Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

АТЕСТАЦІЙНА РОБОТА

Пояснювальна записка

рівень вищої освіти другий (магістерський)

Метод верифікації DHCP сервера в мережі підприємства
(тема)

Виконав: Сапанович С.Б.
(прізвище, ініціали)
студент 2 курсу, групи БІКСм-18-1
Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Безпека інформаційних і комунікаційних систем»
(повна назва освітньої програми)

Керівник проф. Халімов Г.З.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри БІТ _____ Халімов Г. З.
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління

Кафедра Безпеки інформаційних технологій

Рівень вищої освіти Другий (магістерський)

Спеціальність (напрям) 125 Кібербезпека
(код і назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека інформаційних і комунікаційних систем»

(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)

"____" _____ 20__ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студентові Сапановичу Сергію Борисовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Метод верифікації DHCP сервера в мережі підприємства

затверджена наказом по університету від " 04 " листопада 2019 р. № 1649Ст

2. Термін подання студентом роботи до екзаменаційної комісії

3. Вхідні дані до роботи RFC 2460, RFC 4443, RFC 4861, RFC 4429.

4. Перелік питань, що потрібно опрацювати в роботі:

1. Проаналізувати мережні атаки
2. Розробити рекомендації, що до захисту DHCP сервера
3. Реалізація механізмів захисту від мережних атак

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) слайди презентації

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Визначення структури магістерської	*9.09.18-9.03.19*	
	атестаційної роботи, вивчення літератури,		
	пошук додаткової літератури, патентний		
2	Аналіз мережних атак на канальний рівень а	*10.03.19-25.06.19*	
3	Аналіз засобів захисту від мережних атак	*26.06.19-15.07.19*	
4	Розробка налаштувань мережного обладнаня	*16.07.19-8.08.19*	
	для захисту DHCP		
5	Реалізація механізмів захисту від	*9.08.19-31.10.19*	
	мережних атак		

Дата видачі завдання 4 вересня 2018 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Халімов Г.З.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка атестаційної роботи: 63 с., 10 рис., 22 джерел.

СПИСОК ДОСТУПУ, ПРАВИЛО ДОСТУПУ, ПОЛІТИКА БЕЗПЕКИ, ВРАЗЛИВІСТІ, МЕРЕЖА.

Метою атестаційної роботи є розробка методу захисту DHCP сервера на основі правил доступу мережного обладнання.

Областю дослідження в даній роботі було обрано тематику налаштувань мережного обладнання з урахуванням найкращих практик сформульованих CISCO.

Результатом роботи є сформульований перелік правил та політик, що мають бути активовано на мережевому обладнанні а також програмний засіб, що проводить автоматизовано перешрку налаштувань мережного обладнання на предмет відповідості зазначеним правилам.

Проведено тестування розробленого поітики доступу на віртуальному маршрутизаторі CISCO.

ABSTRACT

Master’s thesis: 63 pages, 10 figures, , 22 sources.

LIST OF ACCESS, ACCESS RULES, SECURITY POLICY, VULNERABILITIES, NETWORK.

The purpose of certification is to develop a method of protecting a DHCP server based on access rules for network equipment.

The area of study in this paper was the topic of network equipment settings based on the best practices formulated by CISCO.

The result of the work is a formulated list of rules and policies that must be activated on the network equipment, as well as a software tool that automates the reconfiguration of network equipment settings to ensure compliance with these rules.

Testing of the developed access policy on the CISCO virtual router is carried out.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

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

ПЗ – програмне забезпечення.

IDS – Intrusion detection systems

IPS – Intrusion prevention systems

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

DoS – (англ. «Denial of Service») атака Відмова у доступі.

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

DHCP (англ. *Dynamic Host Configuration Protocol* — протокол динамічної конфігурації вузла)

Доме́нна систе́ма име́н (англ. Domain Name System, DNS) — ієрархічна розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу.

ICMP (англ. Internet Control Message Protocol — міжмережевий протокол керуючих повідомлень) — мережевий протокол, що входить в стек протоколів TCP/IP.

ВСТУП

Маршрутизатори були розроблені для передач дейтаграм до свого м1сця призначення і були програмовані схемамами рішення проблем, таких як затори або збій сегмента мережі. Ці схеми включають в себе зміну маршруту дейтаграм на альтернативний напрям. Тому неможливо стверджувати з будь-якою точністю - який шлях буде обраний дейтаграмою, мандруючою за межі локальної мережі.

Дейтаграмма може рухатися по прямому маршруту, або, швидше за все, подорожувати через кілька маршрутизаторів, розміщених в будь-яких куточках світу. Ці маршрутизатори, найімовірніше, не належать відправнику або одержувачу, а третій стороні. У більшості випадків це не має значення, однак дейтаграми можуть бути скопійовані, і їх безпека може піддаватися ризику, коли вони подорожують через маршрутизатор, без повідомлення відправника або одержувача.

З вище зазначеного можна зробити висновок, що коректні налаштування мережевого устаткування на пряму поліпшують стан захищенності системи обробки та передачі інформації.

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;

1 АНАЛІЗ МЕТОДІВ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ СИСТЕМ

1.1 Основи мережної безпеки

Мережева безпека - це не мета, а процес! [1] Колесо безпеки Cisco (Cisco Security Wheel) добре описує еволюцію системи безпеки рис. 1.1.

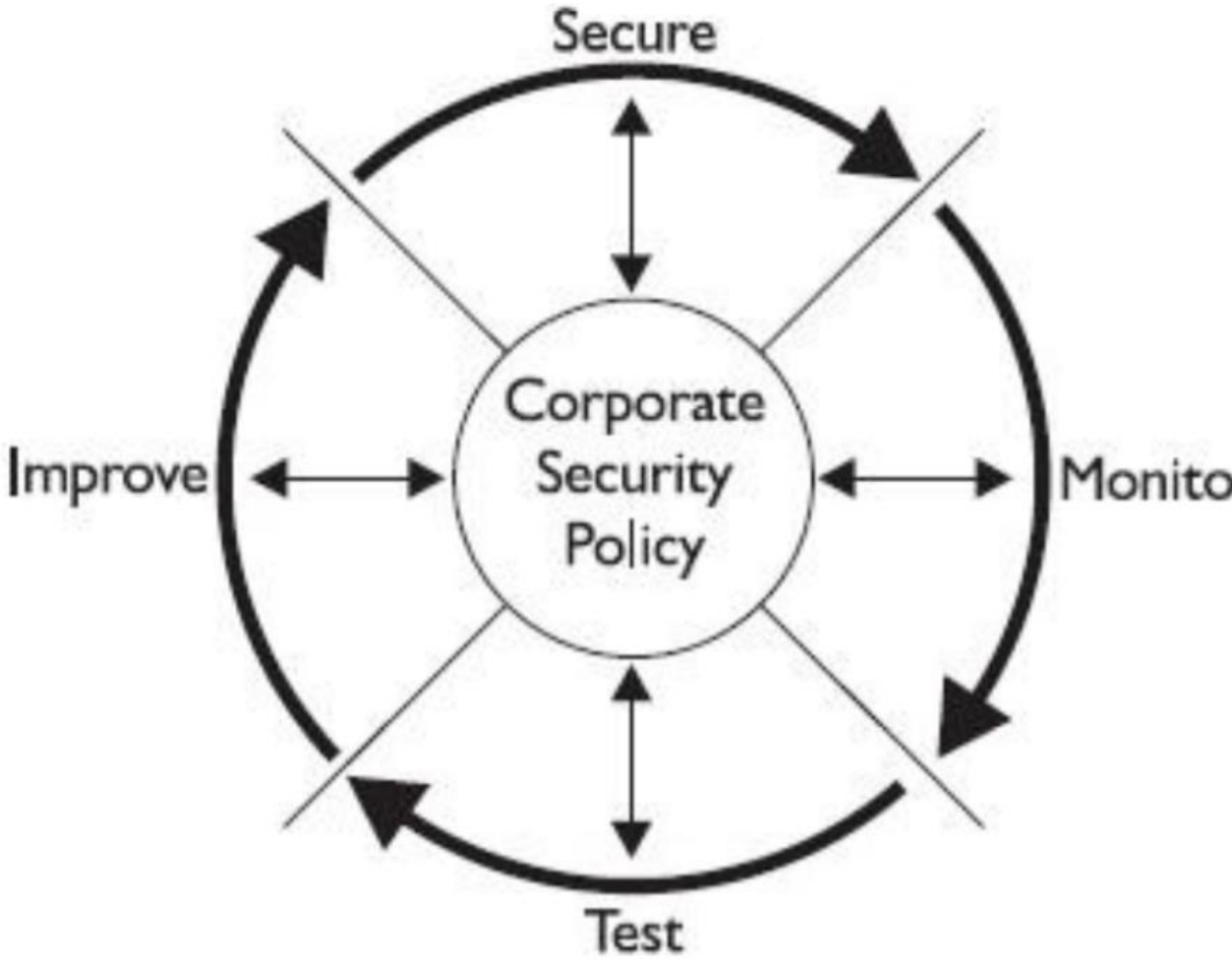

Рисунок 1.1 – Cisco Security Wheel

В основі даного подання лежить корпоративна політика безпеки (Corporate Security Policy), на яку спираються чотири складові: Secure (Забезпечення безпеки), Monitor (Моніторинг), Test (Перевірка), Improve

(Поліпшення системи)

Згідно матеріалам [2], перш ніж проектувати реальну схему захисту мережі, слід виробити адекватну політику безпеки, яка визначає ряд моментів:

1) план придбань і реалізацій, щодо забезпечення безпеки;

2) допустимі і заборонені технології;

3) план дій на випадок інцидентів;

4) допустиму поведінку персоналу;

5) санкції на порушення;

6) ієрархію відповідальності за реалізацію, підтримку, аудит, моніторинг;

7) напрямок подальшого розвитку системи безпеки.

Політика безпеки - це формальний виклад правил, яких повинні дотримуватимя особи, які отримують доступ до корпоративної технології та інформації [2], це затверджений документ, який є результатом компромісу між безпекою і простотою використання, безпекою та послугами, які надаються, і нарешті, між ціною системи і ризиками втрат [3].

Сам документ розбивається на частини – субполітики, які описують окремі елементи схеми безпеки, такі, наприклад, як:

1) віддалений доступ (Remote Access Policy);

2) аутентифікацію (Authentication Policy);

3) антивірусні засоби (Antivirus Policy);

4) парольная політика (Password Policy) та багато іншого.

Слід окремо згадати позицію компанії (організації) щодо підготовки персоналу. Наприклад, стаття «Кожен співробітник як брандмауер» [5] описує позиції компаній Cisco і SAP з даного питання, які витрачають не малих гроші на постійну перепідготовку та перевірку персоналу. Результатом таких дій є різке зниження успішності проведення соціальної інженерії, і посилення системи безпеки щодо внутрішніх загроз. Яка б якісна і дорога не була система, якщо персонал не дотримується правил, закріплені в політиці,

то вона марна.

Secure - реалізація спроектованих процесів і технологій, спрямованих на забезпечення безпеки.

Monitor - процеси і технології безпеки потребують моніторингу з метою оцінювання працездатності та ефективності системи безпеки, виявлення та фіксування порушень і вторгнень.

Test - фаза тестування включає перевірку процесів на адекватність, стійкість і передбачуваність. Завжди краще самому виявити слабкості в своїй системі безпеки, ніж дозволити це іншим.

