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

бакалавр
(освітній рівень)

на тему: "Захист від DDOs атак за допомогою утиліти Iptables на базі ОС CentOS"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Приймаченко Максим Євгенійович
підпис (прізвище та ініціали)

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

Нормоконтроль Тимощук Д.І.
підпис (прізвище та ініціали)

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

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

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)

ло

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Приймаченку Максиму Євгенійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Захист від DDOs атак за допомогою утиліти Iptables на базі ОС CentOS

Керівник роботи Лечаченко Тарас Анатолійович, PhD доктор філософії.,
асистент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «03» 04 2024 року № 4/7-349

2. Термін подання студентом завершеної роботи 14.06.2024

3. Вихідні дані до роботи Вимоги до операційної системи CentOS

4. Зміст роботи (перелік питань, які потрібно розробити)
Проаналізувати DDOs атаки та їх наслідки.
Проаналізувати захист від DDOs атак в операційній системі CentOS
Розробити та протестувати захист серверу за допомогою утиліти iptables
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема, мета. Що таке DoS і DDoS атака. Види DDoS атак. Засоби захисту. CentOS. Iptables. Команди та модулі. Реалізація.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко Ю.С., доцент кафедри МТ		

7. Дата видачі завдання 29.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01 – 01.01	Виконано
2.	Підбір джерел для аналізу DDOs атаки та їх наслідки	30.01 – 04.02	Виконано
3.	Опрацювання джерел в галузі дослідження	05.02 – 19.02	Виконано
4.	Провести аналіз методів захисту від DDoS атаки	22.02 – 11.03	Виконано
5.	Здійснення DDoS атаки на Apache-сервер	15.03-24.03	Виконано
6.	Налаштування правил в утиліті iptables	25.02 – 09.04	Виконано
7.	Оформлення розділу «DDoS атаки та їх наслідки»	10.02 – 04.03	Виконано
8.	Оформлення розділу «Захист від DDOs атак за допомогою утиліти iptables на базі ОС CentOS»	26.03 – 03.05	Виконано
9.	Оформлення розділу «Налаштування та тестування утиліти iptables від botnet трафіку»	12.04-19.04	Виконано
10.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	25.04 – 09.05	Виконано
11.	Оформлення кваліфікаційної роботи	23.05 – 07.06	Виконано
12.	Нормоконтроль	10.06 – 14.06	Виконано
13.	Перевірка на плагіат	17.06.2024	Виконано
14.	Попередній захист кваліфікаційної роботи	19.06.2024	Виконано
15.	Захист кваліфікаційної роботи	27.06.2024	

Студент _____ Приймаченко М.Є.
(підпис) (прізвище та ініціали)

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

АНОТАЦІЯ

Захист серверу на CentOS від DDoS атак // Кваліфікаційна робота ОР «Бакалавр» // Приймаченко Максим Євгенійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-42 // Тернопіль, 2024 // С. 50 , див. рисунок – 23, табл. – 2 , кресл. – - , додат. – -.

КЛЮЧОВІ СЛОВА: CentOS, Firewall, iptables,botnet, synflood, DDoS.

Кваліфікаційна робота присвячена дослідженню та захисту сервера на базі операційної системи CentOS 7 від DDoS атак за допомогою iptables. Атаки типу DDoS представляють значну загрозу для безпеки інформаційних систем, спричиняючи відмову у доступі до ресурсів та порушуючи їхню стабільну роботу. У роботі розглядаються різні механізми та заходи безпеки для ефективного захисту сервера від цих атак.

В першій частині роботи детально описані поняття та наслідки DDoS атак, а також загальні методи захисту від них. Друга частина присвячена огляду операційної системи CentOS 7, вибору та встановленню iptables, а також основним командам та синтаксису для налаштування правил фільтрації трафіку. Третя, практична частина, містить опис конкретних кроків щодо налаштування захисту сервера за допомогою iptables.

Розроблені методи та налаштування забезпечують надійний захист сервера від DDoS атак, підвищують рівень його безпеки та стабільності. Результати роботи можуть бути корисними для системних адміністраторів та фахівців з інформаційної безпеки. Також вони можуть використовуватися в навчальних цілях для студентів, які вивчають питання безпеки операційних систем та методи захисту від мережевих атак.

ABSTRACT

Server protection on CentOS from DDoS attacks // Qualification work of the OR "Bachelor" // Maksym Evgeniyovych Pryimachenko // Ivan Pulyuy Ternopil National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, SBc-42 Group // Ternopil, 2024 // P. 50, fig. - 23, tab. – 2, armchair. – - , add. – -.

KEYWORDS: CentOS, Firewall, iptables, botnet, synflood, DDoS.

The qualification work is devoted to research and protection of a server based on the CentOS 7 operating system from DDoS attacks using iptables. DDoS-type attacks represent a significant threat to the security of information systems, causing denial of access to resources and disrupting their stable operation. The work considers various mechanisms and security measures to effectively protect the server from these attacks.

The first part of the work describes in detail the concepts and consequences of DDoS attacks, as well as general methods of protection against them.

The second part covers an overview of the CentOS 7 operating system, selecting and installing iptables, and the basic commands and syntax for configuring traffic filtering rules. The third, practical part, contains a description of specific steps for setting up server protection using iptables.

The developed methods and settings provide reliable server protection against DDoS attacks, increase the level of its security and stability. The results of the work can be useful for system administrators and information security specialists. They can also be used for educational purposes for students, which study the security of operating systems and methods of protection against network attacks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DDoS	—	Distributed Denial of Service
SYN	—	Synchronize (флаг TCP-з'єднання)
ICMP	—	Internet Control Message Protocol
DoS	—	Denial of Service
NAT	—	Network Address Translation
UDP	—	User Datagram Protocol
TCP	—	Transmission Control Protocol
HTTP	—	Hypertext Transfer Protocol
HTTPS	—	Hypertext Transfer Protocol Secure

ВСТУП

Сучасні інформаційні системи залежать від безперервного та надійного доступу до даних та ресурсів. Операційна система CentOS 7 є важливим елементом інфраструктури багатьох організацій, забезпечуючи цілісність, конфіденційність та доступність їх даних. Однак DDoS атаки можуть становити значну загрозу для безпеки та стабільності роботи серверів.

DDoS (Distributed Denial of Service) атаки являють собою один з найпоширеніших методів порушення роботи системи, заснований на надмірному навантаженні на сервер за допомогою одночасних запитів з багатьох джерел. Успішна реалізація такої атаки може призвести до відмови у наданні послуг, втрати доступу до важливих даних та значних фінансових збитків.

Ця кваліфікаційна робота має на меті дослідити поняття DDoS атак, їх наслідки та можливі методи захисту сервера на базі операційної системи CentOS 7 від таких атак. Основний акцент буде зроблено на використанні iptables для забезпечення ефективного захисту від DDoS атак.

У роботі буде розглянуто встановлення та налаштування iptables на CentOS 7, включаючи обмеження кількості одночасних з'єднань від одної IP-адреси, обмеження швидкості з'єднань, використання модуля tcp_syncookies для захисту від SYN-флуд атак, та налаштування розміру черги з'єднань для зменшення ефективності атак типу Slowloris[7]. Також буде розглянуто використання модуля mod_reqtimeout для веб-сервера Apache, який дозволяє обмежити час очікування.

Додатково, буде показано, як зберегти налаштування iptables для забезпечення їх збереження після перезавантаження системи, а також як перевіряти та моніторити сервер на наявність підозрілої активності для коригування правил iptables при необхідності.

Результати цієї кваліфікаційної роботи сприятимуть підвищенню рівня захищеності сервера на базі операційної системи CentOS 7 від DDoS атак, допомагаючи забезпечити безпеку та надійність інформаційної інфраструктури організацій.

1 ВИДИ DDOS АТАК ТА ЇХ ВПЛИВ

1.1 Визначення DDoS атаки

Розподілена відмова в обслуговуванні (DDoS) - це тип DOS-атаки, коли декілька систем, заражених трояном, націлюються на певну систему, що спричиняє DoS-атаку.

DDoS-атака[1] використовує декілька серверів та інтернет-з'єднань для переповнення цільового ресурсу. DDoS-атака - це одна з найпотужніших видів зброї на кібер-платформі. Коли ви дізнаєтеся про те, що веб-сайт не працює, це, як правило, означає, що він став жертвою DDoS-атаки. Це означає, що хакери атакували наш веб-сайт або комп'ютер, нав'язавши великий трафік. Таким чином, веб-сайт або комп'ютер вийшов з ладу через перевантаження.

Приклад: У 2000 році за однією з перших DDoS-атак стояв Майкл Калче, 15-річний хлопець, який використовував онлайн ім'я "Mafiaboy". Він зламав комп'ютерні мережі різних університетів. Він використовував їхні сервери(див. рисунок 1.1) для проведення DDoS-атаки, яка вивела з ладу кілька веб-сайтів, таких як eBay і Yahoo. У 2016 році Dyn зазнав масованої DDoS-атаки, яка вивела з ладу найбільші веб-сайти та сервіси, такі як Netflix, PayPal, Amazon та GitHub.

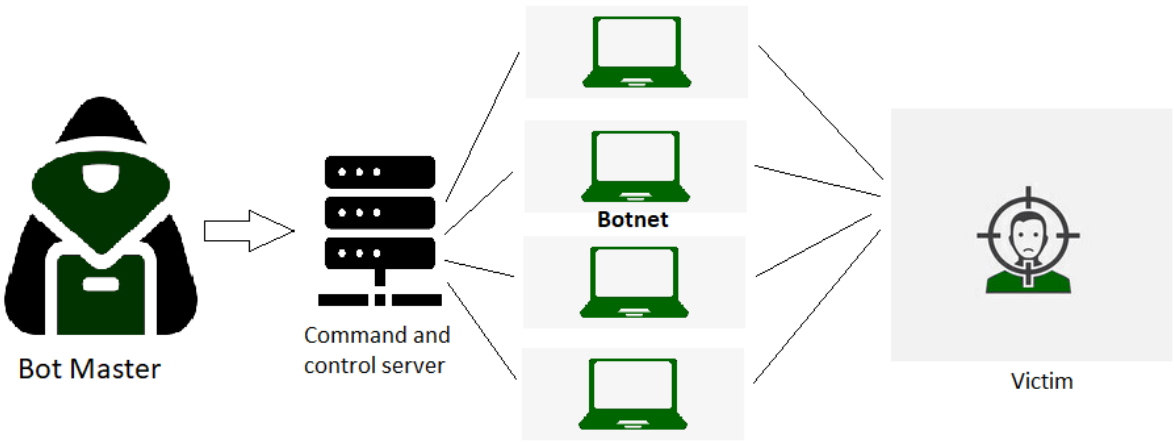

Рисунок 1.1 — Проведення botnet атаки на ціль

DoS розшифровується як "відмова в обслуговуванні"[8]. Це тип атаки на сервіс, який порушує його нормальне функціонування і перешкоджає іншим

користувачам отримати до нього доступ. Найчастіше об'єктом DoS-атаки є онлайн-сервіс[8], наприклад, веб-сайт, хоча атаки також можуть бути спрямовані на мережі, комп'ютери або навіть окремі програми (див. таблицю 1.1).

Таблиця 1.1 — Різниця між DoS і DDoS

DoS	**DDoS**
DoS - це атака на відмову в обслуговуванні.	DDoS розшифровується як розподілена атака на відмову в обслуговуванні.
При Dos-атаці одна система атакує систему-жертву.	У DDoS-атаці декілька систем атакують систему жертви.
Комп'ютер жертви завантажується з пакета даних, надісланого з одного місця.	Комп'ютер жертви завантажується з пакету даних, надісланих з декількох місць.
Dos-атака повільніша в порівнянні з DDoS-атакою.	DDoS-атака працює швидше, ніж Dos-атака.
Може бути легко заблокована, оскільки використовується лише одна система.	Важко заблокувати цю атаку, оскільки декілька пристроїв надсилають пакети і атакують з різних місць.
У DOS-атаці використовується лише один пристрій з інструментами DOS-атаки.	У DDoS-атаці volumeBots використовуються для одночасної атаки.
DOS-атаки легко відстежити.	DDOS-атаки важко відстежити.
Типи DOS-атак: 1. Атаки на переповнення буфера 2. Пінг смерті або ICMP-флуд 3. Teardrop-атака 4. Атака Flooding	Типи DDOS-атак 1. Об'ємні атаки 2. Фрагментаційні атаки 3. Атаки на рівні додатків 4. Атаки на протокол.

Існують різні типи DDoS-атак, згадані нижче:

1. Об'ємні атаки: Об'ємні атаки є найпоширенішою формою DDoS-атак. Вони використовують бот-мережу для перевантаження мережі або сервера великим трафіком, який перевищує можливості мережі з обробки трафіку. Ця атака перевантажує ціль величезною кількістю небажаних даних. Це призводить до втрати пропускної здатності мережі і може призвести до повної відмови в обслуговуванні.

2. Протокольні атаки: Атаки на TCP-з'єднання використовують уразливість в послідовності TCP-з'єднань, яку зазвичай називають тристороннім рукостисканням між хостом і сервером. Робота пояснюється наступним чином. Цільовий сервер отримує запит на початок з'єднання з рукостисканням. В цій атаці рукостискання ніколи не виконується. Підключений порт залишається зайнятим і недоступним для обробки будь-яких подальших запитів. Тим часом кіберзлочинець продовжує надсилати численні запити, перевантажуючи всі робочі порти і вимикаючи сервер.

3. Атаки на додатки: Атаки на рівні додатків (атаки 7-го рівня) націлені на програми жертви, які працюють повільніше. Таким чином, вони можуть спочатку виглядати як легітимні запити від користувачів, і жертва не може на них відповісти. Ці атаки націлені на рівень, на якому сервер генерує веб-сторінки і відповідає на HTTP-запити. Атаки на рівні додатків поєднуються з іншими видами DDoS-атак, спрямованих на додатки, а також на мережу та пропускну здатність. Ці атаки є загрозливими, оскільки компаніям складніше їх виявити.

