ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА

Другий (Магістерський)
Освітній рівень

Галузь знань 17 Електроніка та телекомунікації
Шифр і назва спеціальності

Спеціальність 172 Телекомунікації та радіотехніка
Шифр і назва спеціальності

на тему «Ідентифікаційна модель хакерської атаки на мережеве устаткування»

ДРТР.2015004.01.10.ПЗ

Виконав: студент 2 курсу, група $ТР_м$-19-1 _____ А.О. Казімірко
підпис Ініціали, прізвище

Керівник: канд. техн. наук, доц. _____ А.А. Таранчук
підпис Ініціали, прізвище

До захисту допускаю:

Зав. кафедри: д-р техн. наук, доц. _____ С.К. Підченко
підпис Ініціали, прізвище

11.12.2020 р.

Хмельницький, 2020

Хмельницький національний університет

Факультет *програмування та комп'ютерних і телекомунікаційних систем*
Кафедра *телекомунікацій, медійних та інтелектуальних технологій*
Освітній рівень *другий (магістерський)*
Галузь знань *17 – Електроніка та телекомунікації*
Спеціальність 172 – *Телекомунікації та радіотехніка*
Освітня-професійна програма *Телекомунікації та радіотехніка*

ЗАТВЕРДЖУЮ
Зав. кафедрою ТМІТ
«3» 09 2020 р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Казімірко Андрію Олександровичу

1 Тема роботи: *«Ідентифікаційна модель хакерської атаки на мережеве устаткування»*
керівник роботи Таранчук Алла Анатоліївна, к.т.н, доцент
Затверджено наказом по університету від «1» вересня 2020 р. № 118
2 Строк подання студентом роботи на кафедру: 10.12.2020 р.
3 Вихідні дані (характеристика об'єкта, умов дослідження та ін.)
Мета роботи: *побудова ідентифікаційної моделі хакерської атаки на мережеве устаткування».*
Об'єкт дослідження: *процеси хакерської атаки на мережеве устаткування.*
Предмет дослідження: *ідентифікаційна модель хакерської атаки на мережеве устаткування.*
4. Зміст пояснювальної записки (перелік питань, що їх належить розробити)
1. Безпека інтернет з'єднань та атаки на обладнання.
2. Протоколи мережевої взаємодії.
3. Побудова ідентифікаційної моделі хакерської атаки типу SYN flood.
4. Програмні методи захисту від мережевих атак.

Завдання отримав _____

Науковий керівник _____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів (розділів) дипломної роботи	Строк виконання етапів дипломної роботи	Примітка
1	Аналіз літературних джерел	10.09.2020 р.	*виконано*
2	Написання 1 розділу ДР	22.09.2020 р.	*виконано*
3	Визначення проблеми		
	дослідження	29.09.2020 р.	*виконано*
4	Написання 2 розділу	20.10.2020 р.	*виконано*
5	Розробка моделі	27.10.2020 р.	*виконано*
6	Написання тез конференції	2.11.2020 р.	*виконано*
7	Написання 3 розділу ДР	7.11.2020 р.	*виконано*
8	Теоретичне та практичне		
	моделювання	10.11.2020 р.	*виконано*
9	Написання 4 розділу ДР	24.11.2020 р.	*виконано*
10	Оформлення		
	пояснювальної записки до ДР	26.11.2020 р.	*виконано*
11	Оформлення презентаційних матеріалів	30.11.2020 р.	*виконано*

Студент _____ Казімірко А.О.
Підпис Ініціали, прізвище

Керівник роботи _____ Таранчук А.А.
Підпис Ініціали, прізвище

ЗМІСТ

Вступ

Повсюдне поширення мережевих технологій привело до об’єднання окремих машин в локальні мережі, які спільно використовують загальні ресурси, а застосування технології клієнт-сервер привело до перетворення таких мереж в розподілені обчислювальні середовища та зокрема, до появи такого унікального явища, як Internet [1,2].

Розвиток Internet привів до росту числа підключених до нього людей, організацій, які використовують можливості, що надаються цією мережею. Але широке поширення Internet викликало ріст інтересу до проблеми безпеки і змусило частково переглянути її основні положення.

Річ у тому, що Internet забезпечує зловмисникові неймовірні можливості для здійснення несанкціонованого доступу і збій працездатності серверів (хост–машин) по всьому світу. За статистикою [3] найбільш поширеними атаками є так звані DdoS –атаки (англ. distributed denial of service attack), метою яких є вивести об’єкт атаки з робочого стану, це може стати причиною великих фінансових втрат під час простою або витрат на обладнання для захисту від нього, також втрати зарплатні фахівців. Будь який вебмайстер розуміє, що такий збій його сайтів на 2-3 години завдасть серйозної шкоди бізнесу, а якщо це затягнеться на тиждень, то ресурс швидше за все доведеться піднімати знову з нуля. При цьому, збитки власників платних сайтів і серйозних Е- комерційних ресурсів, можуть становити десятки тисяч доларів в день.

Тому завдання виявлення мережевих атак та організація захисту від таких атак є актуальною. Для кращого розуміння проблеми та вирішення цих завдань потрібна розробка моделей виявлення віддалених атак.

Метою роботи: побудова ідентифікаційної моделі хакерської атаки на мережеве устаткування».

Об’єкт дослідження: процеси хакерської атаки на мережеве устаткування.

Предмет дослідження: ідентифікаційна модель хакерської атаки на мережеве устаткування.

Для досягнення поставленої мети в роботі вирішуються наступні задачі:

1. Провести аналіз забезпечення безпеки інтернет з'єднань та існуючих типів атак на мережеве обладнання.

2. Розглянути протоколи мережевої взаємодії з точки зору їх уразливості до хакерських атак.

3. Побудувати ідентифікаційну модель хакерської атаки на TCP типу SYN flood.

4. Розробити та навести програмні методи захисту від мережевих атак.

Наукова новизна отриманих результатів:

1. Побудована удосконалена ідентифікаційна модель атак з використанням віртуалізації машин, дистрибутиву Linux, що дозволило дослідити принципи створення DoS/DDoS атак типу «відмова в обслуговуванні» та дозволяє, в подальшому, визначити можливі шляхи протидії цим атакам.

Практична значимість отриманих результатів:

1. Проведений аналіз літературних джерел та існуючих рішень показав, що атаки здійснюються як на окремих користувачів, так і на організації, завдаючи при цьому величезного морального та матеріального збитку. Це обумовлює необхідність розробки моделей виявлення найбільш поширених атак, серед яких є атаки на мережеве обладнання, а також засобів захисту, які перешкоджали б їх здійсненню.

2. Представлена класифікація і цілі DDoS – атак. Показано, що атаки включають різноманітні механізми взаємодії, взаємодіючи на програмному рівні. Показано, що атаки типу SYN-flood охоплюють усі основні методи втручання в роботу мережевих додатків.

3. Досліджена можливість правил iptables для захисту від атак типу TCP SYN Flood, UDP, ICMP Flood. Розроблений алгоритм проходження пакетів за правилами iptables.

4. Проведений моніторинг мережі за допомогою аналізатора мережних протоколів Wireshark і на основі аналізу сценаріїв з використанням iptables.

Показано, що скрипти iptables та дистрибутив Linux в основному націлені на маршрутизацію та вбудовані пристрої для захисту від DoS / DDoS атак.

Апробація результатів дослідження: результати досліджень представлені у вигляді доповіді на науково-практичній інтернет – конференції молодих науковців і студентів «Інтелектуальний потенціал-2020.

Дипломна робота складається із вступу, чотирьох розділів, висновків до кожного розділу, висновків, списку використаних джерел, 2 додатків. Загальний обсяг роботи складає 78 сторінок комп’ютерного тексту, у тому числі: 45 рисунків та 8 таблиць, список використаних джерел вміщує 25 найменувань.

1 БЕЗПЕКА ІНТЕРНЕТ З'ЄДНАНЬ ТА АТАКИ НА ОБЛАДНАННЯ

1.1 Проблема віддалених атак

Під віддаленою атакою розуміється віддалена інформаційна дія, програмно здійснювана по каналах зв'язку і характерна для будь-якої розподіленої обчислювальної системи. Основною проблемою в питанні забезпечення мережевої безпеки є захист від віддалених атак, який включає і їх виявлення [4,5].

У роботі під віддаленою атакою розумітимемо віддалену інформаційну дію, програмно здійснювану по каналах зв'язку мережі Internet за допомогою передачі деякого числа Internet пакетів (рисунок 1.1).

Рисунок 1.1 – Віддалені атаки через Internet

Ринок засобів виявлення видалених дій нині досить розвинений і на ньому представлені багато продуктів від різних фірм [6, 7], проте механізми

виявлення атак розробляються тільки після їх здійснення, що є великим недоліком цих продуктів.

Розробка методу виявлення видалених мережевих атак є дуже важливим аспектом у справі забезпечення безпеки комп'ютерів в глобальних і локальних мережах, що використовують для передачі даних стік TCP/IP протоколів. Унаслідок незахищеності IP протоколів, що використовуються, можлива величезна кількість атак, які призводять до відмови системи в обслуговуванні, порушенню цілісності, несанкціонованому доступу до даних і, навіть, до втрати даних.

Нині значна частина методів виявлення базується на аналізі даних аудиту після здійснення атаки. Такий підхід до проблеми видалених атак має свої достоїнства і свої недоліки. До достоїнств можна віднести можливість детального вивчення атаки і виявлення умов, при яких вона виникає і досягає свого результату. До недоліків можна віднести той факт, що, принаймні, одна атака буде успішно здійснена. Для подальшого розгляду введемо поняття сигнатури для видаленої атаки. Під сигнатурою розумітимемо послідовність дій, яка призводить до реалізації цієї атаки, і набір умов, при яких атака станеться.

1.2 Віддалені атаки в Internet

З середини 90-х років значно збільшилося число видалених атак в мережі Internet, а також зріс збиток, що заподіюється цими атаками. Статистика організації CERT [8], присвячена зареєстрованим мережевим атакам, що сталися з 1995 по 2000 рік приведена в таблиці 1.1.

Таблиця 1.1 – Статистика мережевих атак за даними компанії CERT

Рік	Число зареєстрованих порушень
1995	2412
1996	2573
1997	2134
1998	3734
1999	6844
2000	25 000

А вже починаючи з 2010 року, кількість атак вимірюється у мільйонах (рисунок 1.2).

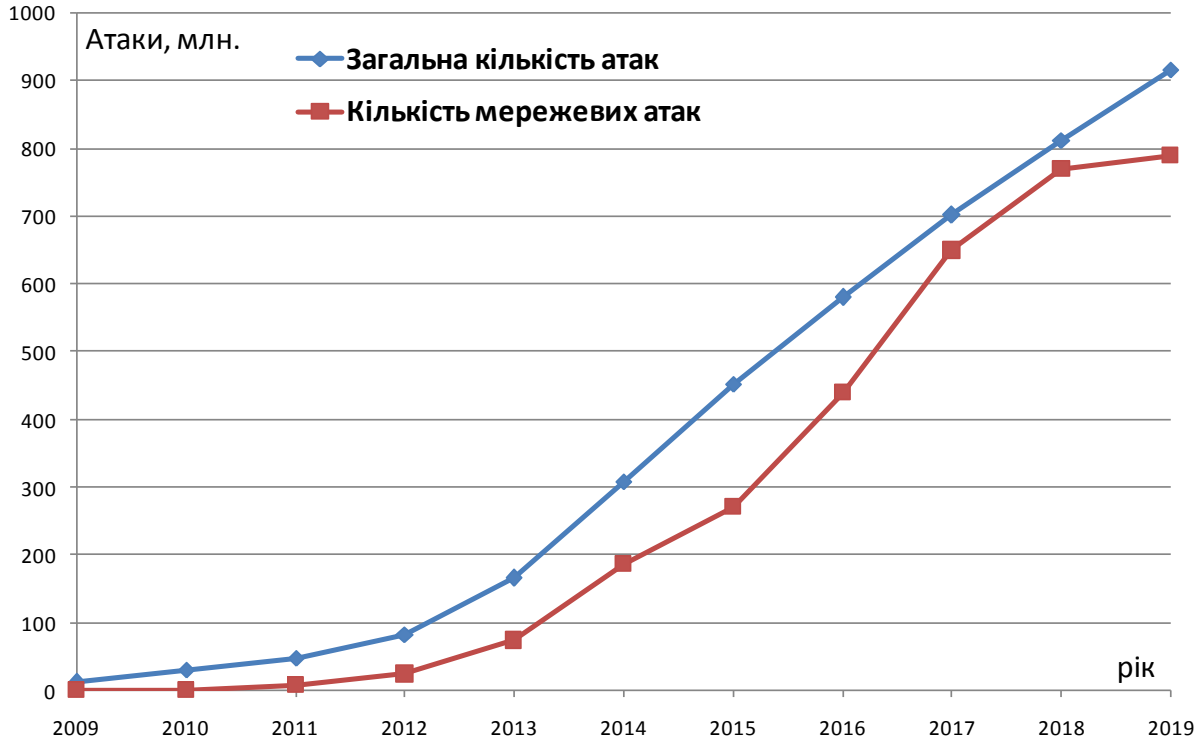


Рисунок 1.2 – Кількість атак [3]

Як можна побачити, мережеві атаки зростають екпоненційно. Фактично файлові атаки зростають набагато меншими темпами. Наявність світової глобальної мережі Інтернет навпаки «стимулює» до розвитку мережевих атак. Статистика 2014-2018 років показала стрімке зростання кібер-атак в мережі Інтернет. За небезпекою, атаки показані на рисунку 1.3.

Дані, приведені на рисунку 1.3 показують зростаючу міру загрози для користувачів Internet, тим самим підкреслюючи необхідність вивчення механізмів видалених атак і розробки засобів захисту від них.

1.3 Систематизація та класифікація віддалених атак

Для того, щоб розробити загальний підхід до виявлення видалених дій, необхідно систематизувати причини успіху видалених атак. Як вже

відзначалося, підхід, що використовується зараз, полягає у детектуванні сигнатур атак після того як вони були проведені.

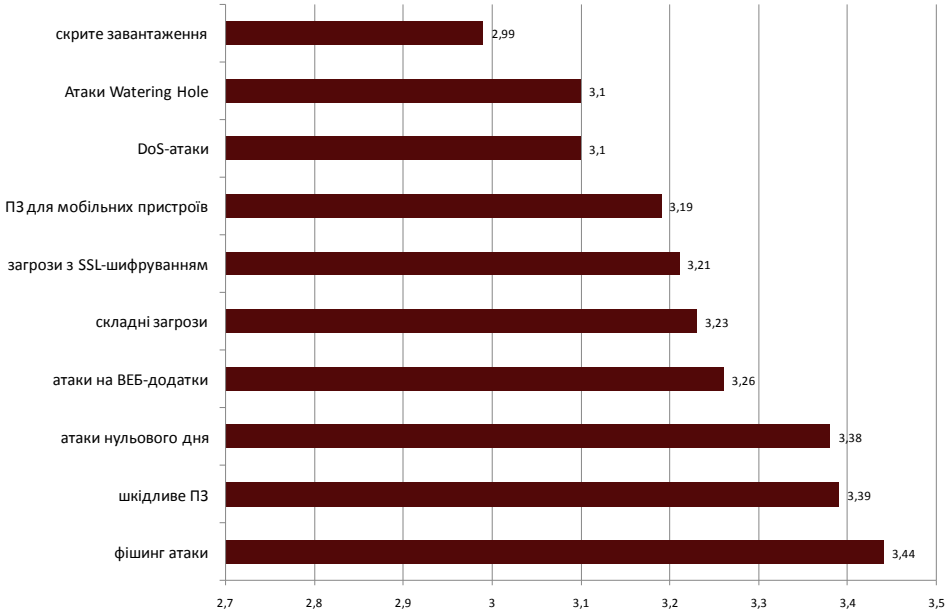


Рисунок 1.3 – Рейтинг загроз за небезпекою (побудовано за інформацією [3, 9])

Запропонований підхід класифікації полягає в аналізі причин успіху таких видалених атак, систематизації в цілому цих причин на основі цієї інформації і виявлення видалених дій на підставі приведеної систематизації.

Основна задача виконання будь-якої класифікації полягає в тому, щоб запропонувати такі характеристики, використовуючи які можна найточніше описати явища, що класифікуються, або об’єкти. Оскільки між локальними і видаленими діями на телекомунікаційних мережах існує велика різниця, те застосування вже відомих узагальнених класифікацій для опису видалених дій не дозволяє досить точно описати саме видалені дії. Це пов’язано з тим, що такі дії характеризуються суто специфічними ознаками для розподілених обчислювальних систем.

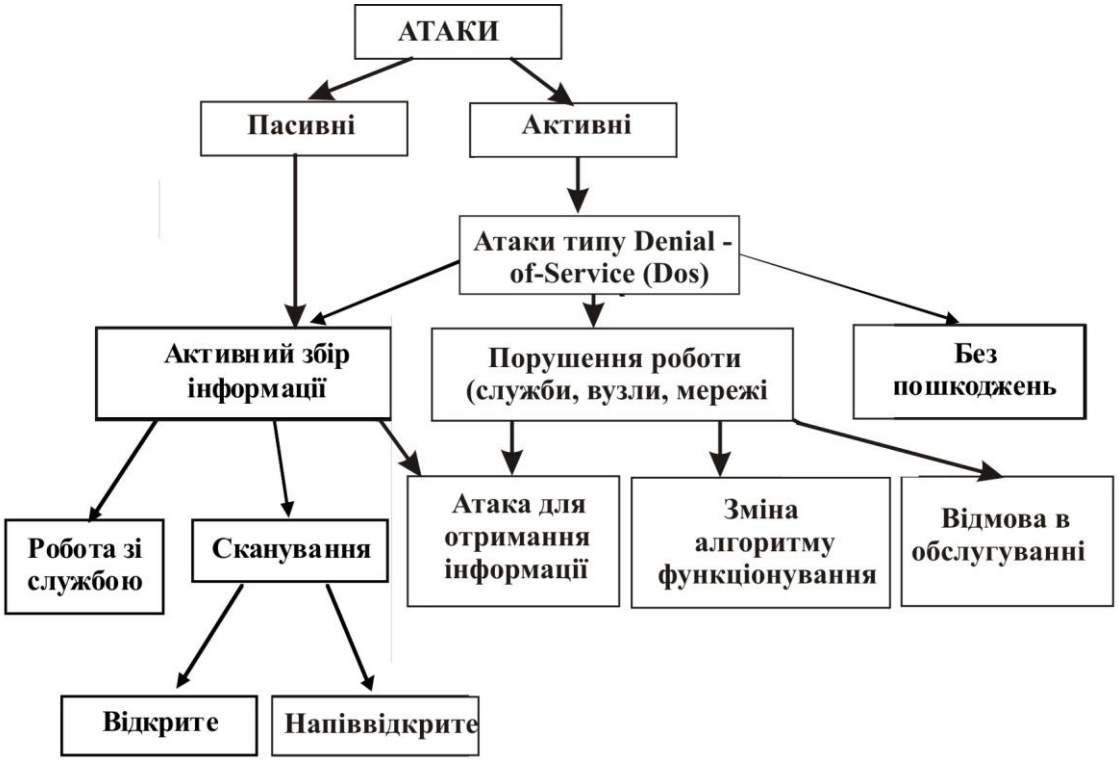


Рисунок 1.4 – Класифікація атак в мережі [2, 5]

1. Пасивні атаки – атаки, при яких виконується збір даних, що передаються в мережі [5, 7]. Атакуюча сторона тільки аналізує пакети даних, що рухаються в мережі. Для учасників мережі ця атака є повністю скритою, атакуюча сторона є невідомою до переходу в активну фазу атак.

2. Активні атаки – атаки, що передбачають створення даних, характер яких відрізняється від очікуваних в системі даних [5, 7].

3. Активні атаки без пошкоджень – атаки, мета яких полягає у проведенні «стрес тестів». Зазвичай притаманна для тестових задач, в яких атакуючі не ставлять за мету втручання в роботу системи, а сама система використовується для оцінки роботи механізмів захисту. Також характерна для атак, при яких атакуюча сторона має на меті добровільно повідомити атаковану про втручання в систему [5,7].

4. Активні атаки для збору інформації – має на меті втручання в роботу системи з метою отримання несанкціонованого доступу до ресурсів системи, збору інформації та даних [5,7].

5. Активні атаки для порушення роботи – один з найбільш відомих видів атак. Починаючи з 2000-х років такі атаки мали на меті виведення з ладу обладнання невеликими групами атакуючих, з 2010-х років атаки типу Denial-Of-Service стають більш поширеними, а цілями – потужні компанії. Виник новий вид атак – Distributed Denial-Of-Service, DdoS. Атаки типу DdoS характеризуються більшою потужністю, масовістю та залученням до атак обладнання інших користувачів, які несвідомо приймають участь в атаці. А з розвитком IoT – виникла нова задача – втручання в роботу IoT з метою отримання інформації з них, а також використання потужностей IoT-пристроїв для участі в DdoS атаках [8].

1.3.1 Різновиди DdoS атак

Неможливо не помітити, що світ поступово підходить до етапу прямої залежності від інформаційних технологій і он-лайн доступу до Мережі. Електронна пошта, SIP-дзвінки, спілкування і безперервне перебування онлайн, проведення платежів або перекладів, Інтернет-купівлі – вже давно доступні з телефонів і планшетів. Саме зараз загроза зупинки безлічі сервісів є актуальною для зловмисників. Тому, використання засобів захисту від DdoS-атак стає таким же актуальним засобом захисту мережі, як брандмауер, система виявлення/запобігання вторгненням або управління уніфікованими загрозами.

У момент проведення DdoS-атаки заражені хости з будь-якої точки світу перевантажують апаратні або програмні ресурси жертви (сервер, мережевий пристрій, мережа) чим викликають відмову в обслуговуванні легітимних клієнтів. Тим самим перериваючи роботу online-сервісів, інформаційних порталів, електронних платежів [6-8].

На рисунку 1.5 відображена проста DdoS-атака. Атакуючі 1 та 2 через проміжні вузли намагаються спотворити роботу цілі.

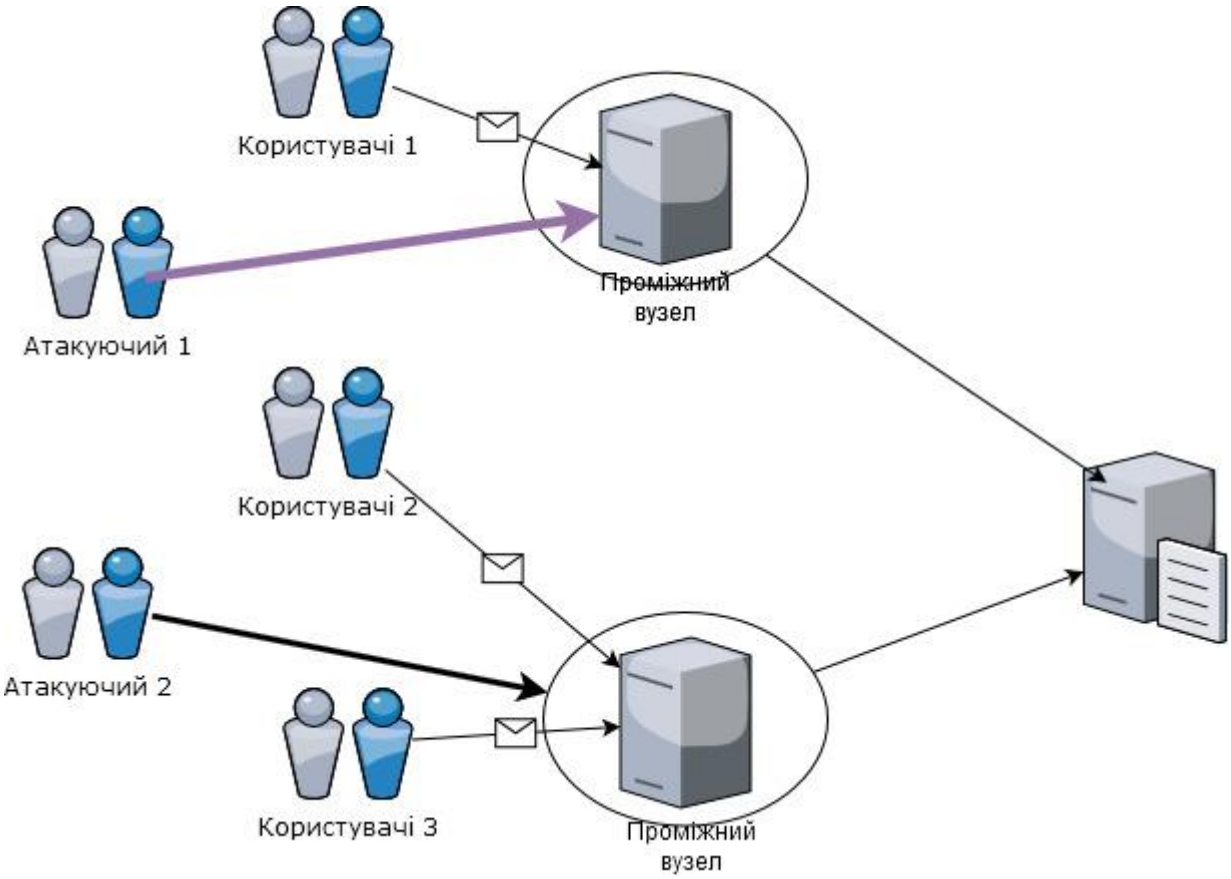


Рисунок 1.5 – Проста DdoS атака

Підходи до проведення DdoS-атак постійно міняються і удосконалюються, також удосконалюються принципи роботи bot-мереж. Для своєчасної реакції на ці зміни з метою недопущення загроз безпеки мережі потрібний постійний моніторинг і аналіз поведінки трафіку в мережі, з чим постійно працюють провідні виробники облаштувань захисту від DdoS.

На сучасному ринку систем захисту від DdoS є присутніми декілька гравців, що пропонують схожі по архітектурі і функціональності рішення. При цьому засоби захисту від DdoS-атак існують як для корпоративних структур різних розмірів, так і для операторів і провайдерів зв’язку с метою захисту їх мережевої інфраструктури і надання сервісу захисту кінцевим користувачам.

1.3.2 Класифікація DdoS-атак

DdoS-атаки можуть бути класифіковані за п’ятьма основними категоріями. У кожному з 5 випадків атаки спрямовані на слабкі місця

реалізацій тієї або іншої категорії [5-8]. Найбільш відома і частіше використовувана атака типу «Відмова в обслуговуванні» (рисунок 1.6).

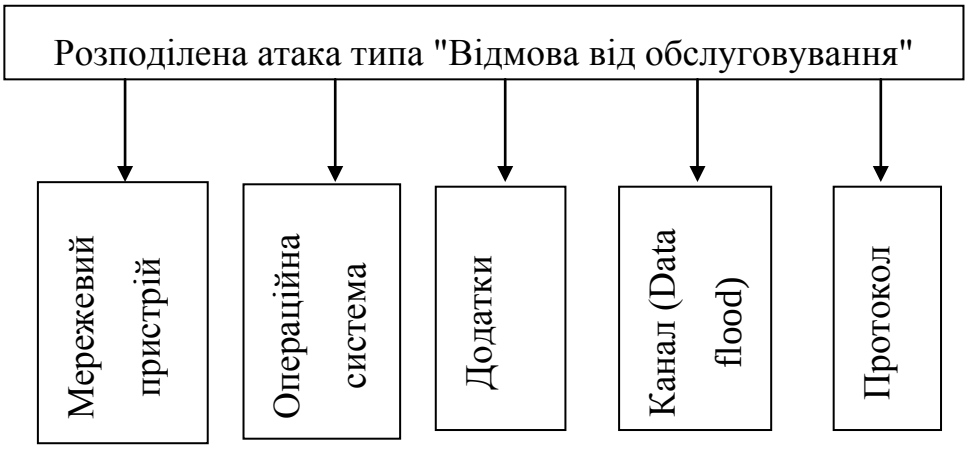


Рисунок 1.6 – Класифікація DdoS атак [5,8]

За класифікацією існують наступні типи атак:

1. Розподілена атака на мережевий пристрій [5,8]. Так, при атаці безпосередньо на мережевий пристрій (англ. Network Device level), можуть бути використані помилки або недоліки програмного забезпечення або особливості апаратної реалізації устаткування, при яких може наставати вичерпання його апаратних ресурсів. Одним з простих прикладів атак на мережевий пристрій є переповнювання його буфера, під час процедури автентифікації користувача за паролем. Використовуючи цю уразливість, зловмисник нейтралізує можливість підключення до пристрою за допомогою протоколів telnet або ssh.

2. Розподілена атака на операційну систему (ОС). Атаки на операційну систему (англ. OS level) проводяться за допомогою використання особливостей реалізації ОС [5, 8]. Наприклад, до цієї категорії DdoS належить атака Ping of Death. У цій атаці ICMP exo – запити (англ. echo request) що мають загальний розмір, який перевищує максимальний розмір IP –пакету, вирушає до потенційної жертви. Ця атака часто призводить до збою роботи операційної системи, оскільки пов’язана з особливостями реалізації стека протоколів TCP/IP.

3. Розподілена атака на додатки (англ. Application – based attacks). Атаки рівня додатка (англ. Application – based attacks) намагаються взаємодіяти з робочими станціями або сервісами на предмет використання їх помилок на рівні мережевих застосувань, які працюють на хостах пристроїв, що піддаються атаці або використати ці застосування для утилізації ресурсів потенційної жертви [5,8] (пошук точок високої алгоритмічної складності і використання їх з метою знешкодження доступних ресурсів віддаленого хосту). Одним з прикладів атак на рівні мережного застосування є finger bomb – коли зловмисник може викликати рекурсивну маршрутизацію на хост жертви.

4. Розподілена атака на канал (англ. Data Flooding) [5,8]. Застосовуючи Data Flooding атаку, зловмисник намагається утилізувати доступну смугу пропускання мережі, хосту або пристрою, пересилаючи великі кількості даних, що спричиняє за собою переповнювання (забивання) каналу зв’язку. В даному випадку, той, що атакує просто використовує бомбардування доступної смуги пропускання, великими безглуздими пакетами з підробленою адресою джерела. Прикладом може служити атака типу ping flood.

5. Розподілена атака на протоколи (англ. Protocol fiture attack) [5,8]. Атака на протокол (англ. protocol attack) використовує стандартні властивості опису протоколу. Наприклад, деякі атаки використовують той факт, що IP адреси джерела можуть бути заміщені, а це не перевіряється жодним механізмом. Деякі, навпаки, сфокусовані на DNS-серверах та запитах і атакують кеш – записи DNS-серверів. Зловмисник, що має власний сервер імен, може змусити DNS-сервер, який атакує, помістити у свій кеш хибний запис, який не відповідатиме адресі призначення.

