Лабораторная работа № 7

# Сканирование уязвимостей

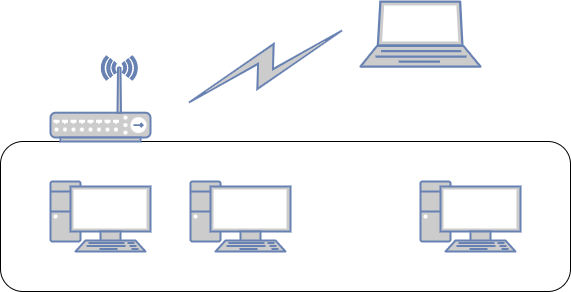
### Цель работы

Используя сетевой сканер nmap и сканер уязвимостей nessus, изучить основные методы анализа сетевой инфраструктуры .

### Задачи

* Подключиться к тестовому стенду, используя подключение Wi-Fi (параметры подключения взять из результатов выполнения ЛР6)
* Выполнить сканирование сети, на основе результатов сканирования сформировать карту сети
* Исследовать узлы сети на предмет открытых портов
* Выполнить сканирование уязвимостей для сервисов на открытых портах.

### Сетевая схема



### Содержание работы

* Подключиться к тестовому стенду, определить IP адрес и подсеть для сканирования.
* Nmap поддерживает CIDR адресацию. Необходимо добавить /*<кол-во бит>* к IP адресу или сетевому имени и Nmap просканирует каждый IP адрес, для которого первые *<кол-во бит>* такие же как и у заданного хоста. Например, 192.168.10.0/24 просканирует 256 хостов между 192.168.10.0 (бинарное: 11000000 10101000 00001010 00000000) и 192.168.10.255 (бинарное: 11000000 10101000 00001010 11111111) включительно. 192.168.10.40/24 сделает абсолютно то же самое.
* Одна из важнейших задач при исследовании любой сети это сократить (иногда довольно большой) набор IP диапазонов до списка активных или интересных для исследования хостов. Задачу обнаружения хостов иногда называют пинг сканированием (ping scan), однако она намного превосходит использование обычных ICMP запросов ассоциирующихся с вездесущими ping утилитами. Пользователи могут полностью пропустить шаг пинг сканирования с помощью опции сканирования с целью составления списка (-sL) или просто отключив его (-PN), или сканировать сеть с помощью произвольных комбинаций мультипортовых TCP SYN/ACK, UDP и ICMP запросов. Целью всех этих запросов является получение ответов, указывающих, что IP адрес в настоящее время активен (используется хостом или сетевым устройством). Опции -P\* (определяющие тип пинг сканирования) могут комбинироваться. Вы можете увеличить шансы обхода строго брандмауэра посылая множество запросов различных типов, используя различные TCP порты/флаги и ICMP коды. Также имейте в виду, что даже если вы определите различные -P\* опции, по умолчанию применительно к целям локальной сети будет производиться и ARP сканирование (-PR), т.к. оно почти всегда быстрее и более эффективно.

**Возможные -P\* опции:**

-sL (Сканирование с целью составления списка)

-sP (Ping сканирование)

-PS *<список\_портов>* (TCP SYN пинг)

-PA *<список\_портов>* (TCP ACK пинг)

-PU *<список\_портов>* (UDP пинг)

-PE; -PP; -PM (указать типы пакетов ICMP)

-PO *<список\_протоколов>* (пинг с использованием определенного IP протокола)

-PR (ARP пинг)

**Сканирование портов**

*-sS (TCP SYN сканирование)*

*-sT (TCP сканирование с использованием системного вызова connect)*

*-sU (Различные типы UDP сканирования)*

*-sN; -sF; -sX (TCP NULL, FIN и Xmas сканирования)*

*-sA (TCP ACK сканирование)*

**Обнаружение служб и версий**

*-sV (Определение версии)*

*-sR (RPC сканирование)*

*-O (Определение ОС)*

Для удобства работы с nmap и построения топологий сети можно использовать Zenmap представляющий собой GUI для nmap (<https://nmap.org/zenmap/>)

Результаты заносим в таблицу:

| **Хост** | **ОС** | **Открытые порты (указать тип tcp/udp и номер порта)** | **Описание сервиса** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

**Сканирование уязвимостей Nessus (**[**https://www.tenable.com/downloads/nessus**](https://www.tenable.com/downloads/nessus)**) или Metasploit**

После установки интерфейс доступен на локальном адресе по порту 8834 (Nessus), либо 3790 (Metasploit)

Указываем для сканирования узлы, обнаруженные nmap на предыдущем этапе. Результаты заносим в таблицу:

| **Уязвимость** | **Критичность** | **Описание** | **Хост:порт либо несколько, где обнаружена уязвимость** | **Возможное решение** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Требования к отчету

Отчет должен содержать:

* Команды, используемые в ходе работы;
* Таблицу, описывающую некоторые узлы сети;
* Таблицу, описывающую некоторые из обнаруженных уязвимостей;
* Команды, реализующие эксплуатацию выбранной уязвимости, а также результаты эксплуатации.

Оформление отчета выполняется в соответствии с требованиями преподавателя.

Материалы для подготовки

<https://nmap.org/book/toc.html>

<https://docs.metasploit.com/>

<https://docs.tenable.com/Nessus.htm>