4. Фрагментаційні атаки: Кіберзлочинець використовує фрагментарність в процесі фрагментації дейтаграм, в якому IP-дейтаграми розбиваються на менші пакети, передаються через мережу, а потім знову збираються. У таких атаках фальшиві пакети даних неможливо зібрати знову.

Як працюють DDoS-атаки?

Логіка DDoS-атаки дуже проста, хоча атаки можуть сильно відрізнятися одна від одної. Мережеві з'єднання складаються з різних рівнів моделі OSI. Різні типи DDoS-атак зосереджуються на певних рівнях. Приклади наведені нижче:

Рівень 3: Мережевий рівень - атаки відомі як Smurf-атаки, ICMP-флуд та IP/ICMP-фрагментація.

Рівень 4: Транспортний рівень - атаки включають SYN Floods, UDP Floods[9] і TCP Connection Exhaustion.

Рівень 7: прикладний рівень - HTTP-шифровані атаки.

1.2 Цілі та наслідки DDoS атак

Незалежно від розміру чи галузі, практично будь-яка організація[2], що має публічний веб-сайт, є вразливою до DDoS-атак. За своєю природою публічні веб-сайти призначені для запрошення відвідувачів, що робить їх потенційною мішенню для зловмисників. Неконтрольовані та погано захищені мережі є особливо вразливими, оскільки в них відсутні механізми безпеки, які б сповіщали адміністраторів про вторгнення, аномальну поведінку або коливання обсягу трафіку.

Але хто стане мішенню? Хоча всі галузі застерігають готуватися до "коли, а не якщо", деякі з них є більш вірогідними мішенями, ніж інші, просто через характер їхнього бізнесу. У випадку з фінансовими послугами DDoS-атаки часто є лише одним з етапів багаторівневої атаки, яку зазвичай використовують як відволікаючий маневр для більш масштабної атаки, спрямованої на викрадення інформації про облікові записи або заволодіння ними. У випадку з провайдерами веб-хостингу та хостинг-провайдерами, їхні клієнти, хоча й не є безпосередньою метою, в кінцевому підсумку стають супутніми жертвами таких атак. Іншими очевидними цілями є веб-сайти роздрібної торгівлі та електронної комерції, чиї доходи значною мірою залежать від того, наскільки їхні веб-сайти доступні та швидко реагують на запити.

Фахівці з безпеки компаній, що надають фінансові послуги, оцінили середню вартість DDoS-атаки на рівні додатків у понад 9 мільйонів доларів США. Навіть найнижча оцінка (з державного сектору) склала $5 млн. Сайти, доходи яких значною мірою залежать від Інтернету, наприклад, сайти електронної комерції, ігрові сайти або сайти веб-хостингу, можуть втрачати

сотні тисяч доларів щохвилини, поки їхні сайти не працюють. І для того, щоб компанія зазнала великих фінансових втрат, не обов'язково, щоб сайт повністю виходив з ладу.

Витрати на відновлення та компенсацію. Усі організації, незалежно від того, залежать вони від доходів чи ні, матимуть певну суму витрат на усунення наслідків аварії. Деякі організації, наприклад, провайдери веб-хостингу, чиї перебої в роботі впливають на тисячі клієнтів, можуть понести значні компенсаційні витрати.

Втрата клієнтів та довіри клієнтів. У світі, де будь-який мислимий продукт можна придбати лише кількома кліками миші, втрата онлайн-клієнтів може бути фатальною. Покупці непостійні, і ніщо не відштовхне їх швидше, ніж недоступний сайт, який не реагує на запити. Коли клієнти залишають погано працюючий або недоступний сайт, вони втрачають не лише миттєвий дохід, але й потенційних лояльних клієнтів, які можуть перейти на сайт конкурента і більше ніколи не повернутися.

Репутація та ділова репутація. Жоден бізнес не хоче потрапляти в заголовки газет через збої в системі безпеки. Клієнти особливо менш пробачливі до таких компаній, як банки та бюро кредитних історій, для яких довіра є важливим фактором. Деяким компаніям може знадобитися час, щоб відновити свою репутацію та бренд після DDoS-атаки, особливо якщо атака використовується як відволікаючий маневр для витоку даних, під час якого персональні дані або дані клієнтів викрадаються або компрометуються.

Загроза судового позову. Організації, які стали жертвами DoS-атак[8], рідко стають об'єктами судових позовів з боку споживачів, але вони можуть бути оскаржені клієнтами, з якими у них укладені угоди про рівень обслуговування (SLA). Уявіть собі велику компанію, яка двічі на місяць отримує заробітну плату від програми, що надається за принципом "програмне забезпечення як послуга". Якщо ця програма вийде з ладу під час виплати зарплати і чеки будуть затримані, провайдер може бути притягнутий до судової відповідальності. Те саме стосується провайдерів хмарних або веб-сервісів - якщо їхні послуги

спричиняють збій у роботі сотень тисяч веб-сайтів інших компаній, вони ризикують отримати позов від цих клієнтів про відшкодування збитків.

З точки зору захисника, очевидних ознак атаки може бути небагато. Часто організація не знає про атаку доти, доки служба підтримки клієнтів не почне отримувати численні скарги на веб-сайт, який повільно реагує на запити, має технічні проблеми або взагалі недоступний. Однак слід пам'ятати, що не всі типи DDoS-атак мають ці ознаки, оскільки деякі з них розроблені таким чином, щоб виглядати як нешкідливий трафік, що має нормальний вигляд. Такі види атак, які часто не споживають багато пропускної здатності, не викликають тривоги, тому їх набагато складніше виявити і усунути без аналізу трафіку.

1.3 Основні методи захисту від DDoS атак

Хостинг-провайдери пропонують різні рівні захисту для зменшення ризиків, пов'язаних з DDoS-атаками[3]. До них відносяться

1. Базовий захист Хостинг-провайдери пропонують базовий захист від DDoS-атак, обмежуючи кількість запитів, які можуть бути зроблені до сервера. Хоча це може допомогти запобігти невеликим атакам, але часто є недостатнім для захисту від більш масштабних атак.

2. Розширений захист Розширений захист від DDoS використовує такі методи, як фільтрація трафіку для виявлення та блокування шкідливого трафіку, що потрапляє в мережу. Крім того, він використовує алгоритми машинного навчання для виявлення та реагування на нові загрози. Цей тип захисту підходить для підприємств середнього та великого бізнесу.

3. Захист на рівні підприємства Захист на рівні підприємства використовує багаторівневі захисні механізми для захисту від складних атак, які включають різні вектори або джерела. Цей підхід включає моніторинг, розвідку загроз, реагування на інциденти тощо.

Існує кілька методів захисту від DDoS-атак, які дозволяють запобігти або пом'якшити їх наслідки, зокрема:

1. Обмеження трафіку до адрес, яким довіряють і які відомі, може допомогти запобігти перериванню роботи сервісів внаслідок DDoS-атаки. Крім того, послуги, які не потрібні, можна вимкнути або заблокувати аналогічним чином.

2. Хмарний захист передбачає використання стороннього сервісу для моніторингу та фільтрації вхідного та вихідного трафіку на сервер або веб-сайт. Такий підхід забезпечує додатковий рівень безпеки, виявляючи та зупиняючи шкідливі запити.

3. Системи запобігання вторгненням (IPS) аналізують шаблони мережевого трафіку в режимі реального часу і можуть ідентифікувати зловмисну активність, яка може призвести до DDoS-атаки. Цей підхід блокує відомий шкідливий трафік і може зупинити атаку на її шляху.

4. Мережа доставки контенту (CDN) розподіляє вхідний трафік на кілька різних серверів, щоб зменшити навантаження на один сервер. Цей підхід може допомогти запобігти DDoS-атакам, перерозподіляючи трафік між кількома серверами.

5. Контролери доставки додатків (ADC) розподіляють трафік між різними серверами і керують запитами, одночасно захищаючи від DDoS-атак. Крім того, використання брандмауера веб-додатків може допомогти заблокувати трафік з підозрілих джерел.

DDoS-атаки є значною загрозою для сучасної цифрової інфраструктури, включаючи веб-сайти та мережі. Їхні наслідки можуть бути складними, тому важливо розуміти та впроваджувати правильні рішення. Хостинг-провайдери пропонують кілька рівнів захисту, тому важливо інвестувати в адекватні заходи безпеки для захисту цифрових активів. Обмеження трафіку, хмарний захист, IPS, CDN та ADC - ось деякі з методів забезпечення захисту від DDoS-атак. Організаціям слід застосовувати багаторівневий і проактивний підхід для постійного захисту своєї цифрової інфраструктури.

2 ЗАХИСТ СЕРВЕРА CENTOS7 ВІД DDOS АТАК

2.1 Огляд операційної системи CentOS7

CentOS 7, створена на основі вихідного коду Red Hat Enterprise Linux (RHEL), є надійною та стабільною операційною системою в екосистемі Linux[4]. Вона успадкувала стабільність і функції безпеки RHEL, забезпечуючи при цьому безкоштовну альтернативу з відкритим вихідним кодом. Ця ОС включає в себе найновіше ядро Linux, пропонуючи підтримку сучасного обладнання, вдосконалені механізми безпеки та покращену продуктивність. Крім того, вона забезпечує послідовне і передбачуване середовище для системного адміністрування.

CentOS 7 має багату історію, яка бере свій початок від попереднього дистрибутива, Red Hat Enterprise Linux (RHEL). Проект був ініційований з метою створення стабільної, керованої спільнотою та безкоштовної альтернативи RHEL, яка вимагає підписки на офіційну підтримку. Розробка включала ретельний процес адаптації та компіляції вихідного коду RHEL. Команда ретельно видалила з RHEL всі матеріали, захищені торговими марками і авторськими правами, забезпечивши при цьому сумісність і бінарну еквівалентність. Це дозволило CentOS слугувати швидкою заміною RHEL, надаючи користувачам стабільну та безпечну операційну систему без пов'язаних з нею витрат на ліцензування. Участь спільноти відіграла вирішальну роль у формуванні платформи. Проект отримав вигоду від активної та пристрасної бази користувачів, які надавали відгуки, звіти про помилки та робили внесок у процес розробки. Результатом спільних зусиль спільноти система стала надійна та високонадійна операційна система, яка широко використовується у різних галузях та організаціях. CentOS 7 стала важливою віхою в історії проекту, продовжуючи успіх і популярність своєї попередниці, CentOS 6. Випущена в липні 2014 року, ОС принесла численні покращення та оновлення, зміцнивши свої позиції як надійного вибору для системних адміністраторів великих і малих організацій.

CentOS 7 має кілька переваг, які роблять її кращим вибором для системних адміністраторів:

Система надає стабільну та надійну платформу, що особливо корисно для корпоративних середовищ, де час роботи та її надійність мають першорядне значення.

ОС розроблено з урахуванням бінарної сумісності з RHEL. Ця сумісність дозволяє системним адміністраторам легко мігрувати між CentOS і RHEL без проблем сумісності, забезпечуючи гнучкість і безперервність.

Платформа може похвалитися великим репозиторієм програмних пакетів, що охоплює широкий спектр програм, бібліотек та інструментів. Ця всеосяжна колекція спрощує встановлення програмного забезпечення і дозволяє адміністраторам задовольнити різноманітні системні вимоги.

CentOS 7 надає пріоритет безпеці за рахунок включення надійних функцій, таких як SELinux (Security-Enhanced Linux), обов'язковий механізм контролю доступу, який обмежує доступ на основі заздалегідь визначених політик безпеки. Він також виграє від частих оновлень та виправлень безпеки.

ОС дуже добре налаштовується, що дозволяє системним адміністраторам пристосовувати свої установки до конкретних вимог. Чи то вибір груп пакунків під час встановлення, чи то точне налаштування конфігурації системи, Платформа забезпечує гнучкість, необхідну для різноманітних середовищ.

Yum (Yellowdog Updater Modified) слугує менеджером пакунків за замовчуванням для CentOS 7. Він спрощує встановлення, оновлення та видалення програмного забезпечення, керуючи залежностями та вирішуючи конфлікти. Yum надає інтерфейс командного рядка, який дозволяє адміністраторам шукати пакунки, отримувати інформацію та ефективно виконувати різні операції з керування пакунками. Він також підтримує багатий набір опцій і плагінів, які розширюють його функціональність.

CentOS 7 пропонує надійну систему керування репозиторіями, яка дозволяє адміністраторам налаштовувати та керувати репозиторіями програмного забезпечення. Сховища слугують централізованим місцем, де пакунки

зберігаються і стають доступними для встановлення. Налаштувавши сховища, адміністратори отримують доступ до великої колекції пакунків. Вони можуть легко встановлювати нове програмне забезпечення, оновлювати наявні пакунки і забезпечувати відповідність системи найновішим патчам безпеки та виправленням помилок. Yum спрощує цей процес, автоматично вирішуючи залежності, забезпечуючи безпроблемне встановлення.

Yum спрощує процес оновлення встановлених пакунків до новіших версій. Адміністратори можуть використовувати команду "yum update" для отримання та встановлення останніх оновлень для всіх встановлених пакунків. Це гарантує, що у системі будуть встановлені найновіші функції, виправлення помилок і патчі безпеки. Крім того, Yum надає інструменти для видалення непотрібних пакунків із системи. Команда "yum remove" дозволяє адміністраторам видаляти пакунки та пов'язані з ними залежності, звільняючи місце на диску та оптимізуючи системні ресурси.