1.3.3 Типова процедура початку підключення

Установка TCP-підключення виконуються за алгоритмом «потрійного рукостискання» – 3-way handshake [9]:

- клієнтом обирається і передається серверу деяке випадкове значення sequence number – C-SYN;

- у відповідь, сервер надсилає у зворотному напрямку клієнтові пакет даних з вмістом підтвердження запиту – C-ACK і власний номер (іж м. sequence number) – сервера S-SYN.

- клієнт надсилає підтвердження – S – ACK.

На рисунку 1.7 наведена схема установки TCP-підключення [10].

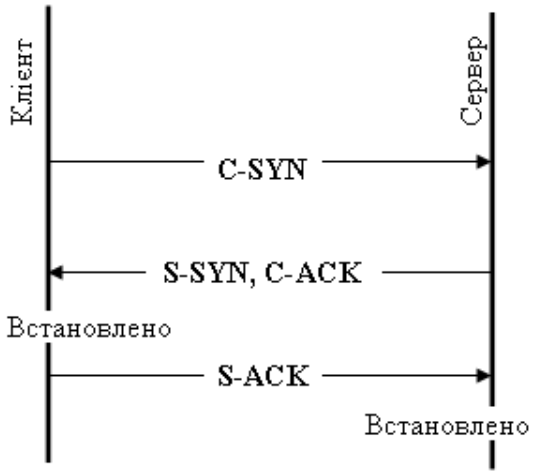


Рисунок 1.7 – Встановлення з’єднання між клієнтом та сервером

Після виконання останнього кроку з’єднання вважається встановленим і можна здійснювати обмін даними.

1.3.4 Загальний опис процедур атак

Опишемо детальніше атаки DdoS, представивши їх прикладами атак, що стали найбільш відомими для цього різновиду втручання [10].

Для спроби злому певного хосту A, атакуюча сторона C може спробувати прикинутися хостом B, отримавши доступ до хосту A на певний період часу. При цьому потрібно виконати такі дії:

1) атакуюча сторона C висилає декілька IP-пакетів в адресу хосту A, що ініціюють з’єднання між C та A з метою з’ясування поточного стану sequence number хосту.

2) атакуюча сторона C надсилає IP-пакет, в якому вже включена адреса хосту B.

3) хост A відповідає пакетом зі своїм значенням номеру послідовності, який далі спрямовується до хосту B. Проте хост B ніколи не отримає його через

те, що він тимчасово виведений з ладу. Атакуюча сторона на основі певного попереднього аналізу має прийняти певні рішення щодо встановлення, яке значення індивідуального номеру послідовності було вислано хосту B.

4) атакуюча сторона C має підтвердити відповіддю, що відбулося «отримання» пакету від хосту A, для цього виславши від імені системи B пакет з відповіддю S-ACK. При цьому, якщо хости A, B та C розміщені в одному сегменті, то для атакуючої сторони задача з'ясування номеру послідовності спрощується – достатньо перехопити пакет, посланий хостом від A до B. Після всіх попередньо виконаних дій стороною атаки C, номер послідовності хосту визначається вірно і з'єднання встановлюється.

Тепер атакуюча сторона може вислати черговій фальшивий IP-пакет, який вже міститиме підроблені дані. Даний алгоритм наведений на рисунку 1.8.

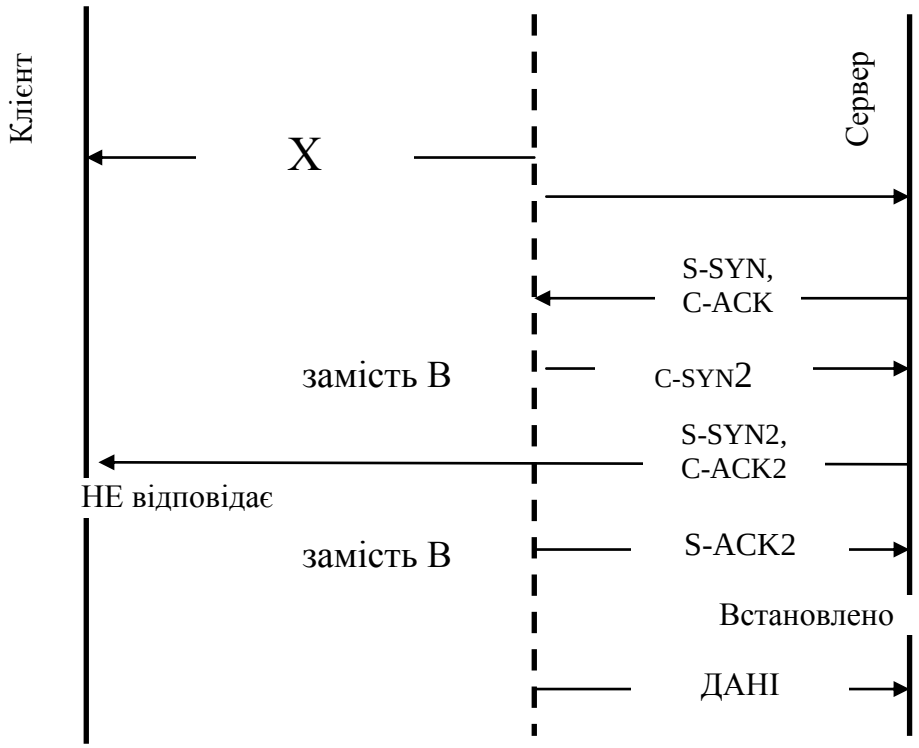


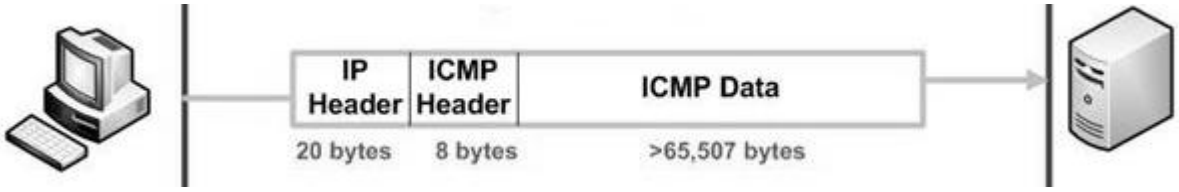
Рисунок 1.8 – Процедура неавторизованого доступу при атаці [5]

1.4 Атаки «відмова в обслуговуванні» та розподілена «відмова в обслуговуванні»

Існує декілька типів атак «відмова в обслуговуванні» на протокол TCP/IP, що ґрунтуються на особливостях стека та обробки пакетів. Якщо атака типу

«Відмова в обслуговуванні» проводиться одночасно відразу з великого числа комп'ютерів, то в цьому випадку говорять про DdoS-атаці. Перерахуємо найбільш відомі [5,7,9]:

1. Атака Ping-of-Death використовує таку уразливість протоколу TCP/IP як фрагментація пакетів даних. В процесі передачі по мережі пакети даних розділяються на фрагменти, які збираються в єдине ціле вже після прибуття на комп'ютер-адресат. Атака відбувається таким чином: на комп'ютер жертви посилається сильно фрагментований ICMP-пакет, розмір якого перевищує допустимий за протоколом – 64 KB. Коли пристрій, що атакується, отримує фрагменти і намагається відновити пакет, ОС зависає та перестає працювати миша і клавіатура. Атакам такого типу можуть піддатися операційні системи сімейства Windows, Mac і Unix.



IP Header та ICMP Header – заголовки IP та ICMP, відповідно; ICMP Data – дані ICMP

Рисунок 1.9 – Тип атаки Ping-of-Death при якій розмір ICMP більше ніж дозволений стандартом [5,9]

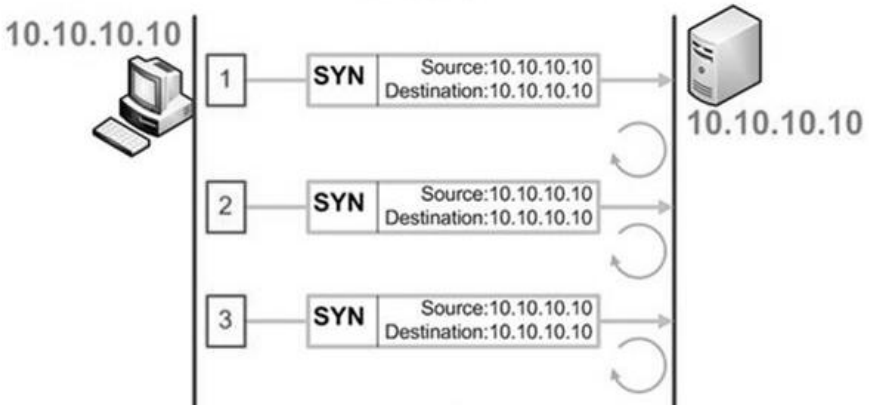
2. Атака SYN-flooding. В основі зв'язку та обміну повідомленнями між хостами користувачів глобальної мережі Інтернет лежить набір протоколів TCP/ IP – це простий набір правил (стек) обміну інформацією, або протокол управління передачею [5,9].

Даний стек має слабкі місця, які полягають в його вразливості до хакерських атак типу TCP SYN Flood при підключенні хост машин користувачів до мережі Інтернет. Користуючись цією слабкістю, хакери можуть атакувати систему певного користувача в будь –який час. Мережева атака SYN Flood полягає у відправці великої кількості пакетів SYN-запитів на

підключення за протоколом TCP до операційної системи іншого хосту, причому пакети надсилаються в дуже короткий інтервал часу [5, 10].

3. Атака Land також базується на використанні особливості протоколу TCP/IP, а саме те що на запит з'єднання треба обов'язково відповісти (рисунок 1.11) [5,9]. Суть атаки Land полягає в тому, що комп'ютер-жертва в результаті дій зловмисників намагається встановити з'єднання сам з собою, що призводить до надмірного навантаження процесора і викликає повний збій ОС або аварійне вимикання хосту.

4. Пакетна фрагментація. Відповідно до протоколу TCP/IP, пакети даних розбиваються на фрагменти. Фрагментація використовується при необхідності передачі IP-дейтаграми, тобто блоку інформації, що передається за допомогою протоколу IP, мережею, в якій максимально допустима одиниця передачі даних менше розміру цієї дейтаграми. Атаки цього типу викликають відмову в обслуговуванні, використовуючи слабкі місця деяких стеків TCP/IP, пов'язаних зі зборкою IP-фрагментів [5,7,9].



Source – адреса джерела; Destination – адреса отримувача

Рисунок 1.10 –Тип атаки Land

Прикладом може служити атака TearDrop, в результаті якої під час передачі фрагментів відбувається їх зміщення, що при зборці пакету викликає їх перекриття. Спроба комп'ютера, що атакується, відновити правильну послідовність фрагментів викликає аварійне завершення системи.

5. Атака DNS flooding полягає в передачі величезної кількості запитів до DNS-сервера. DNS-сервер відповідає за трансляцію символьного імені сервера та його IP-адрес. Велика кількість запитів призводить до перевантаження сервера DNS і робить неможливим звернення до нього інших користувачів [5,9].

6. Атака IP Hijacking. Якщо у попередньому випадку атакуюча сторона ініціювала нове з'єднання, то в даному випадку зловмисник перехоплює увесь мережевий потік [5,7,9], модифікуючи його і фільтруючи довільним чином. Метод є комбінацією «підслуховування» і IP – підміни.

Необхідні умови атаки – атакуюча сторона повинна отримати доступ до сервера, що знаходиться на шляху мережного потоку і мати достатні права керування на ній для створення та перехоплення IP-пакетів.

При передачі даних використовуються значення «номеру послідовності» та «номеру відповіді» (поля IP-заголовку). Виходячи з їх значення, сервер і клієнт перевіряють коректність передачі пакетів.

Існує можливість ввести з'єднання в так званий «десинхронізований стан». Тоді пакети, що присилаються сервером мають значення «номеру послідовності» та «номеру відповіді», які не відповідають очікуваним значенням клієнтом, і навпаки.

В даному випадку атакуюча сторона починає процес «прослуховування» лінії, та може взяти на себе функцію посередника, створюючи коректні пакети для клієнта і сервера і перехоплюючи їх відповіді.

Метод дозволяє в обхід системи захисту сервера з використанням, наприклад, одноразових паролів, оскільки атакуюча сторона транслює початковий етап з'єднання та починає активну роботу з модифікації даних вже після того, як відбудеться авторизація користувача.

З'єднання мережею здійснюється на стадії його установки:

- атакуюча сторона прослуховує сегмент мережі яким проходитимуть пакети сесії, що цікавлять його.

- дочекавшись пакет S – SYN від сервера, атакуюча сторона висилає серверу пакет типу RST (скидання), звичайно, з коректним sequence number, і, негайно, услід за ним фальшивий C – SYN-пакет від імені клієнта.
- сервер скидає першу сесію і відкриває нову, на тому ж порту, але вже з новим sequence number, після чого посилає клієнтові новий S-SYN-пакет.
- клієнт ігнорує S– SYN-пакет, проте атакуюча сторона, що прослуховує лінію, висилає серверу S-ACK-пакет від імені клієнта.
- отже, клієнт і сервер знаходяться в стані ESTABLISHED, проте сесія десинхронізована.

Схема реалізації IP Hijacking наведена на рисунку 1.11.

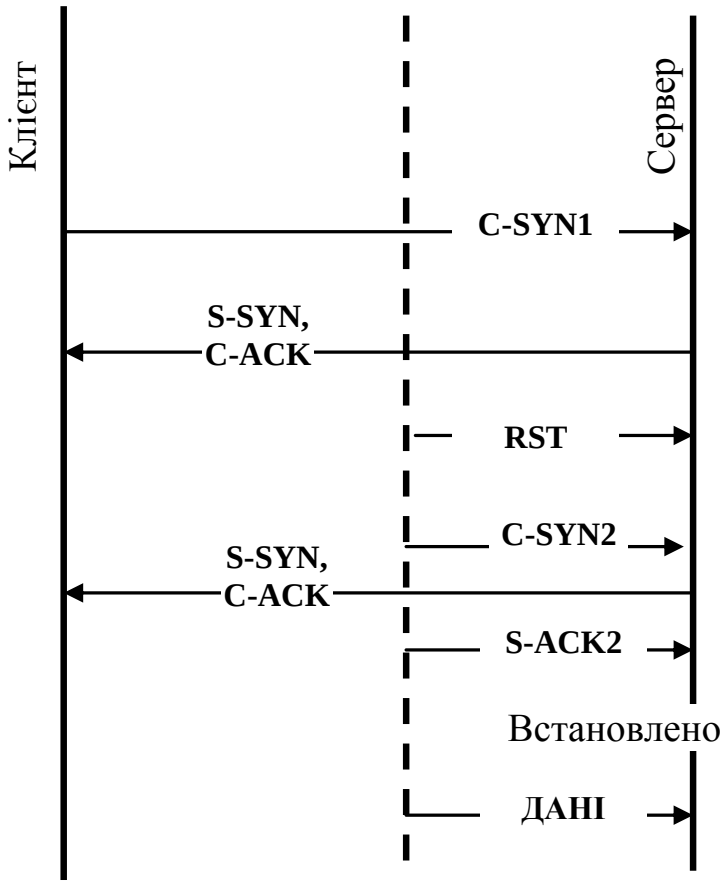


Рисунок 1.11 – IP Hijacking

Зрозуміло, що 100% спрацьовування у цієї схеми немає, наприклад, вона не застрахована від того, що по дорозі не загубляться якісь пакети, послані

атакуючою стороною. Для коректної обробки цих ситуацій програма має бути ускладнена.

DdoS-атака або «розподілена відмова в обслуговуванні» – це різновид DoS-атак. DdoS-атака організовується за допомогою дуже великого числа комп'ютерів, завдяки чому атаці можуть бути схильні сервера навіть з дуже великою пропускною спроможністю Інтернет-каналів.

Для організації DdoS-атак зловмисники використовують ботнет – спеціальну мережу комп'ютерів, заражених особливим видом вірусів. Кожним таким комп'ютером зловмисник може управляти видалено, без відома власника. За допомогою вірусу або програми, що майстерно маскується під легальну, на комп'ютер-жертву встановлюється шкідливий програмний код, який не розпізнається антивірусом і працює у фоновому режимі. У потрібний момент по команді власника ботнета така програма активізується і починає відправляти запити на сервер, що атакується, внаслідок чого заповнюється канал зв'язку між сервісом, на який проводиться атака, і Інтернет-провайдером і сервер перестає працювати.

Розподілену атаку можна провести з допомогою не лише ботнета, але і механізму відображення. Такі атаки називаються DrDOS-атаки (атаки непрямої дії, Distributed Reflection DoS) [11,12]. Вони здійснюються не безпосередньо, а через посередників. Частіше усього DrDoS-атаки відбуваються таким чином: TCP-пакет вирушає не на комп'ютер, що атакується, а на будь-який сервер в Інтернеті, але в якості зворотної адреси вказується саме адреса комп'ютера-жертви. Оскільки будь-який сервер на пакет TCP с SYN-флагом обов'язково відповідає пакетом TCP с прапорами SYN+ACK, довільно вибраний комп'ютер, не підозрюючи про це, відповідає на неправдиві запити і автоматично закидає потоками пакетів комп'ютер-жертву.

Висновки до першого розділу

1. Бурхливий кількісний ріст користувачів Internet і збільшення можливостей, що надаються користувачам, стримується небезпекою віддалених атак. Атаки здійснюються як на окремих користувачів, так і на організації, завдаючи при цьому величезного морального та матеріального збитку. Це обумовлює необхідність розробки моделей виявлення найбільш поширених атак, серед яких є атаки на мережеве обладнання, а також засобів захисту, які перешкоджали б їх здійсненню.

2. Нині механізми виявлення віддалених атак розробляються тільки після аналізу здійснених атак. Основна перевага цього підходу – виявлення усіх тонкощів атаки, а недоліки – атака, хоч би раз, має бути реалізована. У роботі запропонований інший підхід вирішення проблеми виявлення віддалених атак, в основі якого лежить систематизація причин успіху видалених атак.

3. Запропонована систематизація показує, що причини успіху видалених атак зводяться до трьох головних дій – це відхилення від заголовку IP пакету, підміна адрес отримувача та джерела, порушення порядку утворення з’єднань. Необхідно відмітити, що запропонована систематизація видів атак не є повною, оскільки не розглядає, наприклад, атаки, спрямовані на з’єднання між хостами. Незважаючи на цей недолік, ця систематизація дозволяє розробити метод виявлення віддалених дій, яка застосована до атак, здійснюваних на мережевому і транспортному рівнях моделі протоколів взаємодії відкритих систем.

2 ПРОТОКОЛИ МЕРЕЖЕВОЇ ВЗАЄМОДІЇ

2.1 Загальна характеристика протоколу TCP/IP

Acronym TCP/IP – походить від протоколу міжмережевої взаємодії протоколу/контролю та передачі і посилається на сім'ю мережевих протоколів, які є основою для комунікацій для обміну даним, що обмінюються через інтернет та приватними IP мережами. Розвиток TCP/IP почався в 1970 від роботи DARPA. Поки сім'я протоколу використовувала, щоб конкурувати з альтернативними протоколами, як наприклад AppleTalk Apple, IPX/SPX Novell або Netbeui Microsoft, TCP/IP зараз встановив себе як універсальний і всесвітній популярний протокол. Його перевагою є незалежність від платформи і доступність для пристроїв з усіма операційними системами. Причини для успіху стеку протоколу TCP/IP – поява Інтернету, його гнучкість і різносторонність [13].

Ключовими перевагами і характеристики TCP/IP є [13]:

1. TCP/IP може бути використаний незважаючи на мережеву технологію і архітектуру головного комп'ютера. Це створює універсальні, гнучкі з'єднання, вибір мережі і не вимагає ніяких керувань зі сторони центральних адміністрацій. Ця децентралізація гарантує високу надійність. TCP/IP є до того ж повністю прикладний незалежний політичний діяч і може бути використаний для великої різноманітності додатків і цілей. Стандартизовані протоколи, застосовні до програм, роблять TCP/IP універсальним. Поки IP управляє адресацією і мережевими напрямами на мережевому рівні, TCP забезпечує з'єднання, що орієнтовані на транспорт даних.

2. З'єднання орієнтовані на передачу даних через TCP. На відміну від протоколу UDP (протокол призначений для передачі дейтаграм), з'єднання TCP це наскрізні з'єднання з обміном дуплексними даними. Перед обміном даних, партнери комунікації встановлюють зв'язок і визначають параметри обміну даних. Впродовж передачі, TCP може забезпечити передачу даних через

підтвердження. Крім того, здійснюються механізми управління потоком, стискування і запобігання перевантаження хостів.

3. Вищі горизонтальні протоколи, побудовані на стеку протоколу TCP. Ряд протоколів прикладного рівня будуються на TCP/IP. Серед інших, вони включають FTP (протокол передачі файлу), HTTP (гіпертекстовий протокол передачі), Telnet (мережа телетайпу) або SMTP (простий поштовий протокол).

2.2 Структура стека TCP/IP і коротка характеристика протоколів

Стек TCP/IP був створений до появи моделі взаємодії відкритих систем ISO/OSI, тому надамо відповідність рівнів стека TCP/IP рівням моделі OSI умовно [13,14]:

1. Фізичний мережевий рівень. Фізичний мережевий рівень визначає характеристики обладнання, яке буде використовуватися для мережі. Наприклад, фізичний мережевий рівень визначає фізичні характеристики носіїв зв'язку. Фізичний рівень TCP / IP описує апаратні стандарти, такі як IEEE 802.3, специфікація мережевих носіїв Ethernet та RS-232, специфікація стандартних контактних з'єднань.

2. Шар зв'язку даних. Рівень каналу передачі даних визначає тип мережного протоколу пакету, в даному випадку TCP / IP. Рівень каналу передачі даних також забезпечує управління помилками та «обрамлення». Прикладами протоколів рівня каналу передачі даних є кадрування Ethernet IEEE 802.2 та кадрування протоколу PPP (англ. Point-to-Point Protocol).

3. Інтернет-шар. Цей рівень, також відомий як мережевий рівень, приймає та доставляє пакети для мережі. Цей рівень включає потужний Інтернет-протокол (IP), протокол розпізнавання адрес (ARP) та протокол керування повідомленнями Інтернету (ICMP).

2.2.1 Протокол IP

Протокол IP та пов’язані з ним протоколи маршрутизації є, можливо, найбільш значущим з усього набору TCP / IP. IP відповідає за наступне [15]:

1. IP-адресація – Конвенція про IP-адресацію є частиною протоколу IP. У главі 3, «Планування вашої мережі TCP / IP (Завдання)» цієї Конвенції, детально описується адресація Ipv4, а глава 14, Ipv6 (Огляд) детально описує адресацію Ipv6.

2. Зв’язок між хостом і хостом – IP визначає шлях, який повинен пройти пакет, на основі IP-адреси приймаючого хосту.

3. Форматування пакетів – IP збирає пакети в одиниці, які відомі як дейтаграми IP. Дейтаграми повністю описані в Internet Layer.

4. Фрагментація – якщо пакет занадто великий для передачі через мережевий носій, IP на хості розбиває цей пакет на менші фрагменти. Потім IP на приймальному хості реконструює фрагменти в оригінальний пакет.

Щоб уникнути плутанини при зверненні до Інтернет – протоколу, використовується одна з наступних конвенцій:

- коли термін IP використовується в описі, опис застосовується як до Ipv4, так і до Ipv6.
- коли в описі використовується термін Ipv4, опис застосовується лише до Ipv4.
- коли в описі використовується термін Ipv6, опис застосовується лише до Ipv6.

Інші протоколи стеку:

1. Протокол розпізнавання адрес (ARP) концептуально існує між рівнями передачі даних та Інтернетом. ARP допомагає IP-адресові направляти дейтаграми на відповідний приймаючий хост, зіставляючи адреси Ethernet (довжиною 48 бітів) з відомими IP-адресами (довжиною 32 біти).

2. Протокол ICMP. Протокол керування повідомленнями Інтернету (ICMP) виявляє та повідомляє про стан помилок мережі. ICMP повідомляє про наступне:

- скинуті пакети – пакети, які надходять занадто швидко для обробки;
- помилка підключення – хост – адресат, якого неможливо отримати;
- переадресація перенапрямлення хоста – відправника на використання іншого маршрутизатора.

3. Транспортний рівень. Протоколи транспортного рівня TCP / IP [13] гарантують, що пакети надходять послідовно і без помилок, міняючи місцями підтвердження прийому даних та повторно передаючи втрачені пакети. Цей тип спілкування відомий як «наскрізний». Протоколами транспортного рівня на цьому рівні є протокол управління передачею (TCP) та протокол користувальницьких дейтаграм (UDP).

4. Протокол TCP [13]. TCP дозволяє програмам обмінюватися даними. TCP надсилає дані у формі закритої капсули і передається в залежності від символів, а не у вигляді дискретних пакетів. Ця передача складається з початкової точки, яка відкриває з'єднання, всієї передачі в порядку байтів, і кінцевої точки, яка закриває з'єднання.

TCP приєднує заголовок до переданих даних. Цей заголовок містить велику кількість параметрів, які допомагають процесам на машині відправлення підключатися до однорангових процесів на приймальній машині. TCP підтверджує, що пакет досяг пункту призначення, встановлюючи наскрізне з'єднання між хостами відправника та приймача. Тому TCP вважається «надійним, орієнтованим на з'єднання» протоколом.

5. Протокол UDP. UDP, інший протокол транспортного рівня, який надає послугу доставки дейтаграм. UDP не перевіряє з'єднання між хостами приймальної та передавальної сторони. Оскільки UDP виключає процеси встановлення та перевірки з'єднань, а програми, які надсилають невеликі обсяги даних, використовують UDP, а не TCP [14,15].

2.2.2 Шар додатків

Рівень додатків визначає стандартні Інтернет-послуги та мережеві додатки, якими може користуватися кожен. Ці служби працюють з

транспортним рівнем для надсилання та отримання даних. Існує багато протоколів прикладного рівня. У наведеному нижче списку наведено приклади протоколів прикладного рівня [1,2]:

- стандартні TCP / IP послуги, такі як FTP, TFTPI та TELNET команди;
- команди UNIX “r”, такі як rlogin irsh;
- служби імен, такі як NIS + та система доменних імен (DNS);
- файлові служби, такі як служба NFS;
- простий протокол управління мережею (SNMP), який дозволяє керувати мережею;
- протоколи маршрутизації RIP та RDISC.

2.2.3 Стандартні послуги TCP / IP

1. FTP та анонімний FTP – протокол передачі файлів (FTP) передає файли у віддалену мережу та з неї. FTP дозволяє користувачеві вказати ім’я віддаленого хосту та параметри команди передачі файлів у командному рядку локального хосту. Потім in.ftpd демон на віддаленому хості обробляє запити від локального хосту. На відміну від цього rcp, ftp працюють навіть тоді, коли на віддаленому комп’ютері не працює операційна система на базі UNIX. Користувач повинен увійти до віддаленого комп’ютера, щоб встановити ftp з’єднання, якщо лише віддалений комп’ютер не налаштований на анонімний FTP [2,3].

На сьогодні можна отримати величезну кількість матеріалів з анонімних FTP-серверів, підключених до Інтернету. Університети та інші установи створюють ці сервери, щоб пропонувати програмне забезпечення, наукові роботи та іншу інформацію у відкритому доступі. Для входу на цей тип сервера, використовується ім’я для входу anonymous, звідси термін «анонімні FTP-сервери».

2. Telnet – протокол Telnet дозволяє терміналам та процесам, орієнтованим на термінали, обмінюватися даними в мережі, що працює під керуванням TCP / IP. Цей протокол реалізований як програма telnet (на

локальних машинах), так і демон in.telnetd (на віддалених машинах). Telnet надає користувальницький інтерфейс, за допомогою якого два хости можуть обмінюватися даними символами або рядком за рядком. Додаток включає набір команд, які повністю задокументовані на сторінці користувача telnet.

3. TFTP – тривіальний протокол передачі файлів, що надає функції, подібні до ftp, але протокол не встановлює ftp інтерактивне з'єднання. Як результат, користувачі не можуть перераховувати вміст каталогу або змінювати каталоги. Користувач повинен знати повне ім'я файлу, який потрібно скопіювати. Сторінка користувача telnet (1) описує tftp набір команд.

4. Адміністрація мережі. Простий протокол управління мережею (SNMP) дозволяє переглянути макет мережі та стан основних машин [2,3]. SNMP також дозволяє отримувати складну статистику мережі із програмного забезпечення, яке базується на графічному інтерфейсі користувача. Багато компаній пропонують пакети управління мережею, що реалізують SNMP. Приклад є програмне забезпечення SunNet Manager ™ .

5. Протоколи маршрутизації. Протокол інформації про маршрутизацію (RIP) і протокол виявлення маршрутизатора (RDISC) – це два протоколи маршрутизації для мереж TCP / IP.

2.3 Класифікація і цілі DdoS-атак по рівнях OSI

Інтернет використовує модель OSI. Всього в моделі є присутніми 7 рівнів, які охоплюють усі середовища комунікації: починаючи з фізичного середовища (1-й рівень) і закінчуючи рівнем додатків (7-й рівень), на якому «спілкуються» між собою програми [16].

DdoS-атаки можливі на кожному з семи рівнів. Розглянемо їх детальніше та опишемо дії щодо їх запобігання. Для чого зведемо їх опис за 7 рівнями моделі OSI в таблиці 2.1-2.7.

Таблиця 2.1 – 7-й рівень OSI: прикладний

Тип даних	Дані
Опис рівня	Початок створення пакетів даних. Приєднання і доступ до даних. Призначені для користувача протоколи, такі як FTP, SMTP, Telnet, RAS
Протоколи	FTP, HTTP, POP3, SMTP і шлюзи, які їх використовують
Приклади технологій DoS	PDF GET запити, HTTP GET, HTTP POST (форми веб-сайтів: логін, завантаження фото/відео, підтвердження зворотного зв’язку)
Наслідки DdoS-атаки	Нестача ресурсів. Надмірне споживання системних ресурсів службами на сервері, що атакується

Необхідні дії, які необхідно прийняти для запобігання атакам: моніторинг додатків – систематичний моніторинг програмного забезпечення (ПЗ), що використовує певний набір алгоритмів, технологій і підходів (залежно від платформи, на якому це ПЗ використовується) для виявлення атак 7 рівня. Відслідковуючи такі атаки, їх можна раз і назавжди зупинити, а також і відстежити їх джерело. На цьому шарі це здійснюється найпростіше.

Таблиця 2.2 – 6-й рівень OSI: представницький

Тип даних	Дані
Опис рівня	Трансляція даних від джерела одержувачеві
Протоколи	Протоколи стискування і кодування даних (ASCII, EBCDIC)
Приклади технологій DoS	Підроблені SSL запити: перевірка шифрованих SSL пакетів дуже багато забирає ресурсів, зловмисники використовують SSL для HTTP-атак на сервер жертви
Наслідки DdoS –атаки	Системи, що атакуються, можуть перестати здійснювати SSL з’єднання або автоматично перевантажуватися

Для зменшення шкоди необхідно звернути увагу на такі засоби, як розподіл SSL інфраструктури шифрування (тобто розміщення SSL на іншому сервері, якщо це можливо) і перевірка трафіку додатків на предмет атак або

порушення політик на платформі додатків. Хороша платформа гарантує, що трафік шифрується і вирушає назад до початкової інфраструктури з розшифрованим контентом, що знаходився в захищеній пам'яті безпечного вузла.