Improve - розробка нового дизайну мережі, впровадження нових технологій, оновлення обладнання, його ПЗ і конфігурацій.

Об'єктами захисту є:

- устаткування - сервера, робочі станції, маршрутизатори, комутатори, IP-телефони і т.д;
- програмне забезпечення - наприклад, операційна система на сервері або робочої станції.
- дані, що представляють комерційну цінність для компанії.

Як би не старались, і скільки б коштів не вкладали, абсолютної безпеки домогтися неможливо. Безпека і доступність - в асимптотиці речі назад пропорційні. Завжди є причини, що викликають труднощі в захисті. Їх можна класифікувати на 3 групи.

Технологічні вразливості - спочатку TCP/IP спроектували без урахування будь-яких вимог щодо безпеки. Всі операційні системи містять вразливі місця, які постійно виявляються і усуваються. вразливість ОС несе загрозу ресурсів, якими вона управляє.

Слабкість політики безпеки - сюди можна віднести недолік моніторингу системи, відсутність плану відновлення в разі збою, або ж відсутність політики безпеки як такої.

Неправильне налаштування обладнання - використання паролів за замовчуванням або ж взагалі їх відсутність, залишення непотрібних послуг і

портів включеними.

1.2 Мережні атаки

1.2.1. Загрози

Загроза - це ризик втрати внаслідок настання ряду подій завдяки випадку або ж чиїхось навмисних дій.

Зняття ризиків втрат від випадковості здійснюється за допомогою надмірності схеми мережі. Надмірність досягається за рахунок додавання додаткового обладнання, що призводить до збільшення ціни проекту. Однак це неминуче, якщо хочемо домогтися високої надійності системи. Наприклад, може знадобитися забезпечити середній час між збоями (MTBF - mean time between fail) рівним 99.999% [6]. Це приблизно 1 годину простою на 11 років роботи.

Ризики втрат від чиїхось навмисних дій усувається застосуванням комплексного підходу до забезпечення безпеки корпоративної мережі.

Існує чотири основних типи загроз даної категорії:

- непідготовлені загрози (unstructured threats);
- підготовлені загрози (structured threats);
- внутрішні загрози (internal threats);
- зовнішні загрози (external threats);

Непідготовлені загрози реалізуються слабко кваліфікованими суб'єктами, з вельми обмеженими навичками і знаннями в області мережевої безпеки. Вони самі не створюють і не модифікують інструментів злому, а використовують чужі, готові продукти.

Підготовлені загрози здійснюються високо кваліфікованим, мотивованим хакером або ж групою осіб. Всі їх атаки добре сплановані і ведуться не в сліпу, а за цілком конкретних точок цільової мережі. Вони можуть самі створювати і модифікувати існуючі інструменти злому.

Основою внутрішніх загроз є особа, яка має доступ до ресурсів

організації, тобто є внутрішнім резидентом компанії. Якщо до всього іншого він вступить у змову з зовнішньої професійною групою, то ми отримаємо підготовлену внутрішню загрозу, захиститися від якої вкрай складно, так як практично неможливо уникнути втрат. [1] Їх ступінь буде визначатися рівнем доступу службовця до ресурсів.

Зовнішня загроза виходить від осіб, які перебувають поза периметром оборони (може бути як підготовленої, так і немає).

Метою мережевої атаки може бути:

- розвідка (reconnaissance attack);
- отримання доступу (access attack);
- відмова в обслуговуванні (DoS attack);
- маніпуляція даними (data manipulation attack).

В загальному доступі знаходиться безліч програм - інструментів злому. Так, наприклад, будь-хто може дістати собі такі відомі утиліти підбору паролів як L0pht 7 Crack, PWLVIEW, Pwlhack, PWL_Key, ntPassword; або ж утиліти розвідки: NMAP, SATAN, Portscanner, Strobe. Їх можна використовувати і в творчих цілях - перевірка якості пароля або виявлення недоліків конфігурації апаратури і ПЗ (наприклад, не відключений SNMP там, де не передбачається його використовувати).

1.2.2. Класифікація мережних атак і методи протидії та захисту.

Сніффер пакетів є прикладна програма, яка використовує мережну карту, що працює в режимі promiscuous mode (в цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додатком для обробки). При цьому сниффер перехоплює всі мережні пакети, які передаються через певний сегмент. В даний час сніфери працюють в мережах на цілком законній підставі. Вони використовуються для діагностики несправностей і аналізу трафіку. Однак з огляду на те, що деякі мережні додатки передають дані в текстовому форматі (Telnet, FTP, SMTP, POP3 і т.д.), за допомогою сніффер можна дізнатися корисну, а іноді і конфіденційну інформацію (наприклад, імена користувачів і паролі).

Перехоплення імен і паролів створює велику небезпеку, так як користувачі часто застосовують один і той же логін і пароль для безлічі додатків і систем. Багато користувачів взагалі мають один пароль для доступу до всіх ресурсів і додатків. Якщо додаток працює в режимі клієнт/сервер, а аутентифікаційні дані передаються по мережі в читається текстовому форматі, цю інформацію з великою ймовірністю можна використовувати для доступу до інших корпоративних або зовнішніх ресурсів.

Пом'якшити загрозу сніффінга пакетів можна за допомогою таких засобів:

Аутентифікація. Сильні засоби аутентифікації є першим способом захисту від сніффінга пакетів. Прикладом є одноразові паролі (OTP - One-Time Passwords). OTP - це технологія двофакторної аутентифікації, при якій відбувається поєднання того, що у вас є, з тим, що ви знаєте. Типовим прикладом двофакторної аутентифікації є робота звичайного банкомату, який пізнає вас, по-перше, по вашій пластиковій картці і, по-друге, по вводиться вами ПІН-коду. Для аутентифікації в системі OTP також потрібно ПІН-код і ваша особиста картка. Під «карткою» (token) розуміється апаратне або програмне засіб, що генерує (за випадковим принципом) унікальний одномоментний одноразовий пароль. Якщо хакер дізнається цей пароль за допомогою сніффер, ця інформація буде марною, тому що в цей момент пароль вже буде використаний і виведений з ужитку. Зауважимо, що цей спосіб боротьби зі сніффінгом ефективний тільки для запобігання перехоплення паролів. Сніффери, перехоплюючі іншу інформацію (наприклад, повідомлення електронної пошти), не втрачають своєї ефективності.

Інфраструктура що коммутується. Ще одни спосіб боротьби зі сніффінгом пакетів у мережному середовищі є створення комутованої інфраструктури. Якщо, наприклад, у всій організації використовується комутований Ethernet, хакери можуть отримати доступ тільки до трафіку, що надходить на той порт, до якого вони підключені (результат

микросегментации виробленої комутатором). Однак, як можна побачимо пізніше, існують методи, що дозволяють обійти це обмеження (ARP-злом, CAM переповнення).

Анти-сніфери. Третій спосіб боротьби зі сніффінгом полягає в установці апаратних або програмних засобів, які розпізнають сніфери, що працюють у вашій мережі. Ці кошти не можуть повністю ліквідувати загрозу, але, як і багато інших засобів мережевої безпеки, вони включаються в загальну систему захисту. Так звані «антісніффери» вимірюють час реагування хостів і визначають, чи не доводиться хостам обробляти «зайвий» трафік. Одне з таких засобів, що поставляються компанією L0pht Heavy Industries, називається AntiSniff.

Криптографія - найефективніший спосіб боротьби зі сніффінгом пакетів. Вона робить роботу сніфферов марною. Криптографія Cisco на мережевому рівні базується на протоколі IPSec. IPSec є стандартний метод захищеного зв'язку між пристроями за допомогою протоколу IP. До іншим криптографічним протоколам мережевого управління відносяться протоколи SSH (Secure Shell) і SSL (Secure Socket Layer).

IP-спуфинг відбувається, коли хакер, що знаходиться всередині корпорації або поза нею, видає себе за санкціонованого користувача. Це можна зробити двома способами. Поперше, хакер може скористатися IP-адресою, що знаходиться в межах діапазону санкціонованих IP-адрес, або вповноваженим зовнішнім адресою, якому дозволяється доступ до певних мережевих ресурсів. Атаки IP-спуфінга часто є відправною точкою для інших атак. Класичний приклад - атака DoS, яка починається з чужого адреси, що приховує справжню особистість хакера. Зазвичай IP-спуфінга обмежується вставкою помилкової інформації або шкідливих команд у звичайний потік даних, переданих між клієнтським і серверним додатком. Для двостороннього зв'язку хакер повинен змінити все таблиці маршрутизації, щоб направити трафік на помилковий IP-адреса. Якщо йому це вдається, він отримає все пакети і зможе відповідати на них так, ніби він є санкціонованим

користувачем

Загрозу спуфинга можна послабити (але не усунути) за допомогою таких заходів:

Контроль доступу - найпростіший спосіб запобігання IP-спуфинга. Він полягає в правильному підборі управління доступом. Щоб знизити ефективність IP-спуфинга, необхідно відсікти будь-який трафік, що надходить із зовнішнього мережі з вихідним адресою, який повинен розташовуватися всередині нашої мережі. Якщо ж санкціонованими є і деякі адреси зовнішньої мережі, даний метод стає неефективним.

Фільтрація RFC 2827. Можемо припинити спроби спуфинга чужих мереж користувачами нашої мережі. Для цього необхідно блокувати будь-який вихідний трафік, адреса джерела якого не є одним з IP-адрес нашої організації. Цей тип фільтрації, відомий під назвою «RFC 2827», може виконувати і провайдер (ISP). До тих пір, поки всі провайдери не впровадять цей тип фільтрації, його ефективність буде набагато нижче можливою.

Аутентифікація. IP-спуфинг може функціонувати тільки за умови, що аутентифікація відбувається на базі IP-адрес. Тому впровадження додаткових методів аутентифікації робить цей вид атак марним.

DoS є найбільш відомою формою хакерських атак. Вони прості в реалізації і можуть завдати величезної шкоди. Крім того, проти атак такого типу найважче створити гарантований захист. Типи DoS атак:

- TCP SYN Flood;
- Ping of Death;
- Tribe Flood Network (TFN) і Tribe Flood Network 2000 (TFN2K);
- Trinco;
- Stacheldracht;
- Trinity.

Атаки DoS відрізняються від атак інших типів. Вони не націлені на отримання доступу до вашої мережі або на отримання з неї будь-якої інформації. Атака DoS робить вашу мережу недоступною для звичайного

використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми. У разі використання деяких серверних додатків (таких як web-сервер або FTP-сервер) атаки DoS можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих додатків, і тримати їх в зайнятому стані, не допускаючи обслуговування звичайних користувачів. В ході атак DoS можуть використовуватися звичайні Інтернет-протоколи, такі як TCP і ICMP. Більшість атак DoS спирається не на програмні помилки або проломи в системі безпеки, а на загальні слабкості системної архітектури. Деякі атаки зводять до нуля продуктивність мережі, переповняючи її небажаними і непотрібними пакетами або повідомляючи помилкову інформацію про поточний стан мережевих ресурсів.

Існує два різновиди атак даного типу: DDoS (distributed denial of service) - розподілена відмова в обслуговуванні і DRDoS (distributed deflection denial of service) - розподілений відбитий відмову в обслуговуванні.

