НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

Факультет інформатики та обчислювальної техніки

Кафедра технічної кібернетики

«На правах рукопису»
УДК 004.056.5

«До захисту допущено»

Завідувач кафедри
_____ І.Р. Пархомей
(підпис)
“___”_____2018 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 126 «Інформаційні системи та технології»

на тему: Аналіз захищеності комп’ютерних мереж на основі моделювання атак по протоколу IPv6

Виконав: студент другого курсу, групи ІК-72мп
(шифр групи)

Заболотній Ігор Володимирович _____ _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник к.т.н., доцент Пасько В.П._____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент в.о. завідувача кафедри інформаційної безпеки
ФТІ КПІ ім. Ігоря Сікорського, канд. фіз.-мат.наук,
доцент Грайворонський М.В. _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки

Кафедра технічної кібернетики

Рівень вищої освіти – другий (магістерський)

Спеціальність 126 «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ І.Р. Пархомей
(підпис)

«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Заболотньому Ігорю Володимировичу
(прізвище, ім'я, по батькові)

1. Тема дисертації «Аналіз захищеності комп'ютерних мереж на основі моделювання атак по протоколу IPv6»,
науковий керівник дисертації к.т.н., доцент Пасько В.П.., _____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «07» листопада 2018 р. № 4112-с

2. Термін подання студентом дисертації _____12 грудня 2018_____

3. Об'єкт дослідження – мережа по протоколу IPv6.

4. Предмет дослідження – дві тестової лабораторії з обладнанням вендорів Cisco та Aruba.

5. Перелік завдань, які потрібно розробити – аналіз проблеми та існуючих рішень; аналіз можливих видів вразливостей протоколу IPv6 та атак на нього; проектування тестової лабораторії, емулювання мережі та проведення атак; аналіз захищеності комп'ютерної мережі; опис метрик безпеки IPv6.

6. Орієнтовний перелік ілюстративного матеріалу – шість плакатів

7. Орієнтовний перелік публікацій – дві публікації

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз предметної області	13.09.2018 р.	
2	Постановка задачі	15.09.2018 р.	
3	Аналіз можливих видів вразливостей мережевого протоколу IPv6	20.09.2018 р.	
4	Аналіз можливих атак по протоколу IPv6	25.09.2018 р.	
5	Проектування тестової лабораторії	15.10.2018 р.	
6	Проведення атак по протоколу IPv6	01.11.2018 р.	
7	Аналіз стартап-проекту	10.11.2018 р.	
8	Висновки	15.11.2018 р.	

Студент _____ Заболотній І.В.
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Пасько В.П.
(підпис) (ініціали, прізвище)

АНОТАЦІЯ

Розглянуто проблему безпеки мережевого протоколу IPv6, показано основні вразливості цього протоколу на обладнанні Cisco та Aruba, їх переваги та недоліки.

Мета дослідження – створення тестової лабораторії та аналіз рівня безпеки протоколу на мережевому обладнанні двох відомих вендорів та визначення рівня безпеки мережі.

Емульовано тестову лабораторію мережі, що дає можливість проведення ряду атак по протоколу IPv6, а саме: розвідка в IPv6 мережі, Smurf атака, стек заголовків розширення, підміна повідомлення RA, підміна повідомлення NA, підміна DHCPv6 сервера та вторгнення в тунель. Тестова лабораторія може бути використана розробниками Cisco та Aruba для усунення вразливостей в мережевому обладнанні. Дозволяє запобігти атакам зловмисника на мережу шляхом додавання системи виявлення несанкціонованого доступу.

Під час тестування виявлено вразливості обладнання обох вендорів під час розвідки в IPv6 мережі, стеках заголовків розширення та вторгненні в тунель. Реалізація стандартних заходів безпеки не завжди дозволяє попередити розглянуті атаки, крім того, може перешкоджати проходженню клієнтського трафіку, що суттєво впливає на якість обслуговування кінцевих користувачів мережі. При аналізі рівня безпеки, сегменти мережі, відповідають середньому рівню безпеки.

Ключові слова: протокол IPv6, вразливості, безпека, атака, комп’ютерна мережа.

Розмір пояснювальної записки – 105 аркушів, містить 34 ілюстрацій, 26 таблиць, 6 додатків.

ABSTRACT

Examined the problem of security of IPv6 network protocol, shown the main vulnerabilities of this protocol on the equipment of Cisco and Aruba, their advantages and disadvantages.

The aim of the study – creating a test laboratory and analyzing the security level of the protocol on the network equipment of the two well-known vendors and determining the security level of the network.

Emulated test lab of the network that allows for a series of IPv6 attacks: intelligence in IPv6 network, Smurf attack, Extension header stack, RA message substitution, NA message substitution, DHCPv6 server substitution and tunnel invasion. This test laboratory can be used by Cisco and Aruba developers for eliminating vulnerabilities in network equipment. It allows to prevent malicious attacks on the network.

During the testing, the vulnerability of both vendors was detected in IPv6 network intelligence. They are intelligence in IPv6 network, Extension header stack and tunnel invasion. Realization of standard security measures does not always allow to prevent the considered attacks, in addition, it can interfere with the passage of client traffic, which significantly affects on the quality of service of end users of the network. When security level was analyzed, network segments correspond to the average security level.

Keywords: IPv6 protocol, vulnerability, security, attack, computer network.

Explanatory note size – 105 pages, contains 34 illustrations, 26 tables, 6 applications.

Пояснювальна записка
до магістерської дисертації

на тему: Аналіз захищеності комп’ютерних мереж на основі моделювання атак по протоколу IPv6

Київ – 2018 року

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IPv4 – (англ. «Internet Protocol version 4») Інтернет протокол версії 4.

IPv6 – (англ. «Internet Protocol version 6») Інтернет протокол версії 6.

MAC – (англ. «Media Access Control») управління доступом до носія.

EUI-64 – (англ. «Extended Unique Identifier») розширений унікальний ідентифікатор.

IANA – (англ. «Internet Assigned Numbers Authority») «Адміністрація адресного простору Інтернет».

RIR – (англ. «Regional Internet Register») регіональний Інтернет реєстратор.

RFC – (англ. «Request for Comments») запит коментарів.

MTU – (англ. «Maximum Transmission Unit») максимальний розмір блоку корисного навантаження.

ICMPv4 – (англ. «Internet Control Message Protocol for the Internet Protocol Version 4») міжмережевий протокол керуючих повідомлень для міжмережевого протоколу версії 4.

ICMPv6 – (англ. «Internet Control Message Protocol for the Internet Protocol Version 6») міжмережевий протокол керуючих повідомлень для міжмережевого протоколу версії 6.

ARP – (англ. «Address Resolution Protocol») протокол визначення адрес.

ND – (англ. «Neighbor Discovery») пошук сусіда.

CAM – (англ. «Content-addressable Memory») асоціативна пам’ять.

TCAM – (англ. «Ternary Content-addressable Memory») трійкова асоціативна пам’ять

NA – (англ. «Neighbor Advertisement») представлення сусіда.

RA – (англ. «Router Advertisement») представлення сусіднього маршрутизатору.

RD – (англ. «Router Discovery») пошук сусіднього маршрутизатора.

NAT – (англ. «Network Address Translation») перетворення мережевих адрес.

ЦП – центральний процесор.

ВСТУП

Процес впровадження мережевого протоколу нового покоління IPv6 відбувається поступово протягом останніх років (Всесвітній запуск якого відбувся 6 червня 2012 року). Але темпи розвитку всесвітньої мережі Інтернет, значно вищі, що стимулює прискорення переходу на IPv6. Однією з перешкод, що необхідно подолати є страх перед невідомим, так як переналаштування обладнання для роботи з новим протоколом може призвести до непередбачуваних наслідків, зокрема при одночасній роботі з IPv4. Окрім цього, для забезпечення надійного розгортання мережевого протоколу IPv6 необхідно акцентувати увагу на проблемах безпеки. При розробці протоколу IPv4 це був далеко не основний критерій, тому він мав багато вразливостей. З огляду на те, що протокол IPv4 використовувався протягом багатьох років, більшість недоліків, що йому притаманні усувались по мірі їх виявлення, і ці практики добре себе зарекомендували. На час впровадження IPv4, мережі були досить невеликі, і це було не так критично, враховуючи масштаби сучасних мереж, подібні помилки можуть призвести до серйозніших наслідків. Ця робота допоможе відповісти на важливе питання, чи справді в протоколі IPv6 реалізовано рівень безпеки, який відповідає сучасним вимогам? Для цього зібрано наявну на сьогоднішній день інформацію про реалізацію безпеки протоколу IPv6, що спирається на досвід, накопичений через використання IPv4. Загрози та виявлені вразливості протоколу розглядаються на обладнанні Cisco та Aruba. Запропоновані заходи щодо підвищення безпеки перевіряються у тестовій лабораторії.

Одним із завдань проектування мережевого протоколу IPv6 було підвищення вимог безпеки в порівнянні зі своїм попередником, протоколом IPv4. Так в основі протоколу IPv6 лежить твердження, що IPSec повинен використовуватися в даному протоколі за замовчуванням. Однак, в більшості практичних випадків, при використанні IPv6, протокол IPSec не використовується взагалі. До того ж в нових протоколах, які лежать в основі

стека протоколів IPv6, знайдено безліч вразливостей. З метою усунення таких вразливостей були розроблені спеціальні механізми безпеки:

- протокол CGA (англ. "*Cryptographic generated address*") [1], який дозволяє генерувати IPv6 адресу на основі криптографічних алгоритмів і дозволяє запобігти підміну IPv6 адрес в мережі;
- протокол SEND (англ. "*Secure Neighbor Discovery protocol*") [2], який дозволяє убезпечити стандартний NDP протокол шляхом застосування криптографії.

Слід зазначити, що початкові версії вищенаведених механізмів безпеки в IPv6 мережі були розроблені в 2005 році. В останні роки в зв'язку зі зростаючим попитом на нову версію IP протоколу пропонуються удосконалення і доопрацювання даних механізмів. Основні принципи роботи протоколу SEND, а також CGA і їх доопрацювання більш детально розглядаються в роботі.

Крім CGA і SEND розроблені і інші механізми забезпечення безпеки, зокрема:

- протокол SAVI (англ. "*Source Address Validation Improvement*"), який дозволяє гарантувати валідність IP адрес в межах локальної мережі;
- група механізмів забезпечення First-Hop безпеки: IPv6 RA Guard, IPv6 Snooping, DHCPv6 Guard, IPv6 Source Guard і Prefix Guard, IPv6 Destination Guard.

Метою роботи є аналіз існуючих механізмів забезпечення безпеки стека протоколів IPv6, а також проблем у даній області, невирішених в даний час.

Предмет дослідження – безпека мережевого протоколу IPv6.

Об’єкт дослідження – протокол IPv6.

РОЗДІЛ 1. МЕРЕЖЕВИЙ ПРОТОКОЛ IPV6

1.1. Адресація

Початок 2012 року було ознаменовано тривожним, на перший, погляд повідомленням про повне вичерпання адресного Інтернет простору, що відповідає вимогам протоколу IPv4. Ще в кінці 90-х років минулого століття експерти були впевнені, що адресації цього протоколу має вистачити, принаймні, ще років на 30. Але такого стрімкого розвитку мережевих ресурсів припустити не міг ніхто, і почалося впровадження нового джерела розвитку мережевої інфраструктури. Цим джерелом послужив протокол IPv6, розроблений ще в далекі 80-ті роки двадцятого століття. Розробки протоколу були засновані на пошуку альтернативного способу протоколювання Інтернет простору, але ніхто не підозрював, що їх впровадження знадобиться в настільки близькому майбутньому.

По суті, протокол IP шостої версії є повноцінною заміною IPv4, що належить до сімейства протоколів TCP / IP. У новій версії усунуто велику кількість помилок і недоробок з якими зустрічалися користувачі IPv4. Збільшення адресного діапазону, за рахунок 128 бітного формату, стало ідеальним рішенням для збільшення Інтернет простору. Для наочності варто уточнити, що якщо адреси з підтримкою IPv4 виглядали «*000.111.222.333*», то IPv6 виглядають так: «*0000: 1111: 2222: 3333: 4444: 5555: 6666: 7777*».

Після закінчення IPv4 діапазону, паралельне використання протоколів, дасть можливість повного впровадження протоколу, за допомогою поступового збільшення трафіку в IPv6 мережах. Але при цьому, повне виведення IPv4 діапазону буде доступне не скоро, адже існує величезна кількість пристроїв, що не підтримують інноваційну технологію.

Всі пристрої, що підключаються до мережі, спочатку отримують унікальні числові ідентифікатори, звані IP-адресами. Хоча ці числові послідовності і є основою всіх мережевих підключень, їх використання в повсякденному житті велика рідкість. Дякуючи системі доменних імен (DNS),

пересічному користувачеві досить ввести текстовий запит в адресний рядок. А введення нового протоколу адресного простору, забезпечило збільшення унікалізації IP-адрес для нескінченної кількості мережевих пристроїв. Ця унікалізація стала доступною завдяки збільшенню довжини самої адреси. І тепер замість 32 біт, також широко використовуються 128-бітові комбінації, що дозволяє створити до $34 * 10^{38}$ адрес нового рівня, але це лише одне з нововведень.

За допомогою цього протоколу, у кожного підключеного вузла є можливість відправки запитів будь-яким групам серверів, що дає можливість визначення їх місцезнаходження для вибору оптимального варіанту подальшої взаємодії.

Зміни не пройшли повз формати заголовків для пакетів даних. Деякі поля, які існували в IPv4, для нового протоколу стали неактуальними, а деякі були істотно модифіковані. Але з'явилися і нові поля, що відкрили доступ до:

- визначення пріоритетності пакетів даних для стартового хосту;
- забезпечення потокової обробки.

Оптимізація заголовків дала можливість скоротити число полів до восьми. Це дозволило значно прискорити обмін пакетами даних між вузлами. Але при необхідності, є можливість додавання нових полів.

Крім того, впровадження IPv6 дозволило реалізувати практично всі можливості шифрування даних з підтримкою сервісу якісного обслуговування, що вкрай важливо для потокового мультимедійного мовлення.

До теперішнього моменту, практичне впровадження і використання нової версії протоколу здатне вирішити відразу кілька завдань одночасно.

Повноцінне адресне забезпечення великих мереж

Для нині існуючих вузлів з доступом в Інтернет є ряд обмежень по резервації загальнодоступного простору IPv4-адрес. Навіть при використанні простору приватних адрес в інтрамережі (приватній мережі) виникає дефіцит адресації. За допомогою впровадження IPv6 із наступною активацією префіксів

унікальних локальних адрес, даний простір можна буде розширити і застосувати до всіх мережевих ресурсів організацій.

Використання додатків і служб з винятковою підтримкою IPv6

Останні версії операційних систем сімейства Windows містять значний пакет компонентів, розрахованих на роботу тільки з IPv6. Тому розвиток приватної інфраструктури IPv6 дасть можливість повноцінного використання всіх ресурсів операційної системи.

У регіонах з обмеженням IPv4 адресації багато організацій здійснюють підключення з використанням IPv6. При цьому існує необхідність перетворення протоколу для обміну даними з ресурсами з підтримкою IPv4. Паралельне використання обох версій вирішує цю проблему.

Класифікація IPv6 адрес

Як відомо, минула версія протоколу підтримувала два варіанти для користувача IP-адрес:

- статична адреса, яка була незмінним ідентифікатором;
- динамічна, змінювалася при кожному новому підключенні до мережі.

У шостій версії протоколу було вирішено залишити тільки варіант статики. Таке рішення було обумовлено тим, що, в перспективі кожному пристрою в підмережі будь-якого рівня буде доступний свій унікальний ідентифікатор (IP-адреса).

Всі статичні адреси в свою чергу розділені на три категорії:

Unicast. Стандартні адреси з одиничною прив'язкою до мережевого інтерфейсу.

Anycast. Адреси, передбачені для груп мережевих оболонок, і призначаються тільки для маршрутизаторів. Такі адреси розраховані на створення внутрішніх мережевих груп з кількох комп'ютерів.

Multicast. Адреси для групового обміну даними, в основному виділяються регіональним серверам.

Відповідно до цієї класифікації адрес і відбувається їх розподіл.

Виділення, призначення та отримання IPv6-адрес

Згідно з новою політикою делегування для нових IP, присвоєння однієї унікальної адреси є тільки для одного ПК в мережі. При цьому є обов'язковою реєстрація в протокольній базі даних. Основною концепцією в розподілі нових адрес є максимальне використання принципів ієрархічної системи. Згідно з цим принципом надмірний приріст таблиць маршрутизації повинен бути нейтралізований.

Приклад типової ієрархічної схеми для IP-адрес: компанія, виконує розподіл адресного потоку, здійснює передачу кейса IP-адрес в своє регіональне представництво (до таких відносяться інтернет-реєстратури типу RIR). Після чого, розподіл адрес відбувається між компаніями країн регіону, які представляють RIR. Далі блоки передаються інтернет-провайдерам, які займаються розподілом адрес по кінцевих користувачах.

Для організацій, які є місцевими представниками, які претендують на отримання адресних блоків, передбачена вимога про регіональні плани. Такі плани враховують роздачу адрес протягом двох років і подаються в регіональну реєстратуру. І якщо всі вимоги дотримані, провайдер отримує ліцензію на надання послуг.

Для індивідуального розподілу IPv6 адрес, відповідно до їх структури, була визначена наступна схема:

- виділення глобальних префіксів (48 бітних блоків (/ 48)) для провайдерів;
- провайдер виділяє 16 бітні блоки (/ 16) для створення внутрішніх підмереж;
- внутрішніми підмережами провайдера виділяються призначені для користувача 64 бітні адреси (/ 64).

У теорії, такий обсяг адресного простору дозволяє підключити до користувальницької підмережі 18 x 10^{18} пристроїв. З одного боку такі показники здаються надмірними. Але якщо розвиток мережевих ресурсів буде мати таку динаміку і в майбутньому, це дозволить істотно спростити автоматичне конфігурування множинних підключень.

Звичайно, чудово якщо основний провайдер надає послугу підключення протоколу IPv6 в базовому пакеті. По-перше, це спрощує налаштування операційної системи. По-друге, гарантує мінімальне пінгування. І саме це банальна надійність.

Але є і свої нюанси. Перед початком установки необхідно переконатися, що основна точка доступу (маршрутизатор) підтримує новий формат протоколювання. В іншому випадку доведеться зайнятися його перепрошивкою. Але якщо ж обладнання повністю підтримує нову технологію, то для коректної роботи потрібно тільки його безпосереднє налаштування.

Практично всі провайдери надають IPv6 в мережах Ethernet-DHCPv6, який є свого роду коробочним рішенням для роутерів. Тому установка всіх необхідних оновлень і налаштувань відбувається в автоматичному режимі.

1.2. Структура пакету

В IPv6 існують механізми для виявлення хоста. Хости використовують механізм виявлення, в основному, як дослідницький інструмент, але вони також відповідають на запити, інформуючи про свою власну конфігурацію. При ініціалізації хост може відправити запит маршрутизатора для визначення способу конфігурації власної адреси: або з можливістю зміни власної адреси під час роботи, або без такої можливості. Автоконфігурування з можливістю динамічного призначення адреси використовується при видачі адреси хосту за допомогою служби *DHCP*.

1.2.1. Формат заголовка IPv6 і механізми маршрутизації

Інформація про адреси становить лише частину заголовка кожного пакета IPv6 (табл.1.1). Решта інформації необхідна для ефективної оцінки і обробки пакета. Крім основного заголовка пакет IPv6 може містити один або кілька додаткових заголовків, в яких може міститися інформація про маршрутизації, фрагментації, наступні переходи.

Таблиця 1.1. Поля заголовка пакета IPv6

Поле	Довжина	Характеристика
Версія (Version)	4 біта	Значення «0110» вказує на версію 6
Клас трафіку (Traffic Class)	8 біт	Використовується при ідентифікації класу або пріоритету трафіку, для того, щоб пакети могли бути перенаправлені з іншими пріоритетами для забезпечення QoS
Мітка потоку (Flow Label)	20 біт	Пакети, які відповідають певному класу потоку, позначаються для визначення приналежності цього потоку
Довжина корисного навантаження (Payload Length)	16 біт	Довжина в октетах решти пакета, що включає в себе додаткові заголовки
Наступний заголовок (Next Header)	8 біт	Визначає тип заголовка, наступного відразу після заголовка IPv6. Використовуються ті ж значення, що і в полі протоколу IPv4 (RFC 1700)
Межа переходів (Hop Limit)	8 біт	Число зв'язків, через які пакет може бути переданий поки не буде відкинутий. Кожне пересилання зменшує значення цього поля на 1
Адреса відправника (Source Address)	128 біт	Адреса вузла відправника
Адреса призначення (Destination Address)	128 біт	Адреса вузла призначення, яка може бути або остаточною одержувачем або проміжним вузлом

Ця інформація визначається відправником. Додаткові заголовки не обробляються вузлами на маршруті при передачі пакета, вони обробляються тільки вузлом призначення (це може бути вузол остаточного призначення, або вузол проміжного призначення). Довжина додаткового заголовка кратна 8 октетам, що дозволяє вирівняти довжину пакета і не обробляти ці заголовки усіма вузлами при передачі. Кількість додаткових заголовків може бути різною: можуть бути присутніми або всі заголовки, або тільки деякі з них, або вони взагалі можуть бути відсутніми.

Повна специфікація IPv6 включає наступні заголовки (в порядку проходження в датаграму):

- *IPv6 Header* (заголовок дейтаграми)
- *Hop-by-Hop Options Header* (заголовок опцій)
- *Destination Options Header* (заголовок опцій місця призначення)
- *Routing Header* (заголовок маршрутизації)

- *Fragment Header* (заголовок фрагментації)
- *Authentication Header* (заголовок аутентифікації)
- *Encapsulating Security Payload Header* (заголовок безпечних вкладень)
- *Destination Options Header* (заголовок опцій місця призначення)
- Заголовок протоколу верхнього рівня (наприклад, TCP, UDP тощо).

Authentication Header (заголовок аутентифікації)

Цей заголовок забезпечує захист переданих даних завдяки шифруванню на основі криптографічного ключа із застосуванням асиметричних методів кодування. Аутентифікація є механізмом, який дозволяє забезпечити аутентифікацію відправника на рівні IP-протоколу як для IPv4, так і для IPv6. Також даний заголовок допомагає забезпечити перевірку цілісності даних. Цей механізм безпеки більш ефективний ніж раніше використовуваний в IPv4.

Даний метод застосовується тільки для вирішення конкретних завдань безпеки і не може бути використаний як унікальний засіб.

Даний механізм забезпечує цілісність переданих даних шляхом додавання до IP-датаграми інформації аутентифікації. Ця інформація визначається вмістом всіх полів пакету (як заголовків так і призначених для користувача даних). Значення полів і опцій, які змінюються в процесі передачі датаграми, при обчисленні інформації аутентифікації приймаються рівними 0. Інформація аутентифікації визначається відправником датаграми, і перевіряється тільки одержувачем даного пакета.

Оскільки проміжні хости не контролюють безпеку передачі, то наявність такого заголовка не позначається на швидкості обробки пакета. Також наявність заголовка аутентифікації ні до чого не зобов'язує вже сформовану інфраструктуру мережі Інтернет. Дані, необхідні для забезпечення безпеки пакетів, розміщені в окремому заголовку. Якщо система не працює з пакетами, в яких присутній заголовок аутентифікації, то вона просто може їх ігнорувати.

1.3. Повідомлення про вразливості

Для того, щоб зашифрувати дані пакета, застосовується криптографічний алгоритм з використанням несиметричного секретного ключа. Структура пакета так побудована, що алгоритм роботи з секретним ключем не інтегрований в механізм аутентифікації IP.

Це дозволяє використовувати різні механізми генерації секретного ключа без зміни основних принципів IP-безпеки. Неефективно передавати ключ і безліч параметрів алгоритму шифрування для кожного пакета. Виходом з цієї ситуації є те, що механізм генерації ключа будує спеціальну логічну таблицю відповідностей SA (*Security Association*). Ця таблиця зберігає параметри для кожної шифрованої пари (ключ-алгоритм). Механізм безпеки IP повинен прочитати запис цієї таблиці, щоб визначити алгоритм і ключ, використовувані для аутентифікації кожної датаграми.

При формуванні IP-пакета в першу чергу потрібно побудувати асоціацію в таблиці відповідностей SA для даної датаграми. Вибір асоціації в таблиці відповідностей здійснюється на основі ідентифікатора відправника та адреси одержувача пакета. Асоціація, яка буде обрана, визначить алгоритм, тип алгоритму, ключ і інші параметри шифрування.

Сполучною ланкою між механізмом побудови ключа і вибором алгоритму шифрування є індекс відповідності параметрів шифрування SPI (*Security Parameters Index*). Цей індекс є своєрідним кодом в таблиці асоціацій SA (*Security Association*). Цей індекс передується в заголовку аутентифікації пакета. Одержувач, при надходженні пакета, на основі адреси призначення і індексу SPI, який він витягує з заголовка аутентифікації в пакеті, визначає запис в таблиці асоціацій SA. Потім одержувач перевіряє цілісність даних і дешифрує їх.

Next Header (8 біт) – це поле ідентифікує тип наступного заголовка.

Length (8 біт) – додаткова довжина. Це поле містить довжину даних аутентифікації в 32-бітних одиницях. Мінімальне значення цього поля 0. Це означає, що шифрування відсутнє (нульовий алгоритм).

Reserved (8 біт) – це поле не використовується.

Security Paramet ers Index (SPI) (32 біта) – поле індексу параметра. Це поле містить псевдовипадкове число, яке визначає індекс відповідності в таблиці асоціацій SA (таблиця визначає тип алгоритму, параметри шифрування і інше). Значення, рівне 0, використовується при відсутності відповідностей, значення яких від 1 до 255 зарезервовані.

