МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних наук____

Кафедра інформаційних технологій

ДИПЛОМНА РОБОТА

Рівень вищої освіти бакалавр

на тему: Дослідження засобів захисту інформації на канальному рівні

Виконав студент 4 курсу групи К-41
Напрям підготовки 6.050101
комп'ютерні науки
Тулінов В..... І.....

Керівник к.геогр.н., доцент_____
Коваленко Людмила Борисівна_____

Консультант _____
_____

Рецензент к.т.н., доцент_____
Гнатовська Ганна Арнольдівна_____

Одеса 2018

ЗМІСТ

СПИСОК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ

Скорочення

ІС – інформаційна система
КЗЗ – комплекс засобів захисту
ACL – Access Control List (Список контролю доступу)
ARP – Address Resolution Protocol (Протокол перетворення адрес)
BPDU – Bridge Protocol Data Units (Протокол керування мережевими мостами)
CERT – Computer Emergency Response Team (Група комп'ютерної «швидкої допомоги»)
DoS – Denial of Service (Відмова в обслуговуванні)
DNS – Domain Name Service (Служба домених імен)
DHCP – Dynamic Host Configuration Protocol (Протокол динамічного конфігурування хостів)
FTP – File Transfer Protocol (Протокол передачі файлів)
HTTP – HyperText Transfer Protocol (Протокол передачі гипертексту)
IDS – Intrusion Detection System (Система розпізнавання атак)
ICMP – Internet Control Message Protocol (Протокол керуючих повідомлень в мережі Інтернет)
IP – Internet Protocol (Інтернет-протокол міжмережевого обміну даними)
ISP – Internet service provider (Постачальник інтернет-послуг)
MAC – Media Access Control (Рівень управління доступом до середовища передачі)
MITM – Man In The Middle (Мережева атака «людина в середині»
NFS – Network File System (Мережева файлова система)
OSI – Open System Interconnection (Взаємодія відкритих систем)
PKI – Public Key Infrastructure (Інфраструктура управління відкритими ключами)
POP3 – Post Office Protocol Version 3 (Протокол поштового відділу, версія 3)
RADIUS – Remote Authentication in Dial-In User Service (Служба

віддаленої аутентифікації користувача за комутованими лініями)

SNMP – Simple Network Management Protocol (Простий протокол мережевого керування)

SMTP – Simple Mail Transfer Protocol (Простий протокол Електронної пошти)

STA – Spanning Tree Algorithm (Алгоритм сполучного дерева)

STP – Spanning Tree Protocol (Протокол сполучного дерева)

TCP – Transmission Control Protocol (Протокол управління передачею)

TELNET – Terminal Network (Мережевий термінал)

UDP – User Datagram Protocol (Протокол передачі даних користувача)

VLAN – Virtual Local Area Network (Віртуальна локальна мережа)

Wi-Fi – Wireless Fidelity (Стандарт бездротової передачі даних)

Умовні позначення

Mbps – мегабіт в секунду

Gbps – гігабіт в секунду

Терміни

Аккаунт – обліковий запис, що містить відомості, які користувач повідомляє про себе деякій комп'ютерній системі.

Сніффер – мережевий аналізатор трафіку, програма або програмно-апаратний пристрій, призначене для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку.

Sniffing – вид мережевої атаки, також називається «пасивне прослуховування мережі».

Spoofing – загальна назва для мережевих атак, коли один учасник маскується під іншого.

VLAN hopping – несанкціоноване отримання доступу до VLAN.

ВСТУП

Незважаючи на активний розвиток бездротових технологій і засобів зв'язку, найчастіше базою для побудови різних сервісів є технологія Ethernet. Вона поєднує в собі перевірені і відпрацьовані роками алгоритми, величезний вибір всілякого обладнання, дешевизну і простоту настройки, а також високі швидкості передачі інформації. Саме останній фактор не дає провідним локальним обчислювальним мережам піти в історію.

Однак, незважаючи на популярність, технологія Ethernet продовжує залишатися досить вразливою для різного роду атак, спрямованих на «відмова в обслуговуванні», перехоплення трафіку, шахрайство та інше. Міркування безпеки завжди враховуються при розробці нових стандартів і специфікацій в області локальних обчислювальних мереж. Але з новими методами захисту приходять і нові варіанти злому. В даний час, атаки на Ethernet-сегмент можна розділити на наступні великі групи:

1) зміна адресної інформації кінцевих вузлів;

2) зміною адресної інформації проміжних мережевих вузлів;

3) підробка даних легітимного користувача (фальсифікація).

Кожна група атак може бути спрямована як на «відмову в обслуговуванні» так і на перехоплення інформації.

Сучасні корпоративні IP-мережі будуються на базі комутаторів. Це означає, що для забезпечення безпеки передачі інформації можливо два підходи:

1) посилення захисних функцій кінцевих мережевих вузлів;

2) застосування вбудованих функцій безпеки комутаторів.

Перший варіант в більшості випадків важко здійснити через велику кількість користувачів у великих мережах. Набагато простіше в реалізації правильна настройка проміжних мережевих вузлів, які здійснюють фільтрацію трафіку, детектування небезпечної мережевої активності та інші дії, спрямовані на запобігання і блокування дій зловмисника.

В даний момент на кафедрі Інформаційних технологій є навчальна локальна обчислювальна мережа, побудована на базі сучасного обладнання фірми Cisco Systems, яка надає широкі можливості для дослідження різних типів мережевих атак, спрямованих на перехоплення трафіку і вбудованих засобів захисту комутаторів Cisco, за допомогою яких дані атаки можна ефективно запобігти.

Метою даної дипломної роботи є, практична реалізація сценаріїв різних мережевих атак канального рівня і дослідження функцій безпеки комутаторів Cisco Catalyst для їх запобігання.

Для досягнення поставленої мети в роботі необхідно вирішити наступні завдання:

- провести аналіз загроз корпоративних мереж і причин виникнення проблем захисту;
- класифікувати мережеві атаки за способом впливу;
- розробити сценарії мережевих атак на канальному рівні;
- провести моделювання мережевих атак на канальному рівні з використанням обладнання компанії Cisco System;
- дослідити вбудовані функції безпеки на комутаторах Cisco Catalyst 2960;
- реалізувати механізми захисту в розроблених сценаріях мережевих атак;
- здійснити настройку комутаторів в емуляторі Cisco Packet Tracer.

Структура дипломної роботи складається з вступу, чотирьох розділів, висновків, переліку посилань на 11 найменувань, додатків. Повний обсяг проекту становить 51 сторінку, містить 18 рисунків і 2 таблиці.

1 КЛАССИФІКАЦІЯ МЕРЕЖЕВИХ АТАК

Мережеві атаки настільки ж різноманітні, як і системи, проти яких вони спрямовані. Деякі атаки відрізняються великою складністю. Інші може здійснити звичайний оператор, навіть не припускає, які наслідки може мати його діяльність.

Розглянемо основні типи мережевих атак. Діаграма класифікації мережевих атак приведена у додатку А.

Класифікація мережевих атак за характером впливу. За характером впливу мережеві атаки можна класифікувати на пасивні і активні.

Пасивним впливом на розподілену обчислювальну систему називається вплив, який не має безпосереднього впливу на роботу системи, але може порушувати її політику безпеки. Саме відсутність безпосереднього впливу на роботу розподіленої мережі призводить до того, що пасивний віддалений вплив практично неможливо виявити. Прикладом пасивного типового віддаленого впливу служить прослуховування каналу зв'язку в мережі.

Під активним впливом на розподілену мережу розуміють вплив, що надає безпосередній вплив на роботу системи (зміна конфігурації, порушення працездатності і т.п.) і порушує прийняту в ній політику безпеки. Практично всі типи віддалених мережевих атак є активними впливами. Це пов'язано з тим, що в самій природі руйнуючої дії міститься активний початок. Очевидною особливістю активного впливу в порівнянні з пасивним є принципова можливість його виявлення.

Класифікація мережевих атак по цілі впливу. Порушник, здійснюючи атаку, зазвичай ставить перед собою наступні цілі [1]:

- порушення конфіденційності інформації, що передається;
- порушення цілісності та достовірності інформації, що передається;
- порушення працездатності системи в цілому або окремих її частин.

Класифікація мережевих атак за умовою початку здійснення впливу. Віддалений вплив, також як і будь-який інший, може почати здійснюватися тільки за певних умов. У розподілених мережах існують три види умов початку здійснення віддаленої атаки [1]:

1) Атака на запит від об'єкта, що атакується. У цьому випадку атакуючий чекає передачі від потенційної мети атаки запиту певного типу, який і буде умовою початку здійснення впливу.

2) Атака по настанню очікуваної події на об'єкті, що атакується. У цьому випадку атакуючий здійснює постійне спостереження за станом операційної системи віддаленої цілі атаки і при виникненні певної події в цій системі починає вплив. Як і в попередньому випадку, ініціатором здійснення початку атаки виступає сам об'єкт, що атакується.

3) Безумовна атака. У цьому випадку початок здійснення атаки безумовно по відношенню до мети атаки, тобто атака здійснюється негайно і безвідносно до стану системи і об'єкта, що атакується. Отже, в цьому випадку атакуючий є ініціатором початку здійснення атаки.

Класифікація мережевих атак за наявністю зворотного зв'язку з об'єктом, що атакується. Атаки бувають зі зворотним зв'язком і без зворотного зв'язку (односпрямована атака). Віддалена атака, здійснювана при наявності зворотного зв'язку з об'єктом, що атакується, характеризується тим, що на деякі запити, передані на об'єкт, що атакується, атакуючому потрібно отримати відповідь, а, отже, між атакуючим і метою атаки існує зворотний зв'язок, яка дозволяє атакуючому адекватно реагувати на всі зміни, що відбуваються на об'єкті, що атакується. Подібні віддалені атаки найбільш характерні для розподілених мереж.

На відміну від атак зі зворотним зв'язком віддаленим атакам без зворотного зв'язку не потрібно реагувати на будь-які зміни, що відбуваються на об'єкті, що атакується. Атаки даного виду зазвичай здійснюються передачею на об'єкт, що атакується одиночних запитів, відповіді на які атакуючому не потрібні.

Класифікація мережевих атак за розташуванням суб'єкта атаки щодо об'єкта, що атакується. Мережеві атаки можна класифікувати на внутрішньо сегментні і міжсегментні. З точки зору віддаленої атаки надзвичайно важливо, як по відношенню один до одного розташовуються суб'єкт і об'єкт атаки, тобто в одному або в різних сегментах вони знаходяться. У разі внутрішньо сегментної атаки, як випливає з назви, суб'єкт і об'єкт атаки знаходяться в одному сегменті.

Дана класифікаційна ознака дозволяє судити про «ступень віддаленості» атаки.

На практиці міжсегментноу атаку здійснити значно важче, ніж внутрішньо сегментну. Важливо відзначити, що міжсегментна віддалена атака представляє набагато більшу небезпеку, ніж внутрішньо сегментна. Це пов'язано з тим, що в разі міжсегментної атаки об'єкт її і безпосередньо

атакуючий можуть перебувати на відстані багатьох тисяч кілометрів один від одного, що може істотно перешкодити заходам по відображенню атаки.

Класифікація мережевих атак по рівню еталонної моделі ISO / OSI, на якому здійснюється вплив. Міжнародна Організація по Стандартизації (ISO) прийняла стандарт ISO 7498, що описує взаємодію відкритих систем (OSI). Розподілені мережі також є відкритими системами. Будь-який мережевий протокол обміну, як і будь-яку мережеву програму, можна з тим або іншим ступенем точності спроектувати на еталонну модель OSI, що містить сім рівнів: фізичний, канальний, мережевий, транспортний, сеансовий, представницький, прикладний. Така багаторівнева проекція дозволить описати в термінах моделі OSI функції, закладені в мережевий протокол або програму. Віддалена атака також є мережевою програмою. У зв'язку з цим представляється логічним розглядати віддалені атаки на корпоративні мережі, проектуючи їх на еталонну модель ISO / OSI.