Таблиця 2.3 – 5-й рівень OSI : Сеансовий

Тип даних	Дані
Опис рівня	Управління установкою і завершенням з'єднання, синхронізацією сеансів зв'язку у рамках операційної системи через мережу (наприклад, коли ви виконуєте вхід/вихід)
Протоколи	Протоколи входу/виходу (RPC, PAP)
Приклади технологій DoS	Атака на протокол Telnet використовує слабкі місця програмного забезпечення Telnet-сервера на комутаторі, роблячи сервер недоступним
Наслідки DdoS-атаки	Робить неможливим для адміністратора управління комутатором

Необхідні дії для запобігання наслідків такого типу DdoS – атак – підтримка прошивки апаратного забезпечення в актуальному стані для зменшення ризику появи загрози.

Таблиця 2.4 – 4-й рівень OSI: транспортний

Тип даних	Сегменти
Опис рівня	Забезпечення безпомилкової передачі інформації між вузлами, управління передачею повідомлень з 1 по 3 рівень
Протоколи	Протоколи TCP, UDP
Приклади технологій DoS	SYN – флуд, Smurf – атака (атака ICMP-запитами зі зміненими адресами)
Наслідки DdoS –атаки	Досягнення меж за шириною каналу або за кількістю допустимих підключень, порушення роботи мережного устаткування

Необхідні дії – фільтрація DdoS- трафіку, відома як blackholing — метод, що використовується самими провайдерами для захисту клієнтів.

Через свою реалізацію, цей підхід також нерідко робить сайт клієнта недоступним як для трафіку зловмисника, так і для цільового трафіку користувачів. Але все ж блокування доступу дієво використовується провайдерами у боротьбі з DdoS-атаками для захисту клієнтів від таких загроз, як: уповільнення роботи мережного устаткування і відмову роботи сервісів.

Таблиця 2.5 – 3-й рівень OSI: мережевий

Тип даних	Пакети
Опис рівня	Маршрутизація і передача інформації між різними мережами
Протоколи	Протоколи IP, ICMP, ARP, RIP і роутери, які їх використовують
Приклади технологій DoS	ICMP- флуд – Ddos-атаки на третьому рівні моделі OSI, які використовують ICMP-повідомлення для перевантаження пропускної здатності цільової мережі
Наслідки DdoS-атаки	Зниження пропускної здатності мережі, що атакується, і можлива перевантаженість брандмауера

Необхідні дії – обмеження кількості оброблюваних запитів за протоколом ICMP і скорочення можливого впливу цього трафіку на швидкість роботи Firewall і пропускну спроможність інтернет-смуги.

Таблиця 2.6 – 2-й рівень OSI: канальний

Тип даних	Кадри
Опис рівня	Установка і супровід передачі повідомлень на фізичному рівні
Протоколи	Протоколи 802.3, 802.5, а також контролери, точки доступу і мости, які їх використовують
Приклади технологій DoS	MAC-флуд – переповнювання пакетами цих мережевих комутаторів
Наслідки DdoS-атаки	Потоки даних від джерела блокують роботу усіх портів клієнта приймальної сторони

Багато з сучасних комутаторів можуть бути налагоджені таким чином, що кількість MAC адрес буде обмежуватись надійними, які проходять перевірку автентифікації, авторизації і обліку на сервері (протокол AAA) і надалі фільтруються.

Таблиця 2.7 – 1-й рівень OSI: фізичний

Тип даних	Біти
Опис рівня	Передача двійкових даних
Протоколи	Протоколи 100BaseT, 1000 Base-X, а також концентратори, розетки і патч – панелі, які їх використовують
Приклади технологій DoS	Фізичне руйнування, фізична шкода роботи або управлінню фізичними мережними активами
Наслідки DdoS –атаки	Мережне устаткування робиться непридатним і вимагає ремонту для відновлення роботи

Необхідні дії: використання систематичного підходу до моніторингу роботи фізичного мережного устаткування.

2.4 Структура IP пакету

Інтернет – протокол, що є протоколом рівня 3 OSI, бере сегменти даних з рівня 4 (транспорт) і ділить їх на пакети (рисунок 2.1). IP-пакет інкапсулює одиницю даних, отриману з наведеного вище рівня, і додає до свого власного заголовка інформацію [15].

IP заголовок	**Данні**

Інкапсуляція IP пакету

Рисунок 2.1 – Структура IP-пакету

Інкапсульовані дані називаються корисним навантаженням IP. Заголовок IP включає багато необхідної інформації, включаючи номер версії, який в цьому контексті дорівнює 4. Інші подробиці наступні (рисунок 2.2):

1. Версія (англ. Version): версія з номером використовуваного інтернет-протоколу (наприклад, Ipv4).

2. IHL: довжина інтернет-заголовку; довжина усього заголовку IP.

3. DSCP: кодова точка диференційованих послуг; це тип обслуговування.

4. ECN: явне повідомлення про перевантаження; він несе інформацію про затори, помічені на маршруті.

Рисунок 2.2 – Структура заголовку IP-пакету [15]

5. Загальна довжина: довжина усього пакету IP (включає заголовок IP і корисне навантаження IP).

6. Ідентифікація: якщо IP – пакет фрагментований під час передачі, усі фрагменти містять однаковий ідентифікаційний номер. ідентифікувати оригінальний IP – пакет, до якого вони належать.

7. Прапори. Відповідно до вимог мережевих ресурсів, якщо IP –пакет занадто великий для обробки, ці «прапори» вказують, чи можуть вони бути фрагментовані або ні. У цьому 3-бітовому прапорі MSB завжди встановлені в «0».

8. Зміщення фрагмента: це зміщення вказує точне положення фрагмента в початковому пакеті IP.

9. Час життя: щоб уникнути зациклення в мережі, кожен пакет вирушає з деяким встановленим значенням TTL, яке повідомляє мережу, скільки маршрутизаторів (стрибків) може перетнути цей пакет. На кожному стрибку його значення зменшується на одиницю, а коли значення досягає нуля, пакет відкидається.

10. Протокол: повідомляє мережевий рівень на хості призначення, до якого протоколу належить цей пакет, тобто протоколу наступного рівня. Наприклад, номер протоколу ICMP– 1, TCP – 6, UDP– 17.

11. Контрольна сума заголовка: це поле використовується для зберігання значення контрольної суми усього заголовка, який потім використовується для перевірки того, що пакет прийнятий без помилок.

12. Адреса джерела: 32-бітова адреса джерела пакету.

13. Адреса одержувача: 32-бітова адреса одержувача пакету.

14. Опції: це необов’язкове поле, яке використовується, якщо значення IHL більше 5. Ці опції можуть містити значення для таких параметрів, як безпека, маршрут запису, мітка часу і т.інш.

2.5 Недоліки сімейства протоколів TCP/IP

Протоколами називають розподілені алгоритми, що визначають, яким чином здійснюється обмін даними між фізичними пристроями або логічними об'єктами (процесами). Під сімейством протоколів TCP/IP зазвичай розуміють увесь набір реалізацій, описаних в RFC (Requests For Comments, запити на коментування).

Загальним елементом цього сімейства є IP протокол. Усі протоколи мережі Internet є відкритими і доступними. Усі специфікації протоколів доступні з RFC.

Однією з причин популярності TCP/IP є ретельне опрацювання протоколів сімейства TCP/IP, їх функціональність і відкритість, а також можливість нарощування функціональних можливостей. Хоча до теперішнього часу досить очевидно, що вони мають і безліч недоліків, особливо тих, які пов'язані з безпекою, наприклад, немає вбудованих засобів автентифікації, що і робить можливим здійснення атак, заснованих на підміні клієнта.

Схема 7-рівневої моделі сімейства протоколів TCP/IP приведена на рисунку 2.3 [14].

Рисунок 2.3 – Схема 7- рівневої моделі сімейства протоколів TCP/IP

Кожен рівень моделі використовує певний формат повідомлень. При переході з вищого рівня на нижчий рівень повідомлення форматується за правилами нижчого рівня і забезпечується заголовком. На нижчих рівнях виконуються наступні дії:

1. На фізичному рівні здійснюється фізичне з'єднання між комп'ютерною системою і фізичним середовищем передачі.

2. На канальному рівні здійснюється пакетування даних при передачі і розкриття пакетів при прийомі. Одиниця даних на цьому рівні називається фреймом.

3. На мережному рівні здійснюється маршрутизація даних в мережі. Одиницею даних цього рівня є дейтаграма.

2.6 Атаки SYN- flooding як найбільш типова форма атак на мережеве обладнання

Основна ідея атаки SYN-flooding («Смертельне рукостискання») полягає в тому, щоб під час процесу запуску сесії TCP, змушувати хост зберігати досить велику кількість напівз'єднань для вичерпання його ресурсів і не можливості встановлення нових зв'язків [17].

В основі процесу початку TCP сеансу лежить алгоритм «потрійного рукостискання», який реалізується за три кроки (рисунок 2.4) [10]:

1) хост А надсилає пакет з прапором SYN на сервер Б (скор. від англ. synchronize - запит на підключення за протоколом TCP). Якщо відправлений пакет з прапором SYN, це означає, що хост А запитує у хосту Б з'єднання;

2) хост Б надсилає у відповідь пакет з прапором SYN / ACK (скор. від англ. (acknowledges), що містить криптографічну інформацію хосту А;

3) хост А надсилає пакет з прапором ACK до хосту Б, що означає – зв'язок встановлений.

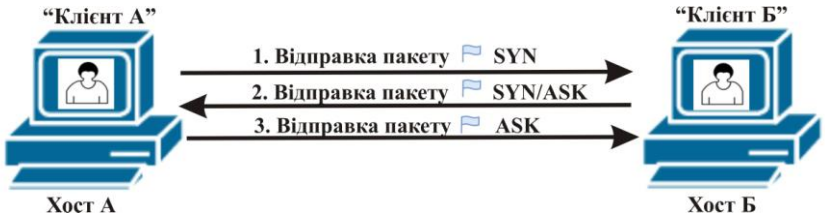


Рисунок 2.4 – Реалізація алгоритму «потрійного рукостискання»

Розглянемо як відбувається атака SYN Flood на деякий хост мережі Інтернет.

Мережева атака TCP SYN Flood використовує тристоронній механізм рукостискання, описаний вище (рисунок 2.4). При цьому, з хосту А зловмисник відправляє пакет з прапором SYN (зазвичай використовується підмінена IP - адреса - англ. spoofing) хосту Б (ціль атаки), запрошуючи ініціалізацію нової

сесії TCP у операційній системі хосту Б. Далі хост Б відправляє пакет з прапором SYN / ACK хосту А. За звичайним тристороннім механізмом рукостискання, при відкритій сесії TCP, хост А повинен надіслати хосту Б пакет з прапором ACK.

Однак атакуюча система А не відповідає ні на один з повернутих пакетів SYN / ACK. У цьому випадку хост Б, очікуючи пакет з прапором ACK від хосту А знаходиться в «напіввідкритому» статусі, встановлюючи неповне з'єднання, яке зберігається у черзі таблиці з'єднань (англ. Transmission Control Block table - TCB). Через 75 секунд неповне з'єднання видаляється із черги TCB і руйнується (рекомендація RFC 4987). Зловмисники використовують цю відкриту сесію, відправляючи на порт хосту Б (ціль атаки) швидкий потік SYN-пакетів, перш ніж хост Б видалить неповні з'єднання з черги TCB у разі не отримання відповідей на надісланий пакет SYN/ACK.

За цей час на хості Б черга запитів на підключення переповниться за рахунок зберігання великої кількості фальшивих «напіввідкритих» з'єднань, які займають всю пам'ять TCB. Коли кількість вхідних з'єднань досягне максимального рівня, тоді всі наступні запити будуть відхилені операційною системою хосту Б. У цьому випадку хост Б взагалі не зможе встановити TCP-з'єднання за рахунок втрати продуктивності. Цей процес називається «відмовою в обслуговуванні» (рисунок 2.5) [17].

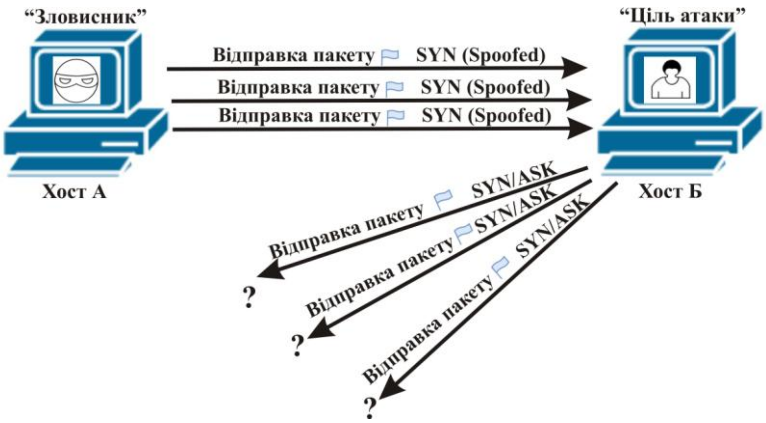


Рисунок 2.5 – Мережева атака SYN Flood та процес - «відмова в обслуговуванні»

Успішна атака залежить від трьох параметрів: розміру загородження; частоти з якою створюються загородження та засобів вибору IP-адрес для підробки (містифікації).

Існує декілька механізмів захисту мережного обладнання (хостів), які можуть частково забезпечити захист від SYN Flood – атак [18]:

1. Настройка стеку. Для цього можна налаштувати стек TCP, зменшивши його час «напіввідкритої» сесії з’єднань, або, іншими словами, тайм-аут звільнення пам'яті, виділеної для з'єднання, а також час виділений на блокування вхідних з'єднань. Але у цих налаштувань можуть бути побічні ефекти у вигляді втрати частини легітимних з'єднань через затримки і нестабільні канали.

2. Реалізація механізму SYN-Cookie. Для створення TCP-з'єднання хост А відправляє хосту Б TCP-пакет з прапором SYN і своїм номером послідовності. Механізм SYN cookies зовсім не використовує чергу SYN. Хост Б відправляє пакет з прапором SYN-ACK, який містить унікальну інформацію, що ідентифікує клієнта Б: IP - адресу; номер порту; час відправки пакету та прийнятий унікальний номер послідовності хосту А. Хост «зловмисника» ніколи не отримує ці пакети і тому не надасть на них відповідь. На завершальній відповіді хостом А ця інформація (хеш) вже включена в пакет з прапором ACK. При успішній перевірці ACK – пакету відповіді на SYN cookie, хостом Б виділиться пам’ять для з’єднання, навіть, якщо в черзі SYN не має відповідного запису. Для використання механізму хешування (порівняння даних) необхідно, щоб усі хости, які приймають участь в передачі трафіку його підтримували. Якщо SYN cookie включені, то «зловмисник» не зможе обійти такі міжмережеві екрани відправкою ACK-пакета з довільним номером послідовності поки не підбере вірний. SYN cookies потрібно включати тільки для публічно доступних портів. Включення механізму SYN cookies – це простий спосіб боротьби проти атаки SYN Flood. Однак при його використанні буде більше завантаженість процесора клієнта під час створення та звірки cookies.

3. Обмеження запитів на нові підключення від конкретного джерела за визначений проміжок часу.

4. Використання мережного протоколу транспортного рівня SCTP (англ. Stream Control Transmission Protocol - протокол передачі з керуванням потоком), який є більш сучасним, на відміну від TCP. Даний протокол використовує механізм SYN cookie та не підданий SYN- Flood атакам. Передача трафіку за протоколом SCTP здійснюється багатьма потоками, а синхронне з'єднання між двома хостами по двох та більше незалежних фізичних каналах (multi-homing) [18].

Висновки до другого розділу

1. Розглянуто характеристику протоколу TCP/IP та стек протоколу TCP/IP. TCP/IP є найбільш завершений, стандартний і у той же час найбільш популярний стек мережевих протоколів. За своєю структурою він повністю відповідає 7 рівневій моделі OSI.

2. Представлена класифікація і цілі DDoS – атак. Атаки включають різноманітні механізми взаємодії, взаємодіючи на програмному рівні: атака на сайти через підбір пар логін – пароль; спроби завантаження великих обсягів даних на веб-сервери: операції зі зміненими заголовками IP-пакетів; маніпуляції з послідовностями ініціалізації з’єднання із сервером, а також атаки на проміжне мережеве обладнання.

3. Розуміння порядку атак базується на визначенні структури IP пакету, що належить до 3-го рівня моделі OSI. Основною проблемою IP пакету є відсутність механізму автентифікації, зміни структури пакету, відхиленні його структури від структури за стандартом.

4. Атаки типу SYN-flood є найбільш типовими за реалізацією та охоплюють основні методи втручання в роботу мережевих додатків. Розуміння принципу створення атаки дозволяє визначити можливі шляхи протидії атакам.

3 ПОБУДОВА ІДЕНТИФІКАЦІЙНОЇ МОДЕЛІ ХАКЕРСЬКОЇ АТАКИ

3.1. Постановка завдання

Близько 90% DDoS атак використовують уразливість TCP протоколу [17]. Широко відомим прикладом подібного роду є атака, відома як затоплення черги напіввідкритих з'єднань. Як було описано в попередньому розділі роботи, при дії такого типу нападу, атакується сервера пакетами із запитами на встановлення з'єднання (TCP SYN flooding). Дослідження атак даного виду широко представлені в науково-технічній літературі, розроблено безліч методів захисту від SYN flood. Однак питання їх якості залишається відкритим.

Напади - це прийоми, які зловмисник використовує для використання вразливості програм. Атака відмовою в обслуговуванні намагається зробити комп'ютерний ресурс недоступним для його призначеного користувача. Атака від повені SYN - це спосіб, який зловмисний хост може спробувати заборонити послуги, що надаються сервером машини, надіславши велику кількість відкритих запитів TCP [17].

Для кращого розуміння процесів, які відбуваються при дії TCP SYN flood, UDP та ICMP flood атак побудуємо ідентифікаційну модель атак з використанням двох віртуальних машин з встановленим програмним забезпеченням Ubuntu 20.04.1 LTS та віртуальної машини підсистеми Windows для Linux версії WSL 2.

3.2 Встановлення на хост віртуальної машини Ubuntu 20.04.1 LTS

Створимо дві відокремлені мережі за допомогою віртуалізації хостів для чого:

Крок 1. Встановимо віртуальну машину за допомогою Hyper-V Quick Create з домашньої сторінки Microsoft [19] (рисунок 3.1):

– запускаємо Hyper-V Quick Create;

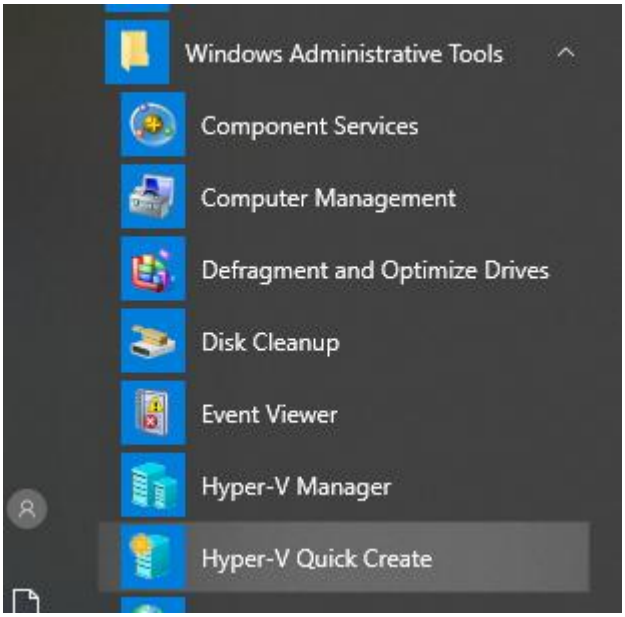
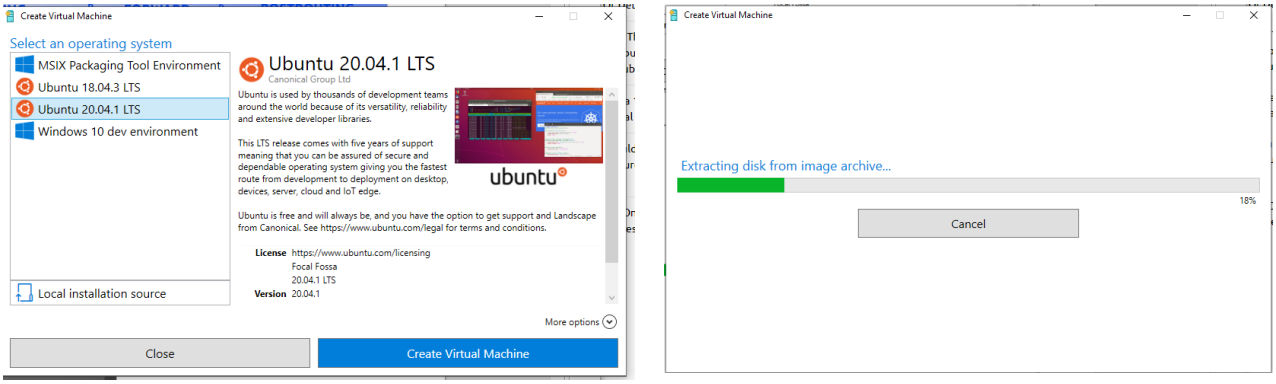


Рисунок 3.1 – Вікно Hyper-V Quick Create

– вибираємо віртуальну машину Ubuntu 20.04.1 LTS “Focal Fossa” [19], характеристиками якої є: покращена продуктивність, стабільність, вона має безліч функцій і містить найновіші драйвери з їх апаратною підтримкою (рисунок 3.2,а). Далі запускаємо Create Virtual Machine (рисунок 3.2,б);



а) б)

Рисунок 3.2 – Встановлення віртуальної машини: початкове вікно Ubuntu 20.04.1 LTS “Focal Fossa” (а); вікно вибору Create Virtual Machine (б)

У результаті правильної установки на екрані з’явиться вікно підтвердження установки віртуальної машини Ubuntu 20.04.1 LTS “Focal Fossa” (рисунок 3.3, а,б);

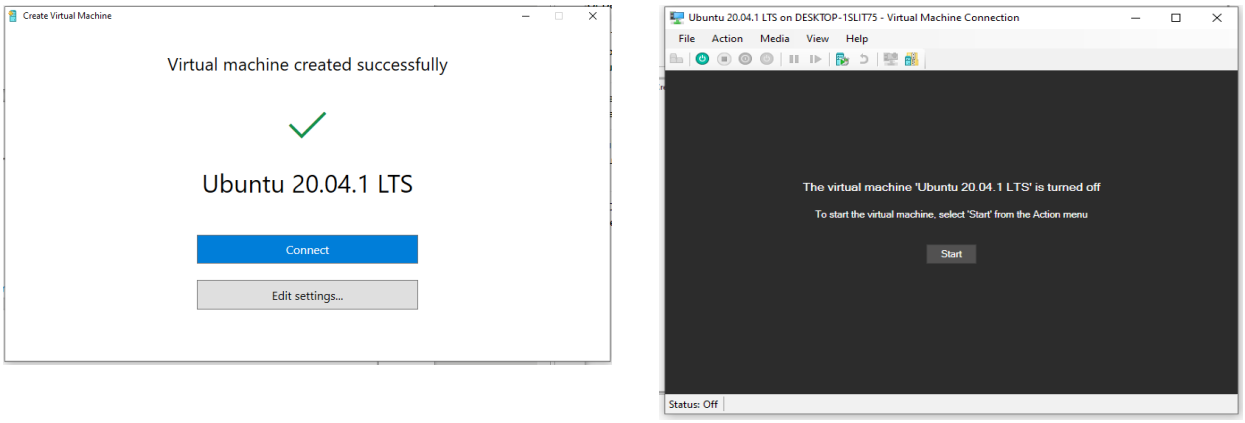


Рисунок 3.3 – Підтвердження установки віртуальної машини Ubuntu 20.04.1B: вікно Connect (а); вікно запуску Hyper-V та старту віртуальної машини (б)

– обираємо Ubuntu, очікуємо запуск інсталятора системи (рисунок 3.4);

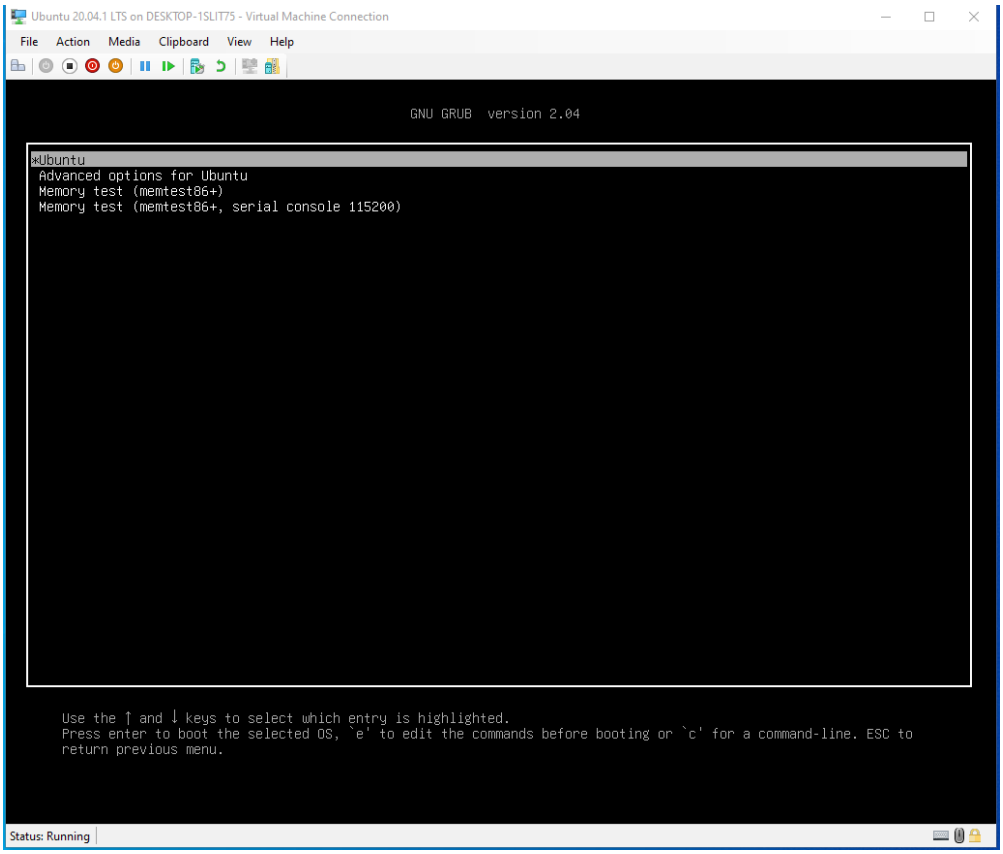
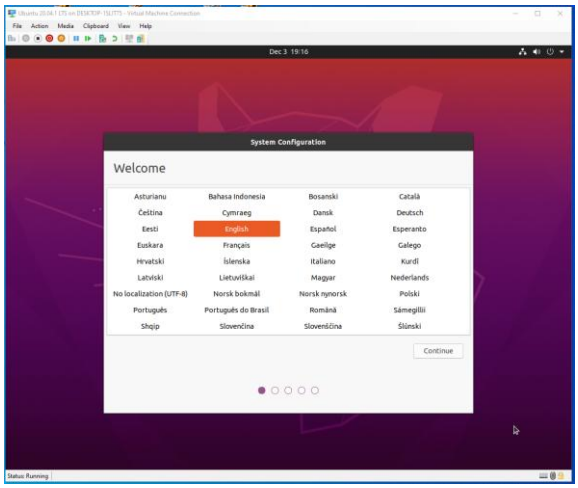
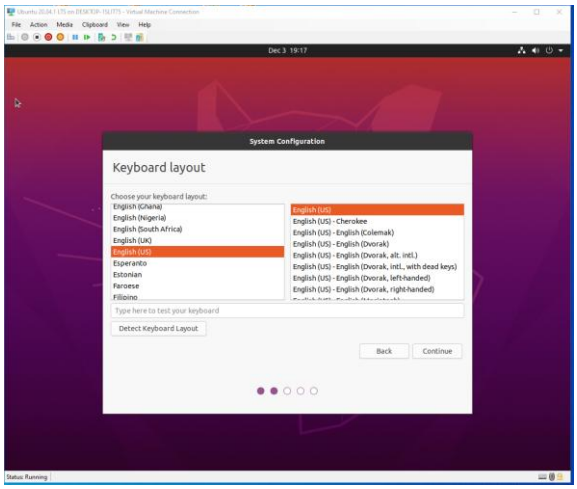


Рисунок 3.4 – Запуск інсталятора системи Ubuntu 20.04.1B

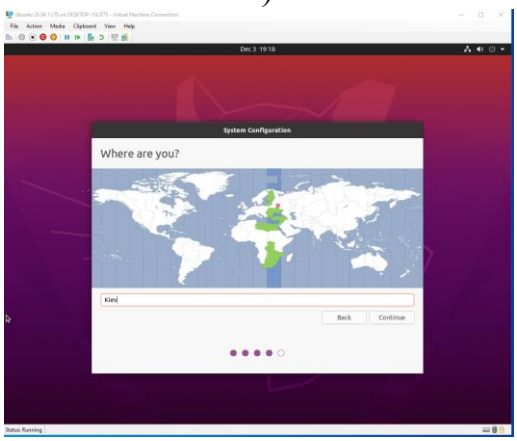
– обираємо мову, клавіатуру, часовий пояс, адміністратора (рисунок 3.5);



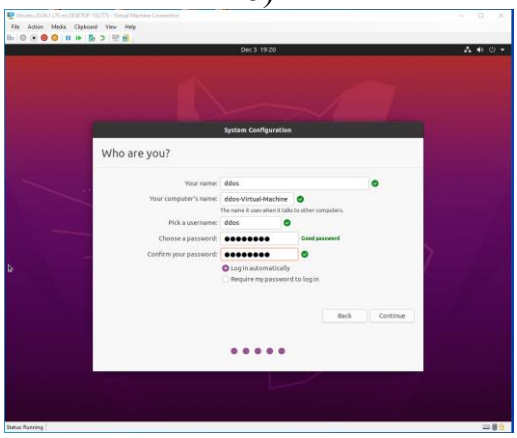
а)



б)



