Хмельницький національний університет
Факультет інформаційних технологій

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система безпеки інформаційної системи від мережевих атак на базі безпечної комп'ютерної мережі відділення Приватбанку у м. Хмельницькому
Назва теми

КРКБ.190102.19.01.03 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *125 «Кібербезпека»*
Шифр, назва

Освітня програма *«Кібербезпека»*
Шифр, назва

Виконав: студент 4 курсу, група КБ-19-1 7.06.23 Гловюк В.С.
Підпис, дата Ініціали, прізвище

Керівник к.т.н., доцент 7.06.23 Джулій В.М.
Підпис, дата Ініціали, прізвище

Нормоконтролер 7.06.23 Мостовий С.В
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки Кльоц Ю.П.
Підпис, дата Ініціали, прізвище

7 06 2023 р.

Хмельницький, 2023

Форма	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
А4		1	КРКБ.190102.19.01.03 ПЗ	Система безпеки	63	
				інформаційної системи		
				від мережевих атак на базі		
				безпечної комп'ютерної		
				мережі відділення		
				ПриватБанку у		
				м. Хмельницькому		
				Пояснювальна записка		
А4		2	КРКБ. 190102.19.01.03 Е8	Аналіз поширених	1	
				мережевих загроз та		
				методів запобігання від них		
А4		3	КРКБ. 190102.19.01.03 Е8	Логічна топологія	1	
				захищеної мережі		
А4		4	КРКБ. 190102.19.01.03 Е8	Загальна схема побудови	1	
				системи захисту		

Зм.	Арк.	№ Докум.	Підпис	Дата	КРКБ.190102.19.01.03 ВП		
Розробив		Гловюк В.С		7.06.23	Система безпеки інформаційної системи від мережевих атак на базі безпечної комп'ютерної мережі Відділення Приватбанку у м. Хмельницькому Відомість проєкту	Літера	Аркуш	Аркушів
Перев.		Джулій В.М		7.06.23		н	1	1
Н. контр.		Мостовий С.В.		7.06.23		ХНУ, КБ-19-1		
Затв.		Кльоц Ю.П.		7.06.23				

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"1" 03 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Главюк В.С.

Прізвище, ім'я, по батькові студента

Тема роботи Система безпеки інформаційної системи від мережевих атак на базі безпечної комп'ютерної мережі Відділення Приватбанку у м. Хмельницькому

Керівник роботи к.т.н., доц. Джулій В.М.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від 01 березня 2023р. №5

2. Строк подання студентом роботи на кафедру 01.06.2023р

3. Вихідні дані до проекту (роботи) спроектувати та реалізувати систему безпеки інформаційної системи від мережевих атак. Передбачити захист від поширених мережевих вразливостей. Вдосконалити існуючі системи запобігання витоку інформації з системи на основі доступних рішень. Вибрати апаратне та програмне забезпечення (обґрунтувати вибір апаратного забезпечення за критерієм простота впровадження – надійність рішення) для моніторингу ті фільтрування мережевого трафіку. Провести аналіз та оцінку захищеності системи від мережевих атак.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Загальний аналіз об'єкта захисту. Реалізація системи захисту мережі. Аналіз ефективності використання системи безпеки. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень): «Аналіз поширених мережевих загроз та методів запобігання від них», «Логічна топологія захищеної мережі», «Загальна схема побудови системи захисту».

6. Консультанти розділів курсового проекту (роботи)

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

7. Дата видачі завдання 1 вересня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів проекту (роботи)	Примі
1	Аналіз предметної області	Січень	–
2	Пошук теоретичної інформації про створення безпечної системи захисту	Січень	–
3	Дослідження існуючих загроз та методів захисту	Лютий	–
4	Постановка задачі	Лютий	–
5	Аналіз теоретичної інформації про методи та сучасні рішення по впровадженню захисту в мережу	Березень	–
6	Початок впровадження та реалізації сучасних методів захисту	Квітень	–
7	Завершення створення системи захисту на базі мережі	Квітень\Травень	–
8	Оформлення пояснювальної записки згідно вимог	Травень	–
9	Оформлення графічної частини	Червень	–
10	Захист КР	08.06.2023	

Студент _____ В.С. Головко
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ _____
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система безпеки інформаційної системи від мережевих атак на базі безпечної комп'ютерної мережі Відділення Приватбанку у м. Хмельницькому».

Автор роботи: Гловюк Володимир Сергійович.

Керівник роботи: Джулій Володимир Миколайович.

Пояснювальна записка: 63 с., 1 додаток, 40 рис., 40 джерел.

Графічна частина: 8 презентаційних слайдів.

ЗАХИЩЕНА СИСТЕМА ВІД МЕРЕЖЕВИХ АТАК, СИСТЕМА БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ, БЕЗПЕЧНА ІНФОРМАЦІЙНА МЕРЕЖА

Мета даної роботи полягає у створенні захищеної інформаційної системи на базі безпечної мережі від атак.

Для досягнення цієї мети було здійснено дослідження предметної області, проаналізовано теоретичну інформацію про проектування захищеної системи інформаційної безпеки, а також створено і розроблену таку систему, яка дозволяє протестувати впровадження певних правил або методів захисту інформації. Для досягнення цих цілей використовувалися різноманітні технології, такі як фірмове програмне забезпечення, спеціальне налаштування апаратного забезпечення, створення відповідних правил фільтрації мережевого трафіку на міжмережевому екрані. Постійний моніторинг стану безпеки мережі та планування заходів з її покращення дозволяє забезпечити надійний захист інформаційної системи від мережевих атак на базі безпечної комп'ютерної мережі.

7.06.2023

ANNOTATION

Course project: «Security system of the information system against network attacks based on the secure computer network of the Privatbank Branch in Khmelnytskyi».

Author of the work: Hloviuk V.S.

Supervisor: Juliy V. M.

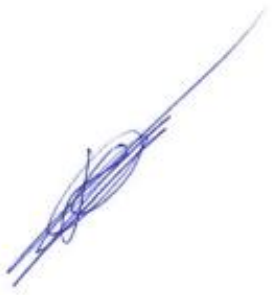
Amount - 63 pages, 1 application, 40 figures, 40 sources.

Graphic part: 8 presentation slides.

The purpose of this work is to create a secure information system based on a secure network against attacks.

To achieve this goal, a study of the subject area was carried out, theoretical information about the design of a protected information security system was analyzed, and a system was created and developed that allows testing the implementation of certain rules or methods of information protection. To achieve these goals, various technologies were used, such as proprietary software, special hardware configuration, creation of appropriate network traffic filtering rules on the firewall. Constant monitoring of the state of network security and planning of measures to improve it allows for reliable protection of the information system against network attacks on the basis of a secure computer network.

7.06.2023



ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІБ - інформаційна безпека

LAN - локальну мережу

CAM - Content Addressable Memory

MAC - Media Access Control

TCP - Transmission Control Protocol

IPS - Information Processing System

DoS - Denial-of-service

CDP - Cisco Discovery Protocol

ARP - Address Resolution Protocol

DHCP - Dynamic Host Configuration Protocol

MitM - Man-in-the-Middle

VLAN - Virtual Local Area Network

ВСТУП

Кібербезпека ніколи не була настільки важливою для економічного процвітання та соціального спокою, як сьогодні. Захист інтелектуальної власності підприємств і особистих даних звичайних громадян є критично важливим. Кіберзлочинці швидші, винахідливіші, краще організовані та оснащені. Фахівці з кібербезпеки постійно виявляють нові загрози та захищаються від нових атак, незалежно від того, чи є це велика компанія або звичайний громадянин. Кібербезпека - це сукупність заходів та технологій, які призначені для забезпечення конфіденційності, цілісності та доступності інформації.

Для всіх вжитих заходів інформаційної безпеки (ІБ). Гонка озброєнь в сфері захисту інформації неминуча.

Сучасні програми безпеки створені для боротьби з традиційними загрозами бізнесу. Але технології розвиваються такими темпами, що стає все важче виявити витоки даних в організаціях.

Створення нових мережевих технологій відразу перетворило традиційні виробничі підприємства в компанії з розробки програмного забезпечення. Вони почали комбінувати інтегроване апаратне забезпечення та ПЗ для підвищення ефективності своїх продуктів, оновлень, простоти використання та ремонтопридатності. Використовувані, як правило, у важливих інфраструктурах - вдома або в корпоративних мережах - ці пристрої надали новий ряд функцій та пристроїв, які полегшують наше життя.

Однак ці «чорні скриньки» несуть нам нові виклики. Вони створені експертами, які думають лише про технічні аспекти, мало інтегровані в системи безпеки. Вони піддають наше життя новим загрозам і забезпечують доступ до інфраструктури, якої раніше не існувало. Такі пристрої практично не контролюються і містять багато вразливостей, тому ми зазвичай не помічаємо втручання в їх роботу. Ці пристрої не враховуються під час виявлення загроз

для організації — часто вони навіть не відображаються в списку пристроїв, які підлягають перевірці внутрішньої безпеки.

Більшість людей не зовсім розуміє, які ризики містять у собі нові пристрої та програмне забезпечення. Прийнято вважати, що якщо вони не містять конфіденційної інформації, то й не критичні для компанії. Насправді зловмисники використовують ці пристрої та ПЗ як приховані канали в мережі, які залишаються непоміченими протягом тривалого часу і ведуть безпосередньо до вразливих даних.

Хоча більшість людей, можливо, і не дуже турбуйтеся про те, що хтось розкриє подробиці того, що саме вони їли на сніданок але, якщо ваш смартфон буде зламаний у тій же мережі, що і ваш холодильник, ви можете позбутися всієї своєї особистої та фінансової інформації і вона буде доступна зловмиснику.

1 ЗАГАЛЬНИЙ АНАЛІЗ ОБ'ЄКТА ЗАХИСТУ

1.1 Характеристика предметної області

Розвиток технологій і збільшення кількості користувачів Інтернету призвели до появи нових загроз безпеці мережі. Це вимагає постійного вдосконалення заходів і технологій забезпечення безпеки комп'ютерних систем і мереж.

У сучасному світі кібербезпека є критично важливим елементом бізнесу, державного управління, наукових досліджень і особистого життя людей. Це впливає на розвиток усієї економіки та суспільства. Тому питання кібербезпеки є актуальним і важливим для всіх сфер діяльності.

За даними Statista, у 2020 році більше 70% підприємств у США мали власний веб-сайт. В той же час, на початку 2021 року компанія Visual Objects провела дослідження, згідно з яким лише 60% малих підприємств мали власний веб-сайт. Тому можна припустити, що загальний відсоток бізнесів з власним сайтом, наразі становить близько 60-70% від усіх підприємств.

Згідно з даними компанії Cisco, у 2020 році більше 90% всіх підприємств у світі мали деякий рівень мережевої інфраструктури, наприклад, локальну мережу (LAN) або бездротовий доступ (Wi-Fi). Водночас, за даними дослідження, проведеного компанією Spiceworks у 2019 році, понад 80% малих підприємств у США мали власну мережу.

Враховуючи інші державні чи приватні підприємства, яким немає потреби мати власний сайт, можна зробити висновок, що майже усі підприємства мають власну комп’ютерну мережу. І питання її захисту стоїть навіть вище ніж захисту веб сайту.

Для захисту від атак на мережу, потрібно розуміти як працює мережа. Чим краще спеціаліст розуміє, як влаштована і функціонує звичайна мереж, тим простіше буде захистити її від перехоплення, аналізу і експлуатації вразливостей. Крім того, важливо вести системний моніторинг мережі з метою

виявлення аномалій і несподіваних подій, які можуть свідчити про атаку на мережу. Загалом, знання про мережеву інфраструктуру та безпеку є ключовими для розуміння загроз і захисту від них. Далі потрібно проаналізувати основні концепції з якими спеціалісти з кібербезпеки стикаються щодня. Крім того, спеціалісти з інформаційної безпеки повинні бути ознайомлені з різними методами атак на мережі, які можуть бути використані для перехоплення, редагування або підробки даних, а також для доступу до незаконних ресурсів.

Мережа - це два або більше комп'ютери, пов'язані між собою з метою обміну даними та ресурсами. Комп'ютерні мережі можуть бути декількох видів:

— локальна мережа - це мережа, яка може складатись з комп'ютерів чи інших мережевих пристроїв, що знаходяться в межах одного фізичного простору, наприклад офісу, школи чи університету;

— глобальна мережа - це комп'ютерна мережа, яка охоплює великий регіон, наприклад місто, країна чи континент.

Як показано на рисунку 1.1, усі мережі складаються з вузлів. Таку назву дали спеціально, щоб її можна було б застосувати до більш широкому кругу пристроїв.

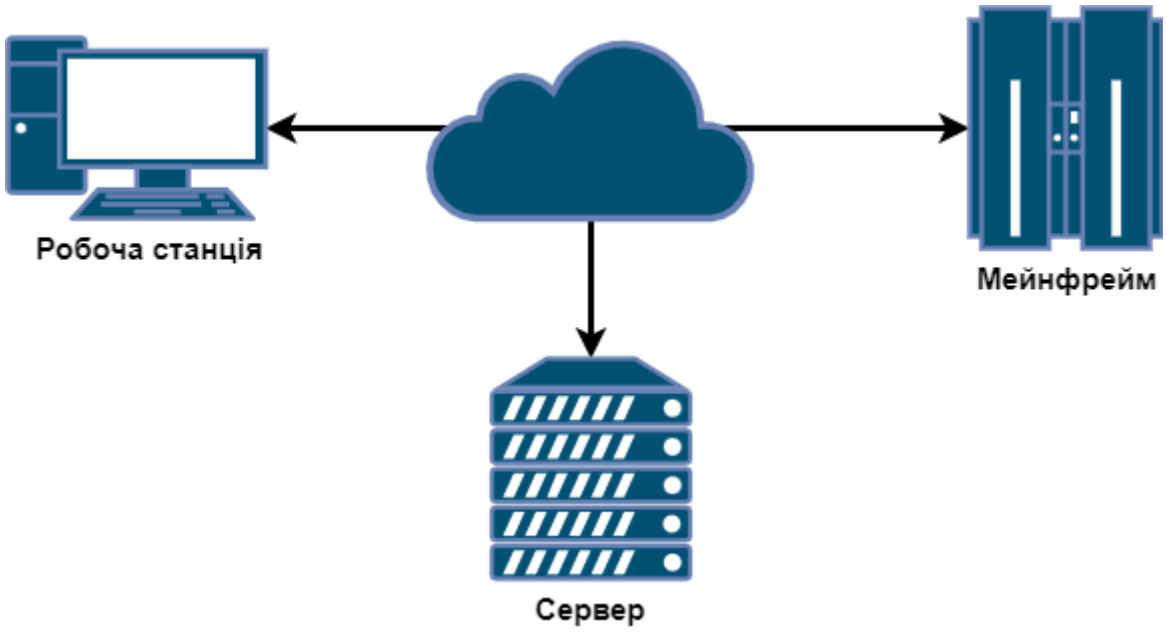


Рисунок 1.1 - Приклад простої мережі

На рисунку 1.1 показані три вузли, підключених до однієї мережі. В кожного такого вузла може бути своя операційна система чи інше обладнання.

Але так як кожен з цих вузлів слідує певним набором загальних правил, або мережевим протоколам, вони можуть безперешкодно взаємодіяти між собою. Щоб ці вузли розуміли один одного і без проблем могли обмінюватись даними, усі вони повинні використовувати одні мережеві протоколи.

Мережеві протоколи виконують багато різних функцій, включаючи декілька наступних:

— форматування та кодування даних - це процеси, які допомагають пристосувати дані для передачі через мережу. Часто дані не знаходяться у відповідному форматі для передачі через мережу, і тому їх потрібно форматувати та кодувати. Протокол може надавати різні методи кодування для правильної передачі даних, наприклад, конвертування тексту англійською мовою в двійковий формат;

— управління потоком даних - це процес контролю обсягу даних, що передаються через мережу. Протоколи можуть використовувати методи управління потоком даних для збільшення пропускної здатності та зменшення затримки. Це досягається шляхом регулювання кількості даних, які можуть бути передані на певний інтервал часу;

— підтримка стану сеансу - це процес збереження інформації про поточний стан з'єднання між двома пристроями під час передачі даних через мережу. Зазвичай протоколи використовують механізми для створення нових з'єднань та завершення вже існуючих, щоб управляти процесом обміну даними між ними;

— виявлення та виправлення помилок - це процес контролю якості передачі даних через мережу. Багато мереж не є повністю надійними, тому дані можуть бути пошкоджені під час передачі. Важливо виявити такі пошкодження і, якщо можливо, виправити їх. Для цього протоколи можуть використовувати різноманітні механізми перевірки цілісності даних, наприклад, контрольні суми

або коди корекції помилок;

— ідентифікація вузлів за допомогою адресації - це процес передачі даних на вірний вузол. Для ідентифікації конкретних вузлів або груп вузлів деякі протоколи використовують механізм адресації. Цей механізм надає можливість встановлювати унікальні адреси для кожного вузла, які дозволяють ідентифікувати та направляти дані до відповідного вузла;

— забезпечення послідовності передачі даних - це проблема, з якою стикаються багато мереж, оскільки вони не можуть гарантувати, що порядок надсилання даних буде відповідати порядку отримання. Протоколи передачі даних, такі як TCP (Transmission Control Protocol) [1, 2], використовують спеціальні механізми керування потоком та виявлення помилок для забезпечення правильної передачі даних у відповідності до послідовності. Крім того, вони використовують механізми підтвердження отримання даних, що дозволяє відправнику впевнитися, що дані успішно доставлені. Тим не менш, у деяких випадках зміна порядку даних може бути корисною. Наприклад, якщо певний пакет даних має вищий пріоритет, ніж інші пакети даних, його можна розмістити в початку черги та передати раніше за інші пакети. Це може бути корисно для гарантування того, що важливі дані будуть оброблені найпершими та не затримуються через велику кількість інших пакетів, які потрібно передати.

IPS (Information Processing System) складається з рівнів, де кожен рівень базується на попередньому і може інкапсулювати дані від рівня вище для того, щоб ці дані могли бути передані між рівнями. Кожен рівень обробляє блок даних протоколу (PDU), який передається від рівня, що стоїть вище.

Маршрутизація в мережі. Ethernet потребує, щоб всі вузли були підключені до однієї локальної мережі. Така вимога стає досить серйозною перешкодою для великих чи глобальних мереж, адже неможливо фізично зв’язати усі вузли один з одним. Однак, застосування адресації відправника та отримувача дозволяє маршрутизувати [3, 4] дані через різні мережі до досягнення необхідного пристрою-отримувача (рисунок 1.2).