Атака типу DDoS починається з розстановки на різних комп'ютерах, мають високошвидкісне підключення до мережі, програм-ботів (Zombie), які координуються з єдиної машини (Zombie-master), яка ініціює атаку. Завдання ботів - здійснювати безперервну посилку пакетів (флуд) на цільової адресу (це може бути як окремий хост, так і точка виходу цілої мережі). Таким чином, здійснюється перекриття всієї доступної пропускної здатності (або заняття інших важливих ресурсів).

Відмінність атаки DRDoS від попередньої полягає в використанні в якості посередників між атакуючим і метою легальних TCP серверів. Джерело (або ж кілька джерел) посилає на них луна-запити (ping) або запити на TCP з'єднання з спуфнутим (підміненим) адресою джерела, в якості якого вказує адресу цілі. І відповіді від багатьох хостів приходять в єдину точку, поглинаючи всю пропускну здатність.

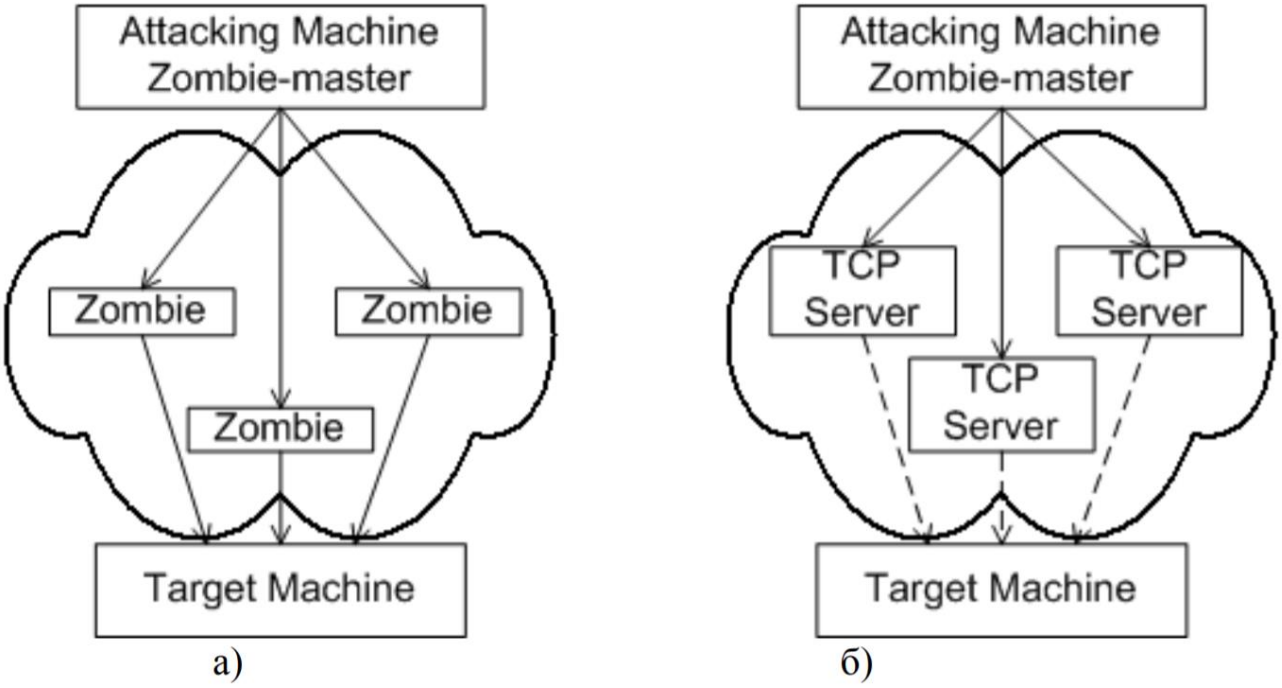

Рисунок 1.2 – Схема атак типу DoS, а) DDoS, б) DRDoS

Загроза атак типу DoS може знижуватися трьома способами:

Функції анти-спуфинга. Правильна конфігурація функцій анти-спуфинга на ваших маршрутизаторах і міжмережевих екранах допоможе знизити ризик DoS. Ці функції, як мінімум, повинні включати фільтрацію RFC 2827. Якщо хакер не зможе замаскувати свою справжню особистість, він навряд чи зважиться провести атаку.

Функції анти-DoS. Правильна конфігурація функцій анти-DoS на маршрутизаторах і міжмережевих екранах може обмежити ефективність атак. Ці функції часто обмежують число напіввідкритих каналів в будь-який момент часу.

Обмеження обсягу трафіку (traffic rate limiting). Якщо трафік, призначений для переповнення вашої мережі, не зупинити у провайдера, то на вході в мережу ви це зробити вже не зможете, тому що вся смуга пропускання буде зайнята. Типовим прикладом є обмеження обсягів трафіку ICMP. При укладанні договору з провайдером на надання послуг (SLA - service level agreement), слід обговорити застосування технології обмеження

доступу (CAR - committed access rate). [7]

Хакери можуть проводити парольні атаки за допомогою цілого ряду методів, таких як простий перебір (brute force attack), «троянський кінь», IP-спуфинг і сніффінг пакетів. Якщо зловмисник, перехопивши пароль, здобуде привілейований доступ, він може створити для себе «прохід», який буде діяти, навіть якщо користувач змінить вже розкритий пароль і логін.

Перш за все, пральних атак можна уникнути, якщо не користуватися паролями в текстовій формі. Одноразові паролі і / або криптографічний аутентифікація можуть практично звести нанівець загрозу таких атак. На жаль, не всі програми, хости і пристрої підтримують зазначені вище методи аутентифікації. При використанні звичайних паролів слід придумати такий пароль, який було б важко підібрати. Мінімальна довжина пароля повинна бути не менше восьми символів. Пароль повинен включати символи верхнього регістру, цифри та спеціальні символи (#,%, $ і т.д.).

С точки зрения администратора, существует несколько методов борьбы с подбором паролей. Один из них заключается в использовании средства L0phtCrack, которое часто применяют хакеры для подбора паролей в среде Windows NT. Это средство быстро покажет вам, легко ли подобрать пароль, выбранный пользователем.

З точки зору адміністратора, існує кілька методів боротьби з підбором паролів. Один з них полягає у використанні засоби L0phtCrack, яке часто застосовують хакери для підбору паролів в середовищі Windows NT. Це засіб швидко покаже вам, чи легко підібрати пароль, вибраний користувачем.

Атаки на рівні додатків можуть проводитися кількома способами. Найпоширеніший з них полягає у використанні добре відомих слабкостей серверного програмного забезпечення (sendmail, HTTP, FTP). Використовуючи їх, хакери можуть отримати доступ до комп'ютера від імені користувача, що працює з додатком. Відомості про атаки на рівні додатків широко публікуються, щоб дати можливість адміністраторам виправити проблему за допомогою корекційних модулів (патчів). На жаль, багато

хакерів також мають доступ до цих відомостей, що дозволяє їм вчитися.

Головна проблема з атаками на рівні додатків полягає в тому, що вони часто користуються портами, за якими дозволено прохід через міжмережевий екран. Наприклад, хакер, який експлуатує відому слабкість web-сервера, часто використовує в ході атаки TCP порт 80. Оскільки web-сервер надає користувачам web-сторінки, міжмережевий екран повинен надавати доступ до цього порту. З точки зору брандмауера, атака розглядається як стандартний трафік.

Повністю виключити атаки на рівні додатків неможливо. Хакери постійно відкривають і публікують в Інтернет все нові вразливі місця прикладних програм. Найголовніше тут - гарне системне адміністрування. Ось деякі заходи, які можна зробити, щоб знизити вразливість від атак цього типу:

1) Читання лог-файлів операційних систем і мережевих лог-файлів, їх аналіз за допомогою спеціальних програм.

2) Оформлення підписки на послуги з розсилки даних про слабкі місця прикладних програм: Bugtrad (http://www.securityfocus.com) і CERT (http://www.cert.com).

3) Використання найсвіжіших версій операційних систем і додатків і найостанніших корекційних модулів (патчів).

4) Використання програмно-апаратних систем розпізнавання атак (IDS)

Мережевою розвідкою називають збір інфрмації про мережу за допомги загальнодоступних даних і програм. При підготовці атаки проти якої-небудь мережі хакер, як правило, намагається отримати про неї якомога більше інформації. Маережева розвідка проводиться в формі запитів DNS, эхо-тестування (ping sweep) и сканування портів. Запити DNS дають змогу зрозуміти, хто володіє тим чи іншим доменом та які адреси цьому домену присвоєні. Эхо-тестування (ping sweep) адрес, відкритих за домоги DNS, дає змогу побачити, які хости реально працюють в даному середовищі. Отримав список хостів, хакер використовує засоби сканування портів, щоб скласти

повний список послуг, підтримуваних цими хостами. І, нарешті, хакер аналізує характеристики додатків, працюючих на хостах. В результаті отриманої информації, яку можна використовувати для взлому.

Повністю позбавитися від мережевої розвідки неможливо. Якщо, на приклад, відключити ICMP на периферійных маршрутизаторах, вы позбавитесь від эхо-тестування, але втратите данні, необхідні для аналізу мережевих збоїв. Крім того, сканувати порти можна і без попереднього эхо-тестування. Просто це займе більше часу, так як сканувати доведеться і не існуючі IP-адреси. Системи IDS на рівні мережі та хостів зазвичай добре справляються с завданням інформування адміністратора мережеву розвідку, що ведеться, що дає змогу підготуватися до майбутньої атаки та інформувати провайдера (ISP), в мережі якої встановлена система, яка проявляє забагато зацікавленості.

Власне кажучи, цей тип дій не є «атакою» або «штурмом». Він являє собою зловмисне використання відносин довіри, існуючих в мережі.

Класичним є ситуація в периферійній частині корпоративної мережі. У цьому сегменті часто розташовуються сервери DNS, SMTP і HTTP. Оскільки всі вони належать до одного і того ж сегменту, злом одного з них призводить до злому і всіх інших, так як ці сервери довіряють іншим системам своєї мережі.

Іншим прикладом є система, встановлена з зовнішнього боку брандмауера, що має відношення довіри з системою, встановленою з його внутрішньої сторони. У разі злому зовнішньої системи хакер може використовувати відносини довіри для проникнення в систему, захищену брандмауером.

Ризик зловживання довірою можна знизити за рахунок більш жорсткого контролю рівнів довіри в межах своєї мережі. Системи, розташовані з зовнішньої сторони брандмауера, ніколи не повинні користуватися абсолютною довірою з боку захищених екраном систем [8]. Відносини довіри повинні обмежуватися певними протоколами і, по

можливості, аутентифицироваться не тільки по IP-адресу, але і за іншими параметрами.

1.2.3 Атаки на другому рівні.

До атак на 2-му рівні відносить сніффінг пакетів. Це мета, а ось способів її досягнення - кілька.

Багато системні адміністратори вважають, що підключення сервера через комутатор є панацеєю від перехоплення мережевого трафіку. Однак це не так. Існує ряд програм - активних сніфферов, здатних реалізовувати такий злом.

Активний сниффер (наприклад, angst) здатний працювати в двох режимах. Перший з них називається man-in-the-middle. Після старту програма починає моніторити адреси arpзапросов, а потім включає arp forwanding на станції, де вона запущена, посилаючи на arpзапрос відповідь, що mac-адресу псевдофорвардера відповідає всім ip-адресами в даній мережі.

