ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет
радіоелектроніки
Кафедра ЕОМ

NURE
Харківський національний університет радіоелектроніки

Методи та засоби боротьби з вразливостями комп'ютерних мереж

Студент групи КСМм-20-1
Баранова Оксана Андріївна

Керівник:
ст. викл. ЕОМ
Єрьоміна Н.С.

Харків 2021

Мета та задачі проекту

NURE
Харківський національний університет радіоелектроніки

Мета: аналіз вразливостей у комп'ютерних мережах та аналіз засобів та методів боротьби з ними.

Зміст:

- **Розглянути поняття комп'ютерних мереж та їх типів у наші дні.**
- **Розглянути види вразливостей у комп'ютерних мережах.**
- **Розглянути приклади реалізації вразливостей.**
- **Проаналізувати методи та засоби боротьби з вразливостями.**
- **Розробити поняття політики безпеки оцифрування сигналу.**
- **Висунути власну політику безпеки в комп'ютерних мережах.**
- **Зробити висновки.**

Поняття комп’ютерних мереж

Комп'ю́терна мере́жа — система зв'язку між двома чи більше комп'ютерами. У ширшому розумінні комп'ютерна мережа — це система зв'язку через кабельне чи повітряне середовище, самі комп'ютери різного функціонального призначення і мережеве обладнання.

3

Класифікація комп’ютерних мереж

NURE
Харківський національний університет радіоелектроніки

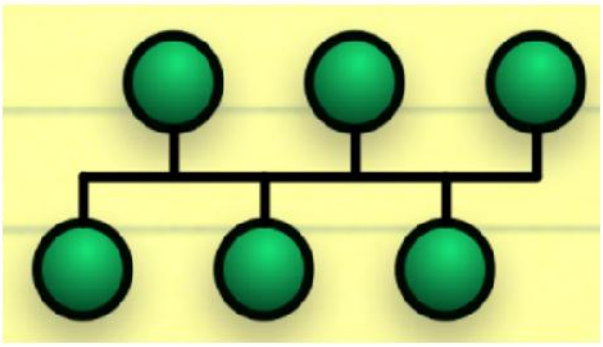
- Персональна мережа
- Локальні мережі
- Кампусні мережі
- Глобальні мережі

- Шина
- Кільце
- Зірка
- Повнозв’язна

4

Загальна шина

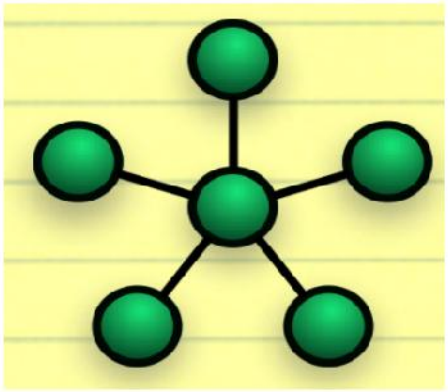
NURE
Харківський національний університет радіоелектроніки



Загальна шина — це загальний кабель (шина або магістраль), до якого підключені всі робочі станції. Термінатор розташований на кінці кабелю, щоб сигнал не відбивався.

5

Топологія «Зірка»



Основною базовою топологією комп'ютерних мереж є топологія типу **Зірка.** Головною відмінністю даної топології є підключення всіх робочих станцій до одного центрального вузла, в ролі якого, в більшості випадків, виступає комутатор, утворюючи фізичний сегмент мережі. Сегменти зіркоподібної топології можуть функціонувати як окремо, так і в складі складної мережевої топології.

6

Типи вразливостей

NURE
Харківський національний університет радіоелектроніки

Внутрішні

Співробітники організації;

Програмне забезпечення;

Апаратні засоби.

Зовнішні

Комп'ютерні віруси;

Шкідливі програми;

Організації та окремі особи;

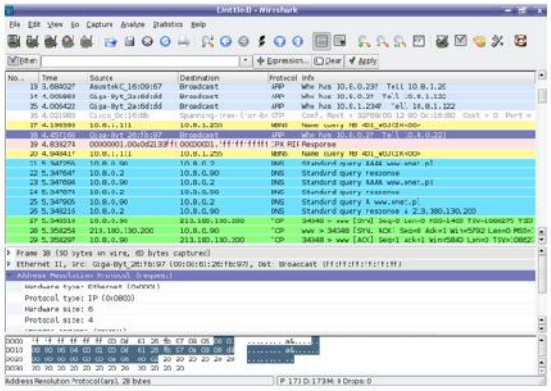
Стихійні лиха.

