МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

«Брестский государственный технический университет»

Кафедра «Интеллектуальные информационные технологии»

Лабораторная работа №8

По дисциплине «Аппаратное и программное обеспечение сетей»

Тема: «Утилита для сканирования и исследования безопасности сети NMAP»

Выполнил:

студент 3 курса

группы ИИ-21(1)

Романко Н.А.

Проверил:

Степанчук В.И.

Брест 2023

Цель: Изучение и практическое применение утилиты для сканирования и исследования безопасности сети nmap.

1. Получите список открытых портов (TCP и UDP) машины, за которой выполняется лабораторная работа (localhost). Воспользуйтесь несколькими методами сканирования. Сравните результаты.

Получаем список открытых TCP портов при помощи команды *nmap -sS localhost*(метод TCP SYN)

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Делаем тоже самое при помощи команды *nmap -sT localhost*(метод TCP Connect)

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Получаем список открытых UDP портов при помощи команды *nmap -sU localhost*(метод UDP-сканирование)

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Автоматически созданное описание

1. Определите операционную систему этой же машины

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

1. Узнать адреса активных хостов в сети

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

1. Просканировать хост №1 разными методами

Воспользуемся методами TCP SYN, UDP-сканирование и сканирование протоколов IP

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

1. Для четырех хостов выполнить следующие действия:
2. Определить, защищен ли хост межсетевым экраном

Проверим защищен ли хост №2 межсетевым экраном при помощи ACK-сканирования

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

В результате есть запись filtered что означает что хост защищен только пакетным фильтром

2)Определить поддерживаемые протоколы

Определим поддерживаемые протоколы для хоста №3 при помощи IP-сканирования

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание3) Выберите оптимальный метод сканирования портов, чтобы избежать обнаружения. Определите открытые и фильтрованные порты и по возможности версии служб. При необходимости используйте RPC-сканирование.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описаниеИзображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описаниеИзображение выглядит как текст, снимок экрана, Шрифт, черно-белый

Автоматически созданное описаниеИзображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

4) Определить операционную систему

Определим операционную систему пятого хоста

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Данный хост послал большое количество «отпечатков», которые соответствуют разным ОС, следовательно, узнать точную ОС не представляется возможным.

Вывод: изучил и практически применил утилиту nmap для сканирования и исследования безопасности сети nmap