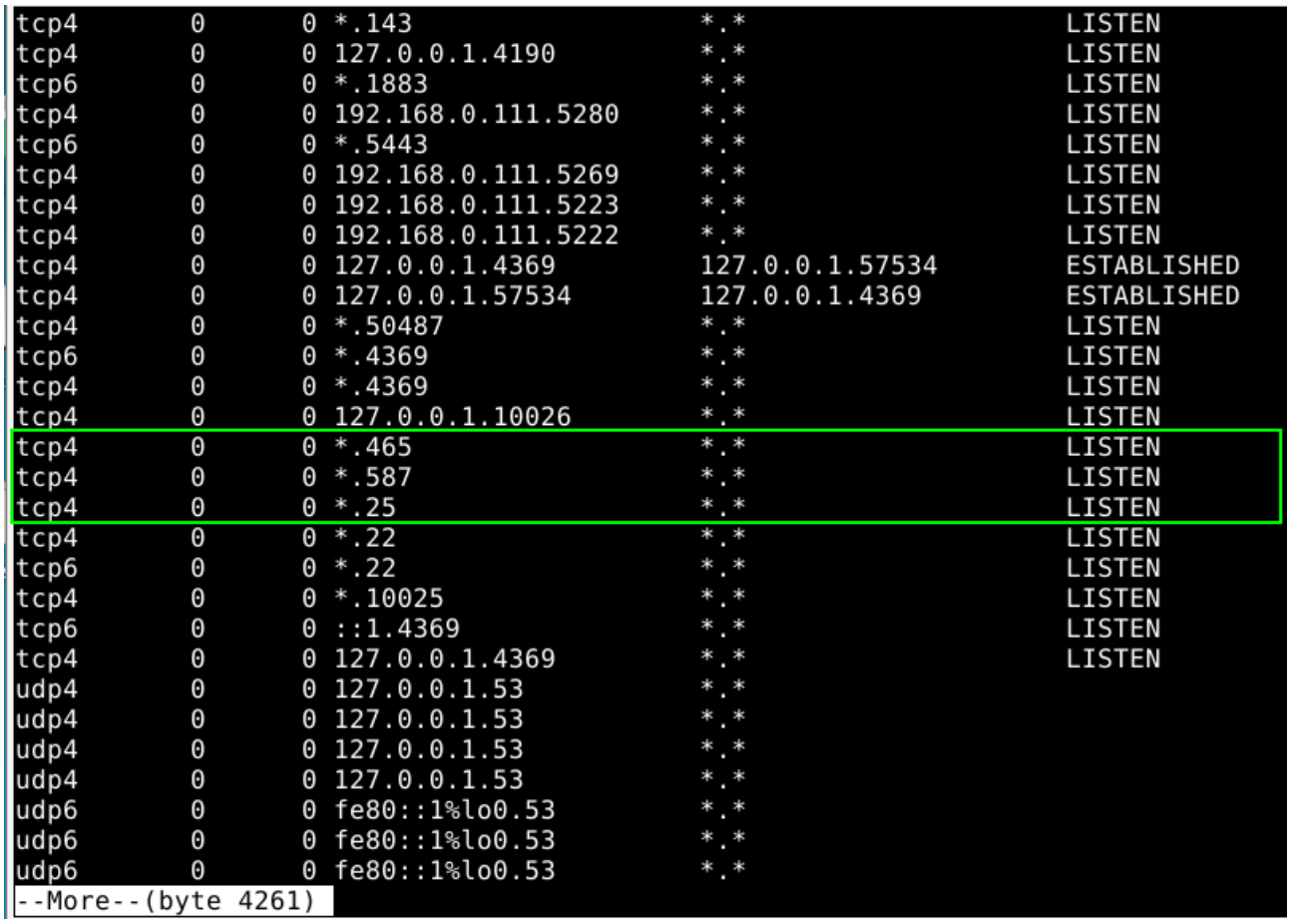


Рисунок 2.3 – Вивід команди `netstat -an`

Кожен рядок представляє один з портів, які сервер слухає для вхідних з'єднань.

В цьому конкретному виводі:

1) `tcp4 *.465 LISTEN`. Сервер слухає порт 465 TCP для SMTPS (SMTP з використанням TLS).

2) `tcp4 *.587 LISTEN`. Це порт 587 TCP для альтернативного SMTP, який часто використовується для аутентифікації перед відправкою електронної пошти клієнтами, наприклад, з використанням STARTTLS.

3) `tcp4 *.25 LISTEN`. Порт 25 - це стандартний порт SMTP для надсилання електронної пошти.

Ці порти є стандартними портами для прослуховування сервером електронної пошти та зазвичай використовуються для обробки вхідних та вихідних з’єднань.

2.3 Parrot Security у ролі засобу атаки

Parrot Security - це дистрибутив Linux, який спеціально розроблений для тестуванні безпеки мереж [7].

За допомогою інструментів доступних Parrot Security можна виконувати тестування на проникнення для оцінки рівня безпеки системи. У нашому випадку Parrot Security буде використаний як засіб для виконання SYN flood атаки.

Parrot Security має ряд інструментів, таких як hping3 та metasploit, які можуть бути використані для запуску та симуляції SYN flood атаки.

На рисунку 2.4 можна побачити параметри налаштування мережі в операційної системи Parrot Security на хості Attacker 1.

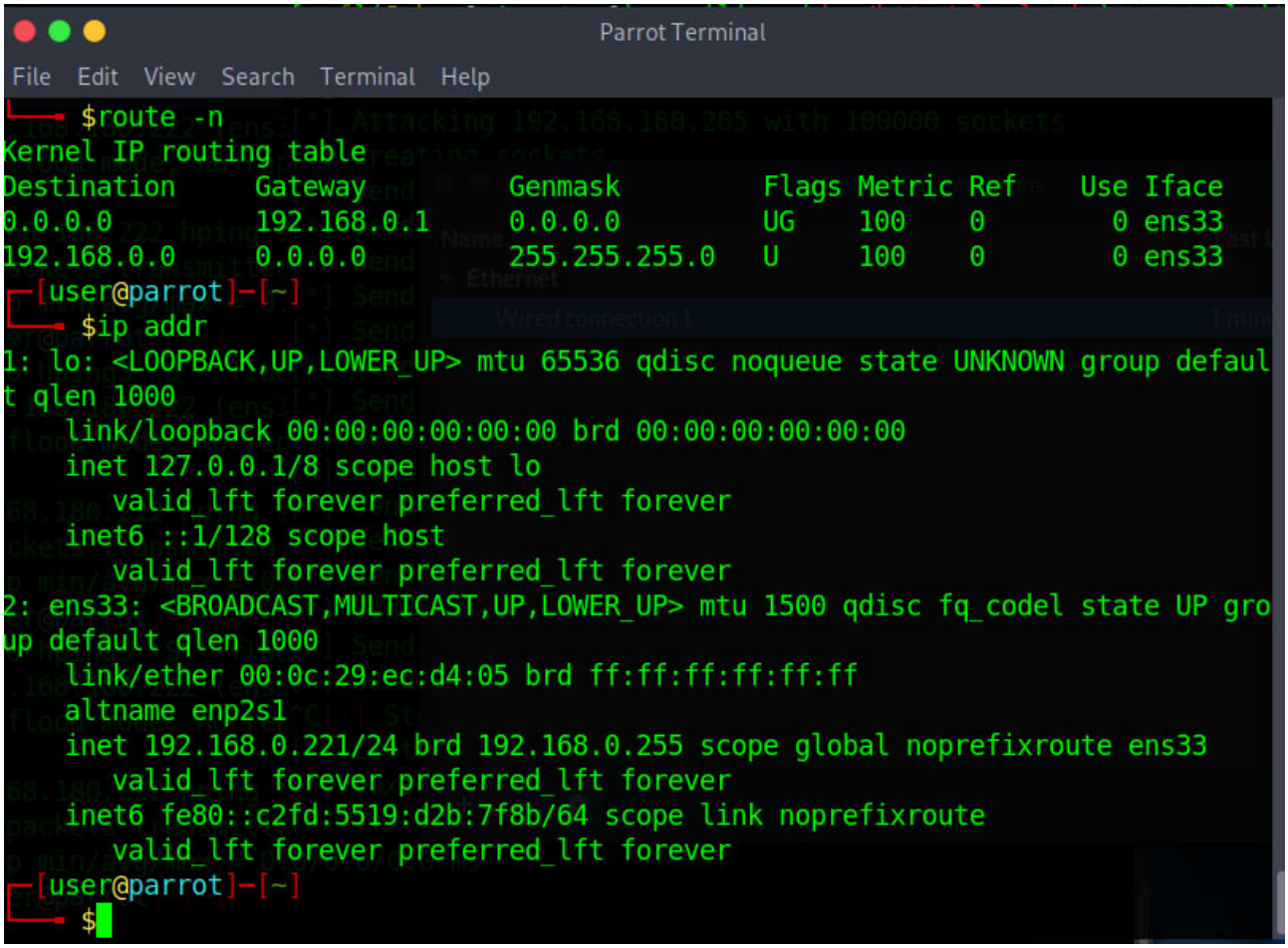


Рисунок 2.4 – Мережеві налаштування Parrot Security

Для здійснення SYN flood атаки в кожній з трьох операційних системи Parrot Security буде використано фреймворк Metasploit.

Metasploit використовується для експлуатації вразливостей, тестування безпеки та запуску атак на системи [8].

Модуль auxiliary/dos/tcp/synflood призначений для здійснення атаки типу SYN flood на цільовий сервер. Цей модуль використовується для створення і відправлення багатьох підроблених пакетів TCP з запитами SYN на цільовий сервер. Для використання цього модуля в Metasploit, зазвичай потрібно вказати IP-адресу та порт цільового сервера, а також можливо вказати інші параметри, такі як швидкість відправки пакетів чи кількість пакетів, що будуть відправлені.