2 МОДЕЛЮВАННЯ МЕРЕЖЕВИХ АТАК НА КАНАЛЬНОМУ РІВНІ

Поширені атаки канального рівня [2, 3]:

- ARP-spoofing (ARP-poisoning) – техніка мережевої атаки, що застосовується переважно в Ethernet, але можлива і в інших мережах, що використовують протокол ARP, заснована на використанні недоліків протоколу ARP і дозволяє перехоплювати трафік між вузлами, які розташовані в межах одного широкомовного домену;
- MAC-spoofing – атака канального рівня, яка полягає в тому, що на мережевій карті змінюється MAC-адреса, що змушує комутатор відправляти на порт, до якого підключений зловмисник, пакети, які до цього він бачити не міг;
- переповнення таблиці комутації – атака заснована на тому, що таблиця комутації в комутаторах має обмежений розмір. Після заповнення таблиці, комутатор не може більше вивчати нові MAC-адреси і починає працювати як хаб, відправляючи трафік на всі порти;
- атаки на DHCP – це може бути підміна DHCP-сервера в мережі (тоді атакуючий може призначати додаткові параметри DHCP, такі як шлюз за замовчуванням) або атака DHCP starvation, яка змушує DHCP-сервер видати всі існуючі на сервері адреси зловмисникові;
- VLAN hopping – несанкціоноване отримання доступу до VLAN;
- Атаки на STP – відправлення повідомлень BPDU для зміни поточної топології STP.

2.1 Протокол ARP та атаки з його використанням

2.1.1 Алгоритм работи ARP

Протокол ARP призначений для визначення адрес канального рівня (MAC-адрес) за відомими IP-адресами. Це дуже важливий протокол, його робота безпосередньо впливає на працездатність мережі в цілому.

Для взаємодії пристроїв один з одним необхідно, щоб у передавального пристрою були IP- і MAC-адреси одержувача. Коли один з пристроїв намагається встановити зв'язок з іншим, з відомою IP-адресою, йому необхідно визначити MAC-адресу одержувача. Набір протоколів TCP / IP має в своєму складі спеціальний протокол ARP (Address Resolution Protocol –

протокол перетворення адрес), який дозволяє автоматично отримати MAC-адресу.

Протокол може використовуватися у наступних випадках [4]:

1) Хост А хоче передати IP-пакет вузлу В, що знаходиться з ним в одній мережі (рис.2.1);

2) Хост А хоче передати IP-пакет вузлу В, що знаходиться з ним в різних мережах, і користується для цього послугами маршрутизатора R (рис.2.2).

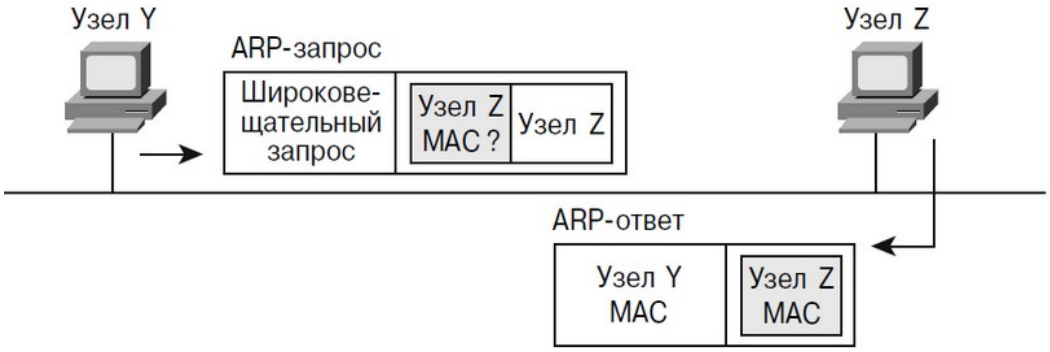


Рисунок 2.1 – Ілюстрація роботи протоколу ARP за умови, що IP-адресат знаходиться в локальній мережі

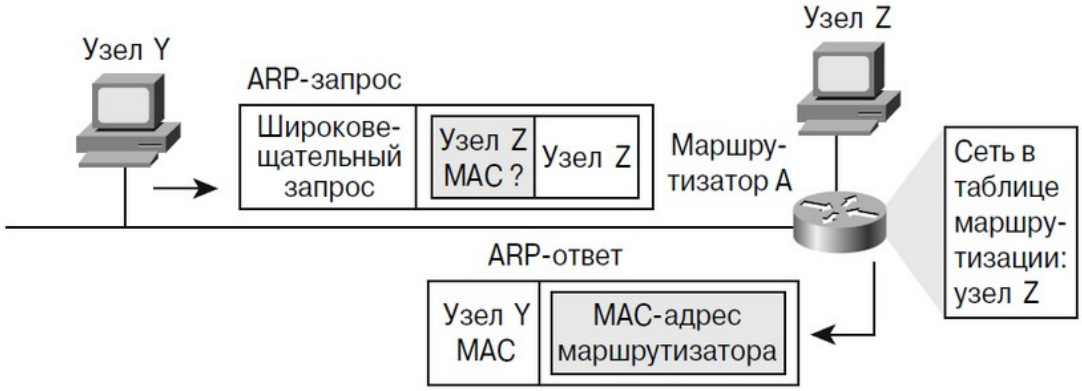


Рисунок 2.2 – Ілюстрація роботи протоколу ARP за умови, що IP-адресат знаходиться у віддаленій мережі

У будь-якому з цих випадків вузлом А буде використовуватися протокол ARP, тільки в першому випадку для визначення MAC-адреси вузла В, а в другому – для визначення MAC-адреси маршрутизатора R. У

останньому випадку пакет буде переданий маршрутизатору для подальшої ретрансляції.

Далі для простоти розглядається перший випадок, коли інформацією обмінюються вузли, що знаходяться безпосередньому в одній мережі. Випадок коли пакет адресований вузлу, що знаходиться за маршрутизатором відрізняється тільки тим, що в пакетах, що передаються після того як ARP-перетворення завершено, використовується IP-адреса одержувача, але MAC-адресу маршрутизатора, а не одержувача.

Деякі пристрої зберігають спеціальні ARP-таблиці, в яких міститься інформація про MAC- і IP-адреси інших пристроїв, підключених до тієї ж локальної мережі. ARP-таблиці дозволяють встановити однозначну відповідність між IP- і MAC-адресами. Такі таблиці зберігаються в певних областях оперативної пам'яті і обслуговуються автоматично на кожному з мережевих пристроїв (рис.2.3 і 2.4). У рідкісних випадках доводиться створювати ARP-таблиці вручну. Кожен комп'ютер в мережі підтримує свою власну ARP-таблицю [4].

Запись в ARP-таблице

Internet-адрес	Физический адрес	Тип
68.2.168.1	00-50-57-00-76-84	Динамический

Рисунок 2.3 – Приклад запису в ARP таблиці

ARP-таблица для адреса 198.150.11.36

MAC-адрес	IP-адрес
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:AB:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

Рисунок 2.4 – Приклад ARP-таблиці для адреси 198.150.11.36

Для передачі даних від одного вузла іншому відправник повинен знати IP- і MAC-адресу одержувача. Якщо він не може отримати шукану фізичну адресу з власної ARP-таблиці, ініціюється процес, що зветься ARP-запитом, який проілюстрований на рис. 2.5.

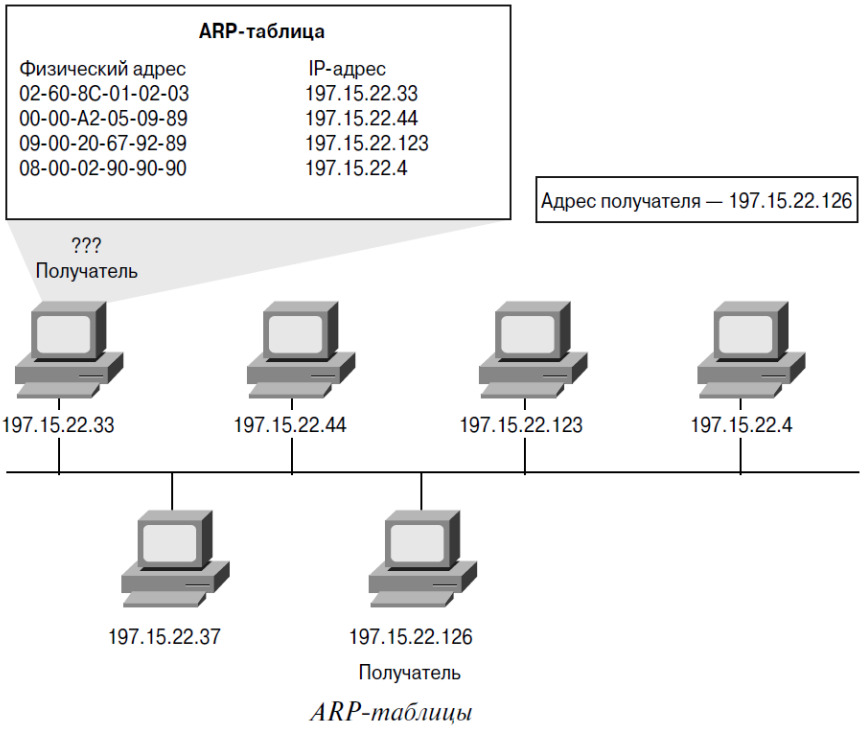


Рисунок 2.5 – Приклад ініціювання ARP-запиту

ARP-запит дозволяє вузлу визначити MAC-адресу одержувача. Вузол створює фрейм ARP-запиту і розсилає його всім мережевим пристроям. Фрейм ARP-запиту складається з двох частин: заголовка фрейму і повідомлення ARP-запиту.

Для того щоб всі пристрої могли отримати ARP-запит, використовується широкомовна MAC-адреса. Якщо IP-адреса пристрою збігається з IP-адресою одержувача в широкомовному ARP-запиті, цей пристрій відповідає відправнику, повідомляючи свою MAC-адресу. Таке повідомлення називається ARP-відповіддю.

Після отримання ARP-відповіді відправник широковещательного ARP-запиту витягує MAC-адресу з поля апаратного адреси відправника і оновлює свою ARP-таблицю. Тепер цей пристрій може належним чином адресувати пакети, використовуючи як MAC-, так і IP-адресу.

Протокол ARP є абсолютно незахищеним. Він не володіє ніякими способами перевірки автентичності пакетів: як запитів, так і відповідей. Ситуація стає ще більш складною, коли може використовуватися самовільний ARP (gratuitous ARP).

Самовільний ARP – така поведінка ARP, коли ARP-відповідь надсилається, коли в цьому (з точки зору одержувача) немає особливої необхідності. Самовільний ARP-відповідь це пакет-відповідь ARP, присланий без запиту. Він застосовується для визначення конфліктів IP-адрес в мережі: як тільки станція отримує адресу по DHCP або адреса присвоюється вручну, розсилається ARP-відповідь gratuitous ARP [4].

Самовільний ARP може бути корисний в наступних випадках:

- оновлення ARP-таблиць, зокрема, в кластерних системах;
- інформування комутаторів;
- повідомлення про включення мережевого інтерфейсу.

Незважаючи на ефективність самовільного ARP, він є особливо небезпечним, оскільки за його допомогою можна запевнити віддалений вузол в тому, що MAC-адреса будь-якої системи, що знаходиться з нею в одній мережі, змінилася і вказати, яку адресу використовувати тепер.

2.1.2 Сценарій проведення атаки ARP-spoofing

Розглянемо схему проведення атаки ARP-spoofing, представлену на рис.2.6. До виконання ARP-спуфинга в ARP-таблиці вузлів A і B існують записи з IP- і MAC-адресами один одного. Обмін інформацією здійснюється безпосередньо між вузлами A і B (сіра стрілка).

