Міністерство освіти і науки України  
Національний технічний університет України

«Київський політехнічний інститут ім. І. Сікорського»

Навчально-науковий інститут атомної та теплової енергетики

Кафедра цифрових технологій в енергетиці

Лабораторна робота №3

з дисципліни «Інформаційне забезпечення безпеки комп’ютерних систем»

Тема: «Дослідження протоколу ARP на Python»

Виконав:

студент 4-го курсу, НН ІАТЕ

групи ТР-23

Ровний Г. О.

Перевірив:

Тітов В.М.

КИЇВ 2025

**Мета роботи:**

ознайомитися з принципами роботи протоколу ARP (Address Resolution Protocol) у локальних мережах, дослідити його функціонування за допомогою мови програмування Python та бібліотеки Scapy; навчитися здійснювати ARP запити, аналізувати ARP-таблиці, виявляти потенційні атаки типу ARP spoofing та реалізовувати базові інструменти для моніторингу мережевої активності.

**Поставлене завдання:**

Ознайомитися з принципами роботи протоколу ARP:

✓ вивчити структуру ARP-пакетів (opcode, hwsrc, hwdst, psrc, pdst);

✓ ознайомитися з механізмом запиту та відповіді в ARP.

Встановити та налаштувати середовище для дослідження

✓ встановити бібліотеку Scapy;

✓ створити віртуальну мережу або перевірити доступ до локальної мережі.

Реалізувати ARP-сканер на Python

✓ написати скрипт, який надсилає ARP-запити в локальну мережу;

✓ отримати список активних пристроїв з IP та MAC-адресами. Візуалізувати ARP-таблицю або мережу

✓ побудувати граф відповідностей IP ↔ MAC;

✓ використати бібліотеки NetworkX або Matplotlib

Дослідити зміну ARP-таблиці при ARP spoofing (опціонально)

✓ запустити фальшиві ARP-відповіді;

✓ виявити зміну MAC-адрес у таблиці жертви.

Зробити висновки щодо безпеки протоколу ARP

✓ проаналізувати вразливості;

✓ запропонувати методи захисту (статичні ARP, IDS, VPN).

**Результат виконання роботи**

**Відповіді на запитання**

1. Що таке ARP і яку роль він виконує у стеку TCP/IP?

ARP (Address Resolution Protocol) — це протокол, який використовується для зв'язування адреси мережевого рівня (Рівень 3) з адресою канального рівня (Рівень 2). У контексті стеку TCP/IP, ARP виконує критично важливу роль: він перетворює IP-адресу (Рівень 3) на MAC-адресу (Рівень 2) в межах однієї локальної мережі (LAN).

1. Який формат ARP-пакета і які його ключові поля (hwtype, ptype, hlen, plen, opcode, hwsrc, hwdst, psrc, pdst)?

Ось детальна відповідь на ваші запитання про протокол ARP. 🌐

**1. Що таке ARP і яку роль він виконує у стеку TCP/IP?**

ARP (Address Resolution Protocol) — це протокол, який використовується для зв'язування адреси мережевого рівня (Рівень 3) з адресою канального рівня (Рівень 2).

У контексті стеку TCP/IP, ARP виконує критично важливу роль: він перетворює IP-адресу (Рівень 3) на MAC-адресу (Рівень 2) в межах однієї локальної мережі (LAN).

Чому це необхідно?

1. Коли ваш комп'ютер (наприклад, з IP 192.168.1.10) хоче надіслати дані роутеру (з IP 192.168.1.1) в тій самій мережі, він знає IP-адресу призначення.
2. Однак на канальному рівні (наприклад, Ethernet або Wi-Fi), пристрої спілкуються не за IP-адресами, а за фізичними MAC-адресами (вшитими в мережеву карту).
3. Щоб надіслати кадр (frame) на роутер, ваш комп'ютер мусить знати MAC-адресу роутера.
4. ARP надсилає широкомовне повідомлення (broadcast) у локальну мережу з питанням: "Хто має IP 192.168.1.1? Повідомте свою MAC-адресу".
5. Роутер (або пристрій з IP 192.168.1.1) відповідає: "Я маю IP 192.168.1.1, і моя MAC-адреса — 00:1A:2B:3C:4D:5E".

Таким чином, ARP є "перекладачем" або "довідником", який дозволяє пристроям у локальній мережі знаходити фізичні адреси один одного, знаючи лише їхні логічні (IP) адреси.