2.4 Здійснення SYN flood атаки на SMTP сервер

На початковому етапі здійснимо перевірку працездатності SMTP сервера з операційної системи Oracle Linux, яка розміщена в локальній мережі (Рисунок 2.5).

```
[root@oraclelinux admin]# ping 192.168.0.120
PING 192.168.0.120 (192.168.0.120) 56(84) bytes of data.
64 bytes from 192.168.0.120: icmp_seq=1 ttl=64 time=0.457 ms
64 bytes from 192.168.0.120: icmp_seq=2 ttl=64 time=0.720 ms
64 bytes from 192.168.0.120: icmp_seq=3 ttl=64 time=0.489 ms
64 bytes from 192.168.0.120: icmp_seq=4 ttl=64 time=0.456 ms
^C
--- 192.168.0.120 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3081ms
rtt min/avg/max/mdev = 0.456/0.530/0.720/0.110 ms
[root@oraclelinux admin]#
[root@oraclelinux admin]# telnet  192.168.0.120 25
Trying 192.168.0.120...
Connected to 192.168.0.120.
Escape character is '^]'.
220 mail.localserver.lan ESMTP Postfix
```

Рисунок 2.5 – Перевірка з’єднання з SMTP сервером

Ці команди вказують на успішне встановлення з'єднання з сервером з IP-адресою 192.168.0.120 через ping та telnet на 25 порт.

Команда `telnet 192.168.0.120 25` підтверджує, що наш комп'ютер зміг підключитися до поштового сервера, який слухає на порту 25 (SMTP). Отримане повідомлення "`220 mail.localserver.lan ESMTP Postfix`" є відповіддю від поштового сервера Postfix, що свідчить про успішну установку з'єднання.

Ці дії демонструють коректну роботу мережі, можливість зв'язку та установки з'єднання з поштовим сервером на порту 25.

На рисунку 2.6 показано вивід команди tcpdump при коректній взаємодії клієнта з сервером.

```
root@mail:/usr/local/etc/rc.d# tcpdump -vvvvvv -i em0 -n port 25
tcpdump: listening on em0, link-type EN10MB (Ethernet), capture size 262144 byte
s
19:27:07.085133 IP (tos 0x10, ttl 64, id 25861, offset 0, flags [DF], proto TCP
(6), length 60)
    192.168.0.130.34984 > 192.168.0.120.25: Flags [S], cksum 0x46c7 (correct), s
eq 1881086926, win 64240, options [mss 1460,sackOK,TS val 4243550814 ecr 0,nop,w
scale 7], length 0
19:27:07.085224 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6),
length 60)
    192.168.0.120.25 > 192.168.0.130.34984: Flags [S.], cksum 0x8279 (incorrect
-> 0xe2c5), seq 2508958575, ack 1881086927, win 65535, options [mss 1460,nop,wsc
ale 6,sackOK,TS val 847309670 ecr 4243550814], length 0
19:27:07.085528 IP (tos 0x10, ttl 64, id 25862, offset 0, flags [DF], proto TCP
(6), length 52)
    192.168.0.130.34984 > 192.168.0.120.25: Flags [.], cksum 0x0f9b (correct), s
eq 1, ack 1, win 502, options [nop,nop,TS val 4243550814 ecr 847309670], length
0
19:27:07.086590 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6),
length 92)
    192.168.0.120.25 > 192.168.0.130.34984: Flags [P.], cksum 0x8299 (incorrect
-> 0xb749), seq 1:41, ack 1, win 1027, options [nop,nop,TS val 847309670 ecr 424
3550814], length 40: SMTP, length: 40
        220 mail.localserver.lan ESMTP Postfix
19:27:07.086951 IP (tos 0x10, ttl 64, id 25863, offset 0, flags [DF], proto TCP
(6), length 52)
    192.168.0.130.34984 > 192.168.0.120.25: Flags [.], cksum 0x0f71 (correct), s
eq 1, ack 41, win 502, options [nop,nop,TS val 4243550816 ecr 847309670], length
 0
^C
5 packets captured
658 packets received by filter
```

Рисунок 2.6 – Вивід команди `tcpdump` при коректній взаємодії з SMTP сервером

Перший пакет показує, що клієнт з IP-адресою 192.168.0.130 відправляє пакет SYN (прапорець [S]) на порт 25 сервера з IP-адресою 192.168.0.120, і цей пакет надсилається з порту 34984.

Другий пакет є відповіддю на перший пакет SYN від сервера з IP-адресою 192.168.0.120. Сервер відправляє пакет SYN-ACK (прапопець [S.]) назад до клієнта 192.168.0.130 з портом 34984.

Третій пакет є підтвердженням SYN-ACK пакету від клієнта з IP адресою 192.168.0.130 та портом 34984. Прапорець [.] в TCP заголовку пакета є прапорцем підтвердження (ACK) і вказує на те, що пакет має підтвердження отримання даних. Цей прапорець є одним з основних в TCP і використовується для підтвердження прийому певної послідовності байтів у TCP-з'єднанні.

Четвертий пакет містить SMTP-відповідь, де сервер відправляє привітання "`220 mail.localserver.lan ESMTP Postfix`" до клієнта з IP адресою 192.168.0.130.

Останній пакет підтверджує отриманий від сервера текст "220 mail.localserver.lan ESMTP Postfix".

Здійснимо SYN flood атаку за допомогою фреймворка Metasploit. Налаштування модуля auxiliary/dos/tcp/synflood атакуючого хоста (Attacker 1) показані на рисунку 2.7.

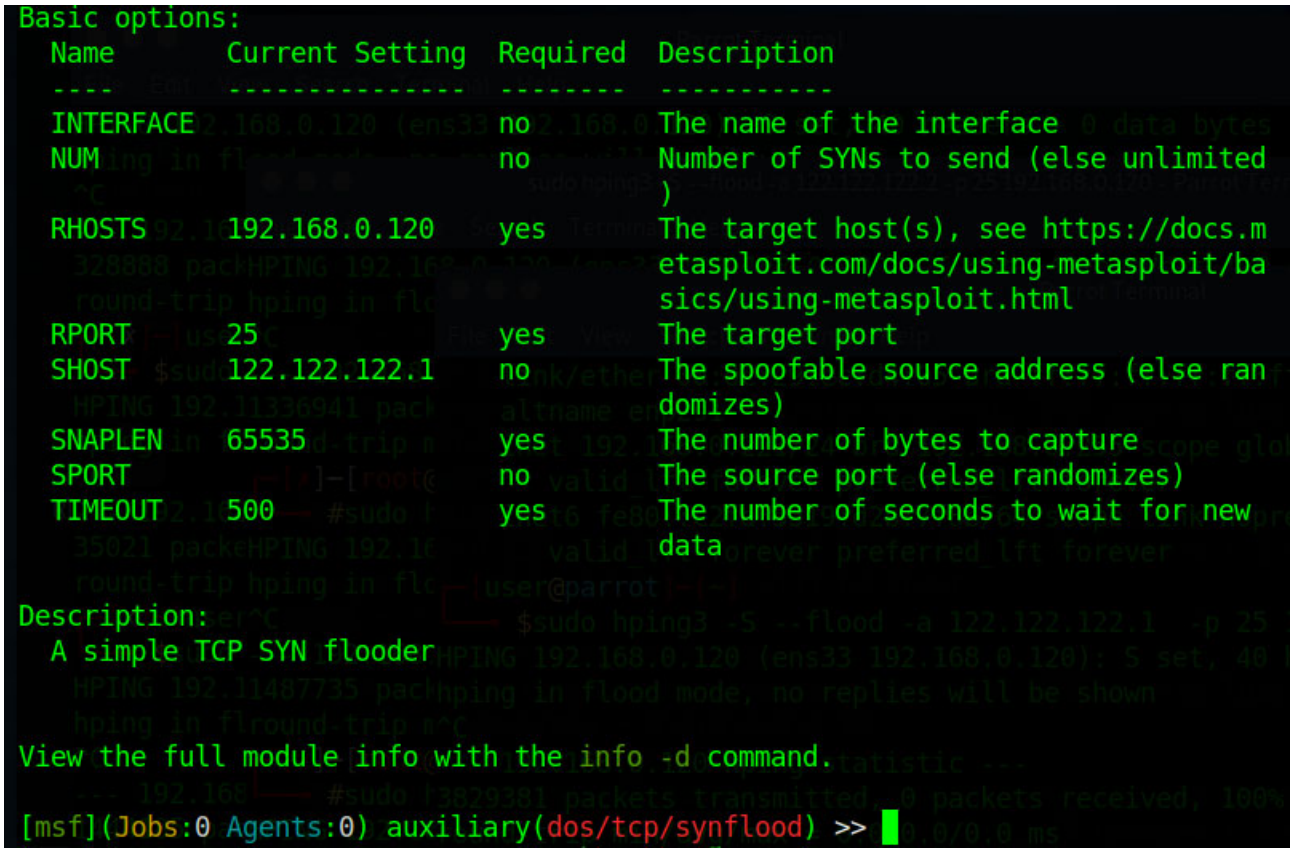


Рисунок 2.7 – Налаштування модуля auxiliary/dos/tcp/synflood

Основні деталі налаштувань:

1) NUM. Значення не встановлено, що означає надсилання необмеженої кількості SYN запитів.

2) RHOSTS 192.168.0.120 - цільовий хост для SYN flood атаки.

3) RPORT 25 - цільовий порт для атаки, що відповідає стандартному порту SMTP.

4) SHOST 122.122.122.121 - підроблена вихідна IP-адреса з якої відправляються SYN запити.

Для підсилення атаки запустимо її одночасно з трьох атакуючих хостів.

На рисунку 2.8 можна побачити результат атаки.

```
[root@oraclelinux admin]# telnet  192.168.0.120 25
Trying 192.168.0.120...
```

Рисунок 2.8 – Перевірка з’єднання з SMTP сервером під час атаки

Цей вивід демонструє спробу підключення до IP-адреси 192.168.0.120 через telnet на порті 25, який використовується для поштового сервера з протоколом SMTP.

Фраза `"Trying  192.168.0.120..."` означає, що виконується спроба встановлення з'єднання з вказаною IP-адресою. Однак у цьому випадку немає подальшого виводу, що вказувати на те, що з'єднання не було успішним.

Атакований SMTP сервер перестав відповідати на запити клієнтів.

