Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи та засоби боротьби з вразливостями комп’ютерних мереж

(тема)

Виконав:

студент II курсу, групи КСМм-20-1

Баранова О.А.
(прізвище, ініціали)

Спеціальність

123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

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

Освітня програма

Комп’ютерні системи та мережі
(повна назва освітньої програми)

Керівник: ст. викл. Єрьоміна Н.С.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

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

Освітня програма Комп’ютерні системи та мережі
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Барановій Оксані Андріївні
(прізвище, ім’я, по батькові)

1. Тема роботи Методи та засоби боротьби з вразливостями комп’ютерних мереж

затверджена наказом по університету від “ 05 ” листопада 2021 р. № 1656 Ст.

2. Термін подання студентом роботи до екзаменаційної комісії 13 грудня 2021 р.

3. Вхідні дані до роботи 1) комп’ютерні мережі; 2) вразливості; 3) системи безпеки.

4. Перелік питань, що потрібно опрацювати у роботі

1) що таке комп’ютерні мережі та їх типи;

2) види вразливостей у комп’ютерних мережах;

3) методи та засоби боротьби з вразливостями;

4) приклади реалізації вразливостей.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Слайд-презентація – 16 слайдів.

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	Аналіз предметної галузі, постановка задачі	09.11.2021 – 13.11.2021	
2	Аналіз комп'ютерних мереж	14.11.2021 – 15.11.2021	
3	Аналіз вразливостей	16.11.2021 – 18.11.2021	
4	Дослідження методів запобігання вразливостям	19.11.2021 – 21.11.2021	
5	Висунення власних правил щодо проблеми	22.11.2021 – 25.11.2021	
6	Оформлення політики безпеки	26.11.2021 – 27.11.2021	
7	Оформлення пояснювальної записки	28.11.2021 – 01.12.2021	
8	Подання кваліфікаційної роботи керівникові та	02.12.2021 – 04.12.2021	
	її попередній захист		
9	Подання кваліфікаційної роботи на рецензу-	05.12.2021 – 08.12.2021	
	вання		

Дата видачі завдання «08» листопада 2021 р.

Студент _____
(підпис)

Керівник роботи _____ ст. викл. Єрьоміна Н.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 76 с., 16 рис., 1 дод., 15 джерел.

КОМП’ЮТЕРНІ МЕРЕЖІ, ВІРУСИ, МЕТОДИ ЗАХИСТУ, ПРОТОКОЛИ ПЕРЕДАЧІ ДАНИХ, ВРАЗЛИВОСТІ, ЕКСПЛОЙТ, СЕГМЕНТАЦІЯ, МЕРЕЖЕВА ФАЙЛОВА СИСТЕМА.

Метою кваліфікаційної роботи є аналіз вразливостей у комп’ютерних мережах та аналіз засобів та методів боротьби з ними. В роботі було досліджено існуючі типи мереж, їх топологія, типи комп’ютерних загроз, їх класифікація, методи та засоби боротьби з ними. Проаналізовані актуальні підходи до організації захисту підприємств та окремих користувачів. Була висунута політика безпеки в комп’ютерних мережах

Були проаналізовані вразливості та їх типи у комп’ютерних мережах. Також висунуті правила та методи для боротьби з вразливостями.

ABSTRACT

Master’s thesis: 76 pages, 16 figures, 1 appendices, 15 sources.

COMPUTER NETWORKS, VIRUSES, PROTECTION METHODS, DATA TRANSMISSION PROTOCOLS, VULNERABILITIES, EXPLOITATION, SEGMENTATION, NETWORK FILE SYSTEM.

The purpose of the certification work is to analyze vulnerabilities in computer networks and analyze the means and methods of combating them. The existing types of networks, their topology, types of computer threats, their classification, methods and means of combating them were studied. The current approaches to the organization of protection of enterprises and individual users are analyzed. A security policy has been put in place on computer networks

Vulnerabilities and their types in computer networks were analyzed. Rules and methods for dealing with vulnerabilities have also been put forward.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІТ – інформаційні технології

ОС – операційна система

ПЗ – програмне забезпечення

API – інтерфейс прикладного програмування (англ., Application Programming Interface)

CCMP – протокол аутентифікації повідомлень із ланцюжком блоків шифру (англ., Cipher Block Chaining Message Authentication Code Protocol)

IDS – система виявлення атак (англ., Intrusion Detection System)

IPSec – безпека інтернет-протоколу (англ., Internet Protocol Security)

L2TP – протокол тунелювання другого рівня (англ., Layer Two Tunneling Protocol)

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

POP3 – поштовий офісний протокол 3 (англ., Post Office Protocol 3)

SSH – безпечна оболонка (англ., Secure Shell)

SSID – ідентифікатор набору послуг (англ., The service set identifier)

TCP/IP – протокол керування передаванням / міжмережевий протокол (англ., Transmission Control Protocol/Internet Protocol)

TKIP – протокол цілісності тимчасового ключа (англ., Temporal Key Integrity Protocol)

TLS – безпека транспортного рівня (англ., Transport Layer Security)

WEP – конфіденційність, еквівалентна дротовому (англ., Wired Equivalent Privacy)

ВСТУП

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери. Вона, будучи системоутворюючим фактором життя суспільства, активно впливає на стан всіх сфер життя. Інформаційні технології увійшли в наше життя, і обійтися без них ми вже не можемо.

Сьогодні інформація важливий, стратегічний ресурс, який впливає на наше життя. Інформація та інформаційні технології можуть бути спрямовані на благо, або ж використані на шкоду. Інформаційна безпека займає уми багатьох людей, як звичайних, так і на державному та міжнародному рівні.

Для забезпечення інформаційної безпеки в комп’ютерних мережах потрібно досліджувати цю область. Методи незаконного впливу на інформацію та інформаційні системи розвиваються з кожним днем. Тому в світі створюються найсучасніші системи безпеки інформації. Сьогодні комп’ютерні мережі є важливим елементом функціонування комп’ютерного середовища. Вони пов’язують між собою користувачів в одну мережу для передачі інформації. Так як комп’ютерні мережі стали дуже розвиненими, існують способи на їх посягання. Тому приділяється увага класифікації шкідливих загроз і особливості їх впливу на комп’ютерну техніку.

У роботі відображені комп’ютерні мережі і їх класифікації, класифікації інформаційних загроз, методи і засоби боротьби з ними.

Тому було прийнято рішення проаналізувати вразливості та їх типи у комп’ютерних мережах. Головною метою є висунення правил та методів для боротьби з вразливостями.

1 КОМП’ЮТЕРНІ МЕРЕЖІ

1.1 Визначення комп’ютерних мереж

Комп’ютерні мережі (від англійської – network) – це мережа ПК, які розташовані на деякій території та що з’єднуються задля спільного користування ресурсами (зображень, інформації, програм та апаратних аспектів).

Головною ціллю по’єднання комп’ютерів до єдиної мережі є шанс надання кінцевим користувачам змоги доступу до будь-яких інформаційних ресурсів (наприклад, відео, зображень, програм, тощо), які рознесені по різним комп’ютерам, та для користування ними спільно. Головною ознакою будь-якої комп’ютерної мережі є розміри території, яку вона може охопити. Розміри охоплення визначаються різницею віддаленості вузлів, що складають її, що дуже впливає на технологічні рішення, що обираються під час побудови комп’ютерної мережі.

Комп’ютерні мережі, які виконують передачу інформації є результатом цифрової революції, які в майбутньому матимуть змогу створити єдиний т головний засіб для комунікації. По всьому світу є тяга до по’єднання комп’ютерів до мережі, яка обумовлена декількома важливими причинами, такими як – пришвидшення передачі інформації та даних, можливість дуже швидкого обміну данними між користувачами, здобуття її та передача листів (факсів, e-mail-листів, електронних даних, тощо), при цьому не потрібно відходити від фізичного місця, також є можливість швидкого отримання будь-якої доступної інформації з будь-якої точки планети, обмін даними між машинами будь-яких виробників, які працюють з різним апаратним та програмним забезпеченням.

Нинішні системи зараз можна розділити, в першу чергу, за ознакою місця знаходження.

Розвиток комп’ютерних мереж бере початок в 1950-х роках двадцятого століття. Еволюція комп’ютерних мереж пов’язана з покращенням апаратної техніки та телекомунікацій. Комп’ютерні мережі можна розглядати як інструмент для передачі даних на необмежені відстані, для цього в них встроєні засоби для кодування та мультиплексування інформації, що знаходить свій розвиток у різних системах телекомунікації [5]. Подивимося спочатку на комп’ютерні істоки мереж для обчислення. Перші комп’ютери 1950-х років – занадто великі, займають багато місця та коштують немало – потрібні були для обмеженого числа обраних користувачів. Зазвичай такі машини могли займати навіть цілі будівлі. Подібні системи не були призначені для комфортної роботи людини, вони застосовувалися в режимі так званої «пакетної обробки».

Рисунок 1.1 – Система пакетної обробки на базі мейнфрейма

Мережі для пакетної обробки, зазвичай, були побудовані на базі мейнфреймів – це потужний та надійний комп’ютер для універсального використання. Розробники робили перфокарти, які включали у себе інформацію та команди для програм, які передавали їх до обчислювального центру. Спеціальні люди вбивали такі карти до комп’ютера, після чого роздруковані результати розробники мали змогу отримати тільки через день.

Виходячи з цього, лише одна неправильно зроблена карта давала затримку, мінімум, на добу. Звісно, для розробників, інтерактивний режим праці, при котрому була можливість оперативно керувати етапами обробки даних за допомогою терміналу, був би легше. Хоча інтересами розробників, на перших етапах розвитку обчислювальних мереж, в значній мірі, нехтували. По-перше була головною ефективність праці найдорожчого елементу такої машини – процесора, при цьому нехтували ефективністю роботи фахівців.

Системи з декількома і більше терміналами стали прообразом мережі, яку ми бачимо зараз. Для того, щоб здешевити процесори, на початку 1960-х років почали з’являтися нові засоби для організації процесу по обчисленню, що дало змогу враховувати інтереси розробників. Стали розвиватися інтерактивні системи з багатьма терміналами для поділу часу. У подібних мережах кожна людина мала змогу отримати персональний термінал, за допомогою якого, вона могла керувати комп’ютером. Кількість одночасно працюючих з комп’ютером розробників визначалася його потужністю – час на реакцію обчислювальної мережі повинен бути малим, для забезпечення була непомітності паралельної роботи з машиною інших людей.

Машини, після виходу за межі обчислювального корпусу, розповсюдились по усьому підприємству. Не дивлячись на обчислювальну потужність, система залишалася централізованою, хоча можливості, такі як додання та виведення інформації, вже стали розподіленими.

Схожі централізовані системи, що мають немало терміналів, зовні стали дуже походити на локальні системи для обчислення. Насправді, будь-який користувач працю за терміналом комп’ютера починав сприймати приблизно так, як і у наші дні він сприймає роботу під час взаємодії з підключеним до мережі домашнім комп’ютером. Людина могла отримати доступ до будь-яких даних та периферійних пристроїв, але у нього була повна ілюзія одноосібного керування машиною, адже користувач міг встановити необхідну йому програму у будь-який момент та майже водночас отримати результат. (Деякі віддалені від обчислювальної техніки люди навіть

були переконані, що всі обчислення виконуються прямо всередині їх дисплея).

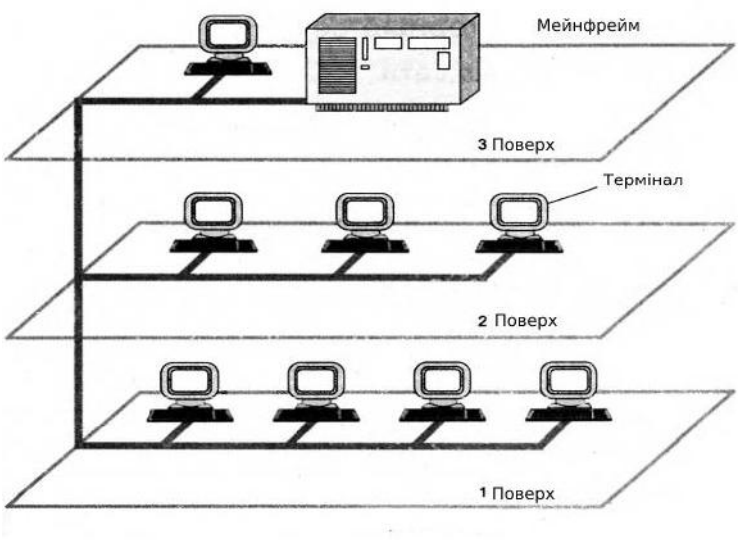

Рисунок 1.2 – Багатотермінальна система

Системи з багатьма терміналами, які функціонують у режимі поділу часу, стали немалим кроком на шляху до створення локальних мереж обчислення.

Але до моменту появи локальних мереж необхідно було подолати ще немалий шлях, так як багатотермінальні мережі, хоча і мали зовнішню характерність розподілених систем, але мали обробку даних централізовано.

При цьому потреба у корпораціях до створення локальних мереж у ці часи не розвинулась, адже в одній мережі не було що додавати в мережу, адже через дуже високу вартість техніки для обчислення підприємства не мали змогу дозволити собі придбати декілька машин. Під час такого періоду був вірний відомий закон Гроша, що емпірично показував планку технології тих часів. Відповідно до закону Гроша, ефективність комп’ютера була пропорційна його вартості у квадраті, тобто можна було сказати, що за однакову суму було краще придбати лише одну машину з великими потужностями, ніж декілька менш потужних, адже їх сумарна потужність була сильно менша за потужність більш дорогої машини.

Але необхідність у поєднанні самих машин, які знаходилися б на великій відстані, до цього моменту повністю назріла. Стартом був етап, на якому необхідно було вирішити просту задачу – доступ до машини з терміналів, які віддаленні від неї на багато сотень, чи тисячі кілометрів. Термінальний блок підключається до комп'ютера в телефонній мережі через модем. Ці мережі дозволили багатьом користувачам отримати віддалений доступ до ресурсів потужних суперкомп'ютерів [12]. Потім була система, що з функціонувала як комп'ютерний термінал, а комутувалася як комп'ютер - комп'ютер.