Для підтримки безпеки і стабільності системи дуже важливо постійно оновлювати систему. Адміністратори повинні використовувати інфраструктуру оновлень CentOS, щоб забезпечити своєчасне встановлення патчів і виправлень безпеки. Команда "yum update" у поєднанні з автоматизованими механізмами оновлення може спростити процес встановлення оновлень на декількох системах.

Ефективний моніторинг продуктивності системи має важливе значення для системних адміністраторів. Використовуючи такі інструменти, як SAR (System Activity Reporter), top та Grafana, адміністратори можуть відстежувати використання системних ресурсів, аналізувати показники продуктивності та виявляти вузькі місця. Це дозволяє проводити проактивну оптимізацію та забезпечує оптимальну продуктивність системи.

Впровадження надійних стратегій резервного копіювання має вирішальне значення для захисту критично важливих даних у разі збоїв обладнання, пошкодження даних або інших непередбачуваних обставин. Адміністратори повинні створювати графіки резервного копіювання, регулярно виконувати резервне копіювання та створювати віддалені сховища резервних копій. Такі

інструменти, як rsync та Bacula, можуть допомогти автоматизувати процес резервного копіювання та спростити відновлення даних.

CentOS 7 пропонує надійні засоби безпеки, які можна покращити за допомогою методів захисту системи. Системні адміністратори повинні налаштувати брандмауери, такі як iptables або firewalld, для контролю мережевого трафіку і захисту своїх систем. Вони також повинні забезпечити автентифікацію користувачів і контроль доступу, відключити непотрібні служби і впровадити системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) для додаткових рівнів безпеки.

Ознайомлення з основними можливостями CentOS 7 є необхідним для системних адміністраторів, які прагнуть оптимізувати свої можливості керування. Розуміння основ операційної системи, використання керування пакунками за допомогою Yum та застосування найкращих практик оновлення, моніторингу, резервного копіювання та безпеки є критично важливими для ефективного системного адміністрування. Вкладаючи час і зусилля у вивчення ОС, адміністратори можуть покращити свої навички, сприяти стабільності системи і забезпечити безпеку своїх середовищ.

2.2 Встановлення iptables на CentOS7

Перед встановленням iptables нам потрібно зупинити, вимкнути і замаскувати службу firewalld.

Зупинимо службу брандмауера:

```
#sudo systemctl stop firewalld
```

Вимкнемо службу firewalld під час завантаження:

```
#sudo systemctl disable firewalld
```

Замаскуймо брандмауер:

```
#sudo systemctl mask --now firewalld
```

Після вимкнення брандмауера ми можемо встановити iptables за допомогою менеджера пакетів yum.

```
#sudo yum install iptables-services -y
```

Запуск та увімкнення IPtables під час завантаження

Після успішного встановлення iptables запустимо його:

```
#sudo systemctl start iptables
```

Потім увімкнемо iptables під час завантаження системи:

```
#sudo systemctl enable iptables
```

Щоб перевірити стан служби iptables, запустіть її:

```
#sudo systemctl status iptables
```

Розташування файлу правил IPtables

У CentOS 7 iptables зберігає конфігурацію правил у каталогах /etc/sysconfig/iptables та /etc/sysconfig/ip6tables.

2.3 Основні команди та синтаксис iptables

Iptables - це інтерфейс командного рядка, який використовується для налаштування і підтримки таблиць для брандмауера Netfilter для IPv4, що входить до складу ядра Linux[5]. Брандмауер порівнює пакети з правилами, визначеними в цих таблицях, а потім виконує вказану дію при можливому збігу.

1. Таблиці - це назва для набору ланцюжків.

2. Ланцюжок - це набір правил.

3. Правило - умова, яка використовується для зіставлення пакетів.

4. Ціль - це дія, яка виконується, коли можливий збіг з правилом. Прикладами цілей є ACCEPT, DROP, QUEUE.

5. Політика - це дія за замовчуванням, яка виконується у випадку відсутності збігу з вбудованими ланцюжками і може бути ACCEPT або DROP.

Синтаксис:

```
#iptables --table TABLE -A/-C/-D... CHAIN rule --jump Target
```

Є п'ять можливих таблиць:

1. filter: таблиця, що використовується за умовчанням для фільтрації пакетів. Він включає такі ланцюжки, як INPUT, OUTPUT і FORWARD.

2. nat : пов’язано з трансляцією мережевих адрес. Він включає ланцюги PREROUTING і POSTROUTING.

3. mangle : для спеціальної зміни пакетів. Вбудовані ланцюжки включають PREROUTING і OUTPUT.

4. raw : налаштовує винятки з відстеження з’єднання. Вбудовані ланцюжки PREROUTING і OUTPUT.

5. security : Використовується для обов’язкового контролю доступу

Є кілька вбудованих ланцюжків, які включені в таблиці. Вони є:

1. INPUT: набір правил для пакетів, призначених для локальних сокетів.

2. FORWARD : для пакетів, що направляються через пристрій.

3. OUTPUT : для локально згенерованих пакетів, призначених для передачі назовні.

4. PREROUTING : для модифікації пакетів у міру їх надходження.

5. POSTROUTING : для модифікації пакетів під час їх відправлення.

Опції доступні у iptables:

1. -A, -append : Додати до ланцюжка, вказаного в параметрах.

Синтаксис:

```
#iptables [-t table] --append [chain] [parameters]
```

На рисунку 2.1 показана команда яка відкидає весь трафік, що надходить на будь-який порт.

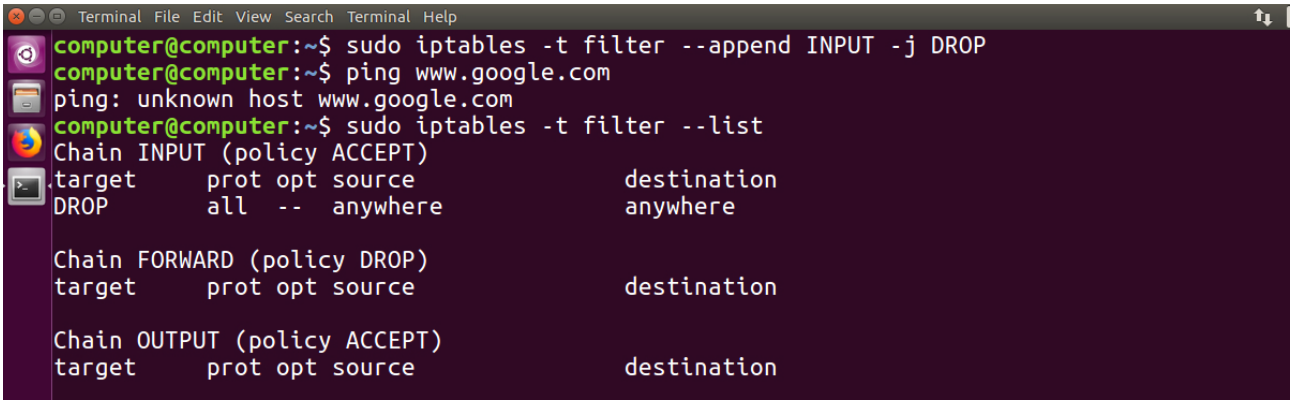

Рисунок 2.1 — Команда яка блокує весь трафік

2. -D, -delete : Видалити правило з вказаного ланцюжка.

Синтаксис:

```
#iptables [-t table] --delete [chain] [rule_number]
```

На рисунку 2.2 показана команда яка видаляє правило 2 з ланцюжка INPUT.

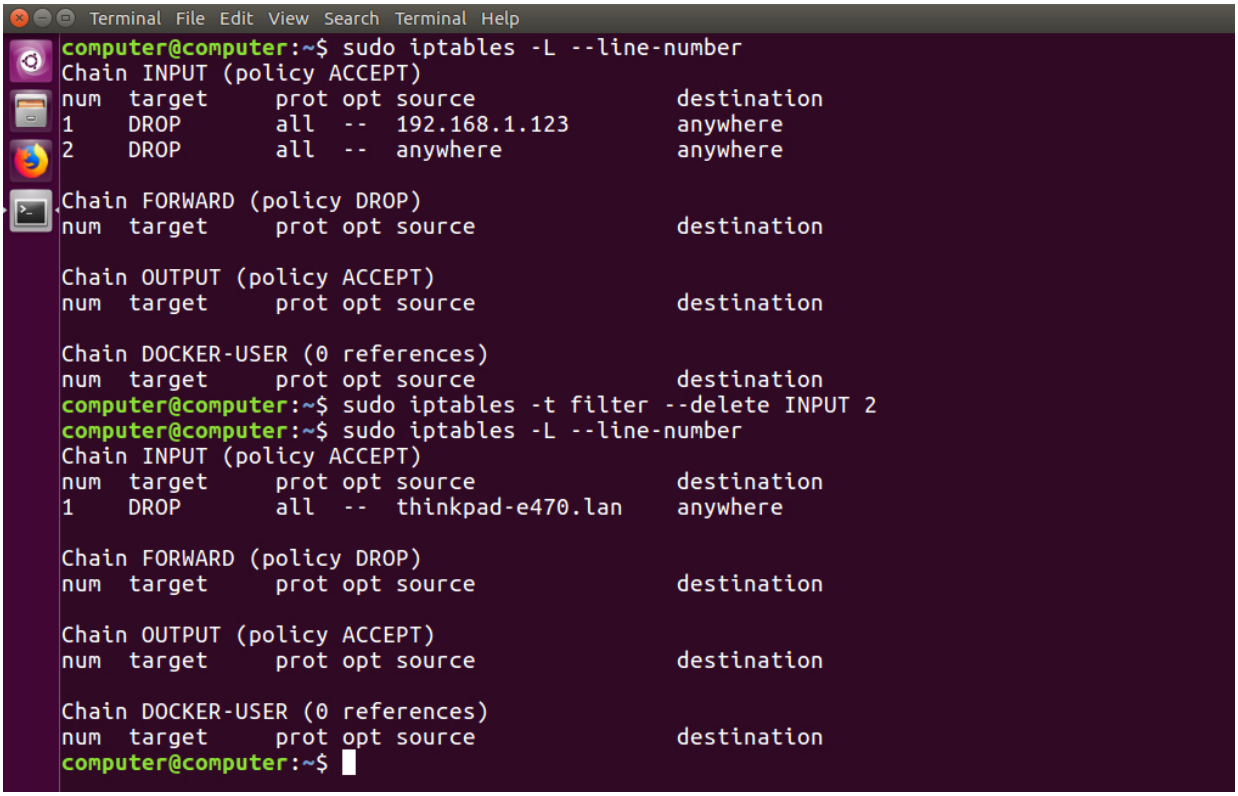

Рисунок 2.2 — Видалення правила з ланцюга

3. -C, -check :Перевіряє, чи присутнє правило у ланцюжку чи ні. Повертає 0, якщо правило існує, і 1, якщо його немає.

Синаксис:

```
#iptables [-t table] --check [chain] [parameters]
```

На рисунку 2.3 показана команда яка перевіряє, чи присутнє вказане правило в ланцюжку INPUT.

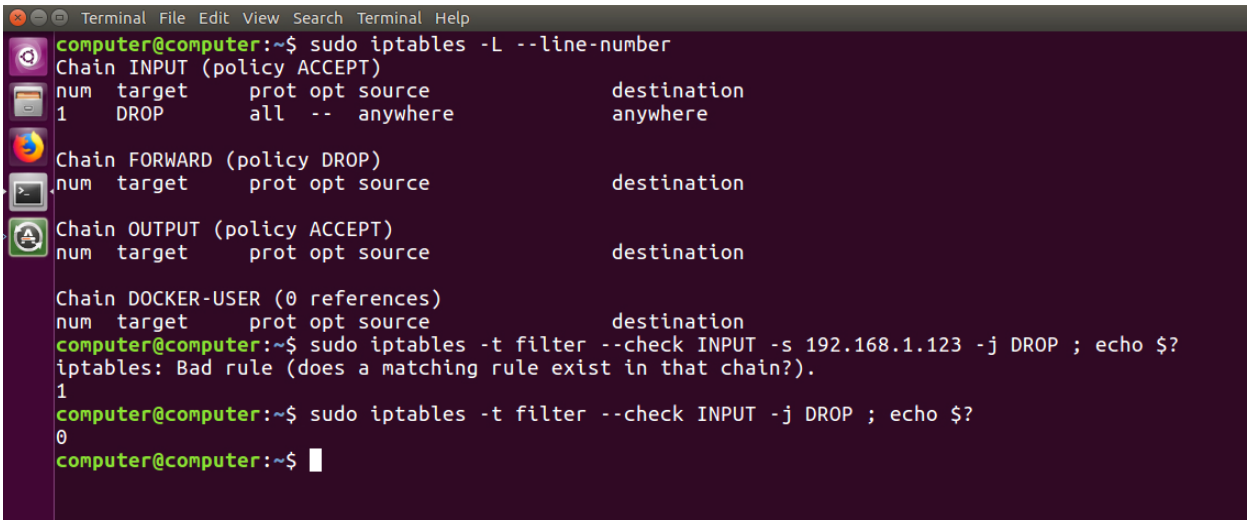

Рисунок 2.3 — Перевірка наявності правила

Параметри, надані командою iptables, використовуються для зіставлення пакета і виконання вказаної дії. Загальними параметрами є:

1. -p, -proto : протокол, якому слідує пакет. Можливі значення: tcp, udp[9], icmp, ssh тощо.

Синтаксис:

```
#iptables [-t table] -A [chain] -p {protocol_name} [target]
```

На рисунку 2.3 показана команда яка додає правило до ланцюжка INPUT для відкидання всіх udp-пакетів.