Authentication Data – дані аутентифікації. Вони є результатом роботи алгоритму шифрування на основі вмісту всієї датаграми. Дані аутентифікації зберігають свій формат для певної пари (SPI і адреса одержувача).

Фахівці, аналізуючи розвиток мережі Інтернет, роблять висновок, що перехід на мережі IPv6 не буде миттєвим. Довгий час будуть існувати як мережі IPv4, так і мережі IPv6. Перший час мережі IPv6 будуть нагадувати острови в океані IPv4. Спочатку вузли, що реалізують IPv6, не надаватимуть всіх необхідних сервісів. Тому є необхідні вимоги для вузлів IPv6: можливість взаємодії з вузлами IPv4; можливість передачі пакетів IPv6 через існуючу інфраструктуру IPv4.

З вище сказаного випливає, що необхідні механізми, які забезпечуватимуть співіснування мереж IPv4 і IPv6. Взаємодія систем, що використовують різні стеки протоколів, зазвичай здійснюється за допомогою застосування таких методів:

- трансляція;
- інкапсуляція (тунелювання);
- мультиплексування.

Трансляція забезпечує узгодження стеків протоколів шляхом перетворення форматів повідомлень. Також при трансляції здійснюється відображення адрес вузлів і мереж, які різним чином трактуються в цих протоколах. Як транслятор елемента можуть виступати: програмний або

апаратний шлюз, міст, комутатор, маршрутизатор і ін. Трансльований елемент розміщується між взаємодіючими мережами і служить посередником при передачі повідомлень з мережі, що використовує один протокол в мережу, яка використовує інший протокол. Трансльований елемент займається перетворенням форматів повідомлень і відображенням адрес.

Ущільнення каналів або мультиплексування має на увазі, що в мережеве обладнання або в операційні системи серверів і робочих станцій вбудовуються кілька стеків протоколів. На вузлах мережі встановлюються кілька стеків комунікаційних протоколів – за кількістю мереж, які використовують різні мережеві протоколи. Необхідно, щоб запит від прикладного процесу правильно оброблявся, проходив через певний стек. Для цього застосовується спеціальний програмний елемент – мультиплексор протоколів або менеджер протоколів. Цей програмний елемент визначає, в яку мережу направлено запит від клієнта.

Інкапсуляція (тунелювання) є одним методом, який допомагає при взаємодії мереж, які використовують різні мережеві протоколи. Інкапсуляція застосовується, коли необхідно здійснити взаємодію двох мереж з однією технологією через транзитну мережу, в якій використовується інша технологія.

В процесі інкапсуляції беруть участь три типи протоколів:

- протокол інкапсуляції;
- транспортуючий протокол;
- несучий протокол.

Транспортуючим є протокол об'єднання мереж, що несе протокол транзитної мережі. Пакети транспортуючого протоколу поміщаються в поле даних і несуть протокол за допомогою протоколу інкапсуляції.

У змішаних мережах IPv4-IPv6 найчастіше використовується мультиплексування і інкапсуляція (тунелювання). Ці методи дозволяють вузлам мережі, що використовує протокол IPv6, обмінюватися з вузлами іншої IPv6 мережі через мережу, в якій застосовується протокол IPv4. Для того, щоб вузли, які підтримують тільки протокол IPv6, могли звертатися до ресурсів мережі IPv4, необхідна наявність додаткових систем: шлюзів транспортного і

прикладного рівня, трансляторів протоколів тощо. Зараз розробляються такі механізми, які дозволяли б протоколу IPv6 без перешкод працювати поверх мереж, які підтримують тільки протокол IPv4. Але в майбутньому обов'язково будуть потрібні механізми, які дозволять передавати IPv4 через мережі, які підтримують тільки протокол IPv6, так як до певного моменту він стане основним мережевим протоколом.

Механізм мультиплексування має на увазі одночасну підтримку вузлів двох стеків протоколів. Для здійснення цього необхідно, щоб у кожного вузла було дві адреси: IPv4 і IPv6. Ці адреси можуть бути ніяк не пов'язані одна з одною. Адреси IPv4 повинні бути унікальними. До моменту вичерпання адресного простору IPv4 процес переходу на IPv6 повинен зайти досить далеко, щоб нові вузли могли отримати всі необхідні послуги, використовуючи виключно засоби протоколу IPv6.

Для реалізації одночасної підтримки двох стеків протоколів потрібні відповідні інфраструктурні сервіси. Наприклад, служба DNS повинні видавати як записи типу « A » з 32-бітовим IP-адресою, так і записи типу « AAAA » с 128 бітовим адресою. Від результату DNS-запиту може залежати те, яким стеком скористатися.

Механізм тунелювання давно використовується в IPv4 для транспортування не IP-пакетів. У випадку з IPv6 застосовується механізм інкапсуляції, який відображений на Рисунок 1.1. Пакет IPv6 поміщається в поле даних пакета IPv4, потім передається звичайною мережею IPv4. Наприкінці пакет IPv6 витягується з поля даних пакета IPv4 і обробляється звичайним чином. Він або транспортується далі (це відбувається вже по IPv6-мережі), або використовується одержувачем. Несучим протоколом є IPv4. Протокол IPv4 грає роль протоколу канального рівня з точки зору IPv6, тому поле Hop Limit в пакеті IPv6 буде зменшено тільки на одиницю (якщо буде потрібно подальше перенаправлення пакета). У загальному випадку повний маршрут пакета IPv6 може включати кілька тунелів через транзитні мережі IPv4.

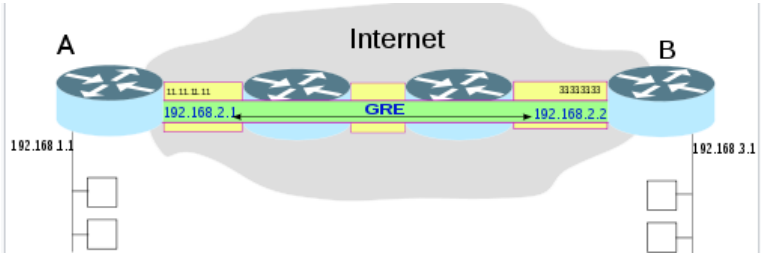

Рисунок 1.1. Механізм інкапсуляції

Підтримка механізму тунелювання розширює функціональні можливості вузлів, які є кінцевими точками тунелю. Це накладає на них додаткові зобов'язання. Приймаючий вузол повинен зрозуміти, що в полі даних отриманого ним пакета IPv4 знаходиться пакет IPv6. Для цього перевіряється поле «Протокол» в заголовку пакета IPv4. Значення цього поля в даному випадку має дорівнювати десятковому числу 41.

Значення максимального розміру пакета (MTU), який може бути відправлений через інтерфейс IPv6 1280 байт. Для того, щоб уникнути зайвої фрагментації, інкапсулююча система повинна використовувати таке значення для MTU пакета IPv6, щоб він разом з заголовком помістився в авторизованному значенні MTU для пакета IPv4. Якщо розмір пересилаючого IPv6 пакета не дозволяє розмістити його цілком в поле даних пакета IPv4, що інкапсулює, вузол може відправити вузлу джерела трафіку IPv6 керуюче повідомлення *ICMPv6*.

При прийманні пакета IPv4, який несе в поле даних пакет IPv6, система повинна застосувати до нього стандартні методи фільтрації трафіку по вихідній адресі: пакет відкидається, якщо це особлива адреса – для широкомовної або під LGPL. Також пакет відкидається, якщо ця вихідна адреса дорівнює 0.0.0.0 або 127.x.x.x. Потім відкидається інкапсулюючий заголовок пакета IPv4, і методи фільтрації повинні бути застосовані вже до пакету IPv6. І у IPv6 є особливі адреси. До них відносяться адреси під LGPL, невизначені адреси, особливі адреси, отримані відображенням IPv4 на IPv6, а також адреси зворотної петлі. Надалі пакет передається стеку IPv6 і обробляється як звичайний пакет IPv6. Вузол не повинен здійснювати подальшу маршрутизацію пакета IPv6, якщо така можливість не передбачена конфігурацією для IPv4

адреси, з якого пакет прийшов. Таким чином, маршрутизація даного пакета IPv6 може здійснюватися, якщо вузол налаштований, як кінцева точка тунелю, початковою точкою якого є IPv4-адреса вузла-відправника.

Оскільки початкова точка тунелю, що здійснює інкапсуляцію пакетів IPv6 в пакети IPv4 – це вузол-відправник по відношенню до пакету IPv4, то ця точка може отримати повідомлення про помилку, що виникла при передачі пакета IPv4 по мережі. У деяких випадках, в залежності від типу повідомлення ICMP, може виникнути необхідність передачі повідомлення про помилку вузлу-відправнику пакета IPv6. Наприклад, якщо ICMP-повідомлення повідомляє про перевищення максимального розміру пакета, то система повинна себе вести у відповідності зі специфікацією для визначення максимального розміру блоку даних IPv4, які можуть бути передані по даному маршруту без фрагментації. Таким чином, необхідно зареєструвати припустиме максимальне значення блоку даних IPv4 і прийняти рішення про те, чи потрібно відправляти керуюче повідомлення ICMPv6 вузлу-джерелу трафіку IPv6.

Обробка інших типів повідомлень IPv4 залежить від того, яка частина повідомлення, яке викликало помилку, що міститься в ICMP-повідомленні. Залежно від реалізації ICMP, повідомлення цього протоколу крім зовнішнього заголовка IPv4 може містити 8 і більше байт поля даних пакета IPv4, до якого відноситься це керуюче повідомлення. Якщо цих даних досить для реконструкції заголовка IPv6, то генерується повідомлення ICMPv6 і відправляється вузлу-джерелу IPv6.

Можна виділити чотири види тунелів:

- хост - хост (рис. 1.2);
- маршрутизатор - хост (рис.1.3);
- хост - маршрутизатор (рис.1.4);
- маршрутизатор - маршрутизатор (рис.1.5).

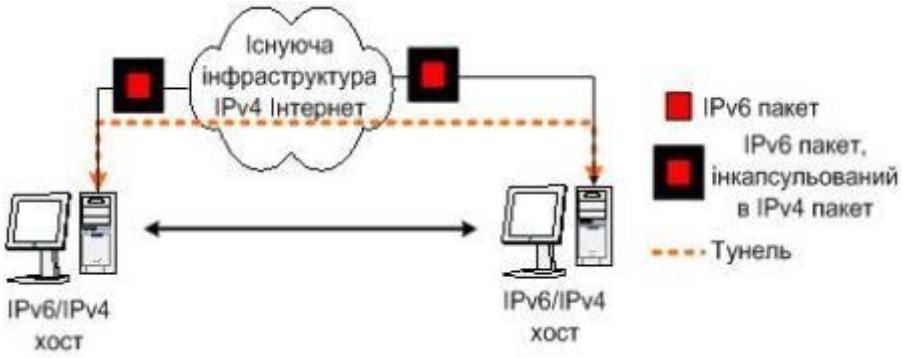

Рисунок 1.2. Тунель виду хост - хост

Рисунок 1.3. Тунель виду маршрутизатор - хост

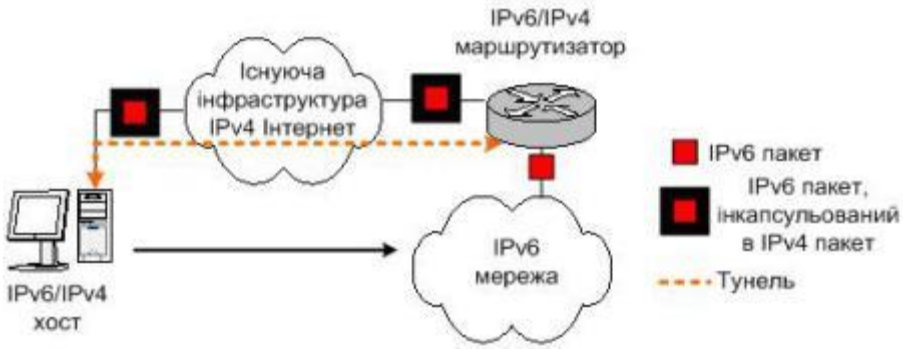

Рисунок 1.4. Тунель виду хост - маршрутизатор

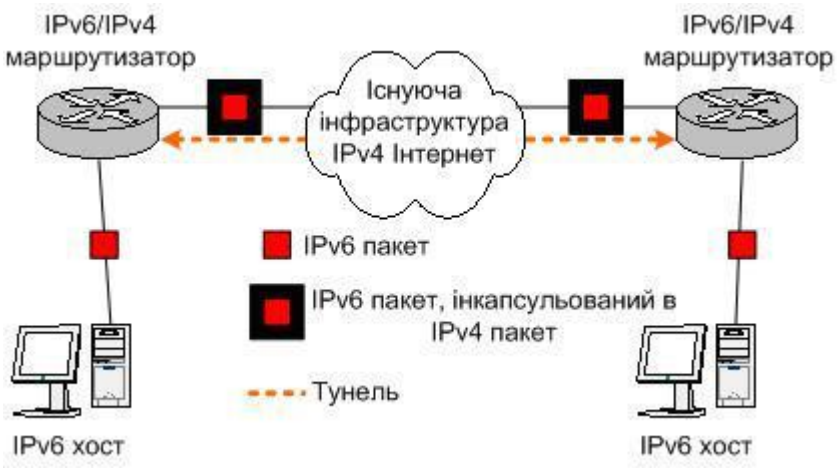

Рисунок1.5. Тунель виду маршрутизатор – маршрутизатор

У двох перших випадках кінцева точка тунелю збігається з кінцевою точкою маршруту пакета IPv6. Адреса кінця тунелю повинна автоматично обчислюватися як функція адреси цільового хоста. Прийнято говорити, що при цьому виробляється автоматичне тунелювання. Для того, щоб автоматичне тунелювання було можливим, необхідно, щоб IPv6-адреси були IPv4-сумісними. По суті, вони повинні виходити з адрес IPv4 приписуванням зліва 96 нульових біт.

Коли кінцева точка тунелю (маршрутизатор) не вирахував за адресою цільового хоста, то доводиться використовувати заздалегідь сконфігуроване тунелювання. При цьому параметри тунелю задаються маршрутною таблицею в інкапсулюючому вузлі. Цей підхід застосовується, коли цільові адреси не є IPv4-сумісним. В такому випадку відправнику необхідно знати IPv4-адресу маршрутизатора з подвійним стеком, який здатний організувати доставку IPv6-пакета.

Обидва кінці тунелю (і автоматичного, і сконфігурованого) повинні володіти IPv4-сумісними адресами.

Можливі три ситуації в залежності від того, якою є кінцева адреса:

- кінцева адреса є адресою протоколу IPv6;
- кінцева адреса є IPv4-адресою;
- кінцева адреса є IPv6-адресою, сумісною з IPv4.

Протокол IPv6 (Internet Protocol version 6) – це новітній варіант інтернет протоколу (IP), зроблений з метою вирішення завдань, які не могла вирішити попередня версія (IPv4) при її застосуванні в інтернеті: це використання довжини адреси 128 біт замість 32, тобто, IPv6 в 4 рази довше.

У наш період часу IPv6 динамічно застосовується у великій кількості сіток по всьому світу, проте поки що ще не отримав настільки великого поширення в Інтернеті, як IPv4.

Інтернет протокол IPv6 відмінно справляється з головними встановленими завданнями. Коли закінчиться адресний простір в IPv4, 2 стека протоколів – IPv6 і IPv4 – стануть застосовуватися паралельно, з поступовим зростанням частки трафіку IPv6 в порівнянні з IPv4.

Особливості IPv6:

- протокол IPv6 містить довжину 128 біт, що дозволяє вирішити основне питання дефіциту ip адрес в інтернеті;
- протокол IPv6 згідно з порівняним IPv4 містить найбільш спрощений заголовок пакета. Тому роутери можуть швидше піддавати обробці пакети і таким чином збільшувати ефективність;
- удосконалена підтримка необов'язкових параметрів. Такі зміни насправді стали суттєвими, так як в новому заголовку необхідно, щоб спочатку поля стали факультативними;
- завищена ступінь захищеності, аутентифікація і конфіденційність є головними особливостями інноваційного IP- протоколу;
- пріоритет потрібен щоб робити різницю в пакетах з усякими умовами до доставки в теперішньому часі;
- мітка потоку використовується з метою конструкції між відправником і отримувачем псевдо-компонування з обумовленими особливостями і умовами. Довжина корисного навантаження інформує, скільки байт направляється за 40-байтовим заголовком;

– наступний заголовок інформує, який з доданих заголовків йде за ключовим;
– максимальне число транзитних вузлів – подобу часу існування (TTL). Допоміжні заголовки містять:
– параметри маршрутизації – всілякі відомості для роутерів;
– параметри отримання – різні дані для одержувача;
– маршрутизація – неповний перелік тимчасових маршрутизаторів в дорозі пакета;
– фрагментація – координування фрагментами дейтаграм;
– аутентифікація – контроль дійсності відправника;
– шифровані дані – відомості про зашифрований вміст.

В інтернет протоколі IPv6 присутні три типи адрес:

– *unicast* – Особистий номер індивідуального інтерфейсу. Пакет, посланий по "Юнікаст" адресі, доставляється інтерфейсу, зорієнтованому в адресі (одне джерело, один одержувач);
– *anycast* – Особистий номер набору інтерфейсів (що відносяться до різних вузлів). Пакет передається по "енікаст" адресі, потім доставляється одному з інтерфейсів, який вказаний в адресі (довколишній, відповідно до міри, яка визначена протоколом маршрутизації). Anycast має одне джерело, кілька можливих одержувачів, але відсилається тільки одному з них;
– *multicast* – Особистий номер набору інтерфейсів (як правило відносяться різним вузлам). Пакет надсилається "мультикаст"-адресою, потім приходить в усі інтерфейси, встановлені цією адресою. Multicast – одне джерело, кілька одержувачів.

У протоколі немає Broadcast (широкомовних) адрес. Їх функції виконують multicast-адреси. А всі нулі і всі одиниці в протоколі IPv6 є можливими кодами для всіх полів, якщо тільки не присутній виняток.

Якщо говорити про моделі адресації то, кожен інтерфейс належить тільки одному вузлу, Юнікаст адреса інтерфейсу може ідентифікувати вузол. Таким чином адреси всіх видів асоціюються з інтерфейсами, а не вузлами.

Юнікаст адреса кореспондується тільки з одним інтерфейсом. Одному інтерфейсу можуть відповідати чимало адрес IPv6 різноманітного виду, тобто *Unicast, Multicast, Anycast*. Але є два винятки з цього принципу:

- Одиночна адреса може підписуватися кільком фізичним інтерфейсам, якщо додаток розглядає ці кілька інтерфейсів як єдине ціле при поданні його на рівні Інтернет.
- Маршрутизатори можуть мати ненумеровані інтерфейси для з'єднань точка-точка, щоб виключити необхідність вручну конфігурувати і оголошувати (advertise) адреси. Адреси не потрібні для з'єднань точка-точка маршрутизаторів, якщо ці інтерфейси не використовуються в якості точки відправлення або призначення при посилці IPv6 дейтаграм. Маршрутизація тут здійснюється за схемою близькою до використовуваної протоколом CIDR в IPv4 [15].

Аналогічно протоколу IP версії 4, дозволено зазначити дві частини: саму мережу і хост. Кілька бітів зліва (яка саме кількість власне залежить від префікса) – це мережа, інші справа.

Визначають пристрій всередині мережі. За зберігання даних про вузол відповідає ідентифікатор інтерфейсу (interface id). На відміну від протоколу IPv4, в новій версії не використовуються мережеві маски підмережі, тому що вони вийшли б дуже довгими і замість цього застосовується префікс. Префікс записується так само через слеш (/) після адреси. Наприклад префікс / 64 позначає, що з IP адреси довжиною 128 біт, мережа це перші 64, а решта частина–це хост (в цьому прикладі другі 64). Таким чином префікс означає скільки біт в адресі є під зберігання даних про мережу.

Саму ір адресу записують 16 розрядному вигляді – адже так коротше і зручніше (а не в десятковому як в IPv4). Адреса розбивається на групи по 16 біт (іменують як хекстети) і кожна зв'язка є чотирма 16-ми цифрами, яка

відділяється двокрапкою (знак :) один від одного. Зробивши висновок, можна сказати, що адреса складається з 8 хекстетів: ([8 хекстетів] * [16 біт в хекстеті] = [128 біт] – загальна довжина адреси).

Ось як виглядає IPv6 адреса: *2001: 0DD8: AB10: 0001: 0000: 0000: 0000: 00AB.*

Якщо говорити про безпеку то, в IPv6 вбудований заголовок аутентифікації. Він виконує функцію захист переданих даних за допомогою шифрування із застосуванням асиметричних методів кодування на основі криптографічного ключа. Тема передбачає собою механізм, який дозволяє забезпечити аутентифікацію відправника на рівні IP-протоколу як для четвертої версії, так і для шостої. Крім того, може допомогти гарантувати перевірку цілісності даних. Дана система захищеності найбільш ефективна в порівнянні з IPv4. Використовується тільки щоб вирішити коло певних завдань безпеки, і не дозволяється використання як унікального засобу.

Опис методу аналізу

Для реалізації порівняльного аналізу продуктивності версій протоколу IP була реалізована мережа *100BaseT* з 2-х сучасних персональних комп'ютерів під керуванням ОС Linux Mint 17, підключених один до одного за допомогою кручений пари 5-ї категорії. Довжина мережі 1 метр. Побудована схема відображає мережу рівня доступу. Схема досліджуваної мережі відображена на рис. 1.6.

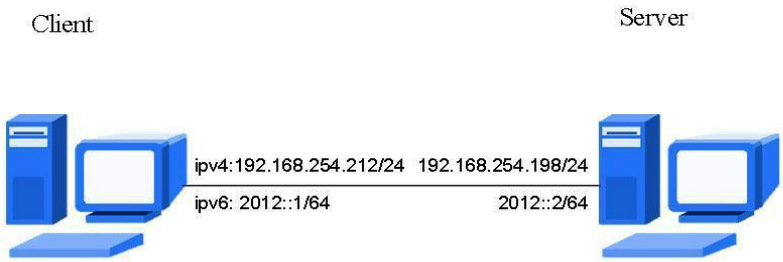

Рисунок 1.6. Схема досліджуваної мережі

Як програмне забезпечення для визначення основних показників продуктивності мережі будемо використовувати програми *ping* і *iperf* версії

2.0.2. Перед проведенням досліджень дамо тестовим комп'ютерам адреси IPv4 і IPv6 на одному фізичному інтерфейсі.

На комп'ютері Client введемо:

ifconfig eth0 192.168.254.212/24
ifconfig eth0 add 2012 :: 1/64 up

На комп'ютері Server:

ifconfig eth0 192.168.254.198/24
ifconfig eth0 add 2012 :: 2/64 up

Продуктивність мережі будемо оцінювати за такими параметрами:

- швидкість передачі даних;
- затримка передачі даних;
- час відгуку.

Швидкість передачі даних

Метою вимірювання швидкості передачі даних будемо використовувати програму iperf, яка працює по клієнт-серверній архітектурі. Клієнт генерує різні типи трафіку (в нашому випадку TCP і UDP) і посилає на сервер.

Для отримання швидкостей передачі даних TCP / IPv4 на комп'ютері "Server" запустимо iperf з параметром "s". На комп'ютері "Client" запустимо

iperf -c 192.168.254.198 -M 1500 -f K -t 10 -i 10

Для отримання швидкостей передачі даних TCP / IPv6 на комп'ютері "Server" запустимо "*iperf -s - V*". На комп'ютері "Client" запустимо

iperf -c 2012 :: 2 -M 9000 -f K -t 10 -i 10 -V.

Вимірювання будемо проводити шляхом зміни параметра "M", який характеризує максимальний розмір TCP сегмента MSS. Для цього встановимо максимальний MTU на мережеві інтерфейси комп'ютера за допомогою такої команди:

ifconfig eth0 mtu 9000

В якості базової методики тестування використовуємо методику RFC-2544 [3], яка має на увазі вимірювання різними значеннями кадрів від 64 до 1518 байт. Отримані результати зведені в табл. 1.2 і відображені на рис. 1.7.

Таблиця 1.2. Залежність швидкості передачі пакетів TCP від розміру пакета

Розмір пакету, біт										
Протокол	64	128	256	512	1024	1280	1518	3000	6000	9000
TCP/IPv4, Мб/с	54,8	74,3	86,1	92,7	95,8	97,1	97,5	98,1	98,5	99
TCP/IPv6, Мб/с	51,2	72,5	84,9	91,1	93,2	95,5	96,1	97,4	98,1	98,8

Аналогічним методом проведемо тестування пропускної здатності мережі при передачі 100 Мбайт даних по протоколах *UDP / IPv4 і UDP / IPv6*. Для цього на сервері "Server" запустимо "*iperf -V -s - uB*". На комп'ютері "Client" для тестування IPv4 запустим команду

iperf -u -t 10 -i 1 -V -c 192.168.254.198 -b 100M -M 1500

Для вимірювання швидкості передачі IPv6 на комп'ютері "Client" запустим команду:

iperf -u -t 10 -i 1 -V -c 2012 :: 2 -b 100M -M 1500

Отримані дані для UDP пакетів різної довжини зведемо в табл. і для наочності відобразимо в Таблиці 1.3.