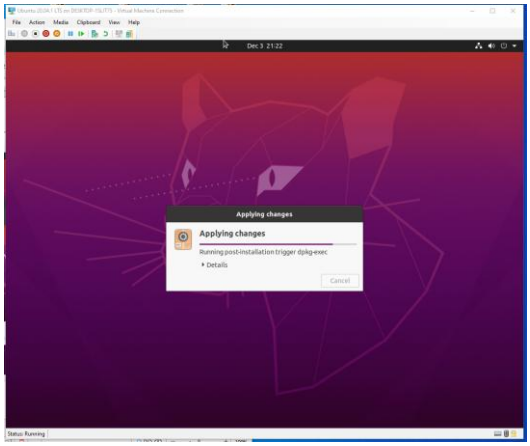
в)



г)

Рисунок 3.5 – Налаштування інтерфейсу системи: вікна вибору мови (а), клавіатури (б), часового поясу (в), адміністратора (г)

– вікна початкового налаштування робочого середовища наведені на рисунку 3.6;



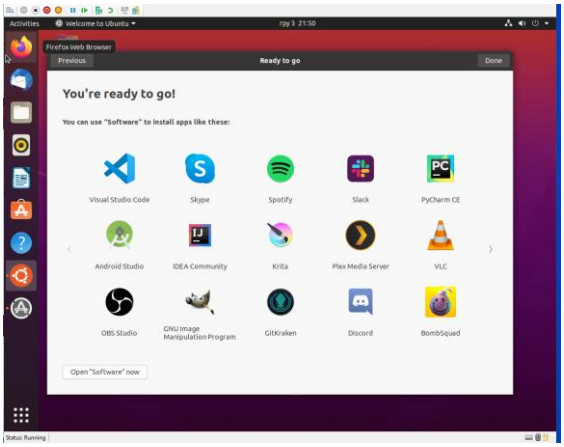
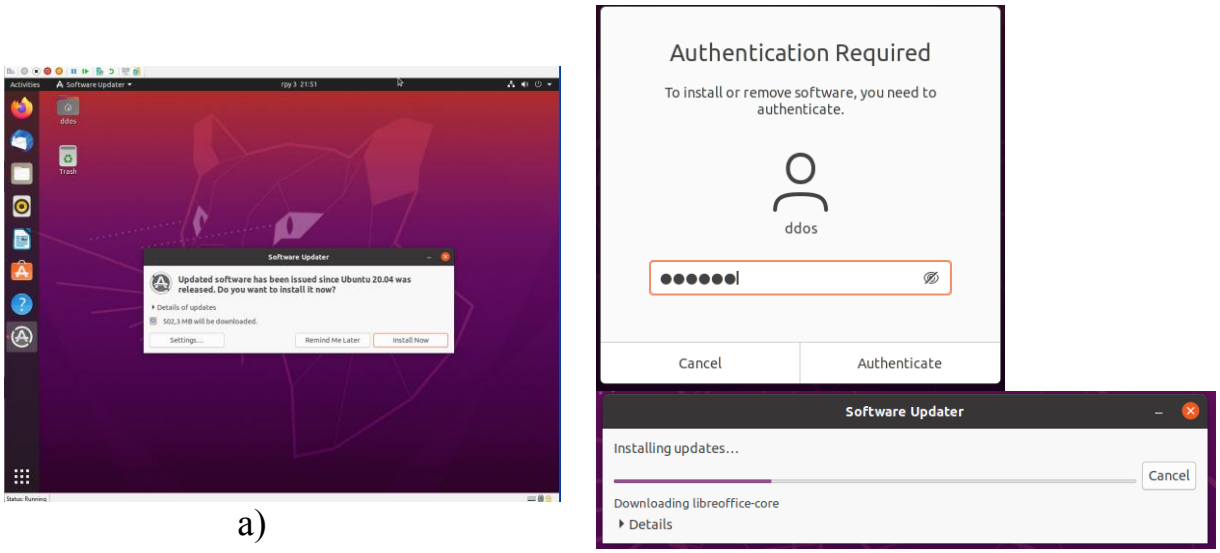


Рисунок 3.6 – Налаштування робочого середовища ОС

– вікна інсталяції оновлень та автентифікації користувача наведені на рисунку 3.7;



а) б)

Рисунок 3.7 – Вікна інсталяції оновлень (а) та автентифікації користувача (б)

– після перезавантаження операційної системи, вибору системи Ubuntu для завантаження віртуальна машина буде готова до роботи (рисунок 3.8);

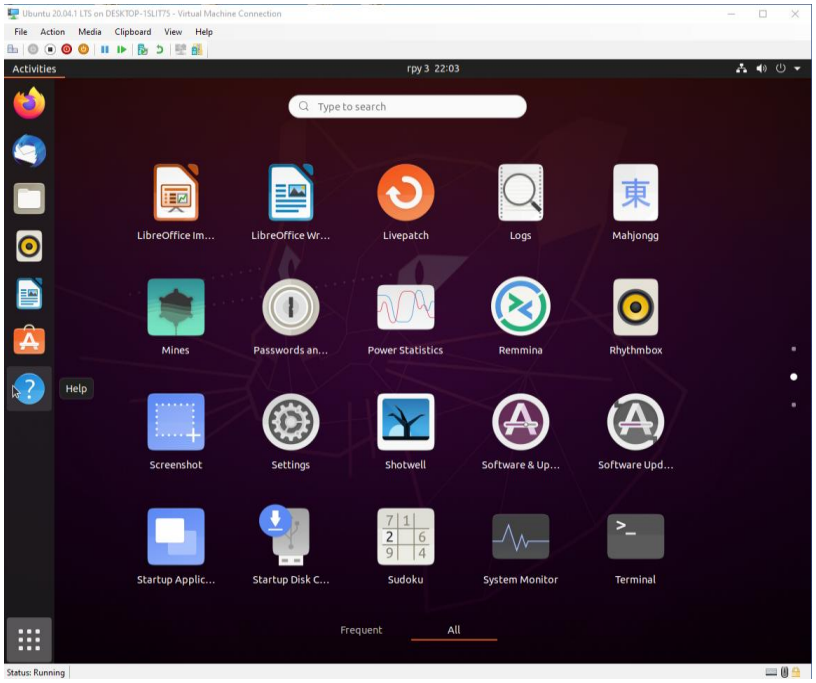


Рисунок 3.8 – Головний інтерфейс ОС Ubuntu 20.04.1В

3.3 Ідентифікаційна модель атаки

Для побудови моделі потрібно зробити наступні три кроки: Крок 1. Для проведення симуляції атаки атакуєма і атакуюча машини повинні знаходитись в одній мережі (обмеження Hyper-V). Для цього зайдемо в налаштування віртуальної машини лінукс і переведемо її в WSL мережу.

Для атак будемо використовувати Windows Subsystem for Linux Installation Guide for Windows 10 для чого в менеджере віртуальних машин потрібно включити WSL (рисунок 3.9).

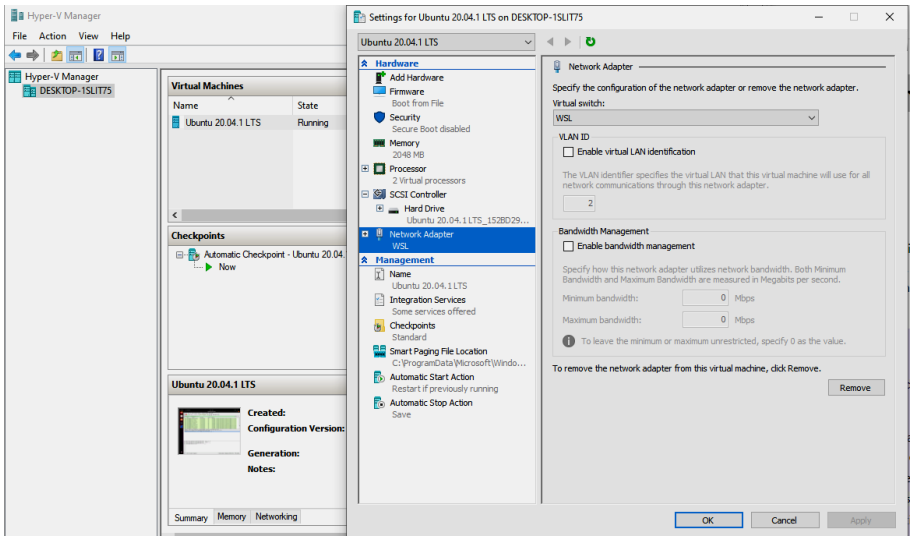


Рисунок 3.9 – Менеджер віртуальних машин WSL

Крок 2. Встановити інструментарій hping3 в дистрибутив Linux (машини зловмисника) за допомогою команди:

«# sudo apt-get install hping3»

Крок 3. Імітуємо атаку TCP SYN-flood. Атака здійснюється зловмисником на машину жертви, при цьому він запустив наступну команду:

hping3 –c1500 -d 120 –S –w 64 –p 80--flood--rand-sourse

За цією командою на машину жертви надсилається 1500 пакетів розміром 120 байт з SYN Flag та розміром вікна TCP пакету – 64 байти. Атаки здійснюються на порт 80 HTTP веб- серверу. Параметр rand-source – означає,

що зловмисник надсилає пакети з максимально можливою швидкістю з підмінениими IP – адресами (рисунок 3.10).

Для ідентифікації атаки необхідно на машину жертви встановити спеціальне програмне забезпечення Wireshark та за допомогою нього здійснити захват трафіку TCP пакетів, що надсилає джерело зловмисника [20].

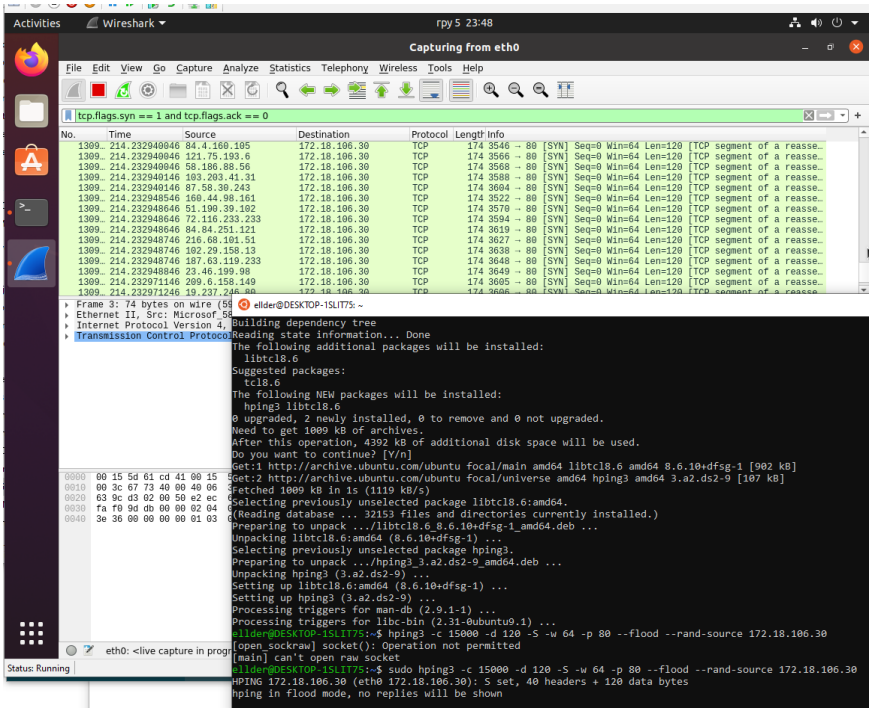


Рисунок 3.9 – Результат виконання команди hping на машину жертви з IP - адресою 172.18.106.30

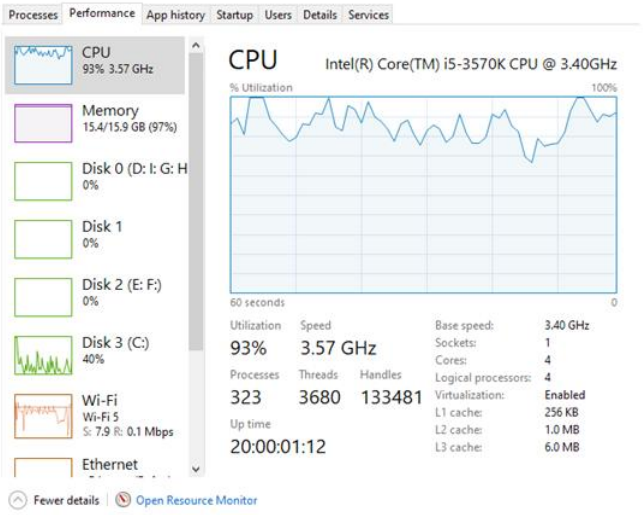


Рисунок 3.10 – Результат перенавантаження процесора (CPU) на 93% на хості жертви при атаці TCP SYN-flood

На рисунку 3.11 наведений результат розподілу пакетів TCP у часі під час надсилання запитів SYN-flood в інтервалі 35-50 секунд (за секунду відправляється майже 90000 пакетів).

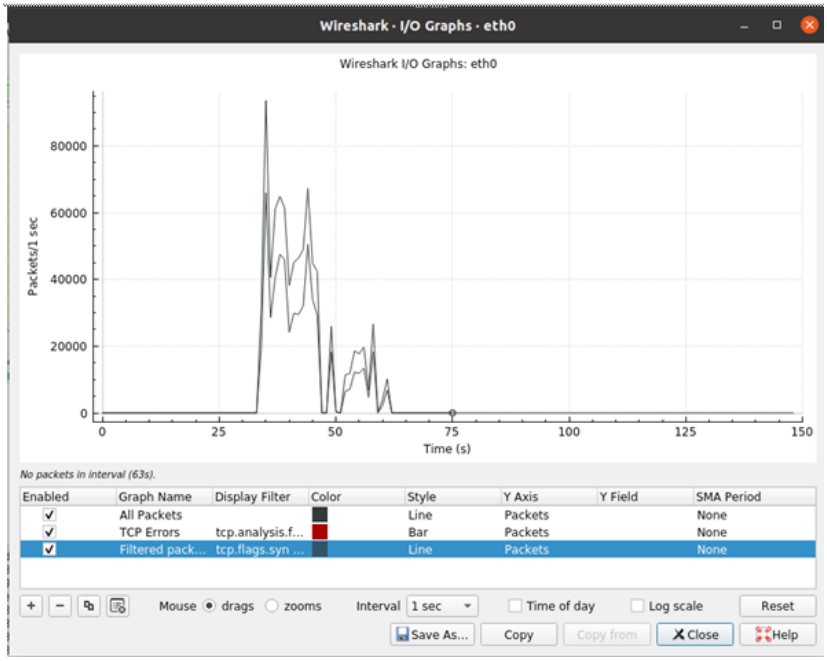
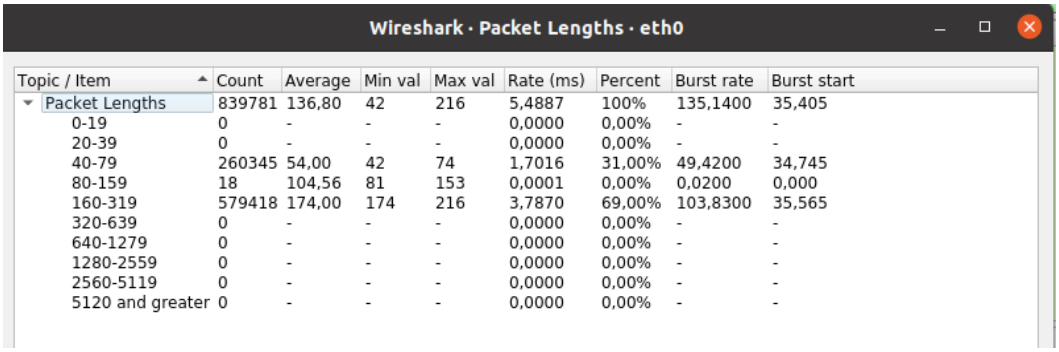


Рисунок 3.11 – Розподіл атаки пакетів TCP за секунду під час атаки

З отриманих статистичних даних за допомогою Wireshark видно, що найбільша кількість IP пакетів (579418 штук), що надсилається зловмисником є розміром від 160 до 319 байт (рисунок 3.12).



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	839781	136,80	42	216	5,4887	100%	135,1400	35,405
0-19	0	-	-	-	0,0000	0,00%	-	-
20-39	0	-	-	-	0,0000	0,00%	-	-
40-79	260345	54,00	42	74	1,7016	31,00%	49,4200	34,745
80-159	18	104,56	81	153	0,0001	0,00%	0,0200	0,000
160-319	579418	174,00	174	216	3,7870	69,00%	103,8300	35,565
320-639	0	-	-	-	0,0000	0,00%	-	-
640-1279	0	-	-	-	0,0000	0,00%	-	-
1280-2559	0	-	-	-	0,0000	0,00%	-	-
2560-5119	0	-	-	-	0,0000	0,00%	-	-
5120 and greater	0	-	-	-	0,0000	0,00%	-	-

Рисунок 3.12 – Вікно даних про розміри IP пакетів

На рисунку 3.13 наведений результат підміни IP- адрес зловмисником, з якого видно, що кожний запит на підключення надходить з різних IP -адрес по

1-2 пакети. Тому що використовувалась підміна джерел (source IP), то не можливо визначити атакуючий хост.

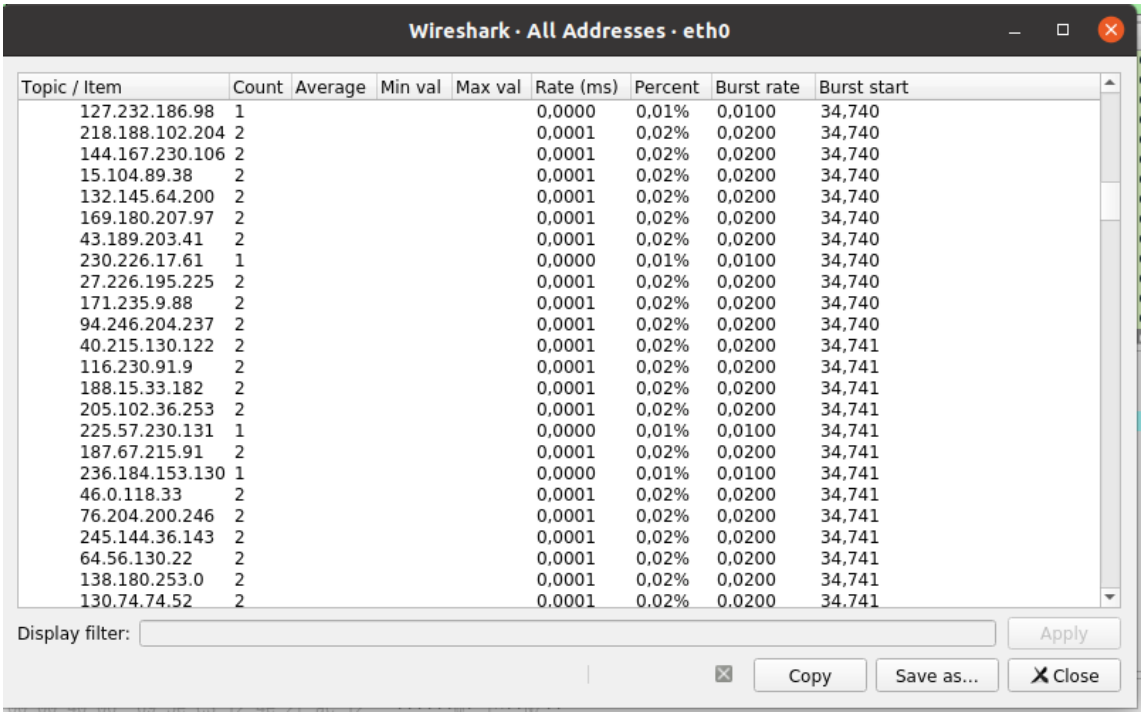
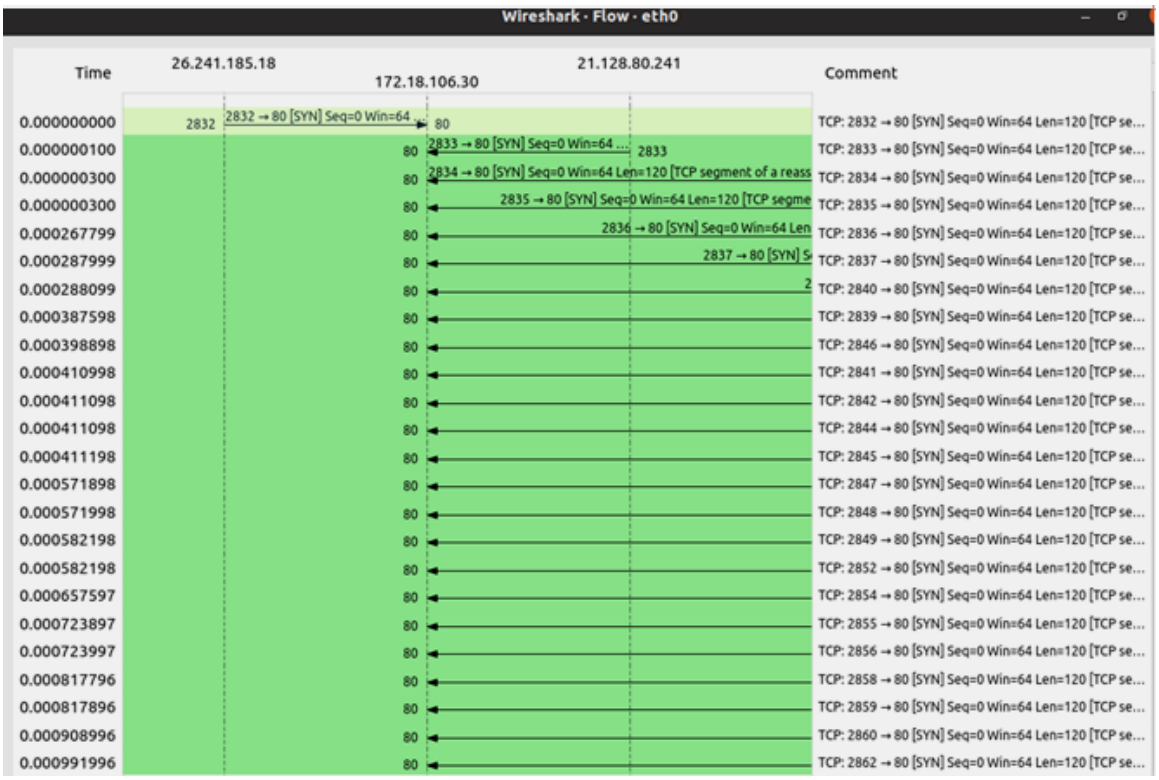


Рисунок 3.13 – Результат підміни IP- адрес зловмисником

Проведемо сканування на визначення хостів в мережі на основі ARP (англ. Address Resolution Protocol – протокол визначення адрес) [21]. Для цього, використаємо nmap і мережі жертви з пулу адрес 172.18.106.16/28 – це утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки (рисунок 3.14). Nmap використовує "сирі" IP пакети для визначення хостів доступних в мережі, які служби (назва програми та версію) вони пропонують, які ОС вони використовують, які типи пакетних фільтрів / брандмауерів використовуються та ще багато інших характеристик [22].

```
nmap -n -sn --send-ip 172.18.106.16/28
```

У результаті сканування проведеного сканування на визначення хостів в мережі на основі ARP можна визначити адресу зловмисника з IP - адресою: 172.18.106.18 (рисунок 3.14).



а)

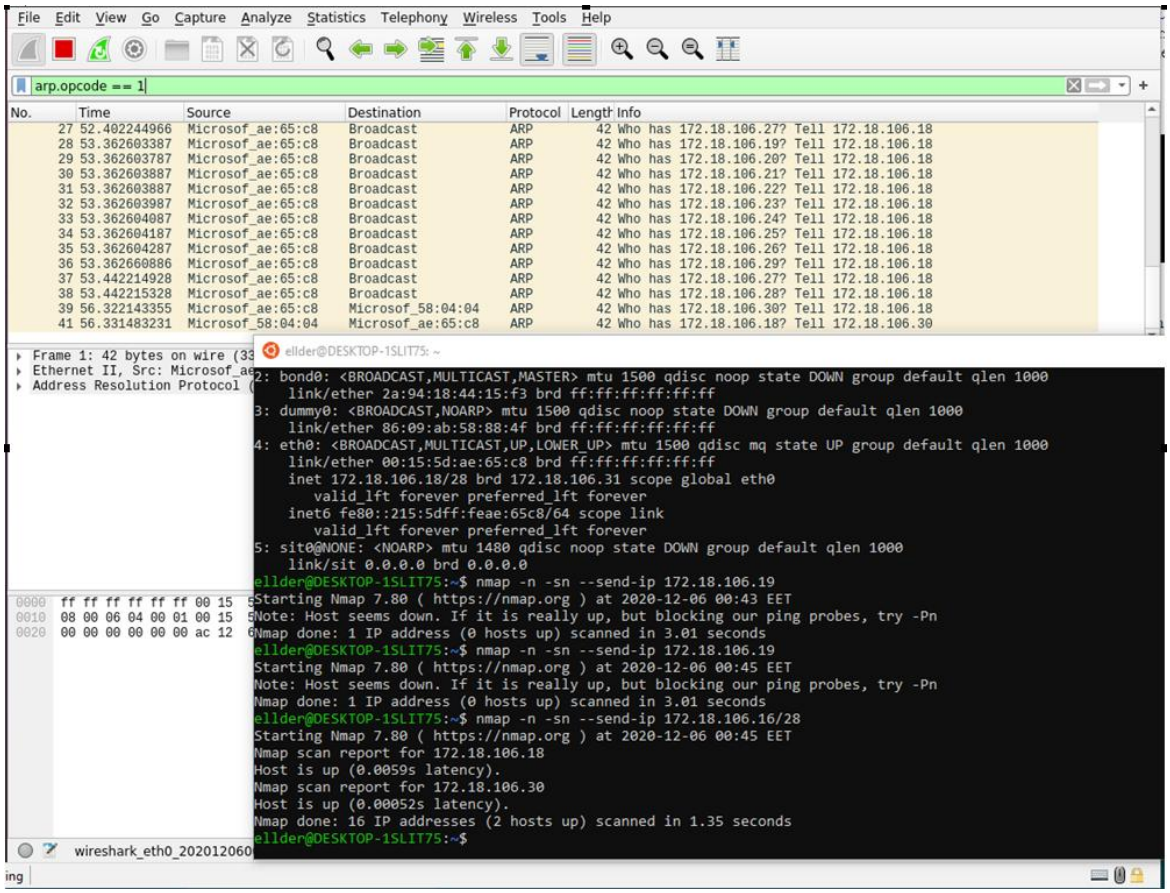


Рисунок 3.14 – Результат сканування: SYN запиту на порт 80 жертви (а); визначення IP- адреси атакуючого 172.18.106.18 (б)

На рисунку 3.15 наведений результат ідентифікації атаки TCP SYN-flood, де червоним виділено надходження великої кількості TCP пакетів, що надсилаються з різних IP-адрес. При використанні фільтру «tcp.flags.syn == 1 and tcp.flags.ack == 1», можна побачити, що кількість пакетів з встановленим флагом SYN та з флагом ACK тільки 3 штуки (для прикладу на рисунку 3.15) Отже, це головний признак атаки TCP SYN flood на машину з IP- адресою 172.18.106.18.

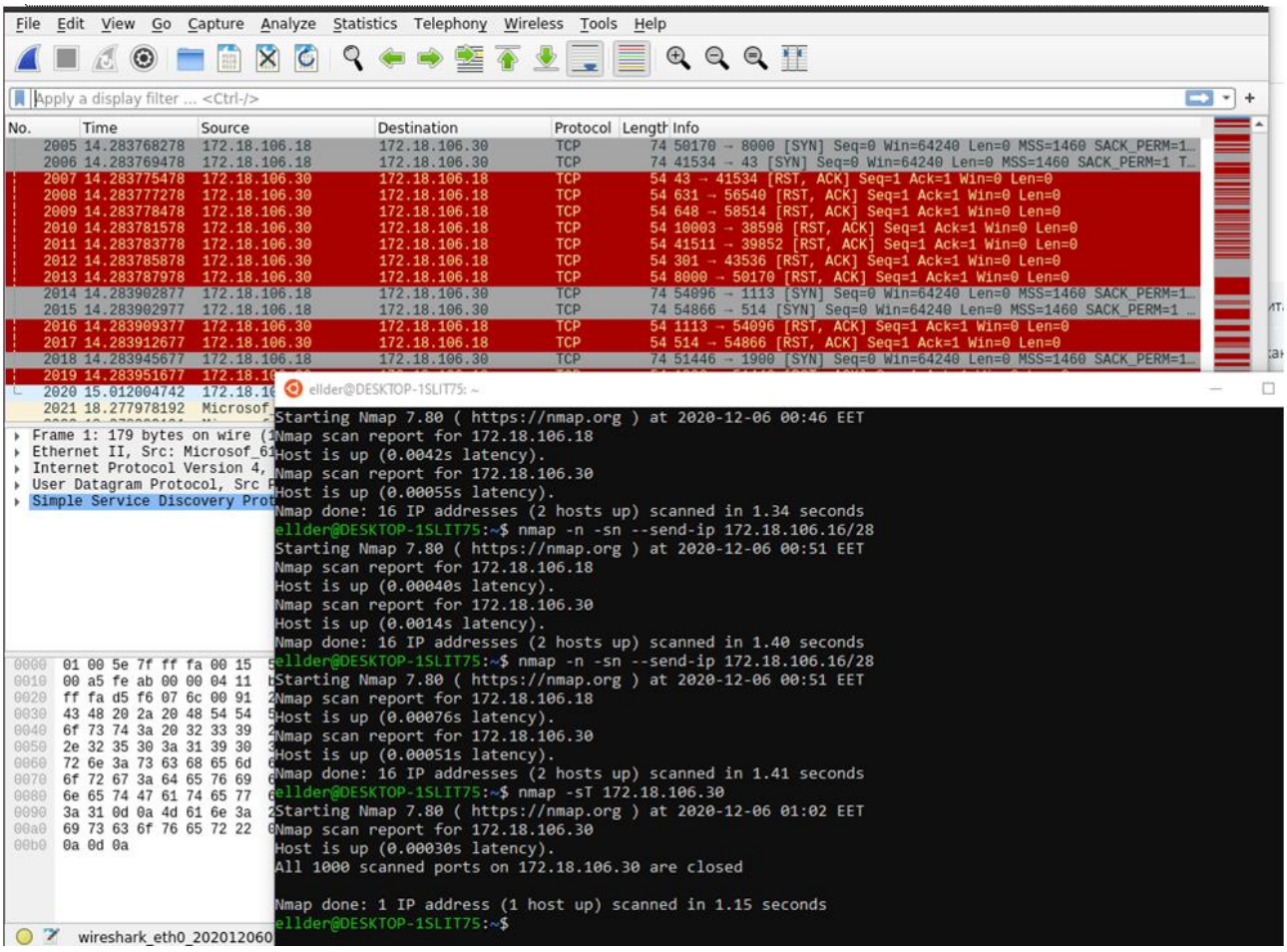


Рисунок 3.15 – Ідентифікація атаки TCP SYN Flood за допомогою Wireshark

Отже (рисунок 3.15), ми отримали ситуацію наведену на рисунку 2.5, де зловмисник відправив на порт 80 хосту – цілі атаки швидкий потік SYN-пакетів, при цьому, не отримав відповіді на надісланий пакет SYN/ACK. З рисунку 3.9 також видно, що пакети надсилаються кожен раз з різних IP- адрес. На хості цілі атаки – жертви з IP - адресою 172.18.106.30 черга запитів на

підключення переповнилась. З рисунку 3.10 видно, що кількість вхідних з'єднань досягла максимального рівня, що призвело до ситуації, коли всі наступні запити відхилені ОС хосту з IP - адресою 172.18.106.30 і він не може встановити TCP- з'єднання за рахунок втрати продуктивності, тобто відбувся процес: «відмова в обслуговуванні».