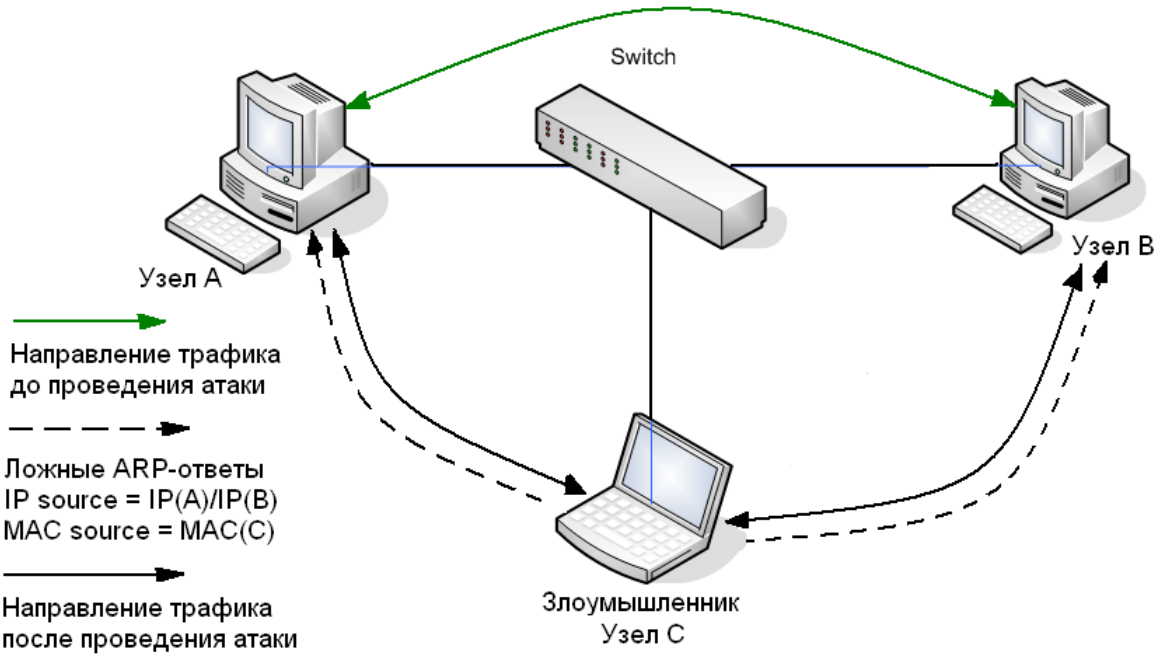


Рисунок 2.6 – Схема проведення атаки ARP-spoofing

В ході виконання ARP-спуфинга комп'ютер С виконує атаку, відправляє ARP-відповіді (без отримання запитів):

- вузлу А: з IP-адресою вузла В і MAC-адресою вузла С;
- вузлу В: з IP-адресою вузла А і MAC-адресою вузла С.

В силу того що комп'ютери підтримують самовільний ARP (gratuitous ARP), вони модифікують власні ARP-таблиці і поміщають туди записи, де замість справжніх MAC-адрес комп'ютерів А і В стоїть MAC-адреса комп'ютера С (пунктирні стрілки).

Після того як атака виконана, коли комп'ютер А хоче передати пакет комп'ютеру В, він знаходить в ARP-таблиці запис (він відповідає комп'ютеру С) і визначає з нього MAC-адресу одержувача. Відправлений за цією MAC-адресою пакет приходить комп'ютеру С замість одержувача. Комп'ютер С потім ретранслює пакет тому, кому він дійсно адресовано – тобто комп'ютеру В (чорні суцільні стрілки).

Для початку в якості вихідних даних приймемо, що:

- локальна мережа типу Ethernet, побудована на некерованих комутаторах;
- відсутність статичних arp-таблиць у жертви;
- наявність персонального брендмауера у жертви;
- атакуючий повинен створити фіктивну запис в arp-таблиці жертви в обхід персонального брендмауера.

Впровадження захисту від ARP-спуфинга популярна ідея серед розробників персональних міжмережевих екранів. Одним з перших продуктів, що реалізував подібну функцію був Agnitum Outpost Firewall. Потім компанія Агава оголосила про вихід свого Agava Firewall з підтримкою аналогічної захисту. У лабораторії Касперського в Kaspersky Internet Security 2011 теж є реалізація захисту від мережевих атак [5].

Насправді, не дивлячись на те, що продукти різні, захист у них побудований за схожим принципом: якщо приходить ARP-відповідь, а система не посилала ARP-запит – робиться висновок, що була спроба фіктивної записи в ARP-таблицю. Це логічно, адже ймовірність того, що прийде достовірна ARP-відповідь притому, що запит не надсилався, дорівнює нулю.

Деякі персональні брендмауери (наприклад Outpost) приймають тільки найперший відповідь на arp-запит, вважаючи інші запити фіктивними. Виходить, якщо атакуючому вдасться відповісти на запит раніше, ніж прийде легітимна відповідь – брендмауер прийме його відповідь, а легітимна відповідь буде відкинута. Тобто відбудеться підміна записи в arp-таблиці жертви. Але цей шлях дуже тернистий: послати свою відповідь раніше, ніж прийде легітимний відповідь не так-то просто. Є більш легкий спосіб провести атаку. Дійсно, існує також можливість модифікування ARP-таблиці шляхом посилки фіктивних ARP-запитів. Такі відповіді брендмауери з легкістю пропускають [5].

Крім того, внесення комп'ютера в список атакуючих в тому випадку, якщо від нього прийшов ARP-відповідь, коли система не посилала запиту не завжди є правильним рішенням.

Розглянемо приклад атаки, представленої на рис.2.7, вузол С посилає ARP-запит вузлу В від імені вузла А. В результаті комп'ютер В пошле ARP-відповідь вузлу А. Але вузол А запиту не посилав. Відповідно брендмауер, що знаходиться на вузлі А, вважатиме вузол В атакуючої системою. Який практичний толк від такої атаки? Якщо брендмауер налаштований на внесення в «чорний список» системи, яка, на його думку, виробляла спробу атаки отримаємо DoS-атаку. Адже в результаті зв'язок легітимного комп'ютера з жертвою порушиться.

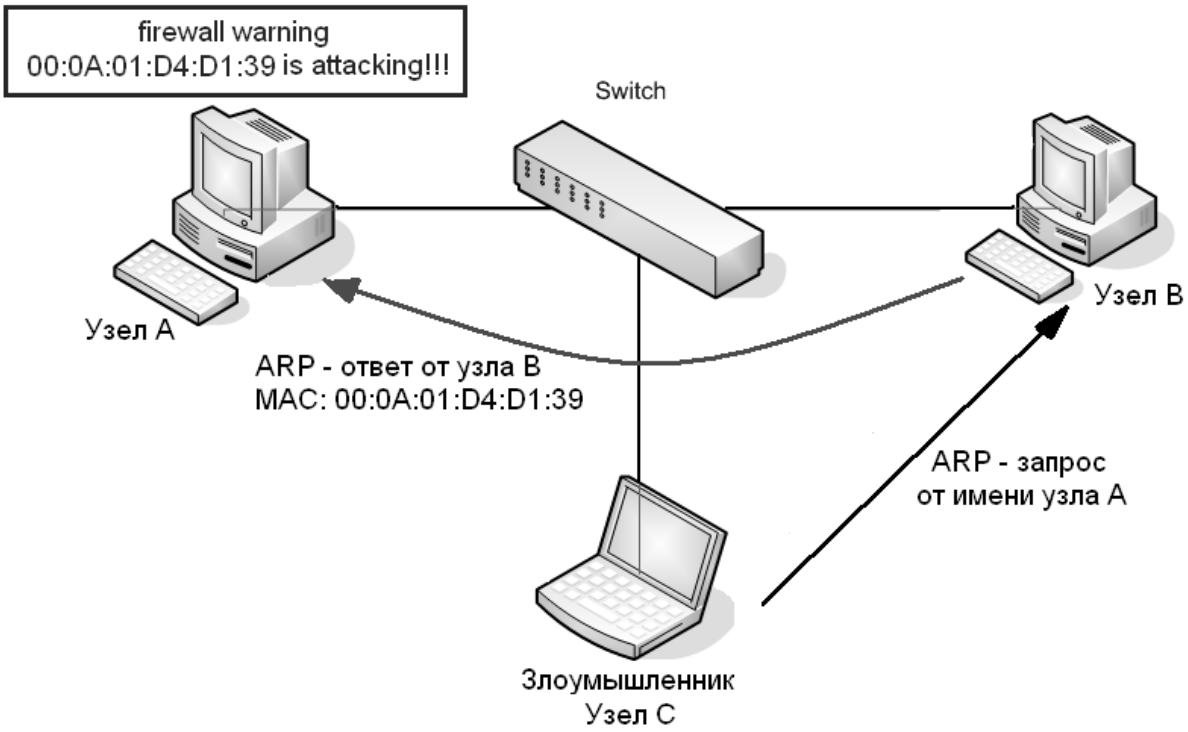


Рисунок 2.7 – Схема організації несправжньої тривоги Фаєрвол

Звідси можна зробити висновок, що сучасні персональні міжмережеві екрани не можуть ефективно запобігати атакам, спрямованим на зміну записів ARP-таблиці.

2.1.3 Інструменти для проведення атаки ARP-spoofing

В даний час існує декілька інструментів для виконання ARP-spoofing'a, що працюють як в ОС Linux, так і в ОС Windows. Найбільш відомі [5]:

- Ettercap
- Cain & Abel
- dsniff
- arp-sk

Всі названі програми поширюються вільно.

Детально розглянемо, як виконується ARP-spoofing. Як інструмент будемо використовувати програму ettercap, проте інші інструменти для виконання ARP-spoofing працюють аналогічним чином. Схема проведення атаки приведена у додатку Б.

Отже, вузли мережі сконфігуровані таким способом:

Вузол А – hostA – 192.168.15.201 – 00:04:75:75:46:B1

Вузол B – hostB – 192.168.15.254 – 00:0A:01:D4:D1:39

Вузол C – hostC – 192.168.15.200 – 00:0A:01:D4:D1:E3

Атаку виконує hostC проти вузлів hostA і hostB.

Встановимо ettercap прийнятим в системі способом:

hostC% # apt-get install ettercap

Виконаємо атаку проти вузлів hostA і hostB:

% # Ettercap -T -M arp -L log /192.168.15.201/ /192.168.15.254/

Опції означають:

- -T – використовувати текстовий (консольний) інтерфейс;
- -M arp – використовувати модуль ARP-spoofing для виконання атаки;
- -L log – записувати журнал перехоплення в файли з ім'ям log. *.

В якості аргументів указуються IP-адреси машин, проти яких потрібно виконувати атаку ARP-spoofing.

Нехай, наприклад, в цей час вузол A звертається до вузла B по протоколу POP3 (port 110), класичного прикладу незахищеного, але дуже поширеного протоколу – перевіряє пошту.

hostA% # nc 192.168.15.254 110

USER user

+ OK

PASS password

+ OK

LIST

+ OK

.

Дані, що передаються між клієнтом hostA і сервером hostB, проходять через вузол C. Вони виводяться на екран і записуються в файли.

Після того як атака завершена для виходу з ettercap необхідно натиснути q. Програма відсилає ARP-пакети для відновлення старих записів в кеші ARP вузлів, щоб вони спілкувалися один з одним безпосередньо.

У поточному каталозі повинні з'явитися два файли, що починаються словом, зазначеним після ключа -L при виклику ettercap:

%# ls log.*

log.eci

log.ecp

Переглянути їх вміст можна за допомогою програми etterlog, що входить в пакет ettercap (рис.2.8):

%# etterlog log.eci

Як видно, пароль був успішно перехоплений.

Подивимося як на вузлі hostA (що атакується) змінюється ARP-таблиця

До атаки:

hostA%# arp -an

? (192.168.15.254) at 00:0A:01:D4:D1:39 [ether] on eth0

? (192.168.15.200) at 00:0A:01:D4:D1:E3 [ether] on eth0

Під час атаки:

hostA%# arp -an

? (192.168.15.254) at 00:0A:01:D4:D1:E3 [ether] on eth0

? (192.168.15.200) at 00:0A:01:D4:D1:E3 [ether] on eth0

Після атаки:

hostA%# arp -an

? (192.168.15.254) at 00:0A:01:D4:D1:39 [ether] on eth0

? (192.168.15.200) at 00:0A:01:D4:D1:E3 [ether] on eth0

```
etterlog NG-0.7.3 copyright 2001-2004 ALoR & NaGA
Log file version    : NG-0.7.3
Timestamp           : Thu Jun 21 12:23:11 2007
Type                : LOG_INFO
1698 tcp OS fingerprint
7587 mac vendor fingerprint
2183 known services
================================================
 IP address   : 192.168.15.201
 MAC address  : 00:04:75:75:46:B1
...
 MANUFACTURER : Sohoware
 DISTANCE     : 0
 TYPE         : LAN host
 FINGERPRINT      :
 OPERATING SYSTEM : UNKNOWN
   PORT     : TCP 110 | pop-3   []
      ACCOUNT : user
 / password
  (192.168.15.201)
================================================
```

Рисунок 2.8 – Зміст файлу log.eci

Якщо дивитися, що відбувається на інтерфейсі eth0 комп'ютера hostA (через який виконується атака), можна побачити, що як тільки починається атака, на інтерфейс надходять ARP-пакети, які вказують, що MAC-адреса машини 192.168.15.254 змінилася. Пакети приходять постійно. Коли атака завершена, MAC-адреса в пакета раптово змінюється на іншу. А потім вони взагалі перестають приходити.