Таблиця 1.3. Залежність швидкості передачі пакетів UDP від розміру пакета

Розмір пакету, біт										
Протокол	64	128	256	512	1024	1280	1518	3000	6000	9000
UDP/IPv4, Мб/с	57,1	76,6	88,3	94,5	97,1	98,2	98,5	99,1	99,5	99,9
UDP/IPv6, Мб/с	53,4	74,3	85,7	92,2	95,4	96,6	96,8	98,2	98,4	99

Час відгуку

Для дослідження залежності часу відгуку від розміру пакета в IPv4 скористаємося програмою ping, яка дозволяє самостійно задавати розмір пакета, якщо він не перевищує MTU. Для протоколу IPv6 існує своя аналогічна версія програми ping - ping6. Для вимірювання часу відгуку по протоколу IPv4 введемо на комп'ютері клієнта команду

ping -s 1500 192.168.254.198

Динаміка потреби в адресному просторі IPv4 в міру глобального впровадження IPv6 показана на рисунку 1.9. На ньому світло-зеленою лінією позначено зростання глобального Інтернету. У міру впровадження протоколу IPv6 частка Інтернету, доступного тільки по IPv4 буде неухильно зменшуватися (темно-зелена крива). Синя лінія відображає розмір сервіс-провайдера, що характеризується, наприклад, числом підключених користувачів. В даному випадку представлений зростаючий провайдер. Нарешті, потреба в адресах IPv4 показана кривою червоного кольору.

У міру розширення клієнтської бази провайдера пропорційно збільшується потреба в додаткових адресах IPv4. У той же час, все більша і більша частина Інтернету стає доступною по протоколу IPv6, що виражається в зворотну тенденцію, коли все менше число призначених для користувача з'єднань засновані на протоколі IPv4. Відповідно, потреба в адресах IPv4 знижується. Нарешті, коли переважна більшість ресурсів Інтернету стане доступними за IPv6, потреба в IPv4 стане незначною. Таким чином завершиться фаза переходу Інтернету на протокол IPv6. Тривалість цієї фази може зайняти кілька років.

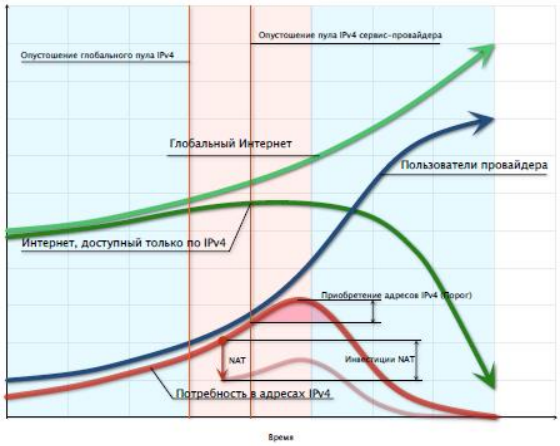

Рисунок 1.7. Спустошення пулу IPv4 сервіс-провайдера

Як видно з графіка, найбільш критичною фазою для сервіс провайдера є проміжок часу моменту спустошення глобального вільного пулу IPv4 до моменту, коли потреба в додаткових адресах IPv4 почне зменшуватися. Ця фаза відзначена на графіку рожевим кольором.

Існує два способи вирішення проблеми з недостатньою кількістю адрес для провайдерів. Перший – це отримання додаткових адрес IPv4. Однак в недалекому майбутньому звернення до RIPE NCC або інший Регіональної реєстратури не дасть бажаного результату через відсутність вільного розподілення адресного простору, і адреси будуть перерозподілятися між гравцями шляхом купівлі-продажу, дарування, об'єднання і поглинання компаній і т.п. Важко сказати, як буде розвиватися цей сценарій і наскільки об'ємним і ліквідним виявиться ринок адресного простору. У будь-якому випадку, другий спосіб – підвищення ефективності використання адресного простору за допомогою технології NAT (*Network Address Translation*), – є більш реальною альтернативою або додатковим рішенням. Цей сценарій показаний на графіку кривої рожевого кольору.

При розробці протоколу IPv6 особливу увагу було приділено можливості додавання нових функцій без втрати ефективності обробки пакетів на мережевому рівні. IPv6 передбачає наявність додаткових заголовків для різних розширень (extension header, EH) - наприклад, для криптографічного захисту даних (*Authentication EH і Encapsulating Security Payload EH*). У той же час базовий заголовок IPv6 містить мінімальну кількість полів і має фіксований розмір. Зокрема, в IPv6 маршрутизатори не виробляють фрагментацію, тому поля, що відносяться до цієї функції, перенесені у відповідний заголовок розширень (*Fragmentation EH*).

Поля, які не підтримуються в IPv6. Фрагментація

Як було згадано вище, протокол IPv6 інакше обробляє фрагментацію пакетів. У разі IPv4, коли маршрутизатор отримує пакет, розмір якого перевищує межу передачі через інтерфейс, маршрутизатор виробляє фрагментацію – дроблення пакета на більш дрібні частини. Надалі вони консолідуються одержувачем в вихідний пакет. Заголовок пакета IPv4 має відповідне поле (*Fragment Offset*), що підтримує цю функцію.

В IPv6 фрагментація проміжними пристроями заборонена. Якщо пакет IPv6 перевищує допустимий розмір для подальшої передачі, маршрутизатор генерує повідомлення ICMP « *packet too big* » (« занадто великий пакет ») і посилає його назад відправнику. В залежності від програми відправник або вибирає розмір пакета, який дозволить йому на всьому шляху прямувати без фрагментації, або дробить пакет самостійно. Як і в IPv4, консолідація фрагментованих пакетів входить в завдання одержувача. Як наслідок, передача пакетів IPv6 вимагає менших витрат від проміжного мережевого обладнання.

Для протоколу IPv6 була розроблена так звана система автоконфігурації без збереження стану (*Stateless Autoconfiguration*). Даний протокол дозволяє різним пристроям, підключеним до мережі IPv6, отримати необхідні установки для доступу в Інтернет без додаткових коштів – наприклад, без сервісу DHCP (*Dynamic Host Configuration Protocol*). Суть підходу полягає в тому, що пристрій отримує адресу, що складається з префікса мережі і ідентифікатора пристрою, автоматично згенерованого з використанням MAC-адреси.

В протокол IPv6 спочатку включена система безпеки, основана на технології IPsec. Передбачено два режими роботи: транспортний і тунельний. У транспортному режимі проводиться захист (шифрування) даних пакета, але не заголовка. З точки зору маршрутизації такий IP-пакет виглядає цілком звичайно, а в завдання одержувача входить декодування вмісту пакета. При використанні тунельного режиму дані всього пакету, включаючи заголовок, шифруються і інкапсулюются в новий пакет. Одержувач, зазначений в цьому новому пакеті, є закінченням захищеного каналу, або тунелю, і в його завдання входить витяг початкового пакету і подальша обробка. Додатково пакет IPv6 містить заголовок аутентифікації (*Authentication EH*) для визначення автентичності та відсутності модифікації даних пакета.

Підтримка мобільності в протоколах IP означає, що термінал може змінити своє місце розташування в мережі і IP-адреса без втрати існуючих зв'язків, які відповідають потокам передачі даних. Для цього мобільні пристрої використовують окремі IP-адреси, за якими пристрою завжди доступні при

передачі даних. За авторизацію мобільного пристрою в мережі і забезпечення відповідності між реальними і мобільними IP- адресами відповідає « Домашній агент » – пристрій, розташований в « домашній » мережі мобільного користувача. Реалізація мобільності в протоколах IPv4 і IPv6 різниться. У разі IPv4 передача даних також проводиться (тунелювання) через « Домашнього агента », в той час як в IPv6 « Домашній агент » забезпечує тільки контролюючі функції (авторизацію і забезпечення відповідності між реальним і мобільним адресами). При цьому передача даних здійснюється між відправником і отримувачем безпосередньо. Такий підхід оптимізує маршрутизацію даних і, як наслідок, підвищує якість передачі.

Наведені особливості протоколу IPv6 покликані поліпшити продуктивність, якість і захист передачі даних. Однак досвід практичного впровадження протоколу IPv6 показує, що зазначені поліпшення досить незначні і в багатьох випадках не використовуються. Навпаки, оператори часто вдаються до перевірених методів, розробленими для мереж IPv4. Так, для конфігурації підключених пристроїв використовується система DHCP, а в області захисту даних технологія IPsec може бути використано в IPv4 майже так само ефективно, як і в IPv6. Ефективна підтримка multihoming (підключення клієнта до кількох сервіс-провайдерів для підвищення надійності) в IPv6 зажадала окремого рішення та істотно ускладнила елегантну структуру маршрутизації, що вважається одним з переваг IPv6. В результаті на практиці multihoming реалізується аналогічно IPv4, що призводить до невиправданого зростання таблиць маршрутизації.

Не дивно, що в середовищі мережевих операторів існує думка, що основна перевага IPv6 – тільки розширення доступного адресного простору.

Практика і проблеми впровадження протоколу IPv6

Стратегія розвитку: співіснування IPv4 і IPv6

Основна проблема переходу від IPv4 до IPv6 – несумісність двох протоколів. Клієнт IPv6 не може безпосередньо спілкуватися з клієнтом, що підтримує тільки IPv4.

Спочатку здавалося, що цю проблему вирішить впровадження «подвійного стека » – коли комп'ютери мережі підтримують обидва протоколи і підключені як до мережі IPv4, так і до мережі IPv6. Дане розділення є логічним, а фізично використовується одна і та ж мережева інфраструктура. Для доступу до ресурсів IPv4 використовується протокол IPv4, а до ресурсів IPv6 – протокол IPv6. Все досить просто, але цю гіпотезу спіткало спростування.

Темпи впровадження IPv6 виявилися незначними. План «подвійного стека» спрацює, якщо в найближчому майбутньому переважна більшість комп'ютерів Інтернету матимуть доступ як до IPv4, так і до IPv6. В такому випадку можна буде просто відключити підтримку IPv4 та Інтернет перейде на новий протокол. Однак реальних передумов для цього немає.

Складність впровадження протоколу IPv6 багато в чому пов'язана з так званим «мережевим ефектом». Цей економічний термін описує явище, коли цінність технології залежить від числа гравців, що її використовують. Дійсно, можливість обмінюватися трафіком IPv6 з парою інших ентузіастів, як це було на початку 2000-х, з практичної точки зору не представляє особливого інтересу. Цей ефект посилюється тим, що велика частина Інтернету як і раніше доступна тільки через протокол IPv4. Розмір цієї частини Інтернету визначає значимість протоколу IPv4 і, в зворотній пропорції, протоколу IPv6 для сервіс-провайдерів.

Кожен новий підключений клієнт повинен мати можливість обмінюватися даними з Інтернетом по протоколу IPv4, що вимагає надання йому адреси IPv4. У той же час важливо відзначити, що обговорювана стратегія і динаміка співіснування двох протоколів заснована на припущенні, що інфраструктура сервіс-провайдера забезпечує повноцінну підтримку IPv6.

Існує значна кількість інтеграційних стратегій, які надають комплексну підтримку IPv6. Взаємодія між IPv4 і IPv6 вимагає певного рівня перетворення

між протоколами IPv4 і IPv6 в хості або маршрутизаторі, при цьому рівню додатків повинно бути зрозуміло, який протокол використовувати.

Основною стратегією для маршрутизації IPv4 і IPv6 одночасно є застосування опорних мереж з подвійним стеком. При цьому для роботи з подвійним стеком повинні бути модернізовані всі маршрутизатори мережі. Взаємодія з IPv4 відбувається за допомогою стека протоколу IPv4 (з пересилкою IPv4-пакетів по маршрутам, отриманим в результаті роботи протоколів маршрутизації, призначених для IPv4), а взаємодія з IPv6 використовує стек IPv6, з'ясовуючи маршрути пересилання пакетів за допомогою протоколів маршрутизації, призначених для IPv6 .

Головні вимоги – наявність у кожного сервера глобального одноадресного (*unicast*) префікса IPv6 і належних записів у DNS, що встановлюють відповідність між іменами хостів та IP-адресами як для IPv4, так і для IPv6. Додатки вибирають між IPv4 і IPv6, виходячи з відповіді, отриманого від бібліотеки розпізнавачів DNS, вибираючи правильну адресу відповідно до типу IP-трафіку і конкретними вимогами, що пред'являються до взаємодії.

В даний час маршрутизація з подвійним стеком – це ефективна стратегія розгортання в певних мережевих інфраструктурах зі змішаними додатками IPv4 і IPv6 (наприклад, в кампусах), що вимагають наявності обох протоколів. Однак, окрім очевидної необхідності модернізації всіх маршрутизаторів мережі, у цього підходу існують і інші обмеження: для всіх маршрутизаторів повинна бути задана подвійна схема адресації, що призводить до подвоєння зусиль по адмініструванню протоколів IPv4 та IPv6, крім того, у маршрутизаторів має бути достатньо пам'яті для зберігання таблиць маршрутизації IPv4 і IPv6.

До того ж, Cisco не рекомендує остаточний перехід до мережі з подвійним стеком до тих пір, поки не буде досягнуто більш повну відповідність між рівнями функціональності і трафіку. Хоча ПО IPv6 для Cisco IOS в повній мірі підтримує подвійний стек, поточна реалізація IPv6 вимагає поліпшення

різних сервісів (наприклад, групових (*multicast*) адрес IPv6) перш, ніж мережу можна буде повністю модернізувати для роботи з подвійним стеком.

З 5 лютого 2008 організація ICANN, контролює використання інтернет-протоколів, почала додавати в DNS-сервери записи, що містять адреси у форматі протоколу IPv6. Це поклало початок переходу від протоколу IPv4 до сучаснішого IPv6. На тепер співіснують мережі, що функціонують по обом протоколам. [1].

Логіка роботи і формати даних двох протоколів істотно відрізняються, тому їх сумісність можна забезпечити зовнішніми по відношенню до них засобами.

Для того, щоб можна було використовувати інфраструктуру мереж IPv4 для передачі пакетів сформованих по протоколу IPv6 запропоновано кілька механізмів:

- механізм подвійного стеку;
- механізм тунелювання;
- механізм трансляції.

Тунелювання – метод передачі IPv6 пакету через IPv4-мережу, коли пакет IPv6 розміщують (інкапсулюють) в пакеті IPv4, як ймовірно і блок даних.

Головною перевагою механізму тунелювання є відсутність необхідності купувати і встановлювати додаткове програмне забезпечення на кожному вузлі.

Механізм тунелювання використовують для часткового вирішення проблеми сумісності між протоколами IPv6 і IPv4. Його не можна застосовувати для зв'язку IPv6-вузлів з IPv4-хостами. Тунелювання призначене для організації зв'язку між IPv6 вузлами або мережами із застосуванням мережевого середовища, що функціонує по протоколу IPv4 [2].

Користувачі сучасних телекомунікаційних мереж використовують в своїх комп'ютерах (мережевих вузлах) операційні системи різних поколінь, що мають різні можливості по адаптації до міри кожного протоколу IPv6. У зв'язку з цим існує проблема адаптації існуючих мереж, що функціонують по протоколу

IPv4, для передачі інформаційних пакетів, створених мережевими ресурсами з протоколом IPv6.

Налаштування тунелю 6to4

Використання такого тунелю можливе в разі, якщо комп'ютер має глобальну IP-адресу. Цей момент є принциповим, оскільки даній технології передбаченому формування унікальної глобальної IPv6 адреси саме по глобальній IPv4 адресі [3]. Оскільки операційна система Windows XP залишається і на даний момент популярною в багатьох користувачів проаналізуємо можливість і особливості налаштування тунелювання в середовищі цієї ОС. Такий механізм може бути реалізовано і в разі використання ОС Windows старших версій.

До недоліків тунелювання слід віднести те, що:

- користувачі створеної нової структури не можуть використовувати ресурси інфраструктури нижчого рівня (тобто мережі, через яку прокладено тунель);
- тунелювання не дозволяє користувачеві нового протоколу обмінюватися даними з користувачами старого протоколу (IPv4) без застосування технології подвійного стека [6].

1.4. Постановка задачі

Статистичні дані свідчать, що протокол мережевого рівня IPv6 є не досить розповсюдженим. Лише 14% провайдерів завершили його впровадження у своїх мережах і лише 4% почали пропонувати IPv6 своїм кінцевим користувачам [1].

На сьогодні безпека протоколу IPv6 є однією з основних проблем, що гальмують його поширення. Оскільки на даний момент цей протокол не використовується в мережах за замовчуванням (відбувається поступовий перехід з IPv4 на IPv6), немає ні найкращих практик та рекомендацій для мережевих адміністраторів, ні будь-яких гарантій, що реалізовані стеки

протоколів IPv6 і методи забезпечення безпеки не мають помилок [2]. Це визначає необхідність дослідження його рівня безпеки.

Задача полягає в організації тестової лабораторії для дослідження рівня безпеки протоколу IPv6 та реалізації заходів для її підвищення.

Для оцінки рівня безпеки протоколу буде застосовано систему CVSS.

Система оцінки CVSS складається з трьох груп метрик:

- основна (визначає основні характеристики уразливості, що є постійними для користувача середовища);
- тимчасова (визначає характеристики уразливості, які змінюються з часом);
- контекстна (визначає характеристики, які є унікальними для користувача середовища).

Кожна група метрик складається із сукупності показників, що формують метрику. А метрика в свою чергу, характеризується числовою оцінкою від 0 до 10 і коротким текстовим описом уразливості і результатів її використання. До групи основних метрик входять показники, які характеризують уразливість:

- вектор доступу (чим ближче зловмисник повинен бути до пристрою жертви, тим нижче оцінка);
- складність доступу (оцінка складності експлуатації уразливості, при наявності доступу до пристрою жертви);
- аутентифікація (оцінка рівнів аутентифікації необхідних для експлуатації уразливості).

Наслідки використання вразливості характеризуються такими показниками: конфіденційність, цілісність, доступність. На основі наведених оцінок можна визначити критичність атаки, що буде відповідати основній оцінці CVSS, тобто: висока (7–10), середня (4– 6.9), низька (0–3.9).

Оскільки метою зловмисника можуть бути різні мережеві пристрої, залежно від виконуваних ними функцій необхідно встановити їх критичність. Максимальний рівень критичності слід встановлювати для пристроїв, невірне функціонування (або припинення функціонування) яких призводить до

неможливості використання ресурсів мережі. Далі в бік зменшення рівня критичності йдуть робочі сервери, функціонування яких є важливою складовою роботи мережі. Мінімальним рівнем критичності володіють персональні робочі станції, порушення в роботі яких, практично не впливають на функціонування мережі в цілому. На основі цієї інформації можна визначити передбачуваний рівень ризику, від експлуатації тієї або іншої уразливості, з наступною інтерпретацією:

A – експлуатація уразливості може привести до невірного функціонуванню або припинення функціонування мережі.

B – експлуатація уразливості може привести до невірного функціонуванню деяких пристроїв мережі.

C – експлуатація уразливості може привести до невірного функціонуванню або припинення функціонування деяких кінцевих пристроїв мережі.

Таким чином, маючи набір вразливостей, які властиві для деякої мережі і знаючи рівень ризику кожної уразливості, можна визначити рівень захищеності мережі.

Висновок до розділу

В першому розділі наведено загальне поняття структури та принципу використання протоколу IPv6.

По суті, протокол IPv6 є заміною IPv4, що належить до сімейства протоколів TCP / IP. У новій версії усунуто велику кількість помилок і недоробок з якими зустрічалися користувачі IPv4. Збільшення адресного діапазону, за рахунок 128 бітного формату, стало ідеальним рішенням для збільшення Інтернет простору. До теперішнього моменту, практичне впровадження і використання нової версії протоколу здатне вирішити відразу кілька завдань одночасно, таких як: повноцінне адресне забезпечення великих мереж, використання додатків і служб з винятковою підтримкою IPv6 і т.д.

Характерні риси IPv6:

- В IPv6 немає Broadcast, ARP. Broadcast більш-менш замінили Multicast адресами і адресами Link Local. ARP протокол замінений протоколом NDP;
- в IPv6 немає технології NAT, яка є в IPv4. Економія адрес в IPv6 не використовується, адрес досить абсолютно всім. Рівень безпеки, який забезпечує NAT в технології IPv4, замінений адресами Unique Local, але не можна забувати, що безпеку повинні забезпечувати міжмережеві екрани - це їхня функція. Назва Nat64 яку можна зустріти в літературі про IPv6 говорить про те, що йдеться про спільне використання технології IPv6, IPv4;
- внаслідок Link Local адресами мережеві пристрої можуть спілкуватися в діапазоні одного локального каналу і тільки в межах його; З'явилася функція, яка називається: «перевірка унікальності IPv6 адреси». Використовується в DHCPv6. Суть її в тому, що після призначення ip-адреси пристрою він посилає icmp запит, destination вибирає дане йому адресу, якщо приходить відповідь – то його адреса не унікальна і потрібно отримувати нову IPv6 адресу;
- з'явилися адреси anycast. У мережі можуть існувати кілька хостів з абсолютно ідентичними IPv6-адресами.
- В протокол IPv6 спочатку включена система безпеки, основана на технології IPsec. Передбачено два режими роботи: транспортний і тунельний. У транспортному режимі проводиться захист (шифрування) даних пакета, але не заголовка. З точки зору маршрутизації такий IP-пакет виглядає цілком звичайно, а в завдання одержувача входить декодування вмісту пакета. При використанні тунельного режиму дані всього пакету, включаючи заголовок, шифруються і інкапсулюються в новий пакет.

РОЗДІЛ 2. ВРАЗЛИВОСТІ ПРОТОКОЛУ IPV6

2.1. Види вразливостей

Розгортання протоколу IPv6 відбувається одночасно із появою нових загроз безпеки кінцевих користувачів та їхніх даних. Загалом, проблеми безпеки пов'язані з протоколом IPv6 можна розділити на дві категорії: ті, що успадковані від його попередника – протоколу IPv4 та нові проблеми, пов'язані із новими можливостями, що були додані до протоколу. Деякі вразливості протоколу не враховані його специфікацією. Такі недоліки неможливо усунути, при цьому не змінюючи сам протокол. Вирішення подібних проблем зазвичай лягає на плечі розробників.

Основні види атак та загрози, які варто розглянути:

- Розвідка в IPv6 мережі. Замість широкомовної розсилки протокол IPv6 використовує групові повідомлення (multicast). І кожен вузол, що використовує IPv6 стає членом хоча б однієї multicast групи, наприклад, *FF02::1* (всі вузли локальної мережі). Зловмисник може використовувати дану особливість для пришвидшення фази розвідки.
- Перевантаження комутаторів. Максимальна кількість IP-маршрутів та MAC-адрес комутатора або маршрутизатора обмежується максимальним розміром CAM і TCAM пам'яті. Включення маршрутизації IPv6 значно зменшує загальну кількість записів TCAM. Це робить комутатор більш уразливим до виявлення атак, а також для створення так званих "прихованих каналів" для передачі даних у заголовках розширення.
- Петля в маршрутизації, при використанні IPv6 тунелів. Тунелювання використовується для передачі даних між островками, де використовується протокол IPv6, через мережу IPv4. Маршрутизатори, що знаходяться на кінцях тунелю працюють із обома протоколами і здійснюють передачу повідомлень, згідно особливостей протоколу тунелювання, що використовується.

При використанні автоматичного тунелювання не відбувається перевірка наявності кінцевих точок тунелю. Зловмисник може використовувати це, надсилаючи пакет через вузол, що не є учасником тунелю в даний момент. В результаті, пакет пересилатиметься з тунелю знову, у нативну мережу IPv6. З цієї мережі, пакет направляється назад в точку входу в тунель. Таким чином пакет буде постійно передаватись в і з тунелю [4]. Жертвами такої атаки будуть вузли, що пересилають повідомлення з та в тунель.

- Атаки пов’язані з роботою ICMPv6. Протокол ICMPv6 є невід’ємною частиною протоколу IPv6. Він повідомляє про помилки та виконує діагностичні функції такі, як ping та traceroute, крім того, має базу для розширення та реалізації нових функцій.
- Процедура NDP – одна із вже реалізованих розширень, що повністю замінює та удосконалює функції протоколу ARP, що працює в мережах з IPv4 [3]. На жаль, і велика частка атак пов’язана саме із цим протоколом.
- Виявлення однакових адрес. Даний механізм використовується кінцевими пристроями для того щоб запобігти появі двох однакових адрес всередині мережі. Він може використовуватись зловмисником для організації DoS атаки.
- Підміна повідомлення Router Advertisement (RA). У протоколі IPv6 реалізовано функцію автоматичного налаштування кінцевих пристроїв. Коли пристрої кінцевих користувачів надсилають запити на отримання мережевих налаштувань (на відміну від DHCP, запит іде на групову адресу), зловмисник може у відповідь надсилати свої налаштування, цим самим виконуючи DoS або MitM атаку.
- “Затоплення” RA повідомленнями
- Як і у попередньому випадку зловмисник підробляє RA повідомлення (можливо, додає нову інформацію про маршрут), але при цьому надсилає їх у великій кількості. Пристрій жертви перевантажується інформацією, що потребує обробки, та вичерпуються його ресурси. Тобто, ситуація призводить до відмови в обслуговуванні.

– Підміна повідомлення *Neighbor Advertisement* (*NA*). Функція, що замінює ARP, який використовується з протоколом IPv4. Зловмисник може видавати себе за “всі станції” в локальній мережі, і тим самим виконуючи DoS або MitM атаку.
– “Затоплення” повідомленнями *Neighbor Solicitation (NS)*. Функція, що практично не відрізняється від ARP, яка використовується з протоколом IPv4. Зловмисник може згенерувати велику кількість запитів на адресу жертви, тим самим перенавантажити інформацією, що потребує обробки. Ресурси пристрою жертви вичерпуються, що призводить до відмови у обслуговуванні.
– Атаки пов’язані з роботою DHCPv6. Окрім автоматичного налаштування в мережі IPv6 також може використовуватись вже знайомий протокол DHCP нової версії. Як не дивно, нова версія має ті ж самі вразливості.
– Вичерпування простору адрес. Зловмисник може вичерпати простір вільних адрес на DHCPv6 сервері.
– Підміна DHCPv6 сервера. Зловмисник може видати себе за DHCPv6 сервер для здійснення *DoS* або *MitM* атаки.