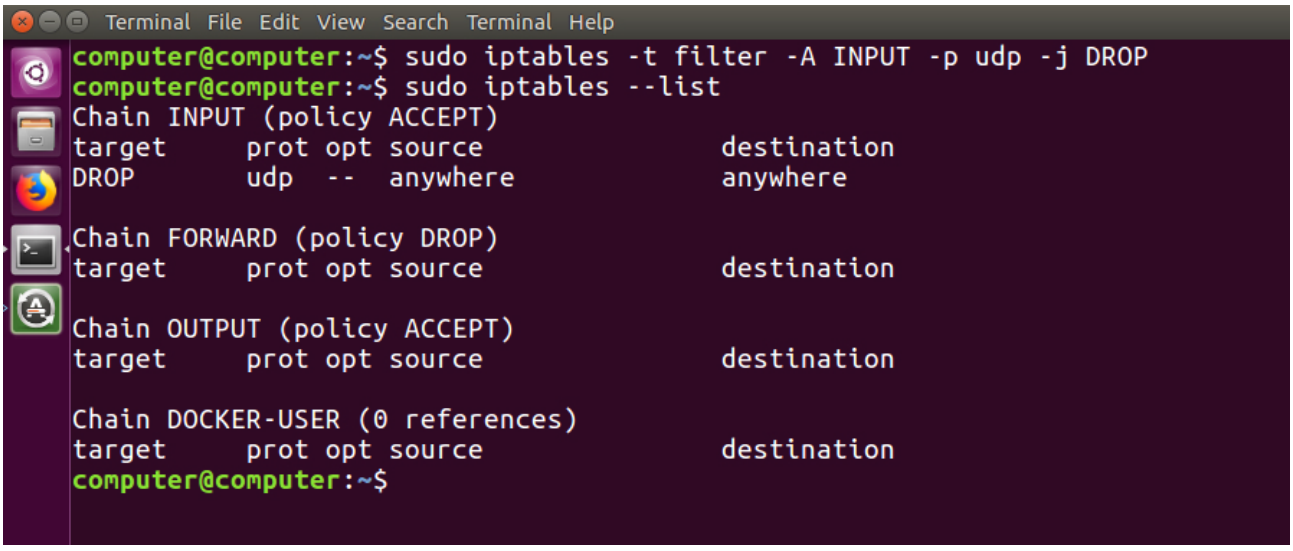

Рисунок 2.4 — Блокування UDP пакетів

2. -s, -source: використовується для співставлення з адресою джерела пакета.

Синтаксис:

```
#iptables [-t table] -A [chain] -s {source_address} [target]
```

На рисунку 2.5 показана команда яка додає правило до ланцюжка INPUT для прийняття всіх пакетів з адреси 192.168.1.230.

Рисунок 2.5 — Прийняття всіх пакетів з вказаної адреси

3. -d, -destination : використовується для співставлення з адресою призначення пакета.

Синтаксис:

```
#iptables [-t table] -A [chain] -d {destination_address} [target]
```

На рисунку 2.6 показана команда яка додає правило до ланцюжка OUTPUT, яке відкидає всі пакети, призначені для адреси 192.168.1.123.

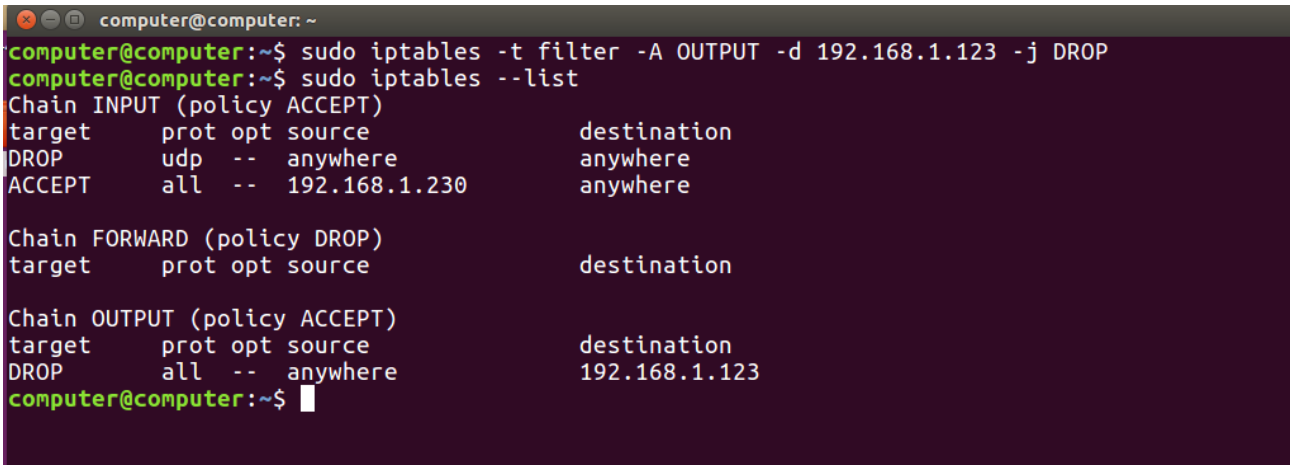

Рисунок 2.6 — Блокування трафіку для 192.168.1.123

4. -i, -in-interface : зіставляє пакети з вказаним in-interface і виконує дію.

Синтаксис:

```
#iptables [-t table] -A [chain] -i {interface} [target]
```

На рисунку показана команда яка додає правило до ланцюжка INPUT, яке відкидає всі пакети, призначені для бездротового інтерфейсу.

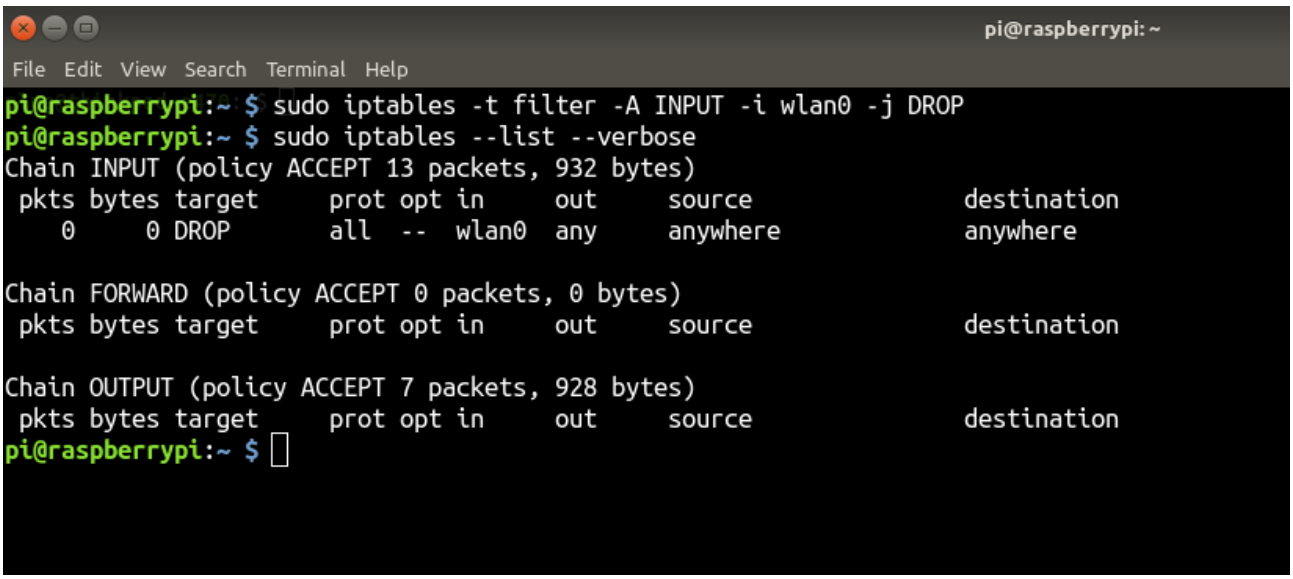

Рисунок 2.7 — Блокування трафіку по бездротовому інтерфейсу

5. -o, -out-interface : зіставляє пакети з вказаним out-інтерфейсом.

6. -j, -jump : цей параметр визначає дію, яку слід виконати над збігом.

Синтаксис:

```
#iptables [-t table] -A [chain] [parameters] -j {target}
```

На рисунку 2.8 показана команда яка додає правило до ланцюжка FORWARD для відкидання всіх пакетів.

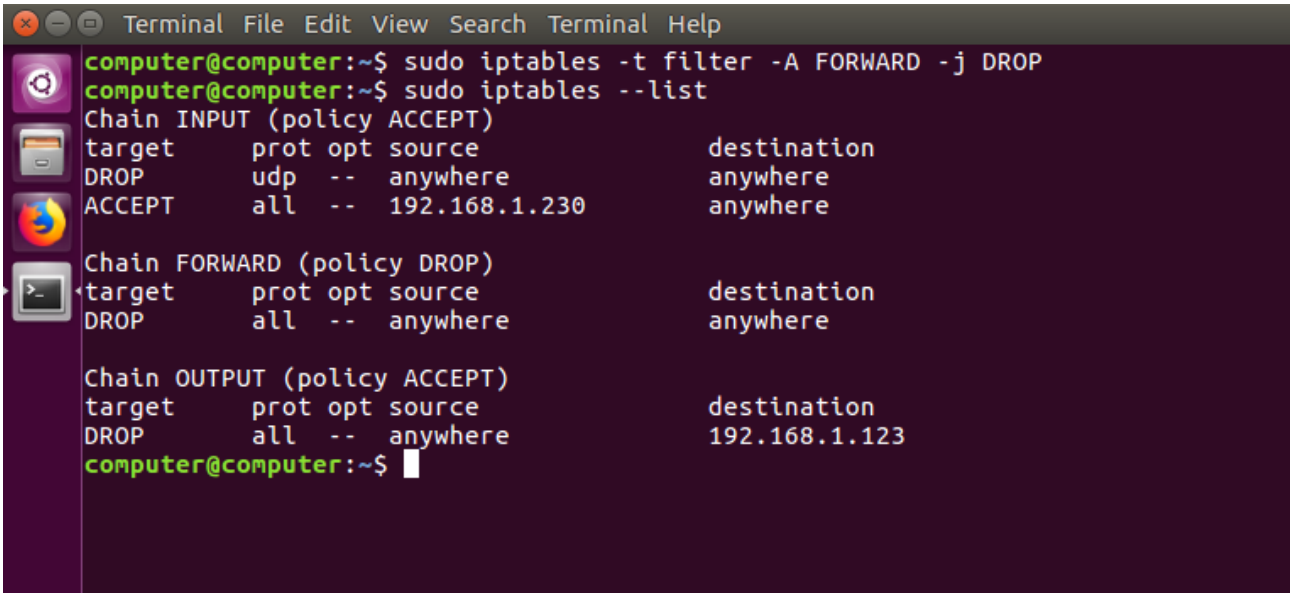

Рисунок 2.8 — Блокування всіх пакетів для ланцюга FORWARD

Ці команди і опції дозволяють вам налаштовувати правила і ланцюжки, які ви створюєте, і дають вам більше контролю над тим, як працює ваш брандмауер. Команда iptables надає широкий спектр опцій, які можна використовувати для налаштування правил брандмауера. Нижче наведено деякі з найпоширеніших опцій:

1. Параметри ланцюжка і правил дозволяють вказати ланцюжок і правило, до якого ви хочете застосувати певну команду.

2. Параметри IP-адреси і порту дозволяють вказати IP-адреси і порти джерела і призначення, до яких має застосовуватися правило.

3. Параметри цілі визначають дію, яку слід виконати, коли правило буде виконано. Наприклад, правило можна використовувати для блокування трафіку, дозволу трафіку або перенаправлення трафіку на інший порт або IP-адресу.

Використовуючи ці опції, ви можете створювати складні правила брандмауера, пристосовані до ваших конкретних потреб. У цьому розділі ми також розглянемо деякі поширені приклади iptables, які ілюструють, як ці опції можна використовувати на практиці. Загалом, розуміння різних команд і опцій iptables має вирішальне значення для створення потужного і ефективного брандмауера. Опанувавши ці інструменти, ви зможете убезпечити свою мережу і захистити свої системи від широкого спектру загроз.

Iptables можна використовувати для захисту сервера шляхом контролю вхідного та вихідного мережевого трафіку. Ось кілька типових випадків використання:

1. Захист сервера за допомогою iptables: Iptables можна використовувати для обмеження вхідного та вихідного трафіку лише тим, що є необхідним для роботи сервера, захищаючи його від потенційних атак.

2. Блокування вхідного трафіку з певних IP-адрес або мереж: Iptables можна використовувати для блокування трафіку з певних IP-адрес або діапазонів мереж, наприклад, пов’язаних із відомою шкідливою діяльністю.

3. Дозвіл вхідного трафіку на певні порти або служби: Iptables можна використовувати для дозволу трафіку на певні порти або служби, наприклад SSH або HTTP, блокуючи трафік до інших портів або служб.

4. Налаштування базового брандмауера за допомогою iptables: Iptables можна використовувати для налаштування базового брандмауера для контролю мережевого трафіку, блокуючи весь вхідний трафік, за винятком певних портів або служб, необхідних для роботи сервера.

5. Обмеження підключень і запобігання DDoS-атакам за допомогою iptables: Iptables можна використовувати для обмеження кількості підключень з однієї IP-адреси, запобігаючи DDoS-атакам та іншим типам зловживань.

Iptables — складний, але важливий інструмент для керування мережевим трафіком і захисту ваших систем.

2.4 Перевірка та моніторинг за допомогою iptables

У сучасну епоху цифрових технологій моніторинг мережевого трафіку стає все більш важливим для компаній і окремих осіб[6]. В умовах зростання кіберзагроз і атак можливість моніторингу мережевого трафіку може допомогти виявити потенційні порушення безпеки до того, як вони перетворяться на серйозні проблеми.