Комп'ютери мають можливість автоматичного обміну даними, що зазвичай є основним компонентом будь-якої комп'ютерної мережі.

На основі цього механізму перша мережа реалізувала обмін файлами, синхронізацію даних, електронну пошту та інші сервіси.

Таким чином, залежно від часу першими виникли WAN (Wide Area Networks), тобто мережі, що з'єднують територіально розосереджені комп'ютери, які можна знайти в різних містах і країнах.

Під час побудови глобальної мережі вперше були введені та апробовані основні поняття сучасних комп'ютерних мереж, такі як багаторівнева компанія протоколів зв'язку, концепція передачі пакетів і маршрутизації.

Глобальна комп'ютерна мережа успадкувала більшу частину найстарішої та найпоширенішої глобальної мережі: телефонну мережу. Головним технологічним нововведенням, яке вивело першу в світі комп'ютерну мережу на передній план, був перехід від правила регіональної ротації, яке десятиліттями успішно використовується в комп'ютерній мережі.

Стало відомо, що за увесь час отримання зв'язку, канал телефонії, який передає дані з однаковою швидкістю, не мав змогу ефективно користуватися різним трафіком комп'ютерної інформації, у якому періоди бурного обміну чергуються з затяжними паузами. Імперичні експерименти та моделювання за допомогою математичних методів доказали, що пульсуючий та значною мірою комп'ютерний трафік, що не чутливий до затримок, сильно

ефективніше може передаватися мережами, які можуть працювати за принципом комутації даних, у той час, коли інформація розділяється на малі порції – пакети, які можуть розрізнено передаватися по системі через наявність адреси останнього вузла на початку пакету.

Через те, що створення якісних мереж зв’язку на немалі відстані може обходитися занадто дорого, тому у початкових глобальних мережах раніше використовували вже існуючі канали для зв’язку, які були спочатку призначені не для таких цілей. Як приклад, протягом декількох років більш глобальні мережі були побудовані на основі каналів телефонії тональної частоти, які були здатні у кожен проміжок часу вести передачу даних для однієї розмови в умовах аналогової форми. Так як швидкість передачі цифрових даних по подібним каналам була невеликою (десятки кілобіт на секунду), набір можливостей, які надаються у глобальних мережах подібного типу звичайно бум обмеженим передачею файлів (звично у режимі фону) та електронною поштою [10]. Окрім малої швидкості подібні канали зв’язку мають і інший недолік, а саме – системи вносять великі спотворені дані. Через це глобальні протоколи мереж, що були побудовані з використанням ліній зв’язку малої якості, різняться комплексними процедурами контролю та відтворення інформації. Звичайним прикладом подібних систем є мережі з номером X.25, що створені ще напочатку 1970-х, у часи, коли аналогові канали з малою швидкістю, що були орендовані у компаній телефонії, були головним типом ліній, які поєднують машини і комутатори глобальної мережі для обчислень.

У 70-х роках міністерство оборони почало роботи щодо поєднанню в одну систему мейнфреймів оборонних та науково-дослідних мереж. Така система, що отримала назву ARPANET, була початковою точкою задля розробки першої та найвідомішої зараз глобальної мережі Інтернет.

Система ARPANET поєднувала машини різних класів, що функціонували під управлінням будь-яких операційних систем з новими модулями, які реалізовували протоколи комунікацій, загальні для всіх машин

у мережі. Операційні системи таких комп’ютерів можна назвати першими системами для зв’язку.

На відміну від багатотермінальної операційної системи, справжня мережева операційна система не тільки дозволяє користувачам виконувати розподілене зберігання та обробку між кількома комп’ютерами, з’єднаними електричними з’єднаннями, але також дозволяє користувачам організовувати розподілене зберігання та обробку. З одного боку, кожна мережева операційна система виконує всі функції локальної операційної системи, з іншого боку, вона має деякі інші інструменти, які дозволяють їй взаємодіяти з операційними системами інших комп’ютерів по мережі. З розвитком мережевих технологій, розвитком комп’ютерного обладнання та появою нових завдань, що вимагають створення мережі, в операційній системі поступово з’явилися програмні модулі, що реалізують мережеві функції.

Розвиток глобальних комп’ютерних мереж значною мірою залежить від розвитку телефонних мереж.

З кінця 1960-х років цифрова передача голосу все частіше використовується в телефонних мережах. Це веде до високошвидкісного цифрового каналу, який підключається до АТС і дозволяє передавати десятки і сотні дзвінків одночасно.

Сьогодні за видами та якістю послуг, що надаються, глобальна мережа обертається навколо локальної мережі, яка довгий час була першою в цьому плані, хоча народилася значно пізніше.

1.2 Типи та топології комп’ютерних мереж

Комп’ютерні мережі класифікуються за типом передачі даних (мережа передачі, від вузла до вузла) та розміром (локальна, міська та глобальна мережа).

Широкомовні мережі мають спільний канал зв’язку, який використовується всіма машинами в мережі. Усі машини отримують коротке

повідомлення, яке називається пакетом, надісланим комп’ютером. Поле адреси на пакеті вказує, кому було надіслано повідомлення. Після отримання блоку машина керує блоком управління. Якщо пакет позначений для цієї машині, він обробляється. Пакети, надіслані з іншого комп’ютера, ігноруються.

Мережі передачі дозволяють надсилати пакети зі спеціальними кодами в адресному полі на всі пристрої одночасно. Коли посилається пакет з таким кодом, він приймається і обробляється всіма машинами в мережі. Ця функція називається розподілом. Деякі завантаження дозволяють надсилати повідомлення на підгрупу пристроїв, які називаються багатоадресною розсилкою. Одним із можливих способів використання цього підходу є блокування кількох символів передачі. Решта n-1 бітів адреси можуть містити номери груп. Кожен пристрій може бути «прописаний» в одну, кілька або всі групи. Коли пакет надсилається певній групі, він доставляється на всі комп’ютери цієї групи.

З іншого боку, мережа передачі між вузлами складається з великої кількості з’єднаних пар машин. У такій мережі пакет повинен досягти кількох проміжних машин, щоб досягти своєї мети. Оскільки часто існує багато можливих шляхів від джерела до приймача, алгоритми для обчислення цих шляхів відіграють дуже важливу роль у мережі передачі між вузлами. Зазвичай (хоча є винятки) малі, географічно існуючі мережі використовують широкомовну передачу, тоді як великі мережі використовують міжвузлову передачу. В останньому випадку це відправник і одержувач, і цю систему іноді називають односторонньою передачею.

Ще однією характеристикою класифікації мережі є її розмір. Локальні мережі (LAN) – це приватні мережі, які зазвичай розташовані в будівлі або на території будь-якої організації площею до кількох квадратних кілометрів. Вони часто використовуються для об’єднання комп’ютерів і робочих станцій в офісах компанії або компанії, яка спільно використовує ресурси (наприклад, принтери), а також для обміну інформацією. Локальні мережі

відрізняються від інших мереж трьома характеристиками: розміром, технологією передачі даних, топологією.

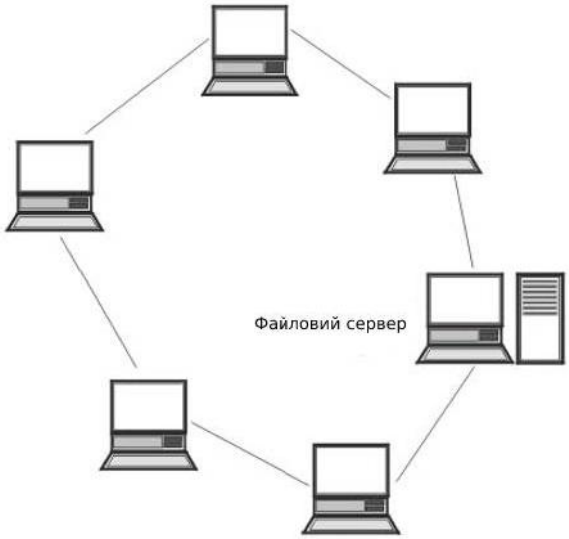

Рисунок 1.3 – Мережі з передачею від вузла до вузла

Локальні мережі обмежені за розміром, а це означає, що час пересилання пакетів обмежений і відомий заздалегідь. Знання цього обмеження дозволяє використовувати певні типи розробки, які інакше були б неможливими. Крім того, це спрощує керування локальною мережею.

Локальна мережа створюється для: роботи в обмеженій географічній зоні, забезпечення доступу багатьом користувачам у широкосмуговому середовищі, забезпечення постійної доступності віддалених ресурсів, підключених до локальних послуг, забезпечення фізичного підключення сусідніх мережевих пристроїв.

Типовими технологіями локальної мережі є: Ethernet, Token Ring, FDDI.

У локальних мережах часто використовується технологія передачі даних, яка складається з одного кабелю, до якого підключені всі машини. Це схоже на те, як телефонні лінії використовувалися в сільській місцевості. Звичайні локальні мережі мають пропускну здатність від 10 до 100 Мбіт/с,

низьку затримку (десяті частки мікросекунди) і дуже мало помилок [1]. Локальні мережі нового покоління можуть обмінюватися інформацією зі швидкістю до 10 Гбіт/с.

При передачі локальної мережі можна використовувати різні топологічні структури. У мережі із загальною шиною (лінійним кабелем) одна з машин завжди є провідною шиною і має право на передачу.

Усі інші транспортні засоби повинні відмовитися від передачі в цей час. Якщо дві машини хочуть доставити пакети одночасно, виникають конфлікти і потрібні спеціальні механізми. Цей механізм може бути централізованим або розподіленим. Наприклад, стандарт IEEE 802.3 під назвою Ethernet визначає мережеву передачу з децентралізованою топологією шини, що працює зі швидкістю від 10 Мбіт/с до 10 Гбіт/с. Ви можете будь-коли завантажити комп’ютер у мережі Ethernet. Коли два або більше пакетів даних стикаються, кожен комп’ютер випадковим чином чекає і знову намагається скопіювати пакет даних.

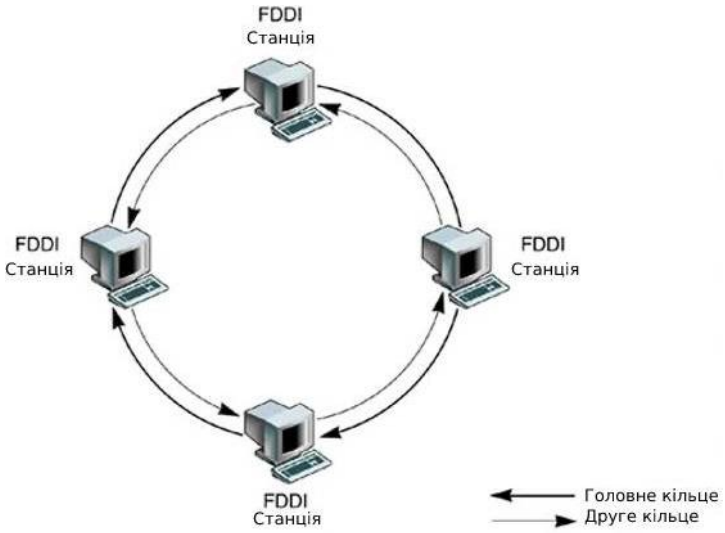

Рисунок 1.4 – Кільцева мережа FDDI

Ще одна система передачі – кільцева. Якщо є кільце, кожен біт проходить через рядок, не чекаючи решти пакета. Зазвичай настає час

переглянути всі пакети, перш ніж надсилати кожну папку до всієї системи. Як і система розподілення, кожна арбітражна система повинна контролювати доступ до лінії. Стандарт IEEE 802.5 визначає популярні локальні мережі, що працюють зі швидкістю 4 і 16 Мбіт/с. Іншим прикладом кільцевої мережі є FDDI (оптична мережа).

Залежно від способу призначення каналу, мережі передачі поділяються на статичні та динамічні. Статичне розподілення використовує циклічний алгоритм і безперервно розподіляється між усіма пристроями через певні проміжки часу, так що машина може передавати дані лише за виділений інтервал часу. У цьому випадку ємність каналу використовується економно, тому що часовий інтервал виділяється машинам, незалежно від того, є їм що передати чи ні. Тому динаміка (тобто доступ до каналу на вимогу) використовується частіше.

Методи динамічного надання доступу до каналів також можуть бути централізованими або децентралізованими. У режимі централізованого доступу до каналу повинен бути арбітр шини, який визначає машину, яка отримує право передачі. Рефері має прийняти рішення на основі отриманих запитів і певного внутрішнього алгоритму. У децентралізованому методі кожна машина повинна сама вирішити, передавати їй щось чи ні. Можна подумати, що такий метод неминуче призведе до розладу, але це не так.

Муніципальні, регіональні або міські (MAN) мережі з’єднують комп’ютери в межах міста. Найпоширенішим прикладом інженерної мережі є система кабельного телебачення. Він став наступником звичайних антенних телевізійних мереж у місцях, де якість передачі з тих чи інших причин була дуже низькою. Загальна антена в цих системах розміщується на вершині пагорба, і сигнал передається до будинків абонентів.

Спочатку почали з’являтися спеціалізовані мережеві структури, розроблені безпосередньо на місці. Потім розробники почали просувати свої системи на ринку, вони почали вести бізнес з міською владою, і зрештою охопили цілі міста. Наступним кроком було створення телевізійних шоу і

навіть читаних каналів, присвячених виключно кабельному телебаченню. Зазвичай вони представляли сферу інтересів [2]. Ви можете підписатися на новини, спорт, кулінарію тощо. До кінця 1990-х ці системи були розроблені виключно для телебачення.

Оскільки Інтернет почав залучати масову аудиторію, кабельні оператори зрозуміли, що з незначними змінами в системі цифрові дані можуть передаватися по тих самих каналах у невикористаній частині спектра (причому в обох напрямках). Відтоді кабельне телебачення поступово переросло в комунальну комп’ютерну мережу. У першому наближенні система MAN може уявити, що телевізійний і цифровий сигнали передаються по одних і тих же лініях. Вони змішуються на пристрої введення і передаються абонентам.