2.2. Механізм дії вразливостей та їх наслідки

Всі великі компанії, які займаються виробництвом мережевого обладнання вже давно говорять про мережі без кордонів. З надзвичайно швидким зростанням мережі Інтернет збільшилася і кількість споживаних IP адрес. IANA розподілила останні пули IPv4 адрес 3 лютого 2011 [1]. Такі реєстратори як APNIC [2], RIPE [3] і ARIN [4], на даний момент, розподіляють останній / 8 блок IPv4 адрес, планується, що інші два реєстратора, LACNIC і AFRINIC, також досягнуто цього стану в найближчі роки. З 2006 року IPv6 протокол перейшов у фазу активного впровадження після проходження тестів і необхідних перевірок [5, 6], які проводила група 6bone [7]. Зараз світ знаходиться в стані, коли IPv6 стає невід'ємною частиною мережевого оточення.

Незважаючи на те, що основна функція протоколів IPv4 і IPv6 залишається однаковою, все ж новий протокол зазнав значних змін, наприклад:

- в IPv6 відсутнє таке поняття як широка розсилка (англ. "*Broadcast*"), яка замінена на групову розсилку (англ. "*Multicast*");
- замість протоколу ARP використовується ICMPv6;
- змінена структура заголовка пакета;
- додана можливість автоматичної конфігурації IPv6-адреси;
- додані нові функції безпеки, такі як: *Cryptographic Generated Address (CGA) і Secure ND (SEND)*, а також додана підтримка IPSec за замовчуванням;
- зміна розміру IP-адреси з 32 до 128 бітів і багато інших.

Із змінами правил взаємодії і нового функціоналу з'явилися і нові уразливості. Саме це стало причиною появи нових механізмів захисту від різних атак, котрі можна було реалізувати на мережевому рівні OSI. Варто зазначити, що подібні механізми безпеки почали з'являтися на світ у вигляді RFC ще починаючи з 2005 року, проте в протоколі IPv4 вони не застосовувалися і розроблялися виключно для протоколу IPv6.

Перехоплення повідомлень RA, RS, NA, NS дозволяє зловмисникові контролювати процес установлення нових налаштувань IP на кінцевому пристрої. Також уразливості NDP можуть бути використані і для здійснення DoS атак, в тому числі атак на процес перевірки дублюючої адреси в мережі.

Крім широко поширених атак на NDP протокол, IPv6 може бути атакований і з інших сторін. Також механізми безпечності, які покликані знизити ризики експлуатації стека протоколів IPv6 відкривають зловмисникові нові можливості для атаки.

Атаки на процес виявлення маршрутизатора

В IPv6 за виявлення маршрутизатора в мережі відповідальний протокол ICMPv6. Пошук клієнт проводить шляхом відправки в мережу на адресу

групового розсилання маршрутизаторів RS пакету. Той маршрутизатор, який першим відповів RA повідомленням, буде обраний в якості шлюзу.

Зловмисник, перехопивши цей інформаційний обмін, може відправити підроблену RA відповідь, вказавши в якості шлюзу себе. Таким чином, весь трафік, спрямований в зовнішні мережі буде проходити через пристрій зловмисника. Комп'ютер атакуючого, в такому випадку, буде виступати в якості проксі-сервера.

Механізм здійснення даної атаки в простому варіанті представлений на Рисунок 2.1. Дана атака може бути модифікована, шляхом відправки на кроці 3 підробленого RA пакета, в якому вказано справжню MAC адресу маршрутизатора і час життя запису рівне декільком годинам.

Таким чином, клієнт через призначений час видалить запис зі своєї таблиці, а зловмисник передасть вже підроблений RA пакет зі своєю MAC адресою. Подібна атака може бути проведена в разі, якщо на клієнті вже встановлено коректно шлюз, або для обходу деяких механізмів безпеки.

Рисунок 2.1. Механізм атаки на процес виявлення маршрутизатора в IPv6

Атака на SLAAC

Як було видно з Рисунок 2.1, для того, щоб автоматично налаштувати IPv6 адресу, клієнт спершу звертається до маршрутизаторів мережі, відправляючи RS сповіщення на адресу групового розсилання маршрутизаторів. Маршрутизатор або видає налаштування, або відправляє клієнта за отриманням налаштувань до DHCPv6 серверу, відправляючи йому відповідь у RA повідомленні.

Перехопивши RS запит клієнта, зловмисник може підмінить RA відповідь маршрутизатора і вказати у відповіді підроблені налаштування. В якості шлюзу за замовчуванням зловмисник вказує свій пристрій і весь трафік клієнта, який передається в зовнішні мережі, буде проходити через атакуючого. Як і в минулій атаці, пристрій зловмисника виступає в якості проксі-сервера між клієнтом і зовнішніми мережами.

Атака на процес виявлення MAC адреси

Припустимо, що клієнт хоче передати інформацію клієнту 2 (Рисунок 2.2). Він знає IPv6 адресу, але не знає MAC адреси даного пристрою. Клієнт відправляє в мережу NS запит в надії отримати MAC адресу необхідного пристрою.

Рисунок 2.2. Механізм атаки на процес виявлення MAC адреси в IPv6

Зловмисник перехоплює цей запит і відправляє підроблену відповідь, вказавши в NA відповіді MAC адресу власного пристрою (крок 2 на Рисунок 2.2). Даний процес називається підміною (англ. "*Spoofing*"). В результаті, вся інформація, яка повинна передаватися клієнту 2, тепер буде передаватися на пристрій зловмисника.

Атака на процес виявлення дублюючої IPv6 адреси

Припустимо, що клієнт з метою перевірки власної IPv6 адреси на унікальність відправляє в мережу NS запит із зазначенням своєї адреси. Якщо на запит інший пристрій не відповість – значить IPv6 адреса унікальна і її можна використовувати. Зловмисник перехоплює NS запит клієнта і відправляє

підроблену NA відповідь, в якій стверджує, що дана IPv6 адреса вже зайнятий (крок 2 на рис. 2.3). Клієнт знову генерує нову IPv6 адресу і знову перевіряє її на унікальність. Зловмисник знову повторює свої дії. Дана атака призводить до відмови в обслуговуванні клієнта, на якою вона відбувається, так як клієнт ніколи не зможе встановити таку IPv6 адресу, яка пройшла би перевірку унікальності.

Рисунок 2.3. Механізм атаки на процес виявлення дублюючої IPv6 адреси

Атака на кеш сусіда

Кожен пристрій зберігає у себе спеціальну таблицю, в яку записуються зіставлення MAC адреси з IP адресою. Нові осередки в даній таблиці з'являються при кожному новому NDP запиті для встановлення MAC адреси віддаленого пристрою. У IPv4 мережі її називали ARP-таблицею, але, так як в стеку протоколів IPv6 відсутній ARP протокол, то цю таблицю прийнято називати просто кешем. Уразливість полягає в тому, що якщо записати в таблицю велику кількість зіставлень, то неможливо буде зберігати нові зіставлення, або і зовсім вийде з ладу.

У прикладі, наведеному на Рисунок 2.4, зловмисник відправляє запити в мережу з префіксом 2001: A: A :: / 64. Так як маршрутизатор (шлюз на Рисунок 2.4) має пряме підключення до цієї мережі, то для кожного нового запиту він формує запис в кеші. У разі, якщо в сканованій мережі існує пристрій, на який направлено запит зловмисника, то маршрутизатор запише зіставлення IPv6 і

MAC адреси даного пристрою. Якщо даний пристрій в мережі відсутній, то запис в кеші все одно буде створений і проіснує кілька секунд.

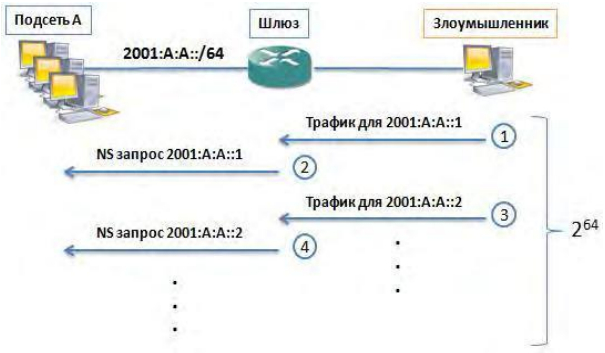

Рисунок 2.4. Механізм здійснення атаки на кеш шлюзу мережі

Якщо пристрій зловмисника досить швидкий, то кеш маршрутизатора (шлюзу на рис. 2.5) заб'ється, що призведе до відмови в обслуговуванні.

Здійснення DoS за допомогою ICMPv6 протоколу

Класична smurf атака – реалізується шляхом відправки зловмисником multicast повідомлення всім хостам в мережі від адреси пристрою-жертви. Всі пристрої мережі, отримавши multicast повідомлення відправляють відповідь. Пристрій-жертва відчуває нестачу ресурсів, внаслідок неможливості обробки такої великої кількості відгуків.

Поширення великої кількості RA [9] і NA запитів. Віддалений пристрій-жертва, отримуючи велику кількість подібних запитів, наприклад, тут представлений список операційних систем, які схильні до атаки RA flood [10] вийде з ладу.

Здійснення DoS атаки за допомогою CGA

Протокол CGA дозволяє створити криптограми IPv6 адреси для підтвердження вірності пристрою джерела. При отриманні CGA адреси одержувач повинен пройти процедуру її перевірки, що може виявитися досить трудомістким процесом. Зловмисник відправляє жертві пакети з великої кількості різних CGA адрес, що змушує пристрій жертви

багаторазово ініціювати процес перевірки CGA адреси і з’їсть його ресурси (рис. 2.5).

Рисунок 2.5. Механізм здійснення DDoS атаки з некоректним CGA

Дана атака можлива в разі, якщо маршрутизатор видає не повний набір налаштувань або не видає налаштування взагалі, перенаправляючи клієнта за додатковою інформацією на *DHCPv6* сервер.

Висновок до розділу

Проведено аналіз вразливостей протоколу IPv6 і інших протоколів, які входять в його реалізацію і необхідні для його коректної роботи, наприклад: протоколи *NDP, IMCPv6, DHCPv6* і т.п.

Також проведено аналіз можливих векторів атак на сімейство протоколів IPv6 і принципів їх реалізації, серед них: атаки на вразливості протоколу *NDP*, *CGA DoS* атак, *ICMPv6 DoS* атак, *DoS* атаки шляхом маніпуляції полями пакета *MTU* або *Current Hop Limit*, атаки на протокол *DHCPv6*, атаки прихованої передачі даних в полях пакета і ін. на додаток наведені програмні засоби реалізації перерахованих атак.

Виходячи з аналізу всіляких атак, в тому числі і абсолютно нових способів компрометації, які з'явилися в силу принципів реалізації та роботи самого протоколу IPv6, можна зробити висновок про його недостатню захищеність без застосування спеціальних захисних технологій.

Також слід зазначити, що в мережі Інтернет з'явилася велика кількість різних утиліт, які можуть бути використані для компрометації протоколу IPv6. Враховувати також слід і той факт, що дані програми стають все простіші в

експлуатації, що робить можливим реалізацію атаки навіть атакуючим з базовим рівнем знань і навичок.

Всі перераховані вище фактори вказують на те, що для сімейства протоколів IPv6 є потреба в додаткових механізмах забезпечення інформаційної безпеки, в тому числі і кардинально нових, так як протокол IPv6 має безліч унікальний особливостей функціонування.

РОЗДІЛ 3. ТЕСТОВА ЛАБОРАТОРІЯ. ДОСЛІДЖЕННЯ РІВНЯ БЕЗПЕКИ ПРОТОКОЛУ IPV6

3.1. Метрики безпеки IPv6

23 лютого 2005 року було опубліковано звіт дослідницької групи NIAC і оприлюднена перша версія CVSS – загальної системи оцінки вразливостей. Ця рейтингова система повинна була забезпечити відкриті та універсальні стандартизовані оцінки небезпеки вразливостей програмного забезпечення. Розвитку цього стандарту сприяли великі IT-компанії, проте, оскільки перша версія самого початку не піддавалася ретельному аналізу з боку безлічі організацій з різних галузей, в ній були виявлені значні недоліки. Основним недоліком CVSS було визнано мале число оціночних критеріїв – існувало багато вразливостей з однаковою оцінкою. Тому була зібрана міжнародна відкрита група CVSS-SIG, завданням якої було виявити і виправити всі подібні недоліки.

1 червня 2007 року було опублікована друга версія CVSS, що одержала широке поширення. Вже у вересні ця версія була закріплена в стандарті безпеки даних платіжних карт PCI DSS. Щоб відповідати вимогам PCI DSS, оператори платіжних систем, що обробляють кредитні карти, повинні продемонструвати, що жодна з цих обчислювальних систем не має уразливості із загальною оцінкою CVSS, більшою чи рівною 4.0. У 2007 році Національний інститут стандартів і технологій США (*NIST*) включив CVSS v2.0 в свій протокол автоматизації безпеки SCAP. У квітні 2011 року CVSS 2.0 був офіційно прийнятий в якості міжнародного стандарту для оцінки вразливостей (ITU-T X.1521)

CVSS 2.0

Оцінка вразливостей по системі CVSS 2.0 проводиться на основі трьох метрик: базової, тимчасової і контекстної. Кожна метрика являється оцінкою

від 0 до 10 балів і коротким текстовим описом, що містить всю необхідну інформацію для виведення цієї оцінки.

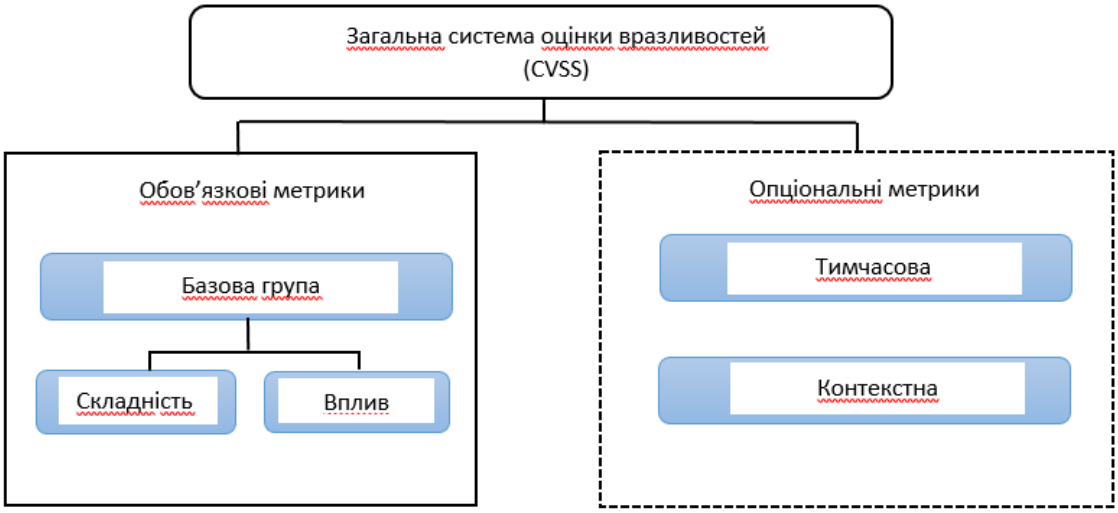

Рисунок 3.1 – Загальна система оцінки вразливостей CVSS

У стандарті CVSS групи метрик визначаються наступним чином:

Базова група метрик відображає невід'ємні і фундаментальні характеристики уразливості, які є постійними з плином часу і призначеними для користувача середовищами.

Тимчасова група метрик відображає характеристики уразливості, які змінюються з часом, але не серед призначених для користувача середовищ.

Контекстна група метрик відображає характеристики уразливості, які є релевантними і унікальними для конкретного середовища користувача.

Базова група метрик включає в себе шість метрик. Перші три – спосіб отримання доступу (*Access Vector*), складність отримання доступу (Access Complexity), показник аутентифікації (*Authentication*) – покликані допомогти отримати уявлення про труднощі, пов'язані з атакою.

Спосіб отримання доступу може бути локальним (*Local*) і віддаленим через суміжну (*Adjacent*) або глобальну (*Network*) мережу, при цьому чим більш віддалено вона атакується зловмисником, тим вище буде базова оцінка.

Складність атаки може бути високою (*High*), середньою (*Mid*) і низькою (*Low*). Передбачається, що у атакуючого вже є готовий експлойт, і під «складністю» мається на увазі складність його використання. Якщо для

успішної експлуатації потрібно лише запустити програму, то очевидно, що складність буде низька. Однак іноді зловмисникові доводиться вдаватися до додаткових дій. Наприклад, якщо він має намір провести фішинг-атаку (атаку, при якій жертва переходить по помилковому посиланню і самостійно вводить конфіденційну інформацію на ресурсі зловмисника, візуально схожу на основний ресурс), то він може використовувати метод соціальної інженерії, і в такому випадку складність експлуатації вважається середньою. Однак соціальна інженерія не завжди приводить до успіху, тому зловмисник може вдатися до перехоплення DNS, атакувавши DNS-сервер. Тоді складність експлуатації буде високою. Чим нижче складність, тим вище числова оцінка базової групи.

Показник аутентифікації відображає складності для атаки, пов'язані з необхідністю надання зловмисником облікових даних. У моделі CVSS аутентифікація може зовсім не вражатися (None), вражатися один раз (Single) або безліч (Multiple) раз. При цьому, якщо вразливість виявлена в самій системі аутентифікації, то вважається, що аутентифікація не вимагається. Якщо потрібна аутентифікація для доступу в локальну мережу, з якої є вразливий додаток, а в самому додатку аутентифікація не вимагається, то вважається, що для експлуатації уразливості аутентифікація не вимагається.

Наступні три метрики базової групи – вплив на конфіденційність, вплив на цілісність і вплив на доступність – визначають можливі наслідки експлуатації уразливості. У кожній з цих метрик вплив може не надаватися (None), опинятися частково (Partial) і бути повним (Complete). Вплив на актив вважається частковим, якщо він може бути обмеженим (наприклад, порушена конфіденційність / цілісність тільки певної частини файлів або переривається доступність лише деяких компонент системи). Якщо до системи є фізичний доступ або доступ з root-правами, то вона вважається повністю скомпрометованою.

Перераховані шість показників підставляються в базове рівняння, закріплене в стандарті. Чим простіше вразливість експлуатується і чим більший

вплив вона робить, тим вище оцінка. Якщо не надається вплив ні на конфіденційність, ні на цілісність, ні на доступність, то числова оцінка базової групи метрик дорівнює нулю.

На прикладі уразливості Heartbleed (CVE-2014-0160) проведемо оцінку базової групи метрик. Ця вразливість є наслідком помилки в пакеті OpenSSL і дозволяє отримати довільні дані з оперативної пам'яті сервера. Для проведення атаки зловмисникові потрібно відправити спеціальним чином сформований запит на атакований сервер. Тобто, зловмиснику досить доступу з глобальної мережі (Access Vector: Network). Складність атаки зводиться до запуску готового експлойта (Access Complexity: Low). Аутентифікація при цьому не потрібна (Authentication: None). Отримання приватного ключа сервера означає часткову втрату конфіденційності (Confidentiality Impact: Partial). Так як прочитати не завантажені в оперативну пам'ять дані не вийде, на цілісності і доступності втрата конфіденційності ніяк не позначиться (Integrity Impact: None, Availability Impact: None). Такий результат публікується у вигляді скороченого вектора (*AV: N / AC: L / Au: N / C: P / I: N / A: N*). Підставивши значення з цього вектора в базове рівняння, отримуємо числову оцінку 5.0 для досліджуваної уразливості.

Другий приклад – вразливість Shellshock, що дозволяє віддалено проводити виконання команд за певних значень змінних оточення всупереч задекларованим можливостям. В даному випадку доступ також можливий через мережу і для експлуатації потрібно лише запуск експлойта без аутентифікації. Однак виконання команд дає можливість порушити не тільки конфіденційність даних (прочитати файли), але і їх цілісність (перезаписати файли) і доступність (наприклад, вимкнути сервер). Тоді ми отримаємо підсумковий вектор (*AV: N / AC: L / Au: N / C: P / I: C / A: C*) і оцінку 10.0, адже всі показники приймають найгірші значення. Очевидно, що якщо в системі існують обидві уразливості, то важливіше спочатку виправити другу уразливість, і базова оцінка дозволяє це зрозуміти.

Наступні дві групи метрик опційні і їх застосування не має сенсу окремо від базової. Кожен показник в них крім основних значень може бути не визначений, і тоді він не буде враховуватися при розрахунку.

Тимчасова група включає три метрики:

Можливість використання (*Exploitability*) уразливості відображається стан методів експлуатації і доступність коду. Розрізняють стадію теоретичного існування експлойта (*Unproven*), стадію існування концепції експлуатації (*Proof Of Concept*) – коли можна провести демонстрацію, але на більшості реальних додатків вона не спрацює, стадію існування сценарію (*Functional*) – коли доступний код експлойта і він працює в більшості випадків без змін, і стадію високої (*High*) небезпеки, якщо експлойт доступний і працює автономно на безлічі пристроїв. Підсумкова числова оцінка тимчасової групи тим вище, чим простіше використовувати уразливість.

Рівень виправлення (*Remediation Level*) відображає стан обробки уразливості. При цьому розрізняють стадію, коли будь-яке рішення недоступно (*Unavailable*), а також стадії існування рекомендацій (*Workaround*), тимчасового рішення (*Temporary*) і офіційного виправлення (*Official Fix*).

Ступінь достовірності джерела (*Report Confidence*), яке повідомило про уразливість – може бути не підтверджена (*Unconfirmed*), не доведена (*Uncorroborated*) і підтверджена (*Confirmed*) вендором ПО.

Кожен з цих показників може змінитися з плином часу. Наприклад, спочатку одним дослідником може бути знайдена сама помилка, а сценарій її експлуатації не розроблений, потім іншим дослідником розроблена концепція або конкретний експлойт.

Як приклад проведемо оцінку тимчасової групи для Heartbleed: на поточний момент доступні відповідний експлойт і офіційний патч для вразливості бібліотеки, також відомо, що уразливість підтверджена. Тоді отримуємо вектор (E: H / RL: OF / RC: C) і оцінку 4.4. Відзначимо, що оцінка відмінна від нуля навіть після випуску офіційного виправлення, оскільки багато користувачів могли не застосувати його.

Контекстна група метрик відображає вплив на ризик для конкретної організації, що використовує вразливе ПО. У той час як оцінка базової і тимчасової групи проводиться аналітиками, що досліджують вразливість, контекстна метрика визначається кінцевим користувачем, так як він має найбільш повну інформацію про оточення, в якому існує вразливість. Контекстна група складається з п'яти метрик:

Імовірність нанесення непрямих збитків (*Collateral Damage Potential*) відображає наскільки сильно можуть постраждати активи, не пов'язані з вразливим додатком. Ця ймовірність може бути низькою (*Low*), середньо-низькою (*Low-Medium*), середньо-високою (*Medium-High*) і високою (*High*).

Щільність цілей (*Target Distribution*) відображає наскільки сильно постраждає система в цілому від експлуатації уразливості. Щільність цілей може бути низькою, середньою або високою.

Вимоги до конфіденційності (*Confidentiality requirements*), вимоги до цілісності (*Integrity requirements*) та вимоги до доступності (*Availability requirements*) – можуть бути низькими, середніми або високими. Це визначається вимогами, що пред'являються до уразливої системи.

CVSS 3.0

На жаль, версія CVSS 2.0 теж виявилася не ідеальною, в ній залишилася проблема недостатньої інформативності оцінки, в даному стандарті також з'являлися уразливості з однаковими векторами, але з різною оцінкою небезпеки. У FIRST (підприємство, що підтримує стандарт) було відправлено відкритий лист з Open Security Foundation, в якому додатково відзначалися наступні проблеми:

1. деякі показники CVSS трактуються неоднозначно – на різних ресурсах в базах вразливостей, що надають оцінки CVSS 2.0, можна знайти ідентичні уразливості, для яких вказані різні складності експлуатації;

2. багато компаній (Oracle, IBM, HP, Cisco) разом з оцінкою CVSS 2.0 почали використовувати свої більш інформативні оцінки або виставляти числову оцінку не у відповідності зі стандартом;

3. відсутність якісної шкали оцінки і, як наслідок, різне трактування числової оцінки різними користувачами.

Робоча група CVSS-SIG розпочала роботу над третьою версією стандарту, і в червні 2015 року вона була опублікована.

До неї були внесені наступні зміни:

- доданий фізичний рівень доступу, що має на увазі доступ до апаратного забезпечення системи;
- виключений середній рівень складності експлуатації – якщо для експлуатації слід дотримуватися спеціальних умов, непідконтрольних атакуючому, або для виконання яких потрібно проводити додаткові атаки, то складність експлуатації вважається високою. В інших випадках – низькою. Окремим показником винесено взаємодію з користувачем (User Interaction: None / Required);
- аутентифікація замінена на оцінку рівня привілеїв (показник Privileges Required) – цей рівень може бути високим, низьким або відсутнім. Останнє значення еквівалентно відсутності аутентифікації, низький рівень відповідає аутентифікації з правами звичайного користувача, а високий – з правами адміністратора. Дана зміна обумовлено тим, що число аутентифікації відображає складність експлуатації менш виразно, ніж якісна складність кожної аутентифікації (отримати права адміністратора складно, аутентифікуватися десять разів з правами звичайного користувача зазвичай не складніше, ніж зробити це один раз);
- скориговані коефіцієнти в рівняннях – оцінка стала менше залежати від складності експлуатації і більше від завданого впливу;
- введено поняття ланцюжка вразливостей. Іноді експлуатація декількох вразливостей одноразово несе набагато більшу небезпеку, ніж кожна з вразливостей окремо;

– метрики впливу з кількісних перейшли в якісні. Замість часткового і повного впливу на конфіденційність, цілісність і доступність оцінюється ще і критичність тієї частини системи, на яку було проведено вплив, в термінах середнього (*Medium*) і сильного (*High*) впливу.