Мережева безпека є ключовим завданням для будь-якої організації, і моніторинг мережевого трафіку - це ключовий елемент комплексної стратегії безпеки. iptables - це потужний застосунок, який дає змогу контролювати мережевий трафік, фільтруючи пакети відповідно до різних критеріїв. Крім фільтрації, iptables можна використовувати для протоколювання мережевого трафіку і створення докладного запису всіх вхідних і вихідних пакетів.

Журналування — це функція, яка дозволяє реєструвати мережевий трафік, який відповідає певним правилам.

Коли пакет відповідає правилу журналювання, iptables записує повідомлення журналу в syslog. За замовчуванням iptables реєструє всі відповідні пакети, що може швидко заповнити системний журнал. Щоб уникнути цього, використовуйте параметр -limit, щоб обмежити швидкість генерації повідомлень журналу. Давайте подивимося на існуючі правила iptables.

Перш ніж почати, дуже важливо зрозуміти поточні правила iptables у нашій системі. На.рисунку 2.9 показана команда яка відображає поточні правила iptables і всі правила журналу.

Рисунок 2.9 — Список поточних правил iptables

Налаштуймо iptables для реєстрації мережевого трафіку за допомогою файлів журналу. Файл журналу може бути будь-яким файлом, у який записує система, наприклад звичайним файлом або іменованим каналом. На рисунку 2.10 показана команда яка дозволяє створити файли журналу,:

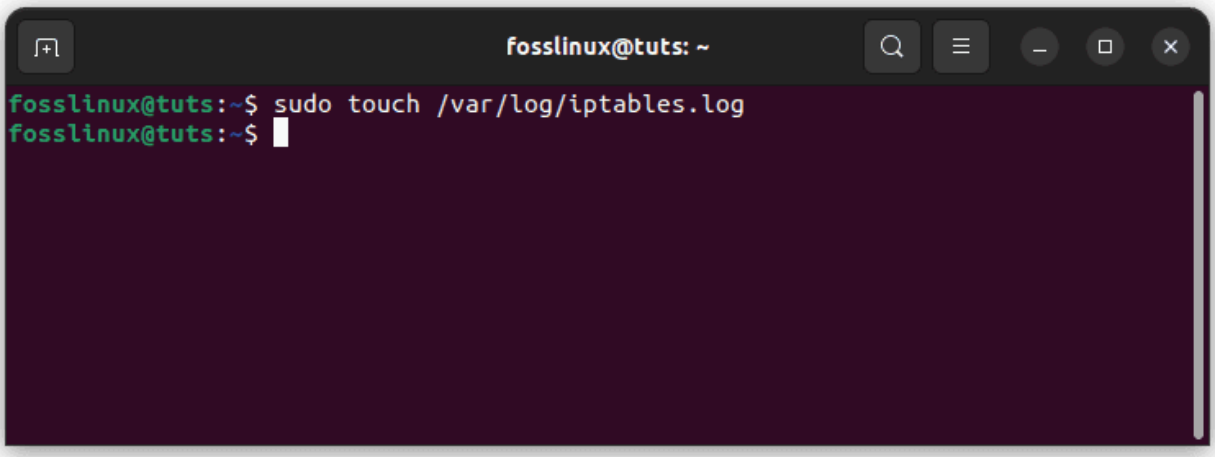

Рисунок 2.10 — Створення файлу журналу

Ця команда створює новий файл із назвою «iptables.log» у каталозі «/var/log». Потім налаштуєм iptables для запису повідомлень журналу в цей файл, додавши правила журналювання до відповідного ланцюжка. Далі конфігуруєм Iptables для запису даних про мережевий трафік у цей файл журналу. На рисунку 2.11 відображені усі команди для налаштування журналювання:

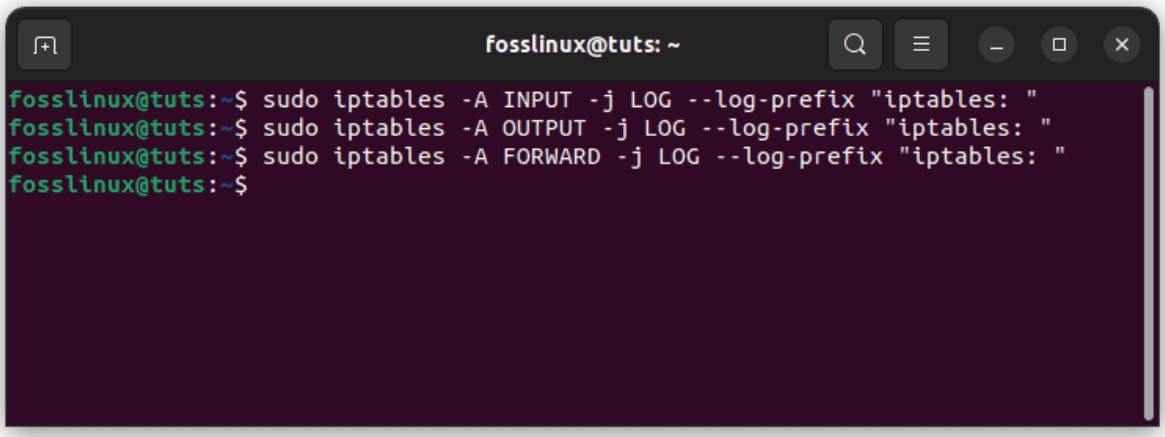

Рисунок 2.11 — Дозвіл iptables записувати мережевий трафік

Ці команди реєструватимуть увесь вхідний, вихідний і переадресований мережевий трафік і додає префікс «iptables:» до кожного запису журналу.

Наступна команда показана на рисунку 2.12 реєструє всі вхідні пакети до файлу “/var/log/iptables.log”:

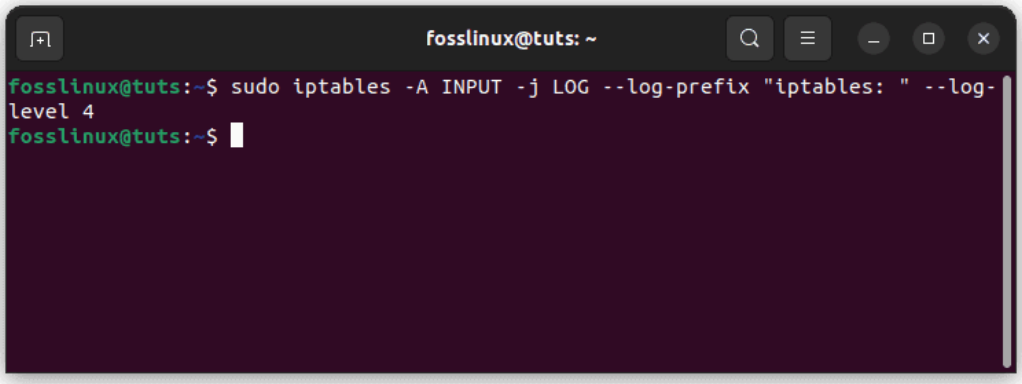

Рисунок 2.12 — Реєстрація всіх вхідних пакетів

У цій команді, показаній на рисунку 2.13, параметр «-j LOG» повідомляє iptables реєструвати пакет, а параметр «–log-prefix» визначає префікс, який потрібно додати до кожного повідомлення журналу. Параметр «–log-level» визначає рівень серйозності повідомлення журналу, зі значенням 4, що вказує на повідомлення рівня «попередження».

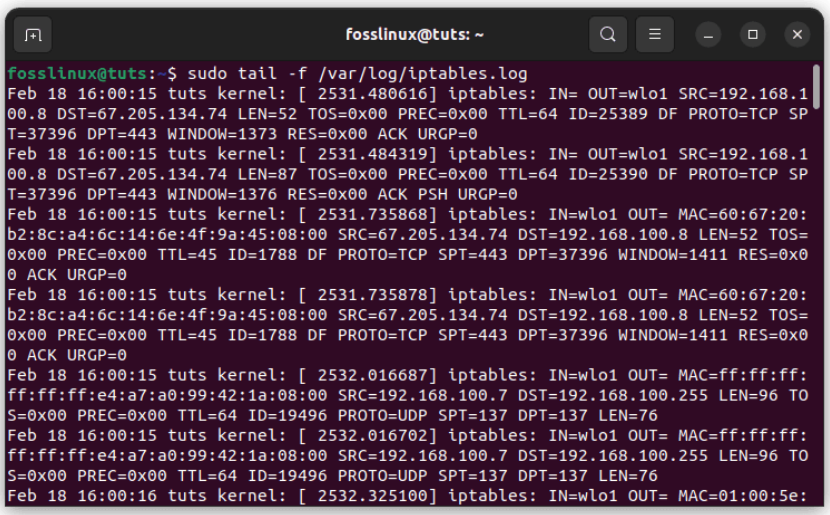

Рисунок 2.13 — Відстеження мережевого трафіку

Ця команда відображає останні рядки файлу журналу та постійно оновлює їх у міру поновлення даних. Ця команда дозволяє контролювати мережевий трафік у час подання запиту. Окрім моніторингу мережевого трафіку в реальному часі, ви також можете аналізувати історичний мережевий трафік за допомогою протоколу iptables. Наприклад, знайдіть конкретні IP-адреси або номери портів у файлах журналу, щоб побачити, які пристрої чи програми генерують найбільше трафіку.

Ось декілька практичних прикладів того, як використовувати журнал iptables для моніторингу мережевого трафіку:

На рисунку 2.14 показана команда яка дозволяє зареєструвати всі вхідні пакети у файл “/var/log/iptables.log.

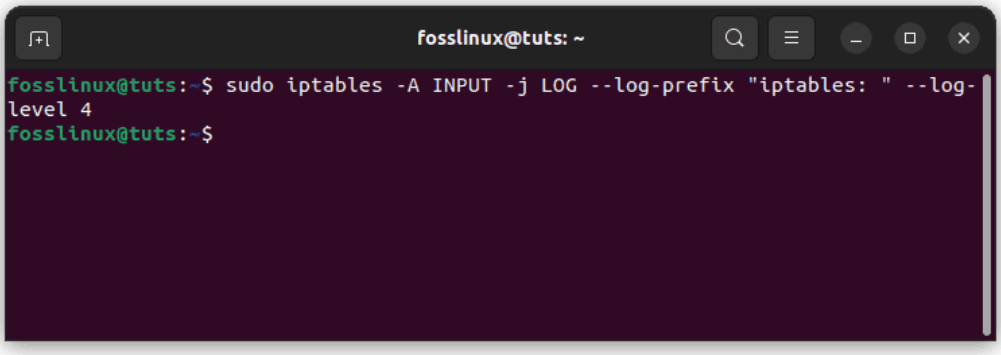

Рисунок 2.14 — Реєстрація всіх вхідних пакетів трафіку

На рисунку 2.15 показана команда яка дозволяє зареєструвати всі вихідні пакети у файл “/var/log/iptables.log.

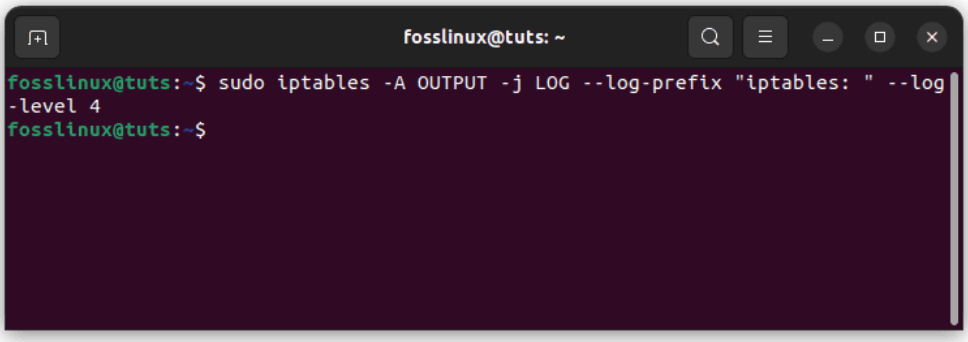

Рисунок 2.15 — Реєстрація всіх вихідних пакетів

На рисунку 2.16 показана команда яка дозволяє зареєструвати всі скинуті пакети у файл “/var/log/iptables.log”.

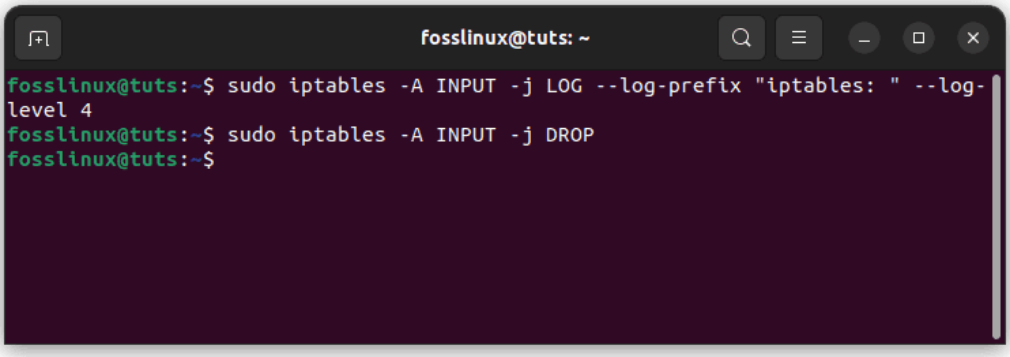

Рисунок 2.16 — Реєстрація всіх скинутих пакетів

У цьому прикладі перше правило реєструє всі вхідні пакети, а друге правило видаляє всі вхідні пакети. Реєструючи пакети перед їх відкиданням, можемо отримати докладний запис усіх відкинутих пакетів.

Ми можемо контролювати iptables для розмежування мережевого трафіку на основі певних правил, а потім записувати лише відфільтрований трафік. Це зменшить потік даних, що реєструються до файлу журналу, і зробити легшим аналіз інформації.