Ідентифікація UDP Flood атаки також можна ідентифікувати використовуючи команду hping3:

hping3 –p 80 –i u1000 --udp 172.10.106.30

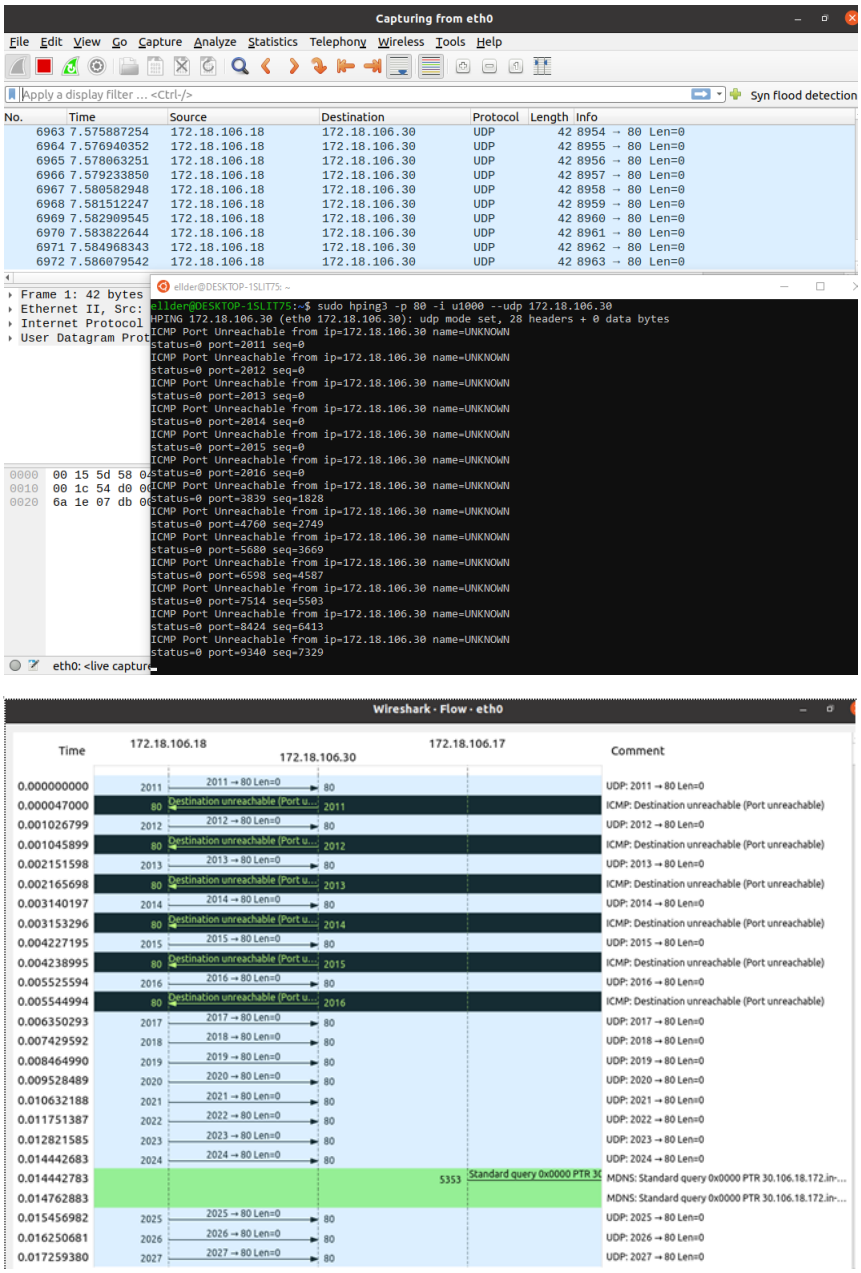


Рисунок 3.15 – Реалізація атаки UDP Flood за допомогою утілити hping3 на IP- адресу 172.10.106.30

Отже, на рисунку 3.15 можна побачити, що відправляється велика кількість UDP-пакетів (за рисунком 3.15: 8054-8963 шт.) великого обсягу порт 80 хосту з IP- адресу 172.10.106.30, який повинен відправити у відповідь ICMP-повідомлення «адресат недоступний». У підсумку машина жертви виявиться перевантаженою, а вся смуга пропускання буде зайнята шкідливим трафіком.

Аналогічним чином ідентифікуємо атаку ICMP Flood, скориставшись утілитою, де 172.18.106.30 – IP-адреса хосту жертви (рисунок 3.16):

hping3 -p 80 --flood --icmp 172.18.106.30

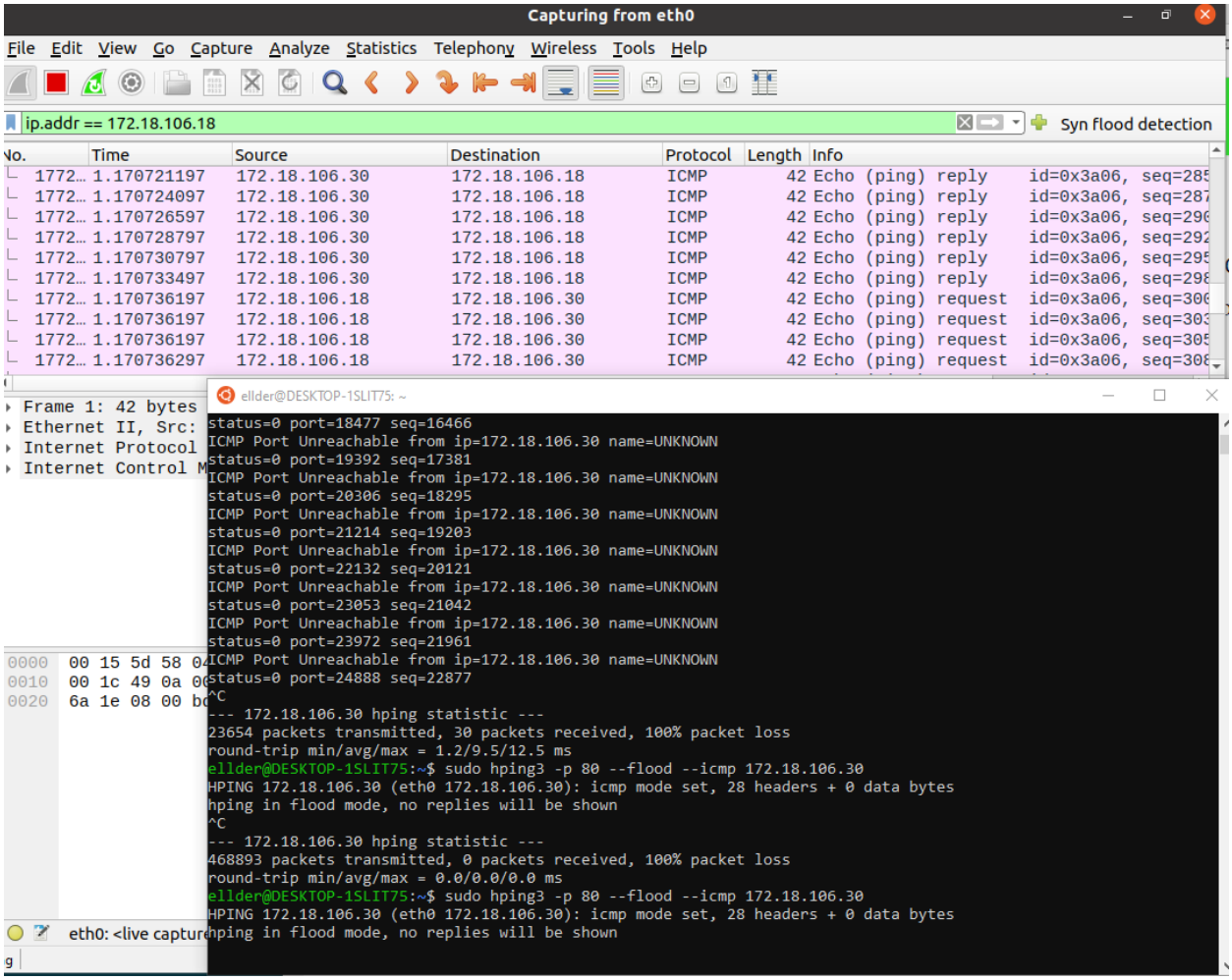


Рисунок 3.16 – Реалізація атаки ICMP Flood на за допомогою утілити hping3 на IP- адресу 172.10.106.30

Результат атаки ICMP Flood за допомогою утілити hping3 на хост з IP-адресою 172.10.106.30 наведений на рисунку 3.17.

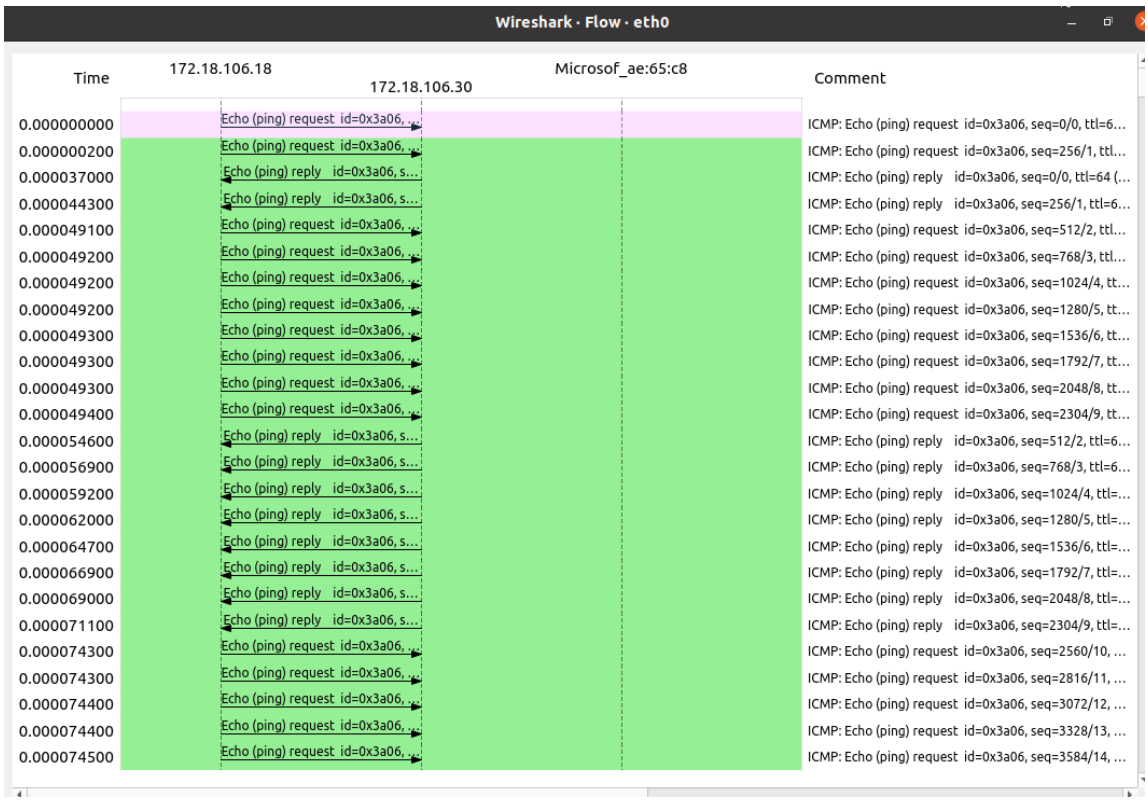


Рисунок 3.17 – Результат атаки ICMP Flood на за допомогою утілити hping3 на хост з IP- адресою 172.10.106.30

Отже, видно, що на хост жертви з IP- адресою 172.10.106.30 посилається сильно фрагментований ICMP-пакет, розмір якого перевищує допустимий (більше 64 Кбайт). При цьому, машина жертви отримує фрагменти і намагається відновити пакет, а сама ОС зависає і перестає реагувати на запити клавіатури та миші.

Висновки до третього розділу

1. Кожна система, яка підключена до Інтернету та обладнана мережевими службами на основі TCP являються потенційною жертвою атаки. DoS-атаки типу SYN- Flood використовують слабкі місця в стеці протоколу TCP/IP. Розподілена відмова в обслуговуванні DDoS призводить до відмови в обслуговуванні та недоступності мережевої послуги або навіть припинення роботи сервера або частини мережі та можуть бути повністю непридатні для клієнтів.

2. Класичні атаки DoS - це індивідуальні атаки, в яких потужний хост генерує трафік, який "переповнює" з'єднання цільового хосту, який заважає авторизованим клієнтам отримувати доступ до мережевих послуг.

Існує кілька способів виконання DoS-атак, таких як: TCP SYN Flood; UDP Flood; ICMP Flood атаки типу «відмова в обслуговуванні», які можна змоделювати за допомогою різних інструментів, таких як Ubuntu 20.04.1 LTS та підсистеми Windows для Linux версії WSL 2.

3. Для кращого розуміння процесів, які відбуваються при дії TCP SYN flood, UDP та ICMP flood атак побудована ідентифікаційна модель атак з використанням двох віртуальних машин з встановленим програмним забезпеченням Ubuntu 20.04.1 LTS та віртуальної машини підсистеми Windows для Linux версії WSL2.

4. Необхідно мати достатньо потужні обчислювальні ресурси, щоб відрізнити зловмисний трафік від легального та вимкнути його або пропускну здатність для обробки всіх запитів.

5. Атака flood складна, і важко відрізнити шкідливі пакети від легальних, використовуючи традиційні та відомі методи. Для цього професіоналам слід використовувати більш складні методи та часто дороге спеціалізоване обладнання.

ПРОГРАМНІ МЕТОДИ ЗАХИСТУ ВІД МЕРЕЖНИХ АТАК

4.1. Механізми захисту мережного обладнання

До програмних засобів захисту від віддалених атак можна віднести програми, основна мета яких є аналіз мережного трафіку на предмет наявності однієї з відомих активних віддалених дій і протидія виявленим діям.

Існує декілька механізмів захисту мережного обладнання (хостів), які можуть частково забезпечити захист від SYN Flood – атак [10-12]:

1. Настройка стеку. Для цього можна налаштувати стек TCP, зменшивши його час «напіввідкритої» сесії з’єднань, або, іншими словами, тайм-аут звільнення пам'яті, виділеної для з'єднання, а також час виділений на блокування вхідних з'єднань. Але у цих налаштувань можуть бути побічні ефекти у вигляді втрати частини легітимних з'єднань через затримки і нестабільні канали.

2. Реалізація механізму SYN-Cookie. Для створення TCP-з'єднання хост А відправляє хосту Б TCP-пакет з прапором SYN і своїм номером послідовності. Механізм SYN cookies зовсім не використовує чергу SYN. Хост Б відправляє пакет з прапором SYN-ACK, який містить унікальну інформацію, що ідентифікує клієнта Б: IP - адресу; номер порту; час відправки пакету та прийнятий унікальний номер послідовності хосту А. Хост «зловмисника» ніколи не отримує ці пакети і тому не надасть на них відповідь. На завершальній відповіді хостом А ця інформація (хеш) вже включена в пакет з прапором ACK. При успішній перевірці ACK – пакету відповіді на SYN cookie, хостом Б виділиться пам’ять для з’єднання, навіть, якщо в черзі SYN не має відповідного запису. Для використання механізму хешування (порівняння даних) необхідно, щоб усі хости, які приймають участь в передачі трафіку його підтримували. Якщо SYN cookie включені, то «зловмисник» не зможе обійти такі міжмережеві екрани відправкою ACK-пакета з довільним номером послідовності поки не підбере вірний. SYN cookies потрібно включати тільки

для публічно доступних портів. Включення механізму SYN cookies – це простий спосіб боротьби проти атаки SYN Flood. Однак при його використанні буде більше завантаженість процесора клієнта під час створення та звірки cookies.

3. Обмеження запитів на нові підключення від конкретного джерела за визначений проміжок часу.

Використання мережного протоколу транспортного рівня SCTP (англ. Stream Control Transmission Protocol - протокол передачі з керуванням потоком). Даний протокол використовує механізм SYN cookie та не підданий SYN- Flood атакам. Передача трафіку за протоколом SCTP здійснюється багатьма потоками, а синхронне з'єднання між двома хостами по двох та більше незалежних фізичних каналах (multi-homing) [10-12].

4.2 Фільтрація трафіку сервера Linux за допомогою утілити iptables

Брандмауер Iptables - це брандмауер, орієнтований на Linux, який використовується в даній роботі.

Програма командного рядка простору користувача iptables використовується для налаштування набору правил фільтрації пакетів Linux 2.4.x та більш пізніших версій. Вона орієнтована на системних адміністраторів. Це утиліта управління брандмауером за замовчуванням у системах Linux. Утілита iptables може бути використана для фільтрації певних пакетів, блокування вихідних або цільових портів та IP-адрес, пересилання пакетів через NAT та багатьох інших речей. Але найчастіше вона використовується для блокування портів призначення та вихідних IP-адрес.

Пакети iptables можуть бути завантажені зі сторінки Netfilter [23]. Проект netfilter - це спільний проект FOSS, керований спільнотою, яка надає програмне забезпечення для фільтрації пакетів для Linux 2.4.x та пізніших серій ядра. Проект netfilter зазвичай асоціюється з iptables та дозволяє фільтрувати пакети,

перетворювати мережеві адреси, реєструвати пакети, чергувати пакети в просторі користувачів та виконувати інші маніпуляції з пакетами.

Загальне програмне забезпечення брандмауера iptables дозволяє визначати набори правил. Кожне правило в IP таблиці складається з ряду класифікаторів (збіги iptables) та однієї підключеної дії (ціль iptables) [24,25].

Крім того, для роботи iptables, відповідним чином повинно бути налаштоване ядро Linux-системи користувача.

При встановленні захисту на хості клієнта пакети надходять з зовнішньої мережі, потрапляють на брандмауер і, спочатку, на мережний адаптер ПК, далі захоплюються його драйвером та потрапляють в ядро ОС і проходять через певну кількість таблиць локального додатку або перенапрямляються транзитом на інші хости мережі за алгоритмом проходження пакетів (рисунок 4.1).

При цьому, існують різні таблиці для різних цілей [24,25]:

– таблиці iptables фільтр: таблиця фільтрів є таблицею за замовчуванням, містить набори правил і найчастіше використовується, якщо не використовується опція -t (–table);

– NAT: використовується для перетворення мережевих адрес (NAT). Якщо пакет створює нове з'єднання, таблиця nat перевіряється на наявність правил;

– Mangle: використовується для зміни або виставлення мітки пакетів і їх інформації заголовка;

– Raw: мета цієї таблиці, головним чином, полягає у виключенні певних пакетів із відстеження з'єднань за допомогою цілі NOTRACK.

Отже, у середній системі Linux є чотири різні таблиці, які не мають завантажених нестандартних модулів ядра. Кожна з цих таблиць підтримує різний набір ланцюжків iptables:

1. IPtables – PREROUTING: raw, nat, mangle. Застосовується до пакетів, що надходять на мережеву карту інтерфейсу (NIC).

2. INPUT: filter, mangle. Застосовується до пакетів, призначених для локального сокету.

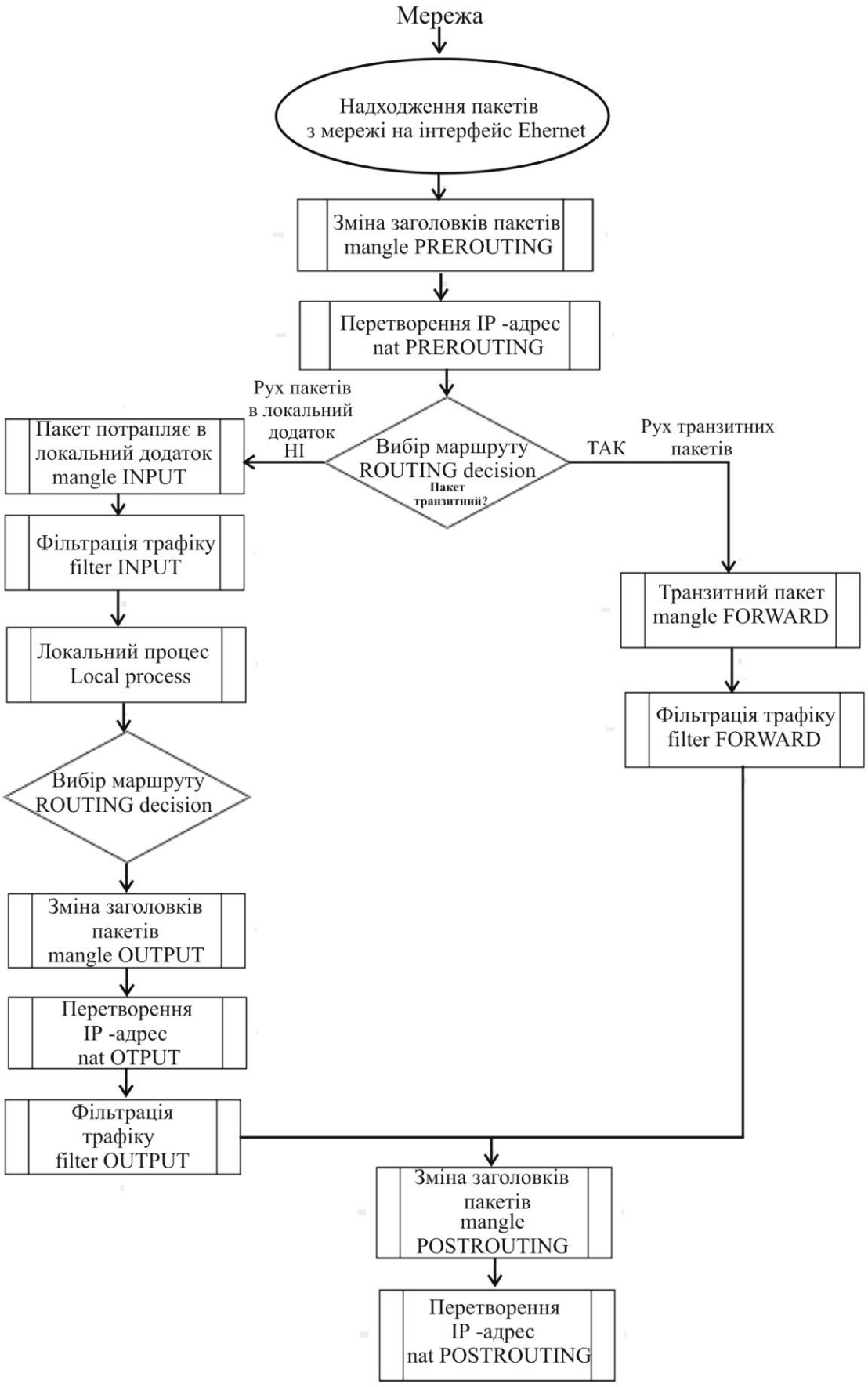


Рисунок 4.1– Алгоритм проходження пакетів через брандмауер

3. FORWARD: filter, mangle. Застосовується до пакетів, які направляються через сервер.

4. OUTPUT: raw, filter, nat, mangle. Застосовується до пакетів, які надсилає сервер (локально генеровані).

5. POSTROUTING: nat, mangle. Застосовується до пакетів, які залишають сервер.

4.3 Захист серверу Linux від DDoS-атак

Більшість типів DDoS-атак на основі TCP використовують високу швидкість передачі пакетів, тобто велика кількість пакетів в секунду є причиною того, що сервер падає.

Деякі атаки SYN легко фільтрувати, оскільки вони мають однакові "незвичні" параметри в заголовку TCP.

Залежно від того, який тип пакетів необхідно заблокувати або змінити, обирається певна таблиця iptables та ланцюжок, яку підтримує вибрана таблиця.

Більшість інструкцій щодо блокування DDoS-атак за допомогою iptables, використовують таблицю фільтрів та ланцюжок INPUT для правил захисту від DDoS. Проблема цього підходу полягає в тому, що ланцюжок INPUT обробляється лише після ланцюжків PREROUTING і FORWARD, і тому застосовується лише в тому випадку, якщо пакет не відповідає жодному з цих двох ланцюжків. Це спричиняє затримку у фільтрації пакету, який споживає ресурси [24,25].

Перший ланцюжок, який може застосовуватися до пакета – PREROUTING і, в ідеалі їм можна відфільтрувати погані пакети в ланцюжку.

Однак таблиця фільтрів не підтримує ланцюжок PREROUTING. Щоб обійти цю проблему, використовують таблицю mangle замість таблиці фільтрів для правил iptables захисту від DDoS. Вона підтримує більшість, якщо не всі правила, які підтримує таблиця фільтрів, а також підтримує всі ланцюжки iptables.

Не рекомендується використовувати таблицю фільтрів та ланцюжок INPUT, щоб блокувати неправильні пакети. Недоліком такого блокування є те, що його не слід використовувати постійно із-за можливості блокування законного трафіку, що надходить із зовнішніх мереж.

Найкращим рішенням для різкого підвищення ефективності клієнтських правил iptables, а отже, кількості трафіку TCP DDoS-атак, який вони можуть відфільтрувати, є використання таблиці mangle та ланцюжка PREROUTING.

Існує 5 простих правил iptables, які можуть захистити від багатьох DDoS-атак на основі TCP [24.25]:

1) блокування недійсних пакетів з використанням таблиць mangle:

```
iptables -t mangle -A PREROUTING -m conntrack --ctstate INVALID -j DROP
```

2) блокування пакетів, які не належать встановленому з'єднанню і не використовують прапор SYN.

```
iptables -t mangle -A PREROUTING -p tcp ! --syn -m conntrack --ctstate NEW -j DROP
```

3) нормальні значення параметрів MSS пакету знаходяться між 536 і 65535 і їх встановлює клієнт. Лише SYN-пакети можуть бути новими пакетами згідно за двома попередніми правилами, які використовують значення TCP MSS, яке не є загальним. Це допомагає блокувати ними потоки SYN. Скористаємось цим:

```
# iptables -t mangle -I PREROUTING -p tcp -m tcp --dport 80 -m state --state NEW -m
tcpmss ! --mss 536:65535 -j DROP
```

4) відкидання пакетів, які використовують підроблені прапори TCP:

```
iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL NONE -j DROP iptables -t
mangle -A PREROUTING -p tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags SYN,RST SYN,RST -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,RST FIN,RST -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,ACK FIN -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags ACK,URG URG -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags ACK,PSH PSH -j DROP
```

5) правила захисту від спуфінгу пакетів, які надіслані з IP-адрес, які використовуються під приватні підмережі:

```
iptables -t mangle -A PREROUTING -s 224.0.0.0/3 -j DROP
iptables -t mangle -A PREROUTING -s 169.254.0.0/16 -j DROP
iptables -t mangle -A PREROUTING -s 172.16.0.0/12 -j DROP
iptables -t mangle -A PREROUTING -s 192.0.2.0/24 -j DROP
iptables -t mangle -A PREROUTING -s 192.168.0.0/16 -j DROP
iptables -t mangle -A PREROUTING -s 10.0.0.0/8 -j DROP
iptables -t mangle -A PREROUTING -s 0.0.0.0/8 -j DROP
iptables -t mangle -A PREROUTING -s 240.0.0.0/5 -j DROP
iptables -t mangle -A PREROUTING -s 127.0.0.0/8 ! -i lo -j D
```

Також можна використати додаткові команди захисту від атак на TCP SYN:

1) скоротити час очікування SYN (див. п 4.1):

```
iptables -A FORWARD -p tcp –syn -m limit –limit 1/s -j ACCEPT
iptables -A INPUT -i eth0 -m limit –limit 1/sec –limit-burst 5 -j ACCEPT
```

2) скоротити час очікування до 5-ти пакетів SYN за секунду:

```
iptables -N syn-flood
iptables -A INPUT -p tcp –syn -j syn-flood
iptables -A syn-flood -p tcp –syn -m limit –limit 1/s –limit-burst 5 -j RETURN
iptables -A syn-flood -j REJECT
```

3) використати SYN-Cookie:

```
sysctl -w net.ipv4.tcp_syncookies=1
sysctl -w net.ipv4.tcp_max_syn_backlog=3072
sysctl -w net.ipv4.tcp_synack_retries=0
sysctl -w net.ipv4.tcp_syn_retries=0
sysctl -w net.ipv4.conf.all.send_redirects=0
sysctl -w net.ipv4.conf.all.accept_redirects=0
sysctl -w net.ipv4.conf.all.forwarding=0
sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
```

4) запобігти команді *ping*

```
sysctl -w net.ipv4.icmp_echo_ignore_all=1
```

5) блокувати певні діапазони IP - адрес:

```
ptables -A INPUT -s 192.168.1.1/8 -i eth0 -j Drop
```

6) блокування усього вхідного трафіку, за винятком трафіку, який дійсно потрібен на сервері клієнта. Дозволити управління лише з надійних джерел. Ці правила обмежують частоту запитів SYN від одного IP до 20 на хвилину.