На рисунку 2.9 можна побачити що SYN flood атака також спричинила значне використання CPU на SMTP сервері.

```
last pid: 28480;  load averages:  3.22,  2.35,  1.26    up 3+02:33:58  20:37:30
769 threads:   12 running, 706 sleeping, 51 waiting
CPU 0:  0.8% user,  0.0% nice,  2.3% system, 23.8% interrupt, 73.0% idle
CPU 1:  0.4% user,  0.0% nice,  0.4% system, 61.6% interrupt, 37.6% idle
CPU 2:  0.0% user,  0.0% nice, 72.9% system,  0.0% interrupt, 27.1% idle
CPU 3:  0.0% user,  0.0% nice,  100% system,  0.0% interrupt,  0.0% idle
Mem: 144M Active, 1315M Inact, 73M Laundry, 1375M Wired, 1047M Free
ARC: 735M Total, 447M MFU, 43M MRU, 1248K Anon, 3505K Header, 240M Other
     279M Compressed, 451M Uncompressed, 1.62:1 Ratio
Swap: 10G Total, 1538M Used, 8702M Free, 15% Inuse

  PID USERNAME    PRI NICE   SIZE    RES STATE    C   TIME    WCPU COMMAND
    0 root        -76    -     0B   704K CPU3     3  26:14  99.83% kernel{if_io
   12 root        -60    -     0B   816K WAIT     0  20:30  84.49% intr{swi4: c
   11 root        155 ki31     0B    64K RUN      0  72.7H  74.59% idle{idle: c
   11 root        155 ki31     0B    64K RUN      2  72.7H  62.88% idle{idle: c
   11 root        155 ki31     0B    64K RUN      1  72.8H  37.75% idle{idle: c
    0 root        -76    -     0B   704K CPU2     2   8:33  36.83% kernel{if_io
    0 root        -76    -     0B   704K -        1  37:47   1.02% kernel{if_co
 1417 root         20    0    71M    13M select   1  15:30   0.31% vmtoolsd{vmt
 1372 root         20   -1   208M    40M select   1   7:46   0.30% Xorg{MainThr
  200 root         20    0    33M  3528K select   1  16:45   0.25% vmtoolsd{vmt
   36 root         20    -     0B    16K geli:w   1   2:53   0.14% g_eli[1] da1
 1449 root         20    0   138M    27M select   0   5:53   0.13% xfce4-termin
28480 root         20    0    15M  4908K CPU1     1   0:00   0.11% top
   32 root         20    -     0B    16K RUN      1   2:58   0.10% g_eli[1] da0
   37 root         20    -     0B    16K geli:w   2   2:11   0.10% g_eli[2] da1
 1399 root         20    0   215M    11M select   0   1:21   0.08% xfwm4{xfwm4}
   12 root        -88    -     0B   816K WAIT     1   3:52   0.06% intr{irq17:
   39 root        -12    -     0B  5120K -        1   4:40   0.06% zpool-zroot{
    7 root        -16    -     0B    32K -        0  14:07   0.04% cam{doneq0}
   33 root         20    -     0B    16K RUN      2   2:46   0.04% g_eli[2] da0
```

Рисунок 2.9 – Різке зростання використання CPU на SMTP сервері під час атаки

Під час атаки CPU використовуються переважно для системних операцій (system), або обробки переривань (interrupt).

На рисунку 2.10 показано вивід команди `netstat` на SMTP сервері, який також підтверджує наявність SYN flood атаки.

```
root@mail:/usr/local/etc/rc.d# netstat -an | more
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 192.168.0.120.25       122.122.122.3.20853    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.1.15906    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.1.15870    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.1.15007    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.1.14412    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.3.19182    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.2.52696    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.1.14110    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.3.18838    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.1.14066    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.3.18692    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.2.52256    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.2.51941    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.2.51831    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.1.13439    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.1.13416    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.1.13097    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.2.51394    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.3.17767    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.2.51346    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.3.17409    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.2.50926    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.3.17315    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.3.16667    SYN_RCVD
tcp4       0      0 192.168.0.120.25       122.122.122.3.16633    SYN_RCVD
```

Рисунок 2.10 – Вивід команди `netstat` на SMTP сервері під час атаки

Під час атаки тисячі з'єднань перебувають у стані SYN_RCVD, що означає, що сервер отримує SYN пакети від клієнта та очікує завершення з'єднання.

Також на рисунку 2.11 з виводу команди `tcpdunp` можна побачити що є велика кількість не завершених запитів на встановлення з'єднання з поштовим сервером на порт 25.

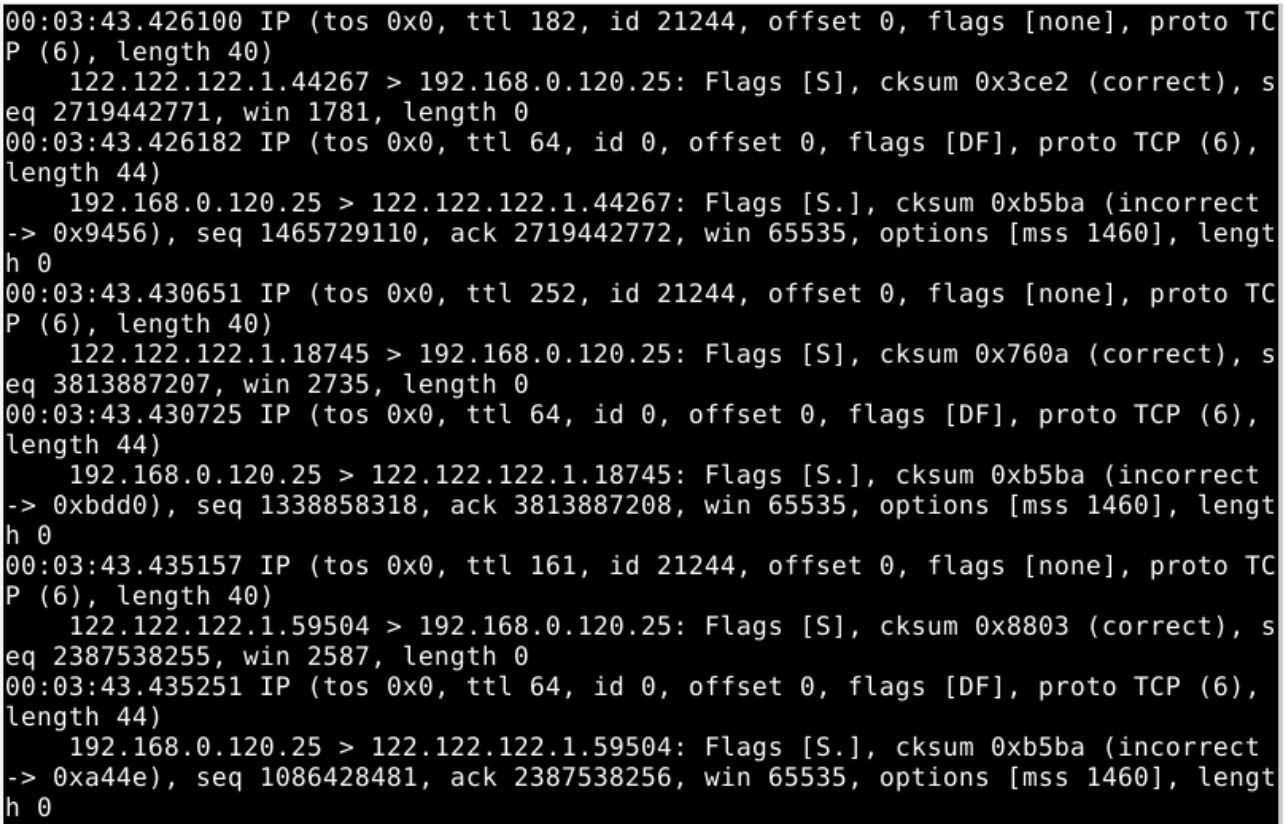


Рисунок 2.11 – Вивід команди `tcpdump` на SMTP сервері під час атаки

Відправники цих пакетів мають фіктивні IP-адреси. Кожен пакет має встановлені прапорці SYN, що означає початок процесу TCP-з'єднання. У відповідь сервер надіслає сигнал підтвердження (SYN-ACK) на фіктивну IP адресу атакуючих.

Цей тип трафіку є типовим для швидкої та потужної SYN flood атаки. У нашому випадку атаку була досить успішною. Поштовий сервер перестав відповідати на запити клієнтів.

3 РОЗРОБКА ЗАСОБІВ ДЛЯ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАКИ

3.1 Технологія проксі як механізм пом’якшення атаки

Технологія проксі може використовуватися як один із механізмів для пом'якшення атак на сервери або мережеві ресурси [2]. Механізм проксі діє як посередник між клієнтом та сервером, приймаючи запити від клієнтів та пересилаючи їх на сервери.

Проксі може фільтрувати вхідні запити, щоб блокувати певні типи запитів і відправляти їх на перевірку що до безпеки.

3.1.1 Брандмауер PF з механізмом SYNPROXY

Брандмауер PF - це брандмауер та система фільтрації пакетів для операційних систем, таких як OpenBSD, FreeBSD та NetBSD [9]. Він використовується для керування мережевим трафіком, забезпечення безпеки мережі та захисту системи від різних видів атак.

Основні можливості PF наступні:

1) Stateful filtering (фільтрація на основі станів). PF веде облік станів підключень, що дозволяє заблокувати або дозволити трафік на основі поточного стану підключення, а не лише на основі IP-адреси та порту.

2) NAT. PF дозволяє змінювати IP-адреси та порти пакетів, що проходять через брандмауер, для реалізації функції NAT.

3) Traffic shaping (формування трафіку). PF може обмежувати швидкість передачі даних або встановлювати пріоритети для різних видів трафіку.

4) Пом’якшення атак. PF може фільтрувати пакети, що відповідають певним атакам.

PF в операційній системі FreeBSD має можливість використовувати механізм SYNPROXY. Цей механізм спрямований на захист від SYN flood атак, які спрямовані на вичерпання ресурсів системи за допомогою підроблених SYN-пакетів.

SYNPROXY в PF використовується для фільтрації трафіку на рівні сеансу та робить це шляхом аналізу SYN-пакетів, які надходять на сервер. Він може сприймати легітимні з'єднання, відмовляючи з'єднанням, які підозріло виглядають, тобто припущенням, що вони є частиною атаки.