Останній пункт зі списку змін заслуговує на окрему увагу. Щоб продемонструвати актуальність положень пункту 6, розрахуємо базову метрику для уразливості *CVE-2018-4871*. Уразливість полягає в читанні за межами буфера в Adobe Flash Player і дозволяє прочитати приватну інформацію з ПК користувача, доступну уразливому додатком (за замовчуванням – недоступно нічого).

З позицій CVSS 2.0 ця вразливість має точно такі ж характеристики, як і Heartbleed. Однак витік приватного ключа сервера дозволяє розшифрувати весь трафік, який коли-небудь приходив на сервер від кого завгодно. Тому збереження конфіденційності приватного ключа сервера набагато важливіше захисту інформації на ПК. У CVSS 3.0 показник конфіденційності у Heartbleed визнається високим, а у щойно описаної уразливості – середнім, підсумкові оцінки 7.3 і 5.3 відповідно.

3.2. Тестування безпеки протоколу

Прослуховування IPv6

Переадресація IPv6 (також відома як "обов'язковий захисник цілісності") насправді є "комплектуюча" функція, яка поєднує в собі:

– охорону *RA / DHCP*;
– очищення адреси IPv6;
– перевірку IPv6 НД.

Оскільки під час перегляду IPv6 включені охоронні функції (якщо увімкнете *snooping* для IPv6), то не потрібно явно налаштувати охорону безпеки *RA / DHCP* на тому ж порту.

Просто налаштування перегляду IPv6 має бути дійсним для більшості ситуацій, однак, якщо потрібна більш просунута конфігурація для охоронця

RA, то необхідно налаштувати певну політику безпеки RA, як це показано в розділі конфігурації охорони RA.

Наступний скрипт показує конфігурацію за замовчуванням для відстеження IPv6.

```
  !
interface GigabitEthernet1/0/1
 ipv6 traffic-filter nofrags in
!
ipv6 access-list nofrags
 !!!! the line below may be uncommented for the most
 !!!!  conservative  environments,  after  studying  the
implications
 ! deny ipv6 any FE80::/64 fragments
 deny ipv6 any FE80::/64 undetermined-transport
 permit ipv6 any any
!
```

Щоб перевірити політику snooping, слід скористатися командою *show ipv6 snooping policy* [назва політики], як показано нижче.

```
!
ipv6 snooping policy HOST
!
!
interface GigabitEthernet1/0/2
 switchport access vlan 201
 switchport mode access
 ipv6 snooping attach-policy HOST
!
```

Зауважимо, що при налаштуванні IPv6 snooping безпека за замовчуванням встановлена на "захист". Цей параметр може викликати проблеми, коли політика snooping додається до порту, до якого підключено сервер DHCPv6. Цей параметр політики надішле повідомлення DHCPv6. Щоб дозволити повідомлення DHCPv6, порт повинен бути налаштований як надійний порт, або потрібно налаштувати певну політику захисту DHCPv6.

Очищення адреси IPv6

Адреса *gleaning* вивчає адреси IPv6 пристроїв, підключених до цього посилання, і є необхідною умовою для більш просунутих функцій FHS, таких як *Source-Guard*. Навчання здійснюється шляхом вивчення інформації в пакетах ND та DHCPv6 (зокрема, адреси, що містяться в них). Проте, повідомлення

сервера DHCPv6 скидаються так, щоб підбирати з повідомлень DHCPv6, політика охорони повинна бути застосована до порту, який з'єднує дійсний сервер DHCPv6, що дозволяє отримувати повідомлення DHCPv6.

Код FHS вивчає адреси та встановлює їх у таблицю зв'язків. Кожен запис містить джерело, з якого було вивчено адресу, саму адресу, MAC-адресу, інтерфейс, vlan, рівень пріоритету, стан та час, що залишився.

Перевірка IPv6 ND

Інспекція ND перевіряє здоровий стан повідомлень ND, які проходять через пристрій. Це також може забезпечити обмеження на кількість адрес для кожного порту. Ця функція впроваджує процес ND, забезпечуючи, що всі сторони крокують за всіма правильними кроками в процесі ND. Процес перевірки ND створює таблицю зв'язків сусідів.

Перевірка нав'язувальної таблиці

У наведеному нижче прикладі в таблиці зв'язків є два елементи, обидва отримані через ND, що належать одному і тому ж пристрою, підключеному на інтерфейсі Ethernet2 / 0 у vlan100 – одна адреса є локальною, а інша – глобальна. Ми можемо бачити, що обидва записи знаходяться в стані REACHABLE, і вони залишаться настільки ще протягом майже 300 секунд.

```
Sw2#show ipv6 neighbors binding
 Binding Table has 2 entries, 2 dynamic
 Codes: L - Local, S - Static, ND - Neighbor Discovery, DH -
DHCP, PKT - Other Packet, API - API created
 Preflevel flags (prlvl):
 0001:MAC   and   LLA   match                0002:Orig   trunk
0004:Orig access
 0008:Orig  trusted  trunk         0010:Orig  trusted  access
0020:DHCP assigned
 0040:Cga   authenticated            0080:Cert   authenticated
0100:Statically assigned
 IPv6 address                                  Link-Layer addr
Interface vlan prlvl  age   state    Time left
 ND  FE80::A8BB:CCFF:FE00:6900                  AABB.CC00.6900
Et2/0      100  0005   11s  REACHABLE  289 s
 ND  2001:DB8:23::2                            AABB.CC00.6900
Et2/0      100  0005   10s  REACHABLE  296 s
```

```
Sw2#
```

Зчитування даних IPv6

Іноді просто контролювати потоки DHCPv6 та ND недостатньо для вивчення адрес (наприклад, перемикач може бути просто перезавантажений, або DAD NS може бути втрачено на шляху до перемикача, а хост вже почав надсилати дані). Щоб і надалі підтримувати правильне представлення прикріплених адрес, цей перемикач може переносити пакети даних з невідомих джерел за посиланням на код очищення адреси, після чого надсилатиме *DAD Neighbour Solicitation* для перевіреної адреси.

Якщо хост дійсно має адресу IPv6, він буде відповідати з оголошенням сусідів. Це буде служити доказом права власності на перший приїзд, і тому новий запис з адресою буде встановлений у таблиці обов'язкових документів.

Щоб увімкнути конфігурацію, налаштуйте ключове слово "data-glean" під політикою snooping, як наведений нижче приклад:

ipv6 snooping policy FOO

data-glean

Наразі ця функція може не застосовуватися на всіх платформах, тому перевірте, чи можете ви застосувати цю політику до налаштувань даних після налаштування.

Відстеження пристрою IPv6

Пристрій відстеження – це розширення основного процесу очищення адреси. За допомогою пристрою відстеження перемикач підтримує валюту зібраних записів адреси. Сталеві записи повторно перевіряються за допомогою обміну даними NS-NA, подібними до початкової перевірки прав власності, і очищуються після несправності.

Це означає, що таблиця обов'язкових зв'язків містить достатньо чітке представлення адрес на посилання та може використовуватися як авторитетне джерело політики для інших функцій, таких як охорона джерел.

Відстеження пристрою вимкнено за замовчуванням та налаштовано відповідно до політики відстеження IPv6.

IPv6 snooping policy FOO можливість відстеження

Ці функції потребують процесорного часу, щоб генерувати та обробляти трафік ND, необхідний для роботи цих функцій. Ці функції слід розгортати лише у ситуаціях, коли потрібна дуже детальна інформація про кінцеві системи. Дані функції не слід розгортати на платформах, які об'єднують велику кількість кінцевих систем, оскільки операції ND можуть пригнічувати процесор. Подальший аналіз має бути зроблено при застосуванні функцій відстеження даних та відстеження пристроїв FHS для забезпечення необхідності цих функцій там, де вони будуть розгорнуті, і що платформа здатна обробляти навантаження.

IPv6 відслідковування ведення журналу

Нестабільність адрес IPv6 представляє особливу проблему для адміністраторів мережі: як зрозуміти, що відбувається з часом на першій лінії зв'язку. Зв'язувальна таблиця на перемикачах з підтримкою FHS являє собою джерело знань, однак ця інформація має стислий характер, і іноді те, що також потрібне, є історичним оглядом. Щоб допомогти в цьому, можна налаштувати ведення журналу перевірки IPv6. За допомогою цієї ввімкнено всі зміни у таблиці зв'язування будуть серіалізовані в звичайні повідомлення syslog, які можна відправити, обробляти та аналізувати, як завжди.

Для реєстрації подій, що відслідковують IPv6, використовуйте наступну конфігураційну лінію:

```
!
ipv6 neighbor binding logging
!
```

Зверніть увагу, що ця діяльність з ведення журналів може генерувати багато повідомлень, якщо платформа є точкою агрегації для великої кількості кінцевих систем. Ця операція реєстрації може збільшити процесор, якщо

повідомлення системного журналу експортуються ззовні, або перевизначити налаштовані журнальні буфери швидше на платформі. Потрібно провести подальший аналіз, щоб визначити вплив цієї функції при розгортанні.

Щоб переконатись, що викрадач-хост не може негативно вплинути на перемикач, якщо ви ввімкнете відслідковування IPv6, ви повинні визначити відповідні ліміти для кількості записів у сусідній таблиці.

Визначення цих обмежень може використовуватися за допомогою *snooping* IPv6. Як показано нижче, політика IPv6 обмежує кількість адрес, які можна отримати в порту, до 2.

```
!
ipv6 snooping policy HOST
 limit address-count 2
!
```

Ця політика дозволяє вивчати дві адреси. Одна з них буде локальною адресою посилання, а іншою адресою буде будь-яка адреса, яка вивчається спочатку (*SLAAC, DHCPv6*, конфіденційність тощо). При використанні цієї функції необхідно належним чином контролювати призначення адрес для кінцевих систем. Наприклад, якщо для пристрою буде призначена адреса через *DHCPv6*, то *SLAAC* і розширення конфіденційності повинні бути відключені в кінцевій системі. Адміністратори повинні мати на увазі, що деякі кінцеві системи не дозволяють вимикати адреси конфіденційності у випадку, якщо *SLAAC* використовується для призначення адрес, тому застосування вищезазначеної конфігурації в середовищі *SLAAC* призведе до збоїв з'єднання, які важко усунути.

При розгортанні цієї функції початкове розгортання політики повинно починатися з більших значень для лімітів, щоб гарантувати, що всі кінцеві системи є доступними, і що поведінка добре зрозуміла. Оскільки відповідні операції підтверджені, цей розмір вікна може бути зменшений.

Розмір сусідньої обов'язкової таблиці може бути додатково обмеженою наступною глобально налаштованою командою.

```
!
ipv6 neigh binding max-entries [max # of entries]
```

```
!
```

Приклад налаштування *snooping* IPv6

Цей приклад конфігурації надає політику захисту від IPv6 на рівні "коробки". Це означає, що ми повинні налаштувати захист RA явно на портах, що з'єднують маршрутизатор, щоб дозволити RA з маршрутизатора на всіх VLAN. Зауважте, що налаштована політика на інтерфейсі має перевагу над глобально налаштованою політикою.

```
ipv6 neighbor binding logging
 ipv6 snooping logging packet drop
 ipv6 nd raguard policy ROUTER
   device-role router
 !
 ipv6 snooping policy SNOOP
    tracking enable
 !
 ipv6 snooping attach-policy SNOOP
 !
 interface Ethernet2/0
  description Trunk to the router
  switchport
  switchport trunk encapsulation dot1q
  switchport mode trunk
  ipv6 nd raguard attach-policy ROUTER
```

Ми можемо перевірити, чи дійсно політика застосовується, як очікується:

```
Sw2#sh ipv6 snooping policies
 Target     Type  Policy        Feature        Target range
 Et2/0      PORT  ROUTER        RA guard       vlan all
 Box        BOX   SNOOP         Snooping       vlan all
 Sw2#
```

Джерело IPv6

Захист від джерела IPv6 спирається на відслідковування IPv6 і використовує точне відображення адрес на першому хопі, побудованому за допомогою обробки адреси / процесів відстеження пристрою. Це може бути використано для того, щоб зробити підроблення адрес.

У наступному прикладі ми дозволяємо RA Guard, ми явно включимо порт E2 / 0 як порт для маршрутизатора, активуємо Source Guard, і заносимо в журнал відкинуті пакети

```
ipv6 nd raguard policy ROUTER
 device-role router
```

```
!
! log which packets are dropped
ipv6 snooping logging packet drop
ipv6 snooping policy SNOOP
 tracking enable reachable-lifetime 300
!
ipv6 snooping attach-policy SNOOP
!
ipv6 source-guard policy SG
!
ipv6 source-guard attach-policy SG
!
!
interface Ethernet2/0
 description Router trunk
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ipv6 nd raguard attach-policy ROUTER
!
! The below is for testing of the device tracking.
!!!!!! ipv6 neighbor binding stale-lifetime  300
!
!
! Log the changes to the binding table
ipv6 neighbor binding logging
!
```

Цей розділ містить приклади конфігурації для різних компонентів FHS і призначений як посилання.

Охоронець RA: порт тільки для хостів.

Проста конфігурація, що дозволяє E0 / 1 як порт хоста. Будь-який RA, отриманий на цьому порту, буде автоматично скинутий.

```
 interface Ethernet0/1
     ipv6 nd raguard
```

Конфігурація, де один порт (E2 / 0) явно налаштований як порт маршрутизатора, а решта портів (за замовчуванням) є портами хоста. RA-guard за замовчуванням увімкнено лише у VLAN100.

У цій конфігурації єдиний порт, на якому приймається RA, - це E2 / 0

```
ipv6 nd raguard policy HOST
!
ipv6 nd raguard policy ROUTER
 device-role router
!
vlan configuration 100
 ipv6 nd raguard attach-policy HOST
```

```
!
interface Ethernet2/0
 description Router
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ipv6 nd raguard attach-policy ROUTER
```

3.3. Оцінювання рівня безпеки

Метою роботи, було створення і супровід полігону тестування та апробації мережевих технологій, послуг і додатків на основі протоколу IPv6 з двома варіантами конфігурациі Cisco і Aruba. З огляду на складність досягнення поставленої мети в повному обсязі, коло вирішуваних завдань обмежив наступними:

- дослідження існуючого програмного забезпечення та встановлення його на інфраструктурі полігону;
- аналіз існуючих ядер операційної системи Linux, і реалізації протоколу IPv6 в них;
- перевірка роботи протоколу «*Neighbor Discovery for IP Version 6*» RFC 2461;
- перевірка роботи протоколу призначення адрес IPv6 "*IPv6 Stateless Address Autoconfiguration*" RFC 2462;
- аналіз існуючих версій програмного забезпечення Cisco IOS та Aruba для маршрутизаторів і реалізації протоколу IPv6 в них;
- перевірка працездатності IPv6 на різних типах інтерфейсів роутера, таких як *Ethernet, Fast Ethernet, ATM LANE, ATM PVC* (RFC 2464, RFC 2492);
- перевірка реалізації і працездатності і механізмів організації тунелів IPv6 поверх існуючої версії протоколу IP;
- перевірка роботи механізмів взаємодії IPv6 між сервером під управлінням ОС Linux і маршрутизатором під управлінням Cisco IOS (BGP4 + згідно RFC 2858) та Aruba;

– реалізація сервісів на транспорті протоколу IPv6, запуск і перевірка працездатності роботи сервісу FTP поверх IPv6, запуск і перевірка працездатності служби сервісу доменних імен для адрес IPv6.

Технологічна база досліджень

Весь полігон створювався на основі вільно поширюваного програмного забезпечення - ОС Linux і супутніх програм. Відкритість вихідного коду дозволила повністю використовувати можливості, що надаються програмним забезпеченням, а також відносно просто зробити налаштування і виправлення помилок. При створенні полігону використовувалися виключно ті елементи, що були в наявності і функціонують на мережі обладнання.

В якості маршрутизатора в першому варіанті конфігурації використовувався Cisco 2811, що добре зарекомендувала в роботі в ATM мережах. На ньому була встановлена безкоштовно надається експериментальна версія IOS 12. Тестові робочі станції мали наступну конфігурацію: P2-400, 256 mb пам'яті, 100 Mbit Ethernet. Сполучення з ATM мережею відбувалося через комутатори Cisco CATALYST. В ході експериментів також використовувався ATM комутатор Cisco SB Catalyst 2960.

Для проведення тестових експериментів були створені такі зміни тестових полігонів.

Полігон 1

Перший полігон створювався для тестування IOS і роботи IPv6 через ATM, PVC, LANE. Два комп'ютери під управлінням Linux (версія ядра 2.4) з'єднувалися через комутатор Catalyst до маршрутизатора Cisco 2811 за допомогою ATM, PVC або LANE з'єднання.

Перевірялася працездатність протоколу "*Neighbor Discovery for IP Version 6*" і протоколу призначення адрес IPv6 «*IPv6 Stateless Address Autoconfiguration*» через локальне з'єднання.

Полігон 2

Другий полігон представляє з себе два комп'ютери під управлінням Linux (версія ядра 2.4), з'єднаних за допомогою мережі через два різних Aruba 3810. На цьому етапі перевірялася працездатність протоколу «*Neighbor Discovery for IP Version 6*» і протоколу призначення адрес IPv6 «*IPv6 Stateless Address Autoconfiguration*» через ATM з'єднання.

Результати тестових випробувань

Відповідно до поставлених технічних завдань були проведені наступні роботи по дослідженню та апробації існуючого вільного та закритого програмного забезпечення. Використані реалізації IPv6 мають різні недоліки, проте дозволяють будувати працездатні фрагменти мережі IPv6.

Загальним недоліком всіх випробуваних варіантів IPv6 є відсутність повної реалізації системи підпису та шифрування даних (обов'язкового розширення IPsec протоколу IPv6). Засоби безпеки для IP описуються сімейством специфікацій IPsec, розроблених робочою групою IP Security. Ці специфікації застосовуються як до IPv4, так і до IPv6.

Була проведена перевірка працездатності протоколу «*Neighbor Discovery for IP Version 6*» (RFC 2461). У зв'язку з тим, що реалізація протоколу грунтується на посилці широкомовних пакетів, в різних мережевих середовищах виникають специфічні проблеми, пов'язані з організацією розсилки цих пакетів. Протокол успішно працює всередині Ethernet (Fast Ethernet) сегментів, в тому числі сегментів, що складаються з декількох комутаторів, пов'язаних між собою за допомогою транків. У разі застосування ATM для зв'язку різних комутаторів Ethernet в одному сегменті протокол Neighbor Discovery працював тільки при використанні PVC.

Аналогічні проблеми виявлені при тестах роботи протоколу «*Address Autoconfiguration*» на різних середовищах передачі: нормальна робота поверх Ethernet / Fast Ethernet, ATM PVC і непрацездатність ATM LANE. Таким чином, при використанні ATM LANE, сегмент мережі розпадається на кілька зон, усередині яких діють протоколи *Neighbor Discovery* і *Neighbor Discovery*. Між

зонами, з'єднаними по LANE ці протоколи не функціонують, однак, звичайний трафік IPv6 нормально передається і поверх ATM LANE.

Проведені експерименти показали кращу працездатність IPv6 на наступних інтерфейсів маршрутизаторів – *Ethernet / Fast Ethernet, ATM PVC*, за умови використання останнього експериментального програмного забезпечення від фірми Cisco. У разі використання Aruba необхідно використовувати ручну настройку адрес IPv6. Для обладнання Cisco підтримка IPv6 заявлена вже в поточних версіях програмного забезпечення, що дозволяє сподіватися на виправлення цих помилок найближчим часом. Існуюче програмне забезпечення дозволяє використовувати тунелі IPv6 over IPv4. На поточний момент успішно експлуатуються такі тунелі, що з'єднують IPv6 полігон мережі MSUNet з зовнішньої, світової, мережею IPv6 (VBNS) і мережею IPS RAS (Інституту системного програмування РАН). Були перевірені наступні зв'язки роботи протоколу *BGP4 +: IOS-IOS, IOS-Zebra*.

У зв'язці IOS-IOS робота протоколу BGP4 + не викликала нарікань, в зв'язці IOS-Zebra програмний маршрутизатор під керуванням Zebra не впорався з обробкою таблиць маршрутизації через численні помилки в ньому. У зв'язку з неадекватною реалізацією, використання поточної версії Zebra вважається недоцільним. Проводилися експерименти з установкою програмного розширення для роботи IPv6 на робочих станціях, що працюють під управлінням ОС Windows NT.

З сайту www.microsoft.com були використані спеціальні драйвера протоколу IPv6. Дана реалізація виявилася цілком працездатною. На серверах був встановлений FTP сервер Libra (libraftp.narod.ru). Також було встановлено і протестовано DNS сервер.

На жаль, поточна версія відповідає на IPv4 запити, але повертає і IPv6 адреси асоційовані з доменним ім'ям.

Порівняємо наявність основних функцій у вирішенні на базі контролерів Cisco і HPE:

Таблиця 3.1. Основні функції на базі контролерів Cisco і HPE

Функція	**Cisco**	**Aruba**
Автоматичне управління радиосреде	RRM	ARM
моніторинг інтерференції	CleanAir	Spectrum Analysis
Виявлення сусідніх ТД	Rogue Detection	Rogue Detection
Моніторинг і контроль додатків	AVC	AppRF + URL Filtering
оптимізація роумінгу	Optimized Roaming	Client Match
Шифрування даних (точка-контролер)	DTLS	IPSec
резервування	SSO, N + 1	Active / Active, Active / Standby
запобігання вторгнень	wIPS	wIPS
позиціонування	Hyperlocation	- (тільки BLE)
Оптимізація передачі сигналу	ClientLink	-
Міжмережевий екран	-	Stateful Firewall
маршрутизація	-	Static, OSPF
Віддалений доступ IPsec / SSL VPN	-	Virtual Intranet Access (VIA)

З таблиці видно, що за основними функціями WiFi у Cisco і Aruba є що протиставити один одному. По суті це схожі технології з різними назвами, хоча у кожного є свої додаткові "фішки", підтримка технологій \ протоколів. У Cisco – це, наприклад, технологія ClientLink, що дозволяє оптимізувати downlink передачу (від точки доступу до клієнта). У HPE – це повноцінний міжмережевий екран, підтримка протоколів динамічної маршрутизації, URL фільтрація. Відзначимо, у HPE додаткові функції не є саме "бездротовими", що робить контролер більш універсальним мережевим пристроєм.

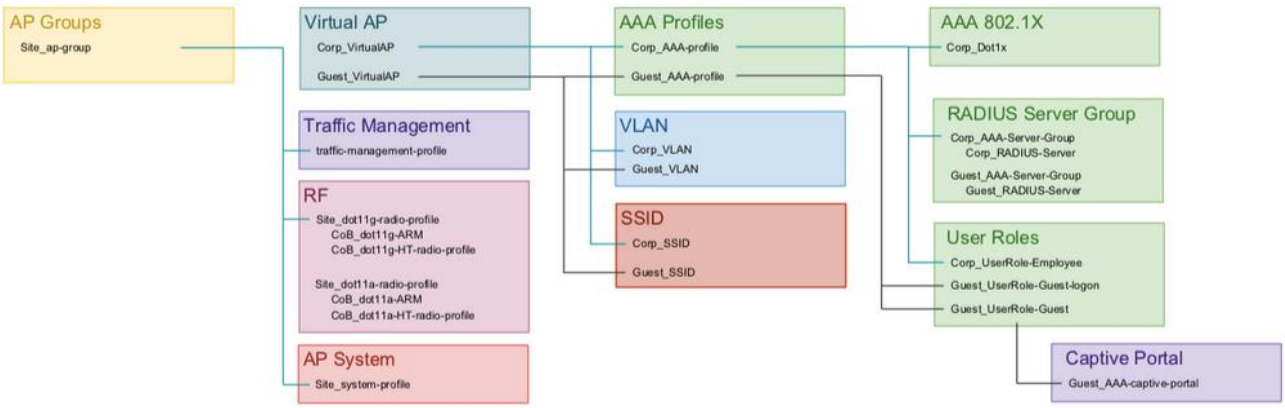

Рисунок. 3.2. Профілі в Cisco

HPE Aruba

На контролері HPE Aruba настройка здійснюється через профілі. Розгалужена структура профілів для настройки бездротових параметрів на точці \ групі точок представлена нижче.

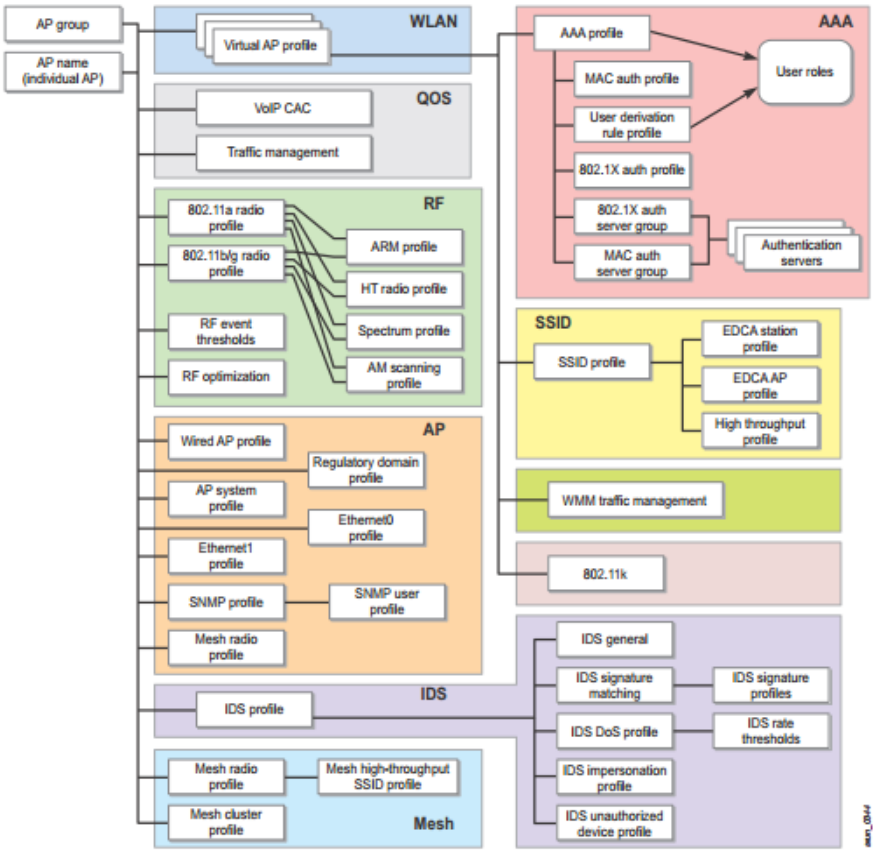

Рисунок 3.3. Профілі в Aruba

Наприклад, щоб створити бездротову мережу, необхідно створити профіль *Virtual AP*, потім прикріпити до нього *AAA profile* і *SSID profile*. Є меню спрощеної налаштування із зазначенням основних профілів (управління радиосреде, QoS, AAA і ін).