%# tcpdump -i eth0 arp

08:34:20.231680 arp reply 192.168.15.254 is-at 00:0a:01:d4:d1:e3 (oui Unknown)
08:34:21.259637 arp reply 192.168.15.254 is-at 00:0a:01:d4:d1:e3 (oui Unknown)
08:34:22.287591 arp reply 192.168.15.254 is-at 00:0a:01:d4:d1:e3 (oui Unknown)
08:34:23.315522 arp reply 192.168.15.254 is-at 00:0a:01:d4:d1:e3 (oui Unknown)
08:34:32.463255 arp reply 192.168.15.254 is-at 00:0a:01:d4:d1:39 (oui Unknown)
08:34:33.491040 arp reply 192.168.15.254 is-at 00:0a:01:d4:d1:39 (oui Unknown)
08:34:34.514988 arp reply 192.168.15.254 is-at 00:0a:01:d4:d1:39 (oui Unknown)

2.2 Сценарій проведення атаки MAC-spoofing

MAC-spoofing – атака канального рівня, яка полягає в тому, що на мережевої карти змінюється MAC-адреса, що змушує комутатор відправляти на порт, до якого підключений зловмисник, пакети, які до цього він бачити не міг [6]. Атаку можна запобігти за допомогою функції port security комутатора.

Цю атаку часто плутають з ARP-spoofing. Насправді це зовсім різні атаки, спільного між якими тільки те, що і та й інша мають відношення до MAC-адресами мережевих пристроїв.

Розглянемо, як можна змінити програмно MAC-адресу мережевого адаптера.

Зміна MAC-адреси в Linux:

% # Ifconfig eth0 down

% # Ifconfig eth0 hw ether 11: 22: 33: 44: 55: 66

% # Ifconfig eth0 up

Або, якщо зміна має бути постійною (для Debian):

auto eth0

iface eth0 inet dhcp

hwaddress ether 01: 02: 03: 04: 05: 06

Приклад наведено для випадку, коли використовується DHCP, але це зовсім не обов'язково.

Зміна MAC-адреси в FreeBSD:

ifconfig em0 link 11: 22: 33: 44: 55: 66

Тут em0 це назва інтерфейсу. Зміна діє тільки до перезавантаження.

2.3 Сценарій проведення атаки переповнення CAM-таблиці комутатора

Утиліта ArpFlood дозволяє організувати відправку масових ARP запитів і експериментувати з різними видами атак на комутатор. Суть атаки полягає в перенасичення пам'яті комутатора, що містить таблицю комутації (рис.2.9). З цією роллю легко справляється не тільки зловмисник, але і деякі програми (наприклад, вірус або SpyWare).

Для здійснення цієї атаки використовується команда [6]:

arpflood.exe -interface 3 -loops 0 -view 0

Вона дозволяє відправити множинні ARP-запити з випадковими MAC-адресами. Аргумент «-loops 0» використовується для запуску утиліти в невпинному режимі, а «-view 0» забороняє висновок результату на екран для підвищення продуктивності. Реакція комутатора цілком очікувана: таблиця комутації миттєво заповнюється MAC-адресами, займаючи весь обсяг вільної пам'яті. Наприклад, Switch 2960 Cisco може тримати в пам'яті не більше 8192 MAC-адрес.

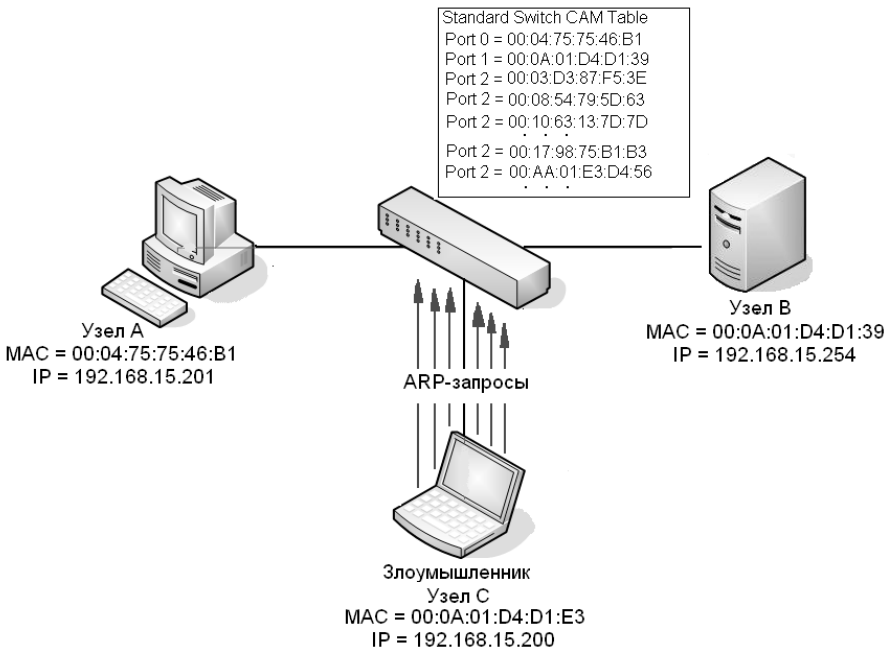


Рисунок 2.9 – Схема організації атаки переповнення CAM-таблиці комутатора

Команда show mac-address-table дозволяє переглядати таблицю комутації. На першому етапі вона складається всього з декількох записів, тоді як після запуску ArpFlood, вільного місця в таблиці більше не залишається (рис.2.9).

З перших секунд атаки комутатор погано реагує на спроби віддаленого управління. Індикація відбувається повільно, а час відгуку на команди – невиправдано велика. Однак, це ніяк не відбивається на основній функції комутатора і його пропускна здатність не страждає. Тобто удар припадає тільки по системі управління, а не на основний функціонал пристрою.

Далі, комутатор, не володіючи достатнім обсягом пам'яті, щоб зберігати всю кореспонденцію MAC-адрес, зобов'язаний перейти в режим хаба, що дозволяє зловмисникові переглядати дані.

Таким чином, зловмисник отримує весь обсяг обміну трафіком між клієнтом з адресою 192.168.15.201 і сервером 192.168.15.254. Слід зазначити, що існує два варіанти розвитку ситуації залежно від того, відбувався обмін трафіком між клієнтом і сервером до початку атаки.

У першому варіанті, де атака починається раніше «спілкування» між сервером і клієнтом, комутатор не встигає записати їх MAC-адреси в таблицю комутації і, під напливом флуду, переходить в режим хаба раніше, ніж клієнт посилає запит на сервер. Відповідно, всі запити клієнта і відповіді сервера з'являються на всіх портах і доступніші зловмисникові в повному обсязі.

У другому варіанті, атака починається після того, як MAC-адреси клієнта і сервера записані в таблицю комутації, що означає неможливість прослуховування. Але, оскільки термін «життя» записів в таблиці комутації обмежений, по закінченню цього часу комутатор втрачає останні відомості про «правильну» комутацію, не може їх отримати через переповнення пам'яті, і далі розвиток подій відбувається за першим варіантом.

За замовчуванням, час «життя» записи в таблиці комутації для Switch 2960 Cisco становить 5 хвилин. Це час можна перевизначити командою:

mac-address-table aging-time 10

параметр задає значення – 10 секунд.

Ще одним наслідком атаки стане зростання трафіку на всіх портах комутатора, який перейшов в режим хаба. Адже те, що раніше транслювалося тільки між двома портами, тепер виявляється доступним на кожному порту, що, зрозуміло, негайно позначається на кінцевих користувачах. Крім того, будь-який комутатор володіє обмеженням за сумарною смугою пропускання. Наприклад, для Cisco Catalyst 2960T-24 цей показник становить 8,8 Гбіт/с (тобто сумарний потік трафіку між усіма портами не може перевищувати 8,8 Гбіт/с). Це означає, що при значних обсягах трафіку, що надходить на всі порти, загальна смуга пропускання може перевищити можливості комутатора [6].

2.4 Сценарій проведення атаки на протокол STP

STP (Spanning Tree Protocol) – мережевий протокол (або сімейство мережевих протоколів) призначений для автоматичного видалення циклів (петель комутації) з топології мережі на канальному рівні в Ethernet-мережах. В даний час протокол STP (або аналогічний) підтримується багатьма Ethernet-коммтутаторамі, як реальними, так і віртуальними, за винятком найпримітивніших [7].

STP використовує алгоритм STA (Spanning Tree Algorithm), результатом роботи якого є граф у вигляді дерева (зв'язний і без простих циклів). Для обміну інформацією між собою комутатори використовують спеціальні пакети, так звані BPDU (Bridge Protocol Data Units). BPDU бувають двох видів: конфігураційні (Configuration BPDU) і панічні TCN (Topology Change Notification BPDU). Перші регулярно розсилаються кореневих комутатором (і ретранслюються іншими) і використовуються для побудови топології, другі відсилаються в разі зміни топології мережі (простіше кажучи, підключенні \ відключенні комутатора) [7].

Конфігураційні BPDU містять кілька полів, серед них найбільш важливі:

- код відправника (Bridge ID);
- ідентифікатор кореневого свіча (Root Bridge ID);
- ідентифікатор порту, з якого відправлений даний пакет (Port ID);
- вартість маршруту до кореневого свіча (Root Path Cost).

Так як пристрої не знають своїх сусідів, ніяких відносин (суміжності / сусідства) вони один з одним не встановлюють. Вони шлють BPDU з усіх

працюючих портів на мультікастову ethernet-адресу 01-80-c2-00-00-00 (за замовчуванням кожні 2 секунди), яку прослуховують всі комутатори з включеним STP.

Топологія без петель формується наступним чином. Спочатку вибирається так званий кореневий міст/свіч (root bridge). Це пристрій, який STP вважає точкою відліку, центром мережі; все дерево STP сходиться до нього. Вибір базується на такому понятті, як ідентифікатор свіча (Bridge ID). Bridge ID це число довжиною 8 байт, яке складається з Bridge Priority (пріоритет, від 0 до 65535, за замовчуванням 32768 + номер vlan або інстанси MSTP, в залежності від реалізації протоколу), і MAC-адреси свого пристрою. На початку виборів кожен комутатор вважає себе кореневим, про що і заявляє всім іншим за допомогою BPDU, в якому представляє свій ідентифікатор як ID кореневого свіча. При цьому, якщо він отримує BPDU з меншим Bridge ID, він починає анонсувати отриманий Bridge ID в якості кореневого. В результаті, кореневим виявляється той комутатор, чий Bridge ID менше всіх.

Після того, як комутатори вибрали root bridge, кожен з інших комутаторів повинен знайти один, і тільки один порт, який буде вести до кореневого. Такий порт називається кореневим портом (Root port). Щоб зрозуміти, який порт краще використовувати, кожен некореневий комутатор визначає вартість маршруту від кожного свого порту до кореневого комутатора. Ця вартість визначається сумою вартостей всіх лінків, які потрібно пройти кадру, щоб дійти до кореневого комутатора. У свою чергу, вартість линка визначається просто – по його швидкості (чим вище швидкість, тим менше вартість). Процес визначення вартості маршруту пов'язаний з полем BPDU «Root Path Cost» і відбувається наступним чином. Кореневої комутатор посилає BPDU з полем Root Path Cost, рівним нулю. Найближчий комутатор дивиться на швидкість свого порту, куди BPDU прийшов, і додає вартість згідно з таблицею 2.1.

Таблиця 2.1 - Таблиця визначення вартості маршруту від порту комутатора до Root bridge

Швидкість порту	Вартість STP (802.1d)
10 Mbps	100
100 Mbps	19

1 Gbps	4
10 Gbps	2

Далі цей другий комутатор посилає BPDU нижчестоящим комутаторам, але вже з новим значенням Root Path Cost, і далі по ланцюжку вниз. Якщо мають місце однакові вартості – кореневих вибирається менший порт.

Далі вибираються призначені (Designated) порти. З кожного конкретного сегмента мережі повинен існувати тільки один шлях у напрямку до кореневого комутатора, інакше це петля. Призначеним портом вибирається той, який має кращу вартість в даному сегменті. У кореневого комутатора всі порти – призначені.

Після того, як обрані кореневі і призначені порти, що залишилися блокуються, таким чином, розриваючи петлю. Приклад настройки портів комутаторів відповідно до протоколу STP демонструє схема, представлена на рис.2.10, в якій чотири комутатора (sw) підключені петлею.

Навіть якщо в мережі немає петель на канальному рівні, все одно така проблема можлива. Для реалізації цієї атаки необхідно знайти 2 підключення до різних комутаторів (наприклад, до двох поверховими комутаторів будівлі). Далі, встановити ще один комутатор, налаштувавши його так, щоб він став кореневим в вийшла петля STP, як на рис.2.11. Це робиться командою: spanning-tree vlan {VLAN_LIST} priority [8].