Проте муніципальні мережі – це не лише кабельне телебачення. Останні розробки високошвидкісного бездротового доступу до Інтернету привели до появи інших MAN, як описано в стандарті IEEE 802.16.

Мережу MAN можна налаштувати бездротовим способом, передаючи сигнали через відкриту телекомунікаційну інфраструктуру. Велика пропускна здатність доступних на даний момент оптичних каналів робить мережу MAN більш функціональною та економічною, ніж раніше. Мережі MAN відрізняються від локальних мереж і VAN наступними функціями.

Мережі MAN з’єднують користувачів, які перебувають у географічній зоні або в області, більшій, ніж зона локальної мережі, але меншій, ніж VAN.

Мережі MAN з’єднують міські мережі, щоб утворити більшу мережу (яка також може запропонувати ефективне підключення до VAN).

Мережі MAN також використовуються для з’єднання кількох локальних мереж, створюючи мостові з’єднання на міських лініях.

Широкомасштабна мережа (WAN) охоплює велику географічну територію, часто всю країну або навіть континент. Об’єднує машини, призначені для виконання прикладних програм (тобто додатків). Хости підключаються до комунікаційних підмереж, які скорочуються як підмережі.

Хости, як правило, належать клієнтам і керуються ними (тобто просто комп’ютерами клієнтів), тоді як підмережа зв’язку, як правило, належить і керується телефонною компанією або провайдером. Завдання підмережі – передавати повідомлення від одного хоста до іншого, так само як телефонна система передає слова від одного мовця до іншого.

Розподілені VAN призначені для виконання таких функцій: зв’язок у великих географічно відокремлених районах, надання користувачам зв’язку в режимі реального часу з іншими користувачами, безперервний доступ до віддалених ресурсів через підключення до локальних служб, надання послуг електронної пошти, всесвітня мережа, надсилання файлів і покупки електронною поштою через Інтернет.

Типові технології розподіленої мережі включають: модемний зв’язок, цифрову мережу з інтегрованими послугами (ISDN), цифрову абонентську лінію (DSL), технологію Frame Relay, а також типи T (США) і типу E (Європа): T1, E1, T3, E3 тощо. Синхронна оптична мережа (SONET) – синхронна передача сигналу 1 рівня (STS-1).

У більшості глобальних мереж підмережа складається з двох окремих компонентів: ліній зв’язку та роз’ємів. Лінії зв’язку, також звані каналами або лініями, передають дані з однієї машини на іншу. Елементи комутації – це спеціалізовані комп’ютери, які використовуються для з’єднання трьох і більше ліній зв’язку. Коли дані відображаються на вхідному рядку, елемент перемикача повинен вказати вихідний рядок, додатковий шлях для цих даних. Раніше не було стандартних термінів для цих назв комп’ютерів. Тепер вони називаються маршрутизаторами. Топологія мережі (від грец. – розташування): спосіб опису конфігурації, розташування та підключення мережі мережевих пристроїв.

Топологія – це принципова схема каналу зв’язку між комп’ютерами або вузлами мережі. Топологія мережі може бути фізичною: вона описує фізичне розташування та зв’язок між вузлами мережі, логічною: описує сигнал всередині фізичної структури, інформаційною: визначає напрямок потоку

інформації, що передається через мережу, і контролює біржа: принцип передачі прав на використання мережі.

Існує багато способів підключення мережевих пристроїв. Розрізняють такі структури: повнозв’язані, взаємопов’язані мережі, загальний носій, зірка, кільце, сніжинка. Розглянемо кожен з них докладніше.

Повністю підключена топологія. Топологія комп’ютерної мережі, в якій кожна робоча станція підключена до всіх інших робочих станцій. Цей варіант громіздкий і малоефективний, незважаючи на свою логічну простоту. Кожній парі має бути призначена окрема лінія, і кожен комп’ютер повинен мати стільки комунікаційних портів, скільки комп’ютерів у мережі [6]. З цих причин мережа може мати відносно невеликий кінцевий розмір. Ця архітектура найчастіше використовується в групах багатьох пристроїв або глобальних мережах з невеликою кількістю робочих станцій.

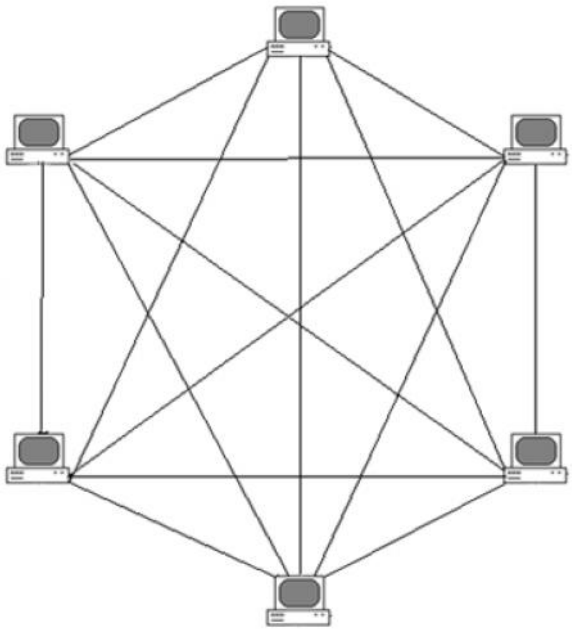

Рисунок 1.5 – Повнозв’язна топологія

Технологія доступу до мережі в цій топології реалізована шляхом передачі маркерів. Маркер – це пакет, оснащений спеціальною послідовністю

бітів (порівняно з пакетом для запису). Він подається послідовно як кільце від комп’ютера до комп’ютера в одному напрямку. Кожен вузол представлений маркером. Після отримання порожнього маркера комп’ютер може відправити дані. Маркери пакетів передаються до тих пір, поки не буде виявлено комп’ютер, якому призначено пакет. На цьому комп’ютері дані отримуються, але маркер переміщується та повертається відправнику.

Коли відправник пакета перевіряє, що пакет був доставлений одержувачу, маркер звільняється.

Недоліки: це громіздкий і неефективний варіант, оскільки він вимагає багато комунікаційних портів на кожному комп’ютері.

По суті, така система – це повністю взаємопов’язана комп’ютерна мережева топологія, в якій кожна робоча станція в мережі з’єднується з кількома іншими робочими станціями в одній мережі. Відрізняється високою стійкістю до збоїв, складністю регулювання і високою вартістю кабелів. Кожен комп’ютер має кілька можливих способів підключення до інших комп’ютерів. Пошкоджений кабель не від’єднує обидва комп’ютери.

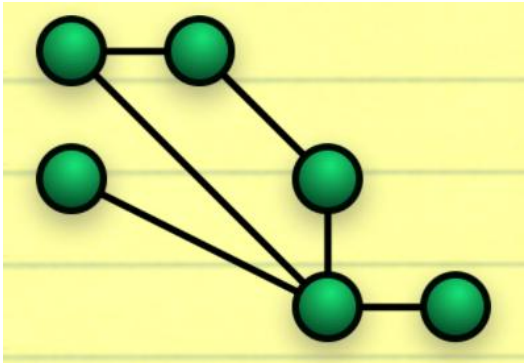

Рисунок 1.6 – Mesh-мережі

Ця топологія дозволяє підключати багато комп’ютерів і, як правило, поширена у великих мережах.

Загальна шина – це загальний кабель (шина або магістраль), до якого підключені всі робочі станції. Термінатор розташований на кінці кабелю,

щоб сигнал не відбивався. У порівнянні з іншими топологіями вона має такі переваги: короткий час встановлення мережі, низька вартість (потрібні мережеві кабелі та пристрої), проста конфігурація, а збої робочої станції не впливають на мережу.

Недоліком є те, що проблеми мережі, такі як обірвані кабелі та збої термінатора, повністю блокують роботу всієї мережі, що ускладнює визначення місця збою та додавання нових робочих станцій, що знижує продуктивність мережі.

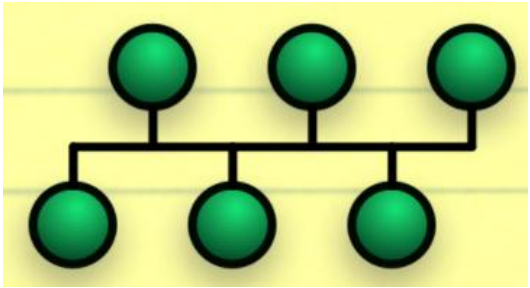

Рисунок 1.7 – Загальна шина

Топологія шини – це топологія, до якої всі пристрої локальної мережі підключені в середовищі мережевого зв’язку. Цю лінію часто називають каналом, автобусом або колією. Кожен пристрій, наприклад, робоча станція або сервер, незалежно підключається до спільного кабелю, який підключається через виділені роз’єми. Кінець шинного кабелю повинен мати відповідний резистор або клему, які можуть приймати електричний сигнал, відображати його та рухатися в іншому напрямку біля шини.

Зірка – це базова топологія мережі, в якій усі мережеві комп’ютери з’єднані з центральним (часто гнучким) вузлом і є частиною тіла мережі. Ці компоненти можуть працювати на добровільній основі або як частина складної топології мережі (зазвичай «дерева»). Оскільки вся інформація обмінюється тільки на хості, це дуже складно, тому без Інтернету нічого не зробити. Центральний вузол зазвичай є найпотужнішим і має всі функції

системи обміну [7]. Звичайно, мережі із зоряною топологією не стикаються, оскільки контроль є повністю центральним.

Метод доступу реалізований за технологією Arcnet. Цей метод доступу також використовує токени для передачі даних. Жетони передаються з одного комп’ютера на інший у порядку зростання. У круговій топології кожен комп’ютер відновлює один маркер.

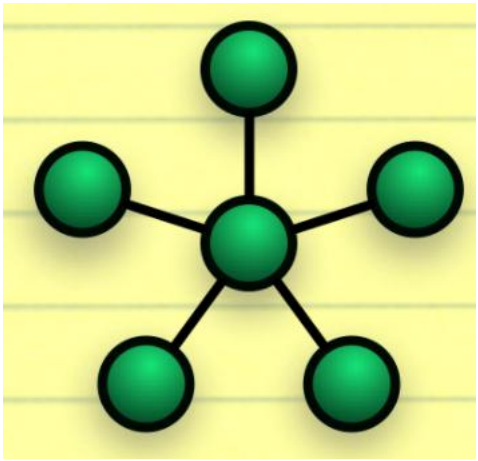

Рисунок 1.8 – Топологія зірка

Перевагами цієї топології є: помилки робочої станції не впливають на роботу всієї мережі, мережа має хорошу масштабованість, прості мережеві помилки та переривання, висока продуктивність мережі (правильно спроектована) і гнучке управління. Недоліком є: збій центрального вузла призводить до відмови всієї мережі (або її сегмента). Мережа зазвичай вимагає більше кабелів, ніж більшість інших топологій. Кількість кінцевих точок у мережі (або сегменті мережі) обмежена кількістю портів на центральному вузлі.

Кільце – це така топологія, у якій будь-який комп’ютер поєднаний з двома іншими комп’ютерами тільки через одне комунікаційне з’єднання: він отримує лише інформацію від одного комп’ютера та надає лише інформацію від іншого. На кожній лінії зв’язку є лише один передавач і один приймач,

які є зірочкою. Це дозволить вам уникнути використання зовнішнього термінатора.

Завдання в кільцевій мережі полягає в тому, що кожен комп’ютер повинен передавати (відновлювати) сигнал і, таким чином, діяти як ретранслятор. Таким чином, ослаблення сигналу по всьому контуру не має значення, а загасання між сусідніми комп’ютерами в ланцюзі не має значення. У цьому випадку немає чітко визначеного центру і всі комп’ютери можуть бути однаковими.

Проте часто в кільці є спеціальний абонент, що керує обміном. Зрозуміло, що наявність цього контролю користувача знижує надійність мережі, оскільки помилка відразу паралізує весь комутатор.

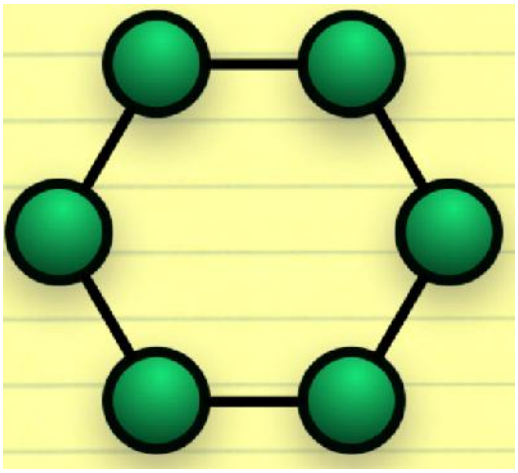

Рисунок 1.9 – Топологія кільце

Комп’ютери в кільці не зовсім однакові (наприклад, на відміну від топології шини). Деяким з них потрібно отримувати інформацію з комп’ютера, який вони надсилають зараз, іншим – пізніше. На основі особливостей цієї топологічної структури створюється метод керування комутацією мережі виключно для «кола». У цих методах право на повторну передачу (або, як кажуть, перехоплення мережі) передається наступному комп’ютеру.

Підключитися до «кільця» нового користувача зазвичай досить легко, хоча під час підключення потрібно буде примусово відключити всю мережу. Для топологій «шини» максимальна кількість користувачів у колі може бути дуже великою (1000 або більше). Кругові топології зазвичай є найбільш завантаженими і забезпечують надійну роботу з максимальним потоком інформації, що надсилається по мережі. Загалом вони неконфліктні (на відміну від інших) і немає центральних користувачів (на відміну від зірочок).

На відміну від інших топологій (зірки, шини), кола не використовують конкуруючі методи передачі даних. Комп’ютери в мережі отримують дані від комп’ютера до списку одержувачів, і якщо дані не надсилаються, вони знову надсилаються. Список призначення формується комп’ютером як генератор маркерів. Мережевий модуль генерує сигнал маркера (зазвичай близько 2-10 байт для запобігання завмирання) і відправляє його в іншу систему (MAC-адреса може збільшитися). Інша система, яка приймає сигнал, не аналізує його, а лише посилає. Це так званий нульовий період.