**2. Який формат ARP-пакета і які його ключові поля?**

ARP-пакет інкапсулюється безпосередньо в кадр канального рівня (наприклад, Ethernet). Він має простий формат:

hwtype (Hardware Type) (2 байти): Тип обладнання. Для Ethernet це значення 1.

ptype (Protocol Type) (2 байти): Тип протоколу мережевого рівня. Для IPv4 це 0x0800.

hlen (Hardware Address Length) (1 байт): Довжина апаратної адреси в байтах. Для Ethernet (MAC-адреса) це 6 (48 біт).

plen (Protocol Address Length) (1 байт): Довжина протокольної адреси в байтах. Для IPv4 (IP-адреса) це 4 (32 біти).

opcode (Operation Code) (2 байти): Вказує на тип операції:

1 = ARP Request (Запит)

2 = ARP Reply (Відповідь)

hwsrc (Source Hardware Address) (6 байт): MAC-адреса відправника.

psrc (Source Protocol Address) (4 байти): IP-адреса відправника.

hwdst (Destination Hardware Address) (6 байт): MAC-адреса одержувача.

pdst (Destination Protocol Address) (4 байти): IP-адреса одержувача.

**3. Чим відрізняється ARP Request від ARP Reply на рівні полів (особливо opcode, hwsrc/hwdst, psrc/pdst)?**

ARP Request (Запит), і ARP Reply (Відповідь) використовують однаковий формат пакета, вони заповнюють поля зовсім по-різному, що відображає їхню мету.

ARP Request — це, по суті, широкомовне "питання" до всієї мережі. А ARP Reply — це "відповідь" на запит, адресована конкретному пристрою.

1. **Як працює ARP-кеш і які наслідки має час життя записів (timeout)?**

ARP-кеш — це тимчасова пам'ять в ОС, де зберігаються нещодавно отримані відповідності "IP-адреса -> MAC-адреса". Коли комп'ютер хоче надіслати дані, він спочатку перевіряє свій ARP-кеш. Якщо він знаходить там потрібну IP-адресу, він одразу бере відповідну MAC-адресу і надсилає дані. Це набагато швидше. Лише якщо запису в кеші немає, пристрій ініціює ARP-запит, а отримавши відповідь, додає нову пару "IP-MAC" до свого кешу.

Однак ці записи не вічні. Вони мають час життя (timeout), який зазвичай становить від кількох до кількадесяти хвилин. Коли цей час спливає, запис видаляється. Це має важливий наслідок: це дозволяє мережі бути гнучкою. Якби пристрій змінив свою IP-адресу (наприклад, отримавши нову від DHCP-сервера) або йому замінили мережеву карту (змінивши його MAC-адресу), старі записи в кешах інших комп'ютерів стали б недійсними. Завдяки тайм-ауту, система змушена через деякий час "забути" старий запис і зробити новий ARP-запит, щоб отримати актуальну MAC-адресу, підтримуючи таким чином коректну роботу мережі.

**5. Як переглянути ARP-таблицю в Windows і в Linux (команди й приклад виводу)?**

У Windows треба відкрити cmd або PowerShell і ввести команду arp -a. У відповідь отримаємо список IP-адрес у вашій локальній мережі, їхні відповідні фізичні (MAC) адреси та тип запису (зазвичай "динамічний", що означає, що він був отриманий автоматично через ARP, або "статичний", якщо його додати вручну).

**6. Що таке ARP-spoofing / cache poisoning і які ризики воно створює (MITM, перехоплення, DoS)?**

ARP-spoofing — небезпечний тип кібератаки, який використовує фундаментальну довірливість протоколу ARP. Протокол був розроблений без вбудованих механізмів перевірки автентичності, тому він вірить будь-якій отриманій ARP-відповіді.

**7. Які ще атаки, пов’язані з ARP, існують окрім класичного spoofing (наприклад gratuitous ARP misuse, ARP flooding)?**

Однією з них є ARP (Gratuitous ARP misuse). Зазвичай безкоштовний ARP (GARP) — це легітимний пакет, який пристрій надсилає, щоб оголосити про свою присутність або зміну IP/MAC-адреси (наприклад, коли сервер перезавантажується). Атакуючий може зловживати цим механізмом, безперервно розсилаючи такі GARP-пакети з підробленими даними (наприклад, стверджуючи, що IP-адреса шлюзу належить йому). На відміну від класичного спуфінгу, де атакуючий часто відповідає на конкретні запити, тут він проактивно проходить по ARP-кеші всіх пристроїв у мережі одночасно, що є значно агресивнішим.

Або ARP-флуд (ARP flooding) — спрямована не на користувачів, а на мережеві комутатори (світчі). Комутатори зберігають таблицю (CAM-таблицю), яка пов’язує MAC-адреси з фізичними портами. Атакуючий генерує тисячі ARP-пакетів з *різними вигаданими* MAC-адресами відправника і "затоплює" ними комутатор. Це призводить до переповнення пам'яті (CAM-таблиці) комутатора. Коли це стається, комутатор переходить у "аварійний режим" (fail-open mode) і починає поводитися як старий хаб: він надсилає всі мережеві пакети на всі порти. Це дозволяє зловмиснику "прослуховувати" весь трафік у мережі.