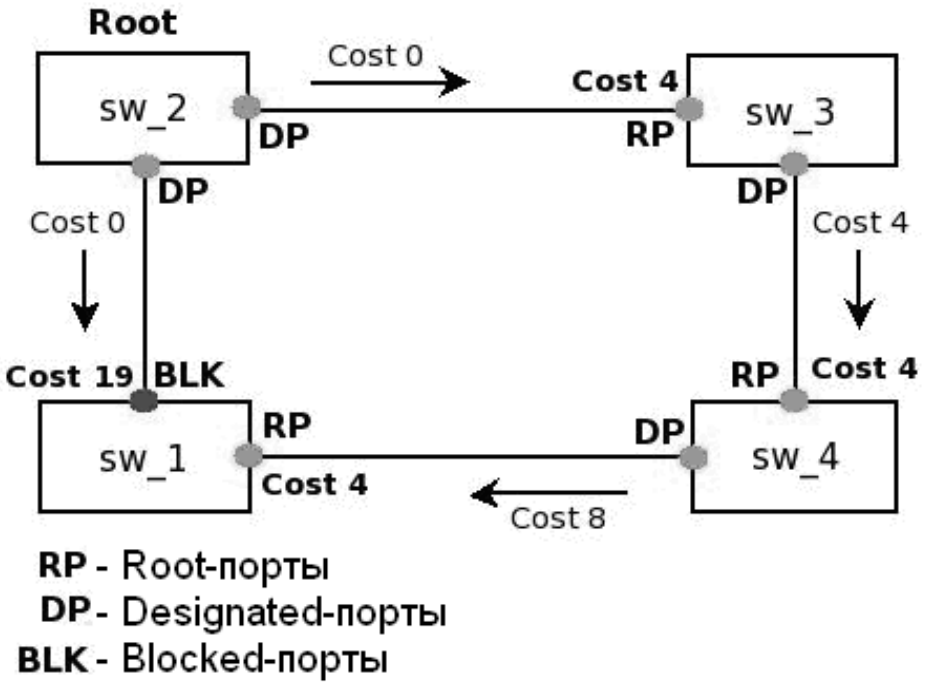


Рисунок 2.10 – Приклад настройки портів комутаторів відповідно до алгоритму SPA

Далі, так як цей новий (ворожий) комутатор не може мати заблокованих портів, порт заблокується на існуючому обладнанні компанії, щоб розірвати петлю. І трафік між двома сегментами піде через ворожий комутатор, де атакуючий зможе зробити з ним все що завгодно, від простого прослуховування до впровадження посередника (Man-in-the-Middle attack), який зможе читати навіть зашифрований зв'язок [8].

Є багато способів провести таку атаку і один з них – використання пари Wi-Fi точок в режимі Bridge. Одна точка ставиться на одному поверсі, інша – на іншому (рис.2.12).

Різновидом такої атаки є злом якогось доступного, наприклад, поверхового комутатора і перенастроювання його як кореневого комутатора STP.

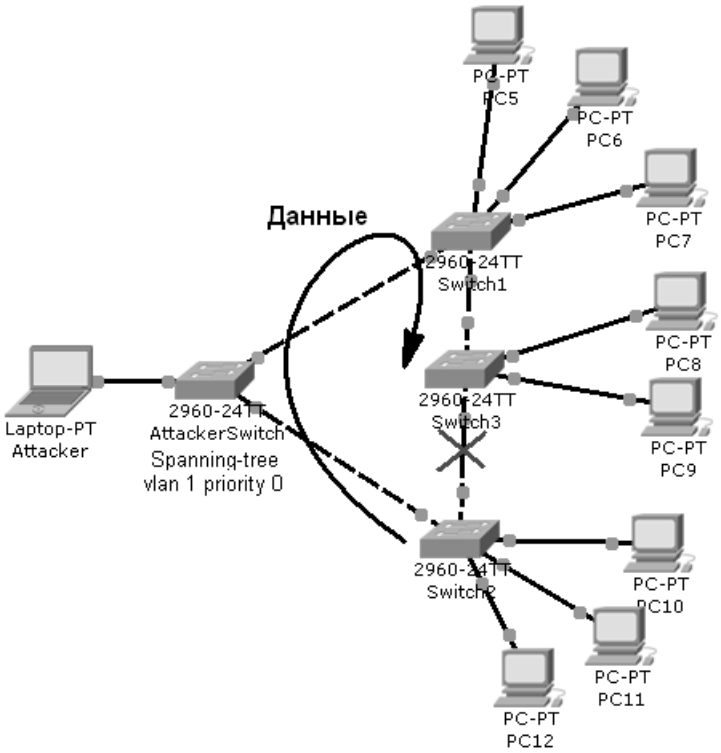


Рисунок 2.11 – Схема проведення атаки на STP протокол

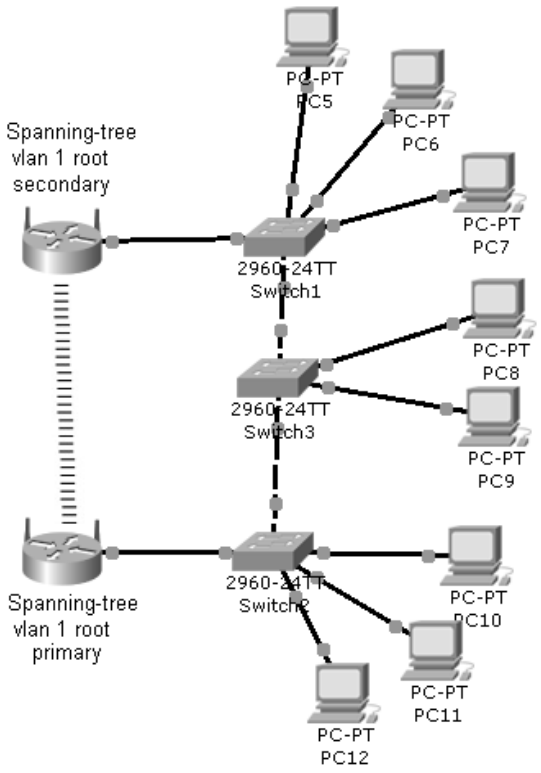


Рисунок 2.12 – Схема проведення атаки на STP протокол з використанням пари Wi-Fi точок

3 ДОСЛІДЖЕННЯ ФУНКЦІЙ БЕЗПЕКИ НА КОМУТАТОРІ CISCO CATALYST 2960

У сучасних локальних мережах обмін інформацією, як правило, передбачає передачу даних через комутатор.

Тому сам комутатор і протоколи, які використовують комутатори можуть бути метою атак. Більш того, деякі настройки комутаторів (як правило, це налаштування за замовчуванням) дозволяють виконати ряд атак і отримати несанкціонований доступ до мережі або вивести з ладу мережеві пристрої.

Однак, комутатор може бути і досить потужним засобом захисту. Так як через нього відбувається все взаємодії в мережі, то логічно контролювати це на ньому.

Звичайно, використання комутатора як засобу захисту передбачає, що використовується не найпростіший комутатор 2-го рівня, а комутатор з відповідними функціями для забезпечення безпеки.

В даному розділі проведемо настройку 24 портового комутатора Cisco Catalyst 2960, використовуючи додаткові вбудовані функції, для забезпечення необхідних політик безпеки мережі.

Розглянемо докладніше функції комутаторів Cisco Catalyst для забезпечення безпеки мережі. Список їх наведено в табл.3.1.

Таблиця 3.1 - Функції комутаторів для забезпечення безпеки роботи мережі на канальному рівні

Функція комутатора	Від яких атак захищає
Port security	Переповнення таблиці комутації, несанкціонована зміна MAC-адреси
DHCP Snooping	Підміна DHCP-сервера в мережі, DHCP starvation
Dynamic ARP Inspection	ARP-spoofing
IP Source Guard	IP-spoofing

IP Source Guard (Dynamic IP Lockdown) – функція комутатора, яка обмежує IP-трафік на інтерфейсах 2-го рівня, фільтруючи трафік на підставі таблиці прив'язок DHCP snooping і статичних відповідностей. Функція використовується для боротьби з IP-spoofingом.

3.1 Функція Port security

Port security – функція комутатора, що дозволяє вказати MAC-адреси хостів, яким дозволено передавати дані через порт. Після цього порт не передає пакети, якщо MAC-адресу відправника не вказано як дозволену. Крім того, можна вказувати не конкретні MAC-адреси, дозволені на порту комутатора, а обмежити кількість MAC-адрес, яким дозволено передавати трафік через порт. Використовується для запобігання [9]:

- несанкціонованої зміни MAC-адреси мережевого пристрою або підключення до мережі;
- атак спрямованих на переповнення таблиці комутації.

Комутатор підтримує такі типи безпечних MAC-адрес:

1) Статичні MAC-адреси:
   - задаються статично командою switchport port-security mac-address mac-address в режимі настройки інтерфейсу;
   - зберігаються в таблиці адрес;
   - додаються в поточну конфігурацію комутатора.
2) Динамічні MAC-адреси:
   - динамічно вивчаються;
   - зберігаються тільки в таблиці адрес;
   - видаляються при перезавантаженні комутатора.
3) Sticky MAC-адреси:
   - можуть бути статично налаштовані або динамічно вивчені;
   - зберігаються в таблиці адрес;
   - додаються в поточну конфігурацію комутатора. Якщо ці адреси збережені в файлі конфігурації, після перезавантаження комутатора, їх не треба заново перенастроювати.

Порушенням безпеки для port security вважаються ситуації:

- максимальна кількість безпечних MAC-адрес було додано в таблицю адрес і хост, чий MAC-адрес не записаний в таблиці адрес намагається отримати доступ через інтерфейс;
- адреса, вчинена або налаштована як безпечна на одному інтерфейсі, з'явилася на іншому безпечному інтерфейсі в тому ж VLAN.

На інтерфейсі можуть бути налаштовані такі режими реагування на порушення безпеки [9]:

- protect – коли кількість безпечних MAC-адрес досягає максимального обмеження налаштованого на порту, пакети з невідомою MAC-адресою відправника відкидаються до тих пір, поки не буде видалено достатню кількість безпечних MAC-адрес, щоб їх кількість була меншою максимального значення, або збільшено максимальна кількість дозволених адрес. Сповіщення про порушення безпеки немає.
- restrict – коли кількість безпечних MAC-адрес досягає максимального обмеження налаштованого на порту, пакети з невідомою MAC-адресою відправника відкидаються до тих пір, поки не буде видалено достатню кількість безпечних MAC-адрес, щоб їх кількість була меншою максимального значення, або збільшено максимальна кількість дозволених адрес. У цьому режимі при порушенні безпеки відправляється оповіщення – відправляється SNMP trap, повідомлення syslog і збільшується лічильник порушень (violation counter).
- shutdown – порушення безпеки призводить до того, що інтерфейс переводиться в стан error-disabled і вимикається негайно, і вимикається LED порту. Відправляється SNMP trap, повідомлення syslog і збільшується лічильник порушень (violation counter). Коли порт в стані error-disabled, вивести з цього стану його можна ввівши команду errdisable recovery cause psecure-violation або вручну включити інтерфейс ввівши в режимі настройки інтерфейсу shutdown і no shutdown. Це режим за замовчуванням.

3.2 Функція DHCP snooping

DHCP snooping – функція комутатора, призначена для захисту від атак з використанням протоколу DHCP. Наприклад, атаки з підміною DHCP-сервера в мережі або атаки DHCP starvation, яка змушує DHCP-сервер видати всі існуючі на сервері адреси зловмисникові. DHCP snooping регулює тільки повідомлення DHCP і не може вплинути безпосередньо на трафік користувачів або інші протоколи. Деякі функції комутаторів, що не мають безпосереднього відношення до DHCP, можуть виконувати перевірки на підставі таблиці прив'язок DHCP snooping (DHCP snooping binding database).

Для правильної роботи DHCP snooping, необхідно вказати які порти комутатора будуть довіреними (trusted), а які - ні (untrusted, в подальшому - ненадійними) [10]:

Ненадійні (Untrusted) – порти, до яких підключені клієнти. DHCP-відповіді, що приходять з цих портів відкидаються комутатором. Для ненадійних портів виконується ряд перевірок повідомлень DHCP і створюється база даних прив'язки DHCP (DHCP snooping binding database).

Довірені (Trusted) – порти комутатора, до яких підключений інший комутатор або DHCP-сервер. DHCP-пакети отримані з довірених портів, не відкидаються.