Принцип дії кругового алгоритму полягає в наступному. Пакети GRE, надіслані від відправника до одержувача, починають йти по шляху, визначеному тегом. Пакети даних надсилаються, поки не досягнуть одержувача.

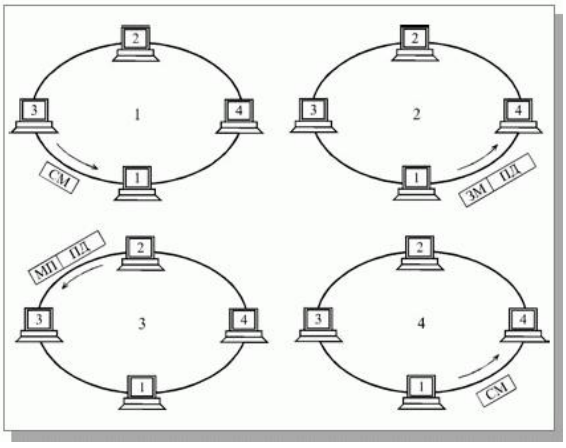

Рисунок 1.10 – Кільцевий алгоритм роботи

До переваг можна віднести: простота встановлення, майже повна відсутність іншого обладнання, є варіант безперебійної праці без видимого падіння швидкості трансферу інформації під час великого завантаження, так як при використанні маркера не має можливості появи колізій [1].

Недоліками можна назвати: при виходу з ладу лише однієї робочої станції, або інші недоліки (знищення кабелю), впливають на працездатність усієї системи, складність конфігурації та налаштування, труднощі пошуку вразливостей, необхідність отримати дві системні плати, на всіх робочих станціях.

1.3 Постановка цілей та задач дослідження

Одразу після того, як було досліджено поняття комп’ютерних мереж, розглянуті їх принципи роботи та топології. За допомогою теоретичного підходу були обґрунтовані методи та схеми побудови комп’ютерних мереж.

Ціллю та метою даного дослідження є аналіз вразливостей у комп’ютерних мережах та аналіз підходів щодо вирішення проблем та запобігання вразливостей у будь-яких типах мереж. Виявлення найбільш дійсних та ефективних методів.

Після аналізу були поставлені такі задачі:

- проаналізувати вразливості у комп’ютерних мережах;
- проаналізувати методи боротьби з ними;
- проаналізувати засоби боротьби з вразливостями;
- скласти рекомендації щодо захисту мереж.

2 ВРАЗЛИВОСТІ В КОМП’ЮТЕРНИХ МЕРЕЖАХ

2.1 Види вразливостей

Існують чотири дії, що можуть бути вироблені з інформацією, які можуть містити в собі загрозу: збір, модифікація, витік і знищення. Ці дії є базовими для подальшого розгляду.

Дотримуючись прийнятій класифікації необхідно розділяти всі джерела загроз на зовнішні і внутрішні. Джерелами внутрішніх загроз є: співробітники організації, програмне забезпечення, апаратні засоби.

Внутрішні загрози можуть проявлятися в наступних формах: помилки користувачів і системних адміністраторів, порушення співробітниками фірми встановлених регламентів збору, обробки, передачі та знищення інформації, помилки в роботі програмного забезпечення, відмови і збої в роботі комп’ютерного обладнання.

До зовнішніх джерел загроз відносяться: комп’ютерні віруси і шкідливі програми, організації та окремі особи, стихійні лиха.

Формами прояву зовнішніх загроз є: зараження комп’ютерів вірусами або шкідливими програмами, несанкціонований доступ (НСД) до конфіденційної інформації, інформаційний моніторинг з боку конкуруючих структур, розвідувальних і спеціальних служб, дії державних структур і служб, що супроводжуються збиранням, модифікацією, вилученням і знищенням інформації, аварії, пожежі, техногенні катастрофи.

Усі перераховані види загроз (форми прояву) можна розділити на свідомі й несвідомі.

За даними Інституту захисту комп’ютерів (CSI) і ФБР більше 50% вторгнень – справа рук власних співробітників компаній. Що стосується частоти вторгнень, то 21% опитаних вказали, що вони зазнали рецидиви «напади». Несанкціонована зміна даних була найбільш частою формою

нападу і в основному застосовувалося проти медичних і фінансових установ.

Понад 50% респондентів розглядають конкурентів як можливе джерело «нападів». Найбільше значення респонденти надають фактам підслуховування, проникнення в інформаційні системи і «нападам», в яких зловмисники фальсифікують зворотну адресу, щоб перенаціліти пошуки на непричетних осіб. Такими зловмисниками найчастіше є скривджені службовці і конкуренти.

2.2 Несанкціонований доступ

Несанкціонований доступ включає у себе декілька типових вразливостей. Тому розглянемо деякі з них.

Аналізатор трафіку в мережах є основним прикладом. Необхідність аналізатора трафіку пояснюється тим, що занадто багато людей по мережі може потрапити до електронної пошти і використовувати призначені для користувача можливості в Інтернеті за рахунок його коштів, а аналізатор трафіку допомагає стежити за станом користувацького трафіку.

Аналізатор трафіку, або сніфер (від англ. To sniff – нюхати) – мережевий аналізатор трафіку, програма або програмно-апаратний пристрій, призначене для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку, призначеного для інших вузлів.

Перехоплення трафіку може здійснюватися: звичайним «прослуховуванням» мережевого інтерфейсу (метод ефективний при використанні в сегменті концентраторів (хабів) замість комутаторів (світчей), в іншому випадку метод малоефективний, оскільки на сніфер потрапляють лише окремі фрейми), підключенням сніфера в розрив каналу, відгалуженням (програмним або апаратним) трафіку і напрямком його копії на сніфер, через аналіз побічних електромагнітних випромінювань і відновлення таким чином трафіку, через атаку на канальному (MAC-spoofing) або мережевому рівні (IP-spoofing), що приводить до перенаправлення трафіку жертви або всього

трафіку сегменту на сніфер з подальшим поверненням трафіку в належну адресу.

На початку 1990-х широко застосовувався хакерами для захоплення призначених для користувача логінів і паролів, які в ряді мережевих протоколів передаються в незашифрованому або слабозашифрованному вигляді [3]. Широке поширення хабів дозволяло захоплювати трафік без великих зусиль у великих сегментах мережі практично без ризику бути виявленим.

Сніфери застосовуються як в благих, так і в деструктивних цілях. Аналіз пройденого через сніфер трафіку дозволяє наступне.

Виявити паразитний, вірусний і закільцований трафік, наявність якого збільшує завантаження мережевого обладнання та каналів зв’язку (сніфери тут малоефективні; як правило, для цих цілей використовують збір різноманітної статистики серверами і активним мережевим обладнанням і її подальший аналіз).

Виявити в мережі шкідливе і несанкціоноване ПО, наприклад, мережеві сканери, флудери, троянські програми, клієнти пірінгових мереж та інші (це зазвичай роблять за допомогою спеціалізованих сніферів – моніторів мережевої активності).

Перехопити будь-який незашифрований (а часом і зашифрований) призначений для користувача трафік з метою отримання паролів і іншої інформації.

Локалізувати несправність мережі або помилку конфігурації мережевих агентів (для цієї мети сніфери часто застосовуються системними адміністраторами).

Оскільки в «класичному» сніфері аналіз трафіку відбувається вручну, із застосуванням лише найпростіших засобів автоматизації (аналіз протоколів, відновлення TCP-потоку), то він підходить для аналізу лише невеликих його обсягів.

В порядку протидії атакам, виробники обладнання намагаються

прикрити найбільш «вузькі» місця в своїх маршрутизаторах (як правило, це процесор маршрутизації) різними засобами – спеціальними фільтрами (rACL), чергами, Шейпера (SPD) і т.д.

2.3 Зараження комп’ютера

Наслідки інфікування комп’ютера шкідливою програмою можуть бути як явними, так і неявними. До неявних зазвичай відносять зараження програмами, які за своєю суттю є вірусами, однак через помилки в своєму коді або нестандартному програмному забезпеченню цільового комп’ютера, шкідливе навантаження виконати не можуть. При цьому свою присутність в системі вони ніяк не виражають. Клас явних наслідків з ростом числа вірусів постійно збільшується. Можна виділити наступні дії.

Ряд вірусів після зараження комп’ютера шукають на жорсткому диску файли, що містять електронні адреси і без відома користувача починають розсилку по ним інфікованих листів.

Приклад: Sircam надсилається на заражений комп’ютер у вигляді файлу, прикріпленого до електронного листа. Ім’я вкладення розділено на дві частини: вірус і файл-приманки, ім’я вкладення створюється на основі вибраного файлу – наприклад, якщо вихідний файл називається photos.zip, ім’я вкладення – photos.zip.pif , фото .zip.lnk, фото .zip .bat або photos.zip.com [1]. Адреса одержувача вибирається з адрес, знайдених на зараженому комп’ютері, а текстові листи призначені для того, щоб вставити якомога менше вмісту та змусити адресата запустити створений файл. Від заражених комп’ютерів до конфіденційних файлів.

Крадіжка інформації, як правило, є крадіжкою конфіденційної інформації. Повідомлення можна надсилати електронною поштою.

Деякі віруси перевіряються без відома користувача і підключаються до різних платних сервісів, для яких на комп’ютері потрібно знайти особисту інформацію.

Приклад набору номера: після входу на комп’ютер вірус починає набирати міжнародні номери телефону для підключення до міжміських служб. Через деякий час користувач має величезний рахунок і неможливо довести, що він нікуди не дзвонив за важливих обставин.

Віддалене керування комп’ютером. Деякі віруси після вторгнення поширили дешеві інструменти для віддаленого зараження комп’ютера за допомогою Backdoor та доставили всі файли через Інтернет на вимогу зловмисника. Комп’ютер користувача був заражений віддаленим вірусом і, можливо, користувач не зможе нічого переглянути та перевірити основний процесор та оперативну пам’ять.

Ботнет – це група комп’ютерів, які централізовано контролюються одним зловмисником, кількість яких зросла в кілька разів і з кожним днем зростає.

Приклад – Bagle-virus – поширюється як вкладення електронної пошти. Адреса та ім’я вкладення відправника – будь-яка, тема – «Привіт», текст – «тест =)» Після зараження він копіюється на жорсткий диск з таким ім’ям yam bbeagle.exe і реєструє цей файл в операційній системі. Автозапуск спробує підключитися до кількох віддалених серверів. Такий вірус був виявлений 18 січня 2004 р., але за задумом автора, перестав розмножуватися через 10 днів, і незабаром з’явилася нова, більш досконала модифікація Bagle-ботнет – це один з найбільших і найвідоміших ботнетів [2].

2.4 Помилкові атаки

Створення фальшивого потоку (порушення автентичності) відноситься до сутності, яка намагається видати себе за іншу сутність.

З розвитком Інтернету та появою несанкціонованого доступу до файлів, документів та особистої інформації, користувачі почали використовувати всі програми своїх систем для захисту інформації. Іноді атаки відбуваються не від зовнішніх користувачів, наприклад, від збоїв в операційній системі.

Без розвитку сучасних інформаційних систем побудова будь-якої сучасної безпечної інформаційної системи практично неможлива, а без розвитку сучасних захисних систем – майже неможлива.

Як уже згадувалося в попередній статті, вказаний метод контролю порушень політики безпеки, тобто застосування засобів, що автоматизують роботу адміністратора, не може замінити фахівця з безпеки. Ці кошти можуть лише автоматизувати пошук деяких відомих вразливостей. Тому треба скептично ставитися до заяв фірм-постачальників, що пропонована ними система виявляє всі уразливості, гарантуючи тим самим стовідсоткову безпеку.

Перед фахівцями відділів захисту інформації та управлінь автоматизації постає завдання правильного вибору системи аналізу захищеності, що враховує технологію обробки інформації в організації.

2.5 DDoS-атака

DDoS-атака (Distributed Denial of Service attack) – комплекс дій, здатних повністю або частково вивести з ладу інтернет-ресурс. В якості жертви може виступати практично будь-який інтернет-ресурс, наприклад веб-сайт, ігровий сервер або державний ресурс. На даний момент практично неможлива ситуація, коли хакер поодинці організовує DDoS-атаку. У більшості випадків зловмисник використовує мережу з комп’ютерів, заражених вірусом. Вірус дозволяє отримувати необхідний і достатній віддалений доступ до зараженого комп’ютера [3]. Мережа з таких комп’ютерів називається ботнет. Як правило, в ботнетах присутній координуючий сервер. Вирішивши реалізувати атаку, зловмисник відправляє команду серверу, який в свою чергу дає сигнал кожному боту розпочати виконання шкідливих мережевих запитів.

Мотиви для здійснення DDoS-атак можуть бути найрізноманітнішими –від конкуренції до особистої неприязні. Основними причинами DDoS-атак можуть бути наступні.

Особиста неприязнь. Ця причина зустрічається досить часто. Деякий час назад незалежний журналіст-дослідник Брайан Кребс розкрив діяльність найбільшого сервісу по здійсненню замовних DDoS-атак – vDOS. Інформація була представлена в повних подробицях, що викликало арешт організаторів даного сервісу. У відповідь хакери організували атаку на блог журналіста, потужність якої досягла 1 Тбіт / с. Ця атака стала найпотужнішою в світі за всі роки.

Розваги. Організувати власні DDoS-атаки у наші дні легко. Цей тип атаки дуже неповний і не анонімний. На жаль, більшість людей, які вирішили вважати себе «хакерами», нічого не знають про такий підхід. Однак багато молодих людей часто проводять DDoS-атаки. Наслідки таких випадків досить різні.

Політичний опір (хакерська активність). DDoS-атака, запущена Omega Hacker у 1996 році, була однією з найперших соціальних атак. Він є членом альянсу злодіїв Omega Cult of the Dead Crew (CDC). Термін хактивізм широко використовується в ЗМІ для позначення соціально правильних кібератак. Типовими мережевими активістами є Anonymous і LulzSec.

Нечесна конкуренція. Такі причини зазвичай з’являються в індустрії ігрових серверів, але навіть у комерційній сфері такі атаки мали місце бути. Все через те, що це трапляється частіше, особливо різними способами.