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

7) найпростіший випадок - атака одного хоста без підробки IP. Це легко усунути обробкою та блокуванням якомога більшої кількості пакетів на секунду.

```
# iptables -A INPUT -p tcp -m state --state NEW -m recent --set -j ACCEPT
```

4.3.1 Перевірка захисту хосту від атак TCP SYN Flood

Використаємо захист брандмауера, використовуючи правила iptable для першого типу атаки TCP SYN Flood [24.25]:

1. На початку, видалимо усі правила (код наведений нижче) (рисунок 4.2).

```
# Видаляємо усі правила
iptables -t raw -F
iptables -F
sysctl -w net/ipv4/tcp_syncookies=1
sysctl -w net/ipv4/tcp_timestamps=1
# Завантажуємо необхідний модуль для ядра Linux
modprobe nf_conntrack
sysctl -w net/netfilter/nf_conntrack_tcp_loose=0
echo 2500000 > /sys/module/nf_conntrack/parameters/hashsize
sysctl -w net/netfilter/nf_conntrack_max=2000000
iptables -t raw -I PREROUTING -p tcp -m tcp --syn -j CT --notrack
```

iptables -I INPUT -p tcp -m tcp -m conntrack --ctstate INVALID,UNTRACKED -j SYNPROXY --sack-perm --timestamp --wscale 7 --mss 1460

iptables -A INPUT -m conntrack --ctstate INVALID -j DROP

2. Далі перевіряємо поточний стан правил та лічильників iptables. Усі лічильники виставлені в нуль в поточному стані таблиці. Використаний фільтр ще нічого не спіймав (рисунок 4.3):

iptables -nvx -t raw -L
iptables -nvx -L

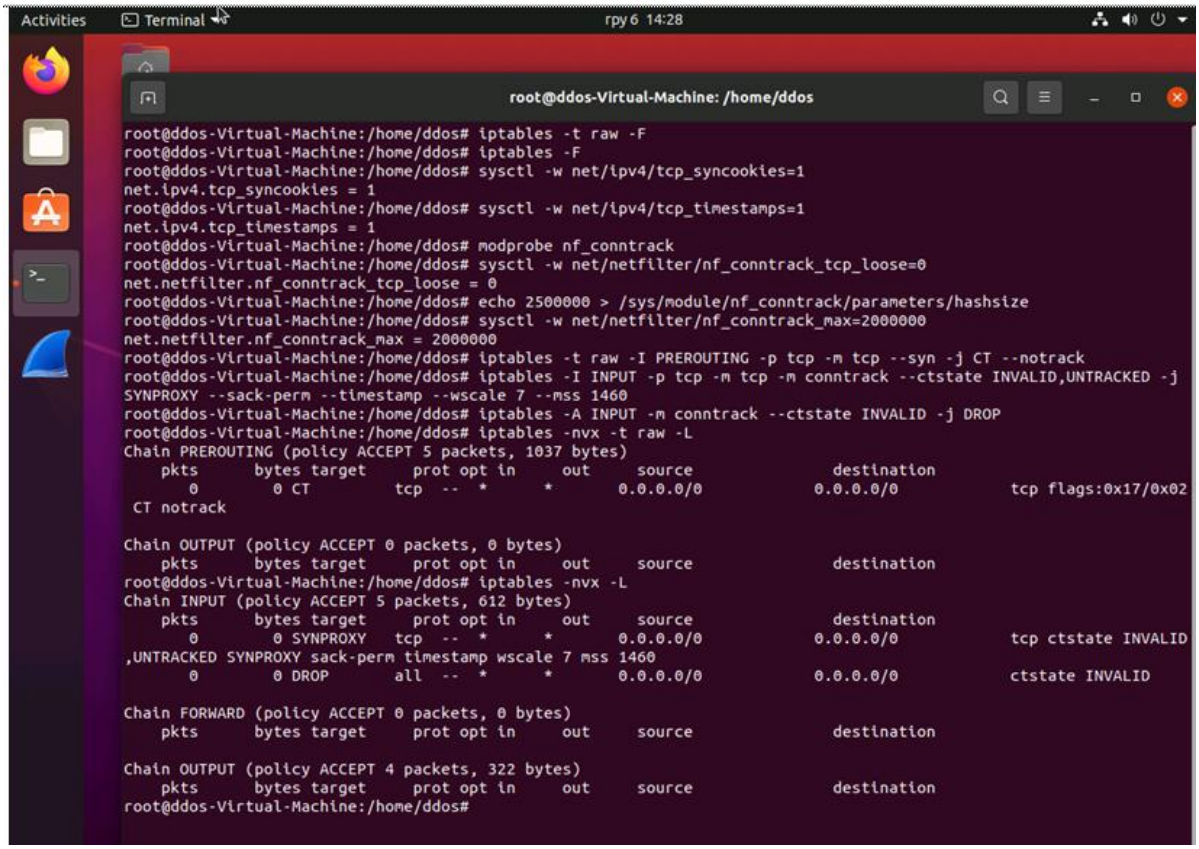
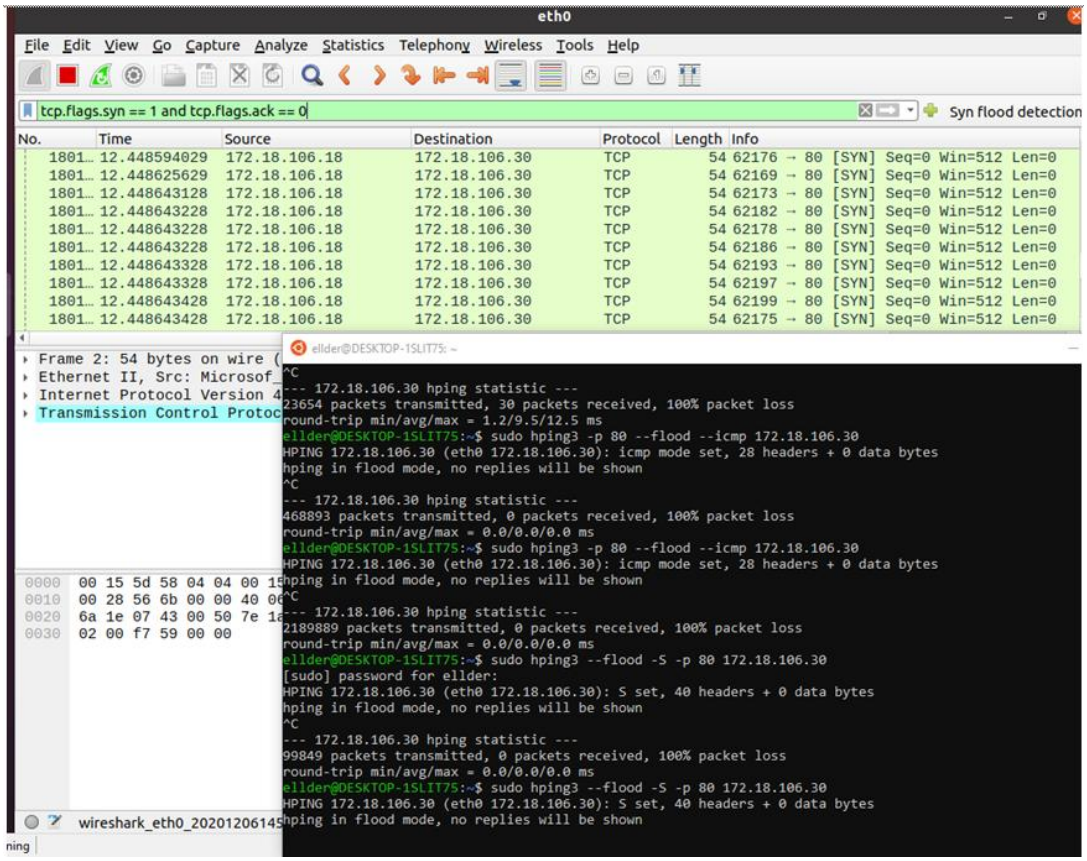


Рисунок 4.2 – Поточний стан правил та лічильників iptables (лічильники виставлені в нуль)

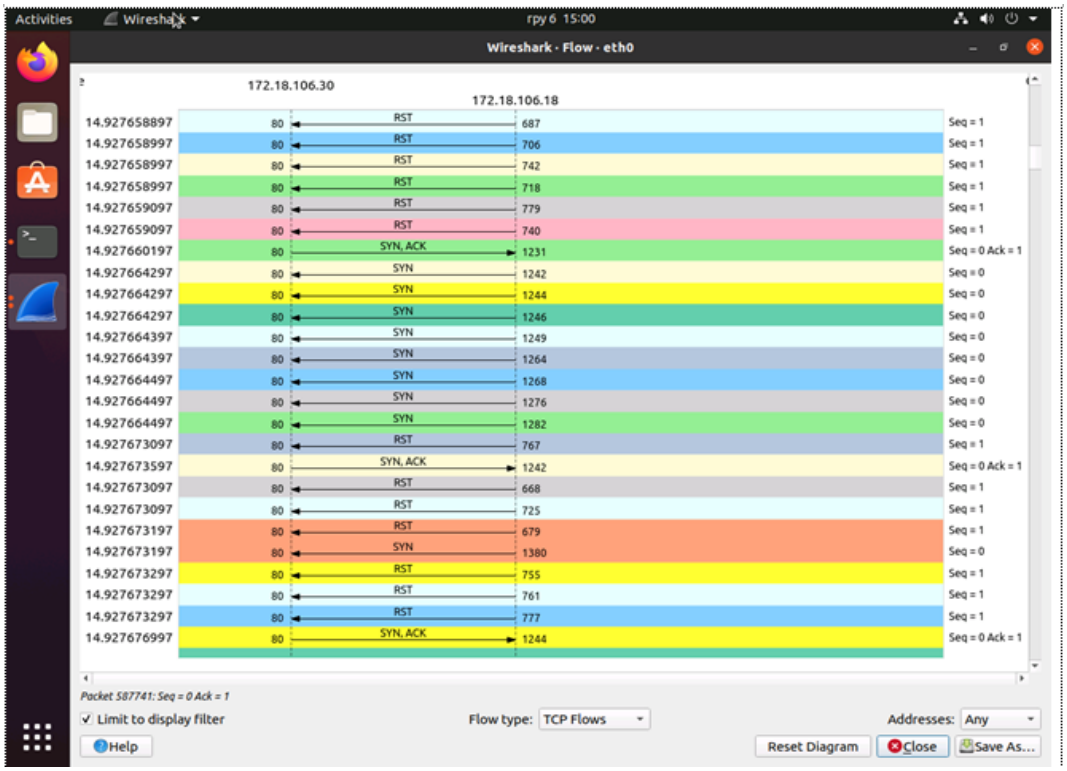
Як і раніше (див.3 розділ), запускаємо атаку, використовуючи команду hping3 (рисунок 4.3):

hping3 --flood –S –p 80 172.18.106.30

hping3 --flood –S –p 80



а)



б)

Рисунок 4.3 – Результат виконання команди hping3 на машину жертви з IP - адресою 172.18.106.30 (а) а графік TCP потоку SYN Flood Attack (б)

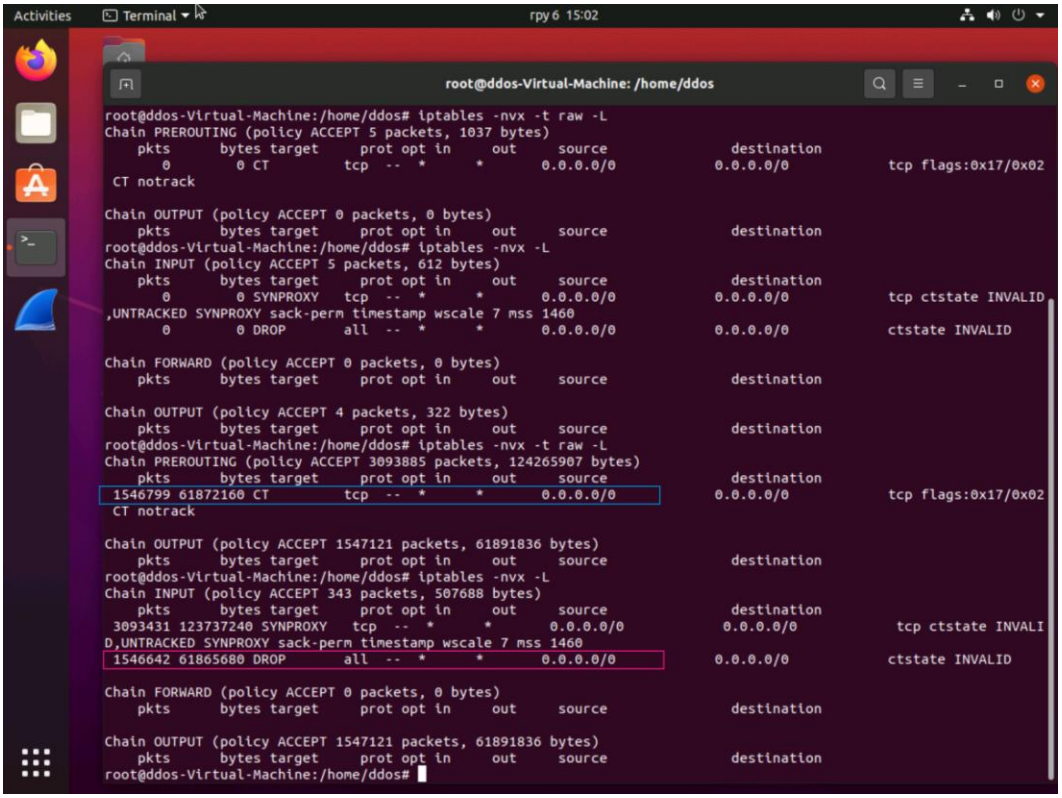


Рисунок 4.4 – Результат блокування атак TCP SYN Flood брандмауером хосту жертви за правилами iptable

4.3.2 Перевірка захисту хосту від атак UDP Flood

Використаємо модуль iptables recent для чого (рисунок 4.5):

Вмикаємо відслідковування трафіку

iptables -A INPUT -p udp – dport 80:80 -m state --state NEW -m recent –set

Дозволимо не більше 2 запитів у секунду

iptables -A INPUT -p udp –dport 80:80 -m state –state NEW -m recent –update –seconds 1– hitcount 2 -j DROP

Далі, здійснюємо атаку UDP Flood на хост жертви з IP - адресою 172.18.106.30 (рисунок 4.6).

На рисунку 4.7 наведений графік UDP потоку атаки UDP Flood.

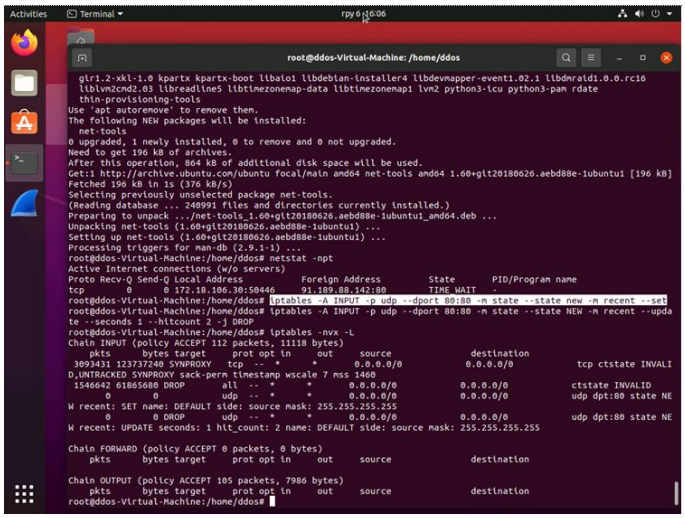


Рисунок 4.5 – Результат виконання команд модуля iptables recent

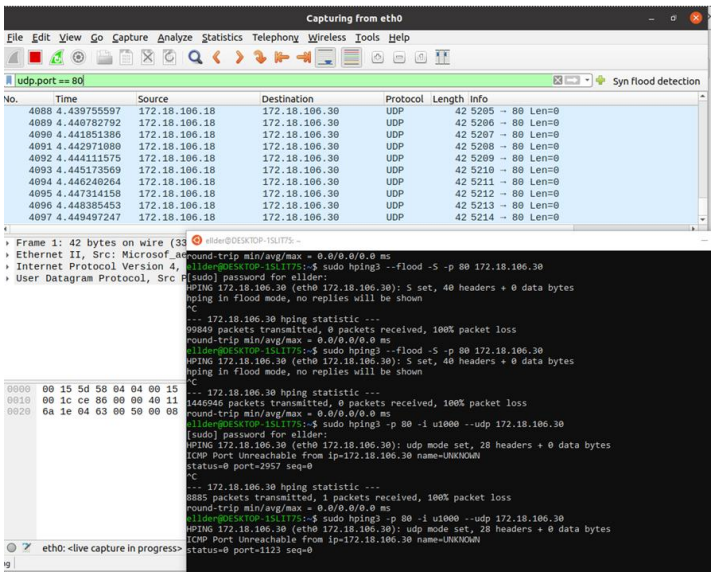


Рисунок 4.6 – Результат виконання команди hping3 на хост жертви з IP - адресою 172.18.106.30

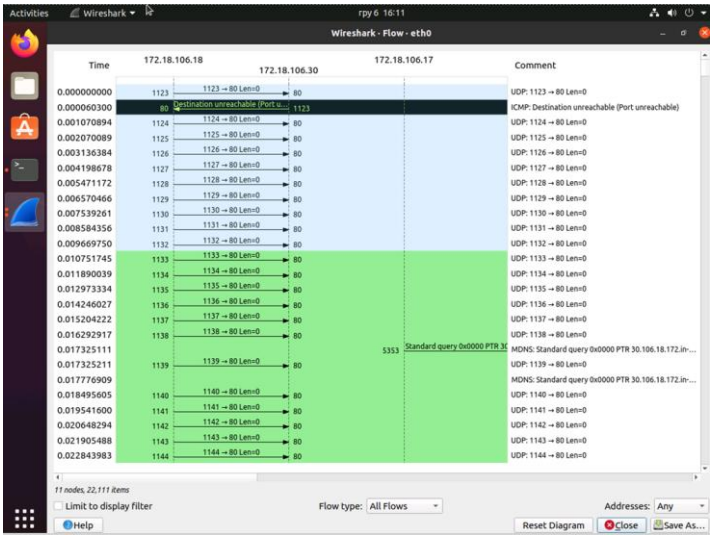


Рисунок 4.7– Графік UDP потоку атаки UDP Flood

Перевіримо статистику iptables (рисунок 4.8).

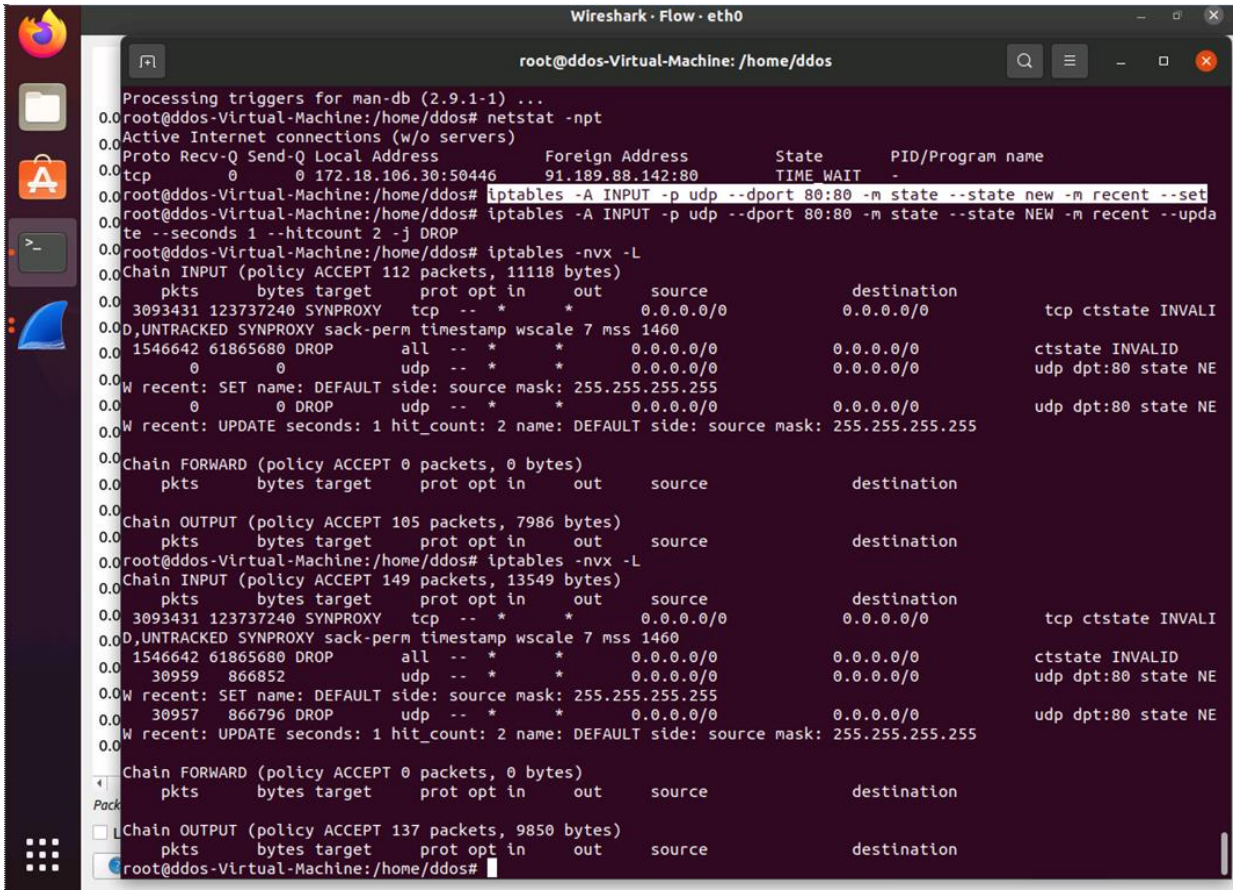


Рисунок 4.8– Результат блокування атак UDP Flood брандмауером хосту жертви

З рисунку 4.8 видно, що отримано 30959 пакетів (866852 байт), за правилами iptable заблоковано брандмауером 30957 пакетів (866796 байт).

4.3.3 Перевірка захисту хосту від атак на ICMP Flood

Для перевірки захисту хосту від атак на ICMP Flood налаштуємо iptables модуль limit, обмежуючись 3 пакетами (рисунок 4.9):

```
# iptables -N icmp_flood
# iptables -A INPUT -p icmp -j icmp_flood
# iptables -A icmp_flood -m limit --limit 1/s --limit-burst 3 -j RETURN
# iptables -A icmp_flood -j DROP
```

Здійснимо атаку ICMP Flood за допомогою команди hping3 на хост жертви з IP - адресою 172.18.106.30 (рисунок 4.10).

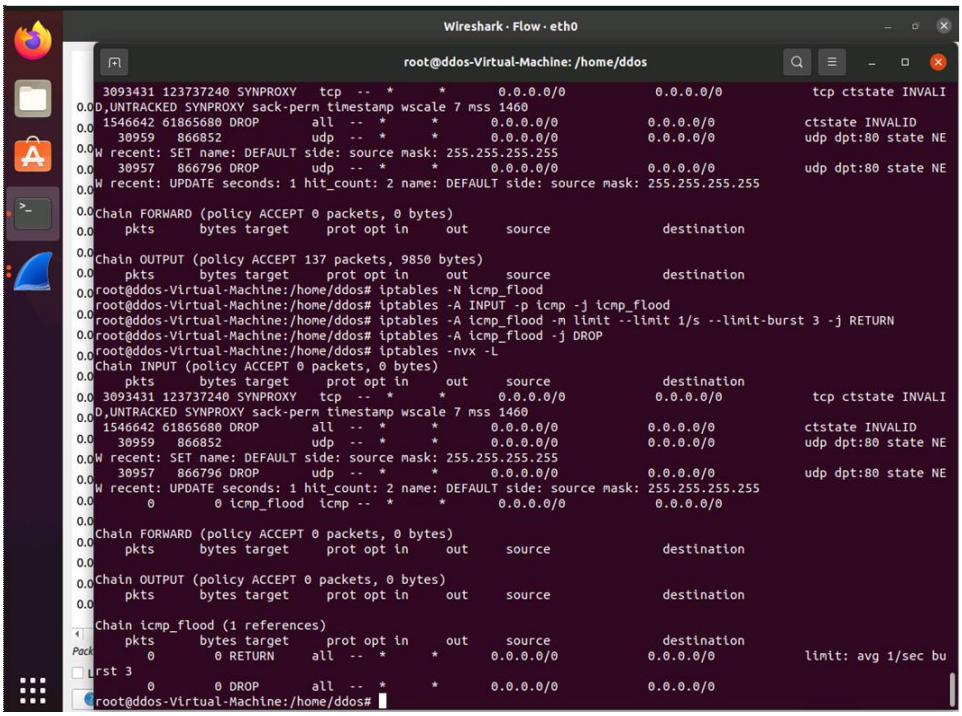


Рисунок 4.9 – Результат виконання команд модуля limit

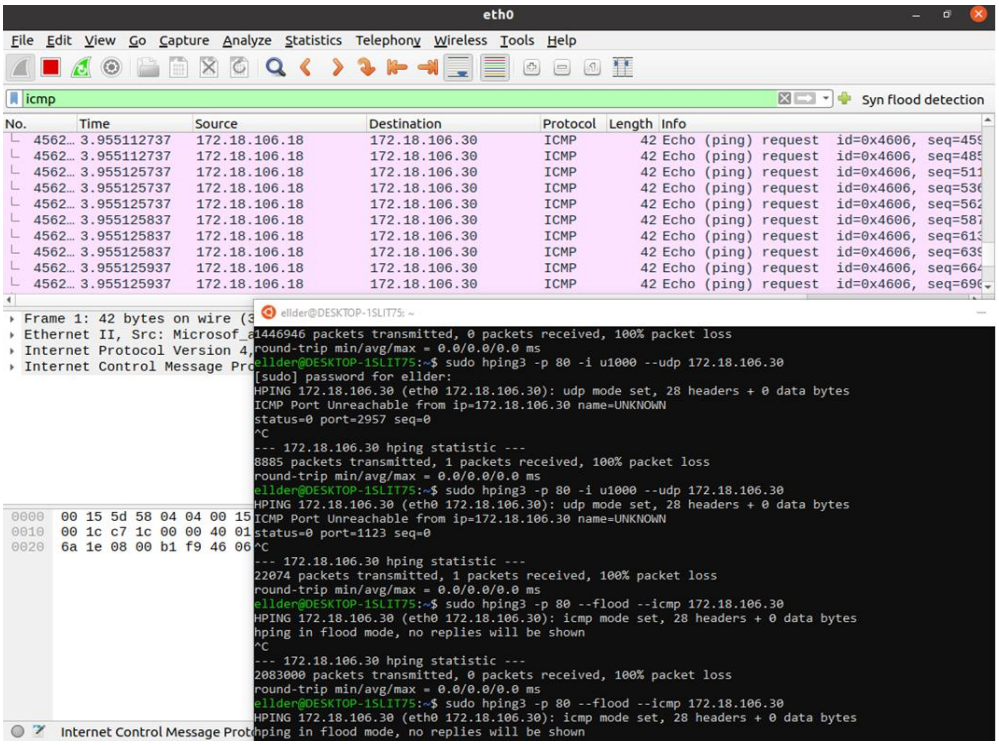


Рисунок 4.10 – Результат виконання команди hping3 на хост жертви з IP - адресою 172.18.106.30

На рисунку 4.11 наведений графік ICMP потоку атаки ICMP Flood.

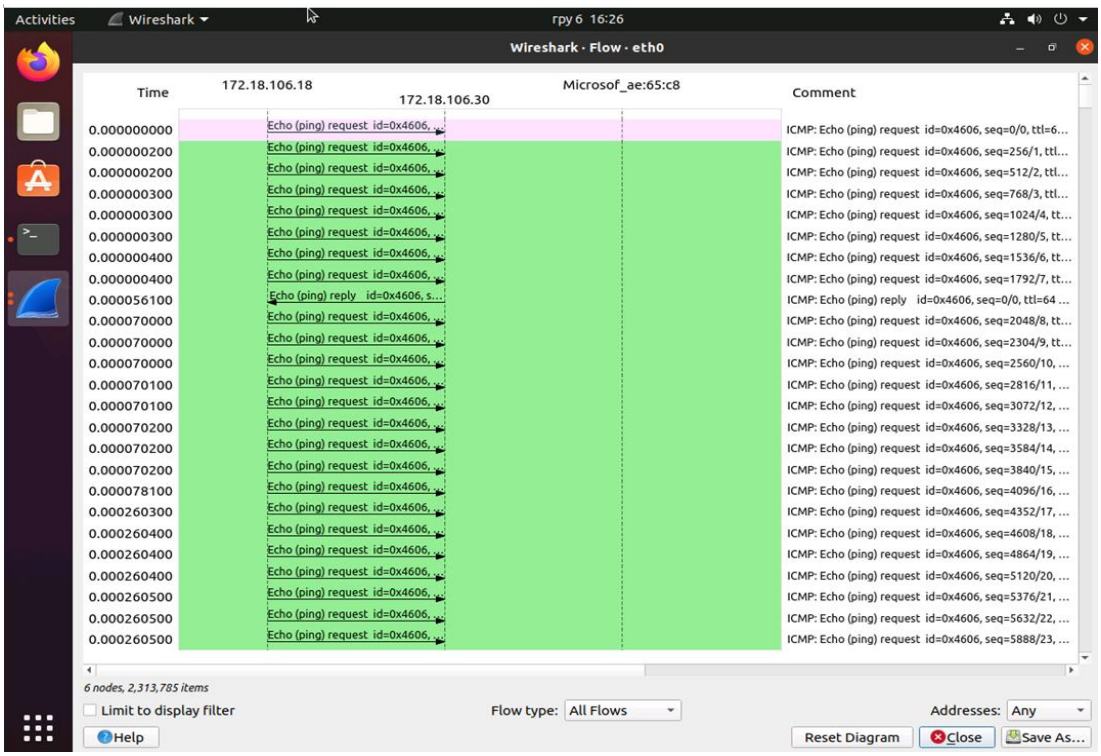


Рисунок 4.11– Графік ICMP потоку атаки ICMP Flood

Перевіряємо статистику iptables (рисунок 4.12).

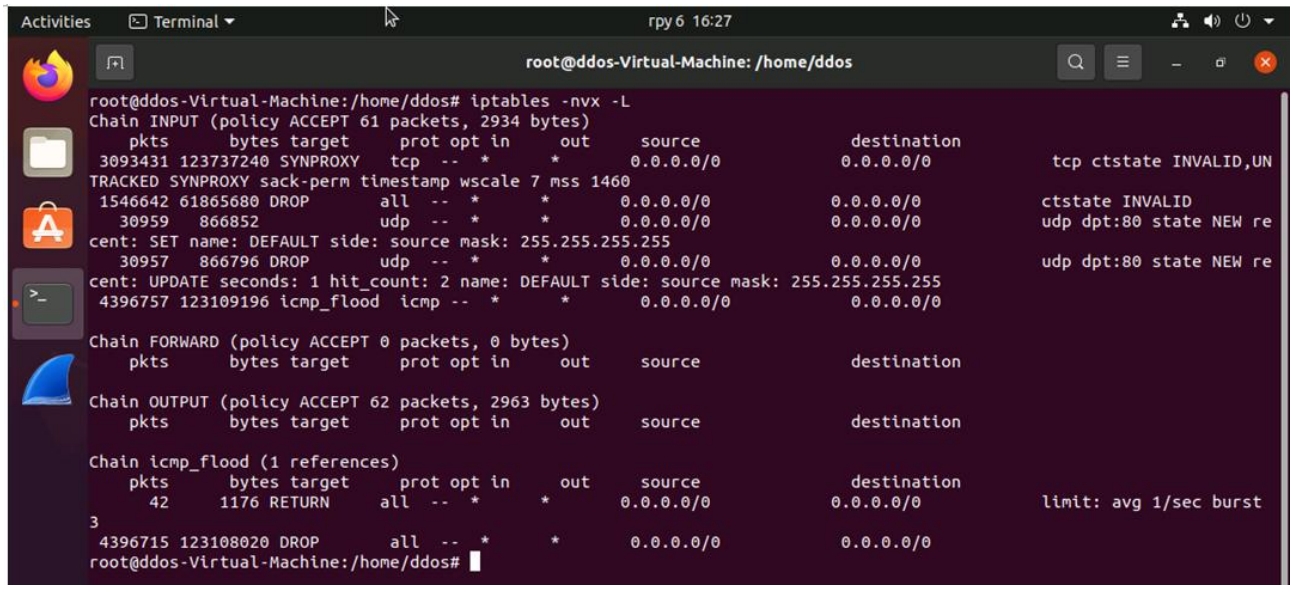


Рисунок 4.12 – Результат блокування атак ICMP Flood брандмауером хосту жертви

З рисунку 4.12 видно, що з мережі отримано 4396757 пакетів, при цьому заблоковано брандмауером – 4396715 пакетів і дозволено 42 пакети.