Для своєї роботи комутатор динамічно будує таблицю відповідності MAC - порт. Другий метод полягає в наповненні мережі помилковими (спуфнутимі) MAC адресами, CAMпамять комутатора переповниться і він переходить в режим роботи «концентратор» (hub). Ефект микросегментации усувається, і сниффер починає слухати весь трафік на своєму порту.

Шляхом підключення пристрою з низьким пріоритетом або за допомогою інструменту генерації пакетів STP (BPDU - bridge protocol data unit) можна частково або повністю перевести на себе весь трафік VLAN і успішно його аналізувати. Якщо зловмисник має доступ до 2-ум портам на різних комутаторах, видаючи себе за корінь дерева STP, він отримує трафік віртуальної локальної мережі.

Якщо через невеликі проміжки часу хакер буде міняти пріоритет, змушуючи протокол постійно перераховувати дерево, вийде атака типу DoS.

Для захисту від STP-злому компанія Cisco доповнила ПО для комутаторів парою опцій:

- захист порту - заборона порту приймати BPDU (bpdu filter);

- захист кореня - заборона перебування за даними портом кореня.

Зловмисник в більшості випадків зможе підключитися лише до портів доступу комутатора. Дані заходи повністю блокують його від будь-яких впливів на STP.

Протокол HSRP (Hot Standby Router Protocol) реалізує надлишкову експлуатацію декількох маршрутизаторів, доступних під одним віртуальним IP і MAC. Між собою маршрутизаториобмінюються багатоадресними (multicast) пакетами (224.0.0.2). На основі пріоритету визначається активний, відповідальний за обробку та передачу всього трафіку.

Якщо порушник може розсилати HSRP-пакети з найбільшим пріоритетом, він здатний:

- перевести всі маршрутизатори в неактивний стан, реалізуючи таким чином атаку типу DoS;
- перевести на себе весь трафік;

Для захисту рекомендується використовувати протокол IPSec для шифрування трафіку HSRP. А в версіях IOS 12.3 (2) T і новіше застосовувати MD5 аутентифікацію.

Найбільш відомим інструментом атаки на HSRP і STP є Irpas.

Зазвичай адміністратори вручну конфігурують все транкові порти. Однак цей процес можна автоматизувати застосуванням DTP. Комутатори самі визначатимуть, що за пристрої підключені до портів і, при необхідності, переводити його в режим магістралі.

Процес налаштування параметрів віртуальних локальних мереж можна автоматизувати застосуванням VTP. Тоді, налаштувавши VLAN на VTP-сервері, на клієнтах цього робити вже не доведеться.

За замовчуванням DTP знаходиться в режимі «активований». Таким чином, підключаючись до порту доступу, хакер заволодіває Транки. Він здатний здійснювати:

- читання широковещательного і многоадресного трафіку всіх віртуальних локальних мереж (в тому числі, протоколів

маршрутизації OSPF і EIGRP);

- участь в VTP, зміна налаштувань VLAN;
- спуфинг ARP.

Для захисту необхідно не забувати змінювати налаштування за замовчуванням, блокувати режим магістралі на портах доступу.

1.3 Системи мережного захисту

Системи виявлення вторгнення (СВВ) - це системи, які збирають інформацію з різних точок комп'ютерної системи (обчислювальної мережі) і аналізують цю інформацію для виявлення як спроб порушення, так і реальних порушень захисту (вторгнень). До недавнього часу найбільш поширеною структурою СВВ була модель, запропонована Дороті Деннінг (D. Denning) [3].

У сучасних системах виявлення логічно виділяють наступні основні елементи: підсистему збору інформації, підсистему аналізу і модуль представлення даних [2].

Підсистема збору інформації використовується для збору первинної інформації про роботу системи.

Підсистема аналізу (виявлення) здійснює пошук атак і вторгнень в систему.

Підсистема подання даних (призначений для користувача інтерфейс) дозволяє користувачеві) СВВ стежити за станом системи.

Підсистема збору інформації акумулює дані про роботу системи. Для збору інформації використовуються автономні модулі - датчики. Кількість датчиків різна і залежить від специфіки системи. Датчики в СВВ прийнято класифікувати за характером інформації, що збирається. Відповідно до загальної структурою інформаційних систем виділяють наступні типи:

- датчики додатків - дані про роботу програмного забезпечення, що працює в системі;

- датчики хоста - функціонування робочої станції системи;
- датчики мережі - збір даних для оцінки мережного трафіку;
- міжмережеві датчики - містять характеристики даних, що циркулюють між мережами.

Система виявлення вторгнення може включати будь-яку комбінацію з наведених типів датчиків.

Підсистема аналізу структурно складається з одного або більше модулів аналізу - аналізаторів. Наявність декількох аналізаторів потрібна для підвищення ефективності виявлення. Кожен аналізатор виконує пошук атак або вторгнень певного типу. Вхідними даними для аналізатора є інформація з підсистеми збору інформації або від іншого аналізатора. Результат роботи підсистеми - індикація про стан системи. У разі, коли аналізатор повідомляє про виявлення несанкціонованих дій, на його виході може з'являтися деяка додаткова інформація. Зазвичай ця інформація містить висновки, що підтверджують факт наявності вторгнення або атаки.

Підсистема подання даних необхідна для інформування зацікавлених осіб про стан системи. У деяких системах передбачається наявність груп користувачів, кожна з яких контролює певні підсистеми системи. Тому в таких СВВ застосовується розмежування доступу, групові політики, повноваження та інше.

Серед методів, використовуваних в підсистемі аналізу сучасних СВВ, можна виділити два напрямки: одне спрямоване на виявлення аномалій в системі, а інше - на пошук зловживань [2]. Кожне з цих напрямків має свої переваги і недоліки, тому в більшості існуючих СВВ застосовуються комбіновані рішення, засновані на синтезі відповідних методів. Ідея методів, використовуваних для виявлення аномалій, полягає в тому, щоб розпізнати, чи є процес, що викликав зміни в роботі системи, діями зловмисника. Методи пошуку аномалій наведені в таблицях 1.1 і 1.2.

Таблиця 1.1 - Виявлення аномалії - контрольоване навчання («навчання з учителем»)

Методи виявлення	Використовується в системах	Опис методу
моделювання правил	W&S	Система виявлення протягом процесу навчання формує набір правил, що описують нормальну поведінку системи. На стадії пошуку несанкціонованих дій система застосовує отримані правила і в разі недостатнього відповідності сигналізує про виявлення аномалії.
описова статистика	IDES, NIDES, EMERLAND, JiNao, HayStack	Навчання полягає в зборі простий описової статистики безлічі показників системи в спеціальну структуру. Для виявлення аномалій обчислюється «відстань» між двома векторами показників - поточними і збереженими значеннями. Стан в системі вважається аномальним, якщо отримане відстань досить велика.
Нейронні мережі	Hyperview	Структура нейронних мереж різна. Але у всіх випадках навчання виконується даними, що представляють нормальна поведінка системи. Отримана навчена нейронна мережа потім використовується для оцінки аномальність системи. Вихід нейронної мережі говорить про наявність аномалії.

Таблиця 1.2 - Виявлення аномалії - неконтрольоване навчання («навчання без учителя»)

Методи виявлення	Використовується в системах	Опис методу
Моделювання безлічі станів	DPEM, JANUS, Bro	Нормальна поведінка системи описується в вигляді набору фіксованих станів і переходів між ними. Де стан є не що інше як вектор певних значень параметрів вимірювань системи.
Описова статистика	MIDAS, NADIR, Haystack, NSM	Аналогічний відповідного методу в контролюючих

Реалізовані в даний час в СВВ методи засновані на загальних уявленнях теорії розпізнавання образів. Відповідно до них для виявлення аномалії на основі експертної оцінки формується образ нормального функціонування інформаційної системи. Цей образ виступає як сукупність значень параметрів оцінки. Його зміна вважається проявом аномального функціонування системи. Після виявлення аномалії і оцінки її ступеня формується судження про природу змін: чи є вони наслідком вторгнення або допустимим відхиленням. Для виявлення зловживань також використовується образ (сигнатура), однак тут він відображає заздалегідь відомі дії атакуючого.

Методи виявлення аномалій спрямовані на виявлення невідомих атак і вторгнень. Для системи СВВ на основі сукупності параметрів оцінки формується «образ» нормального функціонування. В сучасних СВВ виділяють кілька способів побудови «образу»:

- накопичення найбільш характерною статистичної інформації для кожного параметра оцінки;

- навчання нейронних мереж значеннями параметрів оцінки;
- уявлення про події.

Легко помітити, що у виявленні дуже значну роль відіграє множина параметрів оцінки. Тому в виявленні аномалій одним із головних завдань є вибір оптимального безлічі параметрів оцінки.

Інший, не менш важливим завданням є визначення загального показника аномальності. Складність полягає в тому, що ця величина повинна характеризувати загальний стан «аномальність» в системі.

У теперішній час використовується евристичне визначення (вибір) множени параметрів вимірювань, системи що захищається, використання якого має дати найбільш ефективне і точне розпізнавання вторгнень. Складність вибору множени можна пояснити тим, що складові його підмножини залежать від типів вторгнень, що виявляються. Тому одна і та ж сукупність параметрів не буде адекватною для всіх типів вторгнень.

Будь-яку систему, що складається зі звичних апаратних і програмних засобів, можна розглядати як унікальний комплекс зі своїми особливостями. Це є поясненням можливості пропуску специфічних для системи вторгнень тими СВВ, які використовують один і той же набір параметрів оцінки. Найбільш оптимальне рішення - визначення необхідних параметрів оцінки в процесі роботи. Труднощі ефективного динамічного формування параметрів оцінки полягає в тому, що розмір області пошуку експоненціально залежить від потужності початкової множени. Якщо є початковий список з N параметрів, актуальних для передбачаються вторгнень, то кількість підмножин цього списку становить 2^N. Тому не представляється можливим використання алгоритмів перебору для знаходження оптимальної множени. Одне з можливих рішень - використання генетичного алгоритму.

Загальна оцінка аномальності повинна визначається з розрахунку множени параметрів оцінки. Якщо ця множена формується так, як було запропоновано в попередньому вище, то отримання єдиної оцінки є досить непростим завданням. Один з можливих методів - використання статистики

Байеса. Інший спосіб, який застосовується в NIDES, заснований на використанні коваріантних матриць.

Нехай A_1 .. A_n - n вимірів, що використовувались для визначення факту вторгнення в будь-який момент часу. Кожне A_i оцінює різний аспект системи, наприклад – кількість активностей введення-виведення, кількість порушень пам'яті і т.д. Нехай кожний вимір A_i має два значення 1 – вимір аномальне, 0 – немає. Нехай I – це гіпотеза того, що в системі є процеси вторгнення. Достовірність і чутливість кожного виміру визначається показниками

$$P(A_i = 1 | I),\ P(A_i = 1 | -I) \tag{1.1}$$

Імовірність обчислюється за допомогою теореми Байеса.

$$P(I | A_1, A_1, ..., A_n) = P(I | A_1, A_1, ..., A_n | I) \frac{P(I)}{P(A_1, A_1, ..., A_n)} \tag{1.2}$$

Для подій I , швидше за все, буде потрібно обчислити умовну ймовірність для кожної можливої комбінації множени вимірів. Кількість необхідних умовних ймовірностей експоненціально по відношенню до кількості вимірювань. Для спрощення обчислень, але втрачаючи в точності, можемо припустити, що кожне вимір A_i залежить тільки від I і умовно не залежить від інших вимірів A_j де $i \neq j$. Це призведе до співвідношень

$$P(I | A_1, A_1, ..., A_n | I) = \prod_{i=1}^{n} P(A_i | I) \tag{1.3}$$

Тепер ми можемо визначити ймовірність вторгнення, використовуючи значення вимірювань аномалій, ймовірність вторгнення, отриману раніше, і ймовірності появи кожного з вимірів аномальності, які спостерігали раніше

під час вторгнень.