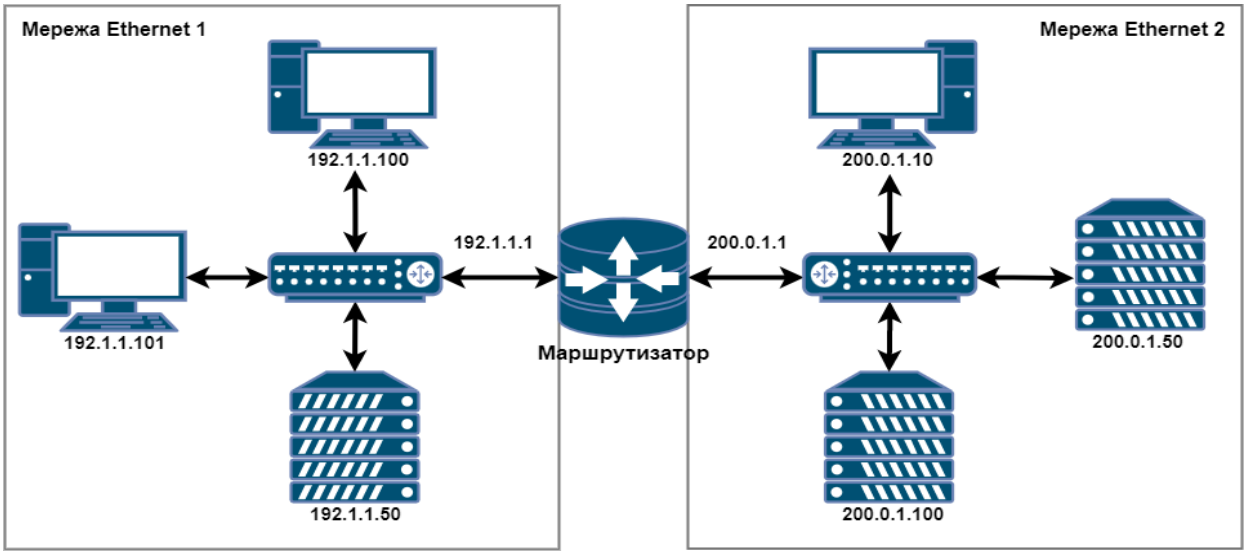


Рисунок 1.2 - Приклад мережі з маршрутизацією, що з'єднує дві мережі Ethernet

На рисунку видно дві мережі Ethernet, кожна з яких має окремі діапазони IP-адрес. У такому випадку, щоб передати дані з одного вузла першої мережі до іншого вузла в іншій мережі система робить наступні кроки:

— у першій мережі операційна система персонального комп'ютера має вузол мережевого стеку, який здійснює інкапсуляцію даних прикладного та транспортного рівнів і формує IP-пакет з вказаною адресою відправника - 192.1.1.101 та адресою одержувача - 200.0.1.50;

— якщо стеку необхідно відправити кадр Ethernet, але IP-адреса призначення не існує в жодній мережі Ethernet, до якої підключено вузол, то стек використовує таблицю маршрутизації операційної системи. В даному випадку таблиця маршрутизації містить запис для IP-адреси 200.0.1.50, що показує, яким шляхом можна дістатись до цієї адреси призначення через маршрутизатор з IP-адресою 192.1.1.1 [5];

— далі для того, щоб знайти MAC-адресу маршрутизатора з адресою 192.1.1.1, операційна система використовує протокол ARP. Після отримання MAC-адреси, вихідний IP-пакет інкапсулюється в кадр Ethernet з вказаною MAC-адресою;

— після отримання кадру Ethernet, маршрутизатор розпаковує IP-пакет та перевіряє його IP-адресу призначення. Якщо адреса не відповідає адресі маршрутизатора, то він визначає, що IP-пакет має бути переданий іншому вузлу в іншій підключеній мережі. Маршрутизатор знаходить MAC-адресу вузла з IP-адресою 200.0.1.50, інкапсулює вихідний IP-пакет у новий кадр Ethernet з цією MAC-адресою і надсилає його до відповідної мережі;

— і в результаті кадр Ethernet дістається до вузла призначення, він розпаковує IP-пакет та обробляє його вміст.

Процес маршрутизації може повторюватися декілька разів, якщо маршрутизатор не може прямо підключитися до вузла з IP-адресою 200.0.1.50 у мережі. У цьому випадку, він перевірить свою таблицю маршрутизації та знайде наступний маршрутизатор, до якого можна направити IP-пакет.

Очевидно, що визначення шляху до кожного вузла мережі окремо стало б непрактичним завданням. Тому, коли для конкретного призначення немає запису в таблиці маршрутизації, операційна система створює запис за замовчуванням, який містить IP-адресу маршрутизатора, через який можна передавати IP-пакети до даного призначення.

1.2 Аналіз відомих мережевих загроз

Внутрішня мережева атака - це атака зсередини мережі, тобто від користувачів, які вже мають доступ до мережі. Ці особи можуть бути співробітниками компанії, партнерами або навіть хакерами, які викрадають дані, щоб отримати доступ.

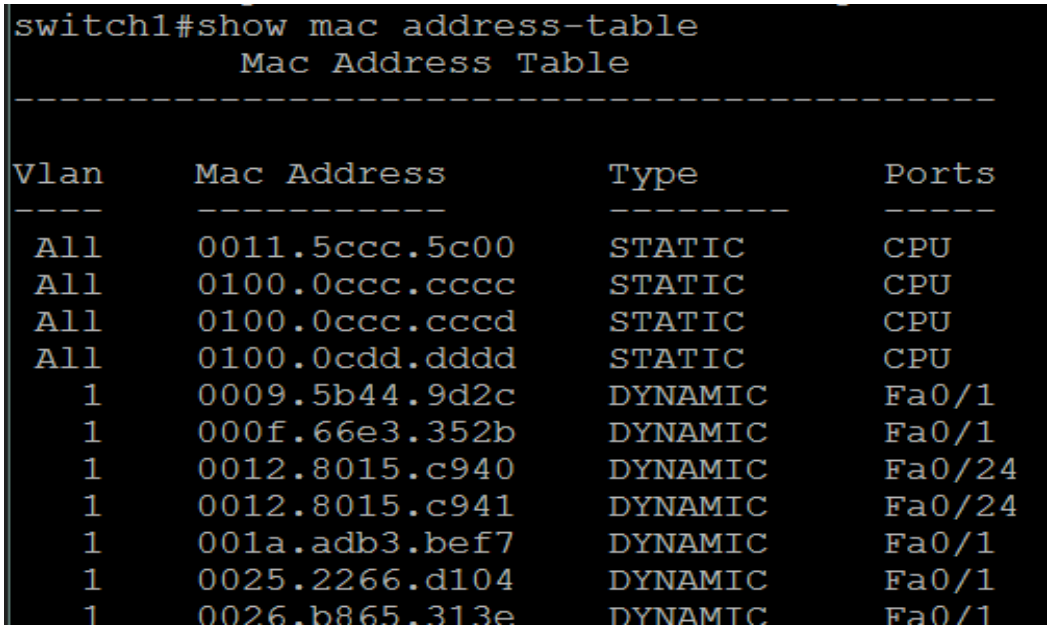
Ці типи атак можуть бути дуже небезпечними, оскільки користувачі вже мають доступ до мережевих ресурсів і можуть використовувати свій доступ для здійснення злочинних дій, таких як крадіжка даних, зміна конфігурацій або збій систем.

Щоб запобігти внутрішнім атакам на мережу, необхідно звернути увагу на такі аспекти, як контроль доступу, моніторинг активності користувача та його поведінки в системі, захист даних для запобігання несанкціонованому доступу та використання зашифрованих методів захисту даних. Крім того, необхідно навчати користувачів правилам безпеки, щоб вони розуміли ризики атак зсередини мережі [10].

Протокол CDP - це протокол, який розробила компанія Cisco Systems, є пропрієтарним і призначений для виявлення сусідніх пристроїв і отримання інформації про них [6, 7]. Цей протокол працює на канальному рівні в моделі OSI і дає можливість обмінюватись спеціальними даними про характеристики пристроїв, таких як тип, номер порту, модель, IP-адреса чи операційна система. Цей протокол може бути корисним при аналізі трафіку в мережі, налаштуванні параметрів пристроїв чи пошуку та усуненні несправностей. Але так як цей протокол є пропрієтарним то він не може використовуватися на пристроях від інших виробників.

CDP flooding - це атака при якій зловмисник надсилає багато фальшивих CDP - пакетів на широкомовний адрес і таким чином займає всю доступну пропускну здатність на лінії. Така атака може призвести до зниження продуктивності мережі або відмови у роботі мережевих пристроїв [8, 9].

У локальних мереж (LAN) використовуються комутатори, які мають таблицю Content Addressable Memory (CAM) (рисунок 1.3). Вона використовується для встановлення відповідності окремих MAC-адрес (Media Access Control) в мережі до фізичних портів на комутаторі [11, 12]. Таблиця CAM дозволяє комутатору направляти дані з фізичного порту безпосередньо до отримувача, у відміну від хаотичної широкомовної передачі даних з усіх портів, яка є характерною для концентраторів. Основна перевага цього методу полягає в тому, що дані пов'язуються з сегментом мережі, який містить комп'ютер, для якого ці дані призначені [13].



```
switch1#show mac address-table
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0011.5ccc.5c00    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0009.5b44.9d2c    DYNAMIC     Fa0/1
   1    000f.66e3.352b    DYNAMIC     Fa0/1
   1    0012.8015.c940    DYNAMIC     Fa0/24
   1    0012.8015.c941    DYNAMIC     Fa0/24
   1    001a.adb3.bef7    DYNAMIC     Fa0/1
   1    0025.2266.d104    DYNAMIC     Fa0/1
   1    0026.b865.313e    DYNAMIC     Fa0/1
```

Рисунок 1.3 - Приклад записів в таблиці CAM комутатор

Атака, при якій здійснюється отруєння таблиці комутатора CAM, є зловживанням, яке призводить до пошкодження записів у таблиці комутатора. Це призводить до перенаправлення мережевого трафіку від очікуваних хостів. Таке зловживання може створити ситуацію DoS (відмова в обслуговуванні), оскільки комутатор стає нездатним пересилати пакети до їх реальних та законних місць призначення.

Усі атаки які будуть перераховані націлені в основному на канальний рівень. MAC poisoning (також може бути відома під назвою MAC spoofing) та MAC flood є двома досить різними атаками на мережу:

— MAC poisoning - це техніка, яка застосовується зловмисниками для того щоб змінити свій MAC-адрес на MAC-адрес іншого користувача в мережі. Ця атака дає змогу підробити ідентифікацію та згодом виконувати дії в мережі від імені легітимного користувача. Призводить до перехоплення трафіка;

— MAC flood - інша атака, яка дозволяє заповнити таблицю комутації мережевого комутатора фальшивими MAC-адресами, що в результаті переповнює її [14]. Внаслідок чого, комутатор стає нездатний правильно направляти мережевий трафік до правильних портів, що одразу призводить до

відмови в обслуговуванні(DoS).

Обидва ці атаки мають великий потенціал викликати значні проблеми з безпекою мережі.

Наступним протоколом який може підпасти під атаку є ARP. Цей протокол використовується для зіставлення MAC-адрес з IP-адресами, щоб пакети могли передаватись по локальній мережі. Мережеві пристрої обмінюються пакетами протоколу ARP, коли один хост знає IP-адрес віддаленого хоста і хоче визначити MAC-адрес цього самого віддаленого хоста.

Атака з отруєнням ARP-кеша є злочинною дією введення не справжнього IP-адреса в зіставлення MAC-адрес в ARP-кеші іншого кінцевого пристрою (рисунок 1.4). Це може бути зроблено шляхом прямої маніпуляції кешем ARP цільового пристрою незалежно від повідомлень ARP, відправлених цільовим хостом. Для цього зловмисник може або добавити новий підроблений запис в кеш ARP цільового, або оновити вже існуючий запис фальшивим IP-адресом і MAC-адресую [15].

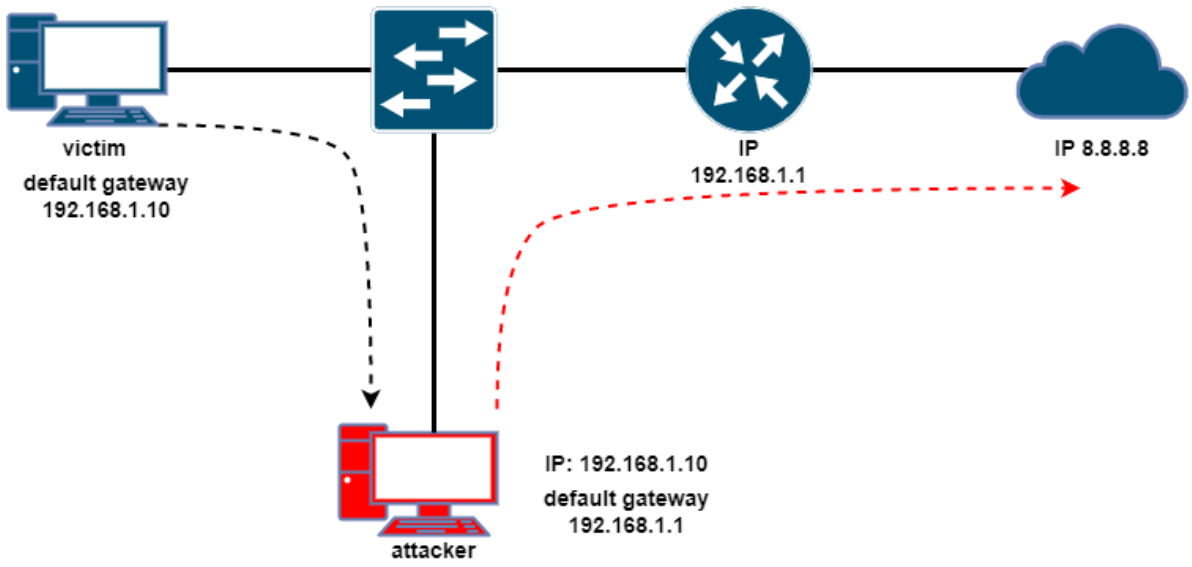


Рисунок 1.4 - Приклад записів в таблиці CAM комутатор

Ці два методи можуть бути пояснені наступним чином:

— створення нового фальшивого запису - для цього до цільового хоста

відправляється повідомлення запиту ARP з підробленими IP-адресами джерела та MAC-адресами в заголовку ARP. Коли цільовий хост отримує повідомлення запиту ARP, він припускає, що з'єднання має бути встановлене і потім створює новий запис у своєму кеші ARP, використовуючи підроблені адреси джерела (IP та/або MAC), надані у заголовку ARP-повідомлення [16];

— оновлення запису із не справжніми адресами - Для цього цільовому хосту надсилається запит ARP або відповідне повідомлення з фальшивими IP-адресами та MAC-адресами. Таким чином, навіть якщо запис уже існує в кеші ARP цільового хоста, він буде оновлений за допомогою використання фальшивих IP/MAC-адрес.

Ще однією областю дослідження стане протокол мережевого рівня. DHCP (Dynamic Host Configuration Protocol) - це протокол, який використовується для автоматичного налаштування IP-адрес, мережевого шлюзу та інших налаштувань для стабільного мережевого з’єднання на комп’ютерах. DHCP дозволяє значно зменшити людські зусилля при налаштуванні та масштабуванні мереж, так як замість того щоб налаштовувати кожен вузол окремо власноруч, можна налаштувати лише сервер DHCP, і всі комп’ютери автоматично будуть отримувати необхідні параметри під час роботи мережі.

Існує декілька видів атак на DHCP. Перша - це DHCP Starvation (рисунок 1.5). Ця атака заснована на проведенні розсилок величезної кількості повідомлень DHCPDISCOVER з метою виснаження адресного простору на сервері DHCP. Сервер DHCP буде реагувати на кожен запит і видавати IP-адресу. Після переповнення допустимого адресного простору сервер DHCP більше не зможе обслуговувати нових клієнтів у своїй мережі, надаючи їм IP-адреси [17, 18].

Другий вектор атак на DHCP вимагає розгорнути зловмисний DHCP-сервер. Потрібно це, щоб видавати клієнтам підроблені мережеві параметри (зокрема адресу шлюзу за замовчуванням) і провести MitM. З точки зору

атакуючого, для цього найкраще насамперед «покласти» легітимний DHCP-сервер, що ми, власне, і зробили вищим.

Рисунок 1.5 - DHCP Starvation Attack

Атаки, які були перераховані це не усі з існуючих а тільки найпоширеніші. Також завжди є можливість попасти під атаку віддаленого виконання коду. Це ти вразливості коли зловмисник може запускати зловмисний код в контексті програмного забезпечення. Також часто компанії втрачають активи через вразливість обхід автентифікації чи авторизації. Тому створення захищеної мережі буде охоплювати більшість з усіх можливих вразливостей [19].

1.3 Обґрунтування вибору додаткових програмних рішень

Перш ніж приступати до тестування вразливостей потрібно визначитись з додатковим програмним забезпеченням.

GNS3 - це спеціальне програмне забезпечення для моделювання мережевих топологій, що дозволяє розробити віртуальні мережі на основі реальних конфігурацій мережевого обладнання. GNS3 являється популярною графічною з відкритим вихідним кодом крос-платформною утилітою (рисунок 1.6). Вона заснована на раніше розробленій Pemu (cisco pix емулятор), Dynamips

(емулятор cisco ios), Dynagen (текстовий інтерфейс для вже згаданої Dynamips). GNS3 надає легкий для розуміння графічний інтерфейс [20].

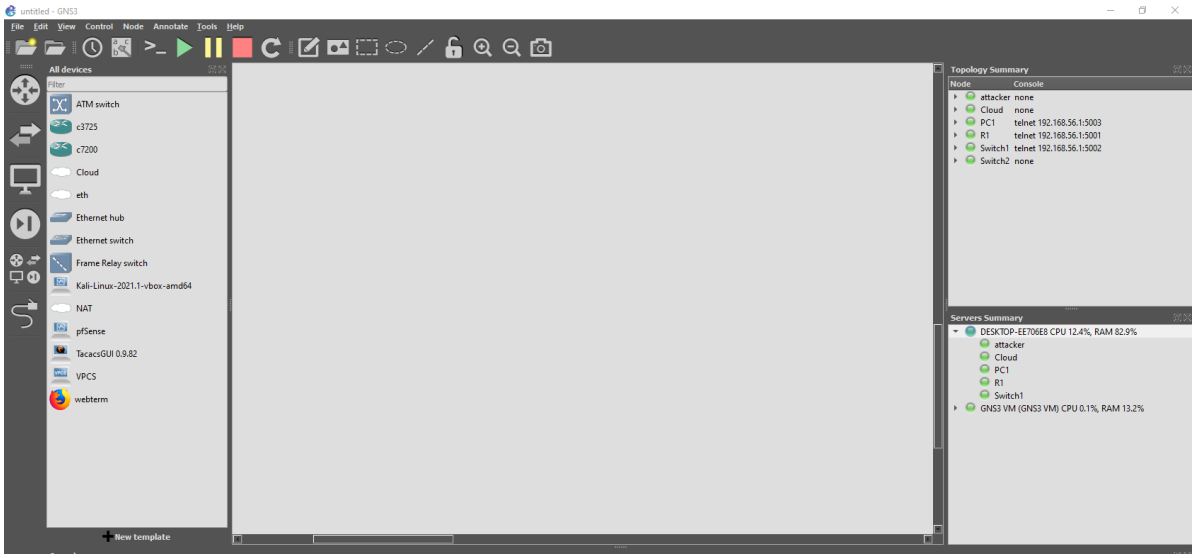


Рисунок 1.6 - Зовнішній вигляд графічного інтерфейсу GNS3

Також слід зазначити і те, що системні адміністратори і інженери постійно використовують дане програмне забезпечення. Причиною є те, що можна моделювати різні образи IOS, нові конфігурації, або навіть розробити та змоделювати частину складної мережі. З цією утилітою це стає набагато простіше ніж у реальному світі і також це набагато швидше та ефективніше.