В меню розділу *Configuration* присутні вкладки для налаштування різних функцій.

Через велику кількість детальних налаштувань, попередньо налаштованих політик і профілів, при налаштуванні в перший раз можна заплутатися. Тут може допомогти кнопка *Show reference*, що показує зв'язки різних сутностей (профіль, політика) один з одним.

Коли заходиш у вкладку *All Profiles*, видно, наскільки багато різних тонких деталей можна налаштувати на контролері Aruba. Кастомізація тут більш детальна ніж в Cisco.

Cisco

Інтерфейс поділений на розділи (*WLANs, SECURITY, MANAGEMENT* і ін.). Немає профілів і референсів. Інтерфейс виглядає більш зручним і інтуїтивно зрозумілим. Однак тут немає такого числа детальних налаштувань та додаткових функцій як в Aruba.

HPE Aruba

Кожному підключеному клієнту прив'язується певна роль зі своїми політиками доступу (*User-centric network, Stateful Firewall*). На контролері є встановлені профілі і правила фаєрвола. З одного боку, це дуже зручно: наприклад, не потрібно налаштовувати з нуля політики гостьового доступу, можна тільки додавати конкретні правила для цієї ролі.

З іншого боку, якщо у вас немає ліцензії на міжмережевий екран (*PEFNG*), тому ролі втрачають сенс. При цьому в налаштуваннях (профілі AAA, наприклад) вони все одно залишаються, так як це одна з ключових сутностей, які використовуються при конфігуруванні.

Cisco, як і Aruba, вміє визначати тип клієнта (*profiling*) по заголовкам HTTP, DHCP. Для певного типу клієнтів (наприклад, *iPad* або *Android-Samsung*) на контролері можна створити політику доступу (*local policy*) з необхідними параметрами і обмеженнями – *ACL, VLAN, QoS*, години роботи та ін.

Налаштовувати контролер бездротової мережі комфортніше через графічний інтерфейс. У командному рядку швидше робити вибірку по параметрам або виконувати налагодження проблеми. Для порівняння, приведу приклад конфігурації WLAN на контролерах. Багато хто знає, що CLI на контролерах Cisco мало схожий на звичайну командний рядок Cisco IOS

(привіт Aironet), звичну багатьом. Так ось, коли дивишся на приклад нижче, закрадається думка, що Aruba більше схожа на Cisco IOS.

HPE Aruba

```
aaa profile "tst-dot1x-peap" mac-default-role "employee" authentication-dot1x "ad-users-radius" dot1x-default-role "employee" dot1x-server-group "default" ! wlan ssid-profile "test123" essid "test123" opmode wpa2-aes ! wlan virtual-ap "virt-ap" aaa-profile "tst-dot1x-peap" ssid-profile "test123" vlan 21
```

Cisco

```
config radius auth add 1 1.1.1 1645 ascii secret123 config wlan create 3 test123 test123 config wlan interface 3 users_vlan21 config wlan security wpa akm 802.1x enable 3 config wlan radius_server auth add 3 1 config wlan broadcast-ssid enable 3 config wlan enable 3
```

У плані моніторингу безпеки обидва рішення виглядають добре. Якщо використовувати тільки контролер (без додаткових серверів), Aruba надає більш детальну інформацію. У Cisco даних з моніторингу мережі менше. Пов'язано це як з відсутністю деяких функцій в принципі (наприклад, міжмережевий екран), так і з загальним підходом Cisco, коли для моніторингу бездротової мережі, зберігання статистики, нам пропонують встановити окрему систему (зрозуміло, від Cisco).

У HPE Aruba система управління і моніторингу, звичайно, теж є. Але при цьому в базі багато речей, які у Cisco можна отримати тільки з додатковим сервером. Наприклад, гостьовий доступ з роздруківкою інформації по підключенню, відправкою по пошті, статистика по трафіку (адреси, url, категорії). В останній версії ПО у Aruba з'явилися також можливості проактивного моніторингу трафіку і бездротової мережі.

Тестування безпеки виконаємо за допомогою набору утиліт IPv6 Toolkit SI6, що являє собою набір інструментів оцінки безпеки, розроблений Фернандо Гонт для оцінки стійкості пристроїв IPv6 та функцій захисту IPv6.

Сценарії тестування

Кожен з наступних сценаріїв був розроблений, щоб ілюструвати різні типи вразливостей, пов'язаних з протоколом IPv6. Список сценаріїв ділиться на 4 основні області, які включають розвідувальні атаки, атаки MITM, атаки DoS та виснаження ресурсів потерпілих. Кожен сценарій буде перевірено, використовуючи загальнодоступні набори інструментів аналізу безпеки IPv6 в мережі, що є єдиною мережею IPv6, яка реалізується в лабораторії університету.

Розвідка

Цей сценарій перевіряє відповіді клієнтів у мережі на сканування інструментів, таких як *alive6* або *scan6* . Сценарій буде включати наступні варіанти:

Сканування за допомогою глобальних одноадресних адрес

Сканування за допомогою посилань-локальних адрес

Сканування за допомогою багатоадресних адрес

Людина-в-середині

Цей сценарій випробовує три поширені методи для запуску атаки MITM у локальній та віддаленій мережах. Інструменти для використання в цьому сценарії включають *fake_router26* , *parasite6* , *redir6* , *na6* , *ra6* та *rd6* . Варіанти в цьому сценарії включають:

Напад MITM у локальній мережі з маршрутизатором

Напад MITM у локальній мережі з маршрутизатором за брандмауером

Напад MITM у локальній мережі з брандмауером

Відмова в обслуговуванні

У цьому сценарії проводяться тести DoS-атак на основі повідомлень IPv6 ND, таких як фальшива реклама маршрутизатора, фальшиві відповіді на DAD і запити на виявлення фальшивих сусідів. У цьому дослідженні будуть перевірені атаки Smurf або ICMP з розробленими пакетами. Інструменти для

використання в цьому сценарії включають *ra6* , *rd6* та *fake_router26* . Варіанти в цьому сценарії включають:

DoS через переадресацію ICMPv6

Налаштування мережі IPv6

Тест-серіал, призначений для цього дослідження, складається з двох маршрутизаторів, одного брандмауера, одного перемикача, одного веб-сервера, одного DNS-сервера та DHCP-сервера, двох клієнтів, однієї моніторної машини та одного нападника. На першій установці, на рисунку 3.4.а., локальна мережа має маршрутизатор як шлюз для доступу до зовнішньої.

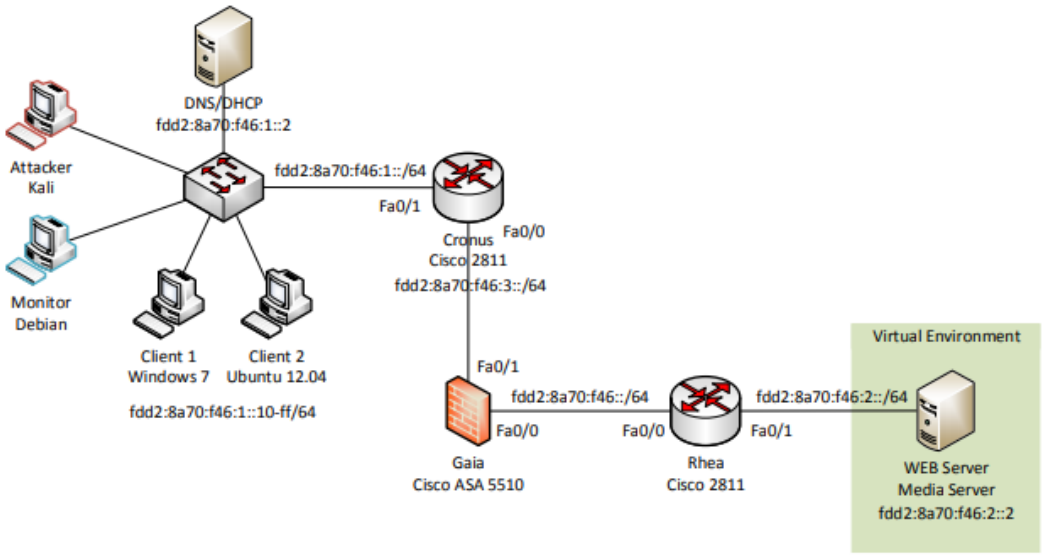

Рисунок 3.4.а Схема для Cisco

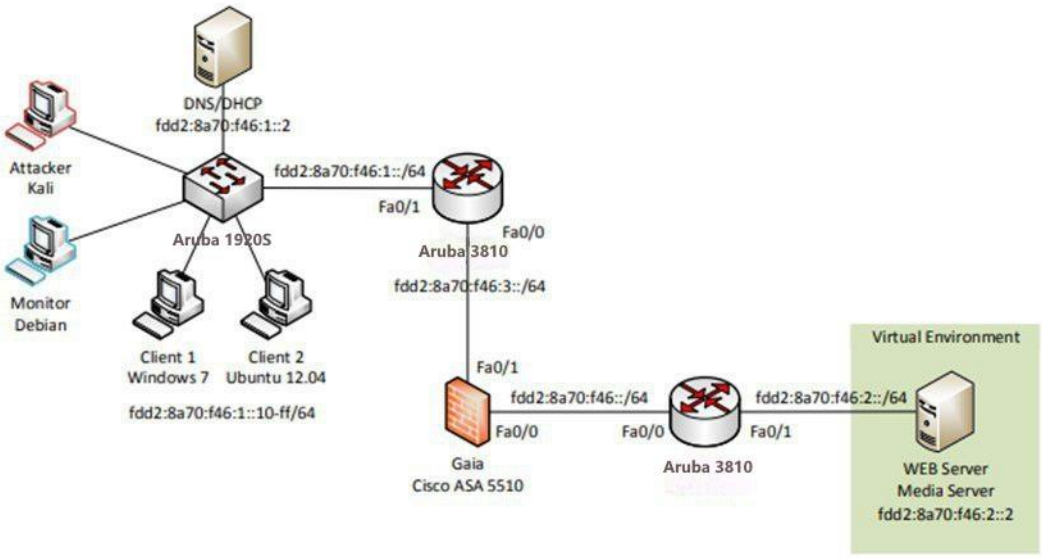

Рисунок 3.4.б. Схема для Aruba

Шлюз у локальній мережі підключається до другого маршрутизатора, який потім підключається до веб-сервера. Другий маршрутизатор і веб-сервер емулюють зовнішню мережу, таку як Інтернет.

Сканування виконаємо наступними командами:

Для Cisco перші два випадки:

```
#  alive6 eth0 fdd2:8a70:0f46:1::0-ff
```

та третій та четвертий для Aruba:

```
#  scan6 -d fdd2:8a70:0f46:1::0-ff -p all -v
```

Результати

З чотирьох клієнтів на яких проводили сканування 3 були в змозі ідентифікувати всі 4 пристрої в локальній мережі.

Проте, коли всі брандмауери вимикалися, обидва інструменти ідентифікували всі пристрої. Використовуючи функції *alive6* сканування займає приблизно 24 хвилини для ідентифікації всіх пристроїв і 25 хвилин для завершення сканування.

Для перевірки результатів scan6 використовувався з різними параметрами.

Рисунок 3.5.а. Результати сканування Cisco

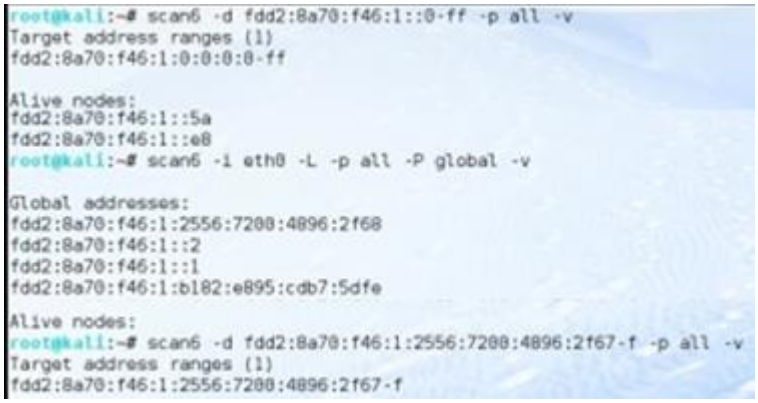

Рисунок 3.5. б. Результати сканування Aruba

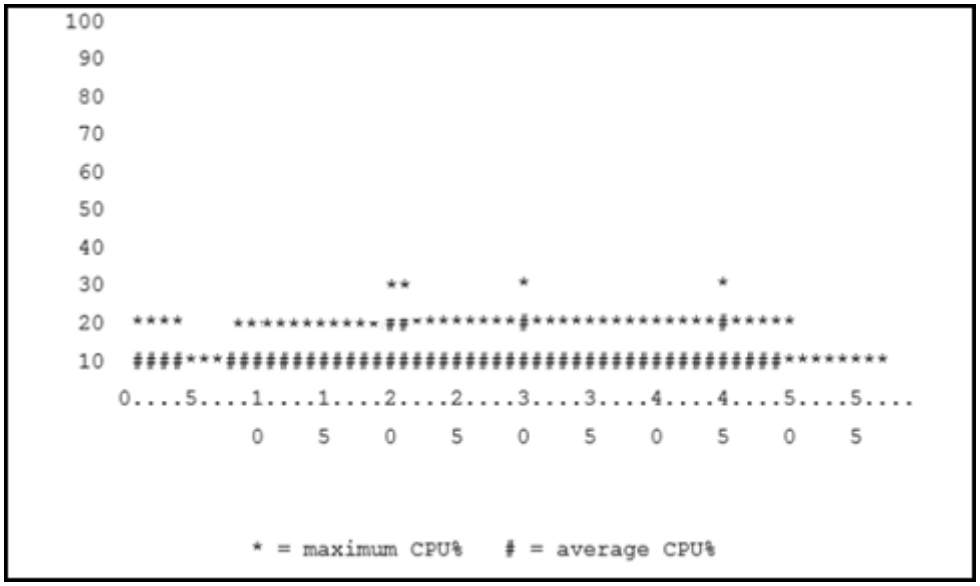

Рисунок 3.6. Завантаження ЦП маршрутизатора Cisco під час атаки

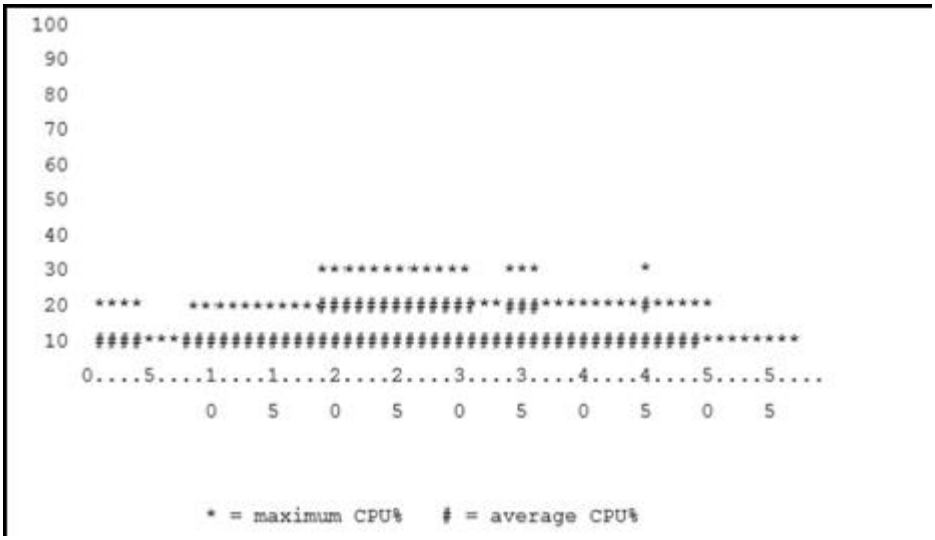

Рисунок 3.7. Завантаження ЦП маршрутизатора Aruba під час атаки

Процедура Smurf атаки

У цьому тесті комп'ютер нападника намагається налаштувати атаку MITM шляхом затоплення реклами фальшивих роутерів у локальній мережі. Атака MITM також перевіряється, коли жертва звернулася до веб-сервера ззовні. Цей сценарій буде перевірено двома різними способами, які включають використання фальшивих рекламних роутерів та повідомлень з переадресацією ICMP.

Атакуючий налаштовується в режимі переадресації, щоб пересилати всі отримані пакети на реальний маршрутизатор і не порушувати зв'язку в мережі.

Для налаштування зловмисника у режимі переадресації використовувались наступні команди для Cisco:

```
redir6 eth0 fe80 :: 31f7: a831: a2b3: 5a08 fdd2: 8a70: 0f46: 2 :: 2 fe80 :: 215: f9ff: fef7: 5949 fe80 :: 224: e8ff: charge7: 7bf8 00: 24: e8: e7: 7b: f8
redir6 eth0 fe80 :: 21a: a0ff: fea4: 4ae9 fdd2: 8a70: 0f46: 2 :: 2 fe80 :: 215: f9ff: fef7: 5949 fe80 :: 224: e8ff: charge7: 7bf8 00: 24: e8: e7: 7b: f8
```

Для Aruba:

```
redir6 eth0 fe80 :: 31f7: a831: 5a08 fdd2: 8a70: 0f46: 2 :: 2 fe80 :: 215: f9ff: fef7:: 224: e8ff: charge7: 7bf8 00: 24: e8: e7: 7b: f8
```

```
redir6 eth0 fe80 :: 21a:8a70: 0f46: 2 :: 2 fe80 :: 215: f9ff:
fef7: 5949 fe80 :: 224: e8ff: charge7: 7bf8 00: 24: e8: e7: 7b: f8
```

До і після кожного тесту на клієнтських комп'ютерах запускаються *ping* та *traceroute* , щоб перевірити шлях пакетів. Крім того, клієнти намагатимуться отримати доступ до веб-сервера після того, як атака MITM працює.

Результати

Коли почалася перша атака, обидва клієнти отримали рекламні повідомлення маршрутизатора та додали IP-адресу до своїх мережевих інтерфейсів. Windows 7 негайно почав використовувати новий маршрутизатор, і на нього було відправлено весь трафік. Результати з Ubuntu 22.09 були переривчасті. У більшості випадків Ubuntu надсилав всі пакети на маршрутизатор. *Ping* та *traceroute* використовувались для перевірки того, що пакети були відправлені через зловмисника. Клієнт відправляв пакети атакуючим і відправляючи пакети на маршрутизатор, і протягом останніх тестів він тільки відправив трафік на маршрутизатор. Трафік проходив лише від одного клієнта до атакуючого і до маршрутизатора, а повертався з маршрутизатора безпосередньо клієнтам.

Випробування доступу до веб-сайту показало, що атака не тільки додає нову IP-адресу, але і змінює параметри мережі в клієнтах. Зокрема, TCP + SYN-пакети, надіслані на початку з'єднання.

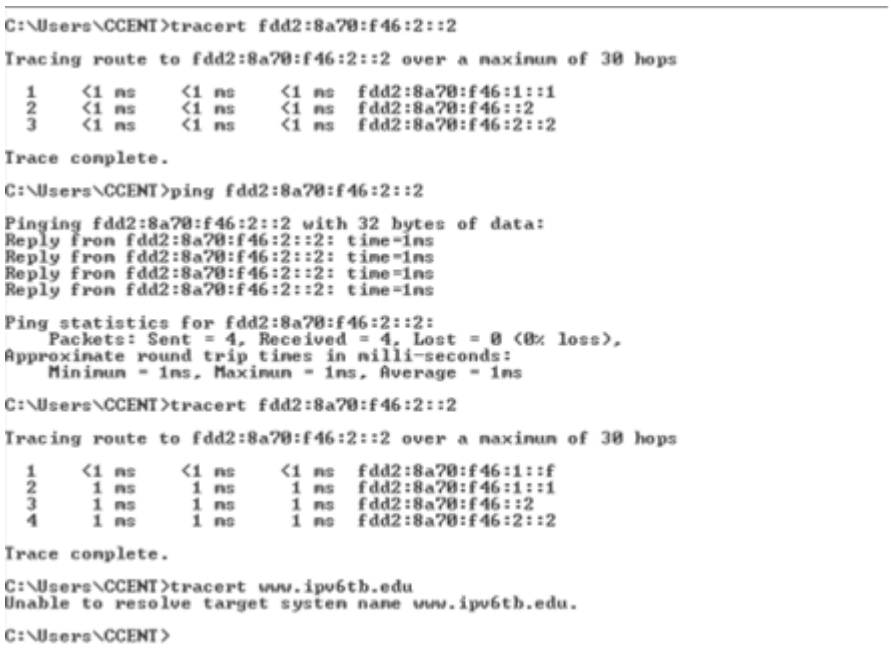

Рисунок 3.8.а: Результати на ПК Windows під час тесту Cisco

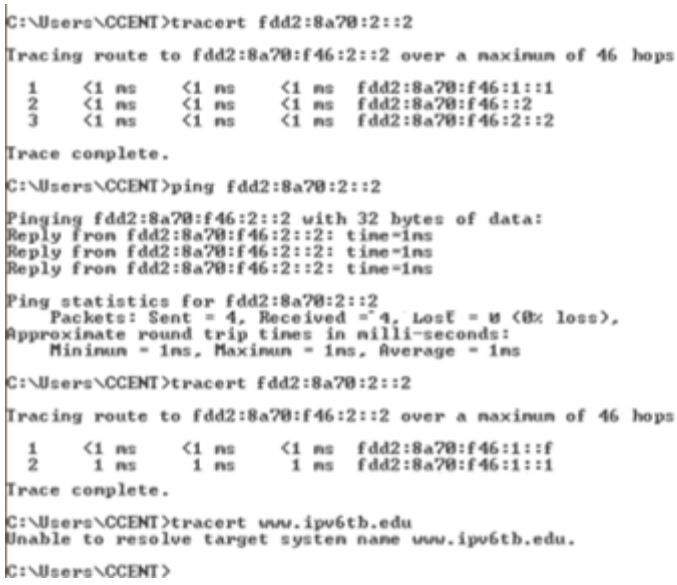

Рисунок 3.8.б: Результати на ПК Windows під час тесту Aruba

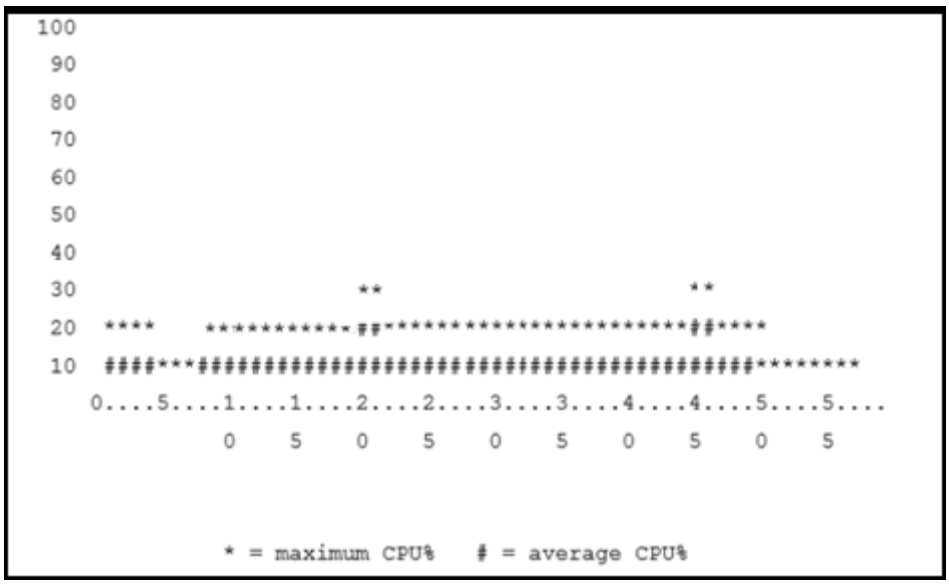

Рисунок 3.9. Завантаження ЦП маршрутизатора Cisco під час атаки

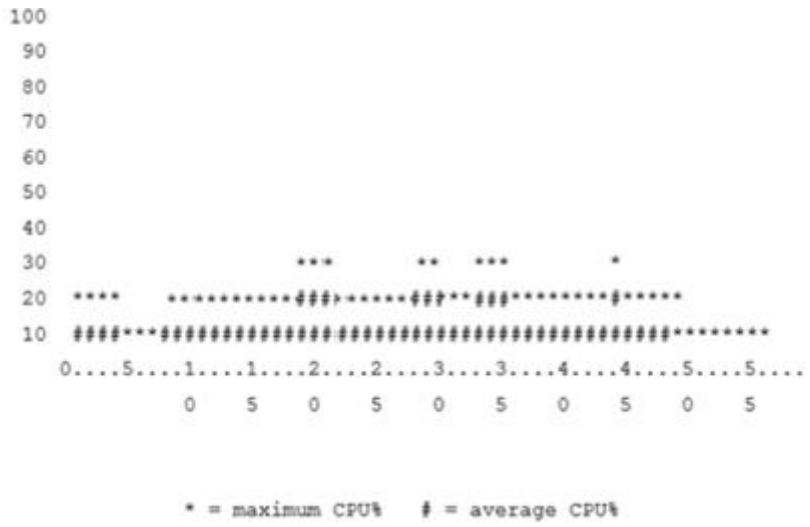

Рисунок 3.10. Завантаження ЦП маршрутизатора Aruba під час атаки

Нарешті, перенаправлення пакетів ICMP, відправлених за допомогою *redir6* , не вплинуло на таблиці маршрутизації клієнтів або їх маршрути. Пакети були отримані, але не вставили новий шлях до таблиць маршрутизації клієнтів.