За замовчуванням, PF пересилає пакети, які є частиною TCP-рукостискання між двома точками. Опція SYNPROXY може використовуватися в PF для того, щоб PF завершив рукостискання з клієнтом, виконав рукостискання з сервером і тільки потім переслав пакети між ними.

Ніякі пакети не будуть відправлені на сервер до завершення клієнтом рукостискання. Це означає, що SYN flood пакети з підробленими вихідними IP-адресами не дістануться до сервера, оскільки відправник не зможе завершити рукостискання.

Цей механізм дозволяє створити віртуальний стан для кожного вхідного SYN-пакету, що дозволяє обійти певні обмеження пов’язані з ресурсами для зберігання станів підключення. Таким чином, SYNPROXY робить більш ефективним реагування на SYN flood атаки.

3.1.2 Налаштування та тестування механізму SYNPROXY

Проведемо налаштування брандмауера PF (Packet Filter) для можливості використання механізму SYNPROXY. На рисунку 3.1 показано частину конфігураційного файлу PF з механізмом SYNPROXY для мінімізації впливу SYN flood атак на SMTP сервер [9].

```
 GNU nano 7.2                          pf.conf
#!/bin/sh
ext_if = "em0"
#
set skip on lo0
set limit { states 3500000, frags 3500000, src-nodes 350000 }
set optimization aggressive
#
scrub in all
#
pass in  quick on $ext_if proto tcp from any to $ext_if port {25,465,587} \
        synproxy state  \
#
```

Рисунок 3.1 – Конфігураційний файл `pf.conf` з механізмом SYNPROXY

Фрагмент конфігурації містить наступні параметри:

1) `ext_if = "em0"` - це зовнішній інтерфейс, через який здійснюється з'єднання з іншими мережами;

2) `set skip on lo0` - відключення обробки трафіку для інтерфейсу lo0 (локальний інтерфейс);

3) `set limit` - налаштування лімітів для кількості станів, фрагментів та джерел, які фільтруються;

4) `set optimization aggressive` - встановлення агресивної оптимізації для покращення продуктивності файрволу;

5) `scrub in all` - проведення очищення пакетів для вхідних з'єднань;

6) `pass in quick on $ext_if proto tcp from any to $ext_if port {25,465,587} synproxy state` - це правило дозволяє вхідні TCP-з'єднання на портах 25 (SMTP), 465 (SMTPS), 587 (submission) та використовує опцію synproxy для зменшення впливу атак типу SYN flood.

Для проведення тестування налаштованого механізму SYNPROXY здійснимо атаку SYN flood аналогічну як в пункті 2.4.

Вивід команди `pfctl -s state` показує поточні стани з'єднань, які обробляються брандмауером PF. У нашому випадку це відображає з'єднання до поштового сервера з IP-адресою 192.168.0.120 з IP-адреси 122.122.122.2. Стан з’єднання PROXY:SRC свідчить про те, що успішно використовується механізм SYNPROXY для зменшення впливу від SYN flood атак (Рисунок 3.2).

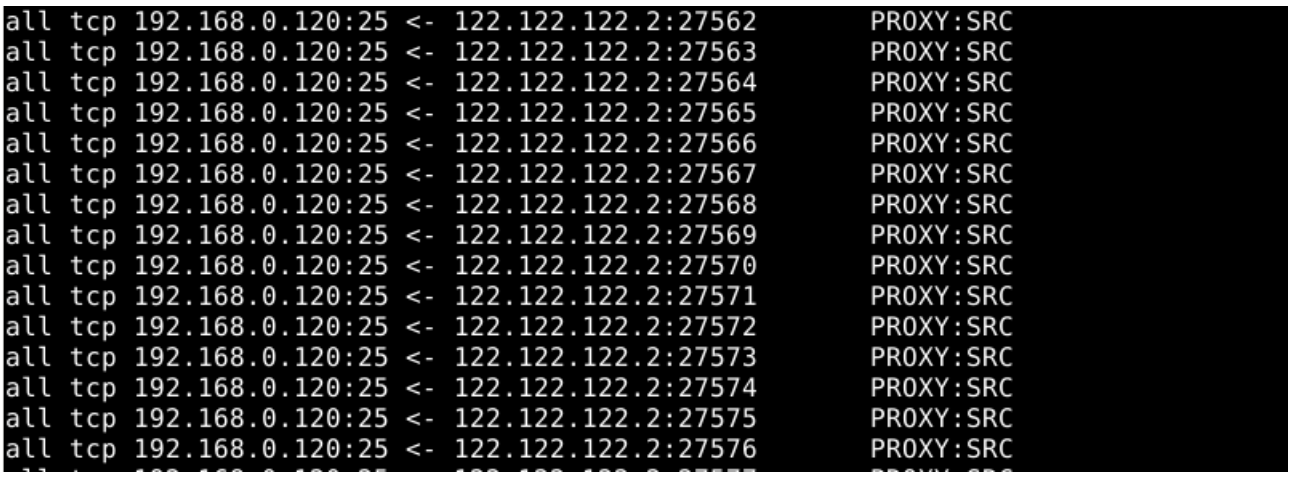
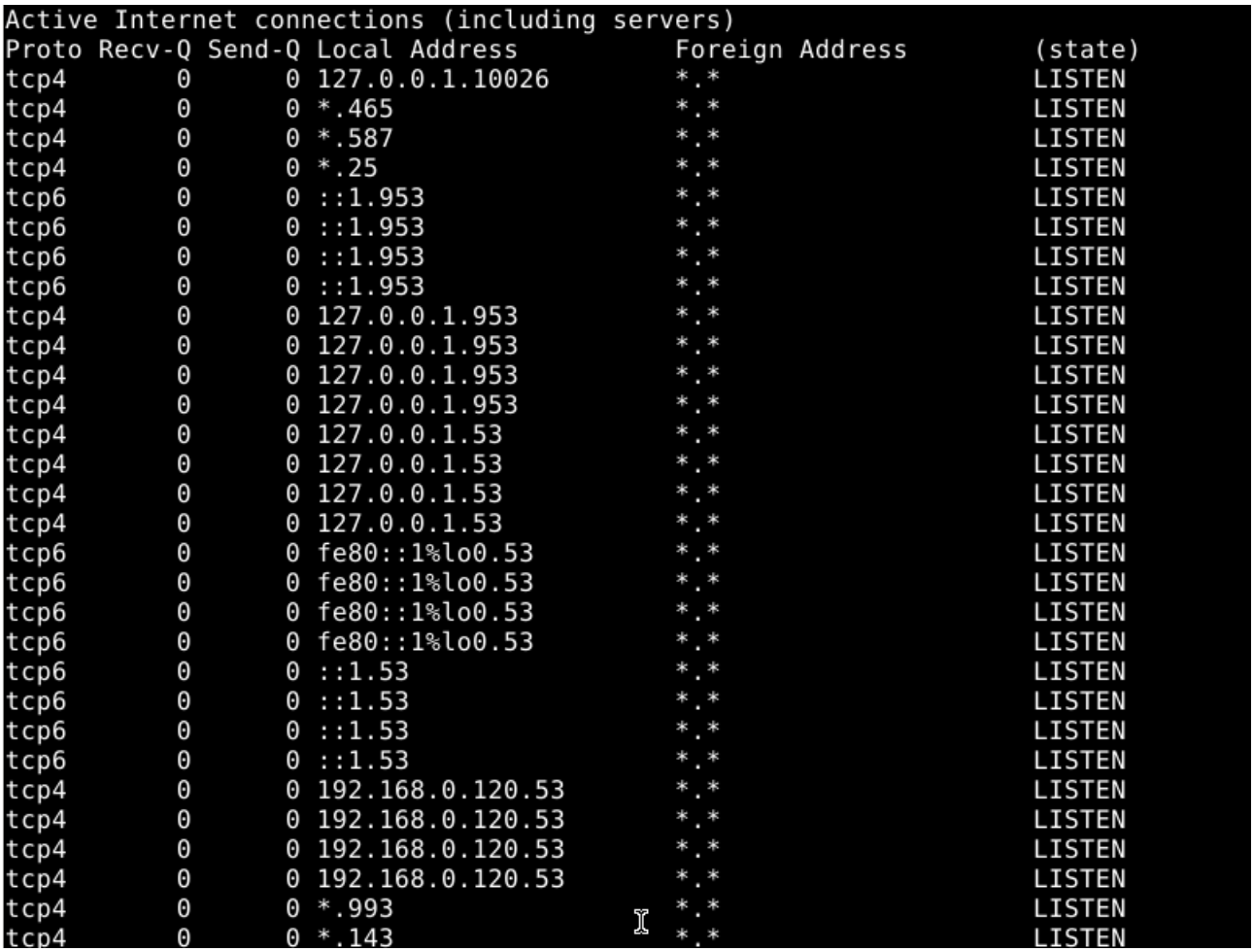


Рисунок 3.2 – Вивід команди `pfctl -s state`

Ці з'єднання є віртуальними. Трафік пройде через брандмауер PF після того, як буде виконано процедуру рукостискання і підтверджено легітимність з'єднання.

На рисунку 3.3 можна побачити що з’єднання до сервера так і не передалось.



```
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 127.0.0.1.10026        *.*                    LISTEN
tcp4       0      0 *.465                  *.*                    LISTEN
tcp4       0      0 *.587                  *.*                    LISTEN
tcp4       0      0 *.25                   *.*                    LISTEN
tcp6       0      0 ::1.953                *.*                    LISTEN
tcp6       0      0 ::1.953                *.*                    LISTEN
tcp6       0      0 ::1.953                *.*                    LISTEN
tcp6       0      0 ::1.953                *.*                    LISTEN
tcp4       0      0 127.0.0.1.953          *.*                    LISTEN
tcp4       0      0 127.0.0.1.953          *.*                    LISTEN
tcp4       0      0 127.0.0.1.953          *.*                    LISTEN
tcp4       0      0 127.0.0.1.953          *.*                    LISTEN
tcp4       0      0 127.0.0.1.53           *.*                    LISTEN
tcp4       0      0 127.0.0.1.53           *.*                    LISTEN
tcp4       0      0 127.0.0.1.53           *.*                    LISTEN
tcp4       0      0 127.0.0.1.53           *.*                    LISTEN
tcp6       0      0 fe80::1%lo0.53         *.*                    LISTEN
tcp6       0      0 fe80::1%lo0.53         *.*                    LISTEN
tcp6       0      0 fe80::1%lo0.53         *.*                    LISTEN
tcp6       0      0 fe80::1%lo0.53         *.*                    LISTEN
tcp6       0      0 ::1.53                 *.*                    LISTEN
tcp6       0      0 ::1.53                 *.*                    LISTEN
tcp6       0      0 ::1.53                 *.*                    LISTEN
tcp6       0      0 ::1.53                 *.*                    LISTEN
tcp4       0      0 192.168.0.120.53       *.*                    LISTEN
tcp4       0      0 192.168.0.120.53       *.*                    LISTEN
tcp4       0      0 192.168.0.120.53       *.*                    LISTEN
tcp4       0      0 192.168.0.120.53       *.*                    LISTEN
tcp4       0      0 *.993                  *.*                    LISTEN
tcp4       0      0 *.143                  *.*                    LISTEN
```

Рисунок 3.3 – Вивід команди `netstat` на SMTP сервері з механізмом SYNPROXY

Отже брандмауер PF керує з'єднаннями, і прозоро обробляє пакети між клієнтом та сервером через механізм SYNPROXY.