Крім того , перевагою являється те, що програмний продукт обробляє інсталяцію і налаштування необхідних утиліт автоматично.

Так як доведеться в основному працювати з мережевим трафіком а саме з різновидами протоколів, обов'язковим до використання стає Wireshark.

Wireshark - це програмний засіб для аналізу мережевих протоколів, який є дуже популярним серед користувачів. За його допомогою можна захоплювати, аналізувати та вирішувати проблеми, що виникають у мережевому трафіку (рисунок 1.7). Wireshark підтримує широкий спектр протоколів і може бути використаний на різних операційних системах, таких як Windows, macOS та Linux [21].

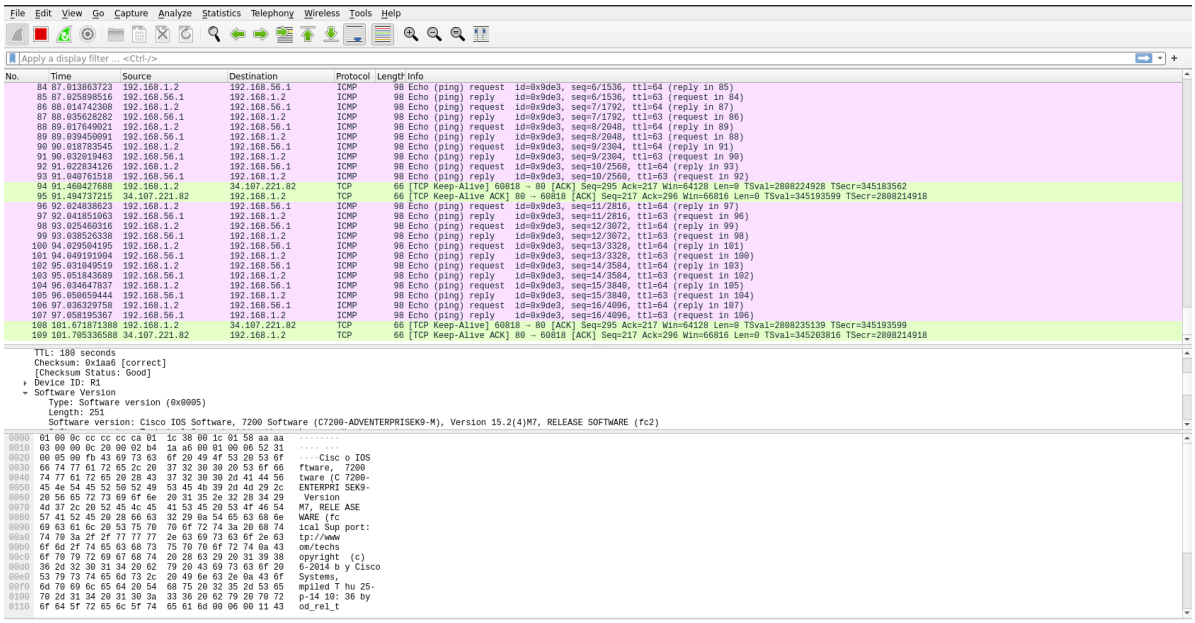


Рисунок 1.7 - Зовнішній вигляд програмного забезпечення Wireshark

За допомогою Wireshark користувачі можуть в реальному часі захоплювати пакети або аналізувати вже завантажені дані в офлайн-режимі. Програма надає детальну інформацію про кожен пакет, включаючи адреси джерела та призначення, тип протоколу, довжину пакета тощо.

Ця інформація може бути використана для виявлення та вирішення проблем у мережі, моніторингу продуктивності мережі та виявлення загроз безпеці. Wireshark також надає функцію фільтрування, яка дозволяє користувачам обирати критерії, на основі яких необхідно звузити захоплений трафік, наприклад, IP-адреса джерела або призначення, тип протоколу, вміст пакета тощо.

Крім цього, Wireshark містить додаткові функції, такі як можливість відновлення мережевих сесій та декодування зашифрованого трафіку. Загалом, Wireshark є потужним інструментом для аналізу та розв'язання проблем мережі, який використовується широкою аудиторією користувачів.

Також знадобиться інструмент для створення мережевих пакетів.

PackEth - спеціальний безкоштовний інструмент для створення

мережевих пакетів. Дане програмне забезпечення підтримує як і графічний режим так і консольний (рисунок 1.8). Він дає можливість створювати та надсилати будь-який мережевий пакет або послідовність пакетів. Він дуже простий у використані, потужний і підтримує багато налаштувань [22].

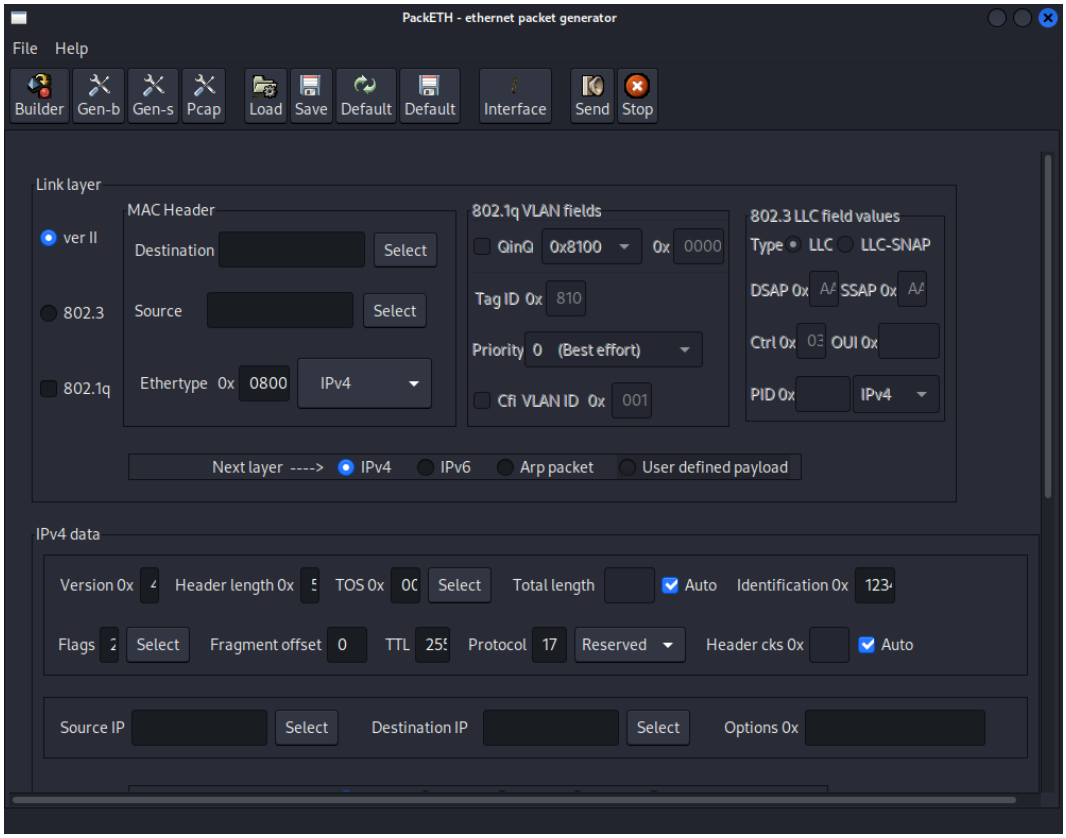


Рисунок 1.8 - Зовнішній вигляд програмного забезпечення PackEth

Особливості :

Можна створити та надіслати будь-який пакет Ethernet. Підтримувані протоколи:

— ethernet II, ethernet 802.3, 802.1q, QinQ, визначений користувачем фрейм ethernet;

— ARP, IPv4, IPv6, визначене користувачем корисне навантаження мережевого рівня;

— UDP, TCP, ICMP, ICMPv6, IGMP, визначене користувачем корисне навантаження транспортного рівня;

— RTP (корисне навантаження з опціями надсилання sin хвилі будь-якої частоти для G.711);

1.4 Постановка та формування задачі

У загальному задача по захисту мережі від атак полягає у запобіганні зловмисниками доступу до інформації, що використовується чи зберігається на серверах і комп’ютерах інформаційної системи підприємства.

Отже, на основі отриманої інформації можемо сформувати задачу. Основною задачею дипломного проекту є - розробка та створення системи захисту мережі від мережевих атак. Перед ти як приступати до виконання цієї задачі необхідно додатково дослідити та проаналізувати вже існуючі рекомендації. Також є інші задачі дипломного проекту. До них відносяться:

— дослідження додаткового теоретичного матеріалу який пов’язаний з мережевими атаками;

— дослідження загальних структури мережі, її складових компонентів;

— дослідити властивості апаратної структури мережевих пристроїв;

— включення заходів безпеки: на основі отриманих результатів після дослідження структури мережевих атак розробляються заходи безпеки, які повинні запобігти або попередити потенційну загрозу;

— визначити можливості використання операційних систем, які встановлені на мережевих вузлах;

— розробка схем можливих мережевих атак;

Після реалізації усіх вище перерахованих завдань, потрібно створити власну систему захищеної мережі і запропонувати певні рекомендації, щодо поліпшення захисту мереж.

2 РОЗГЛЯД ДЖЕРЕЛ МЕРЕЖЕВИХ ЗАГРОЗ

2.1 Вибір оптимальної архітектури безпечної комп'ютерної мережі

Проектування безпечної мережевої архітектури - це процес створення мережі, яка забезпечує високий рівень безпеки та захисту від різних видів загроз. Основні кроки проектування безпечної мережевої архітектури включають наступне:

— аналіз потенційних загроз та вразливостей мережі. Для цього можна використовувати різні інструменти, наприклад, сканери портів та вразливостей, аналізатори трафіку тощо;

— розробка стратегії захисту мережі. На основі аналізу вразливостей та загроз необхідно розробити план захисту мережі, який включає в себе різноманітні технічні та організаційні заходи;

— вибір технологій та рішень для реалізації захисту мережі. На основі стратегії захисту мережі необхідно вибрати відповідні технології та рішення для реалізації захисту мережі;

— розробка конфігурації мережі. На основі вибраних технологій та рішень необхідно розробити конфігурацію мережі, яка забезпечує високий рівень безпеки та захисту;

— тестування та аудит безпеки мережі. Після розробки та впровадження мережі необхідно провести тестування та аудит безпеки мережі для перевірки її ефективності та виявлення можливих проблем [23].

У процесі проектування безпечної мережевої архітектури необхідно враховувати різні фактори, такі як тип діяльності, розмір мережі, кількість користувачів та рівень конфіденційності даних. Також важливо використовувати сучасні технології та рішення для забезпечення високого рівня безпеки мережі.

Моїм об’єктом проектування стало невелике відділення Приват Банку. Створення безпечної мережі тільки для відділення має як і сильні сторони так і

недоліки. З позитивних сторін - це:

— простота застосування - розгортання мережевої інфраструктури в короткі терміни;

— масштабованість та гнучкість - модульна архітектура дозволяє досить просто впровадити ті рішення, які необхідні в даний момент та в подальшому розширення інформаційної системи;

— простота керування - невелика мережа дозволяє реалізувати її адміністрування централізованим;

— готовність до впровадження нових технологій чи рішень.

Також на створення невеликої мережі витрачається значно менше коштів, але це може стати певним обмеженням в вибору обладнання та програмного забезпечення. З недоліків, як уже згадувалось може бути сильно обмежений бюджет, порушення продуктивності і безпеки в разі виходу зі строю одного із сполучних вузлів [24].

Безпечний дизайн мережі, який реалізує кілька рівнів захисту, має вирішальне значення для захисту від загроз і захисту ресурсів у мережі. Дизайн повинен відповідати найкращим практикам безпеки. В любому випадку чудовим рішенням проектування мережі стане вибір принципу модульності.

Принцип модульності під час проектування мережі полягає в тому, щоб розділити мережу на окремі модулі або блоки, кожен з яких виконує певну функцію або послугу. Це дозволяє забезпечити більшу гнучкість та масштабованість мережі, а також полегшує її підтримку та управління.

Кожен модуль може бути розроблений окремо і забезпечувати певні функції, такі як маршрутизація, комутація, безпека, моніторинг тощо. Крім того, модульна мережа може бути більш стійкою до збоїв, оскільки в разі виникнення проблеми можна замінити лише той модуль, який не працює, зберігаючи роботу інших модулів в мережі.

Проектування модульної мережі передбачає визначення функціональних блоків, вибір відповідних протоколів та технологій для кожного блоку, а також

розробку схеми зав’язків між блоками. При цьому важливо враховувати потреби користувачів, розмір мережі та рівень її безпеки.

Щодо моделі мережі я обрав ієрархічну модель. Ієрархічна модель комп’ютерної мережі - це архітектура мережі, що заснована на принципі розбиття мережі на декілька рівнів, кожен з яких виконує свої назначені функції. Така модель розділена на декілька рівнів, кожен з яких забезпечує певну функціональність [25].

Перший рівень - це рівень доступу, це рівень з яким безпосередньо взаємодіє користувач. На цьому рівні розміщуються засоби зв’язку. Цей рівень слугує точкою входу в мережу для користувачів та інших мережевих пристроїв, таких як принтери, сканери, Ip-телефони чи звичайні персональні комп’ютери. Доступ може бути як і бездротовий так і дротовий. Також до пристроїв цього рівня можна віднести комутатори другого рівня моделі OSI. Ці комутатори виконують задачу первинного сегментування мережі.

Оскільки рівень доступу це вхідна точка в мережу для клієнтський пристроїв він в першу чергу повинен забезпечити захист самих користувачів, мережу та інші корпоративні ресурси від зловмисних атак зі сторони підключених клієнтів [26].

Рівень доступу включає в себе наступні технології захисту:

— IP Source guard - захист від IP spoofing, тобто від підміни Ip-адреса джерела;

— Port security - цей метод встановлює обмеження на кількість MAC адрес, які надходять на порт комутатора. Захищає від зловмисної заміни MAC адреси і також захищає від атак, спрямованих на переповнення таблиці комутації;

— DHCP-snooping - створює захист користувачів від отримання адреси від фальшивого DHCP сервера, а також забороняє зловмиснику захопити всі IP-адреси (рисунок 2.1);

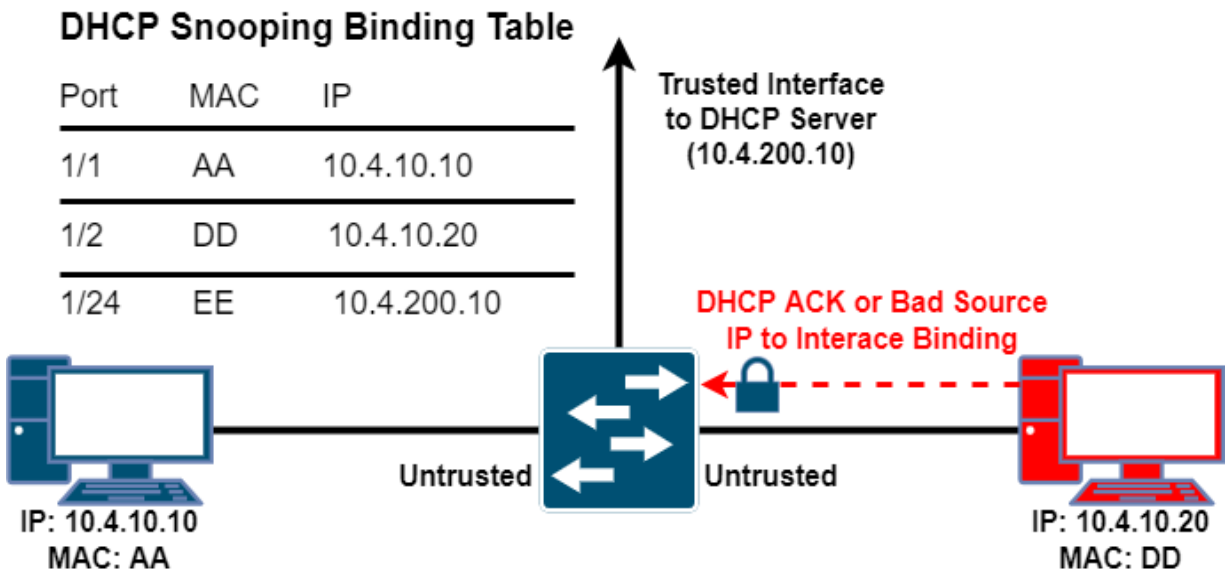


Рисунок 2.1 - DHCP-snooping і ARP Inspection

Також у нашому випадку слід обрати спеціальний комутатор, який підтримує технологію PoE (Power over Ethernet). Ця технологія дозволяє і спрощує підключення до мережі таких пристроїв, як IP-телефони, IP-відеокамери або бездротові точки доступу. У моєму випадку до рівня доступу будуть відноситись кінцеві пристрої та комутатор, а саме сервер, декілька комп'ютерів спеціалістів з відділу по роботі з клієнтами та вузол системного адміністратора [27].

Наступним рівнем мережі є рівень агрегації (Aggregation layer). Цей рівень повинен забезпечувати агрегацію трафіку з різних пристроїв, які уже підключені до першого рівня. На цьому рівні свої задачі виконують маршрутизатори, які надають можливість передавати дані між різними частинами мережі. У моєму випадку основні задачі цього рівня буде виконувати маршрутизатор.

