МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ATICE'2025)

ОДЕСА, УКРАЇНА, 18 ЛИПНЯ 2025 Р.

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

ОДЕСА

2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

INTERNATIONAL HUMANITARIAN UNIVERSITY

INTERNATIONAL CONFERENCE

ADVANCED TECHNOLOGY IN INFORMATION AND COMMUNICATION ENGINEERING

(ATICE'2025)

ODESA, UKRAINE, JULY 18, 2025

CONFERENCE PROCEEDINGS

ODESA

2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

Одеса, Україна, 18 липня 2025 р.

Видавничий дім
«Гельветика»
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL HUMANITARIAN UNIVERSITY

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2025)

Odesa, Ukraine, July 18, 2025

Conference Proceedings

Видавничий дім
«Гельветика»
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025)

Одеса, Україна, 18 липня 2025 р.

Матеріали конференції

Видавничий дім
«Гельветика»
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings. Odesa : International humanitarian university, 2025, 123 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції. Міжнародний гуманітарний університет, 2025. – Одеса: Видавничий дім «Гельветика», 2025. – 123 с.

ISBN 978-617-554-582-9

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГЛОБА Л. С . – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

РУСУ О.П. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.

ЙОНА Л.Г. – к.т.н., доц., Міжнародний гуманітарний університет, Одеса, Україна.

МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.

ПЕДЯШ В.В. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КУЧАЙ О.В. - д.п.н., проф., Національний університет біоресурсів і природокористування України.

ЖИГУЛІН О.А. – д.е.н., проф., Міжнародний гуманітарний університет, Одеса, Україна

ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

2. С. Славінський, «Застосування методів машинного навчання для виявлення фальсифікацій у цифрових документах», КПІ ім. І. Сікорського, магістерська дисертація, 2021. URL: https://ai.kpi.ua/ua/masters/thesis/28521smai-slavinskyi_magistr.pdf

3. CoinMarketCap. Повне гомоморфне шифрування (FHE). URL: https://coinmarketcap.com/academy/uk/glossary/fully-homomorphic-encryption

4. bip.net.ua. «Як підприємцю організувати електронний документообіг». URL: https://bip.net.ua/articles/yak-pidpryyemczyu-organizuvaty-elektronnyj-dokumentoobig/

5. І. М. Шевченко, С. Ю. Смоляр, «Блокчейн у забезпеченні цілісності електронних документів», Журнал якісних моделей та технологій, №2, 2023. URL: https://jqmth.donnu.edu.ua/article/download/14956/14862

6. Національний департамент інформатизації. «Сучасні загрози цифровим даним та методи захисту», Електронний репозиторій НДІПППП. URL: https://repository.ndippp.gov.ua/handle/765432198/1050

Петков Євген Ігорович.
Аспірант, спеціальність 125
“Кібербезпека та захист інформації”,
Міжнародний гуманітарний університет
yepetkov@gmail.com
Науковий керівник
Йона Лариса Григорівна, к.т.н.,
Завідувач, доцент кафедри Комп’ютерної інженерії та інноваційних технологій
Факультету Кібербезпеки, програмної інженерії та комп’ютерних наук
Міжнародного гуманітарного університету
yonalarisa66@gmail.com

ТИПИ СПУФІНГ АТАК ТА ЗАСОБІВ ЗАХИСТУ В ЛОКАЛЬНИХ МЕРЕЖАХ

Анотація. *Дослідження розглядає типи Spoofing-атак та засобів боротьби з ними в мережі рівня доступу.*

Атаки типу спуфінг (spoofing) — це категорія кібератак, у яких зловмисник маскується під іншу особу або пристрій, щоб обдурити користувача, систему або мережу. Основна мета таких атак — отримати несанкціонований доступ, перехопити конфіденційні дані або ввести в оману.

MAC Spoofing атаки. Як правило, мережевий коммутатор L2 рівня за замовчуванням динамічно вивчає MAC-адресу пристроя підключеного до порту, та не контролює кількість MAC-адрес, які він може вивчити на одному порту, і не блокує записи в CAM-таблиці. Зловмисник може використати ці вразливості декількома способами.

- По-перше, підробити (продублювати) MAC-адресу іншого легітимного хоста в локальній мережі. Хакер відправляє Ethernet кадр з такою ж самою MAC-адресою

відправника, і комутатор оновить в своїй CAM-таблиці запис, що посилається на викрадену MAC-адресу вже за портом підключення зловмисника, а не легітимного пристроя. Приклад атаки зображено на рис.1.