Цей сценарій свідчить про те, що атаки MITM з використанням фальшивих рекламних роутерів в IPv6 не настільки ефективні, як ARP в IPv4. Незважаючи на те, що *parasite6* виконує підробку сусідів IPv6 (подібно до IPv4 ARP) на IPv6, результати були непослідовними, і сама мережа стала нестабільною. Використання фальшивих рекламних роутерів успішно вводить

фальшивий маршрут у Windows і захоплює трафік, який надсилається зсередини назовні. Це показує, що зловмисник виконував "половину" MITM, оскільки він міг тільки захоплювати вихідний трафік. Це створює прецедент для наступного сценарію, в якому однакове тестування буде виконуватися за допомогою брандмауера як шлюзу.

Процедура заміни повідомлення RA

У цьому тесті комп'ютер нападника намагається налаштувати атаку MITM шляхом затоплення реклами фальшивих роутерів у локальній мережі. Ці оголошення показуюсь атакуючого як маршрутизатора та прямий трафік у мережі до нього. У цьому сценарії DCHP використовується для налаштування маршрутизатора, щоб рекламувати його в своїх пакетах RA.

Нападник налаштовується в режимі переадресації для пересилання всіх пакетів на справжній маршрутизатор і не порушує зв'язку в мережі. Для налаштування зловмисника у режимі переадресації використовувались наступні команди як для Cisco:

```
#  sysctl -w net.ipv6.conf.all.forwarding=1
#  ip route add default via fe80::215:f9ff:fef7:5949 dev eth0
#  fake_router26 -A fdd2:8a70:0f46:1::/64 -a 30 eth0
```

Так і для Aruba:

```
#  sysctl -w net.ipv6.conf.all.forwarding=1
#  ip route add default via fe80::215:fef7:5949 dev eth0
#  fake_router26 -A fdd2:8a70:1::/64 -a 30 eth0
```

До і після кожного тесту на клієнтських комп'ютерах запускаються *ping* та *traceroute* , щоб перевірити шлях пакетів. Крім того, клієнти намагаються отримати доступ до веб-сервера після того, як атака MITM працює.

Перед початком атаки клієнти отримали адресу IPv6 і мали змогу без проблем користуватися веб-сервером, використовуючи його доменне ім'я. Після запуску атаки комп'ютер Ubuntu змінив маршрут за замовчуванням після отримання фальшивих пакетів реклами маршрутизатора та зареєстрував

фальшивий маршрутизатор у своїй таблиці маршрутизації. У всіх тестах, виконаних у цьому сценарії, атака MITM працювала на клієнті Ubuntu. Подібним чином, ПК Windows також почав надсилати трафік зловмисникові після того, як атака була розпочата. Вона зареєструвала атакуючого як маршрутизатора за замовчуванням у своїй таблиці маршрутизації, і до нього був відправлений весь трафік. Команда *traceroute* показала, що спочатку трафік надсилається нападнику, а потім маршрутизатору.

Втрачений трафік на зловмиснику та моніторі показує, що зловмисник може бачити лише вихідні повідомлення, надіслані жертвою. Зловмисник не отримує ніякої відповіді, яка повертається. Крім того, у клієнта Windows, який втратив зв'язок, не вдалося знайти DNS для вирішення імені веб-сервера та не вийшло отримати доступу до нього. Фактична адреса IPv6 веб-сервера використовувалася замість того, щоб зайти на веб-сервер.

```
C:\Users\CCENT>tracert fdd2:8a70:f46:2::2

Tracing route to fdd2:8a70:f46:2::2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  fdd2:8a70:f46:1::f
  2     1 ms     *        1 ms  fdd2:8a70:f46:1::1
  3     *        *        *     Request timed out.
  4     1 ms    <1 ms    <1 ms  fdd2:8a70:f46:2::2

Trace complete.

C:\Users\CCENT>tracert fdd2:8a70:f46:2::2

Tracing route to fdd2:8a70:f46:2::2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  fdd2:8a70:f46:1::f
  2     1 ms     *        *     fdd2:8a70:f46:1::1
  3     *       <1 ms    <1 ms  fdd2:8a70:f46:2::2

Trace complete.

C:\Users\CCENT>
```

Рисунок 3.11.a. Traceroute від клієнта Windows до веб-сервера під час атаки MITM для Cisco

```
C:\Users\CCENT>tracert fdd2:8a70:f46:2

Tracing route to fdd2:8a70:f46:2::2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  fdd2:8a70:f46:1::f
  2     1 ms     *        1 ms  fdd2:8a70:f46:1::1
  3     *        *        *     Request timed out.
  4     1 ms    <1 ms    <1 ms  fdd2:8a70:f46:2:

Trace complete.

C:\Users\CCENT>tracert fdd2:8a70:f46:2:

Tracing route to fdd2:8a70:f46:2::2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  fdd2:8a70:f46:1::f
  2     1 ms     *        *     fdd2:8a70:f46:1::1


Trace complete.

C:\Users\CCENT>
```

Рисунок 3.11.б. Traceroute від клієнта Windows до веб-сервера під час атаки MITM для Aruba

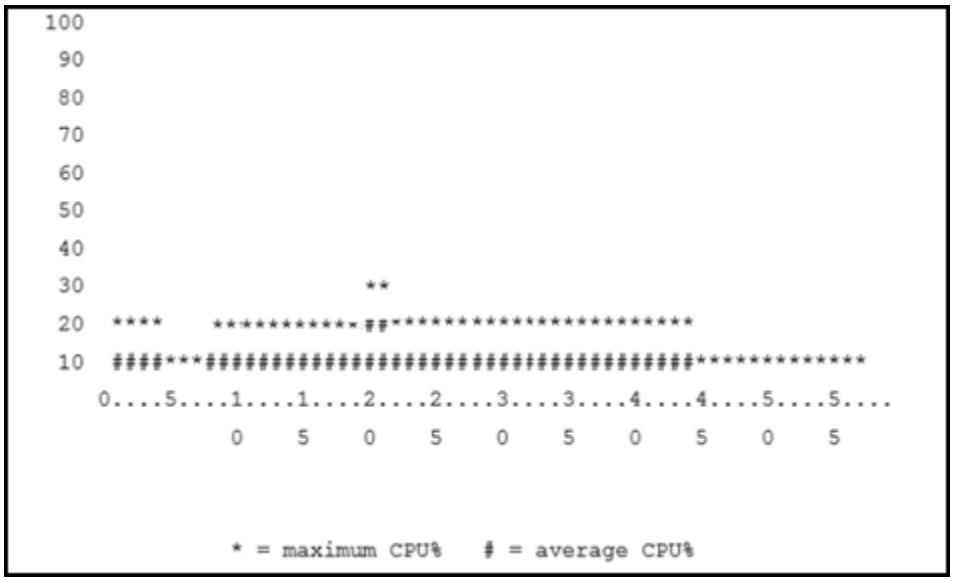

Рисунок 3.12. Завантаження ЦП маршрутизатора Cisco під час атаки

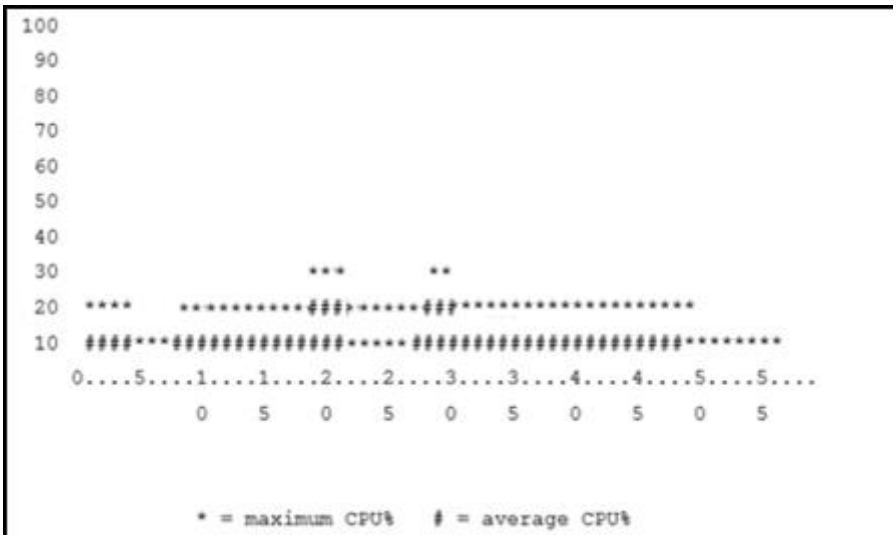

Рисунок 3.13. Завантаження ЦП маршрутизатора Aruba під час атаки

Як і результати, отримані в попередньому сценарії, ці результати показують, що зловмисник може захоплювати трафік, проте він не завершує загальну атаку MITM, оскільки не може прочитати вхідні пакети. Імовірно, що маршрутизатор визначає призначення вхідних пакетів у таблиці сусідів і надсилає пакет прямо до клієнта. Це неможливо підтвердити у захоплених пакетах. Фактично, деякі повідомлення перенаправлення, зроблені за

допомогою Wireshark, дозволяють припустити, що зловмисник може не знаходитися в центрі комунікації. Якщо перша гіпотеза істинна, слід мати брандмауер як шлюз за замовчуванням розірвати з'єднання з клієнтом і відмовитися від атаки MITM. ASA 5510 – це стабільний брандмауер, що відкриває зв'язок із зовнішнім середовищем для клієнта, який його запускає.

Процедура підміни повідомлення NA

У цьому тесті комп'ютер нападника намагається налаштувати атаку MITM шляхом затоплення реклами фальшивих роутерів у локальній мережі. У цьому випадку, враховуючи, що версія IOS у використовуваному брандмауері не підтримує конфігурацію DHCP на пакетах реклами маршрутизатора, SLAAC буде використовуватися без DNS. Тести на веб-сайт зовні виконуються за допомогою адреси IPv6 веб-сервера. Цей сценарій буде перевірений за допомогою фальшивих рекламних роутерів.

Атакуючий налаштовується в режимі переадресації, щоб пересилати всі отримані пакети на реальний маршрутизатор і не порушувати зв'язку в мережі.

Для налаштування зловмисника у режимі переадресації використовувались наступні команди для Cisco:

```
#  sysctl -w net.ipv6.conf.all.forwarding=1
#  ip route add default via fe80::215:c6ff:fefa:470f dev eth0
#  fake_router26 -A fdd2:8a70:0f46:1::/64 -a 30 eth0
```

Для налаштування зловмисника у режимі переадресації використовувались наступні команди для Aruba:

```
#  sysctl -w net.ipv6.conf.all.forwarding=1
#  ip route add default via fe80::215:fef7:5949 dev eth0
#  fake_router26 -A fdd2:8a70:1::/64 -a 30 eth0
```

ICMP-повідомлення переадресації не перевіряються, оскільки вони не дали жодного результату в попередньому сценарії. До і після кожного тесту на клієнтських комп'ютерах запускаються *ping* та *traceroute* , щоб перевірити шлях пакетів. Крім того, клієнти намагаються отримати доступ до веб-сервера після того, як атака MITM працює.

Цей сценарій давав різні результати для кожного клієнта, як це трапилося в попередньому сценарії. Як і в попередньому сценарії, клієнт Windows почав використовувати атакуючого як шлюз за замовчуванням, як тільки почалася атака. З іншого боку, Ubuntu отримав повідомлення PA, створив запис у своїй таблиці маршрутизації, але продовжував використовувати маршрутизатор як шлюз за умовчанням. *Ping* і *traceroute* були успішними в обох випадках. Windows перш за все надіслав всі свої пакети атакуючому. Ubuntu продовжував використовувати маршрутизатор як шлюз за замовчуванням.

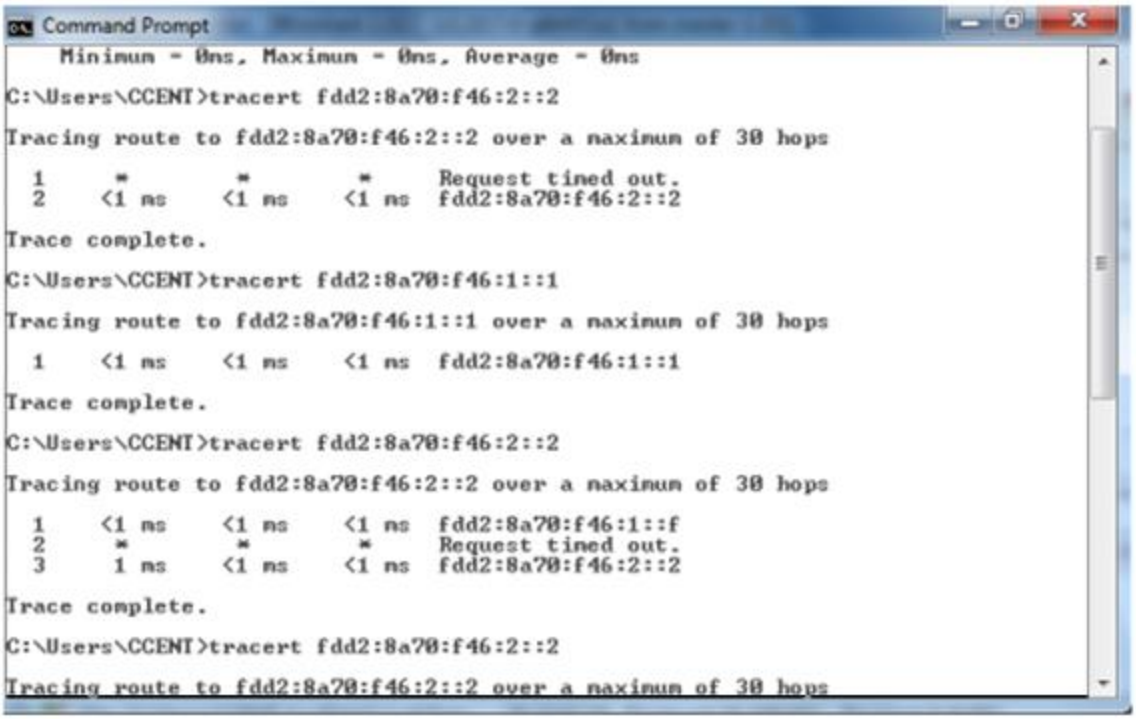

Рисунок 3.14. Traceroute від клієнта Windows під час MITM за брандмауером для Cisco

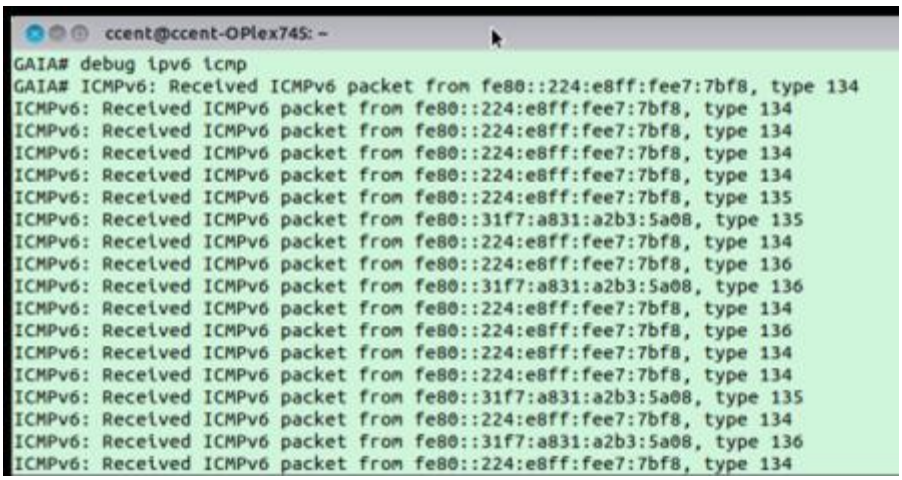

Рисунок 3.15.а. Повідомлення ICMPv6, зняті на брандмауері ASA під час MITM за брандмауером для Cisco

Рисунок 3.15.б. Повідомлення ICMPv6, зняті на брандмауері ASA під час MITM за брандмауером для Aruba

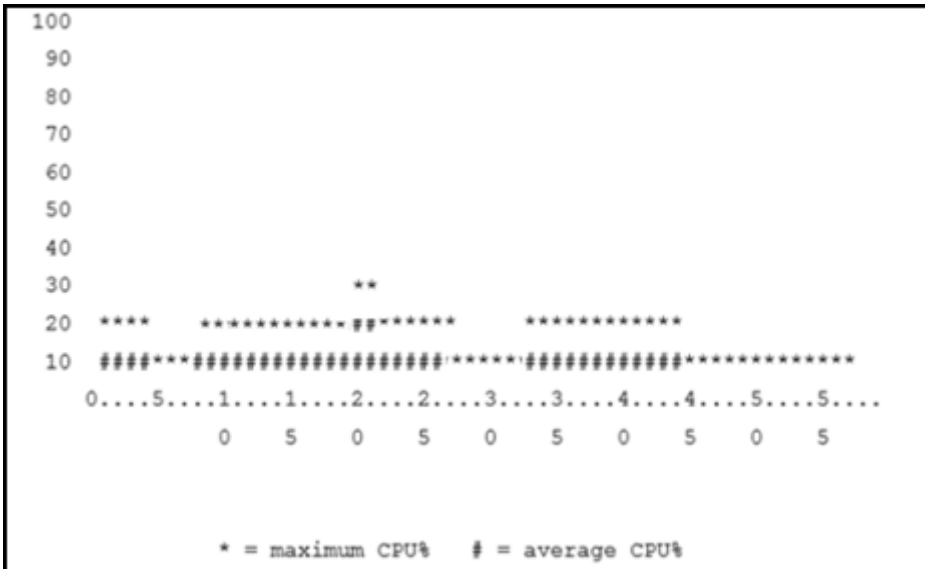

Рисунок 3.16. Завантаження ЦП маршрутизатора Cisco під час атаки

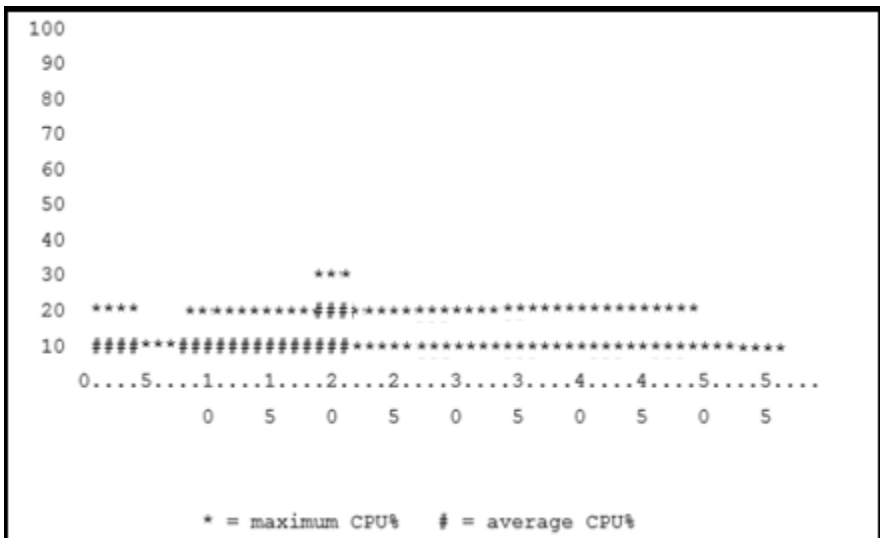

Рисунок 3.17. Завантаження ЦП маршрутизатора Aruba під час атаки

Цей сценарій показав, як працює атака MITM з *fake_router26* . Тестування показало, що брандмауер дозволяє виконувати запити та відповіді за допомогою ехо в цьому сценарії. Цей результат викликав питання про операцію MITM. Подальший аналіз повідомлень, надісланих клієнтом та зловмисником, показує, що зловмисник не пересилає отримані пакети, а замість цього відповідає потерпілому за допомогою ICMP-повідомлення з перенаправленням, що вказує на маршрутизатор. У відповідь жертва повторно передає пакет до шлюзу (у цьому випадку брандмауер), який пересилає пакет назовні. Ось чому брандмауер не порушив з'єднання. Ця поведінка не може бути підтверджена в коробці Ubuntu, оскільки вона відправила всі пакети прямо до брандмауера.

Значна частина атак призводить або до відмови в обслуговуванні, або до перехоплення користувацького трафіку, і у більшості випадків жертвами стають кінцеві пристрої. Більш небезпечними є атаки з використанням заголовків розширення, в результаті яких може відбутись відмова в обслуговуванні на рівні маршрутизаторів, або витік інформації.

Оцінка визначених вразливостей розраховується за основною групою метрик, що в результаті дають числове значення основної оцінки CVSS, оцінки впливу та оцінки вразливості.

Таблиця 3.2. Результати проведеного тестування

Атаки	Внутрішні	Зовнішні	Firewall	Приховані	Розвідка	Наявність			
						вразливості		засобів попередження	
						cisco	Aruba	cisco	Aruba
Розвідка в IPv6 мережі	x	x	x	x	x	+	+	–	–
Smurf атака	x	x				–	–	–	–
Стек заголовків розширення	x		x	x		+	+	–/+	–/+
Підміна повідомлення RA	x		x	x		–	–	–	+
Підміна повідомлення NA	x		x			–	–	–	–
Підміна DHCPv6 сервера	x		x	x	x	–	–	+	+
Вторгнення в тунель	x	x		x	x	+	+	–/+	–/+

Як результат, визначено оцінку рівня ризику вразливості з урахуванням критичності пристрою. Результати представлено у табл. 3.3.

Таблиця 3.3. Оцінки вразливостей

Атаки	Основна оцінка CVSS3	Оцінка впливу	Оцінка вразливості	Оцінка рівня ризику вразливості
Розвідка в IPv6 мережі	0	0	1.2	C
Smurf атака	5.3	2.1	10.7	A
Стек заголовків розширення	4.0	2.6	10.0	B
Підміна повідомлення RA	7.2	6.3	6.5	A
Підміна повідомлення NA	2.1	2.8	3.1	C
Підміна DHCPv6 сервера	7.5	6.9	6.8	A
Вторгнення в тунель	3.0	2.0	10.9	B

За результатами, обладнання Cisco усуває частково вразливості рівня A, залишаються можливими атаки рівня B (стек заголовків розширення та

вторгнення в тунель) та дві атаки рівня С. Це означає, що даний сегмент мережі має середній рівень захищеності.

За результатами, обладнання Aruba усуває вразливості рівня А (підміна повідомлення RA, підміна DHCPv6 сервера) та В (стек заголовків розширення тавторгнення в тунель), але залишається можливими дві атаки рівня С (підміна повідомлення NA та розвідка в IPv6 мережі). Це означає, що даний сегмент мережі має середній рівень захищеності.

Висновок до розділу

Ідеальну систему оцінки вразливостей створити швидше за все неможливо. Навіть в актуальній версії стандарту CVSS 3.0 можуть бути неоднозначні трактування, наприклад, при визначенні важливості приватної інформації. Однак, використання будь-якої версії CVSS в більшості випадків дозволяє правильно розставити пріоритети в обробці вразливостей і оцінити можливі ризики. Найдетальнішу оцінку дозволяє проводити остання версія стандарту. Але якщо в організації вже існує велика база з оцінками, виконаними за попередньою версією CVSS, то перехід на більш сучасну версію може виявитися занадто трудомістким і не принести потрібного результату.

РОЗДІЛ 4. МЕТОДИКА ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ МЕРЕЖІ

Згідно з результатами тестування безпеки Cisco і Aruba мають середній рівень захисту. А отже, вагомої переваги не має жодне мережеве обладнання. З цього слідує, що рівень безпеки залежить не тільки від технічного забезпечення, але і від організаційних заходів.

Для підвищення рівня безпеки кожна організація повинна розробити та впровадити свою політику безпеки.

По-перше, необхідно визнати, що для кожної організації область ІБ має стратегічну важливість, тому вона повинна бути підконтрольна вищому керівництву. По-друге, постачальники ІТ-рішень (як і вендори, що включають інформаційні технології в свою продукцію) повинні надавати такі товари, послуги та рішення, яким замовники зможуть безумовно довіряти.

Завдяки своїй глобальній присутності в сфері забезпечення ІБ компанія Cisco володіє величезною кількістю даних про інтернет-атаки, зараження сайтів, шкідливі програми і активність кіберзлочинності. Це дає унікальну можливість добре розуміти чинники ІБ, що роблять значний вплив на бізнес. Крім того, останніми роками компанія Cisco бере безпосередню участь в аналізі та нейтралізації кожного великого інциденту ІБ.

Завдяки цьому вдалося суттєво удосконалити знання сучасного ландшафту кіберзагроз та зрозуміти, наскільки останнім часом ускладнилися методи, що застосовуються кіберзлочинцями. Недавні звіти Cisco за 2017 рік з інформаційної безпеки містять детальну інформацію про те, наскільки значно просунулися кіберзлочинці в області тіньової економіки і як непросто фахівцям сфери ІБ встигати за зловмисниками.