Останнім рівне моделі є рівень корпоративної мережі (Core layer). Третій рівень, задача якого полягає в забезпечені зв'язку між іншими рівнями. На цьому рівні рекомендується встановлювати високопродуктивні маршрутизатори, що можуть забезпечити швидку та безперебійну передачу даних між різними частинами мережі. Також на цьому рівні рекомендується

встановлювати пристрої чи засоби забезпечення захисту мережі. У моєму випадку через невеликий розмір мережі цей рівень буде спрощений. Роль пристрою який буде забезпечувати захист мережі я обрав pfSense.

pfSense - це безкоштовна операційна система, яка заснована на FreeBSD і призначена для роботи як мережевий маршрутизатор, файрвол та VPN-сервер. pfSense має велику кількість функцій, таких як балансування навантаження, обмеження швидкості, захист від атак та інші. Ця система може бути встановлена як на фізичний сервер, так і на віртуальну машину. Крім того, pfSense має дуже зручний веб-інтерфейс для налаштування всіх необхідних параметрів. Вона дуже популярна серед IT-спеціалістів та системних адміністраторів [28].

pfSense забезпечує високий рівень безпеки за допомогою вбудованих функцій, таких як фаервол, IDS / IPS, VPN і багато інших. Крім того, pfSense має зручний графічний інтерфейс користувача для налаштування всіх цих функцій, що дозволяє легко налаштовувати та керувати системою.

pfSense може бути встановлений на різні типи обладнання, наприклад на фізичний сервер, віртуальну машину або на мережевий пристрій, такий як маршрутизатор або файрвол. Також можна налаштувати pfSense як шлюз між двома мережами, щоб забезпечити безпеку мережі.

Крім того, pfSense має велику спільноту користувачів та розробників, яка надає підтримку та розвиває цю операційну систему. Ця спільнота забезпечує постійне оновлення та вдосконалення pfSense, що робить систему надійною та безпечною для використання в будь-яких умовах.

Так як моя мережа досить невелика, єдине оптимальне місце на мою думку знаходиться між комутатором другого рівня та маршрутизатором. У наступному розділі буде проведене детальне налаштування усіх компонентів мережі, а саме комутатора, маршрутизатора та системи виявлення вторгнень. Усі налаштування будуть націлені на створення захищеного інформаційного середовища.

Так як відділення ПриватБанку містить в собі всього до десяти користувачів, то і загальний розмір мережі буде невеликий (рисунок 2.2).

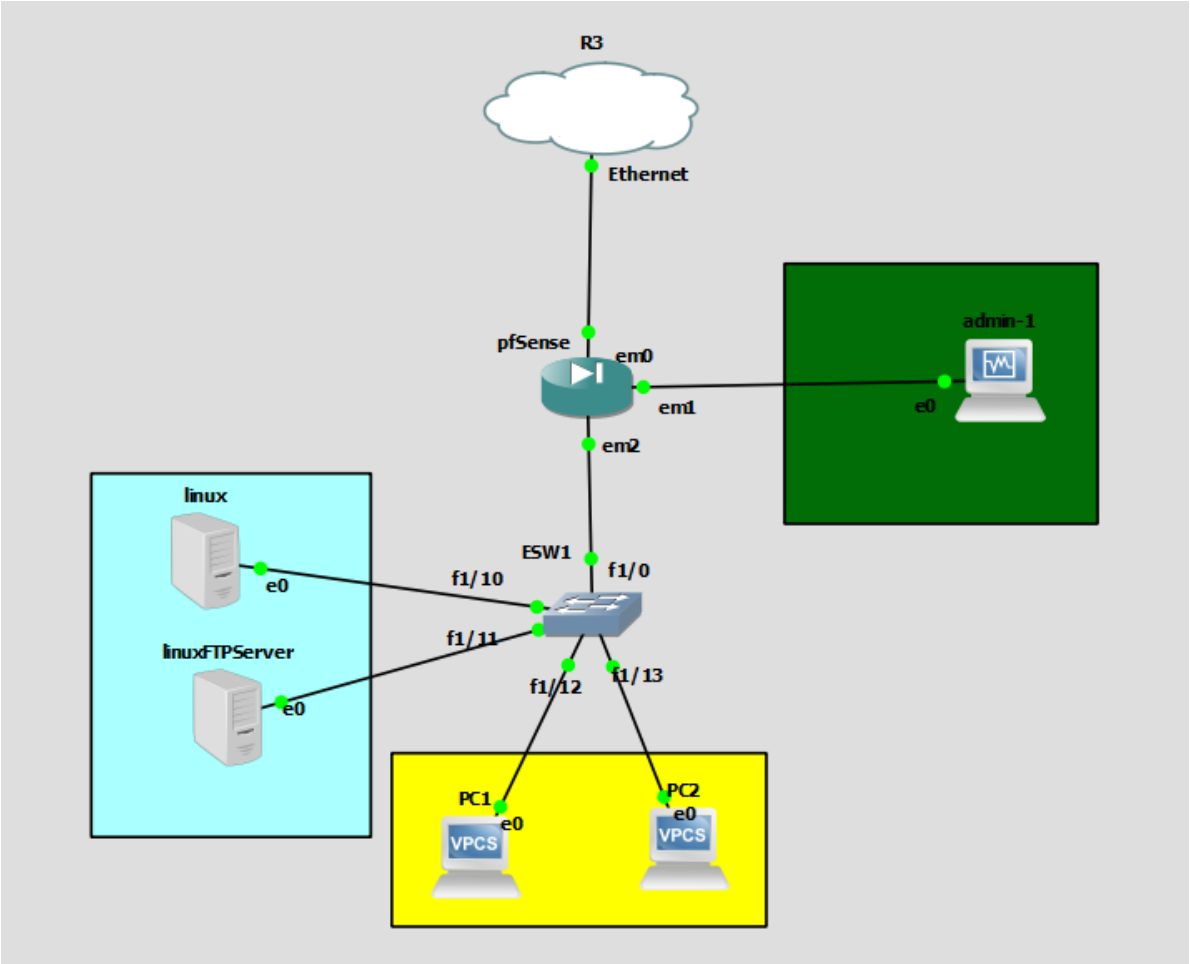


Рисунок 2.2 - Топологія захищеної мережі

У такій мережі окремий модуль, наприклад модуль маршрутизації, може складатись всього з одного пристрою - маршрутизатора. У подальшому буде проведено вибір кожного з компонентів мережі та обґрунтовано цей вибір.

2.2 Вибір компонентів мережі

Після побудови фізичної топології мережі потрібно обрати необхідні мережеві пристрої для її побудови. Під час вибору мережевих пристроїв слід

звертати увагу на кілька ключових факторів, зокрема:

— швидкість передачі даних - це один з найважливіших показників для багатьох підприємств. Якщо планується використовувати мережевий пристрій для передачі великих обсягів даних, то бажано, щоб він мав високу швидкість передачі даних.

— підтримка стандартів - потрібно переконатись, що обрані мережеві пристрої підтримують потрібні стандарти, зокрема Wi-Fi, Ethernet і Bluetooth.

— розмір та дизайн - необхідно обрати мережевий пристрій, який підходить за розміром та дизайном для приміщення підприємства і способу використання.

— функціональність - треба врахувати можливості, такі як підтримка гостьового доступу, підключення до VPN і функціональний діапазон.

— безпека - потрібно обрати мережевий пристрій з належним рівнем безпеки, щоб уникнути загроз викрадення даних.

Я можу порекомендувати наступні пристрої від компанії Cisco для організації захищеної мережі:

1. Комутатор який я рекомендую- це Cisco SG350-10 (рисунок 2.3). Він має 10 портів Gigabit Ethernet і підтримує стандарти PoE (Power over Ethernet), які дозволяють живити підключені до нього пристрої безпосередньо через мережевий кабель. Крім того, цей комутатор має можливість керування трафіком із використанням VLAN та QoS.

Рисунок 2.3 - Зовнішній вигляд комутатора Cisco C9300-24T-E

2. Маршрутизатор який я рекомендую - це Cisco ISR4221/K9 (рисунок

2.4). Компактний маршрутизатор серії Cisco Integrated Services Router (ISR) із уже вбудованим програмним забезпеченням IOS XE. Цей маршрутизатор може запропонувати широкий спектр можливостей для побудови мережі. Він дозволяє забезпечити надійний та безпечний доступ до інтернету, а також забезпечує багатофункціональність для розв'язання різних завдань. Cisco ISR4221/K9 підтримує швидкісний інтерфейс Gigabit Ethernet, що забезпечує швидкий обмін даними між пристроями у мережі. При необхідності також можна додати модулі розширення для розширення функціональності маршрутизатора, наприклад, модуль бездротового доступу до мережі Wi-Fi.

Рисунок 2.4 - Зовнішній вигляд маршрутизатора Cisco ISR4221/K9

3. Останнім компонентом для мережі стане, раніше згадана, система брандмауерного захисту мереж pfSense. Він має багато позитивних сторін:

— pfSense є відкритим програмним забезпеченням і безкоштовним для використання;

— pfSense має простий та зручний графічний інтерфейс користувача (рисунок 2.5);

— pfSense має широкий спектр функцій, таких як файрвол, VPN, балансування навантаження, обмеження швидкості та інші;

— pfSense має розвинену систему безпеки, яка включає в себе файрвол, IDS / IPS та інші функції;

— pfSense може бути встановлений на фізичний сервер або віртуальну машину.

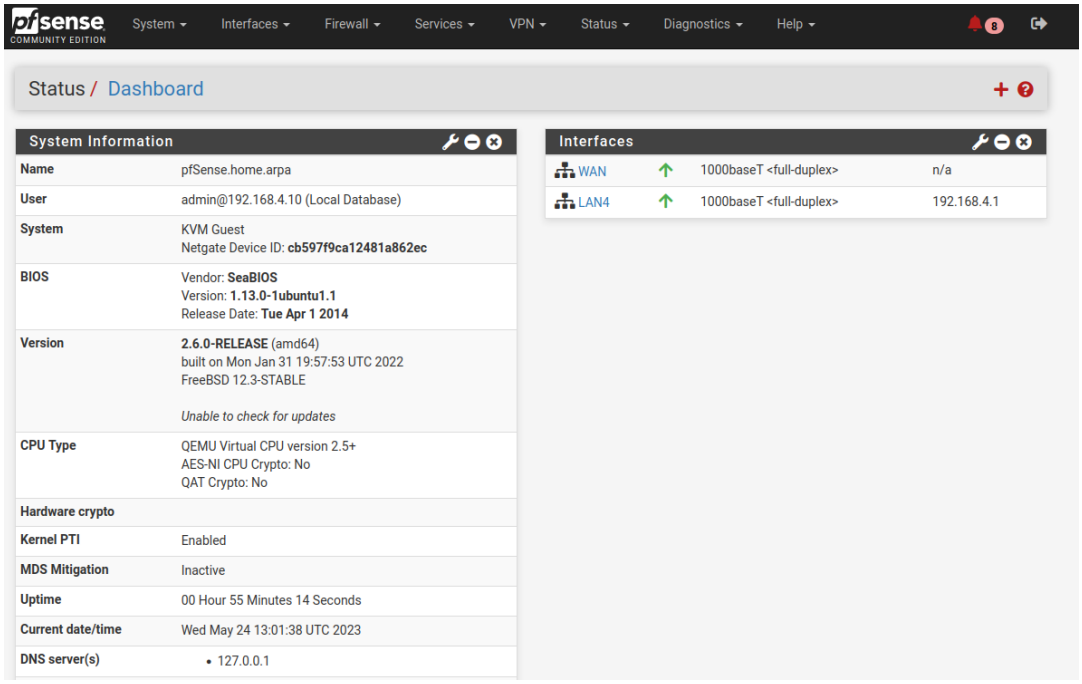


Рисунок 2.5 - Зовнішній вигляд інтерфейсу pfSense

Загалом, pfSense є потужним і надійним рішенням для створення безпечних мереж, якщо його використовувати належним чином.

2.3 Розробка системи захисту на базі вибраної архітектури

Першим кроком по налаштуванню захищеної системи, буде налаштування комутатора. Для початку потрібно зробити загальні налаштування комутатора, щоб забезпечити безперебійну роботу мережі. А потім звернути увагу на можливі вразливості та зробити налаштування по захисту пристрою.

Першим налаштуванням стане сегментація мережі на віртуальні підмережі. VLAN дозволяє об’єднати кінцеві пристрої разом, незалежно від їх фізичного розташування. Для налаштування потрібно виконати наступні кроки:

1. Створити три VLAN на комутаторі з допомогою команди "vlan <ID>";

2. Налаштувати порти комутатора, що приєднані до кінцевих пристроїв, як мережеві порти і прив'язати їх до відповідних VLAN за допомогою команди "switchport mode access" та "switchport access vlan <ID>";

3. Налаштувати порти комутатора, що приєднані до інших комутаторів або роутерів, як транківські порти і додати їх до всіх трьох VLAN за допомогою команди "switchport mode trunk" та "switchport trunk allowed vlan <ID>".

Одна з найпоширеніших помилок при налаштуванні комутаторів доступу (до яких підключаються користувачі, сервери, ip-камери тощо) - не відключення портів, що не використовуються. Типова ситуація, коли "вільні" порти залишають включеними.

Ця ситуація створює величезні ризики, якщо зловмисник отримає фізичний доступ до комутатора він зможе підключитися до корпоративної мережі. Цей факт підсилюється тим, що більшість адміністраторів залишають порти зі стандартними налаштуваннями. Використання налаштувань за замовчуванням означає, що порт знаходиться в VLAN 1 і має увімкнений протокол DTP (switchport mode dynamic desirable). Це дає зловмисникам можливість отримати доступ до інших сегментів мережі (щодо того, наскільки небезпечні VLAN1 та протокол DTP, я розгляну цю тему наступною). Крім того, користувачі часто бездумно підключають свої хаби або свічі до "вільних" портів, що може призвести до створення мережевих петель. У світлі цих потенційних проблем, краще відключати порти, які не використовуються, або переводити їх в невикористовуваний VLAN. Для відключення порта потрібно лише використати команду «shutdown» в режимі конфігурації відповідного інтерфейсу [29].

У комутаторів Cisco існує протокол DTP - динамічний протокол транкінгу, який є власною розробкою компанії. Використовуючи цей протокол, комутатори можуть автоматично визначати, чи є сусідній комутатор налаштований для створення транка, а також визначити, який протокол транкінгу використовувати: 802.1Q або ISL. Особливістю цього протоколу є те,

що він включений за замовчуванням, тому будь-який порт може бути автоматично переведений в режим Trunk при підключенні до іншого порту Trunk.

Якщо на комутаторі SW2 налаштувати порт Trunk та підключити його до SW1, то порт першого комутатора автоматично переведеться в режим Trunk та буде передавати всі доступні VLAN. З одного боку, це зручно, оскільки не потрібно налаштовувати обидва комутатори. Але, з іншого боку, якщо замість SW2 підключиться комп'ютер зловмисника, то ніхто не завадить йому налаштувати свій порт як Trunk та витягти всі VLAN з вашого комутатора. Така ситуація становить загрозу через особливості протоколу DTP. Щоб унеможливити автоматичне перемикання порту в Trunk, необхідно вручну переключити його в стан Access.

Для централізованого керування системою потрібно налаштувати SSH. Слід виконати наступні кроки:

1. Створити користувача та пароль для входу за допомогою SSH на комутаторі;
2. Увімкнути службу SSH на комутаторі за допомогою команди "crypto key generate rsa". Ця команда генерує RSA-ключ шифрування, необхідний для роботи SSH;
3. Налаштувати доступ до SSH за допомогою наступних команди, "username <username> privilege 15 secret 0 <password>", "aaa new-model" та "aaa authentication login default local";
4. Налаштувати порт SSH на комутаторі за допомогою команди - "ip ssh version 2". Ця команда встановлює версію SSH яка підтримується комутатором.

Тепер слід звернути увагу на можливі вразливості комутатора та ввести зміни в налаштування так, щоб запобігти їх. Основними загрозами можуть бути наступні мережеві атаки:

— атака на дерево stp;

— підміна MAC адрес;

— отруєння таблиці CAM;

— атака на ARP;

— атака на VLAN.

Для того, щоб запобігти ряд цих атак, адміністратори безпеки зазвичай покладаються на наявність функції безпеки порту комутаторів. Більшість комутаторів можна налаштувати для обмеження кількості MAC-адрес, які можна дізнатися на портах, підключених до кінцевих станцій.

Port security (безпека портів) - це заходи, які вживаються для забезпечення безпеки мережевих портів на комутаторах або інших мережевих пристроях. Ці заходи можуть включати в себе контроль доступу до портів, обмеження кількості приладів, які можуть бути підключені до порту, та моніторинг активності порту [30, 31].

Основна мета портової безпеки полягає в тому, щоб запобігти несанкціонованому доступу до мережі через фізичний порт. Це може бути корисно у випадках, коли хакерам або злочинцям необхідно мати фізичний доступ до мережі, щоб отримати конфіденційну інформацію або завдати шкоди комп'ютерній системі. Хакер може використати спеціальне програмне забезпечення, щоб підключитися до комутатора та створити на порту тисячі MAC-адрес. Ці адреси записуються до CAM-таблиці комутатора до того моменту, коли вона переповнюється. У процесі атаки хакер заміщує легітимні MAC-адреси своїми власними, що може призвести до їх витіснення або затирання. Якщо CAM-таблиця комутатора переповнена, то він перетворюється на режим fail open mode, який працює як звичайний хаб. Це означає, що кожен пакет, що надходить, буде передаватися по всіх портах, що дозволяє хакеру бачити весь трафік, що проходить через комутатор, Налаштування Port security на комутаторі Cisco може бути здійснене за допомогою таких кроків:

— для початку потрібно зайти в конфігураційний режим комутатора, використовуючи команду enable та ввести привілейований пароль;

— далі перевірити конфігурацію порта, до якого потрібно налаштувати Port security, за допомогою команди show interface «інтерфейс» (наприклад, show interface GigabitEthernet0/1);

— налаштувати Port security на цьому порту за допомогою команди switchport port-security;

— визначити максимальну кількість MAC-адрес, які дозволено вивчити на цьому порту, за допомогою команди switchport port-security maximum «кількість»;

— вказати дії, які необхідно вжити, якщо будь-яка невідома MAC-адреса намагається підключитися до порту. Наприклад, можна налаштувати порт на блокування (за допомогою команди switchport port-security violation {protect | restrict | shutdown}), щоб забезпечити безпеку мережі;

— обов’язково потрібно зберегти конфігурацію за допомогою команди write memory [32].

Потрібно розуміти який саме режим безпеки обрати в п’ятому пункті. Режим Protect - це сама м’яка реакція на перевищення допустимої кількості MAC-адрес. У разі перевищення ліміту (або появи "чужої" MAC-адреси) трафік буде просто відкидатися.

Схема обміну пакетами протоколу ARP вразлива для атак типу ARP-poisoning (або ARP-spoofing), коли зловмисник підроблює адресу хоста X.X.X.X та перехоплює трафік. Щоб запобігти таким атакам, використовують функцію Dynamic ARP Inspection (DAI). Алгоритм роботи схожий на DHCP-Snooping: порти мережі поділяються на довірені та недовірені. Кожен ARP-пакет на недовірених портах проходить аналіз, де порівнюється інформація в цьому пакеті з тією, на яку комутатор довіряє (або зі статично заданою відповідністю MAC-IP або з інформацією з бази DHCP Snooping). Якщо дані не співпадають, то пакет відкидається, а у syslog генерується повідомлення [33].