Крім того, декілька інструментів використовуютья для аналізу файлів журналу iptables і надання розширеніших параметрів звітності та візуалізації. Ці інструменти допоможуть нам обрати шаблони та тенденції у нашій мережі, які важко відокремити за допомогою ручного аналізу.

Зазначу, що журналювання Iptables є невід'ємною ланкою для захисту мережі. Також це потужний інструмент для моніторингу та аналізу мережевого трафіку, його слід використовувати разом з іншими інструментами безпеки, такими як системи IDS, антивірусне програмне забезпечення та регулярний моніторинг безпеки. Різниця між різними засобами захисту полягає в їх підходах і сферах застосування (див. таблицю 2.1).

Таблиця 2.1 — Порівняння iptables із модулем Apache mod_evasive і APF(Advanced Policy Firewall)

	iptables	mod_evasive	APF
Гнучкість та універсальність	Дозволяє створювати складні та детальні правила фільтрації трафіку. Може захищати всі служби та порти на сервері, а не тільки веб-сервер Apache.	Працює тільки з Apache веб-сервером, тому не забезпечує захист для інших сервісів, які можуть працювати на сервері. Налаштування модулю обмежені і не можуть забезпечити такий рівень детальної конфігурації	APF має простішу конфігурацію, що може бути обмеженням для більш детального налаштування. Часто потребує встановлення додаткових модулів для досягнення функціональності

Продовження таблиці 2.1

Продуктивність	Працює на рівні ядра системи, що дозволяє обробляти пакети швидше і з меншими накладними витратами на системні ресурси.	Працює на рівні додатку (Apache), що може призвести до додаткових навантажень на сервер, особливо під час високих обсягів трафіку.	Працює на рівні користувача, що може бути менш ефективним у порівнянні з iptables
Інтеграція та сумісність	Підтримується всіма основними дистрибутивами Linux і інтегрується з іншими інструментами безпеки та мережевими рішеннями.	Може бути використаний тільки з Apache, що обмежує його застосування в середовищах з іншими веб-серверами.	Хоча APF і може бути налаштований для роботи з різними дистрибутивами, його функціональність обмежена
Розширюваність та підтримка спільнотою	Має велику підтримку спільноти та безліч документації, що полегшує налаштування та усунення проблем.	Спільнота навколо mod_evasive значно менша, що може ускладнити пошук допомоги та вирішення проблем.	Хоча APF має своїх прихильників, його спільнота менша, що може впливати на швидкість отримання оновлень і підтримки.

Вибір iptables для захисту сервера CentOS 7 від DDoS атак обумовлений його гнучкістю, універсальністю, високою продуктивністю, інтеграцією з іншими системами безпеки, а також широкою підтримкою спільноти. У порівнянні з іншими методами, такими як mod_evasive для Apache та APF, iptables надає більш детальний контроль та ефективний захист для всіх мережевих сервісів сервера.

3 РЕАЛІЗАЦІЯ ЗАХИСТУ ВІД DDOS АТАК ЗА ДОПОМОГОЮ IPTABLES

3.1 Встановлення обмеження кількості з'єднань на IP

Як обмежити кількість підключень, які використовуються однією IP-адресою до мого сервера для портів 80 і 443 за допомогою iptables?

Нам потрібно використовувати модулі connlimit, які дозволяють обмежити кількість паралельних TCP-з’єднань із сервером на IP-адресу клієнта (або блок адреси).

Це корисно, щоб захистити наш сервер або сервер vps від затоплення, розсилання спаму чи копіювання вмісту.

Використаєм такі команди щоб обмежити кількість одночасних з'єднань від одної IP-адреси:

```
#sudo iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 10 -j REJECT --reject-with tcp-reset
#sudo iptables -A INPUT -p tcp --syn --dport 443 -m connlimit --connlimit-above 10 -j REJECT --reject-with tcp-reset
```

Це правило обмежує кількість одночасних з'єднань до 10 на порт 80 (HTTP) і 443 (HTTPS).

3.2 Обмеження швидкості з'єднань

Встановимо обмеження на кількість нових з'єднань від одного IP за певний період часу.

Перш ніж ми заглибимося в використання connlimit, важливо зазначити, що хоча він може бути ефективним для обмеження вхідних з’єднань, він не завжди може бути ідеальним рішенням для кожного сценарію.

У випадку як DoS-атаки[8], коли зловмисник може використовувати такі методи, як IP-спуфінг або ботнети з кількома розподіленими IP-адресами.

Вони потенційно можуть обійти правила iptables, розподіливши свою атаку між кількома IP-адресами.

Крім того, правила iptables можуть бути неефективними проти атак на прикладному рівні, коли зловмисник маніпулює з'єднанням таким чином, що не запускає правило брандмауера. Крім того, обмеження з'єднань на основі використовуваних протоколів може призвести до негативних наслідків, оскільки певні протоколи (такі як ICMP) необхідні для усунення несправностей і перевірки працездатності мережі.

Таким чином, незважаючи на те, що connlimit може бути цінним варіантом у нашому наборі інструментів iptables, дуже важливо уважно розглянути його обмеження та розгорнути правила брандмауера обережно та з усією зваженістю.

```
    #sudo iptables -A INPUT -p tcp --dport 80 -m state --state NEW
-m recent --set
    #sudo iptables -A INPUT -p tcp --dport 80 -m state --state NEW
-m recent --update --seconds 60 --hitcount 20 -j DROP
    #sudo iptables -A INPUT -p tcp --dport 443 -m state --state NEW
-m recent --set
    #sudo iptables -A INPUT -p tcp --dport 443 -m state --state NEW
-m recent --update --seconds 60 --hitcount 20 -j DROP
```

Це правило обмежує кількість нових з'єднань до 20 за 60 секунд на порти 80 і 443.

3.3 Використання модуля tcp_syncookies

Атака SYN flood — це тип атаки на відмову в обслуговуванні, під час якої зловмисник швидко ініціює TCP-з'єднання із запитом SYN до сервера та не відповідає на SYN+ACK від сервера. Сервер повинен витрачати ресурси (створення TCB для запитів на з'єднання), чекаючи напів-відкриті з'єднання Оскільки було обмеження на кількість «напіввідкритих» з'єднань TCP. Сервер більше не прийматиме нові підключення. Це призведе до того, що система не реагує на законний трафік. Наступні кроки показують, як це було виконано:

1. Зловмисник надсилає на сервер 100 сегментів SYN щосекунди.
2. Зловмисник не відповість на отримані сегменти SYN+ACK.

3. Зловмисник надсилає ці SYN-сегменти з іншою IP-адресою, ніж його власна IP-адреса, щоб не бути спійманим.

4. Як тільки сервер увійде в стан SYN RCVD, він залишатиметься в цьому стані протягом кількох секунд, очікуючи ACK і не приймаючи жодних нових, можливо, справжніх з’єднань,тому стає недоступним.

Модуль tcp_syncookies використовується як механізм захисту від атак SYN flood, які є типом DDoS-атак. Якщо ввімкнено, сервер надішле відповідь SYN-ACK зі спеціально створеним порядковим номером («SYN cookie»), який кодує інформацію про з’єднання.

Це дозволяє серверу уникати збереження стану для з’єднань, доки клієнт не поверне дійсний пакет ACK.

```
#sudo sysctl -w net.ipv4.tcp_syncookies=1
```

3.4 Встановлення обмеження на розмір черги з'єднань

Linux, як і всі операційні системи загального призначення, працює за принципом найкращих зусиль. Це означає, що, як правило, поки є доступні ресурси, додатки можуть запитувати їх. З іншого боку, якщо деякий пул ресурсів вичерпується, це може вплинути на працездатність і швидкість реагування всієї системи.

Отже, навіть якщо, теоретично, Linux не повинен обмежувати використання ресурсів апаратними обмеженнями, він повинен. У наш час це потрібно робити! Багато атак типу «відмова в обслуговуванні» намагаються виснажити цільові ресурси. Щоб уникнути значного впливу, будь-яка сучасна операційна система матиме політику використання ресурсів за умовчанням.

Адміністратору може знадобитися налаштувати політики обмежень відповідно до випадків використання. Крім того, типові параметри зазвичай підходять для загального використання.

Для забезпечення стабільності та швидкості реагування системи існує багато засобів контролю безпеки. Давайте подивимося на які обмеження ми можемо зіткнутися.

Якщо у нас великий трафік або величезна кількість з’єднань, швидше за все, нам знадобиться збільшити системні параметри ulimit за замовчуванням. З іншого боку, якщо система є ймовірною мішенню для атак типу «відмова в обслуговуванні», потрібно встановити деякі параметри, щоб забезпечити ще кращу стійкість.ipp.

Щоб встановити обмеження на розмір черги підключення в Linux, можем налаштувати параметр net.ipv4.tcp_max_syn_backlog. Цей параметр контролює максимальну кількість запитів на підключення в черзі (SYN-ACK), які ще не отримали підтвердження від клієнта, що підключається.

Ось як можна переглянути та встановити цей параметр:

Зменшення розміру черги з'єднань може допомогти зменшити ефективність атаки Slowloris[7].

```
#sudo sysctl -w net.ipv4.tcp_max_syn_backlog=2048
#sudo sysctl -w net.ipv4.tcp_synack_retries=3
```

3.5 Використання модуля mod_reqtimeout для Apache

Модуль mod_reqtimeout для Apache використовується для обмеження часу обробки запитів, що допомагає запобігати атакам повільного читання (slowloris)[7]. Він дозволяє налаштувати час очікування для отримання заголовка запиту та тіла повідомлення. Це може бути корисним для захисту веб-сервера від DDoS-атак, які намагаються вичерпати ресурси сервера, встановлюючи і підтримуючи незавершені HTTP-з’єднання.

Відредагуймо конфігураційний файл Apache, зазвичай /etc/httpd/conf/httpd.conf, додавши наступні рядки:

```
<IfModule reqtimeout_module>
  RequestReadTimeout                    header=20-40,MinRate=500
body=20,MinRate=500
</IfModule>
```

Це означає, що клієнт має 20 секунд на надсилання заголовків запиту, і швидкість передачі повинна бути не менше 500 байт/сек. Після отримання

заголовків у клієнта є 20 секунд на надсилання тіла запиту з мінімальною швидкістю 500 байт/сек.

3.6 Перезапуск сервісів

Для перезапуску сервісів на Linux-базованій системі, як Apache, можна використовувати команди systemctl або service.

Після внесення змін потрібно перезапустити сервер і застосувати конфігурації sysctl.

```
#sudo systemctl restart httpd
#sudo sysctl -p
```

3.7 Збереження правил iptables

Для збереження правил iptables на Linux-системі ви можете використовувати команду iptables-save. Це дозволить вам експортувати поточні правила iptables у файл, який можна згодом використовувати для відновлення конфігурації за допомогою iptables-restore.

Не забудьмо зберегти правила iptables, щоб вони залишилися після перезавантаження:

```
#sudo service iptables save
```

3.8 Перевірка та моніторинг

Переконаємся, що правила застосовані правильно:

```
#sudo iptables -L -v -n
```

Регулярно моніторимо наш сервер на наявність підозрілої активності та корегуєм правила iptables при необхідності.

Перейдемо на локальний сайт, що знаходиться у нас на сервері CentOS(див. рисунок 3.1)

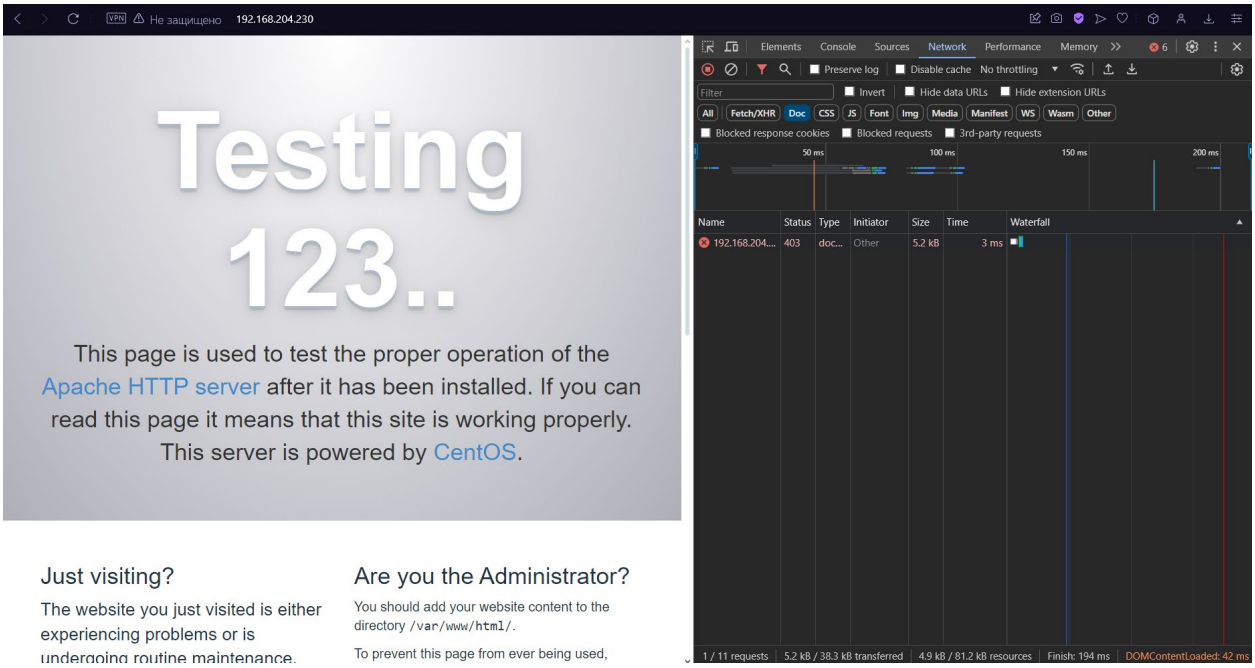

Рисунок 3.1 — Локальний сайт

Судячи з зображення, ми зайшли на сайт з швидкістю 3мс. Тепер за допомогою Kali Linux запустимо завантажений DDoS з типом атаки botnet а також вбудований модуль у ОС під назвою Metasploit(див. рисунок 3.2).