- По-друге, зловмисник може швидко заповнити CAM таблицю комутатора, надсилаючи велику кількість Ethernet кадрів, з різними підробленими MAC-адресами відправника. Після переповнення CAM-таблиці комутатор починає відправляти кадри широкомовним способом на всі свої порти, фактично діючи як хаб. Зловмисник таким чином може отримувати трафік, який йому не відправлявся. Це є MAC flooding, різновид атаки типу MAC Spoofing.

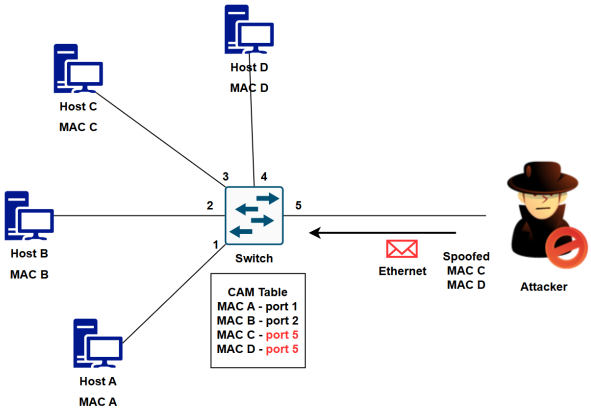

Рисунок 1 – Приклад атаки типу MAC Spoofing

Для боротьби з MAC Spoofing атаками можна використовувати такий функціонал комутаторів доступу як Port security. Активація його дозволяє: по-перше, обмежити кількість MAC-адрес вивчаємих на порту комутатора, по-друге, прив'язати певні MAC-адреси до певних портів комутатора в CAM-таблиці після їх першого вивчення.

Іншим засобом боротьби з MAC Spoofing може використовуватись протокол 802.1x для аутентифікації підключених пристроїв та запобіганню їх несанкціонованому доступу до мережі. Клієнт (який має підтримувати протокол 802.1x) отримає повний доступ до мережі тільки після успішної аутентифікації.

DHCP Spoofing атаки. В основі цього типу атаки лежить підробка зловмисником DHCP сервера в локальній мережі. Легітимні пристрої, які налаштовані на отримання конфігурації мережевого підключення по протоколу DHCP, відправляють запит в локальній мережі (при цьому перший пакет DHCP Discover як правило широкомовний і розсилається всім хостам в підмережі). На цьому етапі зловмистник (фальшивий DHCP сервер) може перехопити клієнтський запит та надіслати назад пропозицію DHCP Offer із підробленими параметрами підключення (IP-адреси, шлюза за замовчуванням, DNS серверів), а відповідно клієнт може прийняти цю пропозицію від нелегітимного DHCP серверу раніше ніж від легітимного. Приклад атаки зображено на рис.2. Таким чином, зловмисний DHCP сервер може навіть організувати атаку "людина посередині" (man-in-the-middle), наприклад, надавши клієнту свою IP адресу як шлюз за замовчуванням. Тоді скомпрометований хост буде пересилати свій трафік через пристрій зловмисника. Або з іншого боку, зловмисник може

просто перевантажити чи зробити локальну мережу непрацездатною, надсилаючи надмірну кількість підроблених відповідей DHCP сервера.