Щоб активувати DAI в потрібному VLAN-і, необхідно використати наступну команду «ip arp inspection vlan 2»

Як вже було згадано до цього, мережеві адміністратори не ставлять перед собою задачу створити система захисту з допомогою вище вказаних команд. В першу чергу потрібно забезпечити повинні забезпечити безпечний доступ дообладнання (як фізичний, так і віддалений). Потім скористатися більшістю раніше наведених рекомендацій (рисунок 2.6).

```
Switch(config)#int fa0/1
Switch(config-if)#description UserA1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#storm-control broadcast level 10.00
Switch(config-if)#storm-control action shutdown
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#ip verify source vlan dhcp-snooping port-security
```

Рисунок 2.6 - Приклад налаштувань комутатора на одному інтерфейсі

Наступним кроком по забезпеченню безпеки буде налаштування pfSense. pfSense є програмним маршрутизатором/фаєрволом на основі операційної системи FreeBSD. Для його коректної роботи потрібно покроково налаштувати мережеві інтерфейси а згодом створити правила фільтрації пакетів для різних сегментів мережі [34, 35].

Після завантаження pfSense з’явиться меню налаштування. Перше що потрібно зробити - це налаштувати мережу і веб-інтерфейс. Потім усі налаштування можна буде виконувати в веб-інтерфейсі. Для цього потрібно:

1. Потрібно вибрати опцію «Set interface(s) IP address»;
2. Обрати інтерфейс для налаштування. Для початку (LAN) (рисунок 2.7);
3. Необхідно задати ip-адрес відповідно створеній інфраструктурі;
4. Вказати маску підмережі;
5. На цьому етапі було запропоновано активувати сервер DHCP для локальної мережі. У моєму випадку в ньому не має потреби;
6. Наступним кроком було запропоновано використовувати для веб

інтерфейсу http з’єднання, але в цьому випадку я залишив https. Так як воно створює шифровану канал передачі даних.

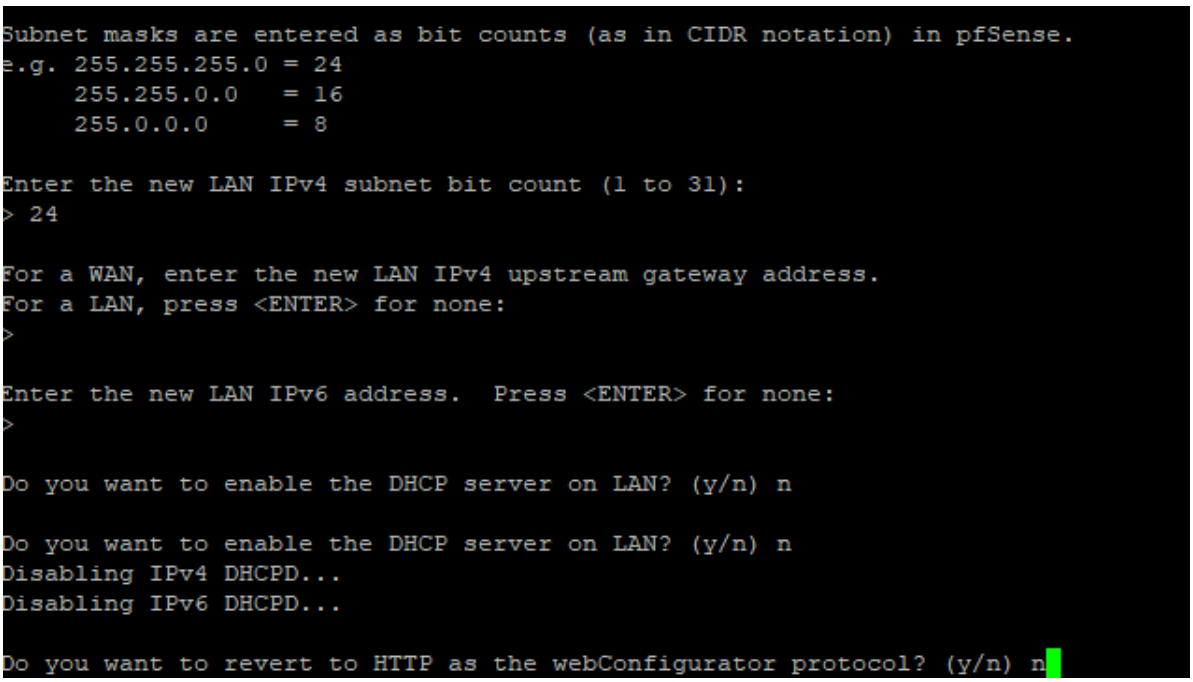


Рисунок 2.7 - Процес налаштування LAN інтерфейсу

Наступним кроком буде додавання VLAN до інтервейсу який направлений в локальну мережу (рисунок 2.8). Це потрібно для того, щоб згодом отримати можливість для кожного з цих віртуальних сегментів створити індивідуальні правила на файрволі. Для цього потрібно:

1. Обрати пункт «Assign Interfaces»;
2. Далі необхідно ввести назву батьківського VLAN інтерфейсу;
3. Перерахувати назви VLAN-ів, я створив vlan2, 3, 4;
4. Далі потрібно ввести назву інтерфейсу для WAN-інтерфейсу;
5. Так само необхідно ввести найменування інтерфейсу для LAN;
6. Після цього потрібно ввести найменування інтерфейсів для раніше створених VLAN;
7. Після того, як найменування для всіх інтерфейсів будуть призначені потрібно виконати підтвердження;

8. В основному меню будуть перераховані всі наші інтерфейси з найменуваннями, але без адрес [36].

Рисунок 2.8 - Результат створення VLAN-ів

Останнє що необхідно створити на даному етапі це призначити ip-адреса для кожної віртуальної підмережі (рисунок 2.9) . Цей і усі наступні етапи можна виконати за допомогою веб-інтерфейсу. Все, що потрібно щоб увійти до нього - це ввести ip-адрес у адресній стрічці браузера.

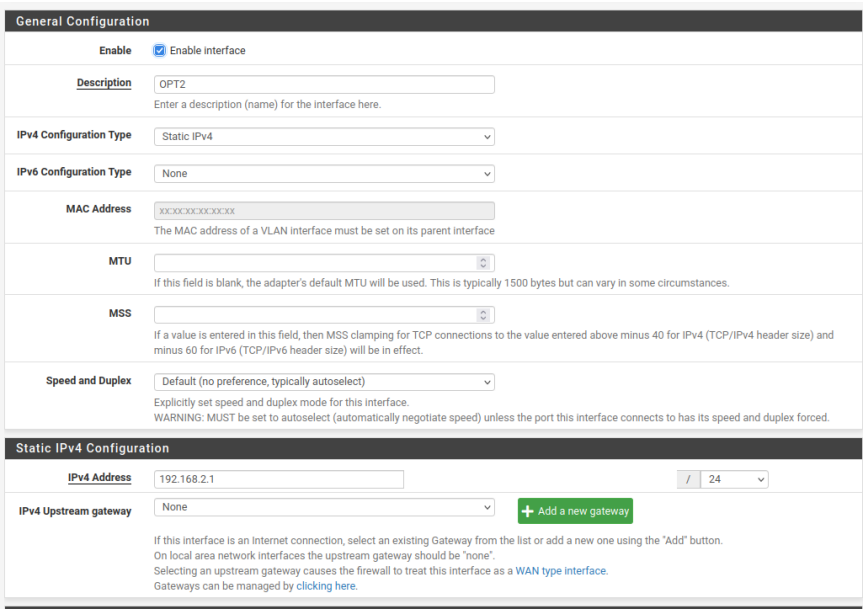


Рисунок 2.9 - Процес налаштування віртуальних інтерфейсів

Для забезпечення безпеки мережі потрібно створити спеціальні правила для системи firewall в pfSense. Firewall - це система захисту мережі, яка дозволяє контролювати трафік, що проходить через неї. Його головна мета полягає в управлінні доступом до ресурсів зовнішньої мережі, а також в захисті від несанкціонованого доступу та небезпечного трафіку [37].

Firewall може фільтрувати пакети, що проходять через нього, на основі різних критеріїв, наприклад, IP-адреси відправника та отримувача, порти, протоколи тощо. Він може приймати рішення про те, як поводитися з пакетами - блокувати їх, пересилати до іншої точки призначення, чи дозволяти проходження.

Основна функція firewall полягає в тому, щоб запобігти несанкціонованому доступу зовнішніх користувачів до ресурсів в мережі компанії, а також запобігти розповсюдженню шкідливих програм, які можуть завдати шкоди комп'ютерам в мережі. Firewall є необхідним елементом інфраструктури безпеки для будь-якої мережі з доступом до Інтернету. Щоб створити необхідні правила спочатку потрібно визначити, які сервіси потрібно надати доступ до мережі, які ip-адреси чи діапазони ip-адрес повинні мати доступу до певних сегментів, які правила слід застосувати для захисту від атак та які правила повинні бути застосовані для обмеження трафіку мережі. Також слід визначити які правила можуть бути застосовані для забезпечення безпеки інтернет-з'єднання та які правила повинні бути застосовані для захисту від шкідливого програмного забезпечення (рисунок 2.10).

У моєму випадку потрібно створити наступні правила:

— VLAN-2 має доступ до інтернету і до VLAN-3;

— VLAN-4 має доступ до всієї мережі;

— VLAN-3 тільки до VLAN-2.

Для того, щоб додати правила потрібно перейти у розділ firewall та вибрати відповідний інтерфейс, трафік якого необхідно фільтрувати.

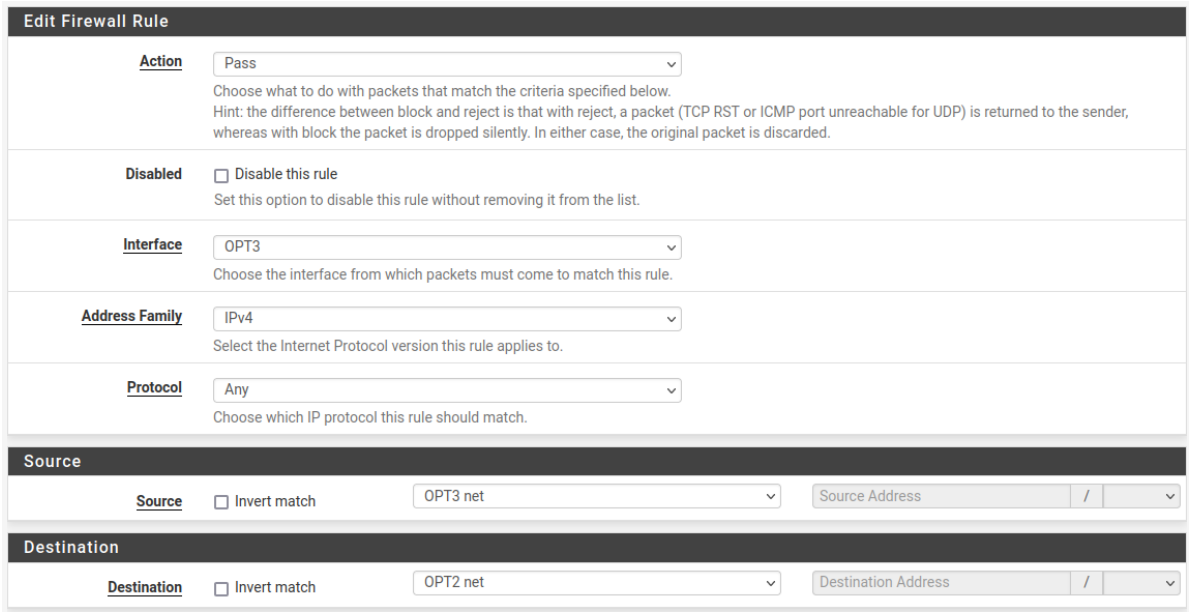


Рисунок 2.10 - Процес створення правил для firewall

Отже у цьому розділі я вже: обрав необхідну модель та мережеві пристрої, що є ключовим етапом у побудові мережі. Тому що він визначає її функціональні можливості та продуктивність. Також, правильне налаштування цих пристроїв допомагає забезпечити ефективну роботу мережі [38].

Створення необхідних налаштувань для захисту від можливих вразливостей чи мережевих атак є критично важливим етапом в розробці будь-якої мережі, оскільки це допомагає зменшити ризик виникнення проблем безпеки та забезпечує стійкість мережі до атак.

2.4 Додаткові процедури захисту

З додаткових методів захисту можна виділити декілька видів.

Ідентифікація та автентифікація користувачів полягає у перевірці введеного логіну та пароля користувача для доступу до ресурсів мережі. Під час ідентифікації визначаються індивідуальні характеристики особи, які дозволяють її розпізнати в системі, наприклад, логін, ID, електронна пошта або

номер телефону. Автентифікація передбачає підтвердження ідентичності користувача шляхом перевірки його введеного логіну та пароля. Після ідентифікації система звертається до бази даних для перевірки вірності введеного пароля.

Для забезпечення безпеки доступу до ресурсів мережі необхідно використовувати достатньо складні паролі та регулярно їх змінювати. Крім того, можна застосовувати двофакторну автентифікацію (2FA), яка передбачає додаткову перевірку, наприклад, за допомогою коду підтвердження, який надсилається на мобільний телефон або електронну пошту. Це дозволяє забезпечити додатковий рівень захисту від можливих атак хакерів або зловмисників.

Антивірусне програмне забезпечення допомагає захистити комп'ютер від різноманітних шкідливих програм, таких як трояни, віруси, черв'яки та інші загрози з Інтернету. Програма сканує всі файли на комп'ютері, щоб виявити будь-які можливі загрози та повідомляє про них користувачеві. Крім того, антивірусна програма здатна блокувати доступ до небезпечних сайтів, перевіряти електронні листи на наявність вірусів та інших загроз, а також моніторити активні процеси в системі.

З огляду на те, що нові види шкідливих програм постійно з'являються, необхідно регулярно оновлювати антивірусне програмне забезпечення для більш ефективного захисту від свіжих загроз. Також важливо уникають відкривання сумнівних файлів та відвідування небезпечних сайтів, щоб зменшити ризик зараження комп'ютера шкідливим програмним забезпеченням.

Захист важливих даних від втрати в разі аварії або несправності комп'ютера можна забезпечити за допомогою резервного копіювання. Цей процес полягає у створенні копій цих даних та їх збереженні на зовнішніх носіях, таких як флеш-карти або жорсткі диски, або в хмарних сховищах в Інтернеті.

Щоб зробити резервне копіювання ефективнішим, рекомендується

створювати регулярні копії важливих даних і зберігати їх на різних носіях або в різних місцях. Також можна скористатися спеціальним програмним забезпеченням для автоматичного резервного копіювання даних з заданими інтервалами часу.

Резервне копіювання даних є важливою практикою, яка допомагає забезпечити безпеку та захист важливих даних від непередбачуваних ситуацій, і це потрібно робити регулярно для зменшення ризиків втрати цих даних.

2.5 Висновок

Завершення розробки системи безпеки інформаційної системи відділення Приватбанку вимагало багато зусиль, але після досліджень та розгляду різних методів захисту інформаційної системи від мережевих атак, була розроблена оптимальна архітектура для безпечної комп'ютерної мережі. Також було проведення ретельного налаштування мережевих пристроїв з урахуванням можливих вразливостей та потенційних атак. Компоненти системи захисту були ретельно перевірені та протестовані на відповідність стандартам безпеки.

Створення системи захисту від мережевих атак базувалася на розробленій архітектурі, що забезпечувала ефективний захист від можливих загроз. Результати тестування вказують на високу ефективність розробленої системи. Також було розглянуто економічну доцільність використання розробленої системи захисту від мережевих атак, що дозволило зрозуміти, що розроблена система дає можливість зменшити витрати на попередження та усунення загроз безпеці інформаційної системи.

Отже, розробка та імплементація системи захисту від мережевих атак була успішною і дозволяє забезпечити надійний захист інформаційної системи Відділення Приватбанку від можливих загроз.

3 АНАЛІЗ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ СИСТЕМИ БЕЗПЕКИ

3.1 Оцінка захищеності розробленої системи захисту від мережевих атак

Після теоретичного дослідження мережевих загроз та створення захищеної мережі необхідно провести оцінку виконаної роботи, а саме методом порівняльного аналізу. Я провів тестування захищеності створеної мною системи захисту та іншого готового рішення.

Необхідно більш детально протестувати типові атаки на протоколи. Такі атаки можуть бути спрямовані на викрадення конфіденційної інформації, порушення цілісності даних або на заволодіння контролем над комп'ютером чи його ресурсами з метою використання їх у кіберзлочинах.

Перша атака яку слід проаналізувати - це атака на протокол CDP. Одна з хороших сторін вразливості CDP, це те що цю атаку неможливо виконати через інтернет, тому що CDP працює тільки всередині локальних мереж, на канальному рівні. Тобто зловмиснику спочатку потрібно буде проникнути в мережу підприємства. Але якщо хакер вже проник в мережу організації чи підприємства, у нього появляється можливість використати дану вразливість. В такому випадку головними цілями зловмисника стануть маршрутизатори, між мережеві екрани та комутатори, компрометація яких призведе до поганих наслідків для всієї мережі організації. Зловмисник має можливість створити підроблені пакети CDP, які містять дані про мережеві пристрої, що зазвичай обмінюються один з одним. Якщо інші пристрої у мережі отримують ці підроблені пакети CDP, то хакер може зібрати повну карту мережі, включаючи адреси IP, порти та інші параметри пристроїв. Що цікаво всі ці пристрої поставляються з увімкненим за замовчування CDP.

Також цей протокол за замовчуванням увімкнений в інших продуктах Cisco, таких як VoIP-телефони та IP-камери. І даний тип атаки може бути ефективний і проти них.

Для аналізу атаки було протестовано одразу дві мережі, одна з них це мережа розроблена в попередньому розділі. Атаки змодельовано з-за допомогою програмного забезпечення GNS-3.

Для моделювання атаки знадобиться фреймворк під назвою «Yersinia» (рисунок 3.1). Він використовується як і пен-тестерами, так і мережевими адміністраторами. Це програмне забезпечення розроблене спеціально для атак на протоколи другого рівня моделі OSI. «Yersinia» підтримує як і консольну версію так і графічну, для зручності роботи і демонстрації атак я обрав саме графічну версію.