Шантаж. У цьому випадку зловмисник попросить у потенційних жертв гроші, щоб запобігти нападу. Або перевищити цей ліміт. Жертвами цих атак часто стають великі організації. Наприклад, до 2014 року атакували Тинькофф Банк та IT-ресурс Habrahabr (найбільший торрент-трекер Rutracker.org).

Розслідування DDoS-атаки може відрізнятися залежно від сервера та його оточення. Багато ощадних організацій вибирають постачальників

захисту від шкідливих програм. Щоб уникнути подібних проблем, необхідно проконсультуватися з фахівцями в даній області.

Технічний прогрес розвивається, злочинці також не зупиняються, і вони роблять все можливе, щоб здійснювати витончені та більш агресивні атаки. Деякі з помітних атак наведені нижче.

Деякі з них можуть здатися незвичними за сучасними мірками, але в той час вони були дуже маштабними.

Пінг смерті. Метод атаки на основі команди ping. Ця атака стала відомою в 1990-х роках через недосконалість мережевих пристроїв. Корінь атаки полягає в тому, що пакет, який надсилається отримувачу, складається не із 64 байт, а із 65535. Через це відбувалася відмова в обслуговуванні завдяки переповненню мережевого стеку.

Атаки, які вплинули на стабільність мережі Інтернет. У 2013 році компанія Spamhaus була мішенню атак із потужністю більш ніж 280 Гбіт/с. Що ще цікаво, зловмисник використав веб-сервер DNS, що був майже повністю завантажений. Тоді мільйони користувачів скаржилися, що завантажити сторінку майже неможливо або вона відображається дуже повільно через проблеми з службою DNS.

Мережні атаки понад 1 Тбіт/с. У 2016 році зловмисники тестували пакетні атаки зі швидкістю 360 Мп/с і 1 Тбіт/с. Такі цифри стали рекордними за увесь час існування глобальної мережі.

3 МЕТОДИ ТА ЗАСОБИ БОРОТЬБИ З ВРАЗЛИВОСТЯМИ

3.1 Класифікація систем виявлення атак

Атака має три етапи. Першим кроком у підготовці є з’ясування передумов для нападу. Пошук і використання вразливостей на цьому етапі запускає атаку на другому етапі. На третьому етапі атака завершується, сліди приховуються тощо. Перший і третій кроки можуть бути нападом. Наприклад, пошук вразливостей за допомогою такого сканера безпеки, як SATAN, вважається атакою.

Традиційні механізми безпеки використовуються в брандмауерах, серверах аутентифікації, системах спільного доступу тощо. Вони працюють лише на другому етапі. Іншими словами, це насамперед засіб блокування, а не прогнозування атак. У більшості випадків він захищає від атак. І навіть якби вони заблокували одну атаку, набагато ефективніше було б заблокувати усі атаки, тобто усунути передумову для окупації.

Повна система інформаційної безпеки повинна працювати на всіх трьох етапах атаки. І на третьому, заключному етапі, важливіше забезпечити належний захист, ніж на перших двух. Адже тільки в цьому випадку можна реально оцінити шкоду, завдану «вдалою» атакою, а також розробити заходи, щоб не повторити спробу подібного.

Існує кілька способів виявлення, блокування та запобігання атак. Першим і найпоширенішим методом є виявлення тривалих атак. Цей метод використовується в «класичних» системах виявлення атак (наприклад, в системах безпеки в Інтернеті з RealSecure), брандмауерах тощо.

Однак недоліком такого підходу може бути можливість повторної реалізації атаки. Другий підхід – запобігти атакам ще до їх реалізації. Наприклад – шляхом пошуку вразливості, яка може бути використана для реалізації атаки, яка запобігає атаці до її початку. Нарешті, третій спосіб –

виявлення та запобігання повторному здійсненню. Отже, системи виявлення атак можна класифікувати за стадією атаки (рисунок 3.1).

Рисунок 3.1 – Системи виявлення атак

Система, яка працює на першому етапі атаки і виявляє вразливості в комп’ютерних системах, які використовуються зловмисниками. Інакше -. вам заборонено бути в класі виявлення атак, але ви не можете слідувати поясненням високого рівня. У фазі атаки така класифікація має сенс.

Система, яка працює на другій фазі атаки і може виявити атаку в процесі реалізації, тобто в режимі реального часу (або близько реального часу). Ці заходи вважаються системами виявлення атак у класичному розумінні цього терміну. Спосіб запуску атаки – як оманлива система.

Системи, що працюють на третій стадії виявлення та виявляють уже здійснені атаки. Ці системи можна розділити на два класи – системи для контролю цілісності, які знаходять зміни контрольованих пакетів, системи для аналізу реєстраційних журналів.

Крім цього, існує ще одна поширена класифікація систем виявлення порушення безпекової політики – за принципом реалізації: host-based, тобто, атаки, спрямовані на конкретний вузол мережі, і network-based, спрямовані на всю мережу чи сегмент мережі. Зазвичай, у цьому випадку, подальша

класифікація зупиняється. Однак системи класу host-based можна розділити ще на три підрівні:

- Application IDS (Intrusion Detection System), що виявляють атаки на конкретні програми;
- OS IDS, що виявляють атаки на операційні системи;
- DBMS IDS, що виявляють атаки на системи керування базами даних.

Виділення виявлення атак на системи управління базами даних (СУБД) в окрему категорію пов’язано з тим, що сучасні СУБД вже вийшли з розряду звичайних додатків і за своїми характеристиками і за складністю наближаються до операційних систем. Таким чином, класифікація систем виявлення атак за рівнем реалізації виглядає наступним чином (рис. 3.2):

Рисунок 3.2 – Атаки за рівнем реалізації

Можна помітити, що такий поділ відповідає рівням інформаційної системи підприємства.

3.2 Системи виявлення атак

Системи контролю цілісності – системи, які працюють за замкненим циклом, обробляючи файли, системні об’єкти та атрибути системних об’єктів

з метою отримання контрольних сум, потім вони порівнюють їх із попередніми контрольними сумами, відшукуючи зміни. Коли зміна виявлена, система надсилає повідомлення адміністратору, фіксуючи час, що відповідає ймовірному часу зміни. Якщо знову повернутися до етапів реалізації атаки, системи цього класу функціонують на третьому етапі, тобто вони можуть однозначно сказати, чи відбувалася атака (точніше зміна контрольованого об’єкта) чи ні.

Обманні системи. Зазвичай, коли йдеться про обман у сфері інформаційної безпеки, тут використовуються методи, які застосовують зловмисники, тобто лазівки для обходу використовуваних засобів захисту, чи крадіжки паролів і робота від імені авторизованого користувача або несанкціоноване використання модемів [5]. Обман може послужити гарною службою не тільки для зловмисників, але й для захисту корпоративних ресурсів. Існує безліч різних варіантів використання обману в корисних цілях: приховування, камуфляж, дезінформація.

Тією чи іншою мірою ці механізми використовують у практиці роботи відділів безпеки. Однак, як правило, ці механізми використовуються не для інформаційної, а для інших сфер безпеки (фізична, економічна і т.д.).

У сфері інформаційної безпеки найбільшого поширення набув перший метод – приховування. Яскравим прикладом використання цього методу для забезпечення інформаційної безпеки можна назвати приховування мережної топології за допомогою міжмережевого екрану. Прикладом камуфляжу є наступний приклад: кожна операційна система має притаманний тільки їй подання механізму ідентифікації користувача, різним кольором і типом шрифту, яким видається для запрошення, текстом запрошення та місцем його розташування. І, нарешті, як приклад дезінформації можна назвати використання заголовків (banner), які давали б зрозуміти зловмиснику, що атакована їм система нібито вразлива.

Робота систем 2 і 3 їх реалізують таким чином, що ці системи емулюють ті чи інші відомі вразливості, яких у реальності немає.

Використання засобів (deception systems), що реалізують камуфляж та дезінформацію, призводить до наступного.

1. Збільшення числа виконуваних порушником операцій та дій. Так як заздалегідь визначити, чи є виявлена порушником уразливість істинною чи ні, зловмиснику доводиться виконувати багато додаткових дій, щоб з'ясувати це. І навіть додаткові дії не завжди допомагають у цьому. Наприклад, спроба запустити програму підбору паролів (наприклад, Crack для Unix або L0phtCrack(LC) для Windows) (рис. 3.3) на сфальсифікований і неіснуючий насправді файл, призведе до марної витрати часу без будь-якого видимого результату. Нападник думатиме, що він не зміг підібрати паролі, тоді як насправді програма злому була просто обманута.

Рисунок 3.3 – L0phtCrack(LC) для Windows

2. Отримання можливості відстежити нападаючих. За той час, коли нападники намагаються перевірити всі виявлені вразливості, в тому числі фіктивні, адміністратори безпеки можуть простежити весь шлях до порушника чи порушників та вжити відповідних заходів.

Наприклад, в інформаційній системі використовують від 5 до 10 зарезервованих портів (з номерами від 1 до 1024). До них можна зарахувати

порти, відповідальні за функціонування сервісів HTTP, FTP, SMTP, NNTP, NetBIOS, Echo, Telnet тощо. Якщо обманні системи (наприклад, RealSecure компанії ISS) емулюють використання ще 100 і більше портів, робота нападника різко збільшується і зловмисник виявить не 5-10, а 100 відкритих портів. При цьому мало виявити відкритий порт, треба спробувати використовувати вразливості, пов’язані з цим портом. І навіть якщо нападник автоматизує цю роботу шляхом використання відповідних програмних засобів (Nmap, SATAN і т.д.), то кількість операцій, які він виконує, все одно істотно збільшується, що призводить до швидкого зниження продуктивності його роботи.

Інструменти аналізу безпеки. Системи аналізу безпеки, такі як сканери або системи безпеки, визначають слабкі місця. Вони можуть призвести до порушення політики. Результати аналізу засобів захисту є "моментальним знімком" статусу захисту Сімонстанів.

Технологія аналітики безпеки є ефективним способом реалізації політики безпеки мережі, перш ніж намагатися її зламати ззовні або всередині.

Одним із варіантів класифікації подібних систем може бути класифікація, що відображає стадії вторгнень, або може бути класифікація, що відображає етапи проведення атак.

Найнебезпечніші уразливості мереж, які можна виявити та усунути з великими зусиллями. При цьому вразливість продуктивності проекту або алгоритму, а отже, і його досконала реалізація (що в принципі неможливо) не знімає властиву вразливість. Наприклад, уразливість стеку протоколів TCP/IP.

Важливість слабкого місця другої категорії (слабого місця реалізації) полягає у виникненні помилок на етапі впровадження в програму або в апаратному забезпеченні правильної безпеки проекту або алгоритму. Ви можете легко визначити та застосувати цей тип уразливості, оновивши код,

який виконує або змінює вихідний код уразливого програмного забезпечення.

Остання причина виникнення вразливостей – помилки конфігурації програмного чи апаратного забезпечення. До них можна віднести, наприклад, доступний на вузлі сервіс Telnet, який не використовується, використання "слабких" паролів або паролів менше 6 символів, облікові записи (accounts) і паролі, зупинені за замовчуванням (наприклад, SYSADM або DBSNMP в СУБД Oracle) , і т.д. Виявити та виправити такі вразливості найпростіше.

Системи аналізу захищеності можуть бути класифіковані за типами вразливостей, що виявляються ними (рис.3.4), описаних вище.

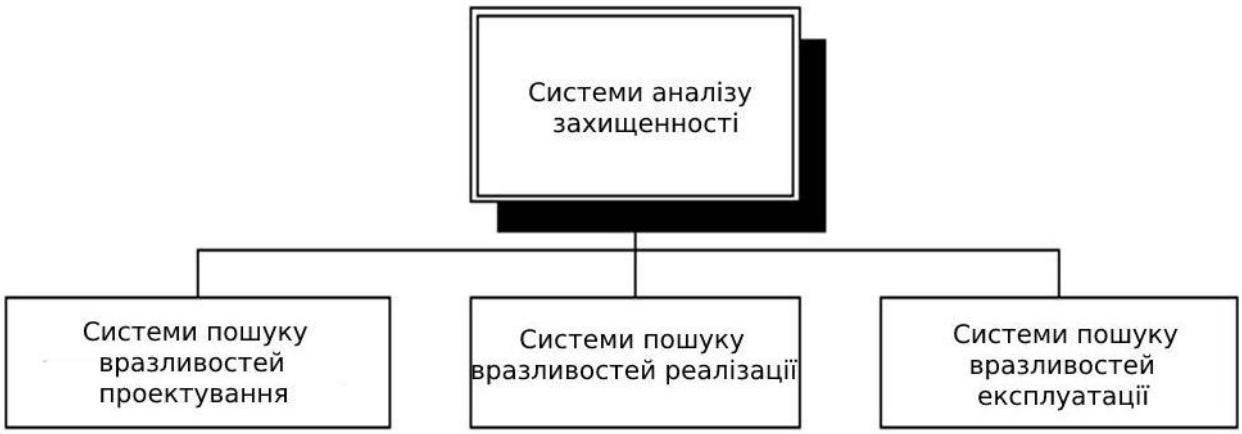

Рисунок 3.4 – Класифікація за типами вразливостей

Системи аналізу захищеності другого та третього класів набули найбільшого поширення серед кінцевих користувачів. Існує кілька додаткових класифікацій цих систем [7]. Наприклад, системи аналізу вихідного тексту і виконуваного коду програмно-апаратного забезпечення, що тестується, і т.д. Перші також застосовуються зазвичай під час сертифікації програмного забезпечення за вимогами безпеки. Найчастіше програмне забезпечення постачається в організації без вихідних текстів. Крім того, аналіз вихідних текстів вимагає високої кваліфікації від персоналу, що їх обслуговує.

Відсутність ефективних систем аналізу вихідних текстів не дозволяє проводити такий аналіз на якісному рівні. Саме тому великий інтерес викликають системи пошуку вразливостей у коді, що виконується, що є найпоширенішим підкласом системи імітації атак, які моделюють різні несанкціонований вплив на компоненти інформаційної системи. Саме ці системи здобули широку популярність у всьому світі через свою відносну простоту і дешевизну. За допомогою таких імітаторів виявляються вразливості ще до того, як їх буде використано порушниками для реалізації атак. До систем даного класу можна віднести SATAN, Internet Scanner, Cisco Secure Scanner і т.д.