За замовчуванням комутатор відкидає DHCP-пакет, який прийшов на ненадійний порт, якщо:

- приходить одне з повідомлень, які відправляє DHCP-сервер (DHCPOFFER, DHCPACK, DHCPNAK або DHCPLEASEQUERY);
- приходить повідомлення DHCPRELEASE або DHCPDECLINE, в якому міститься MAC-адресу з бази даних прив'язки DHCP, але інформація про інтерфейс в таблиці не збігається з інтерфейсом, на якому був отриманий пакет;
- у DHCP-пакеті, що прийшов, не збігаються MAC-адреса, вказана в DHCP-запиті, і MAC-адреса відправника;
- приходить DHCP-пакет, в якому є опція 82.

3.3 Функція Dynamic ARP Inspection

Dynamic ARP Inspection – функція комутатора, призначена для захисту від атак з використанням протоколу ARP. Наприклад, атаки ARP-spoofing, що дозволяє перехоплювати трафік між вузлами, які розташовані в межах одного широкомовного домену. Dynamic ARP Inspection регулює тільки повідомлення протоколу ARP і не може вплинути безпосередньо на трафік користувачів або інші протоколи.

Для правильної роботи Dynamic ARP Inspection, необхідно вказати які порти комутатора будуть довіреними (trusted), а які – ні (untrusted) [10]:

- ненадійні (Untrusted) – порти, до яких підключені клієнти. Для ненадійних портів виконується ряд перевірок повідомлень ARP.
- довірені (Trusted) – порти комутатора, до яких підключений інший комутатор. Повідомлення протоколу ARP отримані з довірених портів, не відкидаються.

Якщо порт ненадійний, комутатор перехоплює все ARP-запити і ARP-відповіді на ненадійних портах перш ніж перенаправляти їх. Комутатор

перевіряє відповідність MAC-адреси IP-адресі на ненадійних портах. Перевірка відповідності MAC-адреси IP-адресі може виконуватися на підставі статичних записів або бази даних прив'язки DHCP.

Алгоритм роботи комутатора з встановленими функціями DHCP snooping і Dynamic ARP Inspection наведено в додатку В.

4 РЕАЛІЗАЦІЯ МЕХАНІЗМІВ ЗАХИСТУ В СЦЕНАРІЯХ МЕРЕЖЕВИХ АТАК

4.1 Організація захисту комутатора від атаки MAC spoofing і переповнення CAM-таблиці

Комутатор має CAM-таблицю, де міститься «прив'язка», які MAC-адреси на якому порту приймаються. Зрозуміло, CAM-таблиця не нескінченна і має свої розміри. Наприклад, комутатор Catalyst 2960 може містити 8192 MAC-адрес, Catalyst 6000 серії – 128000 MAC-адрес.

Коли вся таблиця буде зайнята, нові записи не зможуть додаватися, весь трафік буде проходити на всі порти. Що це дасть атакуючому цілком очевидно. Він може «прослухати» весь мережевий трафік і отримати конфіденційну інформацію. Варто відзначити, що все це дієво для VLAN, в якому знаходиться зловмисник, тобто після переповнення даної таблиці атакуючий не зможе прослуховувати весь мережевий трафік, який «ходить» через комутатор, а лише свого VLAN, але і це не дуже радісно.

Логіка підказує, що для придушення такої атаки необхідно вказати, що на порту комутатора, до якого підключений користувач, може бути, скажімо, не більше однієї MAC-адреси, а в разі якщо з'являється більше однієї, перевести порт у відключений стан і відправити повідомлення адміністратору про порушення безпеки (наприклад, на syslog-сервер).

Розглянемо на прикладі сценарію мережевої атаки. Припустимо, у нас є комутатор Cisco Catalyst 2960 і 24 порти, до яких підключені користувачі і сервер. Потрібно зробити так, щоб на кожному порту міг бути тільки один хост (іншими словами, тільки одна MAC-адреса). Налаштування комутатора виконаємо в мережевому емуляторі Cisco Packet Traser 5.3.2 [11]. Схема моделювання показана на рис.4.1.

Для цього заходимо в режим глобального конфігурування:

Switch # conf t

Потім перейдемо до конфігурації портів, виберемо відразу все, з 1 по 24:

Switch (config) #int range f0 / 1

Потім вкажемо, що всі ці порти є портами доступу:

Switch (config-if-range) #switchport mode access

Включаємо захист порту port-security:

Switch (config-if-range) #switchport port-security

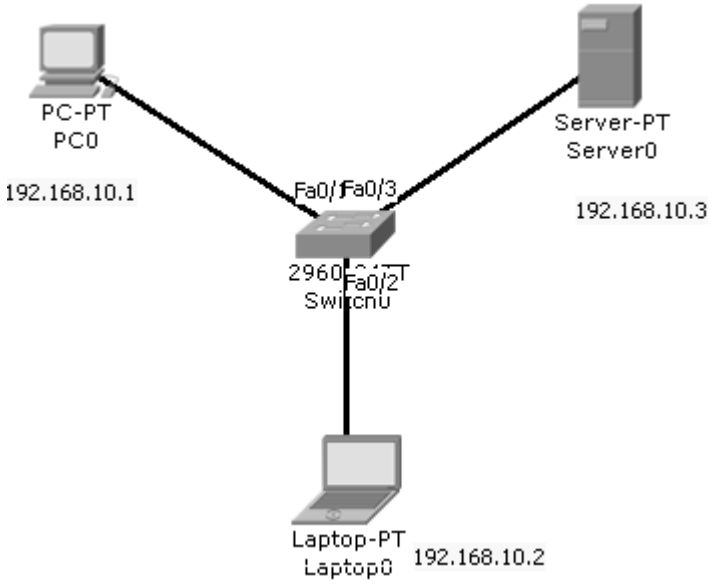


Рисунок 4.1 – Схема моделювання сценарію мережевої атаки переповнення CAM-таблиці комутатора

Вибираємо реакцію на порушення політики безпеки, тобто що буде комутатор робити, коли на порту з'явиться більше MAC-адрес, ніж зазначено. В даному випадку бажано, щоб порт вимикався і надсилалося відповідне повідомлення по SNMP trap і syslog. Дану опцію можна не вказувати примусово, вона діє за замовчанням.

Також існують режими: protect і restrict. Сенс цих режимів полягає в тому, що порт не завершить роботу (тобто переходити в стан shutdown), а лише будуть блокуватися пакети, якщо виявлено порушення, пов'язане з MAC-адресами. Protect від Restrict відрізняється тим, що при виникненні позаштатної ситуації restrict може послати snmp trap і syslog-повідомлення про порушення політики безпеки:

Switch (config-if-range) #switchport port-security violation shutdown

Відповідно вказуємо, скільки MAC-адрес ми готові побачити на цьому порту. В даному випадку 1 MAC-адресу, значення 1, встановлюється за замовчанням.

Switch (config-if-range) #switchport port-security maximum 1

Поставимо порт комутатора в режим навчання, тобто перша MAC-адреса, яка буде отримана через цей порт, буде прописана автоматично в

running-config. Запис буде зберігатися до тих пір, поки не буде перезавантажений комутатор. Або якщо виконати команду «copy running-config startup config» (або просто wr), то значення прив'язки MAC-адреси до порту буде збережено і в подальшому може використовуватися навіть після перезавантаження комутатора.

Switch (config-if-range) #switchport port-security mac-address sticky

Цього заходу цілком достатньо, щоб уникнути атаки на переповнення CAM-таблиці.

Команда для перегляду установок, зроблених на портах, пов'язаних з port-security:

Show port-security interface імя_інтерфейса

Наприклад, виконаємо:

Switch # show port-security int fa0 / 1

Результат виведення налаштувань інтерфейсу fa0 / 1 представлений на рис.4.2.

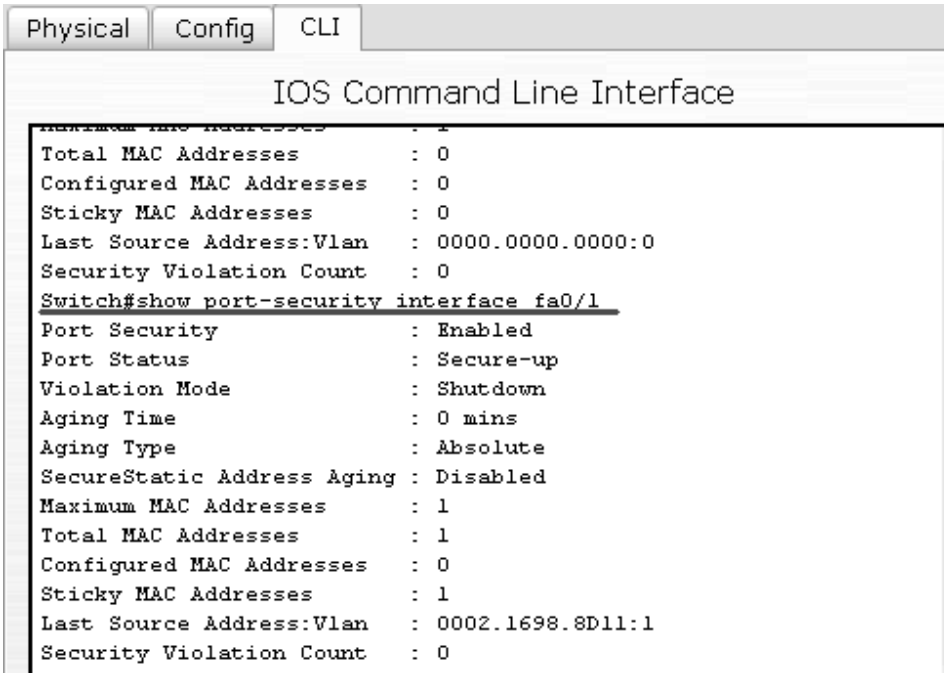


Рисунок 4.2 – Висновок налаштувань інтерфейсу f0/1

Перевіряємо таблицю адрес:

Switch # showmac-address-table

Результат виконання команди представлений на рис.4.3.

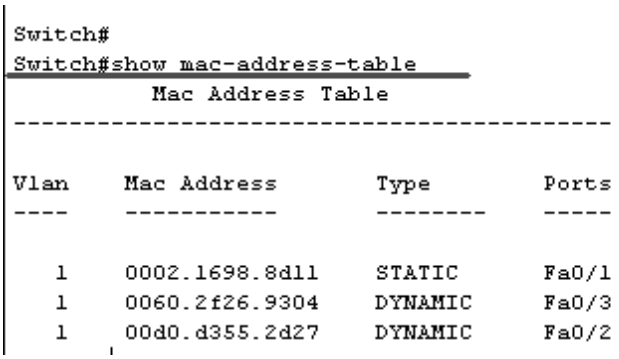


Рисунок 4.3 – Відображення таблиці MAC-адрес комутатора

Тепер спробуємо поміняти MAC-адресу на одному з пристроїв. Наприклад, змінимо MAC- адресу на хості PC1 (0002.1698.8d11) на (0002.1698.8d12), просто замінивши цифру в кінці. При цьому порт відразу ж відключиться. Це говорить про те, що цей порт не пропускає більше однієї MAC-адреси, як ми і вказали в налаштуваннях.

Switch # show interfaces fa0 / 1

FastEthernet0 / 1 is down, line protocol is down (err-disabled)

Як видно порт вимкнувся. Результат виконання команди ping з хоста 192.168.10.1 до хосту 192.168.10.2 наведено на рис.4.4.

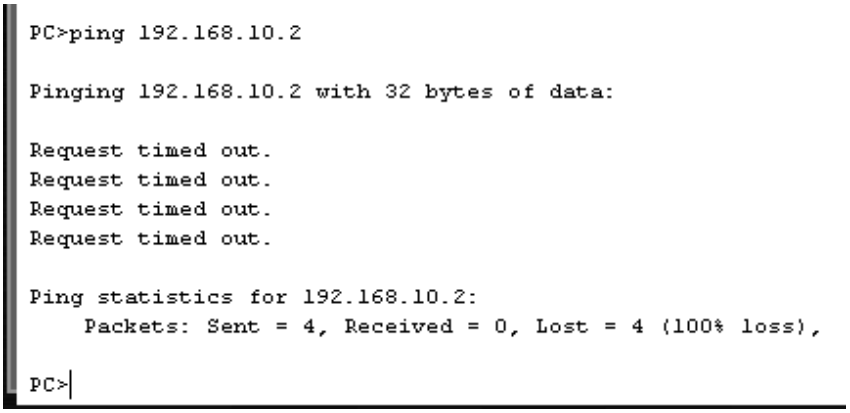


Рисунок 4.4 – Результат виконання команди ping

За замовчуванням порт стоїть в режимі shut down. Якщо цей режим не влаштовує, то можна вказати інший час налаштування комутатора:

Switch (config-if) #switchport port-security violation protect / restrict / shutdown

Піднімаємо порт:

Switch # clear port-security all

Switch (config-if) #no shutdown

Ці ж заходи боротьби допоможуть захистити і від атаки MAC-spoofing. Додатково можна вказати MAC-адреси статично, динамічно або в режимі навчання. Для вказівки статичної MAC-адреси, в режимі конфігурації інтерфейсу необхідно виконати:

Switch (config-if) # switchport port-security mac-address 3234.2343.fa12

де 3234.2343.fa12 – MAC-адреса клієнта.