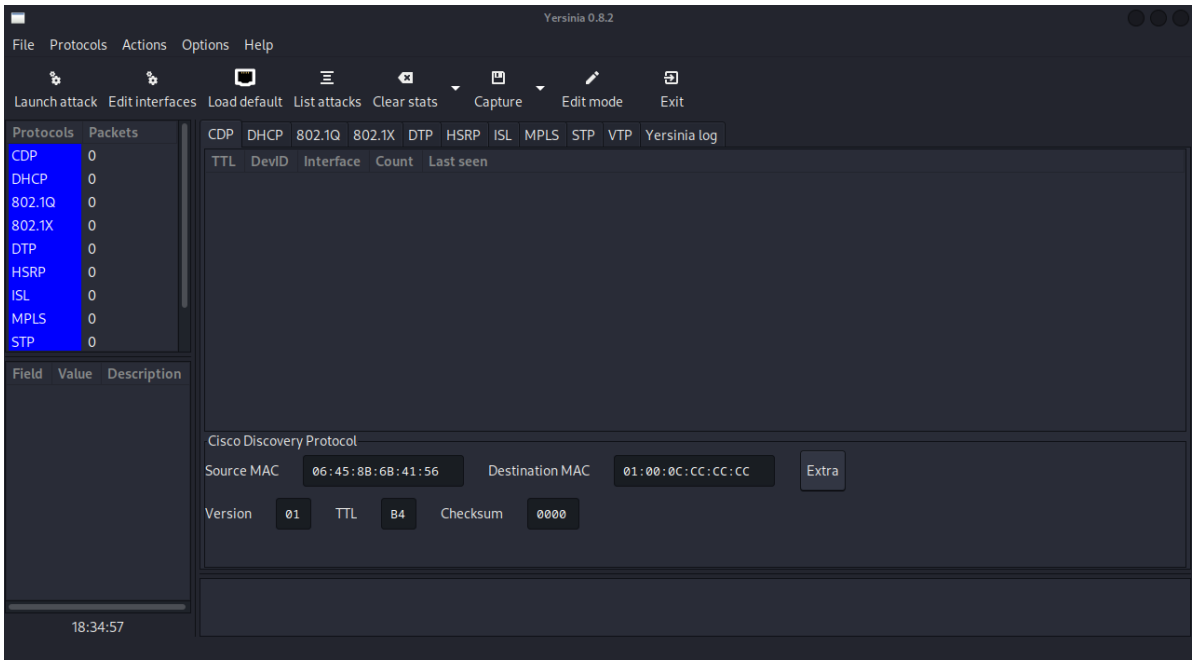


Рисунок 3.1 - Зовнішній вигляд графічної версії «Yersinia»

Перед початком атаки потрібно зачекати поки мережеві пристрої самостійно відправлять хоча б один пакет, або спровокувати CDP відповідь на наш запит. Це необхідно для того, щоб «Yersinia» проаналізував та виявив необхідний пристрій в мережі. За замовчуванням CDP пакет відправляється кожні 60 секунд.

Після отримання одного з пакетів можна помітити, що він не зашифрований. Стає очевидно, що таким чином можна отримати інформацію

про мережевий пристрій а саме:

— mac-address відправника;

— версія Cisco IOS пристрою;

— номер порта з якого було надіслано пакет;

— та інша важлива інформація за якою зловмисники можуть знайти вразливості в пристрої.

Для дослідження наслідків вразливості потрібно зняти певну інформацію до та після атаки. А саме кількість отриманих пакетів та навантаження на процесор комутатора (рисунок 3.2).

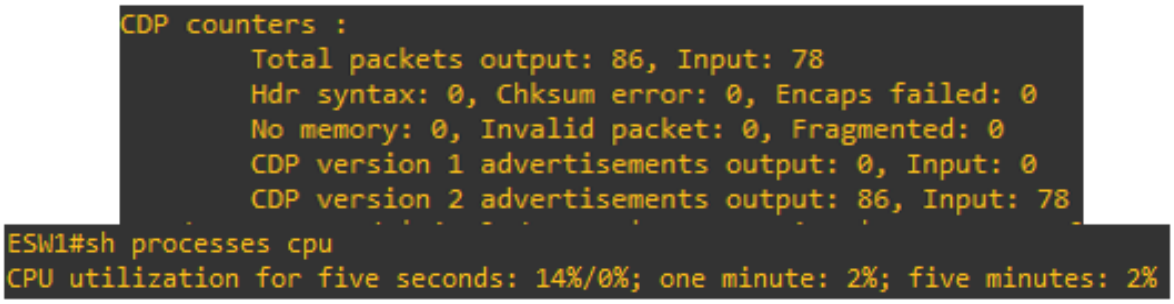


Рисунок 3.2 - Демонстрація навантаження на комутатор до атаки

Для початку атаки в програмному забезпечені «Yersinia» потрібно обрати інтерфейс на який буде націлена атака. Тоді обрати тип атаки а саме «flooding CDP table», і запустити атаку.

Атака на протокол CDP може отримати кілька наслідків:

1. Підроблення даних. Хакери можуть створювати фальшиві CDP-пакети, щоб зробити вигляд справжнього комутатора, або іншого пристрою підключеного до мережі. Наслідком цього може стати передача шкідливого трафіку по мережі;

2. Викрадення інформації про структуру мережі. Під час атаки на мережу, зловмисники можуть отримати доступ до інформації про топологію мережі, включаючи інші комутатори, маршрутизатори чи інші пристрої мережі;

3. Відмова в обслуговуванні. Також атаки можуть спричинити

перевантаження пристрою, що згодом може призвести до відмови в обслуговуванні.

У загальному, атаки такого типу можуть створити значний ризик безпеці мережі, вплинути на її продуктивність та надійність (рисунок 3.3).

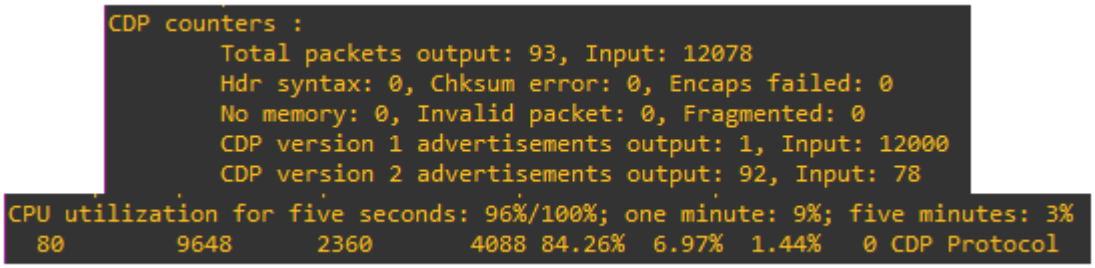


Рисунок 3.3 - Демонстрація навантаження на комутатор після атаки

Згідно з інформацією показаній на рисунку 3.3, можна спостерігати велику кількість вхідних CDP пакетів. І також значне навантаження на процесор комутатора. Як було описано до цього, таке навантаження може спричинити повну відмову в обслуговувані.

Для більш чіткої демонстрації наслідків, слід продемонструвати спробу відправлення ping пакетів з віртуальної імітації ПК яка знаходиться в цій самій мережі, на сервер google (рисунок 3.4).

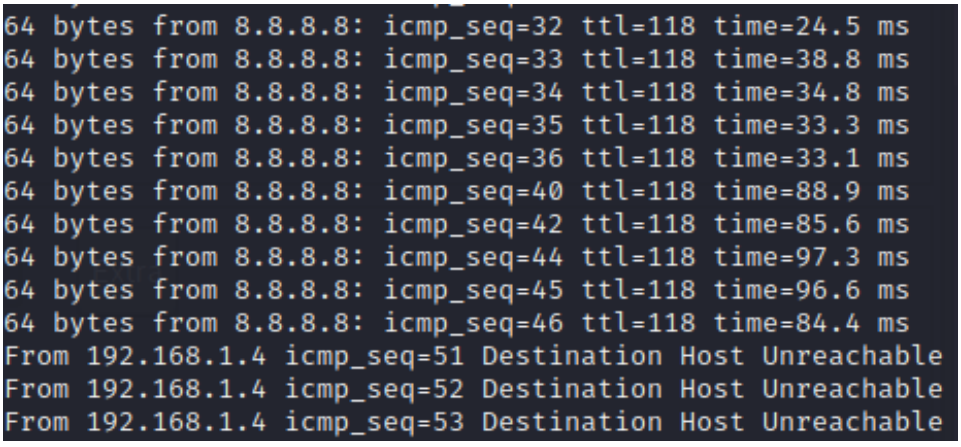


Рисунок 3.4 - Демонстрація спроби пінгування серверу google

Як видно на рисунку 3.4, атака була запущена прямо під час перевірки з'єднання. Як результат можна помітити значне погіршення зв'язку а згодом і повний розрив з'єднання. Тепер необхідно протестувати цю саму атаку на розробленій системі (рисунок 3.5).

```
CPU utilization for five seconds: 2%/0%; one minute: 15%; five minutes: 6%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         3          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2           0       146          0  0.00%  0.00%  0.00%   0 Load Meter
   3        2448       483       5068  1.96%  1.14%  0.61%   0 Exec
```

Рисунок 3.5 - Демонстрація навантаження на комутатор власної системи

Як можна помітити, навантаження на процесор майже немає. Усе навантаження яке є - це інші системні процеси, які не пов'язані із протоколом CDP.

Наступною атакою буде MAC poisoning та MAC flood. Як уже згадувалось обидві ці атаки можуть призвести до значного порушення продуктивності мережі. Для того щоб організувати атаку MAC poisoning потрібно скористуватись раніше описаним програмним забезпеченням PackEth. З допомогою даної програми на потрібно створити шкідливий пакет. Результатом цього дослідження повинно стати повне перехоплення мережевого трафіку одного з користувачів мережі. Для цього на потрібно дізнатись MAC-адресу та IP-адресу жертви. Їх можна знайти в ARP таблиці, яка згодом буде використовуватись в інших атаках (рисунок 3.6).

```
└─# arp -a
? (192.168.1.5) at 00:50:79:66:68:01 [ether] on eth0
? (192.168.1.2) at 00:50:79:66:68:00 [ether] on eth0
? (192.168.1.1) at c4:03:04:98:00:01 [ether] on eth0
```

Рисунок 3.6 - Вміст ARP таблиці.

Для досліду я обрав пристрій з IP-адресою 192.168.1.2 та MAC-адресом 00:50:79:66:68:00. Далі з допомогою PackEth я створив шкідливий пакет та відправив його в мережу (рисунок 3.7).

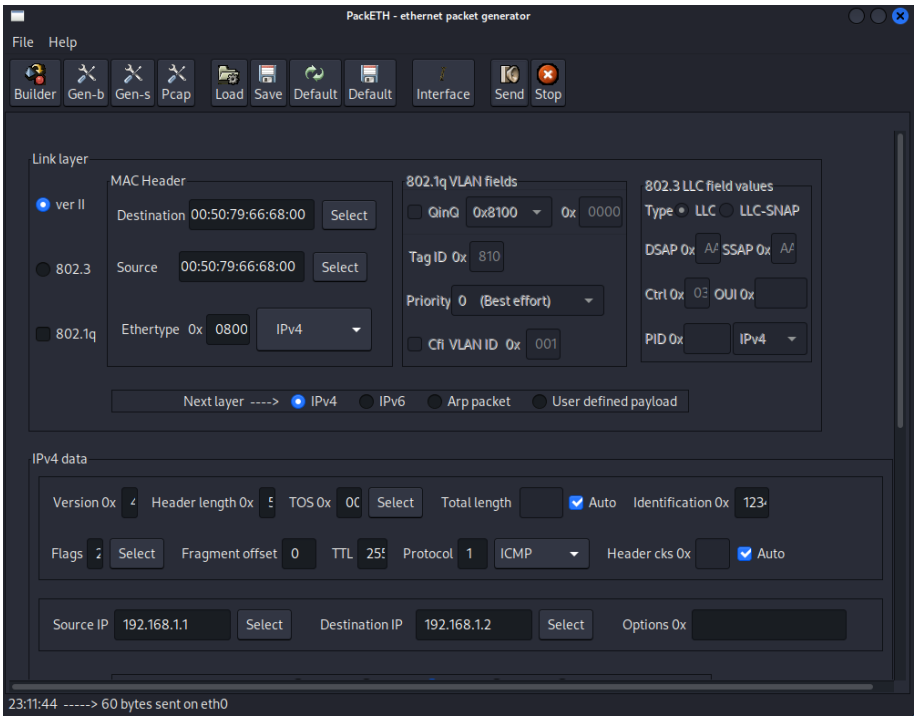


Рисунок 3.7 - Процес створення шкідливого пакету

Для того щоб оцінити результати атаки я завчасно зберіг вміст таблиці MAC адрес на комутаторі. І для порівняння, також переглянув після виконаної атаки (рисунок 3.8).

Vlan	Mac Address	Type	Ports
1	0050.7966.6800	DYNAMIC	Gi0/2
1	0050.7966.6801	DYNAMIC	Gi0/1
1	0800.27c7.e136	DYNAMIC	Gi0/3
1	c403.0498.0001	DYNAMIC	Gi0/0

Vlan	Mac Address	Type	Ports
1	0050.7966.6800	DYNAMIC	Gi0/3
1	0050.7966.6801	DYNAMIC	Gi0/1
1	0800.27c7.e136	DYNAMIC	Gi0/3
1	c403.0498.0001	DYNAMIC	Gi0/0

Рисунок 3.8 - Порівняння таблиці MAC-адрес до та після атаки

Як показано на рисунку 3.8, в таблиці після атаки пристрій з MAC-адресом 0050.7966.6800 підключений до порту Gi0/3. Хоча фізично він підключений до порту Gi0/2. Отже коли інший пристрій в мережі намагатиметься зв’язатись з цим пристроєм, комутатор не буде пересилати його на хост жертву, вони будуть перенаправлені на інших хост. Ця ситуація викликає DoS, так як стає не можливо зв’язатись в цим пристроєм.

Але важливо уточнити, що, як тільки пристрій на який було виконано атаку відправить пакет адресату, комутатор автоматично оновить свою CAM таблицю. І тому запис автоматично стає не пошкодженим. Але зловмисник може продовжити відправляти пошкоджені пакети, що і призведе до нового отруєння CAM таблиці.

Другою атакою на та таблицю CAM є MAC flood. Як уже було згадано раніше, MAC-flood використовується для порушення безпеки мережевих комутаторів. Це досить стара атака, яка націлена на перехоплення мережевого трафіку. Базується ця атака на затоплені таблиці MAC-адрес. Мета полягає в тому, щоб повністю використати обмежену пам’ять в комутаторів, для зберігання таблиці CAM. Іншими словами, коли таблиці MAC-адрес комутаторів переповнюються, вони починають відправляти пакети в широкомовному режимі. І в результаті мережевий трафік може легко бути отриманий іншим пристроєм. Також з можливих наслідків є:

— відключення мережевих пристроїв. Після того як таблиця комутатора переповниться, він може відключати деякі мережеві хости, які будуть намагатися підключитись до мережі;

— значне збільшення навантаження на CPU. Коли комутатор не зможе знайти необхідний MAC-адрес, він почне відправляти всі пакети у широкомовному режимі. І це призведе до збільшення навантаження на центральний процесор, що значно зменшить продуктивність мережевого пристрою;

— погіршення продуктивності мережі. Якщо атака буде продовжуватись

досить довго, то таблиця буде повністю заблокована. І результатом цього стане затруднення пересилання пакетів по мережі, що здом зробить її недоступною для користувачів;

— відкриває можливість для MitM. Після того як комутатор почне відправляти усі пакети в широкомовному режимі, зловмисник з легкістю зможе аналізувати увесь мережевий трафік.

Macof - це спеціальний інструмент, якого основна задача і полягає в затоплені CAM таблиці велико кількістю MAC –адрес (рисунок 3.9).

```
56:6d:72:16:ee:d6 60:76:79:39:b2:da 0.0.0.0.21061 > 0.0.0.0.32543: S 669578902:669578902(0) win 512
9f:b4:14:20:b5:93 62:11:3e:4:da:b7 0.0.0.0.54765 > 0.0.0.0.2575: S 1184587747:1184587747(0) win 512
97:c2:ec:49:bc:80 4:f9:3f:4d:b8:ca 0.0.0.0.36540 > 0.0.0.0.27244: S 1014651868:1014651868(0) win 512
f9:6d:46:54:1f:1c af:ce:7d:71:19:f2 0.0.0.0.31220 > 0.0.0.0.51479: S 334808484:334808484(0) win 512
48:81:b7:1c:4c:ae 4a:ca:df:61:a0:b3 0.0.0.0.60385 > 0.0.0.0.48149: S 2109291113:2109291113(0) win 512
f7:c4:a3:6c:a6:44 79:38:a3:5a:de:f7 0.0.0.0.43375 > 0.0.0.0.40475: S 2145530101:2145530101(0) win 512
e2:af:77:57:17:f3 23:88:c1:55:87:c7 0.0.0.0.41473 > 0.0.0.0.24358: S 190321270:190321270(0) win 512
41:5a:58:1d:ce:bb f7:71:ef:37:c3:a3 0.0.0.0.53718 > 0.0.0.0.23377: S 381662564:381662564(0) win 512
13:2a:9e:43:be:7d da:eb:c4:62:cd:80 0.0.0.0.51000 > 0.0.0.0.40716: S 858179827:858179827(0) win 512
5c:5a:76:6:73:83 70:2c:b8:3e:b7:3e 0.0.0.0.4975 > 0.0.0.0.27900: S 206349107:206349107(0) win 512
```

Рисунок 3.9 - Процес затоплення CAM таблиці

Як і попередніх дослідах, для аналізу результату необхідно порівняти стан комутатора до та після атаки (рисунок 3.10).

```
Dynamic Address Count:                  1
Secure Address (User-defined) Count:    0
Static Address (User-defined) Count:    0
System Self Address Count:              1
Total MAC addresses:                    2
Maximum MAC addresses:                  8192
```

```
Dynamic Address Count:                  8188
Secure Address (User-defined) Count:    0
Static Address (User-defined) Count:    0
System Self Address Count:              1
Total MAC addresses:                    8189
Maximum MAC addresses:                  8192
```

Рисунок 3.10 - Кількість використаних MAC-адрес до та після атаки

Як і у попередніх дослідах, одразу видно наслідки атаки. На рисунку 3.10 зображено кількість можливих і кількість використаних MAC-адрес в таблиці. Так як вони усі використані то новий пристрій буде неможливо під'єднати. А в уже існуючих пристроях значно зменшиться продуктивність передачі інформації, а може навіть повністю зникне. Також можна переглянути таблицю комутатора (рисунок 3.11).