Системи імітації атак з однаковим успіхом виявляють не тільки вразливість реалізації, але й вразливість експлуатації. Функціонувати системи аналізу захищеності, зокрема системи пошуку вразливостей реалізації та експлуатації, можуть на всіх рівнях інформаційної інфраструктури будь-якої компанії, тобто на рівні мережі, операційної системи, СУБД та прикладного програмного забезпечення. Найбільшого поширення набули додатки аналізу захищеності мережевих послуг і протоколів. Пов’язано це, насамперед, із універсальністю використовуваних протоколів. Вивченість та повсюдне використання таких стеків протоколів, як TCP/IP, дозволяють з високим ступенем ефективності перевіряти захищеність корпоративної мережі, що працює в даному мережному оточенні, незалежно від того, яке програмне забезпечення функціонує на вищих рівнях. Прикладом такої системи є Internet Scanner ISS. Другими за поширеністю є засоби аналізу захищеності операційних систем. Пов’язано це також з універсальністю та поширеністю деяких операційних систем (наприклад, UNIX та Windows). Однак, через те, що кожен виробник вносить в операційну систему свої зміни (яскравим прикладом є безліч різновидів ОС UNIX), засоби аналізу захищеності ОС аналізують насамперед параметри, характерні для сімейства однієї ОС. І лише деякі системи аналізують специфічні їй параметри. Прикладом такої системи є System Scanner ISS.

У аналізі безпеки застосовуються дві стратегії. Перша – пасивна реалізується лише на рівнях операційної системи, SUD та додатків. Якщо файли конфігурації та реєстру аналізуються на наявність неправильних параметрів, легкодоступних файлів паролів та інших об’єктів, що порушують політику. Другий актив включає систему аналізу на рівні мережі, яку можна використовувати для відтворення найбільш поширених сценаріїв атак і аналізу стратегій реагування на ці сценарії.

Однак не припускайте, що аналіз безпеки можна використовувати лише для перевірки несанкціонованого доступу до корпоративної мережі відкритого типу (наприклад, Інтернету). Ці системи можна використовувати для аналізу окремих сегментів, але з нижчим показником успіху. Ви можете використовувати систему аналізу безпеки для:

- оцінки рівня безпеки вашої організації;
- перевірки працездатності мережевого, системного та прикладного програмного та апаратного забезпечення;
- зовнішніх аудиторських та консалтингових фірм, які використовують інформаційні дослідження;
- для тестування та сертифікації програмного та апаратного забезпечення.

Оскільки нові вразливості продовжують з’являтися, бази даних аналізу безпеки необхідно постійно оновлювати, щоб ефективно їх ідентифікувати. В ідеалі не повинно бути розриву між появою інформації про вразливості з різних «хакерських» джерел і появою сигнатур баз даних системи виявлення. Однак між повідомленнями існує затримка в часі, незалежно від того, як часто оновлюється база даних уразливостей.

Існує два основних механізми, які сканери використовують для пошуку вразливостей. Сканер уразливостей (сканування) Nunia (приклад сканування).

Сканування – це пасивний аналітичний механізм, за допомогою якого сканер намагається визначити вразливість, не підтверджуючи фактично її

існування. Цей метод є найшвидшим і простим у реалізації. Цей метод називається «виведенням» у сенсі МКС. Цей процес працює з Cisco, щоб визначити відкриті порти на всіх мережевих пристроях і призначити сканований порт заголовка для кожного порту. Кожен отриманий заголовок порівнюється з таблицею правил, визначених мережею. На основі порівняння визначається наявність або відсутність слабких місць.

Тестування – активний механізм аналізу, що дозволяє перевірити, чи є вразливості в аналізованому ВНЗ. Перевірка здійснюється за допомогою моделювання атак з використанням перевірених уразливостей. У термінології МКС цей метод називається «перевіркою». Як частина даних Cisco, цей процес використовується в процесі сканування («логічний вихід») для сканування кожного мережевого пристрою. Цей процес також використовує інформацію про метод атаки для повного підтвердження підозрілих вразливостей і виявлення вразливостей, які не можуть бути виявлені іншими пасивними методами, такими як атаки відмови в обслуговуванні ("Відмова в обслуговуванні").

Фактично ці механізми реалізуються за допомогою наступних методів.

«Перевірка заголовка» (Banner Check) Цей механізм являє собою серію «сканування» перевірок, за допомогою яких можна зробити висновки про вразливості на основі інформації в заголовку запиту та відповіді сканера. Проаналізуйте заголовки сервера Sendmail або FTP, але пам’ятайте, що адміністратор змінив текст заголовка, який повертається для останнього запиту.

«Активне виявлення та аутентифікація». Це також відноситься до розділу «сканування». Однак він заснований на порівнянні впливу цифрового програмного забезпечення з відомими вразливими місцями. Аналогічно антивірусна система втручається і порівнює відскановане програмне забезпечення з антивірусними сигнатурами, що зберігаються в спеціальній базі даних. Варіант – це контрольна сума або дата програмного забезпечення

для сканування, реалізованого в сканері, що працює на рівні операційної системи.

Спеціалізовані бази даних (бази даних кібербезпеки в термінології Cisco) містять інформацію про вразливості та про те, як їх можна використовувати (атаки). Ці дані додаються до інформації про коригувальні дії, щоб зменшити ризики безпеки під час тестування. Ця база даних в основному використовується в системах аналізу безпеки та системах виявлення вторгнень. Принаймні Cisco і ISS.

Цей метод також досить швидкий, але важчий у реалізації, ніж основна перевірка.

«Перевірка на вразливість». Деякі вразливі місця не з’являються, доки їх не простимулювати. З цієї причини справжні атаки запускаються на підозрілі служби або хості. Тести використання моделюють реальні атаки для ефективнішого виявлення вразливостей у вузлах сканування (але з меншою швидкістю). Спонтанні атаки є більш надійним методом аналізу безпеки, ніж сканування ядра, і, як правило, більш надійні, ніж сканування активного виявлення.

Проте в деяких випадках не завжди вдається здійснити фальсифікаційні атаки. Ці ситуації можна розділити на дві категорії: ті, де перевірка призводить до відмови в обслуговуванні хоста або мережі, що аналізується, і ті, де вразливість спочатку непридатна для мережевих атак.

Багато вразливостей безпеки неможливо виявити, якщо службу або комп’ютер не заблоковано чи не зупинено під час сканування. У деяких випадках використання моделювання атак (наприклад, аналіз безпеки критично важливих серверів) недоцільно, оскільки відновлення продуктивності відключених елементів у корпоративній мережі може бути дорогим (матеріалом і часом) [9] . У таких випадках слід використовувати інші засоби керування, такі як активне зондування.

Однак деякі вразливості неможливо перевірити без вимкнення служби або комп’ютера. У цьому випадку ці елементи керування вимкнені, і

користувач може їх активувати. Наприклад, під час онлайн-сканування цій команді присвоюється спеціальна категорія «збій».

Більшість сканерів виконують перевірку безпеки на багатьох рівнях.

Знаходження інформацію в Інтернеті. Цей крок визначає всі активні пристрої в мережі та ідентифікує службу та демонів, які працюють на цих пристроях. Для безпечної системи сканування операційної системи пропустіть цей крок, оскільки на кожному вузлі, який потрібно сканувати, встановлено зручний носій для сканування системи.

Визначте потенційні вразливі місця. Сканер використовує наведену вище базу даних для порівняння зібраних даних з відомими вразливими місцями під час основного сканування або активного сканування аудіо. У деяких системах вразливості класифікуються за рівнем ризику. Наприклад, уразливості сканера поділяються на три рівні ризику: високий, середній і низький.

Однозначно обрана вразливість. Сканер використовує спеціальні методи та моделює конкретні атаки, щоб визначити, чи має вибраний вузол мережі вразливість.

Повідомлення. Автоматично видаляйте вразливі місця. Цей крок рідко використовується в онлайн-сканерах, але широко використовується сканерами (наприклад, системними сканерами). Однак цю функцію можна використовувати різними способами. Наприклад, System Scanner створює певні сценарії (сценарії відновлення), які адміністратори можуть запускати для усунення вразливостей [9]. Після створення цього сценарію буде створено інший сценарій для скасування змін. Це необхідно, якщо вузол перестає працювати належним чином після вирішення проблеми.

Можливість створення звітів для різних категорій спеціалістів. Як мінімум можна виділити три такі категорії: керівництво компанії, керівництво середньої ланки та технічні фахівці. У звітах першої категорії немає жодної технічної інформації про виявлені вразливості або атаки. Вони містять опис загального стану безпеки корпоративної мережі. Звіти другої

категорії можуть містити докладнішу технічну інформацію, наприклад, опис виявлених уразливостей або атак, але без вказівки заходів щодо їх усунення. До цієї категорії також належать звані порівняльні звіти (trend analysis), які показують тенденції у зміні рівня захищеності заданих вузлів корпоративної мережі. До останньої категорії звітів можна віднести технічні звіти, що містять не лише докладний опис кожної з виявлених проблем, але й рекомендації щодо їх усунення, а також посилання на додаткові джерела інформації. Такі категорії звітів прийняті, наприклад, в Internet Scanner та Cisco Secure Scanner.

Підтримка різних форматів створюваних звітів.

Якщо сканер не знаходить вразливостей на вузлі, що тестується, це не означає, що їх немає. Просто це залежить не тільки від сканера, а й від його оточення [10]. Наприклад, для Windows характерний такий випадок: сканер намагається дистанційно проаналізувати системний реєстр, однак у разі заборони на аналізованому вузлі віддаленого доступу до реєстру, сканер ніяких вразливостей не виявить.

Різні реалізації одного й того ж сервісу по-різному реагують на системи аналізу безпеки. Дуже часто на практиці можна побачити, що сканер показує вразливості, яких на вузлі, що аналізується, немає. Це стосується мережевих сканерів, які проводять дистанційний аналіз вузлів мережі. Віддалено визначити, чи існує насправді вразливість чи ні практично неможливо. У цьому випадку можна порекомендувати використовувати систему аналізу захищеності на рівні операційної системи, агенти якої встановлюються на кожен контрольований вузол та проводять всі перевірки локально.

Для вирішення цієї проблеми деякі компанії-виробники пішли шляхом надання своїм користувачам кількох систем аналізу захищеності, що працюють на всіх зазначених вище рівнях, – мережному, системному та рівні додатків. Сукупність цих систем дозволяє з високим ступенем ефективності виявити практично всі відомі вразливості. Наприклад, компанія Internet Security Systems пропонує сімейство SAFEsuite, що складається з чотирьох

сканерів: Internet Scanner, System Scanner, Security Manager та Database Scanner.

Компанія Cisco, що пропонує лише систему аналізу захищеності на рівні мережі, пішла іншим шляхом для усунення проблеми помилкового спрацьовування. Вона поділяє всі вразливості на два класи.

Потенційні – які складаються з перевірок заголовків і так званих активних "підштовхувань" (nudge) аналізованого сервісу чи вузла. Потенційна вразливість, можливо, існує в системі, але активні зондуючі перевірки не підтверджують цього.

Підтверджені – виявлені та існуючі на аналізованому хості.

Перевірки на потенційну вразливість проводяться через колекцію заголовків та використання "несильних підштовхувань". "Підштовхування" використовується для сервісів, які не повертають заголовки, але реагують на прості команди, наприклад, посилка команди HEAD для отримання версії сервера HTTP.

У деяких випадках є вразливості, що важко виявляються або зовсім не виявляються через мережу. Наприклад, перевірка "слабкості" паролів, які використовують користувачі та інші облікові записи. У разі використання мережного сканера вам знадобиться багато часу на віддалену перевірку кожного облікового запису. У той же час, аналогічна перевірка, що здійснюється на локальному вузлі, проводиться на декілька порядків швидше. Іншим прикладом може бути перевірка файлової системи сканованого вузла. У багатьох випадках її не можна здійснити дистанційно.

Переваги сканування лише на рівні ОС криються у прямому доступі до низькорівневих можливостей ОС хоста, конкретних сервісів і деталей конфігурації. Тоді як сканер мережного рівня імітує ситуацію, яку міг би мати зовнішній зловмисник, сканер системного рівня може розглядати систему з боку користувача, що вже має доступ до аналізованої системи та має обліковий запис [11]. Це найбільш важлива відмінність, оскільки

мережевий сканер за визначенням не може надати ефективного аналізу можливих ризиків діяльності користувача.

Багато сканерів використовують більш ніж один метод перевірки однієї і тієї ж уразливості або класу вразливостей. Однак у разі великої кількості перевірок використання кількох методів пошуку однієї вразливості привносить свої проблеми. Пов’язано це зі швидкістю сканування.

Не всі перевірки, розроблені в лабораторних умовах, працюють так, як повинні. Навіть незважаючи на те, що ці перевірки тестуються, перш ніж будуть внесені до остаточної версії сканера. На це можуть впливати деякі фактори:

- особливості конфігурації системи користувача;
- спосіб, яким було скомпільовано аналізований демон або сервіс;
- помилки віддаленої системи.

У таких випадках автоматична перевірка може пропустити вразливість, яка легко виявляється вручну і може бути широко поширена в багатьох системах. Перевірка заголовка разом із активним зондуванням у разі допоможе визначити підозрілу ситуацію, сервіс чи вузол. І хоча вразливість не виявлено, це не означає, що її не існує.

3.3 Заходи безпеки під час використання протоколів TCP/IP

Фільтрація на маршрутизаторі. Фільтри на маршрутизаторі, що з’єднують мережу підприємства з Інтернетом, застосовуються для заборони пропуску датаграм, які можуть бути використані для атак як на мережу організації з Інтернету, так і зовнішні мережі зловмисником, що знаходиться всередині організації.

Слід зазначити, що більш безпечним та керованим рішенням, ніж фільтрація того чи іншого TCP-трафіку наступного від або до комп’ютера користувача є робота користувачів через проксі-сервери. Проксі-сервер перебирає функції надання користувачеві необхідного сервісу і зв’язується з

необхідними хостами Інтернету. Користувач взаємодіє лише з проксі-сервером і не потребує коннективності з Інтернетом. Таким чином, маршрутизатор, що фільтрує, дозволяє проходження TCP-сегментів певного типу тільки від або до проксі-сервера. Переваги цього рішення наступні.