Висновки до четвертого розділу

1. Загалом, є дві стратегії захисту, які завжди слід поєднувати:

Зростання або оптимізація обчислювальних мережевих ресурсів для обробки більшої кількості запитів; відокремлення зловмисного трафіку від легального; блокування або відмова в пріоритетності потенційно зловмисного трафіку.

2. У цій роботі, була досліджена можливість правил iptables (брандмауер) для захисту від атак типу TCP SYN Flood, UDP, ICMP Flood. Розроблений алгоритм проходження пакетів за правилами iptables.

Для визначення законності мережевого трафіку, iptable покладається на набір правил, що містяться в таблицях, які мають бути попередньо визначені у мережевого або системного адміністратора. iptables дозволяє встановлювати правила за якими обробляється мережний трафік, який: надходить з певного джерела; прямує до певного пункту призначення; має певний тип протоколу.

3. За допомогою аналізатора мережних протоколів Wireshark і на основі аналізу сценаріїв з використанням iptables можна настроїти дозвіл / заборону трафіку мережі залежно від його швидкості будь-якої IP адреси комп'ютера, який відправляє пакети. Показано, що скрипти iptables та дистрибутив Linux в основному націлені на маршрутизацію та вбудовані пристрої для захисту від DoS / DDoS атак.

Висновки

1. Проведений аналіз літературних джерел та існуючих рішень показав, що атаки здійснюються як на окремих користувачів, так і на організації, завдаючи при цьому величезного морального та матеріального збитку. Це обумовлює необхідність розробки моделей виявлення найбільш поширених атак, серед яких є атаки на мережеве обладнання, а також засобів захисту, які перешкоджали б їх здійсненню.

2. Розглянуто характеристику протоколу TCP/IP та стек протоколу TCP/IP. Показано, що TCP/IP є найбільш завершений, стандартний і у той же час найбільш популярний стек мережевих протоколів. За своєю структурою він повністю відповідає 7 рівневій моделі OSI.

3. Представлена класифікація і цілі DDoS – атак. Показано, що атаки включають різноманітні механізми взаємодії, взаємодіючи на програмному рівні.

4. Виявлено, що найбільш типовими за реалізацією є атаки типу SYN-flood. Показано, що вони охоплюють усі основні методи втручання в роботу мережевих додатків.

5. Побудована ідентифікаційна модель атак з використанням двох віртуальних машин з встановленим програмним забезпеченням Ubuntu 20.04.1 LTS та віртуальної машини підсистеми Windows для Linux версії WSL2. Це дало отримати розуміння принципу створення атаки дозволяє визначити можливі шляхи протидії атакам.

6. Досліджена можливість правил iptables для захисту від атак типу TCP SYN Flood, UDP, ICMP Flood. Розроблений алгоритм проходження пакетів за правилами iptables. Показано, що скрипти iptables та дистрибутив Linux в основному націлені на маршрутизацію та вбудовані пристрої для захисту від DoS / DDoS атак.

ПЕРЕЛІК ПОСИЛАНЬ

1. «Компьютерные сети. Принципы, технологии, протоколы», Олифер В.Г., Олифер Н.А., 3-е издание. – СПб.: Питер, 2006. – 958 с.: ил.

2. Таненбаум Э. “Компьютерные сети”. Э.Таненбаум, пер. с англ. В. Шрага изд. 4-е, Спб-2010.- 992с.

3. 2020 Cyber Security Statistics. The Ultimate List Of Stats, Data & Trends– Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://t1p.de/i7fo

4. Віддалені мережеві атаки – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/

5. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. НПО «Мир и семья-95», 1997.

6. Лукацкий А.В. Обнаружение атак. – Серия: Мастер систем Изд.: BHV-Санкт – Петербург, 2003.– 268 с.

7. Ленков СВ. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К.: Арий, 2008. – і. Т.2: Информационная безопасность. – 2008. – 344 с.

8. Cohen Fred. Simulating Cyber Attacks, Defenses, and Consequences. Fred Cohen & Associates, March, 1999.

9. Типи атак DDoS. – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://firstvds.ru/technology/types-of-ddos

10. S. Gavaskar, R. Surendiran and Dr. E. Ramaraj, "Three Counter Defense Mechanism for SYN Flooding Attacks", International Journal of Computer Applications, Volume 6 – No. 6, pp. 12-15, Sep. 2010.

11. Detecting DNS amplification attacks / G. Kambourakis, T. Moschos, D. Geneiatakis, S. Gritzalis // Critical Information Infrastructures Security. T. 5141. P. 185–196.

12. Rozekrans T., Mekking M., de Koning J. Defending against DNS reflection amplification attacks // University of Amsterdam, Tech. Rep., Feb. 2013. URL:

https:// nlnetlabs.nl/downloads/publications/report-rrl-dekoningrozekrans.pdf (дата обращения 20.10.2016).

13. RFC 793 – формат TCP протокола.

14. Кручинин С. В. Семиуровневая модель OSI/ISO и стек протоколов TCP/IP: исследование взаимоотношения и интерпретации. – Научно-исследовательские публикации, 2015, №5 (25). – С. 115-120.

15. RFC 790, RFC791 – формат IP протокола.

16. DDoS-атаки: типы атак и уровни модели OSI. – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://firstvds.ru/technology/types-of-ddos

17. W. M. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," RFC 4987, August 2007. [Online]. Available: http://tools.ietf.org/html/rfc4987.

18. Seggelmann, R.; Tuxen, M.; Rathgeb, E.P. SSH over SCTP - Optimizing a multi-channel protocol by adapting it to SCTP // Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2012 8th International Symposium on : journal, 2012. - P. 1-6.

19. Microsoft. Virtualization – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/quick-create-virtual-machine

20. Моделируем и определяем DoS атаку типа TCP SYN Flood при помощи Wireshark – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://networkguru.ru/dos-ataka-tcp-syn-flood/

21 Протокол ARP – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://docstore.mik.ua/tcpip/arp.htm

22. Справочное руководство Nmap (Man Page) – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://nmap.org/man/ru/index.html

23. The netfilter.org project – Назва з екрану. – [Електронний ресурс]. – Режим доступу: http://www.netfilter.org/

24. Руководство по iptables (Iptables Tutorial 1.1.19) – Назва з екрану. – [Електронний ресурс]. – Режим доступу: http://opennet.ru/docs/RUS/iptables/

25. DDoS Protection With IPtables: The Ultimate Guide – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://javapipe.com/blog/iptables-ddos-protection/

Додаток А

Презентація

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем

Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА «ІДЕНТИФІКАЦІЙНА МОДЕЛЬ ХАКЕРСЬКОЇ АТАКИ НА МЕРЕЖЕВЕ УСТАТКУВАННЯ»

Спеціальність 172 – «Телекомунікації та радіотехніка»

Виконав: студент 2 курсу, група $ТР_м$-19-1 А. О. Казімірко

Керівник: канд. техн. наук, доц. А. А. Таранчук

Хмельницький, 2020

Мета роботи – побудова ідентифікаційної моделі хакерської атаки на мережеве устаткування.

Завдання, які вирішуються в роботі

1. Провести аналіз забезпечення безпеки інтернет з'єднань та існуючих типів атак на мережеве обладнання.
2. Розглянути протоколи мережевої взаємодії з точки зору їх уразливості до хакерських атак.
3. Побудувати ідентифікаційну модель хакерської атаки на TCP типу SYN flood.
4. Розробити та навести програмні методи захисту від мережевих атак.

Об'єкт дослідження: процеси хакерської атаки на мережеве устаткування.

Предмет дослідження: ідентифікаційна модель хакерської атаки на мережеве устаткування.

Наукова новизна отриманих результатів:

1. Побудована удосконалена ідентифікаційна модель атак з використанням віртуалізації машин, дистрибутиву Linux, що дозволило дослідити принципи створення DoS/DDoS атак типу «відмова в обслуговуванні» та дозволяє, в подальшому, визначити можливі шляхи протидії цим атакам.

Практична значимість отриманих результатів:

1. Проведений аналіз літературних джерел та існуючих рішень показав, що атаки здійснюються як на окремих користувачів, так і на організації, завдаючи при цьому величезного морального та матеріального збитку. Це обумовлює необхідність розробки моделей виявлення найбільш поширених атак, серед яких є атаки на мережеве обладнання, а також засобів захисту, які перешкоджали б їх здійсненню.

2. Представлена класифікація і цілі DDoS – атак. Показано, що атаки включають різноманітні механізми взаємодії, взаємодіючи на програмному рівні. Показано, що атаки типу SYN-flood охоплюють усі основні методи втручання в роботу мережевих додатків.

3. Досліджена можливість правил iptables для захисту від атак типу TCP SYN Flood, UDP, ICMP Flood. Розроблений алгоритм проходження пакетів за правилами iptables.

4. Проведений моніторинг мережі за допомогою аналізатора мережних протоколів Wireshark і на основі аналізу сценаріїв з використанням iptables. Показано, що скрипти iptables та дистрибутив Linux в основному націлені на маршрутизацію та вбудовані пристрої для захисту від DoS / DDoS атак.

1. КЛАСИФІКАЦІЯ АТАК В МЕРЕЖІ

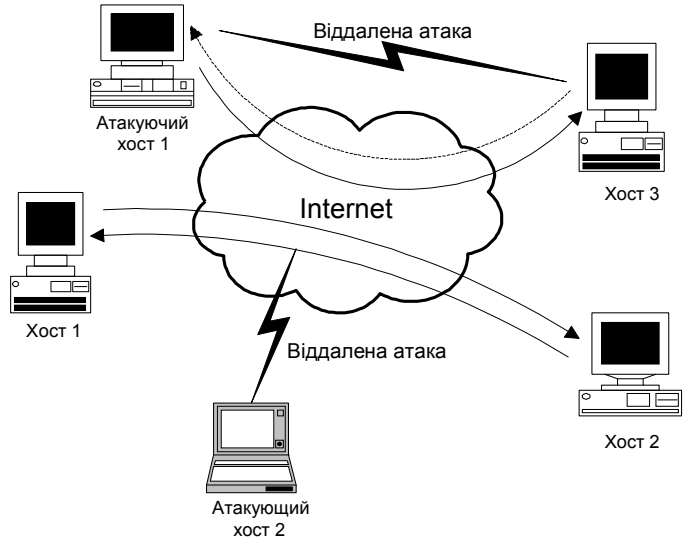


Рисунок 4.1 – Віддалені атаки через Internet

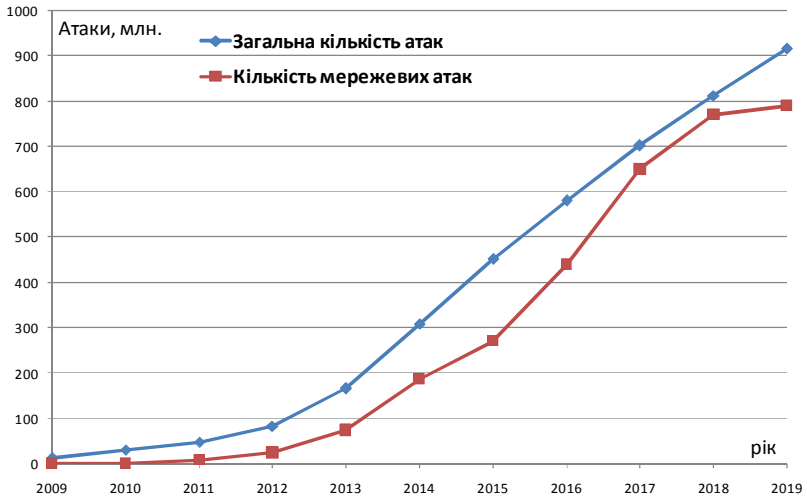


Рисунок 4.2 – Кількість атак

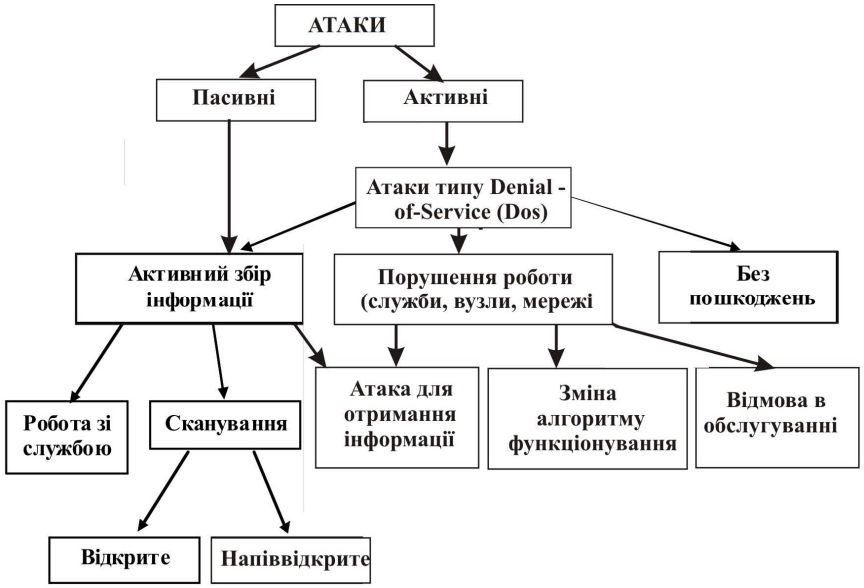


Рисунок 4.3 – Класифікація атак в мережі

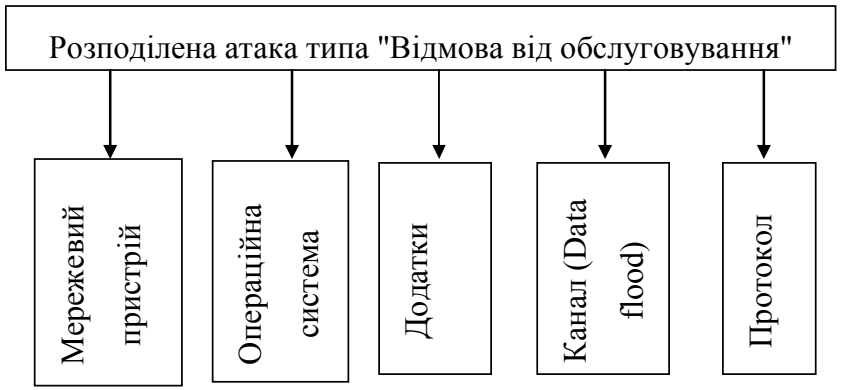


Рисунок 4.4 – Класифікація DdoS атак

2. МОДЕЛЬ МЕРЕЖЕВОЇ АТАКИ SYN FLOOD ТА ПРОЦЕС - «ВІДМОВА В ОБСЛУГОВУВАННІ»

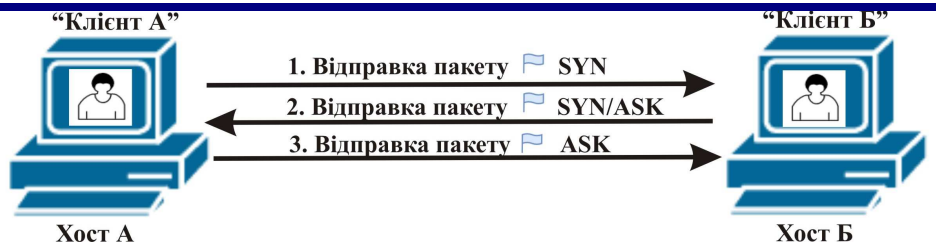


Рисунок 5.1 – Реалізація алгоритму «потрійного рукостискання»

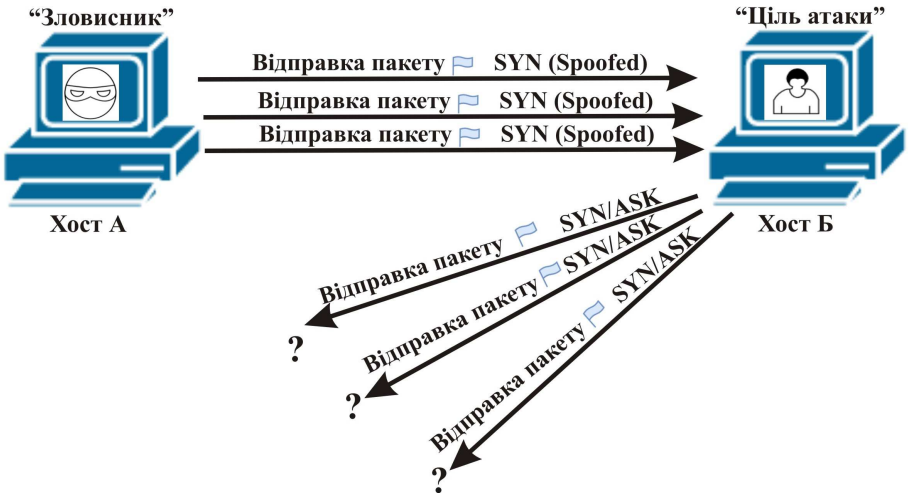


Рисунок 5.2 – Мережева атака SYN Flood та процес - «відмова в обслуговуванні»

1. Хост А (зловмисник) відправляє пакет з прапором SYN з підміненою IP -адресою хосту Б (ціль атаки), запрошуючи ініціалізацію нової сесії TCP у операційній системі хосту Б.
2. Хост Б відправляє пакет з прапором SYN / ACK хосту А. За звичайним тристороннім механізмом рукостискання, при відкритій сесії TCP, хост А повинен надіслати хосту Б пакет з прапором ACK.
3. Однак атакуюча система А не відповідає ні на один з повернутих пакетів SYN / ACK. У цьому випадку хост Б знаходиться в «напіввідкритому» статусі (75 секунд).
4. Зловмисники використовують цю відкриту сесію, відправляючи на порт хосту Б (ціль атаки) швидкий потік SYN- пакетів.
5. На хості Б черга запитів на підключення переповниться і досягне максимального рівня, тоді всі наступні запити будуть відхилені операційною системою хосту Б. Хост Б взагалі не зможе встановити TCP- з'єднання за рахунок втрати продуктивності. Цей процес називається «відмовою в обслуговуванні» (рис. 5.1, 5.2)

2.2 ВСТАНОВЛЕННЯ ВІРТУАЛЬНОЇ МАШИНИ

Крок 1. Для проведення симуляції атаки атакуєма і атакуюча машини повинні знаходитись в одній мережі (обмеження Hyper-V). Для цього зайдемо в налаштування віртуальної машини лінукс і переведемо її в WSL мережу. Для атак будемо використовувати Windows Subsystem for Linux Installation Guide for Windows 10 для чого в менеджере віртуальних машин потрібно включити WSL.

Крок 2. Встановити інструментарій hping3 в дистрибутив Linux (машини зловмисника) за допомогою команди:

«# sudo apt-get install hping3»

Крок 3. Імітуємо атаку TCP SYN-flood. Атака здійснюється зловмисником на машину жертви, при цьому він запустив наступну команду:

hping3 –c1500 -d 120 –S –w 64 –p 80--flood--rand-sourse

За цією командою на машину жертви надсилається 1500 пакетів розміром 120 байт з SYN Flag та розміром вікна TCP пакету – 64 байти. Атаки здійснюються на порт 80 HTTP веб- серверу. Параметр rand-source – означає, що зловмисник надсилає пакети з максимально можливою швидкістю з підміненими IP – адресами (рис. 7.2).

Для ідентифікації атаки необхідно на машину жертви встановити спеціальне програмне забезпечення Wireshark та за допомогою нього здійснити захват трафіку TCP пакетів, що надсилає джерело зловмисника.

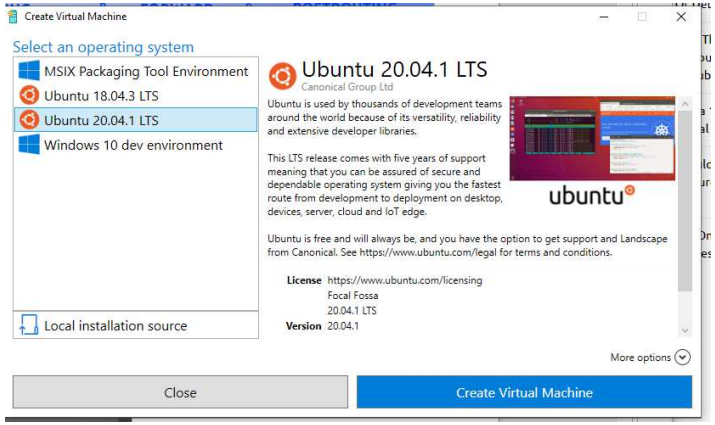


Рисунок 6.1 – Встановлення віртуальної машини: початкове вікно Ubuntu 20.04.1 LTS “Focal Fossa”

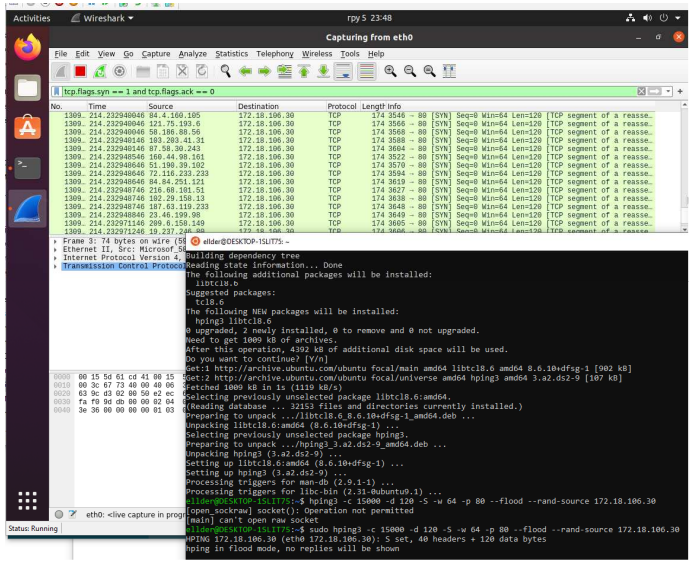


Рисунок 6.2 – Результат виконання команди hping на машину жертви з IP - адресою 172.18.106.30

5 ПОЧАТОК АТАКИ

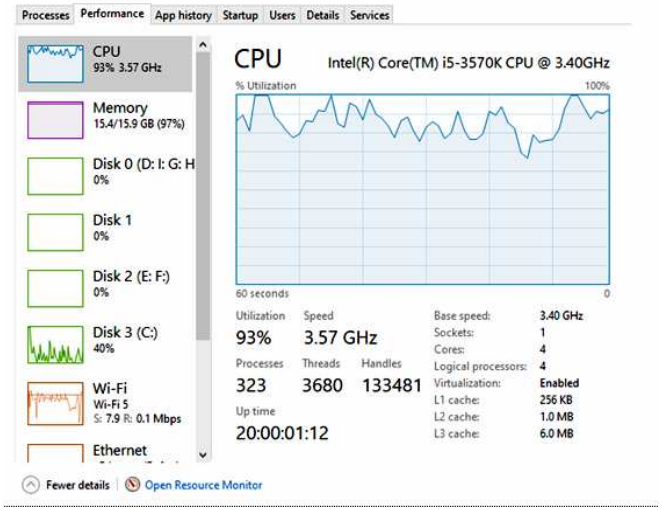


Рисунок 7.1 – Результат перенавантаження процесора

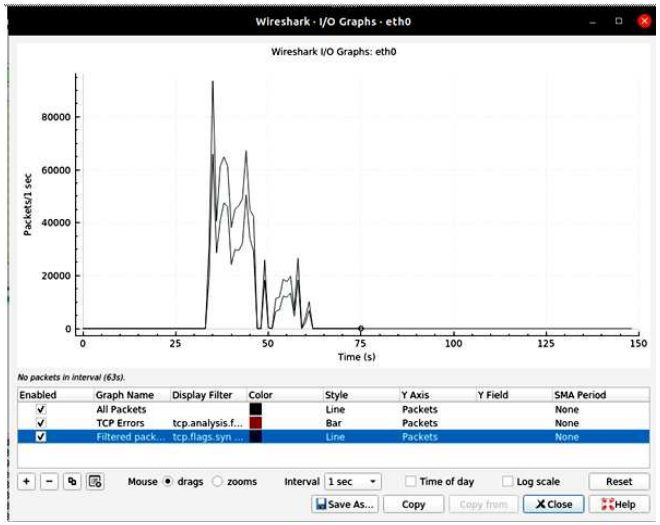


Рисунок 7.2 – Розподіл атаки пакетів TCP за секунду під час атаки

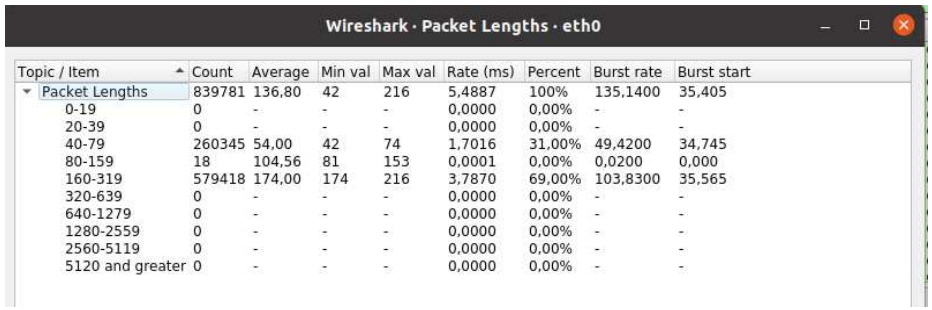


Рисунок 7.3 – Вікно даних про розміри IP пакетів

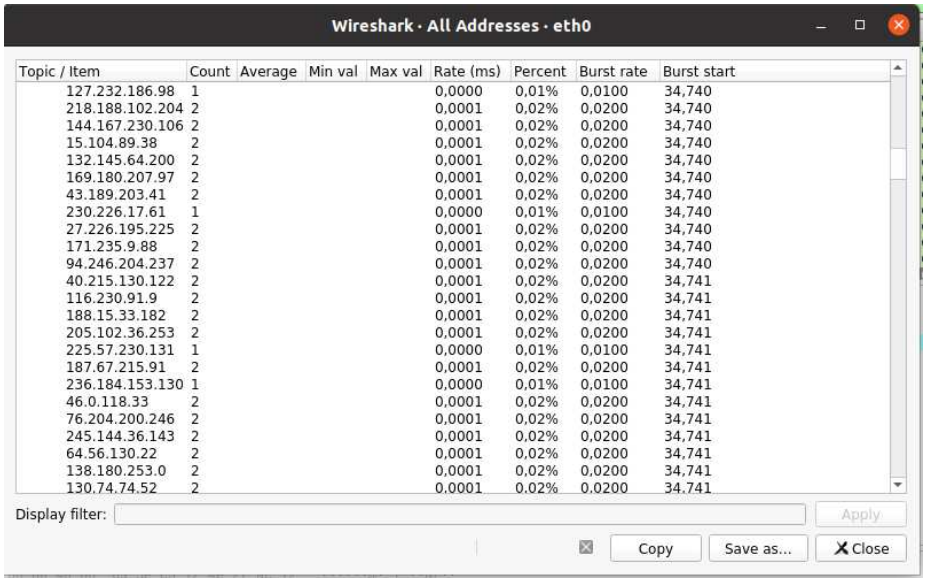
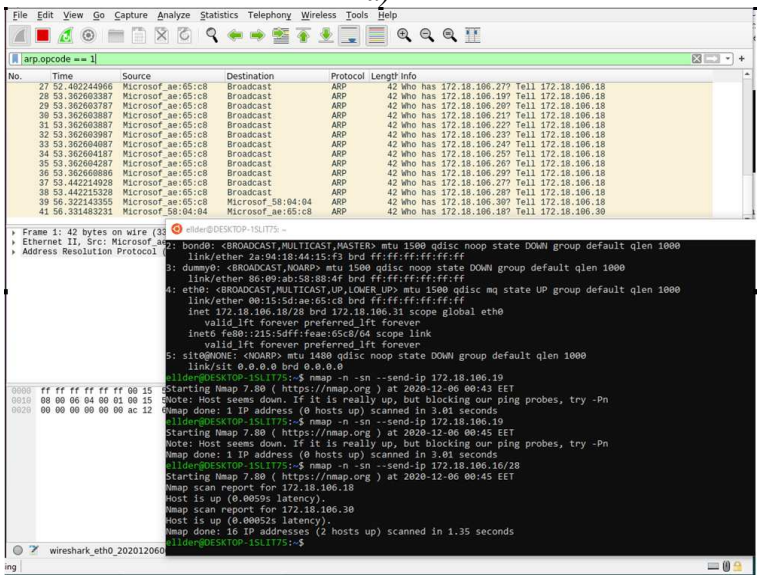


Рисунок 7.4 – Результат підміни IP- адрес зловмисником

6 ІДЕНТИФІКАЦІЯ АТАКИ TCP SYN Flood

а)



б)

Рисунок 8.1 – Результат сканування: SYN запиту на порт 80 жертви (а); визначення IP- адреси атакуючого 172.18.106.18 (б)