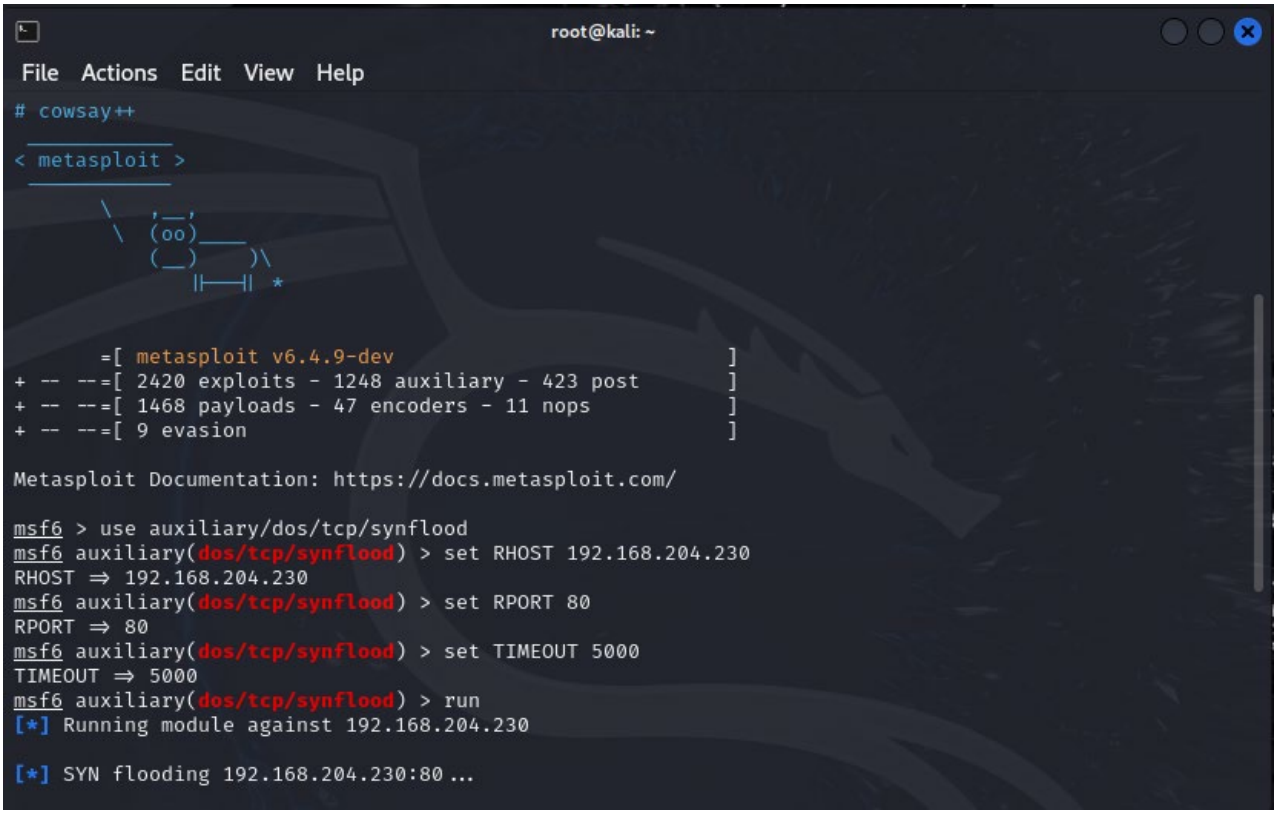

Рисунок 3.2 — Атака synflood за допомогою Metasploit

У даній програмі ми вказуємо нашу IP-адресу 192.168.204.230, порт 80 і також Timeout тривалість часу (у секундах), протягом якого зловмисник чекає перед тим, як надіслати новий SYN-пакет. Після чого можемо скористатись командою run, як на рисунку або ж ввести exploit, що також запустить атаку.

Атака SYN flood з використанням Metasploit передбачає надсилання великої кількості пакетів TCP SYN(див. рисунок 3.3) до цільової системи з метою перевантажити її ресурси та викликати відмову в обслуговуванні (DoS). Це робиться шляхом використання процесу тристороннього рукостискання TCP, залишаючи численні напіввідкриті з’єднання на цілі.

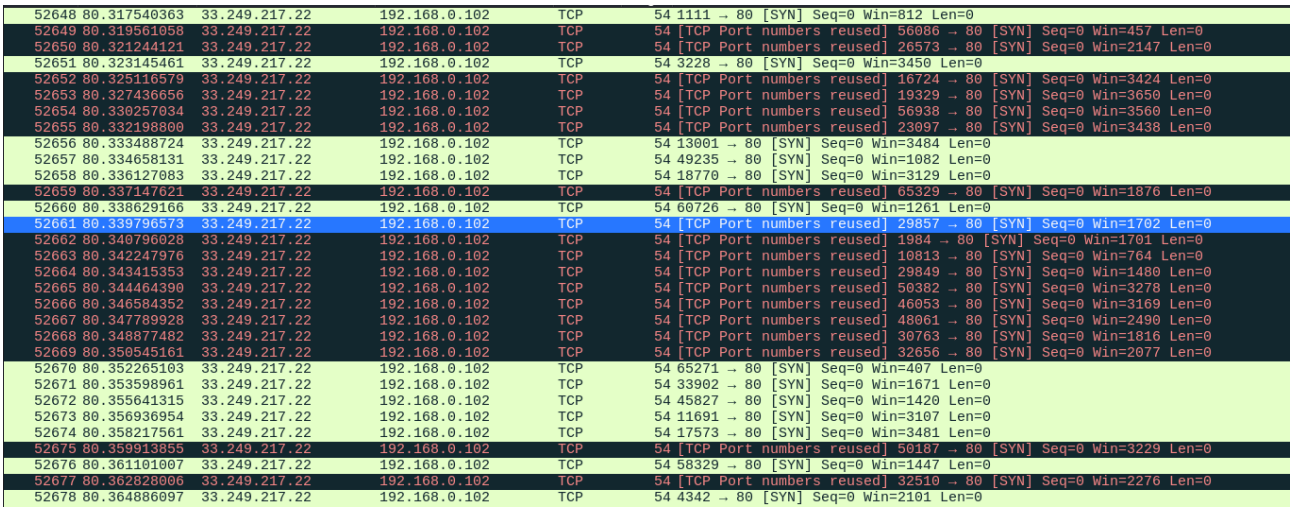

Рисунок 3.3 — Номер порту було повторно використано для нового з'єднання.

Атака Slowloris полягає в надсиланні незавершених HTTP-запитів(див. рисунок 3.4) до цільового веб-сервера, заморожуючи його ресурси і перешкоджаючи обробці інших легітимних запитів. це використовується для зниження доступності сервера без необхідності великої кількості трафіку.

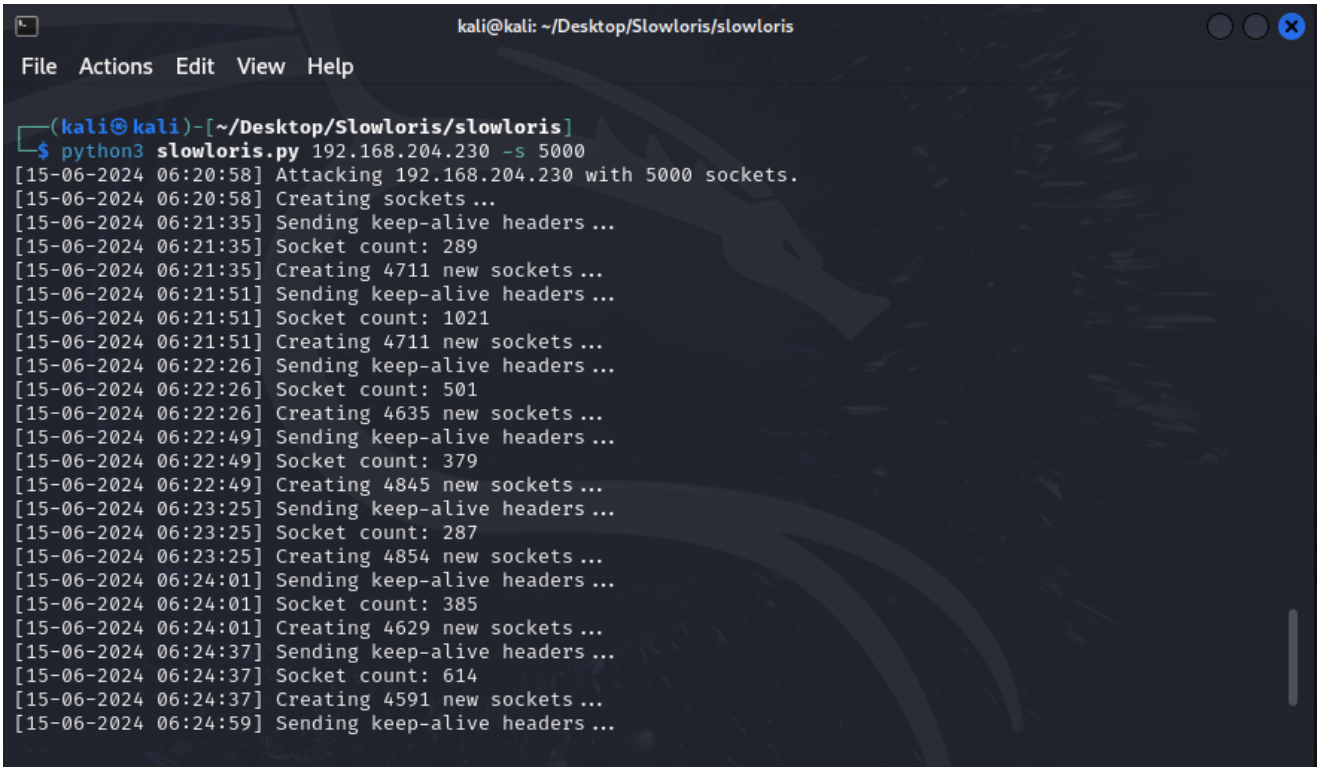

Рисунок 3.4 — Атака botnet за допомогою Slowloris

Спробуємо зайти на наш локальний сайт ше раз(див. рисунок 3.5):

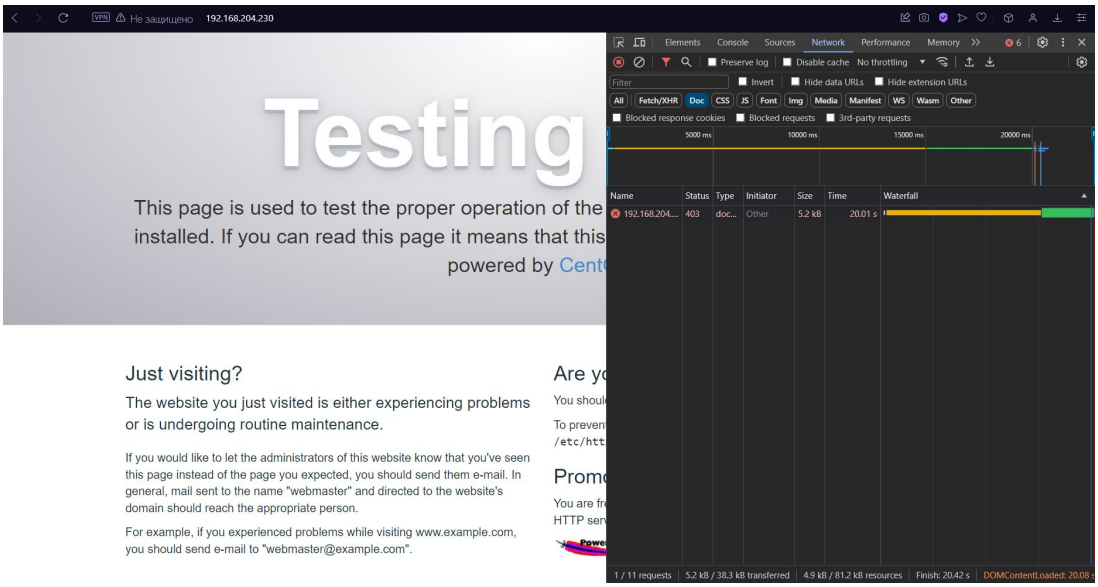

Рисунок 3.5 — Завантажена сторінка із серверу CentOS

Як бачимо завантаження сторінки відбувалось цілих 20с, отже атака пройшла успішно. Було використано 3 віртуальних машини та 2 види атаки на

сервер, а саме SYNFLOOD і botnet. Тепер введемо вище перераховані команди утиліти iptables і подивимось на результат(див. рисунок 3.6).