Здійснимо перевірку працездатності SMTP сервера з операційної системи Oracle Linux, яка розміщена в локальній мережі (Рисунок 3.4).

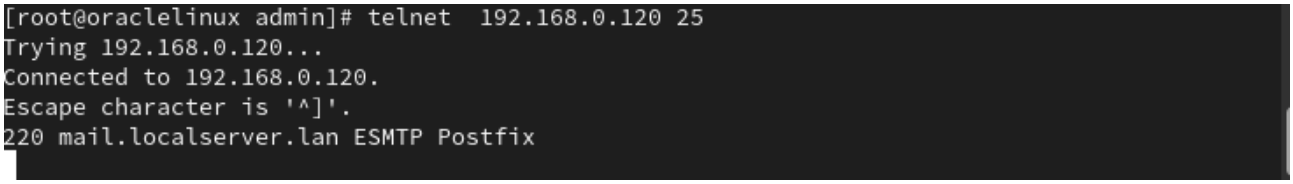


Рисунок 3.4 – Перевірка доступності SMTP сервера під час атаки

Вивід цієї команди вказує на успішне встановлення з'єднання з сервером з IP-адресою 192.168.0.120 на 25 порт. Незважаючи на атаку, SMTP сервер все ще може обслуговувати клієнтів.

Попри всі переваги механізму SYNPROXY для зменшення впливу SYN flood атак його недоліком є значне використання ресурсів сервера. На рисунку 3.5 можна побачити що SYN flood атака також спричинила надмірне використання CPU на SMTP сервері.

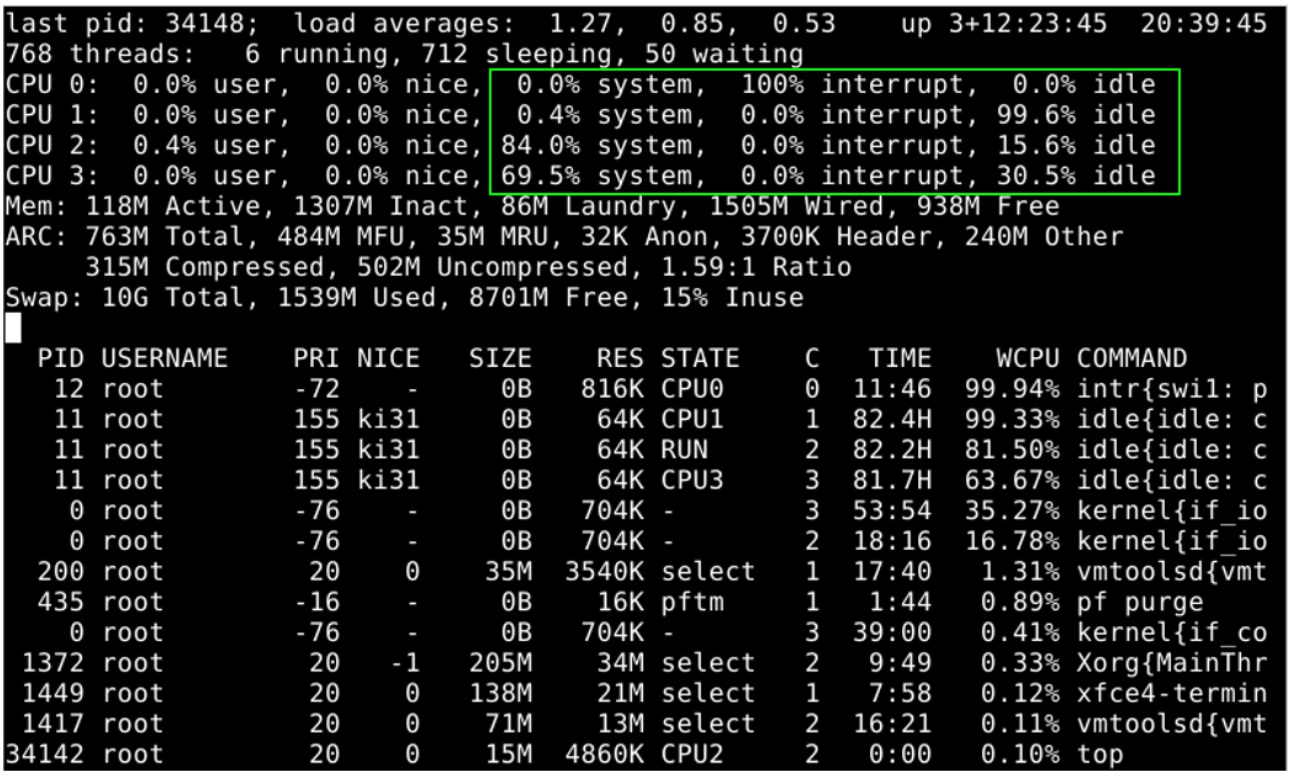


Рисунок 3.5 – Зростання використання CPU на SMTP сервері під час атаки

Це зв’язано з тим, що механізм SYNPROXY, зменшуючи вплив від SYN flood атак використовує значні ресурси сервера для обробки та аналізу SYN пакетів.

В цьому контексті постає питання розробки механізму блокування IP адрес зловмисників при виявлення атаки.

3.2 Розробка додаткового механізму захисту

Додатковий механізм захисту від атак типу SYN flood в операційній системі FreeBSD включає кроки створення програмного модуля, який буде аналізувати стан брандмауера PF в реальному часі, налаштування та запуск модуля як сервісу.

Модуль буде взаємодіяти з брандмауером PF для виявлення атаки та автоматичного блокування IP-адрес зловмисників. Крім цього, програмний модуль буде також відправляти повідомлення за допомогою Signal, які будуть сповіщати про виявлення та блокування SYN flood атаки.

3.2.1 Механізм виявлення та блокування атаки

Розглянемо детальний механізм виявлення та блокування SYN flood атаки за допомогою додаткового програмного модуля:

1) Створення служби-монітору. Налаштовуємо службу, який працюватиме в режимі постійного моніторингу стану брандмауера PF на наявність SYN пакетів із станом PROXY:SRC.

2) Моніторинг з'єднань. Модуль починає перевіряти стан з'єднань з використанням інструментів, які надають доступ до стану брандмауера PF для виявлення з'єднань із станом PROXY:SRC.

3) Відстеження IP-адрес. Модуль відстежує кількість з'єднань для кожної унікальної IP-адреси, яка відправляє пакети зі станом PROXY:SRC.

4) Аналіз з'єднань. Модуль перевіряє кількість з'єднань для кожної IP-адреси зі станом PROXY:SRC. Якщо кількість з'єднань перевищує попередньо задану, реагує на це як на можливу атаку SYN flood.

5) Блокування IP-адрес. Програмний модуль додає IP адресу зловмисника до таблиці PF для блокування нових підключень.

6) Надсилання повідомлення. Після успішного блокування здійснюється повідомлення в месенджер Signal про те, що виявлена за заблокована атака SYN flood.

7) Логування та аудит. Здійснюється ведення журналу подій для запису дій модуля з виявлення атак, блокування IP-адрес та відправлення повідомлень.

Це загальний підхід до створення механізму виявлення та блокування SYN flood атаки.

3.2.2 Модифікація налаштувань брандмауера PF

Для реалізації методу, описаного у розділі 3.2.1, внесемо необхідні зміни до файлу конфігурації pf.conf шляхом додавання відповідних налаштувань.

На рисунку 3.6 показано оновлений вміст конфігураційного файлу брандмауера PF.

```
  GNU nano 7.2                          pf.conf
#!/bin/sh
ext_if = "em0"
#
set skip on lo0
set limit { states 3500000, frags 3500000, src-nodes 350000 }
set optimization aggressive
#
scrub in all
#
#SYN flood SMTP
table <synfloodip> persist  file "/etc/synfloodip"
block drop in quick from <synfloodip>
#
table <synfloodsmtp> persist
block drop in quick from <synfloodsmtp>
#
pass in  quick on $ext_if proto tcp from any to $ext_if port {25,465,587} \
        synproxy state  \
#
```

Рисунок 3.6 – Оновлений вміст конфігураційного файлу `pf.conf`

Додаткові налаштування мають наступні значення:

1) `table <synfloodip> persist file "/etc/synfloodip"`. Створює таблицю <synfloodip> для зберігання IP-адрес та налаштовує її для постійного зберігання у файлі /etc/synfloodip;

2) `block drop in quick from <synfloodip>`. Блокує вхідний трафік з IP-адрес, які містяться у таблиці <synfloodip>;

3) `table <synfloodsmtp> persist`. Створює пусту таблицю <synfloodsmtp> для використання в реальному часі;

4) `block drop in quick from <synfloodsmtp>`. Блокує вхідний трафік з IP-адрес, які містяться у таблиці <synfloodsmtp>.

Ця конфігурацій PF використовується для виявлення та запобігання атакам типу SYN flood на сервер SMTP.

3.2.3 Реалізація програмного модуля

Для реалізації програмного модуля, що автоматично блокуватиме IP-адреси зловмисників, буде використано мову програмування Ruby [10].