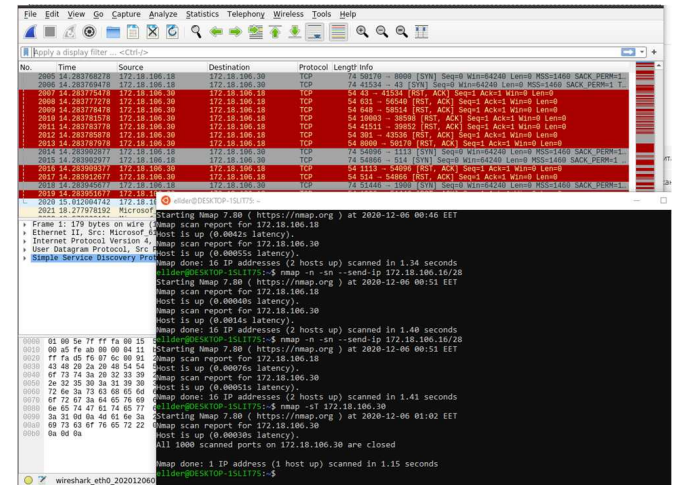


Рисунок 8.2 – Ідентифікація атаки TCP SYN Flood за допомогою Wireshark

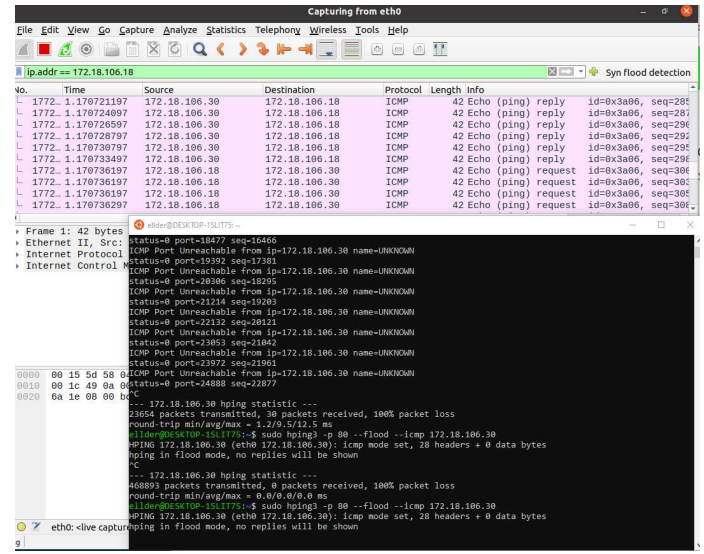


Рисунок 8.3 – Реалізація атаки ICMP Flood на за допомогою утілити hping3 на IP- адресу 172.10.106.30

7 РЕАЛІЗАЦІЯ БРАНДМАУЕРУ ЗА ДОПОМОГОЮ ТАБЛИЦЬ IPTABLES

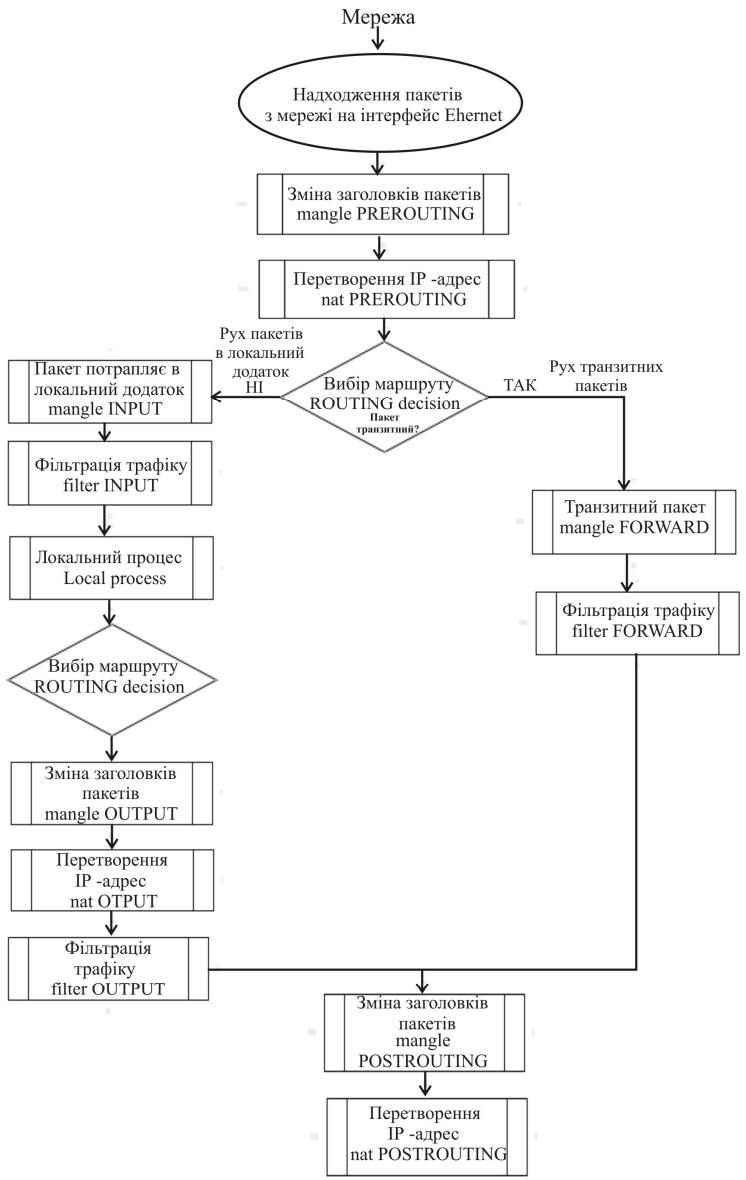


Рисунок 9.1– Алгоритм проходження пакетів через брандмауер

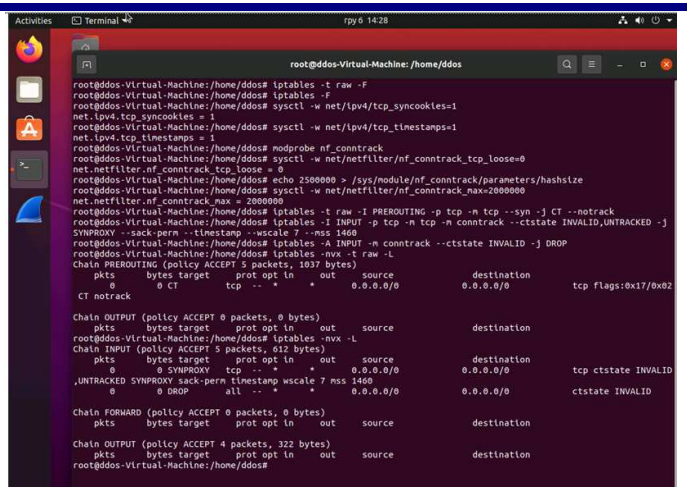


Рисунок 9.2 – Поточний стан правил та лічильників iptables (лічильники виставлені в нуль)

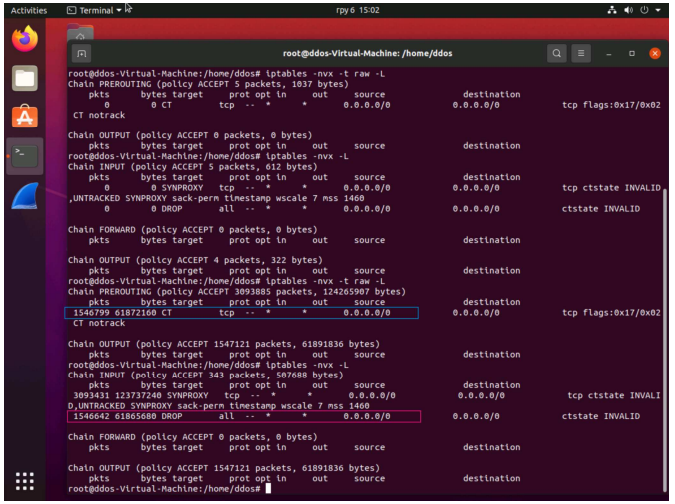


Рисунок 9.3 – Результат блокування атак TCP SYN Flood (фільтр INPUT) (прийнято 1546799 пакетів, за правилами iptable заблоковано брандмауером 1546642 пакетів)

Для перевірки захисту хосту від атак на ICMP Flood налаштуємо iptables модуль limit, обмежуючись 3 пакетами (рисунок 10.1):

```
# iptables -N icmp_flood
# iptables -A INPUT -p icmp -j icmp_flood
# iptables -A icmp_flood -m limit --limit 1/s --limit-burst 3 -j RETURN
# iptables -A icmp_flood -j DROP
```

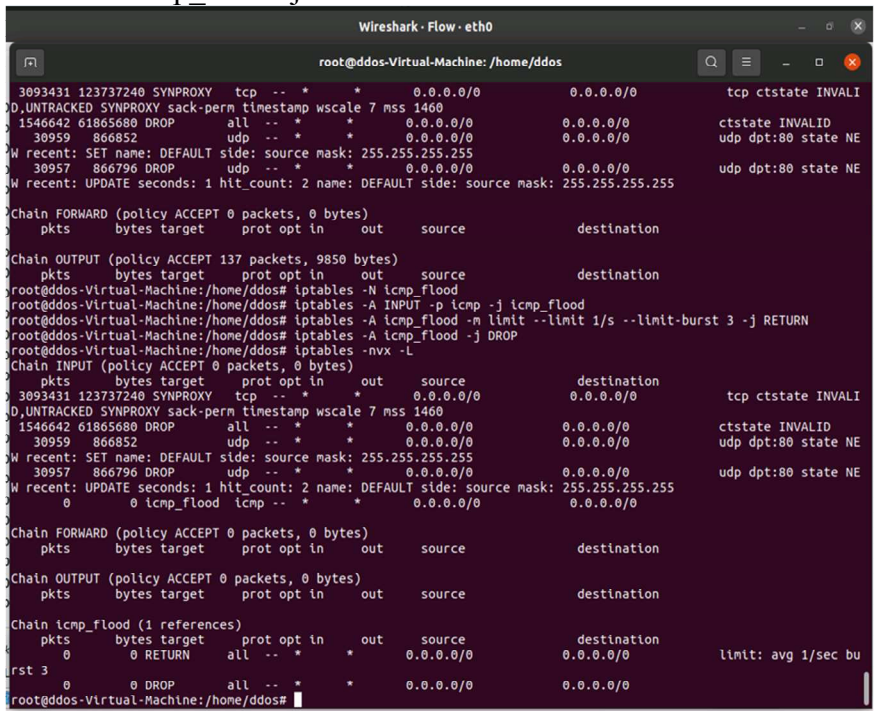


Рисунок 10.1 – Результат виконання команд модуля limit

Висновок. З рисунку 10.3 видно, що з мережі отримано 4396757 пакетів, при цьому заблоковано брандмауером – 4396715 пакетів і дозволено 42 пакети.

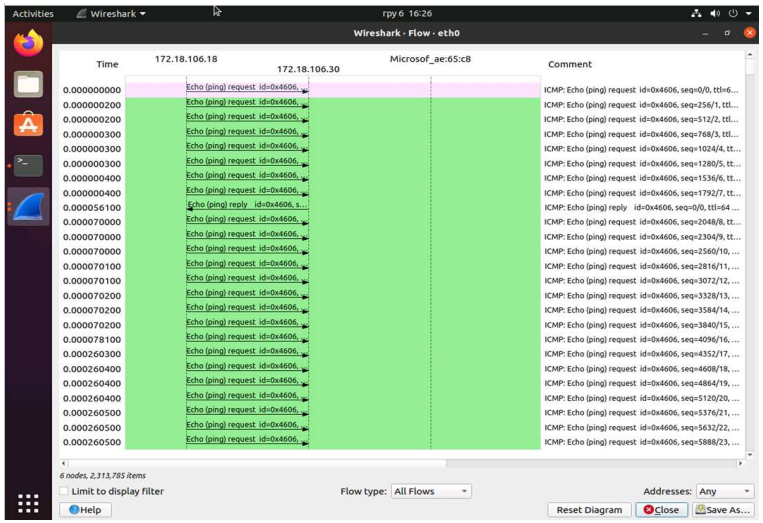


Рисунок 10.2– Графік ICMP потоку атаки ICMP Flood

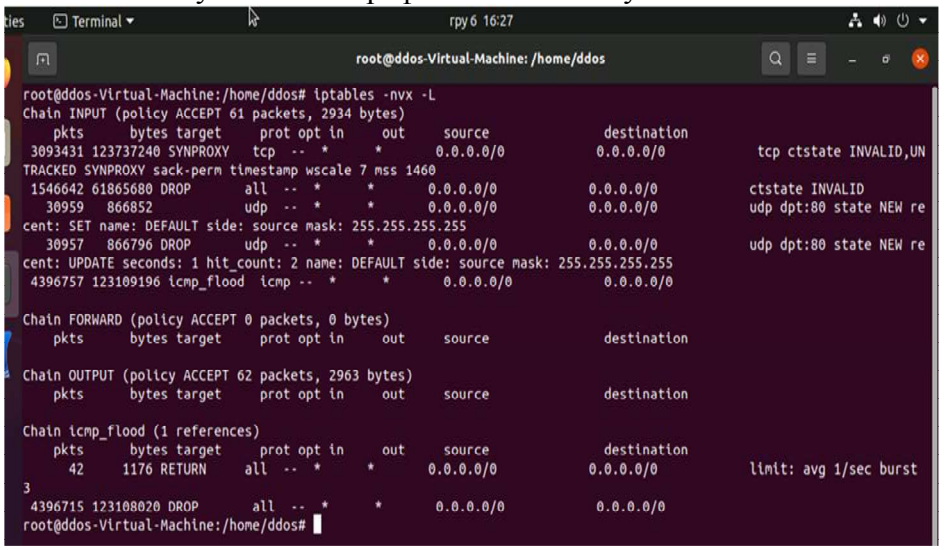


Рисунок 10.3 – Результат блокування атак ICMP Flood брандмауером хосту жертви

ВИСНОВКИ

1. Проведений аналіз літературних джерел та існуючих рішень показав, що атаки здійснюються як на окремих користувачів, так і на організації, завдаючи при цьому величезного морального та матеріального збитку. Це обумовлює необхідність розробки моделей виявлення найбільш поширених атак, серед яких є атаки на мережеве обладнання, а також засобів захисту, які перешкоджали б їх здійсненню.

2. Розглянуто характеристику протоколу TCP/IP та стек протоколу TCP/IP. Показано, що TCP/IP є найбільш завершений, стандартний і у той же час найбільш популярний стек мережевих протоколів. За своєю структурою він повністю відповідає 7 рівневій моделі OSI.

3. Представлена класифікація і цілі DDoS – атак. Показано, що атаки включають різноманітні механізми взаємодії, взаємодіючи на програмному рівні.

4. Виявлено, що найбільш типовими за реалізацією є атаки типу SYN-flood. Показано, що вони охоплюють усі основні методи втручання в роботу мережевих додатків.

5. Побудована ідентифікаційна модель атак з використанням двох віртуальних машин з встановленим програмним забезпеченням Ubuntu 20.04.1 LTS та віртуальної машини підсистеми Windows для Linux версії WSL2. Це дало отримати розуміння принципу створення атаки дозволяє визначити можливі шляхи протидії атакам.

6. Досліджена можливість правил iptables для захисту від атак типу TCP SYN Flood, UDP, ICMP Flood. Розроблений алгоритм проходження пакетів за правилами iptables. Показано, що скрипти iptables та дистрибутив Linux в основному націлені на маршрутизацію та вбудовані пристрої для захисту від DoS / DDoS атак.

ДЯКУЮ ЗА УВАГУ!

Додаток Б

Тези доповіді

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Хмельницький національний університет

Військовий інститут Київського національного університету ім.Тараса Шевченка

ПВНЗ “Університет економіки і підприємництва”

Вінницький національний технічний університет

Західноукраїнський національний університет

Інтелектуальний потенціал - 2020

збірник наукових праць молодих науковців і студентів

сформовано за матеріалами
Всеукраїнської науково-практичної конференції
молодих науковців і студентів
«Інтелектуальний потенціал – 2020»

9-10 листопада 2020 р.

Частина 1

Хмельницький
2020

ББК 74.480.278
С.88

«Інтелектуальний потенціал – 2020» - збірник наукових праць молодих науковців і студентів / Колектив авторів – Хмельницький: ПВНЗ УЕП, 2020. – Частина 1. – 104 с.

ЗМІСТ

інформації було обрано семисегментний індикатор. Цифри на семисегментних індикаторах формуються з надходженням кодових комбінацій з дешифратора, що відповідають певній заданій цифрі.

Перелік посилань

1. Борисенко А. А. Биномиальные автомати - Суми: СумДУ, 2006 р. – с. 120

2. Борисенко А. А. Биномиальный счет и счетчики: монография. – Сумы: СумГУ, 2008. – 152 с.

Аналіз механізмів захисту мережевого устаткування від хакерської атаки типу TCP SYN Flood

Казімірко А.О.
Науковий керівник – к.т.н., доц. Таранчук А.А.
Хмельницький національний університет

В основі зв'язку та обміну повідомленнями між хостами користувачів глобальної мережі Інтернет лежить набір протоколів TCP / IP - це простий набір правил (стек) обміну інформацією, або протокол управління передачею [1].

Даний стек має слабкі місця, які полягають в його вразливості до хакерських атак типу TCP SYN Flood при підключенні хост машин користувачів до мережі Інтернет. Користуючись цією слабкістю, хакери можуть атакувати систему певного користувача в будь –який час. Мережева атака SYN Flood полягає у відправці великої кількості пакетів SYN-запитів на підключення за протоколом TCP до операційної системи іншого хосту, причому пакети надсилаються в дуже короткий інтервал часу [1].

Основна ідея атаки полягає в тому, щоб під час процесу запуску сесії TCP, змушувати хост зберігати досить велику кількість напівз'єднань для вичерпання його ресурсів і не можливості встановлення нових зв'язків.

В основі процесу початку TCP сеансу лежить алгоритм «потрійного рукостискання», який реалізується за три кроки (рис.1) [2]:

1) хост А надсилає пакет з прапором SYN на сервер Б (скор. від англ. synchronize - запит на підключення за протоколом TCP). Якщо відправлений пакет з прапором SYN, це означає, що хост А запитує у хосту Б з'єднання;

2) хост Б надсилає у відповідь пакет з прапором SYN / ACK (скор. від англ. (acknowledges), що містить криптографічну інформацію хосту А;

3) хост А надсилає пакет з прапором ACK до хосту Б, що означає – зв'язок встановлений.

Розглянемо як відбувається атака SYN Flood на деякий хост мережі Інтернет.

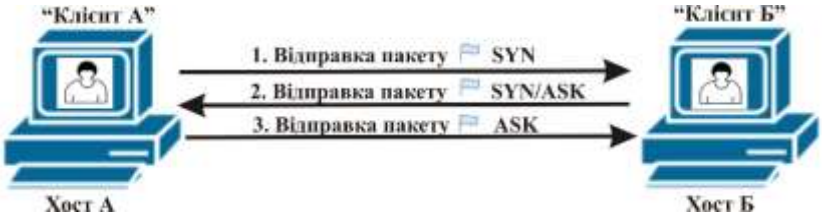


Рисунок 1 – Реалізація алгоритму «потрійного рукостискання»

Мережева атака TCP SYN Flood використовує тристоронній механізм рукостискання, описаний вище (рис.1). При цьому, з хосту А зловмисник відправляє пакет з прапором SYN (зазвичай використовується підмінена IP - адреса - англ. spoofing) хосту Б (ціль атаки), запрошуючи ініціалізацію нової сесії TCP у операційній системі хосту Б. Далі хост Б відправляє пакет з прапором SYN / ACK хосту А. За звичайним тристороннім механізмом рукостискання, при відкритій сесії TCP, хост А повинен надіслати хосту Б пакет з прапором ACK. Однак атакуюча система А не відповідає ні на один з повернутих пакетів SYN / ACK. У цьому випадку хост Б, очікуючи пакет з прапором ACK від хосту А знаходиться в «напіввідкритому» статусі, встановлюючи неповне з’єднання, яке зберігається у черзі таблиці з’єднань (англ. Transmission Control Block table - TCB). Через 75 секунд неповне з’єднання видаляється із черги TCB і руйнується (рекомендація RFC 4987). Зловмисники використовують цю відкриту сесію, відправляючи на порт хосту Б (ціль атаки) швидкий потік SYN- пакетів, перш ніж хост Б видалить неповні з'єднання з черги TCB у разі не отримання відповідей на надісланий пакет SYN/ACK. За цей час на хості Б черга запитів на підключення переповниться за рахунок зберігання великої кількості фальшивих «напіввідкритих» з’єднань, які займають всю пам’ять TCB. Коли кількість вхідних з'єднань досягне максимального рівня, тоді всі наступні запити будуть відхилені операційною системою хосту Б. У цьому випадку хост Б взагалі не зможе встановити TCP- з'єднання за рахунок втрати продуктивності. Цей процес називається «відмовою в обслуговуванні» (рис. 2) [2].

Успішна атака залежить від трьох параметрів: розміру загородження; частоти з якою створюються загородження та засобів вибору IP-адрес для підробки (містифікації).

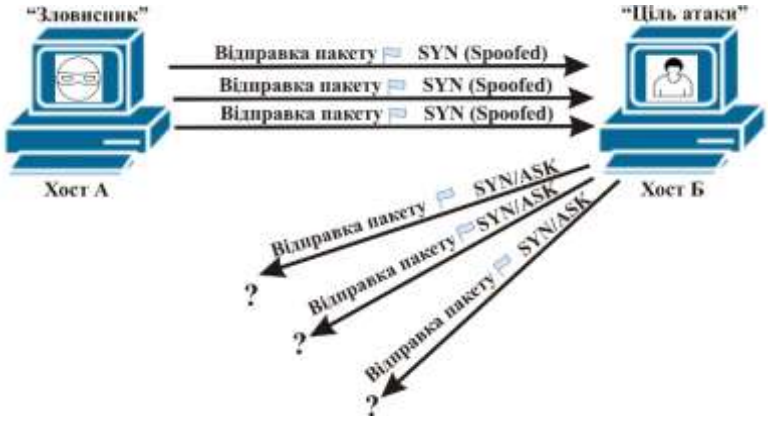


Рисунок 2 – Мережева атака SYN Flood та процес - «відмова в обслуговуванні»

Існує декілька механізмів захисту мережевого обладнання (хостів), які можуть частково забезпечити захист від SYN Flood – атак [3]:

1. Настройка стеку. Для цього можна налаштувати стек TCP, зменшивши його час «напіввідкритої» сесії з'єднань, або, іншими словами, тайм-аут звільнення пам'яті, виділеної для з'єднання, а також час виділений на блокування вхідних з'єднань. Але у цих налаштувань можуть бути побічні ефекти у вигляді втрати частини легітимних з'єднань через затримки і нестабільні канали.

2. Реалізація механізму SYN-Cookie. Для створення TCP-з'єднання хост А відправляє хосту Б TCP-пакет з прапором SYN і своїм номером послідовності. Механізм SYN cookies зовсім не використовує чергу SYN. Хост Б відправляє пакет з прапором SYN-ACK, який містить унікальну інформацію, що ідентифікує клієнта Б: IP - адресу; номер порту; час відправки пакету та прийнятий унікальний номер послідовності хосту А. Хост «зловмисника» ніколи не отримує ці пакети і тому не надасть на них відповідь. На завершальній відповіді хостом А ця інформація (хеш) вже включена в пакет з прапором ACK. При успішній перевірці ACK – пакету відповіді на SYN cookie, хостом Б виділиться пам'ять для з'єднання, навіть, якщо в черзі SYN не має відповідного запису. Для використання механізму хешування (порівняння даних) необхідно, щоб усі хости, які приймають участь в передачі трафіку його підтримували. Якщо SYN cookie включені, то «зловмисник» не зможе обійти такі міжмережеві екрани відправкою ACK-пакета з довільним номером послідовності поки не підбере вірний. SYN cookies потрібно включати тільки для публічно доступних портів. Включення механізму SYN cookies – це простий спосіб боротьби проти атаки SYN Flood.

Однак при його використанні буде більше завантаженість процесора клієнта під час створення та звірки cookies.

3. Обмеження запитів на нові підключення від конкретного джерела за визначений проміжок часу.

4. Використання мережевого протоколу транспортного рівня SCTP (англ. Stream Control Transmission Protocol - протокол передачі з керуванням потоком), який є більш сучасним, на відміну від TCP. Даний протокол використовує механізм SYN cookie та не підданий SYN- Flood атакам. Передача трафіку за протоколом SCTP здійснюється багатьма потоками, а синхронне з'єднання між двома хостами по двох та більше незалежних фізичних каналах (multi-homing) [3].

Перелік посилань

1. W. M. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," RFC 4987, August 2007. [Online]. Available: http://tools.ietf.org/html/rfc4987.

2. S. Gavaskar, R. Surendiran and Dr. E. Ramaraj, "Three Counter Defense Mechanism for SYN Flooding Attacks", International Journal of Computer Applications, Volume 6 – No. 6, pp. 12-15, Sep. 2010.

3. Seggelmann, R.; Tuxen, M.; Rathgeb, E.P. SSH over SCTP - Optimizing a multi-channel protocol by adapting it to SCTP // Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2012 8th International Symposium on : journal, 2012. - P. 1-6.

Модель «розумної» мережі енергопостачання житлового будинку

Ковальчук О.Л., Кучерявий Є.І.
Науковий керівник – к.т.н., доц. Таранчук А.А.
Хмельницький національний університет

В країнах ЄС активно впроваджуються «інтелектуальні» мережі Smart Grid, які поєднують в собі елементи традиційної електроенергетики та новітні електроенергетичні технології, комплексні інструменти контролю та моніторингу, інформаційно-комунікаційні технології та «інтелектуальні» вимірювальні системи [1,2].

В Україні на даний момент показник втрат електроенергії досягає 15%. При цьому в розвинених країнах Європи він становить лише 6%. Домогтися таких же показників на українській території може допомогти впровадження технології Smart Grid. Оптимальний результат досягається за рахунок впровадження інноваційних рішень, ефективного регулювання і управління розподілом електроенергії [1].

В даній роботі побудована імітаційна модель «розумної» мережі енергопостачання житлового будинку в симуляторі Cisco Packet Tracer [3],

Mon Dec 07 16:28:56 EET 2020, Степюк Віктор Іванович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 13%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 82818 Название: Ідентифікаційна модель хакерської атаки на мережеве устаткування Добавлено в БД: 2020-12-07 Авторы: Казімірко Андрій Олександрович Руководители: Таранчук Алла Анатолівна Консультанты: Оппоненты:	Символы	Лексемы	Символы	Лексемы
	71947	606	340 (0%)	6 (1%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Имя пользователя: Kafedra TMIT KhNU
ID проверки: 1005392516
Дата проверки: 07.12.2020 18:35:41 EET
Тип проверки: Doc vs Internet + Library
Дата отчета: 07.12.2020 18:45:05 EET
ID пользователя: 100005657

Название файла: Казімірко_ТРм-19-1

Количество страниц: 74 Количество слов: 11811 Количество символов: 84240 Размер файла: 8.50 MB ID файла: 1005684577

95 слов помечены как "исключенные" и не учитываются в подсчете слов

Обнаружены модификации текста (могут влиять на процент совпадений)

4.14% Совпадения

Наибольшее совпадение: 0.94% с Интернет-источником (http://jak.bono.odessa.ua/articles/ddos-ataki-tipi-ataki-i-rivni-...

4.14% Источники из Интернета	167	Страница 76
0.16% Источники из Библиотеки	3	Страница 77

0.03% Цитат

Цитаты	1	Страница 78
Ссылки	1	Страница 78

0.05% Исключений

Некоторые источники исключены автоматически (фильтры исключения: количество найденных слов меньш...

Нет исключенных Интернет-источников

0.05% Исключенного текста из Библиотеки	17	Страница 78

Модификации

Обнаружены модификации текста. Подробная информация доступна в онлайн-отчете.

Замененные символы	10
Подозрительное форматирование	24 страница

ВІДЗИВ

на дипломну роботу другого (магістерського) рівня студента групи ТРм-19-1
Казімірко Андрія Олександровича

«Ідентифікаційна модель хакерської атаки на мережеве устаткування»

Internet забезпечує зловмисникові неймовірні можливості для здійснення несанкціонованого доступу і збій працездатності серверів по всьому світу. За статистикою найбільш поширеними атаками є так звані DdoS –атаки, метою яких є виведення об'єкту атаки з робочого стану, це може стати причиною великих фінансових втрат під час простою або витрат на обладнання для захисту від нього.

Тому завдання виявлення мережевих атак та організація захисту від таких атак є актуальною.

Метою роботи є: побудова ідентифікаційної моделі хакерської атаки на мережеве устаткування».

Об'єктом дослідження є: процеси хакерської атаки на мережеве устаткування.

Предметом дослідження є: ідентифікаційна модель хакерської атаки на мережеве устаткування.

За змістом робота є закінченою та містить достатньо посилань на літературу. Викладення матеріалу є послідовним та логічно правильним. Наведені у роботі алгоритми, коди програм та висновки мають достатнє обґрунтування та детальне пояснення. Мова викладення роботи є технічно грамотною, зрозумілою та не перенасиченою спеціальними термінами.

З точки зору оформлення дипломна робота представлена пояснювальною запискою обсягом 78 сторінок, складається з чотирьох основних розділів та 2-х додатків. Оформлення пояснювальної записки знаходиться на належному рівні.

Серед позитивних сторін дипломної роботи слід відмітити наступне:

1. Побудована удосконалена ідентифікаційна модель атак з використанням віртуалізації машин, дистрибутиву Linux, що дозволило дослідити принципи створення DoS/DDoS атак типу «відмова в обслуговуванні» та дозволяє, в подальшому, визначити можливі шляхи протидії цим атакам.

2. Досліджена можливість правил iptables для захисту від атак типу TCP SYN Flood, UDP, ICMP Flood. Розроблений алгоритм проходження пакетів за правилами iptables.

3. Проведений моніторинг мережі за допомогою аналізатора мережних протоколів Wireshark і на основі аналізу сценаріїв з використанням iptables. Показано, що скрипти iptables та дистрибутив Linux в основному націлені на маршрутизацію та вбудовані пристрої для захисту від DoS / DDoS атак.

4. Результати досліджень апробовані і представлені у вигляді доповіді на науково-практичній інтернет – конференції молодих науковців і студентів «Інтелектуальний потенціал-2020.

Серйозних недоліків робота не містить. Присутні незначні неточності, орфографічні та стилістичні помилки, які не впливають на суть роботи.

Вважаю, що дана робота відповідає загальним вимогам щодо дипломних робіт другого (магістерського) рівня, і заслуговує оцінки “добре”, а Казімірко Андрій Олександрович – присвоєння кваліфікації магістра зі спеціальності 172 – “Телекомунікації та радіотехніка”.

Рецензент:
д.т.н., професор кафедри
телекомунікацій та радіотехніки  Бойко Ю.М.

Завідувачу кафедри телекомунікацій
медійних та інтелектуальних технологій
д.т.н, доценту Підченко С.К.
здобувача вищої освіти
Казімірко Андрія Олександровича,
ФПКТС, 2 курс, ТРм-19-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

10.12.2020 — дата

Казімірко А.О. — підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ ПО КАФЕДРИ Телекомунікацій, медійних та інтелектуальних технологій (ТМІТ)

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: «Ідентифікаційна модель хакерської атаки на мережеве устаткування»

Автор: Казімірко Андрій Олександрович

Спеціальність: 172 Телекомунікації та радіотехніка

Освітня програма: Телекомунікації та радіотехніка

Науковий керівник: Таранчук Алла Анатоліївна

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	**Відповідає**
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягненні. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження: Збіги (4,14%), що виявленні в роботі не є плагіатом. Часткові збіги відповідають частовживаним словосполученням та назвам. Критичних запозичень немає. Дипломна робота допускається до захисту.

10.12.2020 р.

Науковий керівник роботи
к.т.н., доц. Таранчук А.А.

Зав. каф. ТМІТ
д-р.т.н., доц. Підченко С.К.