Для вказівки динамічної MAC-адреси нічого додаткового не робиться, необхідно тільки включити функцію port-security, як було описано вище.

Щоб вказати режим навчання MAC-адрес, необхідно виконати в режимі конфігурації інтерфейсу команду:

Switch (config-if-range) #switchport port-security mac-address sticky

Можна вказати час життя записів ARP-таблиці. Наприклад, вкажемо, що ARP-таблиця має таймер в 60 секунд.

Switch (config-if-range) #arp timeout 60

Команда призведе до того, що MAC-адресу буде перебувати в ARP-кеші 60 секунд без оновлення.

4.2 Організація захисту атак на DHCP-сервер

Існує кілька способів атакувати DHCP-сервер [11]:

1) Зловмисник може сформувати і послати DHCP-серверу величезну кількість DHCP-запитів з різними MAC-адресами. Сервер буде виділяти IP-адреси з пулу, і рано чи пізно весь DHCP-пул закінчиться, після чого сервер не зможе обслуговувати нових клієнтів. Даний вид атаки можна класифікувати як DoS (Denial of Service – отказаз в обслуговуванні). Порушується працездатність мережі.

Метод боротьби з такими атаками називається DHCP snooping. Розглянемо, як це працює. Коли комутатор отримує пакет, то він порівнює MAC-адресу, вказану в DHCP-запиті, і MAC-адресу, який був прописаний на порту комутатора. Якщо адреси збігаються, то комутатор відправляє пакет далі. Якщо адреси не збігаються, то комутатор відкидає пакет.

2) Зловмисник може поставити свій DHCP-сервер і видавати свої настройки користувачам мережі (може вказати будь-DNS, Gateway і т.п.), і

скористатися вже на свій розсуд, починаючи від прослуховування трафіку до підробки DNS-відповідей, та ін.

Якщо в мережі існує декілька DHCP-серверів, то на запит будуть відповідати всі сервери, але клієнтом буде оброблена тільки перша відповідь. Який з DHCP-серверів відповість швидше і чия відповідь швидше дійде до клієнта залежить від багатьох факторів, таких як: завантаження DHCP-сервера, завантаження мережі і т.п.

Для того щоб зловмисник був упевнений, що саме від його DHCP-сервера клієнт отримає відповідь, атакуючим може бути попередньо проведена DoS-атака на легальні DHCP-сервера способом, описаним раніше.

В технології DHCP snooping існує поняття довірчих і недовірчих портів (trusted і untrusted відповідно). Довірчі порти – це порти, з яких може приходити відповідь DHCP (DHCPOFFER і так далі), а недовірчі порти – це порти, з яких не можуть приходити відповіді DHCPOFFER.

Довірчі порти вказуються вручну. Всі порти, які не вказані довірчими, автоматично стають недовірчими. Порт, який безпосередньо підключений до DHCP-сервера, повинен бути оголошений як довірчий (trust порт).

Розглянемо налаштування DHCP snooping для схеми, наведеної на рис.4.5. На комутаторах Switch0 і Switch1 включений DHCP snooping. Порт Fa0/3 комутатора Switch1 і порт Fa0/2 комутатора Switch0 вказані довіреними, так як комутатор, на якому включений DHCP snooping буде перенаправляти DHCP-запити тільки на довірені порти. Всі інші порти оголошені ненадійними, так як на ненадійних портах повідомлення DHCP-сервера будуть відкидатися.

Порядок настройки наступний:

1) Налагодження та перевірка роботи DHCP-сервера та DHCP-ретранслятора без включеного DHCP snooping.

2) Включення DHCP snooping. Після включення DHCP snooping на комутаторі і в відповідних VLAN, всі порти комутатора за замовчуванням вважаються ненадійними.

3) Вказівка довірених портів. Ті порти, до яких підключені комутатори і які ведуть до DHCP-сервера (або порти до яких сервер підключений), повинні бути налаштовані як довірені.

4) Налаштування політики обробки опції 82.

5) Включення або виключення додаткових перевірок DHCP-повідомлень.

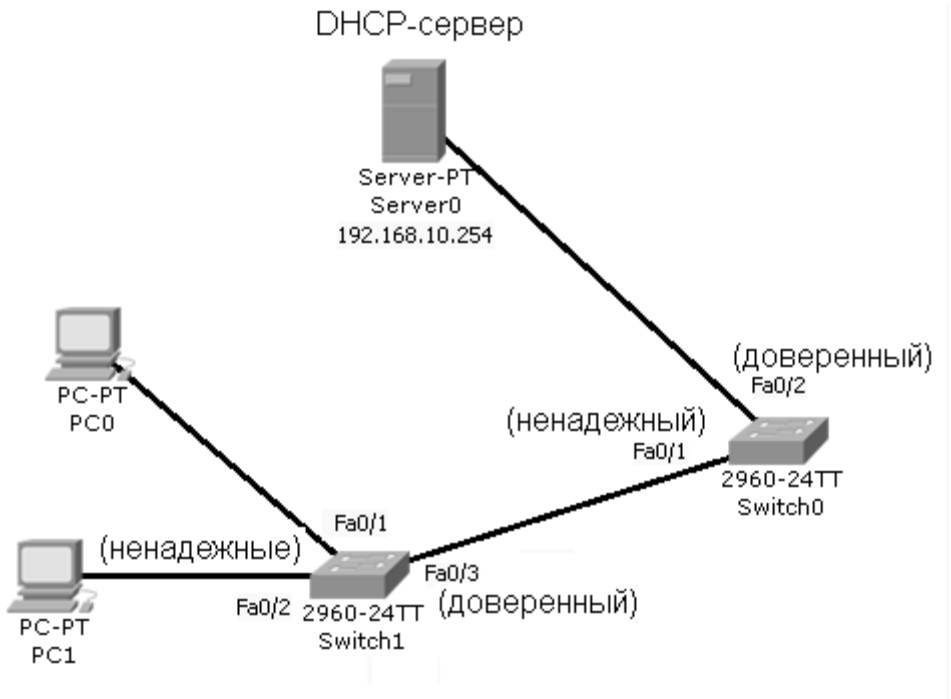


Рисунок 4.5 - Модель мережі для настройки DHCP snooping

Після того, як DHCP snooping включений на комутаторі, по міру видачі адрес клієнтам, починає заповнюватися база даних прив'язки DHCP. У базі даних прив'язки DHCP зберігаються (інформація зберігається тільки про ненадійні порти):

- MAC-адреса клієнта;
- орендована IP-адреса клієнта;
- час оренди в секундах;
- ідентифікатор VLAN;
- ідентифікатор порту до якого приєднаний клієнт.

DHCP snooping налаштовується для кожного VLAN. Для настройки DHCP snooping необхідно спочатку включити snooping в режимі глобальної конфігурації, потім включити на потрібному VLAN, потім вказати trust-порти. Розглянемо на прикладі.

Switch (config) # ip dhcp snooping

Switch (config) # ip dhcp snooping vlan 10

Switch (config) #int f0 / 1

Switch (config-if) #ip dhcp snooping trust

В даному прикладі ми включили захист DHCP на VLAN 10. Інтерфейс f0 / 1 у нас підключений безпосередньо до DHCP-сервера, тому на ньому ми включили trust.

Також можна включити або виключити опцію 82 DHCP (яка відповідає за інформацію relay, тобто через які комутатори пройшов даний пакет, аналогію можна провести з таблицею маршрутизації). Робиться в режимі глобального конфігурування командою:

Switch (config) #ip dhcp snooping information option

Також є можливість включити обмеження кількості запитів DHCP в секунду. Робиться це на інтерфейсі, в нашому випадку f0/1. До цього параметру треба ставитися з обережністю. Якщо кількість запитів в секунду буде більше, ніж ми вказали (в нашому прикладі 100), то запити будуть відхилені.

Switch (config) #interface fa0/1

Switch (config-if) #ip dhcp snooping limit rate 100

4.3 Організація захисту проти атак ARP-spoofing

Так само, як і при реалізації функції DHCP snooping, на обох комутаторах схеми, зображеної на рис. 4.6, необхідно прописати команду ip dhcp snooping, вказати VLAN командою ip dhcp snooping vlan 10 в режимі глобальної конфігурації. Потім на інтерфейсах fa0/1 Switch1 і fa0/3 Switch0, що дивляться в бік DHCP сервера, потрібно прописати команду ip dhcp snooping trust.

Далі командою ip arp inspection vlan 10, де 10 – номер VLAN, включається функція захисту від ARP spoofing атак, яка дозволяє комутатора стежити за кожною прив'язкою IP до MAC адресу кожного пристрою в усій мережі. Здійснюється ця функція таким чином, що комутатор спостерігає за довіреними інтерфейсами, реєструє чи проходять через нього DHCP запити і становить таблицю прив'язки IP адрес до MAC адрес. Таблицю прив'язок можна подивитися командою show ip dhcp snooping binding.

Обов'язково потрібно вказати довірені лінії зв'язку між комутаторами, щоб пакети, що проходять через них, не піддавалися обстеженню на відповідність MAC і IP адреси. У нашому випадку це лінія між fa0/1 Switch1 і fa0/4 Switch0. Отже, в режимі конфігурації даних портів необхідно прописати команду ip arp inspection trust.

Приклад для комутатора Switch0

Switch0 (config) #ip dhcp snooping

Switch0 (config) #ip dhcp snooping vlan 10

Switch0 (config) #interface fa0 / 3
Switch0 (config-if) #ip dhcp snooping trust
Switch0 (config) #ip arp inspection vlan 10
Switch0 (config) #interface fa0 / 4
Switch0 (config-if) #ip arp inspection trust

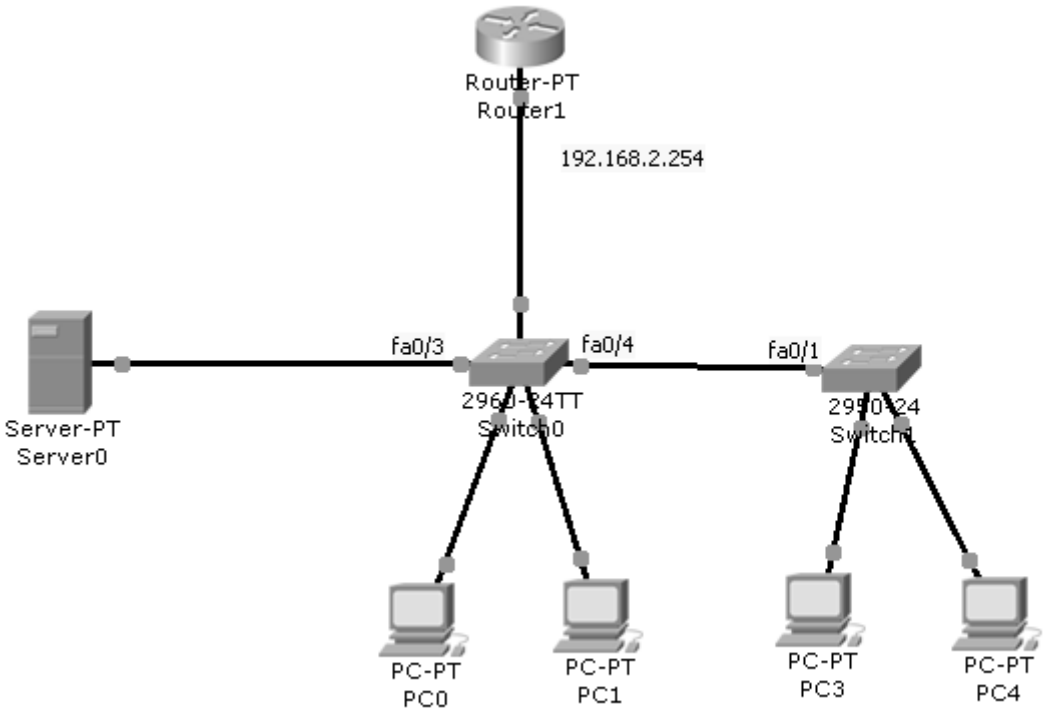


Рисунок 4.6 – Модель мережі для налаштування Dynamic ARP Inspection

Таким чином, ми захистили від ARP spoofing атаки ті хости, які отримали адресу автоматично. Залишається завдання захистити від підміни записи в ARP таблиці комутаторів статичні адреси DHCP сервера або шлюзу.