Ruby - це мова програмування з відкритим вихідним кодом, яка відома своєю простотою та гнучкістю. Вона має спрощений спосіб написання коду, що робить її приємною для використання та розробки. Ruby часто використовується для створення веб-додатків, автоматизації завдань, розробки ігор та великої кількості програмного забезпечення. Це потужний інструмент з активною спільнотою, яка підтримує розвиток мови та надає багато корисних бібліотек та фреймворків для різних потреб програмістів. В додатку Б подано лістинг програмного модуля.

Програмний модуль реалізований у вигляді скрипта. Зазначений скрипт реалізує механізм виявлення та запобігання атаки SYN flood на сервер електронної пошти.

Покрокова робота програмного модуля наступна:

1) Визначається шлях до конфігураційного файлу (synflood_check.conf), файлу виведення блокованих IP-адрес (synfloodip), та команди для блокування IP-адрес у брандмауері (pfctl -t synfloodsmtp -T add -f).

2) Перевіряється наявність конфігураційного файлу. Якщо файл відсутній, генерується помилка. Завантажуються значення конфігурації з файлу, в тому числі максимальна допустима кількість з'єднань для спрацювання механізму блокування та стан, який потрібно перевірити.

3) Виконується команда pfctl -s state для отримання стану поточних з'єднань брандмауера. Лічильник підраховує кількість входжень вказаного стану PROXY:SRC у виводі команди pfctl -s state.

4) Якщо кількість з'єднань перевищує максимально допустиму, виконуються наступні дії:

а) виділяються унікальні IP-адреси, які знаходяться в стані PROXY:SRC;

б) IP-адреси додаються до файлу заблокованих IP-адрес;

в) виконується команда pfctl, щоб додати ці IP-адреси до таблиці блокування брандмауера;

г) генерується повідомлення для надсилання через Signal із зазначенням дати, часу та кількості IP-адрес, які було заблоковано.

5) Повідомлення, яке містить кількість з'єднань та кількість унікальних IP-адрес, які були заблоковані, надсилається через Signal.

По завершенню перевірки виводиться відповідне повідомлення у вікно консолі, яке буде направлене у файл журналу сервісу моніторингу SYN flood атак.

3.2.4 Налаштування та запуск сервісу моніторингу.

Для автоматизації виявлення атаки і блокування IP-адрес зловмисників у FreeBSD буде використано запуск скрипту `synflood_check.rb` як сервісу за допомогою інструментів управління сервісами операційної системи [5]. Для цього створимо файл `synflood_check_service` у каталозі `/usr/local/etc/rc.d` та зробимо його виконуваним. У додатку В показано вміст файлу для налаштування сервісу `synflood_check_service`. Цей скрипт призначено для запуску `synflood_check.rb` як сервісу у FreeBSD. Він використовує `/etc/rc.subr` для управління сервісами.

Основні моменти налаштування сервісу наступні:

1) Визначення сервісу та його залежностей.

2) Визначення команд запуску, зупинки та статусу сервісу.

3) Запуск `synflood_check.rb` як безкінечного циклу, що запускається в фоні:

а) `synflood_check_service_start` - ця функція запускає скрипт `synflood_check.rb` в безкінечному циклі і записує його вивід у файл `/var/log/synflood_check.log`. Скрипт буде виконуватись кожні 6 секунд;

б) `synflood_check_service_stop.` - ця функція зупиняє виконання `synflood_check.rb`, знищуючи його PID-файл;

в) `synflood_check_service_status` - ця функція показує статус сервісу, перевіряючи наявність PID-файлу.

Вивід команди перевірки статусу сервісу можна побачити на рисунку 3.7

```
root@mail:/var/log#
root@mail:/var/log# service synflood_check_service status
synflood check service is running with PID 35875.
root@mail:/var/log#
root@mail:/var/log#
```

Рисунок 3.7 – Вивід команди `service synflood_check_service status`

Тепер скрипт `synflood_check.rb` налаштований як сервіс в операційній системі FreeBSD. Це забезпечує автоматичне виявлення та блокування IP-адрес зловмисників під час атаки типу SYN flood на сервер SMTP.

3.2.5 Тестування розробленого захисту

Для перевірки роботи розробленого програмного модуля захисту від атаки типу SYN flood, здійснимо тестову атаку, яка буде ідентичною до тієї, що була описана у пункті 2.4.

Вмісту файлу журналу сервісу `synflood_check.log` свідчить про те що захист спрацював коректно (Рисунок 3.8).

```
2023-11-18 20:43:53 +0200
Number of connections: 177998
IP attacker: ["122.122.122.3", "122.122.122.2", "122.122.122.1"]
```

Рисунок 3.8 – Вмісту файлу `synflood_check.log`

Також можна переконатись що IP адреси зловмисників заблоковані перевіривши вміст таблиці брандмауера PF (Рисунок 3.9).

```
root@mail:/var/log# pfctl -t synfloodsmtp -T show
   122.122.122.1
   122.122.122.2
   122.122.122.3
root@mail:/var/log#
```

Рисунок 3.9 – Вивід вмісту таблиці `synfloodsmtp`

Після виконання блокування IP зловмисників використання ресурсів сервера значно зменшилось (Рисунок 3.10)

```
last pid: 34268;  load averages:  1.11,  1.14,  0.78    up 3+12:29:10  20:45:10
768 threads:   5 running, 712 sleeping, 51 waiting
CPU 0:  0.0% user,  0.0% nice,  0.0% system,  0.0% interrupt,  100% idle
CPU 1:  0.0% user,  0.0% nice,  0.0% system,  0.0% interrupt,  100% idle
CPU 2:  0.7% user,  0.0% nice,  0.0% system,  0.0% interrupt, 99.3% idle
CPU 3:  0.0% user,  0.0% nice,  5.4% system,  0.0% interrupt, 94.6% idle
Mem: 121M Active, 1308M Inact, 86M Laundry, 1507M Wired, 933M Free
ARC: 764M Total, 484M MFU, 36M MRU, 182K Anon, 3703K Header, 240M Other
     316M Compressed, 503M Uncompressed, 1.59:1 Ratio
Swap: 10G Total, 1539M Used, 8701M Free, 15% Inuse
WARN Manager - Messages have been last received 47 days ago. The Signal protocol
 expects that incoming messages are regularly received.IME    WCPU COMMAND
   11 root        155 ki31     0B    64K CPU2     2  82.3H 100.00% idle{idle: c
   11 root        155 ki31     0B    64K RUN      1  82.4H  99.80% idle{idle: c
   11 root        155 ki31     0B    64K CPU0     0  82.4H  99.64% idle{idle: c
   11 root        155 ki31     0B    64K CPU3     3  81.8H  86.68% idle{idle: c
    0 root        -76    -     0B   704K -        3  55:23  13.29% kernel{if_io
 1372 root         20   -1   205M    35M select   2   9:50   0.22% Xorg{MainThr
    0 root        -76    -     0B   704K -        2  39:02   0.16% kernel{if_co
 1417 root         20    0    73M    15M select   0  16:22   0.14% vmtoolsd{vmt
 1449 root         20    0   138M    21M select   1   7:59   0.10% xfce4-termin
```

Рисунок 3.10– Використання CPU на SMTP сервері після бокування IP атакуючих

Ця статистика вказує на використання CPU на SMTP сервері. CPU 0, CPU 1 та CPU 2 відображають дуже низький рівень використання. CPU 3 використовується системними процесами на рівні 5.4%. Це пов'язано з тим, що атака продовжується. Блокування трафіку від IP-адрес зловмисників також вимагає певних ресурсів для системних операцій або процесів, які виконуються на даному ядрі (CPU 3), в той час як інші процесори перебувають у стані простою.

Проте, в цілому система перебуває в стані простою, з великою кількістю вільних ресурсів.

Після блокування IP адрес зловмисників автоматично відправляється повідомлення про інцидент в месенджер Signal про те, що виявлена та заблокована атака SYN flood (Рисунок 3.11).

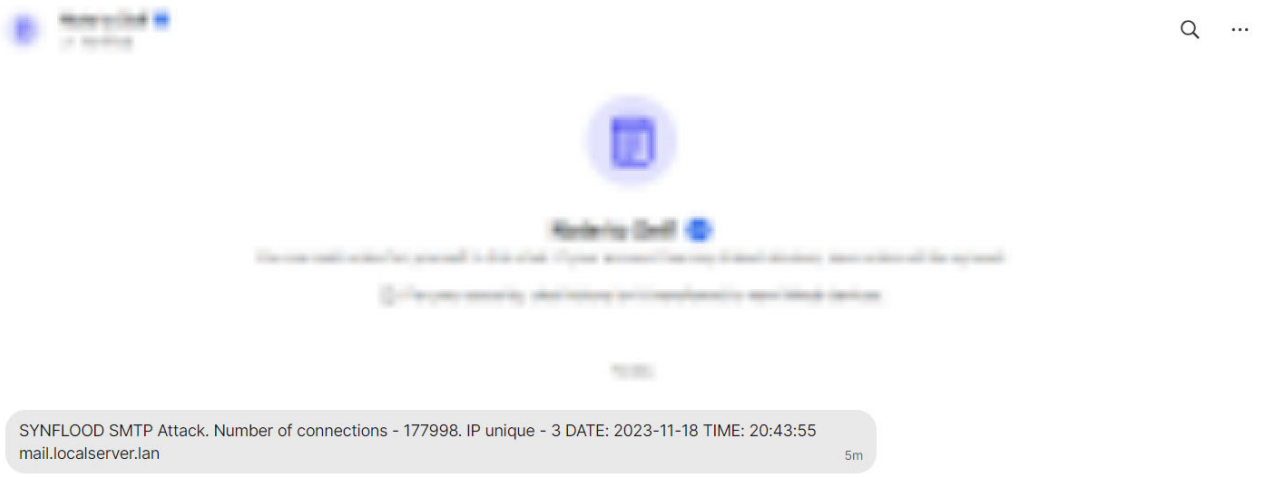


Рисунок 3.11– Приклад повідомлення про SYN flood атаку в месенджері Signal

Створений захисний механізм від SYN flood атак виконує свої завдання коректно, успішно виявляючи та блокуючи IP-адреси зловмисників.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою даної кваліфікаційної роботи є проектування та створення засобу мінімізації впливу SYN Flood атак на поштовий сервер. При створенні подібних засобів потрібно дотримуватись основні правила і норми експлуатації комп'ютерів та периферійних пристроїв під час проведення дослідження.