7

Несанкціонований доступ

NURE
Харківський національний університет радіоелектроніки

Аналізатор трафіку, або сніфер



Зараження комп'ютера

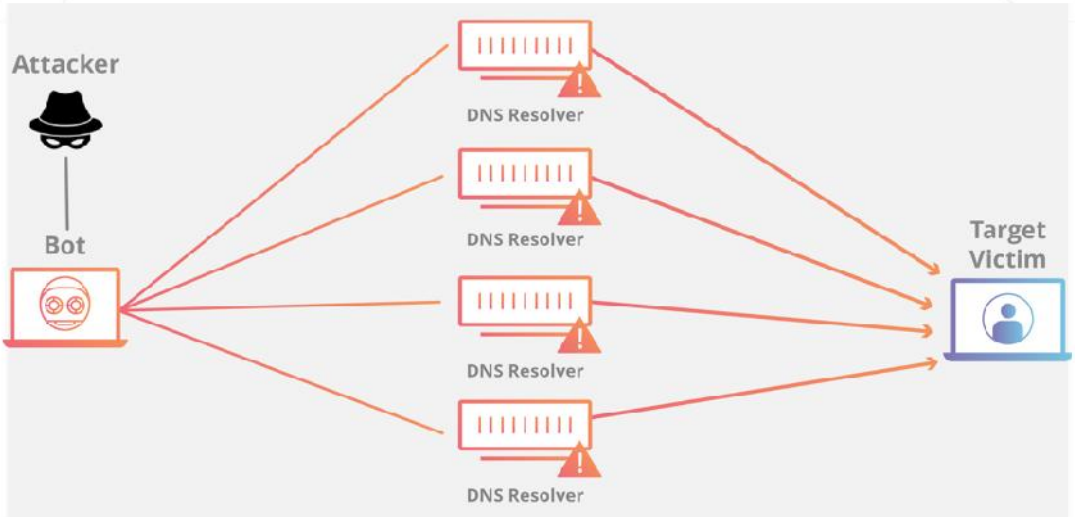
8

Sircam

Sircam розсилав себе з заражених комп'ютерів у вигляді файлів, вкладених в листи електронної пошти.

9

DDoS-атака



DDoS-атака (Distributed Denial of Service attack) – комплекс дій, здатних повністю або частково вивести з ладу інтернет-ресурс.

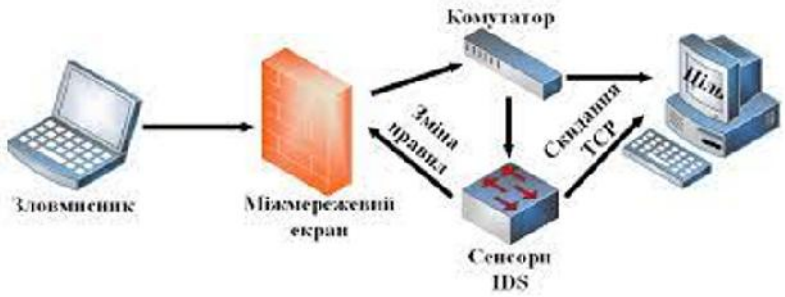
10

Класифікація систем виявлення атак

Перший, і найпоширеніший спосіб – це виявлення вже реалізованих атак.

Другий шлях – запобігти атакам ще до їх реалізації.

Третій шлях – виявлення вже скоєних атак та запобігання їх повторному здійсненню.



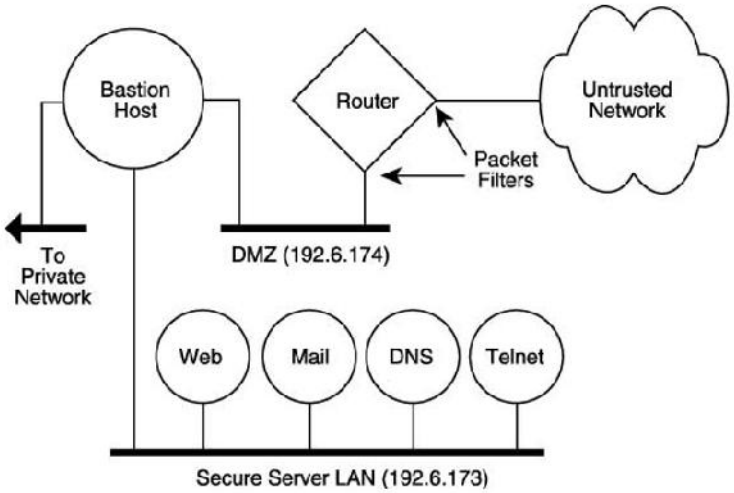
11

Імітація атак

"Імітація атак" (exploit check). Деякі вразливості не виявляють себе, поки їх не "підштовхнуть". Для цього проти підозрілого сервісу чи вузла запускаються реальні атаки. Перевірка методом "exploit check" дозволяє імітувати реальні атаки, тим самим з більшою ефективністю (але меншою швидкістю) виявляти вразливості на вузлах, що скануються.

12

Фільтрація на маршрутизаторі



13

Політика безпеки

- Антивірусна політика
- Обсяг і повноваження
- Політика доступу
- Політика прийнятного використання
- Політика бездротового доступу
- Політика паролів
- Політика аутентифікації

14

Висунута політика безпеки в комп'ютерних мережах

Компанія повинна підтримувати ACL для регулювання трафіку UDP і TCP.

L2TP з IPSec слід застосовувати для забезпечення належного захисту для тих, хто намагається отримати доступ до комп'ютерів організацій віддалено.

Для цілей шифрування слід використовувати заходи безпеки 802.11, такі як CCMP, TKIP тощо.

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

15

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;
- Наведені приклади вразливостей та висунуто методи боротьби з ними;
- Висунута власна політика безпеки для комп'ютерних мереж.

16