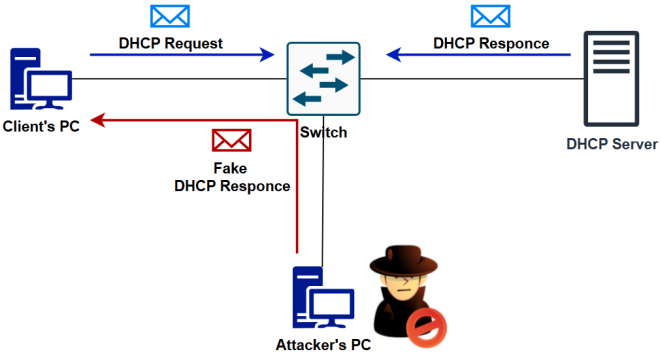

Рисунок 2 – Приклад атаки типу DHCP Spoofing

Можливий засіб боротьби з даним типом атак – це активація на комутаторах рівня доступу функції DHCP snooping. Цей функціонал дозволяє розділити всі порти комутатора на довірені та недовірені (trusted, untrusted). За замовчуванням всі порти недовірені (untrusted) – до них підключають клієнтів. З недовірених портів комутатор приймає DHCP запити, але видаляє відповіді DHCP сервера. Тільки окремі порти налаштовуються адміністратором як довірені (trusted), і тільки до таких портів підключають легітимний DHCP сервер, відповіді якого будуть передаватись комутатором на інші порти. Крім цього, комутатор з DHCP snooping аналізує інформацію в DHCP пакетах (запити від клієнтів та відповіді сервера), на основі якої будує базу прив'язки DHCP snooping binding table, яка містить по кожному клієнту: MAC адресу, порт підключення, IP адресу отриману в оренду, час оренди IP-адреси, клієнтський VLAN, тощо. Ця база прив'язки DHCP параметрів важлива і для функціонування інших функцій безпеки на комутаторах доступа, таких як Dynamic ARP Inspection, та IP Source Guard.

Треба зазначити, що таким критично важливим пристроям в локальної мережі, як сервери, маршрутизатори, як правило налаштовують статичну IP-адресу та статичні параметри підключення замість динамічного отримання параметрів IP.

ARP Spoofing атаки. Для реалізації цієї атаки зловмисник надсилає жертві підроблені ARP пакети, тим самим асоціює свою MAC-адресу з IP-адресою зовсім іншого пристрою локальної мережі. Особливістю ARP протокола є те, що зловмисник може надсилати ARP відповідь навіть якщо і не було ARP запита від клієнта, тим самим отруюючи ARP кеш жертви.

Розглянемо ситуацію на рисунку 3. Клієнт потребуючи взаємодії зі «шлюзом за замовчуванням» своєї мережі знає IP адресу шлюза (192.168.0.1), але не знає його MAC адреси. Для динамічного визначення MAC-адреси пристрою за відомою IP-адресою у локальній мережі використовується протокол ARP (Address Resolution Protocol). Також кожен пристрій підтримує свою локальну ARP-таблицю (кеш), де зберігає відповідність IP-адрес до MAC-адрес інших пристроїв мережі. Але зловмисник в цій же локальній мережі може відправляти підроблені ARP відповіді, наприклад:

- Клієнту-жертві: «IP-адреса шлюзу 192.168.0.1 має MAC-адресу С (зловмисника)»;

- Шлюзу: «IP-адреса клієнта 192.168.0.11 має MAC-адресу C (зловмисника)».

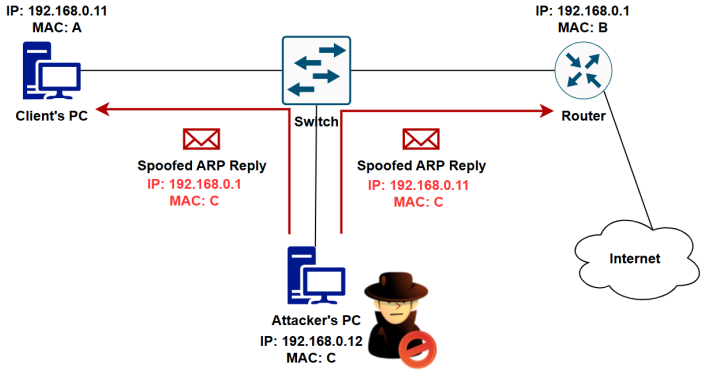

Рисунок 3 – Приклад атаки типу ARP Spoofing

Таким чином жертви ARP Spoofing атаки в локальній мережі будуть відправляти Ethernet пакети неправильному хосту (зловмиснику). Зловмисник в свою чергу, може отримувати чужий трафік з важливою інформацією, персональними даними, а також займатися підміною даних. Перенаправляючи пакети між скомпрометованими жертвами атаки, як в розглянутому випадку, зловмисник здійснює атаку "людина посередині" (man-in-the-middle).