В загальному, поняття охорона праці в комп'ютерних системах являє собою дотримання всіх вимог і нормативів, що присутні в законодавчих актах про охорону праці. Закони цієї області спрямовані на якісну і безпечну експлуатацію робочих приладів і приміщень, дотримання санітарно-гігієнічних умов праці і захист від інших небезпечних чинників на підприємстві. Ці засоби є складовими дослідження математичного і програмного забезпечення автоматизованої системи підбору команди розробників комп'ютерних систем. В основних законодавчих актах про охорону праці приділяється велика увага поліпшенню умов праці в усіх галузях господарства, впровадженню сучасних засобів техніки безпеки і забезпечення санітарно-гігієнічних умов, що запобігають виробничому травматизму і професійним захворюванням.

Охорона життя і здоров'я людини є пріоритетним напрямком соціальної політики держави. В Україні прийнято закон прямої дії «Про охорону праці», який регламентує захист конституційного права працівників на безпечні умови праці. Законодавство України про охорону праці складається із загальних законів України та спеціальних законодавчих актів. Загальними законами України, що визначають основні положення з охорони праці є Конституція України, Закон України «Про охорону праці», Кодекс законів про працю (КЗпП), Закон України «Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності».

Виконання досліджень кваліфікаційної роботи передбачали використання ПК, де площа та об'єм для одного робочого місця оператора визначається згідно

вимог НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями», зокрема площа повинна становити не менше 6,0 квадратних метрів, об'єм - не менше 20,0 кубічних метрів.

Згідно вимог охорони праці та державних санітарних правил, стіни, стеля та підлога приміщень, в яких розміщені ЕОМ, повинні бути виготовлені з матеріалів, дозволених для оформлення приміщень органами державного санітарно-епідеміологічного нагляду.

Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця операторів (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном), повинні бути надійно захищені діелектричними щитками та сітками з метою недопущення потрапляння працівника під напругу.

Організація робочого місця оператора повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам. У приміщенні, де одночасно експлуатуються понад п'ять електронно-обчислювальних машин (ЕОМ), на помітному та доступному місці мають бути встановленні аварійні резервні вимикачі, які можуть повністю вимкнути електричне живлення приміщення, крім освітлення [11].

Дотримання правил значно знижує наслідки несприятливої дії на працівників шкідливих та небезпечних факторів, які супроводжують роботу з відео-дисплейними терміналами, зокрема можливість зорових, нервово-емоційних переживань, серцево-судинних захворювань. Виходячи з цього, роботодавець повинен забезпечити гігієнічні й ергономічні вимоги щодо організації робочих приміщень для експлуатації електронно-обчислювальних машин (ЕОМ) з ВДТ, робочого середовища, робочих місць з ЕОМ, режиму праці і відпочинку при роботі з ЕОМ тощо, які викладені у нормах НПАОП 0.00-7.15-18. Відповідно до встановлених гігієнічно-санітарних вимог роботодавець зобов'язаний забезпечити в приміщеннях з ЕОМ оптимальні параметри виробничого середовища [11].

Для захисту від прямих сонячних променів, які створюють прямі та відбиті відблиски з поверхні екранів персонального комп’ютера і клавіатури повинні бути передбачені сонцезахисні пристрої, вікна повинні мати жалюзі або штори.

Основні задачі охорони праці при використанні комп'ютерної техніки:

- аналіз впливу факторів виробничого середовища на здоров'я і працездатність користувачів персональних комп’ютерів;

- вдосконалювання методів оцінки працездатності і стану здоров'я користувачів ПК;

- розробка і впровадження організаційно-технічних, гігієнічних і соціально-економічних заходів щодо раціоналізації виробничого середовища;

- розробка і впровадження профілактичних і оздоровчих заходів, що дозволяють зберігати здоров'я людини і підвищувати її працездатність;

- вдосконалення методик навчання користувачів ПК питанням охорони праці.

Вимогам нормативних актів з охорони праці мають відповідати:

- умови праці на кожному робочому місці;

- безпека технологічних процесів, машин, механізмів, обладнання й інших засобів виробництва;

- стан засобів колективного та індивідуального захисту;

- санітарно-побутові умови.

При дослідженні методів і засобів створення програмних систем та проектуванні системи захисту від атак на сервери важливо було проаналізовати та враховати необхідні вимоги щодо охорони праці при використанні електронно-обчислювальної техніки і забезпечити умови для зручної та ефективної роботи працівників.

4.2 Забезпечення захисту працівників суб’єкта господарювання від іонізуючих випромінювань

Працівники, які виконують роботи з радіоактивними речовинами, повинні перебувати під постійним медичним наглядом, використовувати засоби

індивідуального захисту від радіації та прилади індивідуального дозиметричного контролю (універсальні радіометри) для своєчасного виявлення і вимірювання рівня випромінювання [12].

Захищаючись від зовнішнього іонізуючого опромінювання при роботах із закритими джерелами випромінювання, тобто такими, які виключають можливість потрапляння радіоактивних речовин у навколишнє середовище, перш за все необхідно не допустити переопромінення працівників.

Основним способами захисту від цього є:

- зменшення активності джерела, з яким контактують працівники під час конкретного технологічного процесу – досягається шляхом використання речовин із меншою активністю;

- зменшення часу контакту з джерелом випромінювання – досягається шляхом вдосконалення організації робіт і технологічного виробничого процесу та проведення попередніх тренінгів працівників;

- збільшення відстані між людиною і джерелом – використовується, як правило, при контакті з точковим джерелом випромінювання шляхом використання дистанційних універсальних маніпуляторів та інших автоматизованих пристроїв;

- розташування між людиною і джерелом захисного екрану (стаціонарного, пересувного, розбірного, настільного тощо), тобто пристрою, який зменшує інтенсивність випромінювання до безпечного рівня [12].

Для виготовлення екранів, а також для захисту працівників в стаціонарних спорудах, використовується бетон, чавун, сталь, алюміній, скло, свинець та інші матеріали. Від дії рентгенівських променів застосовують екрани зі сталевого листа товщиною 0,5-1 мм або алюмінію товщиною 3 мм, спеціальної гуми. Оглядові вікна виконують з плексигласу товщиною 30 мм або з покритого оловом скла товщиною 9 мм.

Для захисту шкіри від забруднень радіоактивними речовинами та запобігання їх попаданню всередину організму, захисту від альфа і бета-випромінювання передусім застосовуються засоби індивідуального захисту (ЗІЗ) від радіації.

Отже, засоби захисту від радіації використовуються у тих випадках, коли інші заходи недостатньо ефективні: при переході через зони збільшеної інтенсивності випромінювання, при ремонтних та налагоджувальних роботах у аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення.

З урахуванням зазначеного прогнозу на території області може виникнути складна радіаційна обстановка наслідки якої вимагатимуть від органів виконавчої влади, органів місцевого самоврядування, суб'єктів господарювання, на які покладено виконання завдань щодо захисту населення і територій від надзвичайних ситуацій, оперативного реагування та дій [12].

Місцеві органи виконавчої влади, органи місцевого самоврядування, суб'єкти господарювання здійснюють для забезпечення захисту людей від впливу іонізуючих випромінювань наступні заходи:

- приймають згідно з законодавством України рішення щодо застосування на підвідомчій території заходів втручання у разі радіаційних аварій;

- організовують проведення в установленому порядку щорічні обстеження з метою оцінки стану захисту людини від впливу іонізуючих випромінювань та ведення екологічного паспорта підвідомчої території;

- здійснюють організаційне керівництво системою обліку та контролю доз опромінення населення на підвідомчій території;

- організовують контроль за виконанням заходів щодо захисту людини від впливу радіонуклідів, що містяться у будівельних матеріалах;

- затверджують відповідні плани щодо захисту населення від радіаційних аварій та їх наслідків;

- забезпечують постійну готовність засобів оповіщення населення на підвідомчій території про виникнення радіаційної аварії;

- організовують контроль за виконанням заходів щодо захисту населення від радіаційних аварій та їх наслідків;

- забезпечують населення, в місцях його проживання, інформацією щодо рівнів опромінення людини та заходів захисту від впливу іонізуючих випромінювань, що виконуються на підвідомчій території;

- розроблюють та впроваджують програми захисту людей від впливу іонізуючих випромінювання;

- здійснюють оповіщення населення у разі виникнення радіаційної аварії та інформування про рятувальні та профілактичні заходи у зв’язку з цим.

Для виконання вищезазначених заходів залучаються органи управління, сили і засоби обласної територіальної та функціональних підсистем єдиної державної системи цивільного захисту (далі – ЄДС ЦЗ), порядок дій яких визначено Планом реагування на надзвичайні ситуації, пов'язаних з викидом радіоактивних речовин.

Режими захисту робітників і службовців на суб'єктах господарювання вводяться в дію рішенням керівників об'єктів. Незалежно від місця розміщення суб'єкту господарювання (в населеному пункті або за його межами) на його території вводиться в дію свій режим захисту з урахуванням рівнів радіації, виміряних на об'єкті, і реального ступеню захисту працівників і службовців.

При виникненні комунальної радіаційної аварії окрім термінових робіт щодо стабілізації радіаційного стану (включаючи відновлення контролю над джерелом) місцеві органи виконавчої влади, органи місцевого самоврядування, суб'єкти господарювання одночасно здійснюють заходи, спрямовані на:

- зведення до мінімуму кількості осіб з населення, які зазнають аварійного опромінення;

- запобігання чи зниження індивідуальних і колективних доз опромінення населення;

- запобігання чи зниження рівнів радіоактивного забруднення продуктів харчування, питної води, сільськогосподарської сировини і сільгоспугідь, об'єктів довкілля (повітря, води, ґрунту, рослин тощо), а також будівель і споруд.

Для населення, робітників та службовців суб'єктів господарювання, які можуть потрапити в зону випадіння радіоактивних опадів, доцільно завчасно, виходячи з конкретних місцевих умов, розрахувати варіанти режимів радіаційного захисту [13].