Проксі-сервер знаходиться під контролем адміністратора підприємства, що дозволяє реалізовувати різні політики для диференційованого управління доступом користувачів до сервісів і ресурсів Інтернету, фільтрації даних (захист від вірусів, цензура тощо), кешування.

З точки зору Інтернету від імені всіх хостів користувача підприємства діє один проксі-сервер, тобто є тільки один потенційний об’єкт для атаки з Інтернету, а безпеку одного проксі-сервера, легше забезпечити, ніж безпеку безлічі комп’ютерів [12].

Аналіз мережевого трафіку. Аналіз мережевого трафіку проводиться для виявлення атак, здійснених зловмисниками, що знаходяться як в мережі організації, так і в Інтернеті.

Захист маршрутизатора. Заходи щодо захисту маршрутизатора проводяться з метою запобігання атакам, спрямованим на порушення схеми маршрутизації датаграм або захоплення маршрутизатора зловмисником.

Захист хоста. Заходи захисту хоста проводяться для запобігання атак, мета яких – перехоплення даних, відмова в обслуговуванні, або проникнення зловмисника в операційну систему.

Превентивне сканування. Адміністратор мережі повинен знати та використовувати методи та інструменти зловмисника та проводити превентивне сканування мережі організації для виявлення слабких місць у безпеці до того, як це зробить зловмисник. Для цієї мети є також спеціальне програмне забезпечення – сканери безпеки.

Загальні заходи щодо підвищення безпеки мережі. Оперативне встановлення виправлень для програм (Patching). Системні адміністратори повинні захищати найважливіші свої системи, оперативно встановлюючи виправлення програм на них. Тим не менш, встановити виправлення для

програм на всіх хостах у мережі важко, оскільки виправлення можуть з’являтися досить часто. В цьому випадку треба обов’язково вносити виправлення до програм на найважливіших хостах.

Виявлення вірусів та троянських коней. Для максимальної ефективності вони мають бути встановлені на всіх комп’ютерах у мережі. На встановлення антивірусних програм на всіх комп’ютерах і регулярне оновлення антивірусних баз в них може витрачатися досить багато часу – але інакше цей засіб не буде ефективним. Користувачам слід показувати, як їм самим робити ці оновлення, але при цьому не можна повністю покладатися на них.

Окрім звичайної антивірусної програми на кожному комп’ютері вони потрібні для сканування додатків для електронних листів на поштовому сервері. Таким чином, можна виявити більшість вірусів до того, як вони досягнуть машин користувачів.

Міжмережеві екрани – найважливіший засіб захисту мережі організації. Вони контролюють мережевий трафік, що входить до мережі та виходить із неї. Міжмережевий екран може блокувати передачу до мережі будь-якого виду трафіку або виконувати ті чи інші перевірки іншого виду трафіку. Добре сконфігований міжмережевий екран може зупинити більшість відомих комп’ютерних атак.

Хакери часто використовують маловідомі вразливі місця в комп’ютерах для того, щоб вкрасти файли із зашифрованими паролями. Потім вони використовують спеціальні програми для відкриття паролів, які можуть виявити слабкі паролі у цих зашифрованих файлах. Хоча цей засіб використовується зловмисниками, він буде також корисним і системним адміністраторам, щоб своєчасно виявити слабкі паролі.

Шифрування. Атаки часто проникають до мережі за допомогою прослуховування мережного трафіку в найважливіших місцях та виділення з нього імен користувачів та їх паролів. Тому з’єднання з віддаленими машинами, які захищаються за допомогою пароля, повинні бути

зашифровані. Це особливо важливо, якщо з’єднання здійснюється через Інтернет або з важливим сервером. [14] Є ряд комерційних та безкоштовних програм для шифрування трафіку TCP/IP (найбільш відомий SSH).

Сканери вразливих місць. Це програми, які сканують мережу у пошуках комп’ютерів, уразливих до певних видів атак. Сканери мають велику базу даних уразливих місць, яку вони використовують під час перевірки того чи іншого комп’ютера на наявність у нього вразливих місць.

Грамотне конфігурування комп’ютерів щодо безпеки. Програми для пошуку підключених модемів. Для пошуку підключених модемів атакуючі можуть використовувати програми дзвінків великої кількості телефонних номерів. Оскільки користувачі зазвичай конфігурують свої комп’ютери самі, вони часто виявляються погано захищеними і дають можливість для організації атаки на мережу. Системні адміністратори повинні регулярно використовувати програми для перевірки телефонних номерів своїх користувачів та виявлення налаштованих подібним чином комп’ютерів.

Рекомендації з безпеки (security advisories). Рекомендації з безпеки – це попередження, що публікуються групами по боротьбі з комп’ютерними злочинами та виробниками програм про нещодавно виявлені вразливі місця. Рекомендації зазвичай описують найсерйозніші загрози, що виникають через ці вразливі місця і тому займають мало часу на читання, але є дуже корисними. Вони описують загрозу і дають досить конкретні поради про те, що потрібно зробити для усунення вразливого місця. Двома найкориснішими є рекомендації, які публікує група боротьби з комп’ютерними злочинами CIAC і CERT.

Засоби виявлення атак (Intrusion Detection). Системи виявлення атак оперативно виявляють комп’ютерні атаки. Вони можуть бути встановлені за міжмережевим екраном, щоб виявляти атаки, що організуються зсередини мережі. Або вони можуть бути встановлені перед екраном між мережею, щоб виявляти атаки на міжмережевий екран. Додатки можуть мати різноманітні можливості.

Засоби виявлення топології мережі та сканери портів. Ці програми дозволяють скласти повну картину того, як влаштована ваша мережа і які комп'ютери працюють, а також виявити всі сервіси, які працюють на кожній машині. Атакуючі використовують ці засоби для виявлення вразливих комп'ютерів та програм на них.

Системні адміністратори повинні використовувати ці засоби для спостереження за тим, які програми та на яких комп'ютерах працюють у їхній мережі. З їх допомогою можна виявити неправильно налаштовані програми на комп'ютерах і встановити виправлення на них.

Інструкції щодо дії у критичних ситуаціях. У кожній мережі, незалежно від того, наскільки вона безпечна, відбуваються будь-які події, пов'язані з безпекою (можливо навіть помилкові тривоги). Співробітники організації повинні знати, що потрібно робити в тому чи іншому випадку.

Політика безпеки. Організації повинні написати безпекову політику, в якій визначався б очікуваний рівень захисту, який повинен бути скрізь однаково реалізований.

Найважливішим аспектом політики є вироблення єдиних вимог щодо того, який трафік повинен пропускатися через міжмережні екрани мережі. Також політика повинна визначати, як і які засоби захисту (наприклад, засоби виявлення атак або сканери вразливих місць) повинні використовуватися в мережі. Для досягнення єдиного рівня безпеки політика повинна визначати стандартні безпечні конфігурації різних типів комп'ютерів.

Тестування міжмережевих екранів та WWW-серверів на стійкість до спроб їх блокування. Атаки на блокування комп'ютера поширені в Інтернеті. Атакуючі постійно виводять із ладу WWW-сайти, перевантажують комп'ютери або переповнюють мережі безглуздими пакетами. Мережі, які дбають про безпеку, можуть організувати атаки проти себе самі, щоб визначити, які збитки може бути завдано їм [13].

4 ПРАВИЛА ТА МЕТОДИ ДЛЯ БОРОТЬБИ З ВРАЗЛИВОСТЯМИ

4.1 Політика безпеки

Для політики безпеки мережі очікується, що кожна організація після проведення вичерпного дослідження розробить політику на основі різних факторів. Однак політика підлягає змінам, корегуванням, оскільки з’являються нові технології та інші передові технології стають фінансово можливими. Хороша політика може містити наступні компоненти.

Обсяг і повноваження – повинні включати, хто фінансує та санкціонує політику, а також тих, на кого вона безпосередньо впливає.

Політика доступу – визначає прийнятні правила доступу для персоналу управління, обслуговуючого персоналу мережі та користувачів. Вона також визначає конкретні привілеї та обов’язки, що стосуються різних категорій користувачів мережі. Визначена політика повинна охоплювати процедури модифікації програмного забезпечення, налаштування параметрів ОС, додавання програмного забезпечення до систем і, що найважливіше, введення нових пристроїв до мережі. Важливі елементи політики доступу можуть бути включені як частина політики мережі.

Політика прийнятного використання – вкажіть очікувану поведінку користувачів і визначте технології, які будуть включені, такі як мобільні телефони, пейджери, комп’ютери тощо.

Політика бездротового доступу – визначає обставини, за яких бездротовий пристрій можна використовувати в мережі компанії.

Політика аутентифікації – це більш розширена політика паролів, яка визначає політику локальних паролів доступу та надає директиви для процесу віддаленої автентифікації.

Заява про доступність – вказує, що користувачі повинні очікувати щодо доступності ресурсу. У ньому мають бути описані відомі ризики, проблеми

відновлення та резервування. Також має бути включена контактна інформація для повідомлення про несправності мережі або системи.

Політика безпеки комутаторів і маршрутизаторів – пояснює, як мають бути налаштовані маршрутизатори та комутатори, які підключаються до виробничої мережі.

Антивірусна політика – визначає інструменти, які потрібно використовувати, і спосіб їх реалізації.

Політика обслуговування мереж та IT-систем – визначає, наскільки зовнішньому та внутрішньому персоналу дозволено обробляти технологію компанії та мати доступ до неї. Політика повинна визначати, чи дозволено дистанційне обслуговування технології та за яких обставин. У ній також має бути детально описано, чи можна здійснити аутсорсинг, [14] як ним керувати та законний процес, якого слід дотримуватися, якщо це необхідно.

Політика повідомлення про порушення – класифікує порушення на ті, про які слід повідомити, і вказує особу, якій вони повідомляються. Політика повинна містити вказівки щодо поводження із зовнішніми інцидентами безпеки, особу, яка реагує на інцидент, та механізм реагування на ситуації залежно від точки контакту.

Компанія не надає доступ до мережі через незахищений бездротовий зв’язок. Лише тим системам з винятковим винятком або тим, які відповідають вимогам цієї політики, буде дозволено підключатися до мережі.

Область застосування. Політика поширюється на кожен пристрій, підключений до внутрішньої мережі. Це включає всі пристрої бездротового зв’язку, здатні передавати пакетні дані.

Ось що має робити кожна бездротова мережа, щоб відповідати цій політиці:

- підтримувати зареєстровану та відстежувану апаратну адресу, тобто MAC-адреси;
- підтримувати апаратне шифрування "точка-точка" мінімум 56 біт;
- підтримка надійної автентифікації користувача, яка перевіряється

щодо зовнішніх баз даних, таких як RADIUS, TACAS+ або щось подібне;

- примусове виконання.

Порушення цих правил будь-яким працівником тягне за собою дисциплінарні стягнення, аж до звільнення з роботи.

Аутентифікація користувача – має передбачати методологію перевірки бездротової системи як законного користувача окремо від ОС або комп’ютера, що використовується.

Історія редакцій. Замінюватиме посилання лише клієнт або компанія. Ця політика стандартизована, щоб спростити додавання унікальних політик до організації або тих, які ідеально підійдуть.

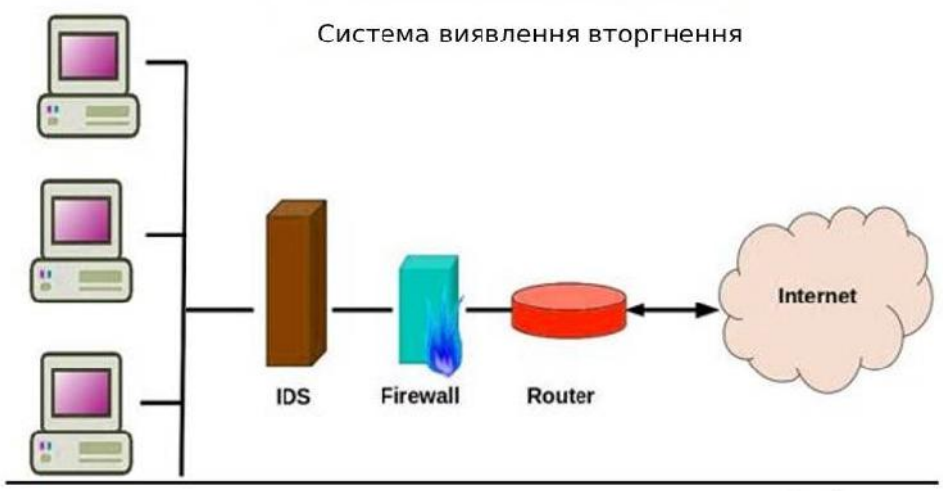

Рисунок 4.1 – IDS

Моніторинг політики безпеки мережі. Комплексна політика безпеки мережі повинна передбачати критерій моніторингу мережі як рутинної діяльності. Основна мета моніторингу мережі полягає в тому, щоб вказати на слабкі місця, які можуть бути використані хакерами. Насамперед, слід запровадити моніторинг мережі, щоб переконатися, що користувачі мережі дотримуються політики.

Процес моніторингу може бути таким же простим, як організований збір і перегляд файлів журналів, створених мережею в нормальному режимі

роботи. Поява кількох невдалих входів в систему може свідчити про те, що особа (користувач) потребує подальшого навчання або зловмисної спроби злому. Складні розширені системи розміщені в кінці спектру для моніторингу мережевого трафіку. Такі пристрої, як IDS (рис. 4.1), використовуються для пошуку ознак, таких як підписи, які сигналізують про те, що щось не так. У разі червоного прапорця датчик IDS повідомляє консоль керування IDS директора, яка ініціює процес пом’якшення, щоб уникнути атаки. Заходи пом’якшення можуть включати створення списку в брандмауері або маршрутизаторі, щоб чітко блокувати контакти з цього джерела.