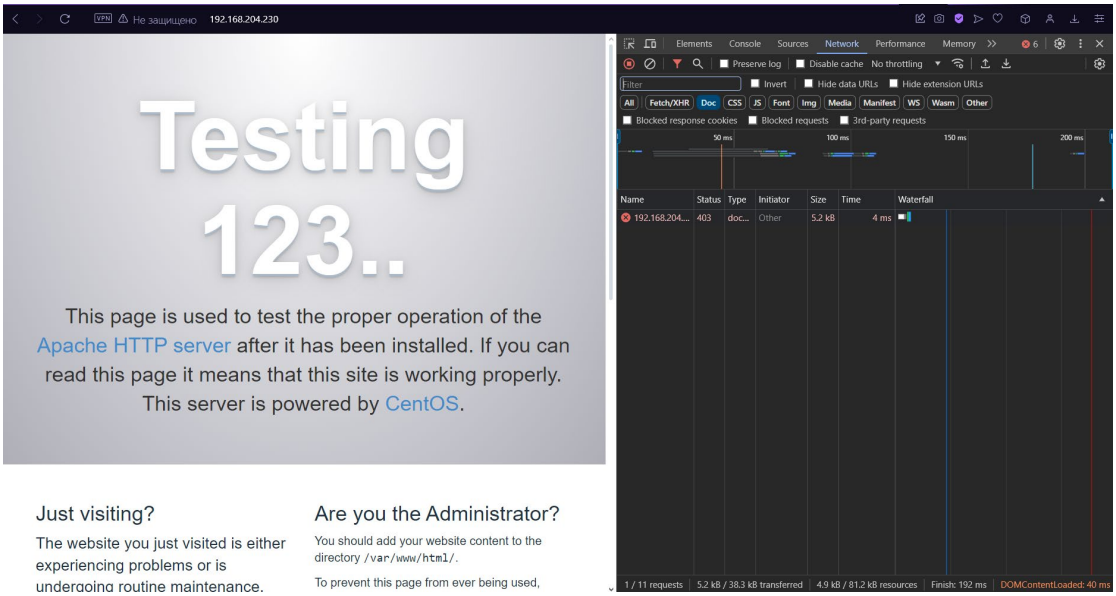

Рисунок 3.6 — Атака після налаштування iptables

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Організація безпечної роботи електроустановок

Державна політика в галузі промислової безпеки та охорони праці ґрунтується за принципом пріоритетності життя людини над результатами виробничої діяльності. Сьогодні безліч різних електроустановок використовуються в промисловості, будівництві, житлово-комунальному господарстві, на транспорті, в сільському господарстві та інших галузях, в медичних, культурних закладах та в побуті.

Поєднання зусиль органів державної влади, громадських, профспілкових організацій та роботодавців у вирішенні загальних проблем запобігання нещасним випадкам та професійним захворюванням є також важливим питанням. За таких умов великого значення набувають саме питання безпечної експлуатації електроустановок споживачів.

При експлуатації електроустановок споживачів, одним із основних нормативно-правових актів з охорони праці є НПАОП 40.1-1.21-98 – «Правила безпечної експлуатації електроустановок споживачів». Вимоги цих Правил поширюються на працівників, що обслуговують діючі електроустановки споживачів напругою до 220 кВ включно і є обов’язковими для всіх споживачів та виробників електроенергії, незалежно від їх відомчої належності і форм власності на засоби виробництва.

Під час експлуатації діючих електроустановок, електричних станцій, електричної частини пристроїв теплової автоматики, теплотехнічного вимірювання і захисту, засобів дистанційного керування, сигналізації і технічних засобів автоматизованих систем керування, засобів диспетчерського і технологічного керування в енергосистемах, районних котелень, що обслуговуються споживачами, під час виконання в них монтажних, налагоджувальних, випробувальних, ремонтних і будівельних робіт повинні виконуватись вимоги цих Правил. В цих Правилах викладені основні вимоги, щодо убезпечення працівників під час експлуатації електроустановок.

Первинні засоби пожежогасіння, які застосовуються в електроустановках, мають відповідати Правилам пожежної безпеки в Україні – НАПБ А.01.001-2004. Електрообладнання, конструкції, комплектувальні деталі, вузли вітчизняного та іноземного виробництва повинні відповідати вимогам чинних нормативних документів в Україні.

Електрообладнання, яке підлягає в Україні обов‘язковій сертифікації, повинно супроводжуватись сертифікатом відповідності або свідоцтвом про визнання іноземного сертифіката згідно з Державною системою сертифікації УкрСЕПРО.

Машини, механізми, пристосування і інструмент, що застосовуються в електроустановках, повинні бути справні і випробувані відповідно до чинних нормативних документів і строків.

У разі постачання електрообладнання з-за кордону організація – замовник повинна отримати сертифікат відповідності до укладення контракту на його поставку.

Паспорт, інструкція та інша експлуатаційна документація, що поставляється з обладнанням чи виробами, повинна мати переклад українською мовою.

Можливі відхилення від нормативної документації повинні бути узгоджені з Держпраці, Держстандартом та організацією-замовником до укладання контракту на їх постачання. Копії погоджень і сертифікати долучаються до паспорта обладнання або виробу.

Для організації безпечної експлуатації електроустановок споживачів, керівник підприємства зобов’язаний забезпечити утримання, експлуатацію і обслуговування електроустановок відповідно до вимог чинних нормативних документів.

Для цього він повинен:

1. Призначити відповідального за справний стан і безпечну експлуатацію електрогосподарства з числа інженерно-технічних працівників, які мають електротехнічну підготовку і пройшли перевірку знань у встановленому порядку (далі – особа, відповідальна за електрогосподарство);

2. забезпечити достатню кількість електротехнічних працівників;

3. затвердити Положення про енергетичну службу підприємства, а також посадові інструкції і інструкції з охорони праці;

4. встановити такий порядок, щоб працівники, на яких покладено обов'язки з обслуговування електроустановок, вели ретельні спостереження за дорученим їм обладнанням і мережами – оглядом, перевіркою дії, випробуванням і вимірюванням;

5. забезпечити перевірку знань працівників у встановлені строки згідно з вимогами "Правил технічної експлуатації електроустановок споживачів»;

6. забезпечити проведення протиаварійних, приймально-здавальних і профілактичних випробувань та вимірювань електроустановок згідно з правилами і нормами (ПТЕ);

7. забезпечити проведення технічного огляду електроустановок.

При експлуатації електроустановок споживачів повинні виконуватись організаційні заходи, що убезпечують працівників під час роботи та технічні заходи, що створюють безпечні умови виконання робіт.

До основних організаційних заходів відносять:

1. Роботи в електроустановках стосовно їх організації поділяються на такі, що виконуються: за нарядом-допуском (далі нарядом), за розпорядженням та в порядку поточної експлуатації.

2. Організаційними заходами, якими досягається безпека робіт в електроустановках, є:

1. Затвердження переліку робіт, що виконуються за нарядами, розпорядженнями і в порядку поточної експлуатації;

2. призначення осіб, відповідальних за безпечне проведення робіт;

3. оформлення робіт нарядом, розпорядженням або затвердженням переліку робіт, що виконуються в порядку поточної експлуатації;

4. підготовка робочих місць;

5. допуск до роботи;

6. нагляд під час виконання робіт;

7. переведення на інше робоче місце;

8. оформлення перерв в роботі та її закінчення.

До технічних заходів, що створюють безпечні умови виконання робіт відносять:

1. Порядок підготовки робочого місця;

2. вимикання (зняття напруги);

3. вивішування плакатів безпеки. Обгородження робочого місця;

4. перевірка відсутності напруги;

5. встановлення заземлень.

Кожен повинен знати і пам’ятати, що змінювати послідовність виконання технічних заходів, що створюють безпечні умови виконання робіт забороняється.

Безпека кожного із нас залежить насамперед від особистої свідомості небезпеки при експлуатації електроустановок споживачів.

4.2 Техніка безпеки при роботі з ПК

В умовах сьогодення багато видів виробничої, наукової та навчальної діяльності, пов’язані з підвищеним навантаженням на зорову систему — очі. У комбінації з гіподинамією та нервово-емоційною напругою тривале збереження основної робочої пози нерідко стає причиною розвитку зорового й загального стомлення, що може привести до зниження працездатності. Зорова система людини погано пристосована до розглядання зображення на екрані монітора. Тому у користувача персонального комп’ютера може виникати головний біль і запаморочення, очі починають сльозитися, з’являється втома, двоїння зображення. Це явище отримало назву «комп’ютерний зоровий синдром». Як же уникнути шкідливого впливу монітора на очі і знизити їхню втомлюваність?

Як з’ясувалося, максимальний час, протягом якого людина безпечно може працювати на комп’ютері, становить не більше п’яти годин. Тим, хто сидить за комп’ютером довше, проблем зі здоров’ям не уникнути. А ось перелік найбільш частих порушень і симптомів, що виникають у результаті тривалої роботи за комп’ютером:

1. Неясність зору, коли людина дивиться вдалину;

2. двоїння в очах;

3. утрудненість концентрації уваги;

4. хворобливі відчуття в очах, сверблячка, різь і сльозотеча, печіння, стомлення;

5. головний біль у надбрівній частині чола, в потиличній, тім'яний і скроневих частинах голови;

6. пропуски в наборі, зсув слів або цифр, перескакування з рядка в рядок, повторення знаків у тексті;

7. відчуття поколювання й біль в руках, зап'ясті, долонях, напруга у верхній або нижній частині тулуба.

Усе це — симптоми перенапруги. Вони виникають через недотримання принципів ергономіки (ергономіка — наука, яка комплексно вивчає особливості виробничої діяльності людини в системі «людина-техніка-довкілля» задля її ефективності, безпеки та комфорту). Головний привід для занепокоєння й найбільша загроза здоров'ю — статичність пози, нерухомість, особливо м'язів голови, які потребують динамічного режиму роботи. Тому при роботі на комп'ютері насамперед потрібно подумати про створення комфортного робочого місця та спеціального рухового режиму для м'язів усього тіла й особливо очей.

Воно має бути гарно освітлене. У кімнаті повинно бути стільки світла, скільки вдень на вулиці. Займатися потрібно при верхньому або настільному світлі, промені світла не повинні потрапляти прямо в очі. Природне світло має падати зліва збоку. Відстань від екрана до очей має бути не меншою 50 сантиметрів, при цьому екран повинен розташовуватися на рівні очей або трохи нижче. Корисно, час від часу, робити гімнастику для очей. І ще одне правило: моргайте кожні 3–5 секунд — це природній спосіб «змащення», очищення поверхні ока та захист від неприємних відчуттів, таких як сверблячка та печіння очей, їх почервоніння. Особливо це відчувають люди, що носять контактні лінзи.

Не слід також забувати про «спеціальне харчування» для очей. Варто вживати продукти, що зміцнюють судини сітківки ока: чорниці, чорну смородину, моркву. Корисні для очей також вітаміни (особливо комплексні полівітаміни, у яких вітаміни сполучаються з мікроелементами: цинком, кальцієм).

Дотримуючись цих порад, ви значно зменшите долю ризику погіршення стану свого здоров’я, а зокрема зору, під час тривалої роботи за комп’ютером.

ВИСНОВКИ

У ході кваліфікаційної роботи було проведено дослідження проблеми DDoS атак на сервери з операційною системою CentOS 7 та розроблено ефективні методи захисту від таких атак. DDoS атаки є поширеним методом атаки на системи, що може призвести до простоїв, втрати даних та порушення безпеки інформаційної інфраструктури організацій.

У рамках роботи було розглянуто різні механізми та заходи безпеки, які можуть бути використані для захисту від DDoS атак. Було досліджено можливості iptables як інструменту для забезпечення безпеки серверів. Основні методи захисту включали налаштування обмежень кількості з'єднань, обмеження швидкості з'єднань, використання tcp_syncookies, а також налаштування модуля mod_reqtimeout для Apache.

Для ефективного захисту серверів були впроваджені наступні заходи:

1. Встановлення обмежень кількості з'єднань на IP.
2. Обмеження швидкості з'єднань для запобігання надмірному навантаженню.
3. Використання модуля tcp_syncookies для захисту від SYN-флуд атак.
4. Налаштування розміру черги з'єднань для зменшення ефективності атак Slowloris.
5. Використання модуля mod_reqtimeout для Apache, щоб обмежити час очікування запиту.

Також було розроблено та реалізовано методи перевірки та моніторингу серверів для виявлення підозрілої активності та своєчасного реагування на загрози. Особлива увага приділялася збереженню та автоматичному відновленню правил iptables після перезавантаження системи.

Важливість розробленої системи полягає в її універсальності та широкому спектрі застосування. Вона може успішно застосовуватися для виявлення та блокування різних типів DDoS атак, забезпечуючи високу надійність та безпеку серверів CentOS 7.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is a DDoS Attack. URL: https://www.geeksforgeeks.org/what-is-ddosdistributed-denial-of-service/ (дата звернення: 04.02.2024).
2. Learn how DDoS attacks can cripple your network, website, or business. URL: https://www.f5.com/labs/learning-center/what-is-a-distributed-denial-of-service-attack (дата звернення: 04.02.2024).
3. Levels of Protection Against DDoS Attacks. URL: https://solutions-cloud.net/cybersecurity/ddos-attacks-understanding-effects-and-protection/ (дата звернення: 04.02.2024).
4. Mastering CentOS 7. URL https://tuxcare.com/blog/mastering-centos-7-key-features-every-system-administrator-should-know/ (дата звернення: 04.02.2024).
5. iptables command in Linux. URL https://www.geeksforgeeks.org/iptables-command-in-linux-with-examples/ (дата звернення: 04.02.2024).
6. Iptables and logging: How to monitor network traffic. URL https://www.fosslinux.com/100268/iptables-and-logging-how-to-monitor-network-traffic.htm (дата звернення: 04.02.2024).
7. Ванца, В., Тимощук, В., Стебельський, М., & Тимощук, Д. (2023). МЕТОДИ МІНІМІЗАЦІЇ ВПЛИВУ SLOWLORIS АТАК НА ВЕБСЕРВЕР. Матеріали конференцій МЦНД, (03.11. 2023; Суми, Україна), 119-120.
8. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). СИСТЕМА ЗМЕНШЕННЯ ВПЛИВУ DOS-АТАК НА ОСНОВІ MIKROTIK. Матеріали конференцій МЦНД, (17.05. 2024; Ужгород, Україна), 198-200.
9. Іваночко, Н., Тимощук, В., Букатка, С., & Тимощук, Д. (2023). РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД UDP FLOOD АТАК НА DNS СЕРВЕР. Матеріали конференцій МНЛ, (3 листопада 2023 р., м. Вінниця), 177-178.