Однак для отримання більш реалістичної оцінки P ($I|A_1..A_n$), необхідно враховувати вплив вимірювань A_i один на одного.

У NIDES, щоб враховувати зв'язку між вимірами, при розрахунку використовуються коваріантні матриці. Якщо вимірювання A_1 .. A_n являє собою вектор A, то складене вимір аномалії можна визначити як

$$A^T C^{-1} A \tag{1.4}$$

де C - коваріантна матриця, що представляє залежність між кожною парою вимірювань аномалій.

Один із способів формування «образу» нормального поведінки системи полягає в накопиченні в спеціальній структурі вимірювань значень параметрів оцінки. Ця структура називається профайлом. Основні вимоги, які пред'являються до структури профайла: мінімальний кінцевий розмір, операція оновлення повинна виконуватися як можна швидше.

У профайлі використовується кілька типів вимірювань, наприклад, в IDES використовуються такі типи [13]

Показник активності - величина, при перевищенні якої активність підсистеми оцінюється як швидко прогресуюча. У загальному випадку використовується для виявлення аномалій, пов'язаних з різким прискоренням в роботі. Приклад: середнє число записів аудиту, оброблюваних для елемента, що захищається системи в одиницю часу.

Розподіл активності в записах аудиту - розподіл у всіх типах активності в свіжих записах аудиту. Тут під активністю розуміється будь-яка дія в системі, наприклад, доступ до файлів, операції введення-виведення.

Вимірювання категорій - розподіл певної активності в категорії (категорія - група підсистем, об'єднаних по якомусь загальному принципу). Наприклад, відносна частота реєстрації в системі (логінів) з кожного фізичного місця знаходження. Уподобання у використанні програмного

забезпечення системи (поштові служби, компілятори, командні інтерпретатори, редактори та інше).

Порядкові виміру - використовується для оцінки активності, яка надходить у вигляді цифрових значень. Наприклад, кількість операцій введення-виведення, ініційованих кожним користувачем. Порядкові зміни обчислюють загальну числову статистику значень певної активності, в той час як вимір категорій підраховують кількість активностей.

При виявленні аномалій з використанням профайла в основному застосовують статистичні методи оцінки. Процес виявлення відбувається наступним чином: поточні значення вимірювань профайла порівнюють зі збереженими значеннями. Результат порівняння - показник аномальності в вимірі. Загальний показник аномальності в найпростішому випадку може обчислюватися за допомогою деякої загальної функції від значень показника аномалії в кожному з вимірі профайла. Наприклад, нехай M1, M2 ... Mn, - вимірювання профайла, а S1, S2 ... .Sn, відповідно, являють собою значення аномалії кожного з вимірів, причому чим більше число Si, тим більше аномалії в і-тому показнику. Яка об'єднує функція може бути вагою сум їх квадратів:

$$a_1 s_1^{\,2} + a_2 s_2^{\,2} + \ldots + a_n s_n^{\,2} > 0 \qquad (1.5)$$

де a_i - показує відносна вага метрики M_i.

Параметри M1, M2 ... Mn, насправді, можуть залежати один від одного, і тому для їх об'єднання може знадобитися більш складна функція.

Основна перевага полягає в тому, що застосовуються добре відомі статистичні методи.

Недоліки:

Нечутливість до послідовності виникнення подій. Тобто статистичне виявлення може втратити вторгнення, яке проявляється у вигляді послідовності подібних подій.

Система може бути послідовно навчена таким чином, що аномальна поведінка буде вважатися нормальним. Зловмисники, які знають, що за ними спостерігають за допомогою таких систем, можуть навчити їх для використання в своїх цілях. Саме тому в більшості існуючих схем виявлення вторгнення використовується комбінація підсистем виявлення аномалій і зловживань.

Важко визначити поріг, вище якого аномалії можна розглядати як вторгнення. Заниження порогу призводить до помилкового спрацьовування (false positive), а завищення - до пропуску вторгнень (false negative).

Існує обмеження до тіпів поведінкі, Які могут буті змодельовані, вікорістовуючі чисті статистичні методи. ! Застосування статистичних технологій для Виявлення аномалій требует припущені, что дані надходять від квазістатічного процесса.

Інший способів представлення «образу» нормального поведінки системи - навчання нейронної мережі значеннями параметрів оцінки.

Навчання нейронної мережі здійснюється послідовністю інформаційних одиниць (далі команд), кожна з яких може перебувати на більш абстрактному рівні в порівнянні з використовуваними параметрами оцінки. Вхідні дані мережі складаються з поточних команд і минулих W команд, які обробляються нейронною мережею з метою передбачення наступних команд; W також називають розміром вікна. Після того як нейронна мережа навчена безліччю послідовних команд захищається системи або однієї з її підсистем, мережа являє собою «образ» нормального поведінки. Процес виявлення аномалій є визначення показника неправильно передбачених команд, тобто фактично виявляється відмінність у поведінку об'єкта. На рівні рецептора (рис. 2) стрілки показують вхідні дані останніх W команд, виконаних користувачем. Вхідний параметр задає кілька значень або рівнів, кожен з яких унікально визначає команду. Вихідний реагує шар складається з одного багаторівневого, який передбачає наступну можливу команду користувача [14].

Недоліки:

- топологія мережі і ваги вузлів визначаються тільки після величезного числа проб і помилок;
- розмір вікна - ще одна величина, яка має величезне значення при розробці; якщо зробити вікно маленьким то мережу буде не досить продуктивною, надто великим - буде страждати від недоречних даних.

Переваги:

- успіх даного підходу не залежить від природи вихідних даних;
- нейронні мережі легко справляються з зашумленими даними;
- автоматично враховуються зв'язку між різними вимірами, які, без сумніву, впливають на результат оцінки.

2 ДОСЛІДЖЕННЯ ФУНКЦІЙ БЕЗПЕКИ НА КОМУТАТОРІ CISCO

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.2.1.

Таблиця 2.1 - 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.

2.1 Функція Port security

Port security – технологія призначена для контролю підключених до комутатора пристроїв і запобігання аномалій або атак, націлених на переповнення таблиці MAC-адрес (CAM table overflow). За допомогою Port Security встановлюється максимальна кількість MAC адрес на конкретний світчпорт (мережевий порт, який оперує на 2-му рівні OSI) або VLAN, і контролюється доступ по заданих MAC-адресами.

Використовується для запобігання [3]:

- Не авторизована зміна MAC-адрес мережно обладнання або не авторизований доступу до локальної мережі;
- атак націлена на переповнення ARP-таблиці комутатора.

Способи роботи з MAC-адресами:

1) Static MAC-адреси - пускає тільки заздалегідь введений руками MAC-адресу (може бути використано разом з Dynamic типом);

- назначаються командою в командному рядку switchport port-security mac-address mac-address в режимі налаштування інтерфейсу комутатора;
- зберігаються в ARP-таблиці комутатора;
- додаються в поточну конфігурацію мережного обладнання Cisco Catalyst.

2) Dynamic - пропускає і запам'ятовує (на заданий період часу) будь-які MAC-адреси, поки не досягне дозволеного максимуму;

- динамічно конфігугуються системию;

- зберігаються тільки в ARP-таблиці комутатора;
- видаляються при перезавантаженні мережного обладнання.

3) Sticky MAC-адреси - вчить нові MAC-адреси, записуючи їх в конфігурацію;:

- дозволяє сконфігурувани статично або динамічно;
- зберігаються в ARP-таблиці комутатора;
- доповнюють поточну конфігурацію мережного обладнання. Якщо MAC-адреси збережені в конфігураційниий файлі то після перезавантаження, їх не обов'язково заново налаштовувати.

Несанкціонованим доступом до мережі для port security є наступні ситуації:

- максимальний обсяг безпечних MAC-адрес внесено в в ARP-таблицю комутатора, чий MAC-адреса не знайена в ARP-таблиці намагається приймати/відправляти пакети через інтерфейс комутатора;
- MAC-адреса, видана або сконфігурована як умовно безпечна на одному інтерфейсі, з'явилася на другому умовно безпечному інтерфейсі в тому ж VLAN мережі.

На інтерфейсі можуть бути налаштовані такі дії в разі перевищення повноважень [3]:

- protect – фрейми з новими MAC адресами ігноруються, все інше продовжує працювати. Режим хороший тим, що порт продовжує працювати, але поганий тим, що адміністратор швидше за все ніколи не дізнається, що в його мережі відбуваються такі дивні речі.
- restrict – ідентичний режиму protect за тим винятком, що комутатор по SNMP повідомляє, що сталася така неприємна ситуація, крім того, записує інформацію про це в syslog (якщо налаштований) . Коли кількість безпечних MAC-адрес досягає допустимого обмеження сконфігурованого на порту, пакети з невідомою MAC-адресою пакета ігноруються, доки не буде досягнуто безпечної

кількості MAC-адрес, щоб їх кількість була в межах допустимого значення, або переконфігуровано кількість допустимих адрес.

- shutdown – несанкціонований доступ призводить до того, що порт комутатора переводиться в стан error-disabled і перестає приймати будь-які пакети. Генерується оповіщення SNMP trap, повідомлення syslog і збільшується лічильник вторгнень (violation counter). Коли порт в режимі error-disabled, вимкнути його можна набравши команду в терміналі errdisable recovery cause psecure-violation або вручну включити інтерфейс набравши команду в режимі настройки інтерфейсу shutdown і no shutdown.

2.2 Функція DHCP snooping

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 дозволяє:

захистити клієнтів в мережі від отримання адреси від неавторизованого DHCP-сервера;

регулювати які повідомлення протоколу DHCP відкидати, які перенаправляти і на які порти.

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): Серед них[4]:

Ненадійні (Untrusted) – порти, до яких підключені клієнти. DHCP відповіді, що надходять з цих інтерфейсів ігноруються комутатором. Для ненадійних портів виконується перевіри DHCP пакетів і створюється БД прив'язки DHCP (DHCP snooping binding database).

Довірені (Trusted) – інтерфейси комутатора, до яких підключений інше мережне обладнання або довірений DHCP-сервер, який працює за рахунок перенаправлення DHCPNAK. DHCP-пакети отримані з цих інтерфейсів без перешкод проходять через комутатор.

Початкові конфігурації комутатор відкидає DHCP-пакет, який прийшов на ненадійний порт, якщо:

- приходить одн з пакетів, які відправляє DHCP-сервер (DHCPOFFER, DHCPACK, DHCPNAK або DHCPLEASEQUERY);
- приходить пакетів DHCPRELEASE або DHCPDECLINE, де в заголовку міститься MAC-адреса з БД прив'язки DHCP, але дані про порт комутатора в таблиці DHCP не відповідають інтерфейсу, на який був отриманий пакет;
- у DHCP-пакеті, що отримав комутатор, не відповідає MAC-адреса, що вказана в DHCP-запиті, і MAC-адреса джерела відправки цього пакету;
- приходить DHCP-пакет з опцією 82.