Для прикладу захистимо ARP записи тільки для статичної адреси шлюзу 192.168.2.254 і його MAC адресу 0033.22a3.fa12. Для цього необхідно створити ARP список доступу з режиму глобальної конфігурації обох комутаторів командою arp access-list GW, де GW – назва списку доступу. Потім потрібно вказати статичну IP адресу і MAC адресу шлюзу командою permit ip host 192.168.2.254 mac host 0033.22a3.fa12. Далі необхідно прив'язати створений список доступу до VLAN 10 командою ip arp inspection filter GW vlan 10 static.

Тепер у разі, якщо будь-якої хост в мережі, підключений до комутатора Switch0 або Switch1, вирішить змінити свою IP адресу на адресу шлюзу, то комутатор, відразу помітить невідповідність IP і MAC адреси і відключить порт.

Повернути порт в активний стан можна або вручну командами shut і no shut, або скористатися функцією errdisable recovery cause arp-inspection, яка включить порт через 300 секунд. Для зміни інтервалу часу можна скористатися командою errdisable recovery interval 60, де 60 – час в секундах. Нижче наведено приклад налаштування комутатора:

```
Switch0 (config)#arp access-list GW
Switch0(config-arp-nacl)#permit ip host 192.168.2.254 mac host
0033.22a3.fa12
Switch0(config-arp-nacl)#exit
Switch0(config)#ip arp inspection filter GW vlan 10 static
Switch0(config)#errdisable recovery cause arp-inspection
Switch0(config)#errdisable recovery interval 60
```

4.4 Організація захисту проти атак на протокол STP

Як відомо, STP (Spanning Tree Protocol) – це протокол, призначений для запобігання зациклення пакетів в мережі, при наявності дублюючих маршрутів. Що може зробити атакуючий? Атакуючий може також «прикинутися» комутатором, направити в сторону комутатора BPDU-пакет, в якому він може підробити пріоритет, MAC-адресу, для того щоб стати «кореневим комутатором» і з його допомогою перехопити мережевий трафік.

Кореневим комутатором стає той, у якого найвищий пріоритет. Якщо пріоритет у кількох комутаторів однаковий, то для вибору кореневого комутатора використовується MAC-адреса, у якій він менше, той і стає кореневим.

Постараємося позбутися цієї уразливості. Для цього необхідно:

- Заборонити ходіння BPDU-пакетів з портів, в яких ми точно знаємо, що там немає ніяких комутаторів. І в разі якщо такий пакет все ж прийшов, переводити цей порт в shutdown.
- Захистити кореневий комутатор, щоб ні за яких умов не міг бути обраний інший кореневої комутатор, в тому числі і наш атакуючий (атакуючому не важко поставити пріоритет краще, ніж у справжнього

головного комутатора, і MAC-адресу поменше, що буде гарантувати, що атакуючий представляється root).

Перейдемо до реалізації даної ідеї безпосередньо на комутаторі (рис. 4.6).

Для початку на всіх портах доступу поставимо спеціальний режим STP, який називається portfast. Після цього клієнт, підключений до порту, не братиме участі в дозволі маршрутів по алгоритму STP, і дані будуть передаватися йому відразу. Якщо дана опція включена не буде, то спочатку підключений клієнт ініціює перерахунок маршрутів за алгоритмом STP (це може зайняти досить багато часу, десятки секунд і навіть більше), і лише після того починатимуть передаватися призначені для користувача дані через порт.

За замовчуванням portfast на Cisco Catalyst відключений, і це потрібно буде настроїти вручну.

Будемо конфігурувати Portfast на портах f0/1 і f0/2.

Switch0 # conf t

Switch0 (config) #int range f0 / 1 - 2

Switch0 (config-if-range) # spanning-tree portfast

Далі вкажемо, що на цих портах ходіння BPDU-пакетів протипоказано, для цього в режимі глобальної конфігурації необхідно зробити наступне:

Switch0 (config) # spanning-tree portfast bpduguard default

Тепер при появі на портах, на яких вказано режим STP portfast, BPDU-пакета, порт буде відключатися, тобто переходити в режим shutdown.

І останнє, необхідно убезпечити Root Bridge. Для цього необхідно перейти в конфігурацію інтерфейсу, до якого підключений інший комутатор, і зробити наступне:

Switch0 (config) # int f0 / 4

Switch0 (config-if) spanning-tree guard root

Тепер, у разі якщо з'явиться зловмисник і направить в сторону комутатора пакет BPDU з максимальним пріоритетом і меншим MAC-адресою, це не дозволить стати йому «кореневим комутатором».

ВИСНОВКИ

У дипломній роботі розглянуті основні проблеми, пов'язані з безпекою мереж на канальному рівні моделі OSI. Проаналізовано різні типи атак на локальні комп'ютерні мережі, а також сучасні методи їх виявлення і попередження. Запропоновано найбільш перспективні напрямки розвитку систем виявлення вторгнень, засновані на використанні вбудованих функцій безпеки комутаторів Cisco Catalyst.

В ході роботи були змодельовані найбільш прості, але ефективні типи атак:

1) arp-spoofing;
2) dhcp-spoofing;
3) виснаження DHCP;
4) MAC-flooding.

Без використання вбудованих функцій безпеки комутаторів все атаки, при невеликих витратах часу, дозволили домогтися бажаного ефекту (відмова в обслуговуванні/перехоплення інформації). Після детальної настройки захисних функцій атаки виявилися абсолютно неефективними.

Окремі сценарії мережевих атак, а також механізми їх виявлення були реалізовані програмно за допомогою засобів мережевого емулятора Cisco Packet Tracer 5.3.2.

Створені в ході роботи конфігураційні файли і сценарії атак дозволяють наочно продемонструвати вразливість в мережі Ethernet і методи їх нейтралізації. Отримані дані планується використовувати при підготовці лабораторних робіт курсу «Комп'ютерні мережі».

ПЕРЕЛІК ПОСИЛАНЬ

1. Біячуєв Т.А. Безпека корпоративних мереж./ під ред. Л.Г.Осовецкого – СПб: СПб ГУ ІТМО, 2004.– 161 с.

2. Computer Security Journal vol. XIV, #1 2. Лапоніна О.Р . Intrusion Detection Systems (IDS). 2006г. [Електроний ресурс]. Режим доступу: http://citforum.ru/security/internet/firewalls_ids/2.shtml

3. Абрамов Е.С. Построение адаптивной системы информационной безопасности // «Известия ЮФУ. Технические науки». Тематический выпуск «Информационная безопасность». - Таганрог: Изд-во ТТИ ЮФУ, 2011. – №12 (125). – С. 99-109.

4. Wikipedia. Address Resolution Protocol [Електроний ресурс]. Режим доступу: http://en.wikipedia.org/wiki/Address_Resolution_Protocol.

5. Чубин И. ARP-spoofing [Електроний ресурс]. Режим доступу: http://xgu.ru/wiki/ARP-spoofing

6. MAC-spoofing [Електроний ресурс]. Режим доступу: http://xgu.ru/wiki/MAC-spoofing.

7. Wikipedia. Spanning Tree Protocol [Електроний ресурс]. Режим доступу: http://ru.wikipedia.org/wiki/STP

8. Половко И.Ю. Методы тестирования эффективности сетевых СОА // «Известия ЮФУ. Технические науки». Тематический выпуск «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ, 2009. – №11 (100). – С. 110-116.

9. Брюс Александер, Тони Аллен, Матт Карлинг и др. Руководство по технологиям объединенных сетей Cisco. Изд. 4-е. – М.: Издательский дом «Вильямс», 2005. – 1040 с.: ил.

10. Официальный сайт Cisco Systems. Программа Cisco Packet Tracer [Електроний ресурс]. Режим доступу: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html.

11. Джеймс Бони. Руководство по Cisco IOS. – СПб.: Питер, М: Издательство «Русская редакция», 2008. – 784 с.: ил.

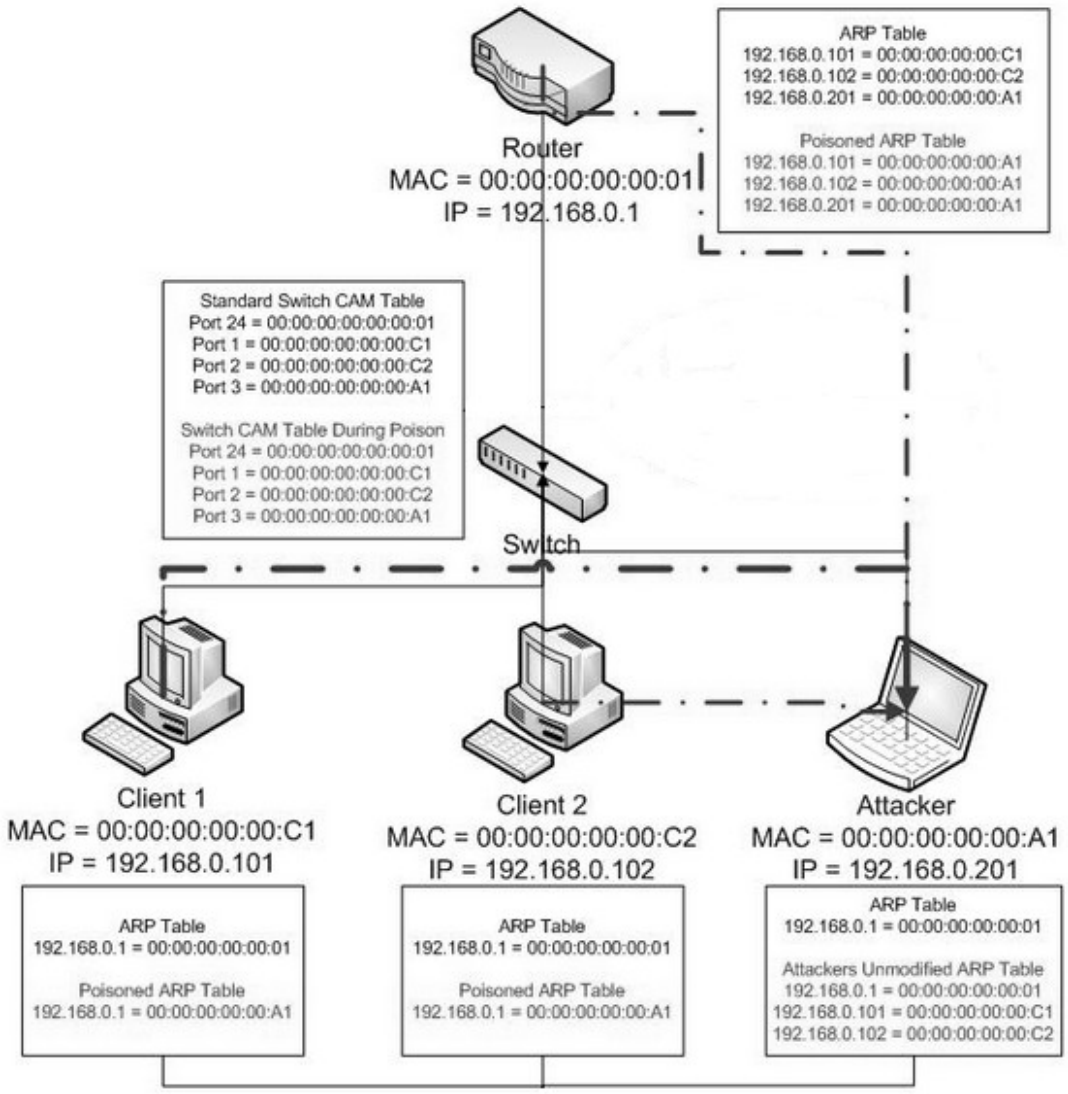
Д О Д А Т К И

Додаток А

Діаграма класифікації мережевих атак

Додаток Б

Схема проведення атаки ARP-spoofing



Додаток В

Алгоритм роботи комутатора з встановленими функціями захисту