Destination Address	Address Type	VLAN	Destination Port
cc01.0a84.0000	Self	1	Vlan1
0800.27c7.e136	Dynamic	1	FastEthernet1/3
c403.0498.0001	Dynamic	1	FastEthernet1/0
7eba.2e3f.93a6	Dynamic	1	FastEthernet1/3
086f.f761.1094	Dynamic	1	FastEthernet1/3
6e70.c23c.e28e	Dynamic	1	FastEthernet1/3
def6.1c6d.556a	Dynamic	1	FastEthernet1/3
5876.4318.c088	Dynamic	1	FastEthernet1/3
a68b.c64d.d518	Dynamic	1	FastEthernet1/3
9c8c.b56c.0c3a	Dynamic	1	FastEthernet1/3
8e9f.f414.12a0	Dynamic	1	FastEthernet1/3
7232.c102.7b34	Dynamic	1	FastEthernet1/3
3227.3929.d678	Dynamic	1	FastEthernet1/3
0862.d044.40a7	Dynamic	1	FastEthernet1/3
30e6.5868.5999	Dynamic	1	FastEthernet1/3
1461.4e4a.6f0e	Dynamic	1	FastEthernet1/3
74b3.ce0e.014b	Dynamic	1	FastEthernet1/3
28c7.1d07.37e6	Dynamic	1	FastEthernet1/3
7c02.7914.44c6	Dynamic	1	FastEthernet1/3
e46a.4319.344d	Dynamic	1	FastEthernet1/3
def2.5f6c.30d7	Dynamic	1	FastEthernet1/3

Рисунок 3.11 - Вміст MAC-таблиці комутатора

У результаті атаки MAC-flood можуть з'явитись фальшиві записи в MAC-таблиці комутатора. Це стається тому, що шкідливе програмне забезпечення відправляє несправжні мережеві пакети до комутатора. В результаті він створює новий запис кожного разу коли отримує цей шкідливий пакет. Згодом він не може правильно визначити, на який порт потрібно передати пакет, і тому розміщує запис про MAC-адресу на всі порти, або на той, на який прийшов пакет. Якщо атака тривала достатньо довго, то таблиця може бути заповнена фальшивими записами і це може привести до проблем з функціонуванням мережі (рисунок 3.12).

```
64 bytes from 192.168.1.1: icmp_seq=119 ttl=255 time=6.41 ms
64 bytes from 192.168.1.1: icmp_seq=120 ttl=255 time=4.32 ms
64 bytes from 192.168.1.1: icmp_seq=121 ttl=255 time=2.38 ms
64 bytes from 192.168.1.1: icmp_seq=122 ttl=255 time=9.30 ms
64 bytes from 192.168.1.1: icmp_seq=123 ttl=255 time=249 ms
64 bytes from 192.168.1.1: icmp_seq=126 ttl=255 time=273 ms
64 bytes from 192.168.1.1: icmp_seq=127 ttl=255 time=246 ms
64 bytes from 192.168.1.1: icmp_seq=128 ttl=255 time=255 ms
64 bytes from 192.168.1.1: icmp_seq=130 ttl=255 time=358 ms
64 bytes from 192.168.1.1: icmp_seq=131 ttl=255 time=246 ms
```

Рисунок 3.12 - Демонстрація зниження з'єднання під час атаки

Тепер необхідно протестувати даний тип атаки на системі власної розробки (рисунок 3.13).

Destination Address	Address Type	VLAN	Destination Port
cc02.45ac.0000	Self	1	Vlan1
cc02.45ac.0000	Self	4	Vlan4
0800.2704.76d1	Dynamic	2	FastEthernet1/10
0ca8.122a.0002	Dynamic	2	FastEthernet1/0
0ca8.122a.0002	Dynamic	3	FastEthernet1/0
0050.7966.6800	Dynamic	3	FastEthernet1/12

Рисунок 3.13 - Вміст MAC-таблиці комутатора захищеної системи

За результатами мережа витримала атаку MAC-poisoning і MAC-flood, це означає, що мої заходи забезпечення безпеки працюють ефективно. MAC-poisoning та MAC-flood - це типи атак на мережу, які можуть призвести до зниження швидкості мережі, переповнення таблиць комутації та інших проблем з мережевою доступністю [39].

Щоб запобігти цим атакам, я використав методи захисту порту комутатора. Моя мережа успішно відбила атаку, це свідчить про те, що я вжив досить ефективних заходів забезпечення безпеки мережі.

Наступна досить типова атака це отруєння ARP кешу. Для більш детального дослідження наслідків, як і в попередніх експериментах потрібно оцінити ціль до та після атаки, а саме її ARP таблицю (рисунок 3.14).

```
PC1> arp

c4:03:04:98:00:01  192.168.1.1 expires in 109 seconds
00:50:79:66:68:00  192.168.1.2 expires in 113 seconds
08:00:27:c7:e1:36  192.168.1.10 expires in 116 seconds
```

Рисунок 3.14 - ARP таблиця PC1

Як показано на рисунку, записи в таблиці тимчасові. Тому потрібно використати другий метод отруєння, а саме створення нового фальшивого запису. Як і в попередніх дослідах потрібно власноруч створити підроблений пакет ARP на хост PC1. Це можна зробити за допомогою вже раніше використовуваного PackEth (рисунок 3.15).

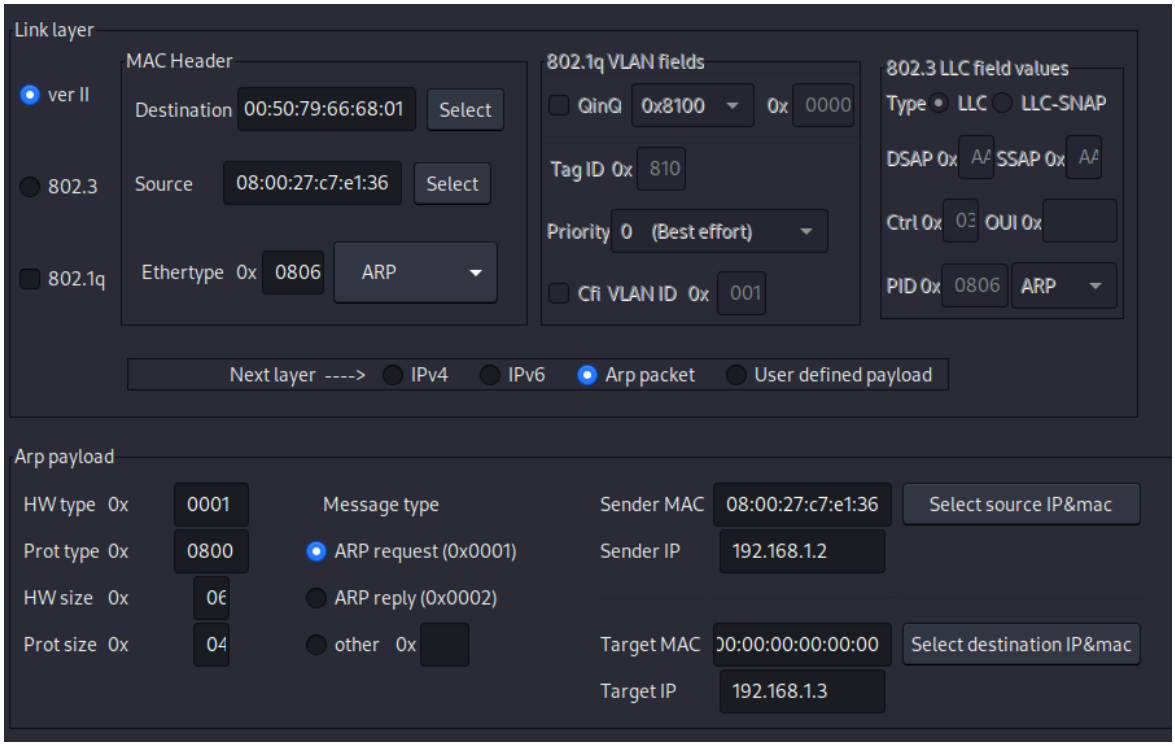


Рисунок 3.15 - Створення фальшивого ARP-запиту

Як видно на рисунку 3.16, таблиця має інший вигляд. Деякі записи зникли, так як вони автоматично видаляються через деякий час. І з'явився дещо інший запис. В ньому співставленні MAC-адрес, який раніше належав пристрою зловмисника і IP-адрес, який належить сусідньому віртуальному комп'ютеру. Тому поки таблиця вузла PC1 буде залишатись пошкодженою,

весь мережевий трафік, який відправляється вузлом PC1 на PC2, буде перенаправлятись на вузол зловмисника. Ця атака схожа на MitM, але не до кінця реалізована [40].

```
PC1> arp

08:00:27:c7:e1:36  192.168.1.2 expires in 114 seconds
```

Рисунок 3.16 - Вигляд отруєної таблиці PC1

Наступна атака - це логічний розвиток попередньої. DoS-атака, яка базується на отруєні кешу ARP, полягає в тому, щоб не дати хосту-жертві отримати зв'язок з одним чи декілька вузлами в локальній мережі. По-перше, шкідливий хост пошкоджує кеш ARP хоста-жертви, використовуючи метод отруєння кеша ARP. Таким чином, кеш ARP хоста жертви оновлюється підробленими записами (IP-адресою та MAC-адресою), що відповідає неправильній асоціації IP-адрес та неіснуючих MAC адрес. Пізніше, коли хост-жертва спробує відправити пакети на інший пристрій, пакет буде відправлений на неіснуючий вузол, викликаючи ситуацію атаки DoS. Отже, хост-жертва не зможе відправляти пакети хосту-одержувачу.

Ця атака може бути особливо ефективною в тому випадку, коли у хоста-жертви та потенційного хосту-одержувача є велика кількість обмінів даними в рамках мережі, так як це може призвести до значних перебоїв у роботі.

Для реалізації даної атаки потрібно знову створити несправжній пакет (рисунок 3.17), в якому будуть поєднані справжній IP-адрес сусіднього хоста і неіснуючий MAC-адресом.

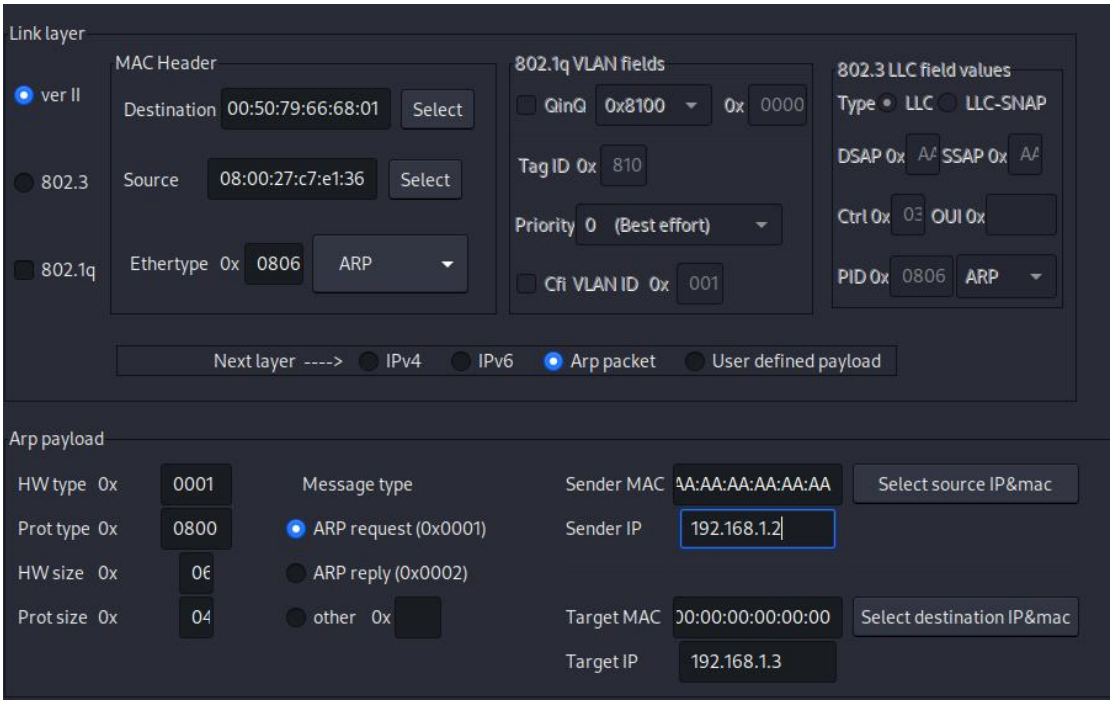


Рисунок 3.17 - Процес створення пакетів для DoS атаки на PC1

На рисунку 3.17 зображено створення шкідливого пакета одно адресного ARP-запиту для ушкодження кеша ARP вузла PC1. На рисунку 3.18, буде показано вміст отруєної кеша ARP вузла PC1 після атаки.

```
aa:aa:aa:aa:aa:aa  192.168.1.1 expires in 53 seconds
aa:aa:aa:aa:aa:aa  192.168.1.2 expires in 55 seconds
aa:aa:aa:aa:aa:aa  192.168.1.4 expires in 58 seconds
```

Рисунок 3.18 - Вигляд отруєної ARP таблиці PC1

Раніше було згадано, що можна провести атаку DoS і зробити для цього вузла недоступним один або декілька інших вузлів. Зрозуміло, щоб став недоступний тільки один пристрій то потрібно створити тільки один відповідний запис в таблиці. А щоб повністю відгородити даний пристрій від мережі, потрібно заповнити таблицю усіма можливими шкідливими записами якими він може скористатись для встановлення з'єднання з іншими пристроями. Тому я створив додаткові записи з IP-дресами сусіднього пристрою та маршрутизатора. Також, як і в попередніх дослідах потрібно

перевірити наслідки атаки, а саме спробувати з’єднатись з іншими пристроями чи з глобальною мережею (рисунок 3.19).

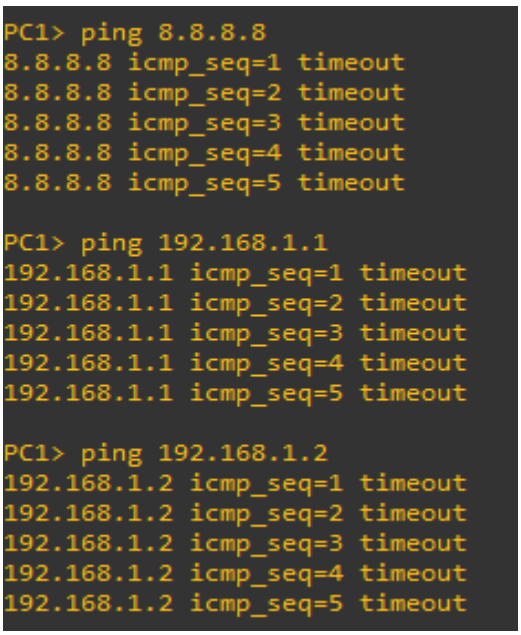


Рисунок 3.19 - Ситуація DoS на пристрої PC1

На рисунку 3.19 продемонстрована спроба зв’язатись з глобальною мережею потім з маршрутизатором і сусіднім пристроєм. Як і очікувалось в пристрою-жертви повністю зник зв’язок.

Наступним підтипом атаки ARP-poisoning є атака MitM. За такими атаками зазвичай стоїть схема, в якій зловмисник розташований між користувачем та сервером. Цей процес є непомітним для обох сторін і сприймається як звичайний обмін даними, проте насправді нападник може перехоплювати та змінювати інформацію, яка передається. Це може бути використано для викрадення паролів, конфіденційної інформації та інших видів кібератак та шахрайства.

Дана атака полягає у пере направленні мережевого трафіку між двома цільовими вузлами на шкідливий вузол. Потім зловмисний хост перенаправляє отримані пакети в початкове місце призначення, так що зв'язок між двома цільовими хостами не буде перерваний, і користувачі обох хостів не помітять,

що їхній трафік перехоплюється зловмисником.

При таких атаках зловмисний користувач спочатку включає маршрутизацію IP-пакетів свого хоста, щоб працювати як маршрутизатор і мати можливість пересилати перенаправлені пакети. Потім, використовуючи техніку отруєння кеша ARP, зловмисний користувач пошкоджує кеші ARP двох цільових хостів, щоб змусити два хоста переслати всі свої пакети шкідливому хосту. Це надзвичайно ефективно, якщо врахувати, що можуть бути отруєні не лише хости, а й маршрутизатори/шлюзи. Весь інтернет-трафік для хоста може бути перехоплений за допомогою атаки MitM на хост та маршрутизатор локальної мережі (рисунок 3.20).

Для проведення такої атаки потрібно буде постійно створювати шкідливі пакети. Щоб це процес автоматизувати краще використати інструмент який спеціалізується для даної атаки. Arpspoof - це інструмент, який дозволяє здійснювати атаку "ARP spoofing" в локальній мережі.

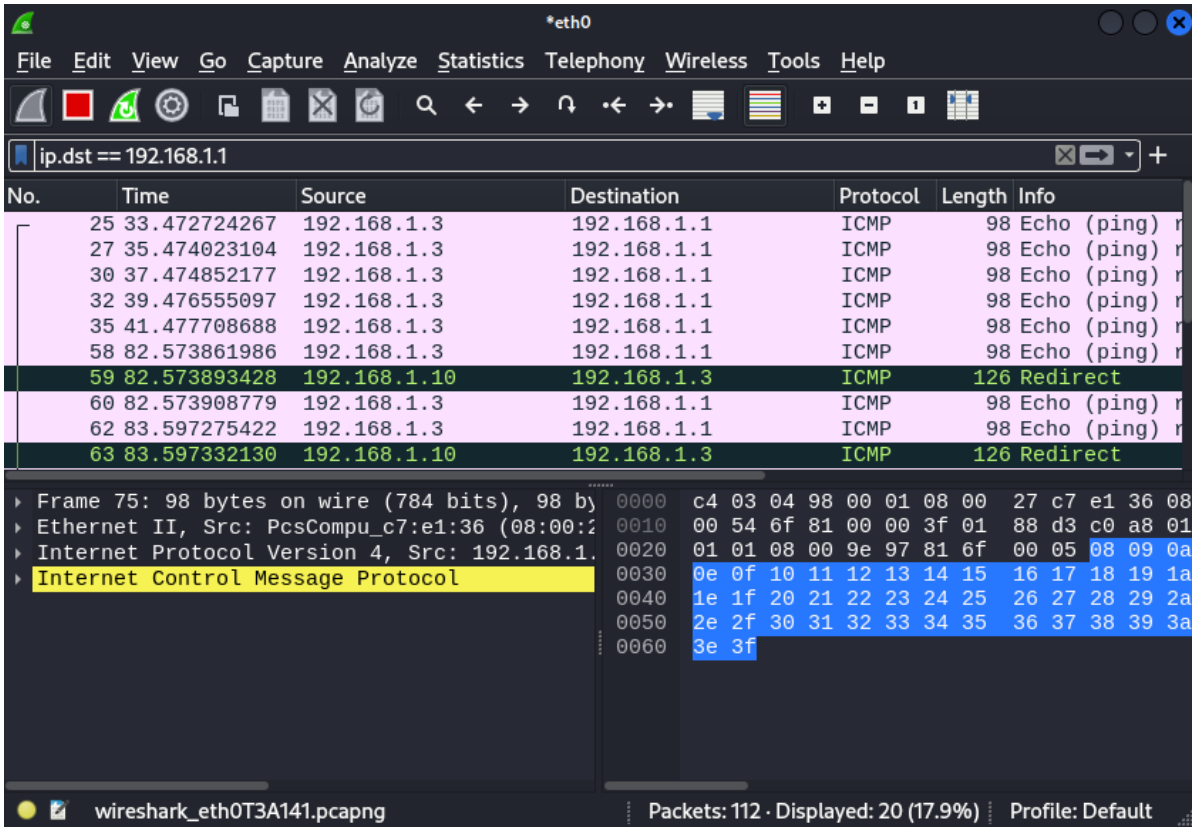


Рисунок 3.20 - Процес перехоплення мережевого трафіку

Після проведення атаки з’являється можливість повністю перехоплювати трафік за допомогою спеціалізованого програмного забезпечення. У моєму випадку я використав wireshark. Як показано на рисунку 3.20, пристрій зловмисника може проаналізувати пакети які відправлялися вузлу з ip-адресом 192.168.1.1 від 192.168.1.3 і навпаки.