2.3 Функція Dynamic ARP Inspection

ARP spoofing - атака, спрямована на перехоплення трафіку між хостами. Якщо припустити, що в мережі є сервер з IP адресою 192.168.1.50. То атакуючий пристрій заспамлює мережу, повідомляючи, що IP адреса 192.168.1.50 належить йому. Комутатор отримав це повідомлення і додасть запис в свою ARP-таблицю, куди запише IP адресу сервера, що відповідає MAC адресі атакуючого пристрою. Так, дані відправлені будь-яким хостом на сервер з IP адресою 192.168.1.50 неминуче потраплять на атакуючий

пристрій, який потім перешле ці дані на сервер, щоб не викликати підозру.

Для протидії цій атаці, Cisco розширила базову функцію DHCP Snooping і додала до неї свого роду надбудову, яка становить таблицю всіх прив'язок IP адрес, виданих за допомогою DHCP сервера.

2.4 Захист від підробленого DHCP сервера

DHCP [4] транспортує параметри конфігурації стека протоколу від центрально керованих серверів до хостів TCP / IP.

DHCP Snooping означає, що комутатор спостерігає за процесом присвоєння IP адрес за допомогою протокола DHCP. Це запобігає появі нелегальних DHCP серверів і DHCP атаки шляхом настройки довірених і недовірених портів. DHCP повідомлення з довірених портів передається без перевірки. При типовій конфігурації довірені порти використовуються для підключення DHCP сервера або DHCP ретранслятора, а до недовірених портів підключаються клієнти. З недовірених портів комутатор буде пересилати тільки DHCP запити, але не відповіді. Якщо з недовірених порту отримано повідомлення DHCP відповіді, комутатор підніме тривогу і зробить певні дії з портом, згідно налаштувань, наприклад виключення або створення «чорної діри».

Якщо включена прив'язка DHCP Snooping, комутатор збереже у відповідній таблиці інформацію про кожного DHCP клієнта з недовірених портів (включаючи MAC адреса, IP адреса, оренду IP, номера VLAN і порту). Маючи таку інформацію DHCP Snooping можна комбінувати з іншими модулями, такими, як dot1x і ARP, або самостійно реалізувати контроль доступу користувачів.

Захист від підробленого DHCP сервера: якщо комутатор перехоплює відповідь DHCP сервера (включаючи DHCPOFFER, DHCPACK і DHCPNAK), він підніме тривогу і зробить певні дії, відповідно до налаштувань (виключення порту або створення «чорної діри»).

Захист від перевантаження DHCP: Щоб уникнути великої кількості повідомлень DHCP, атакуючих процесор, користувач може обмежити швидкість отримання DHCP пакетів на довірених і недовірених портах.

Запис зв’язних даних DHCP: DHCP Snooping при пересиланні DHCP пакетів буде записувати сполучні дані, виділені DHCP сервером. Можна так само завантажити ці дані на сервер з метою відновлення втраченої інформації. Сполучні дані, в основному, використовуються для настройки динамічних призначених для користувача портів dot1x. За детальною інформацією про dot1x зверніться, будь ласка, до глави «Налаштування dot1x».

Додавання довірених користувачів: можна додати записи в список довірених користувачів відповідно до параметрів сполучних даних; ці користувачі отримають доступ до всіх ресурсів без dot1x аутентифікації.

Автоматичне відновлення: через деякий час після виключення порту або створення «чорної діри», потрібно автоматично розблокувати порту або MAC адреси і відправити при цьому інформацію на сервер через syslog.

Функція журналу: Коли коммутатор знаходить не нормальні пакети, він повинен відправляти інформацію на сервер журналу через syslog.

Шифрування приватних повідомлень: зв'язок між комутатором і внутрішньою системою управління безпекою мережі TrustView відбувається через приватні повідомлення. Користувачі можуть шифрувати ці повідомлення в версії 2.

Функція додавання опції 82: різні опції 82 додаються в DHCP повідомлення відповідно до статусу аутентифікації користувача.

2.4.1 Конфігурації DHCP Snooping

Послідовність завдань конфігурації DHCP Snooping.

1) Включити DHCP Snooping.

ip dhcp snping enable

no ip dhcp snping enable

2) Включити функцію прив'язки DHCP Snooping.

ip dhcp snping bind enable

no ip dhcp snping bind enable

3) Включити функцію прив'язки ARP DHCP Snooping.

ip dhcp snping binding arp

no ip dhcp snping binding arp

4) Включити функцію опції 82 DHCP Snooping.

ip dhcp snping inform enbl

no ip dhcp snping inform enbl

5) Встановити версію приватних пакетів.

ip dhcp snping inform enbl

no ip dhcp snping inform enbl

6) Встановити зашифрований ключ DES для приватних пакетів.

enable trust view key 0/7

no enable trust view key

7) Встановити адресу DHCP сервера.

ip user helper address A.B.C.D [port

<udp port>] source <ip Addr>

(secondary|)

no ip user helper address (secondary|)

8) Налаштувати довірені порти

ip dhcp snping trast

no ip dhcp snping trast

9) Включити функцію прив'язки DHCP Snooping DOT1X

ip dhcp snping bind dot1x

no ip dhcp snping bind dot1x

10) Включити функцію прив'язки DHCP Snooping USER.

ip dhcp snping bind user cntrl

no ip dhcp snping binding user cntrl

11) Додати записи в статичний список.

ip dhcp snping bind user address vlan interface (ethernet|)

no ip dhcp snping binding user interface (ethernet|)

12) Встановити дії захисту.

ip dhcp snping action {shut down|blackhole} [recovery]

no ip dhcp snping action

13) Встановити обмеження швидкості передачі DHCP повідомлень.

ip dhcp snping limit-rate

no ip dhcp snooping limit-rate

14) Включити відладку.

debug ip dhcp snping packet

debug ip dhcp snping event

debug ip dhcp snping update

debug ip dhcp snping binding

15) Налаштувати атрибути опції 82 DHCP Snooping:

Налаштувати атрибути опції 82 DHCP Snooping.

ip dhcp snping information option

sub scriber id format {hex | acsii | vs-hp}

Встановлює зміст суб-опції remote-id опції 82. Команда no повертає стандартний формат.

ip dhcp snping inform option remote id {standard | <remote-id>}

no ip dhcp snping inform option

remote-id

Дозволяє недовіреним портам приймати DHCP пакети з опцією 82. Якщо не включено, все недовірених порти будуть відкидати DHCP пакети з опцією 82.

ip dhcp snping information option allowuntrusted

no ip dhcp snooping information option

allow-untrusted

Встановлює роздільник для параметрів суб-опцій опції 82. Команда no встановлює роздільник за замовчуванням - slash.

ip dhcp snooping information option

delimiter [colon | dot | slash | space]

no ip dhcp snooping information option

delimiter

Задає метод створення опції 82, користувачі можуть самостійно визначити параметри суб-опції remoteid.

ip dhcp snooping information option selfdefined remote-id {hostname | mac | string WORD}

no ip dhcp snooping information option selfdefined remote-id

Призначений для користувача формат remote-id для опції 82.

ip dhcp snooping information option selfdefined remote-id format [ascii | hex]

Задає метод створення опції 82, користувачі можуть самостійно визначити параметри суб-опції circuteid.

ip dhcp snooping information option selfdefined subscriber-id {vlan | port | id

(switch-id (mac | hostname)| remote-mac) | string WORD}

no ip dhcp snooping information option type

self-defined subscriber-id

Призначений для користувача формат circuit-id для опції 82.

ip dhcp snooping information option selfdefined subscriber-id format [ascii | hex]

Встановлює зміст суб-опції circuit-id опції 82. Команда no повертає стандартний формат.

ip dhcp snooping information option

subscriber-id {standard | <circuit-id>}

no ip dhcp snooping information option

subscriber-id

2.4.2 Типове застосування DHCP Snooping

Як показано на рисунку 2.1, пристрій Mac-AA - звичайний користувач, підключений до недовірених порту 1/0/1 комутатора, отримує IP

налаштування через DHCP, IP адреса клієнта 1.1.1.5. DHCP сервер і шлюз підключені до довірених портів комутатора, 1/0/11 і 1/0/12 відповідно. Зловмисник Mac-BB, підключений до недовірених порту 1/0/1 комутатора, намагається підробити DHCP сервер (посилаючи пакети DHCPACK). Функція DHCP Snooping на комутаторі ефективно виявить і блокує такий тип мережевої атаки.

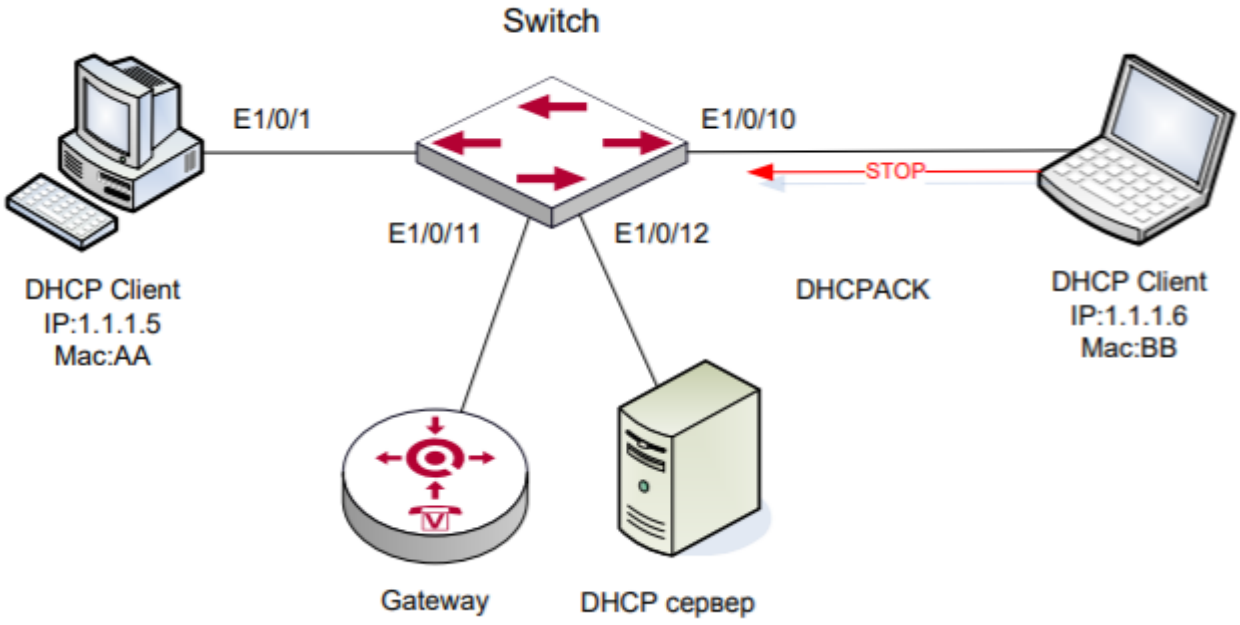

Рисунок 2.1 – Схема застосування DHCP Snooping

Послідовність налаштування:

switch#

switch#config

switch(config)#ip dhcp snping enble

switch(config)#interface ethernet 1/0/11

switch(Config-If-Ethernet1/0/11)#ip dhcp snooping trust

switch(Config-If-Ethernet1/0/11)#exit

switch(config)#interface ethernet 1/0/12

switch(Config-If-Ethernet1/0/12)#ip dhcp snooping trust

switch(Config-If-Ethernet1/0/12)#exit

```
switch(config)#interface ethernet 1/0/1-10
switch(Config-Port-Range)#ip dhcp snooping action shutdown
switch(Config-Port-Range)#
```

3 РЕАЛІЗАЦІЯ МЕХАНІЗМІВ ЗАХИСТУ ВІД МЕРЕЖНИХ АТАК

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

Комутатор має ARP-таблицю, де зберігаються «прив'язка», які адреси на якому порту приймаються. ARP-таблиця має певний обсяг відведений для зберігання MAC-адрес. Наприклад, комутатор Catalyst 2960 може зберігатися 8192 MAC-адрес.