Для боротьби з ARP Spoofing атаками можна використовувати статичні ARP записи на окремих пристроях, але це не ефективно в мережах з великою кількістю пристроїв та ускладнює адміністрування. Більш гнучкою є активація на комутаторах доступу функції Dynamic ARP Inspection (DAI), яка працює разом із функціоналом DHCP snooping. Комутатор з функцією DAI інспектує клієнтські ARP пакети та перевіряє на відповідність IP-адрес до MAC-адрес у ARP відповідях з власною базою прив'язки DHCP snooping binding table. Якщо у клієнському ARP пакеті невірна інформація – він буде відкинутий. Подібно до DHCP snooping, в конфігурації DAI також визначаються довірені та недовірені порти (trusted, untrusted). Відповідно все клієнтське обладнання підключається до недовірених портів, де DAI перевіряє ARP-пакети, а в довірені порти підключаються сервери, маршрутизатори, тощо.

IP Spoofing атаки. В цьому типу атаки зловмисник змінює свою вихідну IP-адресу в заголовку IP пакетів, щоб приховати свою особу або видати себе за інший пристрій (довірений сервер або довіреного користувача). Цей тип атаки може бути використаний як частина DoS/DDoS атаки. Наприклад, якщо зловмисник відправить велику кількість підроблених запитів на сервер від різних «відправників», а віддалений сервер буде намагатись відповідати на кожен такий запит, відкриваючи велику кількість TCP сессій і витрачаючи свої ресурси. Або з іншого боку, якщо на одну легітимну IP-адресу клієнта прийдуть відповіді від серверів, які він не замовляв – це також приклад атаки на відмову ресусів. Приклад атаки зображено на рис.4.

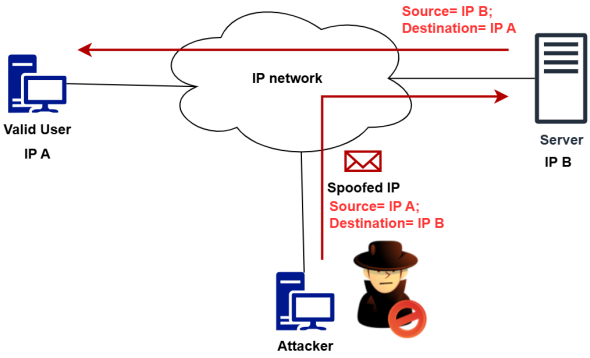

Рисунок 4 – Приклад атаки типу IP Spoofing

Для боротьби з IP Spoofing атаками можна використовувати безпосередньо на комутаторі рівня доступу функціонал IP Source Guard для перевірки дійсності вхідної IP-адреси пакета який поступає на порт комутатора. IP Source Guard може використовувати таблицю прив'язки DHCP snooping binding table (якщо такий активовано та клієнт використовує протокол DHCP для мережевого налаштування) або статичні прив'язки IP-адрес до портів підключення недовірених пристроїв. Таким чином, будь-який вхідний IP пакет з вихідною IP-адресою, відмінною від тієї, що призначена по DHCP або статичної конфігурації, буде видалено. Також на маршрутизаторах це може бути Anti-spoofing функціонал який фільтрує на основі списків контролю доступу (ACL), або перевірки в таблиці маршрутизації зворотнього маршрута до підмережі від якої прийшов вхідний IP пакет через той самий інтерфейс маршрутизатора на який був прийнятий цей пакет.

Висновок. Таким чином такі функції комутаторів рівня доступу як Port security, DHCP snooping, Dynamic ARP Inspection та IP Source Guard дають можливість заблокувати переважну більшість спуфінг атак безпосередньо в локальній мережі та якомога ближче до потенційного джерела проблеми. Перелічені функції безпеки підтримуються не у всіх моделях та виробниках комутаторів доступу, що потрібно враховувати при проектуванні надійної, відмовостійкої та безпечної мережі. Також протоколи аутентифікації та ідентифікації клієнтів мають важливе значення, так само, як професійне адміністрування, конфігурація мережі, моніторинг та вчасне виявлення підозрілих активностей. Безперечно, для зменшення потенційного впливу розглянутих атак типу "людина посередині" (man-in-the-middle) необхідне використання протоколів шифрування трафіку.

Література

1. The Cisco Learning Network. Layer 2 Security Features. URL: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKLCEA4/members-choice-layer-2-security-features.
2. Wikipedia. MAC spoofing. URL: https://en.wikipedia.org/wiki/MAC_spoofing.
3. Wikipedia. ARP spoofing. URL: https://en.wikipedia.org/wiki/ARP_spoofing.
4. Wikipedia. IP address spoofing. URL: https://en.wikipedia.org/wiki/IP_address_spoofing.