Найбільше занепокоєння викликає те, що можливості кіберзлочинців безперервно ростуть, особливо в тому, що стосується компрометації систем безпеки та ухилення від виявлення. У першій половині 2015 року візитною карткою зловмисників стало наполегливе прагнення розробляти нові й удосконалювати старі стратегії по ухиленню від систем виявлення. Завдяки

таким тактикам як обфускація (заплутування) коду, кіберзлочинцям часто вдається подолати системи захисту і довгий час непомітно здійснювати шкідливу активність.

У нинішній час організації вже не можуть дозволити собі розглядати ризики ІБ на рівні з іншими бізнес-ризиками. Тому перше, що необхідно змінити, – це відношення до інформаційної безпеки. Важливо, щоб ІБ і супутні ризики перебували під особливим контролем вищого керівництва (ряд директорів, генеральних і виконавчих директорів): в сучасних реаліях необхідний саме такий рівень уваги.

Оскільки сама по собі сфера ІБ зазвичай вищому керівництву погано зрозуміла, потрібні інвестиції в надійні джерела інформації. Такими джерелами можуть стати, наприклад, відповідні правоохоронні органи або приватні експерти. Дуже важливо почати розглядати ризики ІБ окремо від усіх інших ризиків, що враховуються в організації. Потрібно відмовитися від звичних сценаріїв: ті способи, якими ІБ реалізовувалася протягом останніх 20-30 років, стали неактуальні перед обличчям сучасних кіберзагроз.

Вище керівництво організацій потребує розширення своїх уявлень про інформаційну безпеку, і для початку, слід відповісти на наступні питання:

- керівництво організацій має розуміти ризики ІБ приблизно так само, як розуміються фінансові або інші бізнес-ризики в контексті ділових операцій;
- керівники ІТ-напрямків, в свою чергу, повинні вміти дохідливо викладати всі ці міркування, тобто пояснювати, які кошти застосовуються для досягнення поставлених цілей і чому були обрані саме ці кошти.

РОЗДІЛ 5. РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

5.1Опис ідеї технології

Головною ідеєю є графічне представлення моделі мережі на обладнанні вендорів Cisco та Aruba. Ідея проекту – перевірити рівень вразливості мережевого протоколу IPv6 в залежності від виробника обладнання. Це дає можливість в подальшому полегшити вибір для IT-компаній та підприємств під час закупки.

Таблиця 5.1 Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Аналіз та порівняння рівня безпеки мережі на обладнаннях вендорів Cisco та Aruba	Виробники мережевого обладнання	Усунення вразливостей в безпеці мережевого протоколу, можливість бути конкурентноспроможними на ринку IT
	Корпорації, підприємства, data-центри	Безпечне використання мережевого обладнання в своїх цілях на підприємствах

Таблиця 5.2 Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№	Техніко-економічні характеристики ідеї	Продукція конкурентів			W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		MUK Disribution	ERC	MTI			
1.	Широкий вибір мережевого обладнання на складі	+	+	-	Немає	Немає	Склади постійно оновлюються сучасним обладнанням
2	Проектна дистрибуція	+	-	-	Немає	Немає	Кваліфіковані інженери створять конфігурацію під потреб замовника
3	Налаштування обладнання у замовника	+	+	-	Не достатньо досвіду для налаштування	Немає	Спеціалісти гарантують працездатність системи

Конкурентами в Україні являються найбільші дистриб`ютори: MUK Disribution та ERC. В табл. 5.2 наведено аналіз потенційних техніко-економічних переваг ідеї (чим відрізняється від існуючих аналогів та замінників) порівняно із пропозиціями конкурентів.

5.2 Технологічний аудит ідеї проекту

Дану ідею можна реалізувати, використовуючи технології, наведені в табл. 5.3.

Таблиця 5.3 Технології здійснення ідеї проекту

№	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1.	Аналіз та порівняння рівня безпеки мережі на обладнаннях вендорів Cisco та Aruba	Емулятори побудови мережі UNetLab та Iris	Наявна, потребує розширення продуктової лінійки нових моделей	Частина – вільна, частина – за плату
		Використання консольних команд, утиліти Kali Linux	Наявна	Вільна
		WireShark	Наявна	Вільна
Обрана технологія реалізації ідеї проекту:1				

Всі можливі технології реалізації проекту наявні та доступні у вільному доступі, оберемо умулятор Iris для побудови мережі Aruba, так як він містить найбільшу базу обладнання даного вендора та має найкращу сумісність з наступним використанням мережі.

5.3 Аналіз ринкових можливостей запуску стартап-проекту

Визначимо ринкові можливості, які можна використати під час ринкового впровадження проекту, та ринкові загрози, які можуть перешкодити реалізації проекту.

Спираючись на оцінювання нижче, можна зробити висновок, що ринок є привабливим для входження.

Таблиця 5.4. Попередня характеристика потенційного ринку стартап-проекту

№	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	3
2	Загальний обсяг продаж, грн/ум.од	70000
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Немає
5	Специфічні вимоги до стандартизації та сертифікації	Немає
6	Середня норма рентабельності в галузі (або по ринку), %	190%

Тепер визначимо потенційні групи клієнтів, їх характеристики та сформуємо орієнтовний перелік вимог до товару для кожної групи. Результати, наведено у табл. 5.5.

Таблиця 5.5 Характеристика потенційних клієнтів стартап-проекту

№	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Створення нових підприємств, оновлення мережевого обладнання державного сектору	ІТ-компанії, державні установи, банки, сфери послуг через інтернет	Маленькі компанії можуть також бути зацікавлені в наданому функціоналі. Проте потреба не є такою гострою так як вони використовують порівняно невеликі мережі, а отже, потреби в масштабних закупках немає. На відміну від великих компаній, для яких цей функціонал є критичним	Головною вимогою є збереження даних з мінімальною можливістю їх втратити, безпечний обмін інформацією всередині підприємства

Як бачимо, цільовою аудиторією є великі компанії та підприємства, що мають локальні мережі великого розміру та мають обмін даних з віддаленими офісами.

Наступним кроком потрібно проаналізувати ринкове середовище, особливо важливо розуміти можливі загрози, які спричинять конкуренцію на ринку вендорів мережевого обладнання.

У табл. 5.6 розглянемо фактори загроз, що впливають на вибір замовника.

Таблиця 5.6 Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
1	Підвищення складності налаштування	Функціонал надає додаткові можливості до налаштування та вимагає додаткових знань та вмінь з боку мережевого адміністратора	Покращення рівня знань адміністраторів
2	Можливість збільшення часу затримки під час обміну інформацією	Система потребує додаткового сканування і аналізу мережі, в разі виявлення загрози, вона має бути знешкоджена	Горизонтальне масштабування обладнання завдяки безпечному мережевому з'єднанню

Таблиця 5.7 Фактори можливостей

№	Фактор	Зміст можливості	Можлива реакція компанії
1	Безпечне використання мережевих ресурсів	Збільшення кількостів звернень до віддалених офісів через мережевий протокол	Компанія має можливість розвиватись у віддалених куточках
2	Можливість проведення аналізу мережі та відстеження трафіку	Завчасне попередження від можливи атак на мережу підприємства	Підвищення кваліфікації спеціалістів по підтримці мережі

Наступним кроком проведемо аналіз пропозиції.

Таблиця 5.8 Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари замінники
	Extreme Networks	Інші дистриб'ютори	Чехія, Німеччина	Великі компанії, підприємства	Відсутні
Висновки:	Необхідно надавати унікальний функціонал, та покращені алгоритми безпеки мережі	Існує можливість появи нових конкурентів, але незначна, оскільки це складний та тривалий процес	Основні постачальники мережевого обладнання	Клієнти диктують свої умови, а саме безпека та захист даних підприємства	Відсутні

Як бачимо з табл. 5.8, що конкуренція наявна, проте вона не є значною. Даний аналіз мереж має на меті показати можливі недоліки в безпеці мережевого обладнання, тому що конкуренти зосереджують увагу більше на створенні нових моделей, а не на безпеці. Завдяки цьому моє дослідження є корисним для виробників Cisco та Aruba. Саме завдяки проведеним атакам можна зрозуміти, як де необхідне допрацювання.

Таблиця 5.9 Обґрунтування факторів конкурентоспроможності

№	Фактор конкурентоспроможності	Обґрунтування
1	Проектна дистрибуція	Наявність кваліфікованих інженерів дає можливість сформувати ТЗ та запропонувати специфікацію для реалізації проекту у замовника
2	Наявність навчального центру	Отримання сертифікації, підвищення рівня знать у сфері мережевого налаштуваня
3	Широкий вибір мережевого обладнання на складі	Мультивендорний дистрибютор може запропонувати мережеве обладнання від різних виробників зі складу

Таблиця 5.10 Порівняльний аналіз сильних та слабких сторін системи

№	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні з MUK Distribution						
			-3	-2	-1	0	+1	+2	+3
1	Проектна дистрибуція	20	X						
2	Наявність навчального центру	15		X					
3	Широкий вибір мережевого обладнання на складі	15		X					

На основі SWOT-аналізу розробимо альтернативи ринкової поведінки для виведення стартап-проекту на ринок та орієнтовний оптимальний час їх ринкової реалізації з огляду на потенційні проекти конкурентів, що можуть бути виведені на ринок.

Таблиця 5.11 SWOT аналіз стартап-проекту

Сильні сторони (S): – Сумісність з обладнанням інших виробників – Безкоштовна заміна обладнання – Прошивки у відкритому доступі	Слабкі сторони (W): – Ціна мережевого обладнання – Необхідна допомога кваліфікованого інженера при налаштуванні – Складність у підтримці
Можливості (O): – Віддалене управління системами – Горизонтальне масштабування підприємства – Розширення мережі шляхом додавання нового обладнання – Аналіз та контроль безпеки мережі	Загрози (T): – Атаки – Недостатність бюджету – Неправильне налаштування мережі

Таблиця 5.12 Альтернативи ринкового впровадження стартап-проекту

№	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1	Навчання адміністраторів для подальшого управління мережею	Головний ресурс – люди, даний ресурс - наявний	1-3 місяці
2	Реклама	Залучення власних коштів для реклами товару	2-3 місяці
3	Написання статей та опис товару на відомих ресурсах	Головний ресурс – час, даний ресурс - наявний	2-3 тижні
4	Презентація товару на конференціях та інших IT заходах	Ресурс – час та гроші для участі, наявні	1-3 місяці

5.4 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку.

Таблиця 5.13. Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Проектні інженери. Вік: від 18 до 60. Місце проживання: не важливо. Сімейний стан: не важливий. Сфера зайнятості та рівень заробітної плати: IT сфера, від 30 тис. грн.	Даний продукт можна використовувати як засіб побудови мережі	1 коммутатор на 24 порти, 1 маршрутизатор на невелику компанію та середню компанію	Інтенсивність конкуренції в сегменті велика, оскільки більшість конкурентів орієнтовано на великих клієнтів, таких як корпорації та компанії	Сегмент дозволяє вийти на ринок та показати переваги даного продукту у контексті продуктів-аналогів
2	Підприємства. Сфера зайнятості – будь-яка.	Система дозволяє розгортати мережі, аналізувати трафік різного походження та будь-якої ієрархії, тому компанії усіх сфер можуть бути зацікавлені в даному продукті	3-5комутатори, 2 роутера в залежності від розміру підприємства	Інтенсивність конкуренції помірна, залежить від наданого функціоналу товарами замінниками та бажань користувачів	Сегмент дозволяє вийти на ринок та показати переваги даного продукту у контексті продуктів-аналогів
Які цільові групи обрано: IT сфера та великі підприємства, у яких виникає необхідність зберігати та оброблювати великі масиви даних.					

Оскільки цільовою групою виступають компанії та підприємства різних сфер, оберемо стратегію масового маркетингу.

Таблиця 5.14 Визначення базової стратегії розвитку

Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
Надання функціональності що відсутня у товарів-замінників, підтримка клієнтів	Проведення реклами, освітлення унікальної функціональності через інтернет ресурси та інші канали, контакт напряму з споживачами; формування лояльності і прихильності споживачів	Зниження ступеню замінності товару; Прихильність клієнтів; Відмінні властивості товару; Відмінні характеристики товару;	Стратегія диференціації

Таблиця 5.15 Визначення базової стратегії конкурентної поведінки

Чи є проект «першопрохідцем» на ринку	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, які?	Стратегія конкурентної поведінки
Ні, оскільки є товари-замінники, але дані товари замінники не мають деякого необхідного функціоналу	Так, ціль компанії знайти нових споживачів та, частково, переманити існуючих у конкурентів задля задоволення потреб останніх	Компанія частково копіює характеристики товару конкурента, основна ціль компанії розробка нового унікального функціоналу, з підтримкою основного функціоналу конкурентів	Стратегія заняття конкурентної ніші

Таблиця 5.16 Визначення стратегії позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту
1	Відмінні властивості товару	Стратегія диференціації	Унікальність функціоналу;	Надійність Актуальність
2	Підтримка з боку розробника	Стратегія диференціації	Підтримка клієнту; Ліцензії.	Клієнтоорієнтованість
3	Відповідність загальновживаним інтерфейсам	Стратегія диференціації	Підтримка та вдосконалення сучасних всім знайомих інтерфейсів	Стабільність Зручність

Тобто, у якості базової стратегії розвитку було обрано стратегію диференціації та стратегію заняття конкурентної ніші, яка має базову стратегію конкурентної поведінки.

5.5 Розроблення маркетингової програми стартап-проекту

Таблиця 5.17 Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
1	Можливість шифрування даних та тунелювання	Підвищення рівня захищеності даних під час обміну інформацією	Існуючи конкуренти мають меншу швидкість передачі даних
2	Можливість розбиття на локальні мережі	Можливість легкого розгортання кількох локальних мереж	Існуючи конкуренти не мають можливості сканування поточного трафіку
3	Можливість налаштування політик користувачів	Система надає обмежений доступ для певних користувачів	Конкуренти не мають захищеної системи адміністрування

Таблиця 5.18 Опис трьох рівнів моделі товару

<table>
<tr><td>Рівні товару</td><td colspan="3">Сутність та складові</td></tr>
<tr><td>1. Товар за задумом</td><td colspan="3">Розгортання мережі на підприємстві, забезпечення надійного використання інтернету працівниками</td></tr>
<tr><td rowspan="7">2. Товар у реальному виконанні</td><td>Властивості/характеристики</td><td>М/Нм</td><td>Вр/Тх/Тл/Е/Ор</td></tr>
<tr><td>Зручність налаштування</td><td>Нм</td><td>Е</td></tr>
<tr><td>Збільшення швидкості обчислень</td><td>Нм</td><td>Тх</td></tr>
<tr><td>Гнучкість планування ресурсів</td><td>Нм</td><td>Тх</td></tr>
<tr><td colspan="3">Якість: відповідність загальновживаним нормам</td></tr>
<tr><td colspan="3">Пакування: обладнання та супутні комплектуючі з інструкцією</td></tr>
<tr><td colspan="3">Марка: Cisco/Aruba</td></tr>
<tr><td rowspan="2">3. Товар із підкріпленням</td><td colspan="3">До продажу: наявна повна документація, акції на придбання декількох товарів, знижки для певних сегментів на покупку товару</td></tr>
<tr><td colspan="3">Після продажу: додаткова підтримка спеціалістів налаштування, підтримка з боку розробника</td></tr>
<tr><td colspan="4">За рахунок чого потенційний товар буде захищено від копіювання: захист інтелектуальної власності, патент</td></tr>
</table>

Таблиця 5.19 Визначення меж встановлення ціни

Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
інформація відсутня	приблизно 50 тис. грн..	від 30 тис. грн.	10-30 тис. грн

Таблиця 5.20 Формування системи збуту

Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
Отримання продукту	Ліцензії	Нульовий та/або однорівневий	Традиційна

Таблиця 5.21 Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Отримання продукту / функціональності	Електронна пошта, телефон, факс, електронна форма на сайті	Унікальні властивості товару	Привернути увагу клієнтів, освітити унікальну функціональність	Творча та класична
2	Отримання підтримки від компанії		Якісна підтримка	Дати зрозуміти що клієнт може розраховувати на підтримку зі сторони розробника	

В результаті було створено ринкову програму, що включає в себе визначення ключових переваг концепції потенційного товару, опис моделі товару, визначення меж встановлення ціни, формування системи збуту та концепцію маркетингових комунікацій.

Висновок до розділу

В даному розділі було розглянуто стратегії та підходи з розроблення стартап-проекту, визначено наявність попиту, динаміку та рентабельність роботи ринку, як результат, було встановлено, що існує можливість ринкової комерціалізації проекту. Розглянувши потенційні групи клієнтів, бар'єри входження, стан конкуренції та конкурентоспроможність проекту було встановлено, що проект є перспективним. Розглянуто та вибрано альтернативу впровадження стартап-проекту та доведено доцільність подальшої реалізації проекту.

ВИСНОВКИ

Сканер – це перший інструмент, використовуваний зловмисником для виявлення їх жертв та визначення можливих атак на запуск. IPv6 пропонує деякий захист від цих інструментів, хоча це не завжди виявляється надійним засобом. Великий розмір адрес IPv6, доступних для інтерфейсів, ускладнює використання сканерами традиційного способу тестування всіх IP-адрес, що відправляють ICMP-пакети. У першому сценарії, що використовує alive6, цей процес займає так довго часу, що використання його в реальній мережі з префіксом / 64 буде непрактичним.

Використання створеного пакету exo-пакетів ICMPv6, а також простих пакетів echo ICMPv6, є кращим способом пошуку адрес IPv6, що використовуються. Перевага розроблених пакетів полягає в тому, що вони також можуть знайти хости Windows. Під час сканерів один із результатів полягав у тому, що системи Windows не реагують на багатоканальні ехоподібні пакети ICMPv6.

Однак створені пакети створюють відповідь із систем Windows, які можуть використовуватися для сканування мережі. Нарешті, час, необхідний для сканування мережі, використовуючи багатоадресні пакети, є мінімальним.

Тестування повідомлень про рекламу маршрутизації в атаках MITM показує, що спосіб, яким операційні системи обробляють ці пакети, можуть створювати вразливість системи безпеки. У цьому випадку важко призначити відповідальність, оскільки стандарт не вказує, яким чином слід обробляти ці пакети, таким чином операційні системи мають свободу реалізації власних рішень. Як було показано, Windows має деякі проблеми з обробкою цих пакетів.

Виходячи з результатів, робиться висновок, що спосіб обробки повідомлень PA робить різницю між безпечним або небезпечним середовищем. Можливо, що повністю сумісна мережа IPv6, яка використовує IPsec, подолає ці проблеми, однак зараз ОС повинні знайти надійний механізм для перевірки повідомлень RA. Ці рішення можуть передбачати додаткові пакети, що

надсилаються по мережі, перевірка MAC-адреси, встановлення пріоритетів мережі на основі часу або навіть ручна перевірка. Всі ці методи також приносять нові проблеми, які можуть зробити їх непрактичними.

Незважаючи на те, що атаки MITM в IPv6 все ще можливі, їх налаштувати трохи складніше, ніж це робиться в мережі IPv4, коли вузли IPv6 використовують адреси локальної лінії. Однак важливо зазначити, що повна реалізація IPsec в IPv6 дозволить подолати цю проблему, принаймні теоретично, через її процес аутентифікації. Атака MITM не може бути успішною в підключенні IPsec, або, принаймні, це буде складніше для реалізації.

Використання інструмента fake_router26 показало, що атака MITM частково реалізована. Фактично, ця атака перетворює атакуючу машину на сніффер, який фіксує весь трафік, що надходить від жертв, але не може зафіксувати трафік на них. Це відбувається тому, що коли жертва встановлює зв'язок із призначенням, спілкування відбувається лише між ними, а атакуючий не може відстежити трафік у комутованій мережі. Щоб зафіксувати весь трафік, атакуючий повинен або рекламувати іншу мережу, так і виступати як шлюз, або видати себе за маршрутизатор і виконувати роль проксі-сервера.

Випробування показали, що атака MITM також може стати атакою "Відмова в обслуговуванні", оскільки це впливає на конфігурацію DNS мережі з DHCP. Регулярні користувачі намагатимуться отримати доступ до веб-сайту або служби і не зможуть це зробити через атаку. Основною проблемою використання рекламних повідомлень маршрутизатора є те, що жертва перестає слухати DHCP-сервер, і тому не отримує IP-адресу. Це може призвести до зриву роботи корпоративної мережі, яка стає атакою відмови в обслуговуванні.

Наявні відмови в наданні послуг все ще становлять проблему в IPv6. Спосіб, яким операційні системи обробляють пакети RA, не є проблемою лише для атак MITM, а також для атак відмови в обслуговуванні. Велика кількість цих повідомлень примушує жертви використовувати всі свої ресурси при їх обробці та в кінцевому рахунку збої. Незважаючи на те, що різні операційні

системи відрізняються від цих повідомлень, вони, принаймні, повинні обмежувати ресурси, доступні для цього завдання, або встановлювати обмеження на кількість використаних ресурсів. Системи Windows досягли деяких успіхів у цьому полі, але це все ще залишається позаду.

Операційні системи не захищають свої таблиці маршрутизації від підроблених маршрутів, що може призвести до відмови в обслуговуванні при різних ситуаціях. Операційні системи повинні мати можливість ідентифікувати, коли підроблені або недійсні маршрути були введені в їх таблиці маршрутизації підробленими рекламними повідомленнями для маршрутизації. Операційні системи можуть продовжувати додавати декілька маршрутів до своїх таблиць і мати більше одного шлюзу. Ubuntu робить хорошу роботу в цьому відношенні. Windows все ще потребує деяких удосконалень.

Більшість нападів, описаних у цьому звіті, дійсні лише локально, і їхнє охоплення обмежене. Однак, наприклад, в бездротовій мережі ці атаки можуть мати великий вплив і створювати серйозні проблеми. У корпоративних мережах подібні атаки не настільки ефективні, як хочеться хакерам, але все ж таки бездротові мережі, такі як ті, що використовуються в аеропортах чи кав'ярнях, є вразливими, оскільки хакери мають доступ до фізичних носіїв та даних. Користувачам, підключеним до цих мереж та використанням веб-служб, яким потрібна конфіденційна інформація, можуть виникнути проблеми з безпекою, які можуть впливати на їхню інформацію.

Отже, рекомендується продовжити це дослідження, використовуючи деякі ідеї, представлені в даній роботі, як відправну точку для інших тестів, таких як атаки MITM з використанням проксі-сервера або атак DoS і MITM з використанням перенаправлених повідомлень.

ПЕРЕЛІК ПОСИЛАНЬ

1. Aura T. Cryptographically generated addresses (CGA). – 2005.

2. Bagnulo M., García-Martínez A., Azcorra A. Efficient security for IPv6 multihoming // ACM SIGCOMM Computer Communication Review. – 2005. – Т. 35. – №. 2. – С. 61–68.

3. Bos J. W., Özen O., Hubaux J. P. Analysis and optimization of cryptographically generated addresses // Information

4. Bagnulo M., Arkko J. Cryptographically Generated Addresses (CGA) Extension Field Format. – RFC 4581, October, 2006.

Security. – Springer Berlin Heidelberg, 2009. – С. 17–32.

5. Arkko J., Ericsson Ed., Kempf J. Secure neighbor discovery (SEND). – RFC 3971, March, 2005.

6. Combes J. M. et al. CGA as alternative security credentials with IKEv2: implementation and analysis // SAR–SSI'12: 7th Conference on Network Architectures and Information Systems Security. – 2012. – С. 53–59.

7. Bagnulo M. Hash–based addresses (HBA). – 2009.

8. Davies E., Krishnan S., Savola P. IPv6 transition / co-existence security considerations. – 2007.

9. McGann O. IPv6 packet filtering: дис. – National University of Ireland Maynooth, 2005.

10. Krishnan S. Handling of Overlapping IPv6 Fragments. – 2009.

11. Deering S. E. Internet protocol, version 6 (IPv6) specification. – тисяча дев'ятсот дев'яносто вісім.

12. Davies E., Mohacsi J. Recommendations for filtering icmpv6 messages in firewalls. – RFC 4890, May, 2007

13. Gont F., Ermini M., Liu W. Requirements for IPv6 Enterprise Firewalls. – April, 2014.

14. Jankiewicz, E., Loughney, J., and T. Narten, IPv6 Node Requirements, RFC 6434, December 2011.

15. Loughney J. IPv6 node requirements. – 2006.

16. Korver B. The Internet IP Security PKI Profile of IKEv1 / ISAKMP, IKEv2, and PKIX. – 2007.

17. Graveman R. et al. Using IPsec to Secure IPv6-in-IPv4 Tunnels // RFC4891, May. – 2007.

18. Devarapalli V., Dupont F. Mobile IPv6 operation with IKEv2 and the revised IPsec architecture. – 2007.

19. Frankel S., Krishnan S. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. – RFC 6071, February, 2011 року.

20. Bi J. et al. SAVI Solution for DHCP. – May, 2014.

21. McPherson D., Halpern J., Baker F. Source Address Validation Improvement (SAVI) Threat Scope. – 2013.

22. Bagnulo M., Garcia-Martinez A. SEcure Neighbor Discovery (SEND) Source Address Validation Improvement (SAVI). – 2014.

23. Mohacsi J. et al. IPv6 Router Advertisement Guard. – 2011 року.

24. Gont F. Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard). – 2014.

25. IPv6 First-Hop Security Configuration Guide, Cisco IOS Release 15S [Електронний ресурс]: Cisco Systems. – 26 Nov 2012. – Режим доступу: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-s/ip6f-15-s-book .pdf.

ДОДАТКИ

ДОДАТОК А

Схема мережі на обладнанні Cisco

ДОДАТОК Б

Схема мережі на обладнанні Aruba

ДОДАТОК В

Схема попередження вторгнень

ДОДАТОК Г

Схема профілів контролера Cisco та Aruba

ДОДАТОК Д

Схема механізму атаки на процес виявлення маршрутизатора.

Схема механіхму атаки на кеш шлюзу мережі

ДОДАТОК Е

Таблиця результатів проведеного тестування