Уявімо ситуацію, в якій нам необхідно стати посередником між робочою станцією і сервером. Для цього необхідно 2 комп'ютери, підключених до різних комутаторів. Атакуючий 1 вводить в оману свій комутатор щодо того, де знаходиться робоча станція, шляхом спуфинга її MAC-адреси. Атакуючий 2 вводить в оману дугою комутатор щодо місцезнаходження сервера шляхом спуфинга MAC-адреси сервера.

Таким чином, коли робоча станція намагається щось відправити серверу, її комутатор направляє цю інформацію атакуючому 2, той передає її своєму напарнику 1, а той сервера. Легко переконається, що дана ланцюжок працює і у зворотному напрямку.

Ще більш проста атака через спуфинг адрес називається CAM-переповнення. CAM - це пам'ять комутатора, де він зберігає інформацію про вчинених відповідностях MAC-адрес - порт. Якщо на одному порту генерувати дуже багато неіснуючих адрес, то незабаром пам'ять комутатора переповниться, і він перейде в режим концентратора. Таким чином, атакуючий отримає доступ до всього сегменту мережі, підключеного до комутатора, і зможе прослуховувати чужі переговори.

Для боротьби з цією атакою були використані можливості, що надаються технологією port-security, реалізованої на комутаторах Cisco.

Дана технологія дозволяє обмежити кількість MAC адрес, які

комутатор може вивчити з певного інтерфейсу, ввести штрафні санкції на порушення, дозволити тільки певним станціям підключатися до даного порту.

Розглянемо на прикладі промодельованої мережної атаки . Конфігурація комутатора буде представлено в мережному емуляторі Cisco Packet Traser 5.3.2 [9].

Схема моделювання показана на рис.3.1.

Для цього переходимо до меню глобального конфігурування:

Switch # conf t

Потім пункт меню конфігурації портів та обераємо всі порти комутатора, з 1 по 24:

Switch (conf) #int range f0/1 Потім сконфігуруємо таким чином, що всі ці порти будуть портами доступу набравши команду: Switch (config-if-range) #switchport mode access

Далі обераємо метод захисту комутатора port security: Swi tch (config if range) #switch port «port security»

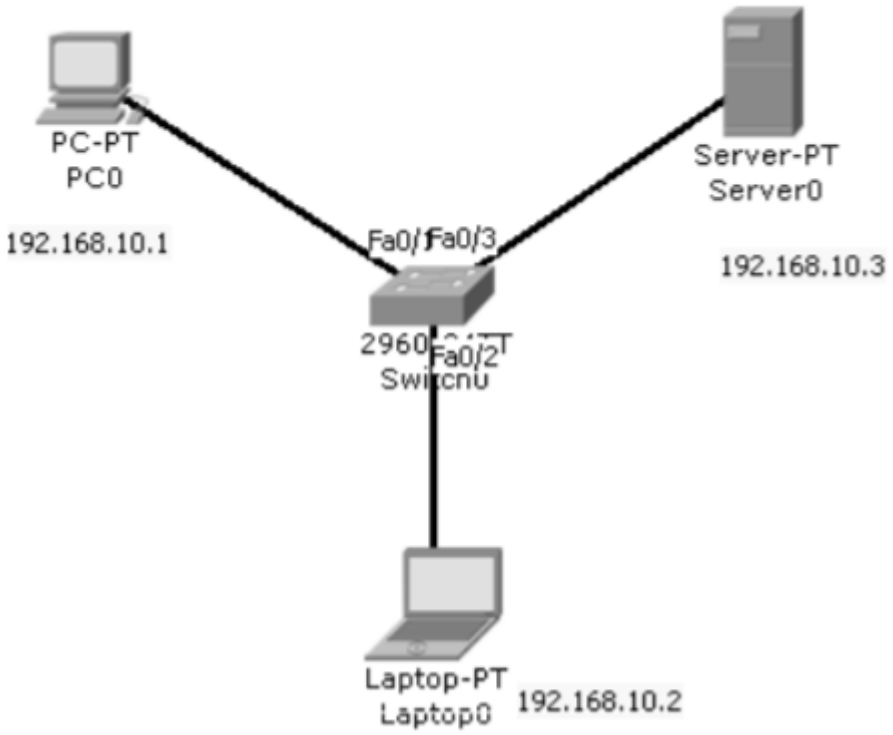

Рисунок 3.1 – Моделювання мережної атаки на комутатор MAC spoofing

Обираємо реагування на порушення безпеки, що буде робити комутатор, коли в порту з'являється більше одного MAC-адреса. У цьому випадку треба, щоб порт був відключений і відправлено відповідне повідомлення SNMP trar і syslog. Цю опцію можна вказати примусово, але вона працює за замовчуванням.

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 MACадреса, 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 runningconfig 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:

Наприклад, виконаємо:

Switch # show port-security int fa0 / 1

Результат виведення налаштувань інтерфейсу fa0 / 1 представлений на рис.3.2.

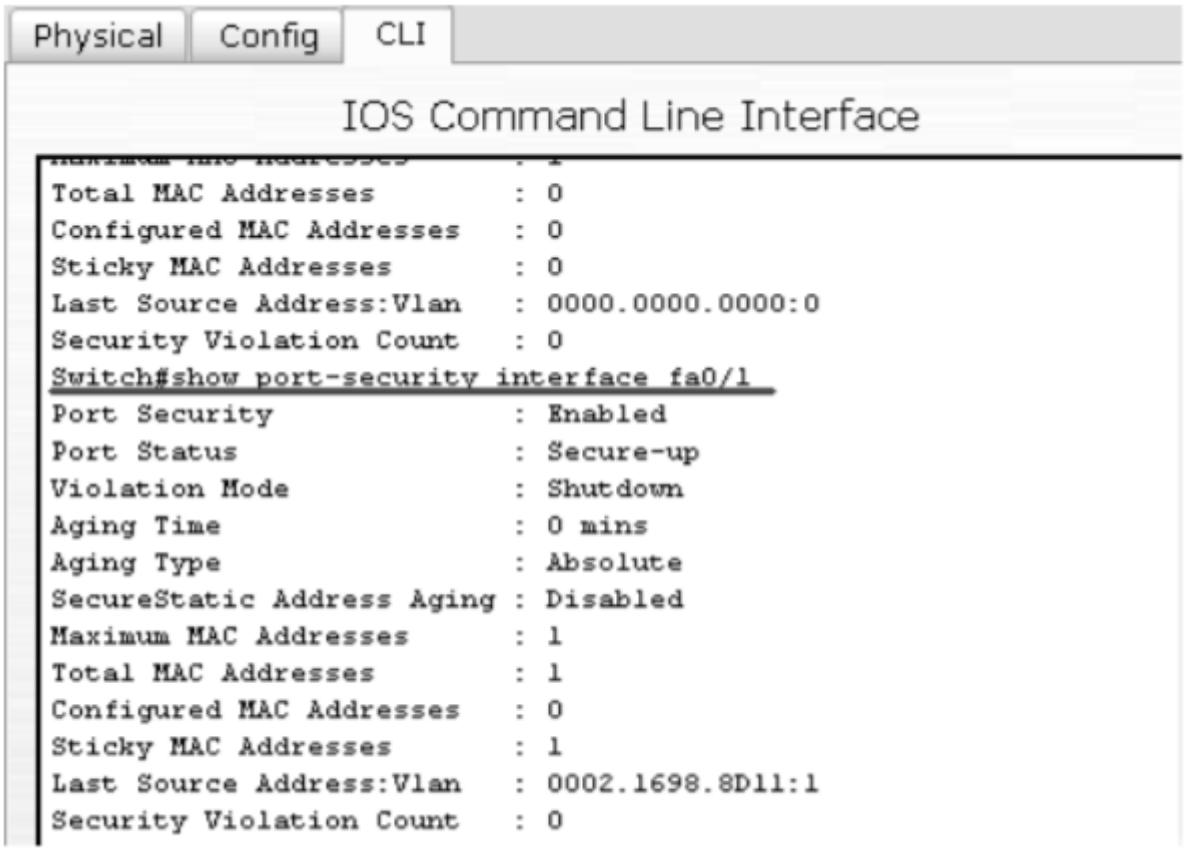

Рисунок 3.2 – Висновок налаштувань інтерфейсу f0/1

Перевіряємо таблицю адрес:

Switch # showmac-address-table

Результат виконання команди представлений на рис.3.3.

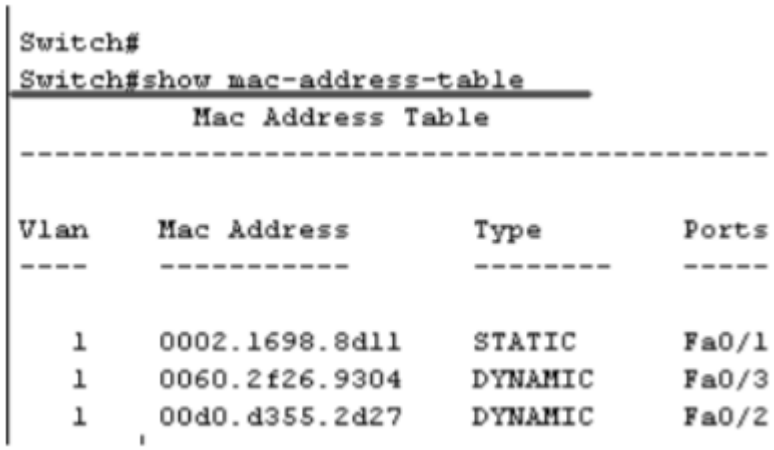

Рисунок 3.3 – Відображення таблиці MAC-адрес комутатора

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.3.4.

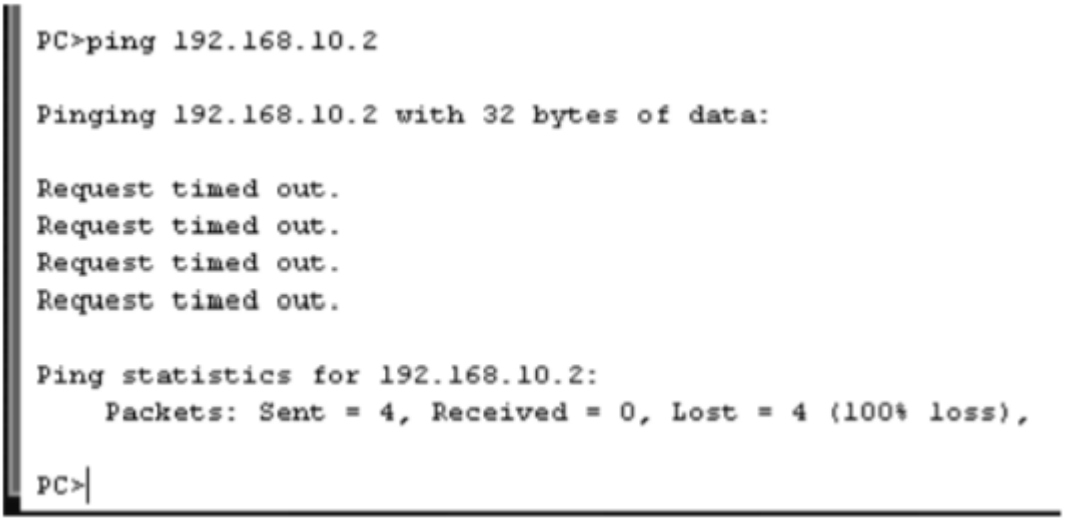

Рисунок 3.4 – Результат виконання команди ping

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 ARPкеші 60 секунд без оновлення.