Щоб атака справді вважалася успішною, зв’язок між пристроями повинен залишитися, що і показано на рисунку 3.21.

```
PC1> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=255 time=7.976 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=255 time=7.509 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=255 time=6.706 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=255 time=6.577 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=255 time=6.727 ms
```

Рисунок 3.21 - Демонстрація справного зв’язку після атаки

Отже залишилось протестувати власну система на вразливість до цієї атаки (рисунок 3.22).

```
SW1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.4.100           -   cc02.45ac.0000  ARPA   Vlan4

SW1#sh processes cpu
CPU utilization for five seconds: 12%/0%; one minute: 2%; five minutes: 1%
```

Рисунок 3.22 - Демонстрація завантаженості на комутатор та його ARP-таблиця

На рисунку 3.22 зображені дані з комутатора моєї мережі. З-за допомогою них можна зробити висновок, що моя мережа не є вразливою до атак на протокол ARP, тобто можна припустити, що налаштування, які я виконав в попередньому розділі успішно захистили мою мережу.

3.2 Рекомендації по створенню політик безпеки

Звичайно важливим елементом, створення успішна робота системи безпеки є політика безпеки. Щоб забезпечити безпеку організації, необхідно мати конкретну мету та план дій, і навіть найсучасніші заходи захисту не допоможуть без цього. Для визначення керівної ідеї потрібні загальні уявлення про напрямки дій, тому політика безпеки - це важлива концепція. Отже, ось кілька загальних кроків, які можна включити в політику безпеки:

— потрібно встановити стандарти паролів. Необхідно вимагати складних паролів, які складаються з комбінацій символів, цифр та великих і малих літер. Рекомендовано змінювати паролі принаймні раз на квартал, і не дозволяти використовувати ті ж самі паролі для кількох облікових записів;

— встановити політику блокування екрану. Змусити користувачів блокувати свої комп'ютери, якщо вони не працюють на них, і вимагати пароль для розблокування;

— регулярно проводити навчання з безпеки інформації. Необхідно проводити тренінги та навчальні курси для всіх співробітників, щоб показати їм, як виявляти шахрайства, фішингові атаки та інші загрози безпеці;

— обов’язково використовувати антивірусне програмне забезпечення. Потрібно інсталювати антивірусне програмне забезпечення на всіх пристроях в офісі та переконатися, що воно постійно оновлюється;

— регулярно перевіряти права доступу. Потрібно обмежити доступ до конфіденційних даних тільки для співробітників, які повинні мати доступ до них, і перевіряти ці права на регулярній основі;

— забезпечити резервне копіювання даних. Регулярно робити резервні копії важливих даних і зберігати їх в безпечному місці, окрім того, потрібно переконатися, що завжди є можливість відновити дані з цих копій у разі необхідності.

Також важливо враховувати зміни у загрозах та технологіях з часом і

оновлювати свої політики відповідно. Регулярно проводьте перегляд та аудит своїх політик безпеки, щоб переконатися в їх ефективності та актуальності.

Нарешті, потрібно не забувати про важливість залучення всіх співробітників до практик безпеки. Співробітники повинні бути навчені про правила безпеки інформації та зобов'язання їх дотримуватися. Також можна встановити систему відповідальності за порушення політики безпеки, що допоможе забезпечити її ефективність.

3.3 Висновок

Отже по завершенню цього розділу, можна зробити декілька висновків. У цьому розділі я провів декілька тестувань захищеності власної захищеної мережі та іншої мережі, яка потенційно могла б використовуватись в підприємстві.

Я змоделював декілька типових мережевих атак на мережеві процеси та протоколи. На основі цих результатів я зрозумів, що необхідність в такій системі захисту є однією з першочергових. Адже навіть такі типові атаки змогли нанести досить сильне порушення безпеки та значно зменшити ефективність передачі даних.

Також я надав певні рекомендації по створенню політик безпеки. Як було раніше, при розробці системи безпеки не можна цілком покладатися на технічні засоби. Навіть найсучасніші апаратні пристрої захисту або системи запобігання вторгненням повністю не захистять організацію, якщо відсутня конкретна мета та хоча б приблизний план її досягнення.

ВИСНОВКИ

На сьогодні перегони озброєнь хакерів та спеціалістів з безпеки набрали над швидких обертів. В світі починають набирати популярності цілі кібер війни, тому в такий час необхідно знайти мотивацію створювати все досконаліші системи захисту.

З виконанням даної кваліфікаційної роботи я отримав глибокі знання про теоретичні основи систем безпеки інформаційної системи.

У першому розділі було проведено визначення понять "безпека інформаційної системи" та "мережева атака", оглянуто існуючі методи захисту інформаційної системи від мережевих атак та проаналізовані можливі загрози безпеці інформаційної системи Відділення Приватбанку.

У другому розділі проведено розробку системи безпеки інформаційної системи на основі вибраної оптимальної архітектури комп'ютерної мережі для Відділення Приватбанку, розроблено та імплементовано систему захисту від мережевих атак на базі цієї архітектури та надані додаткові процедури для створення системи захисту.

У третьому розділі проведено оцінку ефективності розробленої системи захисту від мережевих атак, аналіз економічної доцільності використання розробленої системи та порівняння з існуючими рішеннями на ринку з подальшими рекомендаціями щодо подальших покращень.

Виконання даної кваліфікаційної роботи дозволило студенту здобути глибокі знання про безпеку інформаційних систем та навички розробки системи безпеки для конкретного відділення Приватбанку у м. Хмельницькому, що можуть бути корисними у майбутній професійній діяльності.

В загальному потрібно сказати, що ні один спеціаліст не зможе створити ідеальну систему безпеки, яка забезпечить цілковитий захист, але це не привід самостійно не створювати щось, що буде прямувати до ідеальної системи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Protocol TCP/IP. *Fortinet*. URL: https://www.fortinet.com/resources/cyberglossary/tcp-ip (дата звернення: 12.04.2023).

2. TCP/IP Deep Dive Analysis with Wireshark. *Wireshark* URL: https://www.wireshark.org/docs/ (дата звернення: 27.04.2023).

3. Routing Information Protocol. *IBM*. URL: https://www.ibm.com/docs/en/i/7.1?topic=routing-information-protocol (дата звернення: 15.04.2023).

4. Blokdyk G. Routing Information Protocol a Complete Guide - 2020 Edition. Emereo Pty Limited, 2020. 308 c.

5. IP address (Internet Protocol address). *TECHTARGET NETWORK* URL: https://www.techtarget.com/whatis/definition/IP-address-Internet-Protocol-Address (дата звернення: 18.04.2023).

6. Cisco Discovery Protocol (CDP). *Cisco* URL: https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x (дата звернення: 18.04.2023).

7. Topology Discovery Using Cisco Discovery Protocol. URL: https://arxiv.org/ftp/arxiv/papers/0907/0907.2121.pdf (дата звернення: 20.04.2023).

8. CDP FLOODING. *NETVEL* URL: https://netvel.sk/en/cdp-flooding-attack-2/ (дата звернення: 21.04.2023).

9. CDP Flooding. *Nabil Abdat*. URL: https://nabeelabdat.wordpress.com/2016/08/12/cdp-flooding/ (дата звернення: 21.04.2023).

10. Basic Network Attacks in Computer Network. URL: https://www.geeksforgeeks.org/basic-network-attacks-in-computer-network/ (дата звернення: 22.04.2023).

11. MAC address (media access control address) URL:

https://www.techtarget.com/searchnetworking/definition/MAC-address (дата звернення: 24.04.2023).

12. Network Attack and Defense. URL: https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c21.pdf (дата звернення: 25.04.2023).

13. What is defense in depth. URL: https://www.cloudflare.com/learning/security/glossary/what-is-defense-in-depth/ (дата звернення: 27.04.2023).

14. MAC flooding attack and How to prevent MAC flooding attack. URL: https://www.omnisecu.com/ccna-security/what-is-mac-flooding-attack-how-to-prevent-mac-flooding-attack.php (дата звернення: 27.04.2023).

15. ARP Spoofing URL: https://www.imperva.com/learn/application-security/arp-spoofing/ (дата звернення: 24.04.2023).

16. Network Attacks and Network Security Threats. URL: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/ (дата звернення: 30.04.2023).

17. Dynamic Host Configuration Protocol (DHCP). URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top (дата звернення: 24.04.2023).

18. Understanding and Preventing DHCP Starvation Attacks. URL: https://ritcsec.wordpress.com/2022/05/06/understanding-and-preventing-dhcp-starvation-attacks/ (дата звернення: 01.05.2023).

19. What Is Network Security. URL: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html (дата звернення: 03.05.2023).

20. GNS3. URL: https://docs.gns3.com/docs/ (дата звернення: 03.05.2023)

21. TCP/IP Deep Dive Analysis with Wireshark. URL: https://www.wireshark.org/docs/ (дата звернення: 05.05.2023)

22. PackEth. *UBUNTU manuals* URL:

https://manpages.ubuntu.com/manpages/trusty/man1/packeth.1.html (дата звернення: 07.05.2023).

23. Computer Network Architecture. URL: https://www.javatpoint.com/computer-network-architecture (дата звернення: 08.05.2023)

24. Computer Network Architecture. URL: https://www.uobabylon.edu.iq/eprints/publication_12_22267_1450.pdf (дата звернення: 10.05.2023)

25. Hierarchical Network Model. URL: https://networkdirection.net/articles/network-theory/hierarchicalnetworkmodel/ (дата звернення: 11.05.2023)

26. Most Common Types Of Network Vulnerabilities. URL: https://www.digitaldefense.com/blog/what-are-the-most-common-types-of-network-vulnerabilities/ (дата звернення: 13.05.2023)

27. Network Security in 2023: Threats, Tools, and Best Practices. URL: https://www.catonetworks.com/network-security/ (дата звернення: 13.05.2023)

28. Firewall. URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/ (дата звернення: 13.05.2023)

29. Dynamic Trunking Protocol. URL: https://www.grandmetric.com/knowledge-base/design_and_configure/how-to-configure-dynamic-trunking-protocol-dtp-cisco/ (дата звернення: 15.05.2023)

30. Configuring Port Security. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/sec_port.html (дата звернення: 17.05.2023)

31. Port Security on Cisco IOS Switch. URL: https://www.geeksforgeeks.org/configuring-port-security-on-cisco-ios-switch/ (дата звернення: 17.05.2023)

32. Cisco IOS. URL: https://docs.oracle.com/en-us/iaas/Content/Network/Reference/ciscoiosCPE.htm (дата звернення:

20.05.2023).

33. Defense Against ARP Flood Attacks. URL: https://support.huawei.com/enterprise/en/doc/EDOC1000178177/a7ad216c/defense-against-arp-flood-attacks (дата звернення: 22.05.2023).

34. What are cyber threats and how to safeguard your data. URL: https://preyproject.com/blog/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them (дата звернення: 23.05.2023).

35. ARP Spoofing or ARP Poisoning. URL: https://www.wallarm.com/what/arp-spoofing-or-arp-poisoning (дата звернення: 24.05.2023).

36. Networking Software. URL: https://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html (дата звернення: 24.05.2023).

37. Network Security. URL: https://www.forcepoint.com/cyber-edu/network-security (дата звернення: 25.05.2023).

38. Computer Network Defense. URL: https://www.roguelogics.com/computer-network/?utm_source=rss&utm_medium=rss&utm_campaign=computer-network (дата звернення: 26.05.2023).

39. Data-Link Layer: MAC Flooding. URL: https://www.vicarius.io/vsociety/blog/data-link-layer-mac-flooding (дата звернення: 26.05.2023).

40. ARP Spoofing or ARP Poisoning. URL: https://www.wallarm.com/what/arp-spoofing-or-arp-poisoning (дата звернення: 27.05.2023).

ДОДАТОК А

(обов’язковий)

Графічна частина

ЗАГРОЗИ	НАСЛІДКИ	ЗАПОБІГАННЯ
CDP flooding	завантаження ЦП пристороюCisco, відмова в обслуговувані	відключення протоколу на пристрої
ARP spoofing	перехоплення зв'язку між двома пристроями, відмова в обслуговувані	ARP inspectin
MAC poisoning	зміна роботи комутатора на принцип роботи концентратора	налаштуванн port security на пристрої
DHCP starvation	ічерпання всіх доступних IP-адрес, MitM	DHCP - snooping
DTP attack	отримання доступу до сісідніх підмереж	вручну налаштувати порт на режим access

					КРКБ 190102.19.01.03 ПЗ
Зм.	Арк.	№ докум.	Підпис	Дата	Логічна топологія захищеної мережі
Розроб.		Главюк В.С			Літера: — Маса: — Масштаб: —
Перевір.		Джулій В.М			Аркуш 2 / Аркушів 3
Н.Контр.		Мостовий С.В			ХНУ КБ-19-1
Т.Контр.					
Затв.		Кльоц Ю.П			

					КРКБ 190102.19.01.03 ПЗ	
Зм.	Арк.	№ докум.	Підпис	Дата	Загальна схема побудови системи захисту	Літера / Маса / Масштаб
Розроб.		Гловюк В.С				
Перевір.		Джулій В.М				Аркуш 3 / Аркушів 3
Н.Контр.		Мостовий С.В				
Т.Контр.						ХНУ КБ-19-1
Затв.		Кльоц Ю.П				

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015417572

Дата перевірки:
04.06.2023 22:10:16 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
04.06.2023 22:11:02 EEST

ID користувача:
100008300

Назва документа: **Гловюк**

Кількість сторінок: **63** Кількість слів: **11797** Кількість символів: **88367** Розмір файлу: **2.38 MB** ID файлу: **1015080230**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

3.52%
Схожість

Найбільша схожість: **1.42%** з джерелом з Бібліотеки (ID файлу: **1011379842**)

2.88% Джерела з Інтернету	95	Сторінка 65
2.43% Джерела з Бібліотеки	73	Сторінка 66

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Підозріле форматування	11 сторінок

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 11%**

	Документ		Сумарний збіг по Базі Даних	
ID: 114653 Назва: Система безпеки інформаційної системи від мережевих атак на базі безпечної комп'ютерної мережі Відділення Приватбанку у м. Хмельницькому Додано в БД: 2023-06-04 Автора: Гловюк В.С. Керівники: Джулій В.М. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	66581	1050	637 (1%)	15 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Метод організації тестових випробувань цифрового об'єкта діагностування із застосуванням нечіткої логіки

Автор: Головюк Володимир Сергійович
Спеціальність: 125 – Кібербезпека
Освітня програма: Кібербезпека
Науковий керівник: Чешун Віктор Миколайович, к.т.н, доцент
Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 96.48%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 100%.

Згідно з Положенням про дотримання академічної доброчесності в Хмельницькому національному університеті (http://www.khnu.km.ua/root/files/01/10/03/0005.pdf) така авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту.

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1. Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 3.52%, з яких 1.42% є збігами з одним джерелом, зумовленими наявністю типових фразеологічних виразів предметної області, а також формулюваннями, які утворюють загальновживані фрази.
2. Інші три збіги є збігами в назвах використаних друкованих видань, розміщених в переліку джерел посилань

Керівник роботи _____ В.М. Джулій

Завідувач кафедри кібербезпеки _____ Ю. П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Гловюк В.С.
Тема: «Система безпеки інформаційної системи від мережевих атак на базі безпечної комп'ютерної мережі відділення Приватбанку у м. Хмельницькому»
Галузь знань 12 «*Інформаційні технології*»
Спеціальність 125 - «*Кібербезпека*»
Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 63;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена дослідженню питань, пов'язаних з розробкою та впровадженням системи захисту інформаційної системи від мережевих атак на базі безпечної комп'ютерної мережі. Для досягнення цієї мети було виконано аналіз можливих мережевих загроз та вразливостей та обрано відповідні методи захисту та запобігання. Робота має на меті допомогти підприємству створити безпечну систему для передачі та зберігання конфіденційної інформації, створити зручні механізми для підтримки та подальшого вдосконалення цієї системи.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проведено аналіз існуючих мережевих вразливостей, які можуть нанести значну шкоду системі. Та відповідних захисних рішень, щоб усунути ці недоліки. У другому розділі було проаналізовано вимоги та потреби підприємства з урахуванням специфіки, визначено необхідні компоненти мережі та обрано на основі цього аналізу необхідну мережеву архітектуру. На основі створеної архітектури, було створено та налаштовано необхідну безпечну мережеву інфраструктуру. У третьому розділі була виконана оцінка ефективності та тестування захищеності від типових мережевих атак.

4. Позитивні сторони кваліфікаційної роботи полягають у тому що, застосування відповідних пристроїв і процедур дозволило забезпечити надійний захист від мережевих атак на систему. Підприємство отримало нову захищену систему на основі безпечних мережі, яка може впоратись з великим навантаження та стримати інші типові мережеві атаки. Завдяки застосуванню відповідних технологій та процедур вдалося забезпечити більш високий рівень захисту інформації та скоротити можливість несанкціонованого доступу. Реалізована система є надійним інструментом для використання підприємством ціллю якого є передача конфіденційної інформації.

5. Негативні сторони проекту: В розробленій системі захисту через деякий час може з'явитися недолік недостатньої оновленості програмного та апаратного забезпечення.

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому Загальна оцінка кваліфікаційної роботи є позитивною. Весь матеріал в ній структурований та є чітким та послідовним. Усі розділи роботи мають логічну послідовність, що забезпечує зрозуміння представленого матеріалу в рамках заданої тематики. Пояснювальна записка містить багато наглядних пояснень. Графічний матеріал допомагає наочно проілюструвати доцільність та ефективність прийнятих рішень для досягнення мети проектування.

8. Інші зауваження Деякі окремі аналізи захищеності подані занадто деталізовано, що може ускладнити сприйняття матеріалу.

9. Оцінка дипломної роботи Оцінивши представлену кваліфікаційну роботу, можна зробити висновок, що робота заслуговує оцінки «відмінно/ A (4,75)».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Гурман Іван Васильович, к.т.н, доцент кафедри інженерія програмного забезпечення, Хмельницького національного університету

«_7_» _____червня_____ 2023 . _____ (підпис)