4.2 Висунута політика безпеки в комп’ютерних мережах

Немає єдиного остаточного механізму для повного захисту мережі, оскільки практично будь-яка система безпеки може бути скомпрометована або підірвана. Вторгнення можуть бути ззовні або зсередини. Тому найефективнішим способом захисту мережевої системи може бути впровадження різних рівнів бар’єрів безпеки. Це змушує зловмисника обійти більше однієї системи, щоб отримати доступ до критичних активів цілі.

Першим основним кроком у застосуванні політики безпеки є визначення конкретної політики, яку ви прагнете забезпечити. Заходи безпеки впроваджуються, щоб обмежити персонал у їх повсякденній діяльності. У деяких випадках ці заходи виявляються «надзвичайно» обмежуючими, через що виникає спокуса посилити правила безпеки. Ці мережеві заходи впроваджуються для оптимізації роботи співробітників у звичайних умовах і, отже, мають бути чітко визначені. Вони дають рекомендації щодо того, як реагувати на виникнення аномалій. У цьому контексті наведений нижче розділ пояснює, як кожен принцип заходів безпеки мережі має застосовуватися для захисту систем та іншої цінної інформації.

Безпека пристрою. Розробляючи інфраструктуру безпеки вашої мережі, вам доведеться визначити пріоритети різних сегментів мережі відповідно до їх вимог безпеки. Наприклад, деякі сервери будуть доступні та відкриті для всіх, тоді як інші будуть обмежені для певної частини співробітників. Таким чином, для забезпечення ефективної безпеки для різних підрозділів і категорій, ви встановлюватимете бар'єри, які можуть обмінюватися лише певними типами трафіку у вигляді приватних мереж, напівприватних мереж і публічних мереж. Такі обмеження для різних сегментів мережі можуть бути засновані на таких пристроях, як комутатори, шлюзи, мости та маршрутизатори, які можуть контролювати вхідний і вихідний потік пакетів у різні сегменти.

Кожен пристрій зв'язку та моніторингу, розгорнутий у мережевій системі, має бути належним чином налаштований відповідно до вимог політики. Доступ має ґрунтуватися на призначених користувачам привілеях. Крім того, вбудоване програмне забезпечення або операційні системи розгорнутого пристрою повинні бути сучасними. Крім зазначених вище вказівок, у контексті безпеки пристрою слід також враховувати наступні заходи.

Виправлення та оновлення безпеки слід застосовувати регулярно, щойно постачальники випустять їх. Усі служби, які не використовуються, слід вимкнути.

Кожному співробітнику слід призначити NDA про нерозголошення інформації про пристрої, розгорнуті в межах периметра.

Компанія повинна підтримувати ACL для регулювання трафіку UDP і TCP.

Доступ до Інтернету. Політики, що стосуються доступу до Інтернету, включають всі порти, які автоматично блокують усі веб-сайти, визнані невідповідними, особливо ті, що стосуються платформ соціальних мереж. Доступ до Інтернету повинен ґрунтуватися на характері роботи користувача. В організації Інтернет і мережа – це те саме, що вони з'єднують важливі

активи організації, такі як розділи облікових записів, сервери тощо. Перш ніж користуватися, доступ до Інтернету слід ретельно відстежувати та відповідним чином фільтрувати.

Політика VPN. VPN розроблено для використання виключно на комп’ютерах, що належать організації, оскільки він забезпечує спосіб захисту даних, коли вони передаються через ненадійну мережу. Кожен віддалений доступ до корпоративної мережі має здійснюватися через стандартну операційну систему разом із VPN з дійсним корпоративним схваленням.

Рисунок 4.2 – Політика VPN

Віддалений доступ до комп’ютерів компанії з дому через Інтернет має бути заборонений, щоб уникнути зловмисного доступу. L2TP з IPSec слід застосовувати для забезпечення належного захисту для тих, хто намагається отримати доступ до комп’ютерів організацій віддалено. Брандмауери також мають бути налаштовані на фільтрацію клієнтського трафіку.

Політика портового зв’язку. Лише основні служби, такі як HTTP, слід залишати відкритими, навіть якщо вони не використовуються. В іншому випадку всі інші порти, вихідні чи вхідні, повинні бути суворо заблоковані для непотрібних служб. Наявність кількох непотрібних відкритих портів збільшує ймовірність злому в системі. Тому порти, підключені безпосередньо

до Інтернету, повинні бути обмежені або позначені як порти у вхідному з’єднанні або використовувати лише авторизовані послуги зв’язку.

Політика щодо бездротової локальної мережі. Ефективна мережева політика повинна мати вказівки щодо належної автентифікації користувачів, механізм відстеження аномалій у бездротовій локальній мережі та методику відповідної заміни WEP, щоб зупинити можливе зловживання бездротовою мережею. Для цілей шифрування слід використовувати заходи безпеки 802.11, такі як CCMP, TKIP тощо. Нижче наведено список деяких підозрілих подій у бездротовій мережі, які завжди слід враховувати для виявлення вторгнень:

- MAC-адреса, яка змінюється випадково;
- закрита мережа з кількома неправильними SSID;
- кадри маячків із небажаної точки доступу;
- дубльовані MAC-адреси на кадрах.

Політика віддаленого підключення. Оскільки все більше організацій збільшують мережеві зв’язки між своїми співробітниками, щоб підвищити продуктивність, порушення даних стають все більш масовими. У більшості випадків зловмисник бере на себе сеанс, блокуючи віддаленого користувача та використовуючи його облікові дані для доступу до мережі компанії, як якщо б він був віддаленим хостом у мережі. Неправильне управління конфіденційною інформацією віддалених користувачів також може призвести до експлуатації системи. Лише авторизованим користувачам слід надавати прямий доступ до критичного сервера організації, тоді як інші мають бути строго в обмеженому режимі через утиліту SSH або віддалений вхід.

Політика правил брандмауера. Кожен раз, коли користувач підключається до незахищеної відкритої мережі, він відкриває ворота доступу для потенційних зловмисників, щоб проникнути в систему. У таких випадках може знадобитися використання брандмауерів на кінці точки підключення, оскільки вони захищають засоби зв’язку та приватні мережі.

Наведені нижче вказівки повинні стати в нагоді під час розгортання брандмауера в різних сегментах мережі.

Для доступу до виділеного сервера ідентифікація сервера приховується за допомогою брандмауера проксі між віддаленим користувачем і виділеним сервером.

У разі фільтрації трафіку на основі порту призначення та джерела/IP-адреси слід встановити брандмауер з фільтрацією пакетів, оскільки він також збільшує швидкість передачі.

Однак, коли швидкість передачі не важлива, тоді конфігурація перевірки таблиці станів може бути доречною, оскільки вона динамічно перевіряє з’єднання та пересилає пакет.

Якщо необхідно забезпечити додаткові заходи безпеки для внутрішньої мережі організації, NAT повинен доповнювати брандмауер.

Нарешті, ви можете застосувати фільтрацію IP-пакетів, якщо потрібен більш високий рівень регулювання, крім запобігання зв’язку між IP-адресою та вашим сервером.

Політика вторгнення. Для крайньої лінії захисту ідентифікатори мають бути розміщені для моніторингу аномалій та виявлення несанкціонованого доступу, оскільки антивірусних заходів та заходів брандмауера недостатньо. Крім того, співробітники служби безпеки або менеджери з ризиків повинні регулярно перевіряти систему на предмет будь-якої підозрілої діяльності. Щоб пом’якшити підвищені привілеї, змінені дозволи, неналежні права аудиту, неактивні користувачі, зміну реєстру та багато іншого, необхідно використовувати Advance Antivirus із вбудованим IPS/IDS. Програмне забезпечення IDS налаштовується через ОС, тоді як перехоплення IDS для програмного забезпечення розгортається як апаратна програма в основному через причини продуктивності.

Політика проксі-сервера. Проксі-сервери використовуються для оборонних і наступальних цілей і зазвичай знаходяться між користувачем і сервером.

Політика безпечного зв’язку. Дані, що передаються в незашифрованому вигляді через різні канали, такі як маршрутизатори та комутатори в мережі, схильні до таких атак, як SYN flooding, викрадення сеансу, спуфінг та перехоплення. Ви не можете повністю контролювати пристрій, через який передаються дані. Проте, принаймні, ви можете захистити самі дані від злому або канал передачі від того, щоб дані були доступними до певного рівня або ступеня. Щоб протистояти таким атакам, ви можете використовувати тактику шифрування, наприклад SSh, IPsec, SSL і TLS, оскільки вони можуть віртуально шифрувати будь-який тип зв’язку, наприклад HTTP, IMAP, POP, FTP і POP3. Це тому, що пакети SSL можуть легко переміщатися через NAT-сервери, встановлювати брандмауери та будь-який пристрій у мережі, якщо відповідні порти залишаються відкритими на пристрої. Якщо є потреба передати дані, цінні для вашої організації, вам потрібно вжити конкретних ініціатив. Нижче наведено деякі з них.

- переконайтеся, що атаки MITM не впливають на дані, що передаються;

- переконайтеся, що будь-яка неавторизована особа між джерелом і сервером не порушить канал передачі;

- ідентифікація комп’ютерів і людей, які надсилатимуть пакети, має бути аутентифікована.

Політика DMZ. Сервери або системи, такі як електронна пошта, бази даних, веб-сервери тощо, які потребують доступу до загальнодоступного Інтернету, мають бути розгорнуті в певній підмережі, яка відокремлюється зовні від внутрішньої. Це робиться для того, щоб уникнути атак з боку чорних капелюхів, оскільки доступ до публічних доменів є легким.

Основною метою безпеки мережі є забезпечення конфіденційності, доступності та цілісності кожного активу в межах периметра мережі.

ВИСНОВКИ

В результаті виконання даної роботи був проведений аналіз структури комп’ютерних мереж, їх топології, вразливостей.

Детально досліджені існуючі методи вирішення та запобігання вразливостей. Проведений аналіз існуючих програмних та апаратних засобів, які сприяють цьому.

У роботі були вивчені комп’ютерні мережі і їх класифікації. Представлені найбільш використовувані топології – «шина», «зірка», «кільце» і ін. Особливу увагу було приділено загрозам безпеки інформації в комп’ютерних мережах і засобів захисту від них. Основними засобами захисту мереж є протоколювання і аудит, кошти архівації, екранування трафіку, ідентифікація і аутентифікація.

Розглянуто найпоширеніші антивірусні програми, такі як Kaspersky Internet Security, Dr.Web, Norton Antivirus, Avast. Різновиди комп’ютерних вірусів і способи їх шкідливого впливу на роботу системи – файлові віруси, різновиди троянських програм, шпигунське програмне забезпечення, макровіруси, черви, шифрувальники шкідливих програм. Наведені приклади вразливостей та висунуто методи боротьби з ними. Висунута власна політика безпеки для комп’ютерних мереж.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Алгоритмы преобразования и классификации трафика для обнаружения вторжений в компьютерные / Большев Александр Константинович. - С.-Петерб.: Гос. электротехн. ун-т (ЛЭТИ), 2011.- 311 с.

2. Асанович, В. Я. Информационная безопасность: анализ и прогноз информационного воздействия / В.Я. Асанович, Г.Г. Маньшин. – Минск: Амалфея, 2006. – 203 с.

3. Баранова, О.А. Методи та засоби боротьби з вразливостями комп‘ютерних мереж / О.А. Баранова // ІІ Міжнародна студентська наукова конференція «Глобалізація наукових знань: міжнародна співпраця та інтеграція галузей наук», 22 жовтня 2021. – Зб. матеріалів форуму. – Т. 1. – Біла Церква − с. 98-99.

4. Безобразов, С. В. Алгоритмы искусственных иммунных систем и нейронных сетей для обнаружения компьютерных вирусов: автореферат диссертации на соискание ученой степени кандидата технических наук: 05.13.19 / Безобразов Сергей Валерьевич; Белорусский государственный университет. – Минск, 2009. – 22 с.

5. Бирюков, А. А. Информационная защита. Защита и нападение/ А.А. Бирюков. – Москва: ДМК Пресс, 2012. – 474 с.

6. Богуш, В. А. Компьютерные сети: курс лекций/ А.В. Богуш, И.С. Терех, Министерство образования Республики Беларусь, учреждение образования Белорусский государственный университет информатики и радиоэлектроники. – Минск: БГЭУ, 2006. – 104 с.

7. Бони, Джеймс. Руководство по Cisco IOS для профессионалов = Cisco IOS in a Nutshell: / Дж. Бони; [пер. с англ. Е. Шикарева]. - [2-е изд.]. - Москва: Русская Редакция; Санкт-Петербург: Питер, 2007. – 784 с.: ил.

8. Борщев, Б. В. Интернет и информационная среда / Б. В. Борщев// Научно-техническая информация. Информационные процессы и системы. –

2009. – № 2. – С. 1-14.

9. Брандман, Э. М. Глобализация и информационная безопасность общества / Э.М. Брандман // Философия и о-во. – 2006. – № 1. – С. 31–41.

10. Буза, М. К. Архитектура компьютеров: учебник для студентов специальностей "Информатика", "Прикладная математика", "Вычислительные машины, системы и сети" учреждений, обеспечивающих получение высшего образования / Михаил. Константинович. Буза. – Минск: Новое знание, 2007. - 558 с. – Библиогр.: с. 552-553.

11. Галатенко, В. А. Основы информационной безопасности/ В.А. Галатенко. – М.: Изд-во "Интернет-университет информационных технологий – ИНТУИТ.ру", 2003. –280 с.: ил.

12. Гатчин, Ю. А. Основы информационной безопасности: учебное пособие /Ю.А. Гатчин, Е.В. Климова – СПб: СПбГУ ИТМО, 2009. – 84 с.

13. Гатчин, Ю. А. Теория информационной безопасности и методология защиты информации / Ю.А. Гатчин, В. В. Сухостат. – СПб.: СПбГУ ИТМО, 2010. – 98 с.

14. Гергель, А. В. Компьютерные сети и сетевые технологии: учеб. метод. пособие/ А. В. Гергель. – Н. Новгород: Изд-во ННГУ, 2007. – 107 с.

15. Гладкий, А. А. Безопасность и анонимность работы в Интернете. Как защитить компьютер от любых посягательств извне / Алексей Александрович Гладкий. – Москва: Литрес, 2012. – 320 с.