3.2 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

IPадреси 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 – отказ 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 DHCPсервера, завантаження мережі і т.п.

Для того щоб зловмисник був упевнений, що саме від його DHCPсервера 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.3.5. 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 DHCPсервера будуть відкидатися.

Порядок налаштування наступний:

1) Налагодження та перевірка роботи DHCP-сервера та DHCPретранслятора 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 DHCPповідомлень.

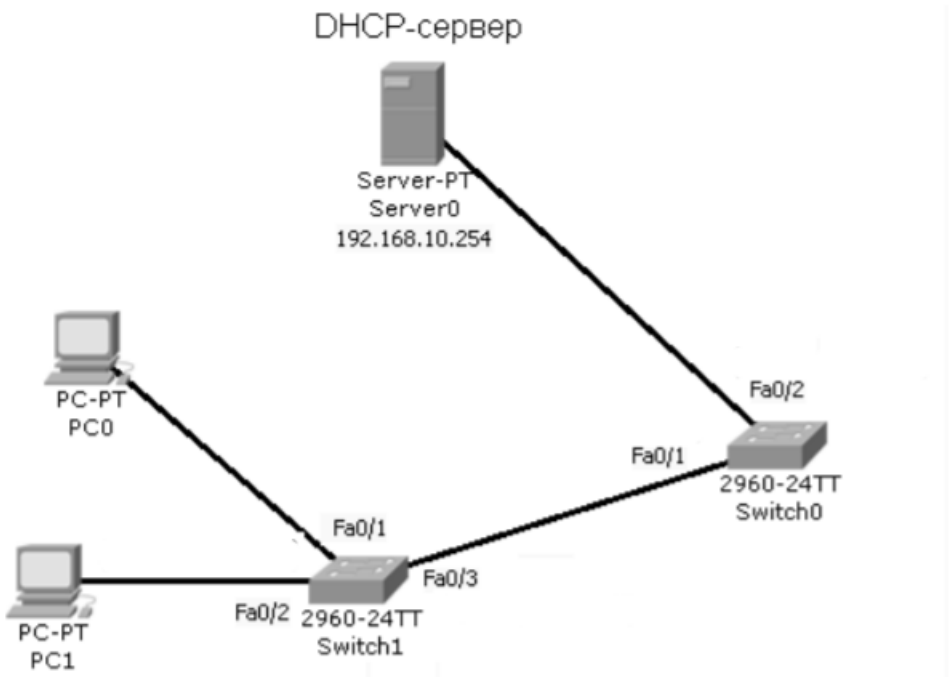

Рисунок 3.5 - Модель мережі для настройки DHCP snooping

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 trustпорти. 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 вказали (в нашому прикладі 100), то запити будуть

відхилені.

Switch (config) #interface fa0/1

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

3.3 Організація захисту проти атак ARP-spoofing

Так само, як і при реалізації функції DHCP snooping, на обох комутаторах схеми, зображеної на рис. 3.6, 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

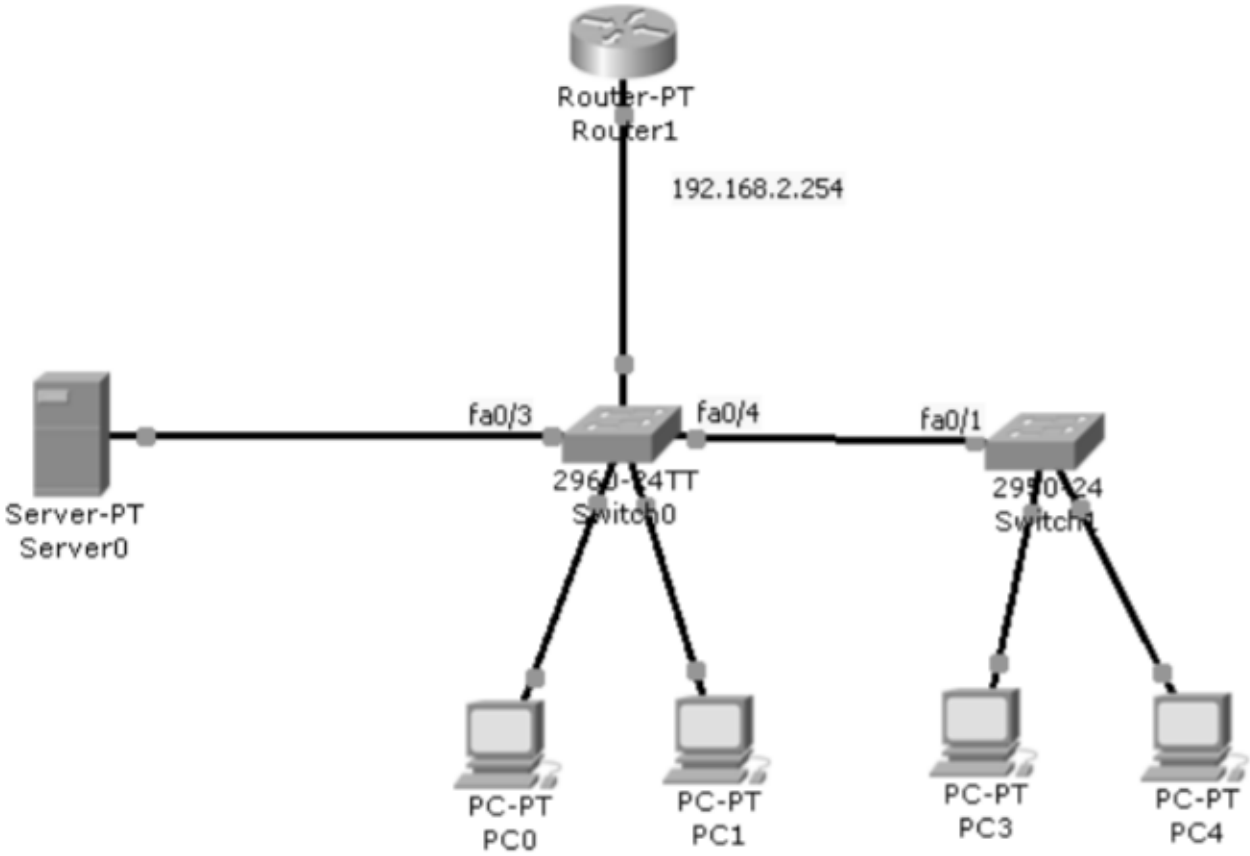

Рисунок 3.6 – Модель мережі для налаштування Dynamic ARP Inspection

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

3.4 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. 3.6).

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, BPDUпакета, 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 МАСадресою, це не дозволить стати йому «кореневим комутатором».

ВИСНОВКИ

У магістерська атестаційній присвячена основним проблемам, пов'язаним 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.

Під час виконання роботи було визначено поняття та особливості функціонування мережевого обладнання та технологій пов' язаних з ним, наведено та проаналізовано можливі загрози, та сформульовано перелік правил, що базується на найкращих практиках налаштування мережевого обладнання Cisco. Розробленопрограмний засіб, що власне проводить аудит, та видає звіт. А також протестовано його на віртуальному маршрутизаторі.

Розроблений метод захисту DHCP придатний для безпосереднього застосування при аудиті будь-яких мереж, що базуються на технологіях Cisco.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

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) 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.
4) Безмалый В. Парольная защита: прошлое, настоящее, будущее / В. Безмалый // Журнал «КомпьютерПресс». – 2008. – №9. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.compress.ru/article.aspx?Id= 20509&iid=901.
5) Джеймс Бони. Руководство по Cisco IOS. – СПб.: Питер, М: Издательство «Русская редакция», 2008. – 784 с.: ил.
6) SUN, Haobin, et al. Applying Binary Patch Comparison to Cisco IOS. In: Proceedings of the 2017 VI International Conference on Network, Communication and Computing. ACM, 2017. p. 38-42.
7) CCNP BCMSN Exam Certification Guide, David Hucaby (Building Cisco Multilayer Switching Networks), Osborne/McGraw-Hill, 2000
8) Построение виртуальных частных сетей (VPN) на базе технологии MPLS, составитель М. Захватов, Cisco Press, 2004
9) Blair G. S., Stefani J. B. Open distributed processing and multimedia. – Addison-Wesley Longman Publishing Co., Inc., 1998.
10) Глоба Л. С. Розподілені системи та мережі. Посібник для студентів технічних спеціальностей/Рек. МОН України, НТУУ “КПІ”, Інститут телекомунікацій, кафедра інформаційно-телекомунікаційних мереж //К.:

Норітаплюс. – 2007. – С. 223-237.

11) Tanenbaum A. S., Van Steen M. Distributed systems: principles and paradigms. – Prentice-Hall, 2007.
12) https://dt.ua/UKRAINE/kilkist-kiberzlochiniv-v-ukrayini-zbilshuyetsya-na-2-5-tisyachi-na-rik-266179_.html
13) Лєнков С. В. и др. Шляхи підвищення захисту авторського права за допомогою використання цифрових водяних знаків //Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2018. – №. 56. – С. 33-40.
14) Knopová, M. The Third World War? In The Cyberspace. Cyber Warfare in the Middle East [Text] / Knopová, M. // Acta Informatica Pragensia. – 2014. – Т. 3, № 1. – С. 23–32.
15) Ruban, I. V. An approach to cyber security support [Text] / Ruban, I. V. //Системи обробки інформації. – 2015. – №. 11. – С. 6–8.
16) Kora, A. D. Nagios based enhanced IT management system [Text] / Kora, A. D., Soidridine, M. M. // International Journal of Engineering Science and Technology (IJEST) – 2012. – Т.4, №. 4. – P. 1199–1207.
17) Cigala, V. Job–Oriented Monitoring of Clusters [Text] / Cigala, V. //International Journal on Computer Science and Engineering. – 2011. – Т. 3. – №. 3.
18) Cigala, V. Job–Oriented Monitoring of Clusters [Text] / Cigala, V. //International Journal on Computer Science and Engineering. – 2011. – Т. 3. – №. 3.
19) Сидоров, И. А. Инструментальный комплекс метамониторинга распределенных вычислительных сред [Текст] / Сидоров, И. А., Опарин, Г. А., Скоров, В. В //Параллельные вычислительные технологии. – 2014. – С. 159–167.
20) Tarasov, A. G. Integration of computing cluster monitoring system [Text] / Tarasov, A. G. //Proc. of the First Russia and Pacific Conference on Computer Technology and Applications (RPC 2010). – 2010. – С. 221–224.

21) Amoroso, Edward, G., Intrusion Detection // 1st ed., Intrusion.Net Books, Sparta, New Jersey, USA, 1999

22) Stefan Axelsson, “Research in Intrusion-Detection Systems: A Survey” // Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, 1999