З урахуванням вищезазначеного, режими радіаційного захисту вводяться в дію місцевими органами виконавчої влади, органами місцевого самоврядування,

суб'єктами господарювання з метою захисту людей від впливу іонізуючого випромінювання у разі загрози або виникнення надзвичайних ситуацій, пов'язаних з радіаційними аваріями.

ВИСНОВКИ

Забезпечення безпеки поштових серверів від атак, зокрема SYN Flood, є одним з завданням у сфері безпеки інформаційних технологій. Дана магістерська робота мала на меті створення та перевірку ефективності засобу захисту від впливу SYN Flood атак на поштовий сервер.

Об'єктом дослідження був поштовий сервер, який є ключовим елементом для обміну електронною поштою та зберігання користувацьких даних. Дослідження включало аналіз існуючих методів захисту, розробку системи захисту на основі операційної системи FreeBSD та брандмауера PF, а також валідацію та дослідження ефективності розробленого програмного рішення.

В рамках роботи було створено та впроваджено заходи захисту, а також проведено оцінку їх ефективності в реальних умовах. Було реалізовано комплексний засіб захисту, який поєднує ефективні технології та механізми реагування на SYN Flood атаки. Розроблений механізм функціонує у режимі реального часу, автоматично блокуючи спроби атак та відправляючи повідомлення про їх виявлення за допомогою месенджера Signal.

Ця робота важлива у контексті підвищення доступності та безвідмовності роботи поштових серверів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Simple Mail Transfer Protocol [Електронний ресурс]. — URL: https://datatracker.ietf.org/doc/html/rfc5321 (дата звернення: 19.11.2023).

2. TCP SYN Flooding Attacks and Common Mitigations [Електронний ресурс]. — URL: https://datatracker.ietf.org/doc/html/rfc4987#appendix-A (дата звернення: 19.11.2023).

3. SYN flood attack [Електронний ресурс]. — URL: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/ (дата звернення: 19.11.2023).

4. Transmission Control Protocol [Електронний ресурс]. — URL: https://datatracker.ietf.org/doc/html/rfc793 (дата звернення: 19.11.2023).

5. FreeBSD Documentation [Електронний ресурс]. — URL: https://docs.freebsd.org/en/ (дата звернення: 19.11.2023).

6. Postfix Documentation [Електронний ресурс]. — URL: http://www.postfix.org/documentation.html (дата звернення: 19.11.2023).

7. Parrot Security Edition [Електронний ресурс]. — URL: https://parrotsec.org/ (дата звернення: 19.11.2023).

8. Metasploit Documentation [Електронний ресурс]. — URL: https://docs.metasploit.com/ (дата звернення: 19.11.2023).

9. FreeBSD Manual Pages – PF [Електронний ресурс]. — URL: https://man.freebsd.org/cgi/man.cgi?pf.conf (дата звернення: 19.11.2023).

10. Documentation Ruby [Електронний ресурс]. — URL: https://www.ruby-lang.org/en/documentation/ (дата звернення: 05.11.2023).

11. Жидецький В.Ц. Охорона праці користувачів комп′ютерів. Львів: Афіша, 2011. 176 с.

12. Желібо Є. П., Сагайдак І. С. Безпека життєдіяльності. Навчальний посібник для аудиторної та практичної роботи. К.:ЕКОМЕН. 2011. 200 с.

13. Депутат О. П., Коваленко І. В., Мужик І. С. Цивільна оборона. Навчальний посібник. За редакцією полковника В.С. Франчука. Львів: Афіша. 2000. 336 с.

Додаток А – Публікація

Демчук Василь Сергійович
здобувач вищої освіти
факультету комп'ютерно-інформаційних систем і програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Тимощук Віталій Дмитрович
здобувач вищої освіти
факультету прикладних інформаційних технологій та електроінженерії
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

ЗАСОБИ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАК

В мережі Інтернет SYN flood атака - це одна із найпоширеніших видів DOS атак на мережеві системи, спрямованих на переповнення сервера запитами на встановлення TCP-з'єднання. Для запобігання та мінімізації впливу таких атак існують різноманітні заходи захисту, що охоплюють технічні рішення та програмні механізми [1].

Один із ефективних способів захисту - використання SYN Cookies. Це технічне рішення дозволяє серверу обробляти підозрілі запити на встановлення з'єднання, не зберігаючи повну інформацію про них, тим самим запобігаючи переповненню пам'яті.

Ще одним засобом є збільшення розміру черги (Backlog), що дозволяє серверу тимчасово зберігати більшу кількість з'єднань в черзі та знижує ймовірність успішної реалізації атаки. Зменшення часу очікування на отримання підтвердження SYN-пакета шляхом скорочення SYN-RECEIVED Timer також сприяє у захисті від SYN flood атак.

Використання додаткових механізмів, таких як відновлення найстаріших напіввідкритих TCP-контекстів (TCB) та застосування SYN Cache сприяє ефективному управлінню з'єднаннями та ресурсами пам'яті.

У рамках даної роботи було розроблено та впроваджено захисне програмне забезпечення, базоване на технології SYNPROXY в брандмауері PF [2]. Цей комплексний програмний засіб поєднує в собі ефективні технології та механізми реагування на атаки типу SYN flood. Реалізований механізм функціонує у реальному часі, автоматично блокуючи спроби атак та надсилаючи повідомлення про виявлені атаки за допомогою месенджера Signal.

Застосування сукупності технічних та програмних рішень, таких як SYN Cookies, збільшення Backlog, скорочення SYN-RECEIVED Timer, використання SYN Cache, і програмного рішення з використанням SYNPROXY дозволяє ефективно нейтралізувати SYN flood атаки, забезпечуючи надійний захист мережевих ресурсів.

Список використаних джерел:

1. TCP SYN Flooding Attacks [Електронний ресурс]. — URL: https://datatracker.ietf.org/doc/html/rfc4987#appendix-A (дата звернення: 19.11.2023).
2. FreeBSD Manual Pages – PF [Електронний ресурс]. — URL: https://man.freebsd.org/cgi/man.cgi?pf.conf (дата звернення: 19.11.2023).

Додаток Б – Лістинг файлу synflood_check.rb

```
#!/usr/bin/env ruby


require 'open3'


class SynFloodCheck
  CONFIG_FILE =
'/home/root/synfloodsmtp/synflood_check.conf'.freeze
  OUTPUT_FILE = '/etc/synfloodip'.freeze
  BLOCKLIST_COMMAND = 'pfctl -t synfloodsmtp -T add -f'.freeze


  def initialize
    # Check if the configuration file exists
    check_config_file
    # Load configuration values
    load_config
  end


  def check
    # Fetch the count of state occurrences
    count = fetch_state_count
    puts count
    # If count exceeds the maximum allowed count, perform blocking
and alert actions
    if count > @max_allowed_count
      unique_ips = extract_unique_ips
      puts unique_ips
      block_ips(unique_ips)
      send_alert(count, unique_ips.count)
    else
      puts "No action needed."
    end
  end
```

```
  private

  def check_config_file
    return if File.exist?(CONFIG_FILE)

    puts "Error: Configuration file not found."
    exit
  end

  def load_config
    # Read configuration lines from the file
    config_lines = File.readlines(CONFIG_FILE)
    # Extract the maximum allowed count and state to check from
the configuration
    @max_allowed_count = config_lines.first[/max_allowed_count =
(\d+)/, 1].to_i
    @state_to_check = config_lines.last[/state_to_check =
"([^"]+)"/, 1]
  end

  def fetch_state_count
    # Execute the command and capture its output
    stdout, _stderr, status = Open3.capture3('pfctl -s state')

    unless status.success?
      puts "Error: Unable to execute pfctl -s state"
      exit
    end

    # Count the occurrences of the specified state in the output
    stdout.scan(@state_to_check).count
  end
```

```
  def extract_unique_ips
    # Execute the command and capture its output
    stdout, _stderr, _status = Open3.capture3('pfctl -s state')
    # Extract unique IP addresses with the specified state from the output
    stdout.scan(/all [a-z]+ \d+\.\d+\.\d+\.\d+:\d+ <- (\d+\.\d+\.\d+\.\d+):\d+.*#{@state_to_check}/)
          .map { |match| match[0] }
          .uniq
  end

  def block_ips(ips)
    # Write the unique IP addresses to a file
    File.open(OUTPUT_FILE, 'a') do |file|
      ips.each { |ip| file.puts(ip) }
    end

    # Use the command to add the IP addresses to the blocklist table
    system("#{BLOCKLIST_COMMAND} #{OUTPUT_FILE} > /root/mailscript/addtable 2>&1")
  end

  def send_alert(total_ips, unique_ips)
    # Compose an email subject with the current date, time, and hostname
    subject = compose_subject
    # Compose the message for the alert
    signal_message = "SYNFLOOD SMTP Attack. Number of connections - #{total_ips}. IP unique - #{unique_ips}"

    # Send the alert using the Signal messaging app
    `signal-cli -u +380XXXXXXXXX send -m "#{signal_message} #{subject}" +380YYYYYYYYY`
  end
```

```
  def compose_subject
    # Return a string with the current date, time, and hostname
    "DATE: #{Time.now.strftime('%Y-%m-%d')} TIME:
#{Time.now.strftime('%H:%M:%S')} #{"mail.localserver.lan".strip}"
  end
end


# Create a new instance of the SynFloodCheck class and perform the
check
checker = SynFloodCheck.new
checker.check
```

Додаток В – Файл сервісу `synflood_check_service`

```
#!/bin/sh

# PROVIDE: synflood_check_service
# REQUIRE: LOGIN
# KEYWORD: nojail

. /etc/rc.subr

name="synflood_check_service"
rcvar=synflood_check_service_enable

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

synflood_check_service_start()
{
    while :; do
     /usr/local/bin/ruby   /root/synfloodsmtp/synflood_check.rb   >>
/var/log/synflood_check.log
     sleep 6
    done &
     echo $! > /var/run/${name}.pid
}

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



synflood_check_service_status()
{
    if [ -e "/var/run/${name}.pid" ]; then
```

```
     echo "synflood check service is running with PID `cat
/var/run/${name}.pid`."
    else
     echo "synflood check service is not running."
    fi
    exit 0
}


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