**8. Як алгоритмічно виявити ARP-спуфінг? Назвіть принаймні два різні методи.**

Пасивний метод ґрунтується на виявленні конфліктів. Спеціалізоване ПЗ або система виявлення вторгнень (IDS) прослуховує весь ARP-трафік у мережі. Вона веде власну базу даних IP-MAC пар. Алгоритм спрацьовує, коли система бачить пакет, що суперечить наявним даним. Наприклад, якщо система знає, що IP-адреса 192.168.1.1 (шлюз) пов'язана з MAC-адресою AA:BB:CC:00:11:22, і раптом бачить ARP-відповідь, яка стверджує, що той самий IP 192.168.1.1 тепер належить DD:EE:FF:33:44:55 (MAC-адресі атакуючого), вона негайно фіксує це як аномалію і піднімає тривогу.

Активний метод полягає в перехресній перевірці. Замість того, щоб просто довіряти ARP, система може використовувати інший, більш надійний протокол для перевірки. Наприклад, коли система отримує підозрілий ARP-пакет, вона може надіслати ping (ICMP-запит) на IP-адресу, про яку йдеться. Коли справжній пристрій відповість на цей ping, система-детектор подивиться на джерело MAC-адреси у кадрі Ethernet, що містить ICMP-відповідь. Якщо ця MAC-адреса (справжнього пристрою) не збігається з тією, що була вказана у підозрілій ARP-відповіді, це є беззаперечним доказом атаки.

**9. Опишіть простий план дій при виявленні ARP-спуфінгу у мережі (які кроки слід виконати).**

Перший крок — точно визначити, хто є джерелом атаки. За допомогою інструментів моніторингу потрібно зафіксувати MAC-адресу та IP-адресу зловмисника, які він використовує у підроблених ARP-пакетах.

Маючи MAC-адресу атакуючого, адміністратор повинен зайти в інтерфейс управління мережевим комутатором. Там він переглядає MAC-таблицю комутатора, щоб побачити, на якому фізичному порту світиться ця MAC-адреса. Це вкаже на кабель, до якого підключений зловмисник. Найшвидший спосіб зупинити атаку — адміністративно вимкнути (shut down) цей порт на комутаторі, фізично відрізавши зловмисника від мережі.

Після ізоляції атакуючого мережа все ще заражена. Потрібно примусово очистити ARP-кеші на всіх постраждалих пристроях. Найефективніший спосіб — змусити легітимний пристрій (наприклад, роутер, чию адресу підробляли) надіслати ARP (Gratuitous ARP) пакет. Цей широкомовний пакет оголосить усій мережі правильну "IP-MAC" пару, змушуючи всі пристрої оновити свої кеші правильними даними.).

**10. Як статичні ARP-записи допомагають і які у них обмеження? Наведіть приклад ситуації, статичний ARP не допоможе.**

Статичні ARP-записи — це один з найпростіших методів захисту. Це правило, яке адміністратор вручну прописує на комп'ютері або сервері, що каже: "IP-адреса X завжди дорівнює MAC-адресі Y". Наприклад, на своєму ноутбуці ви можете створити статичний запис, що IP-адреса шлюзу 192.168.1.1 завжди належить MAC.

**11. Що таке DHCP snooping і як він у зв’язці з Dynamic ARP Inspection (DAI) захищає мережу?**

DHCP Snooping — Спочатку вмикається ця функція. Комутатор починає слузати весь DHCP-трафік. Він будує довірену базу даних (DHCP binding table), яка точно знає: який IP-адресу отримала яка MAC-адреса і на якому фізичному порту комутатора цей пристрій знаходиться. Комутатор також блокує фальшиві DHCP-сервери в мережі.

Dynamic ARP Inspection — після того, як DHCP Snooping створив цю довірену базу даних, вмикається DAI. Тепер комутатор перехоплює кожен ARP-пакет у мережі. Для кожного пакета він проводить перевірку: він заглядає у базу даних, створену DHCP Snooping, і перевіряє чи дійсно IP-адреса та MAC-адреса з цього ARP-пакета відповідають тому, що записано в базі.

**12. Які мережеві пристрої та їхні функції (наприклад port security, 802.1X) допомагають запобігти ARP-атакам?**

Port Security — як базова ф-ція дозволяє обмежити кількість MAC-адрес, які можуть працювати на одному фізичному порту комутатора. Ця функція не зупинить класичний ARP-спуфінг (оскільки атакуючий використовує свою одну MAC-адресу), але вона ефективно блокує атаки типу ARP-флуд.

802.1X (Port-Based Network Access Control) — це набагато суворіший механізм. Коли пристрій підключається до порту комутатора, цей порт залишається неактивним. Пристрій спочатку повинен пройти автентифікацію яку перевіряє центральний сервер (RADIUS). Лише після успішної перевірки особи порт активується.

**Висновок:**

У результаті виконання лабораторної роботи було