**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**Лабораторная работа № 6**

на тему «Nmap сканирование с помощью зомби»

|  |
| --- |
| Выполнил: студент группы ВКБ43 |
| Ковалев Данил Петрович |
| (Фамилия, имя, отчество) |
| Проверил: доцент |
| Решетникова Ирина Витальевна |
| (Фамилия, имя, отчество) |

**Цель:** научиться использовать метод “зомби” при помощи утилиты nmap.

# **Ход работы:**

**Задание 1.** Получить IP-адресы машин, на которые будет производиться атака.

Для выполнения лабораторной работы будет использоваться система контейнеризации Docker. Конфигурация Docker compose представлена на рисунке 1. В нашем случае были заданы фиксированные IP-адреса для разных виртуальных машин соответственно. IP-адрес зомби машины – 192.168.6.11, а IP-адрес целевой машины – 192.168.6.22.

Проясним немного конфигурацию. Зомби-машина (zombie): настройка net.ipv4.ip\_id=1 гарантирует последовательные IPID, правило iptables автоматически отвечает RST на SYN/ACK, IP. Целевая машина (target): nginx по умолчанию открывает порт 80, порт 22 закрыт (имитирует закрытый порт).

Изображение выглядит как текст, снимок экрана, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 1 – docker compose для выполнения лабораторной работы

**Задание 2.** Провести сканирование с помощью утилиты nmap ip-адрес будущей машины зомби.

Настройки PC1 представлены на рисунке 3. Здесь мы также назначаем IP-адрес и маску подсети, как в теории для лабораторной работы.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 3 – настройки PC1

**Задание 3.** Настроить маршрутизатор.

Для настройки маршрутизатора используется конфигурация, которая представлена в теории для лабораторной работы. Здесь мы назначаем только IP-адрес и маску подсети. Результат представлен на рисунке 4.

Изображение выглядит как текст, программное обеспечение, число, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 4 – настройки маршрутизатора

**Задание 4.** Настроить сервер.

Для настройки сервера будем использовать конфигурацию, которая предложена в условии к лабораторной работе. Здесь опять-таки настраиваем только IP-адрес и маску подсети. Результат представлен на рисунке 5.

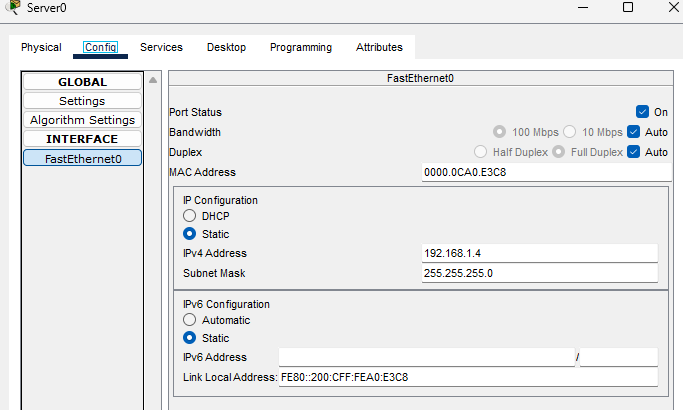


Рисунок 5 – настройки сервера

**Задание 5.** Настроить Local Database для роутера.

Для настройки Local Database для роутера будем использовать конфигурацию, которая представлена в условии лабораторной работы. Команды для выполнения задания представлены на рисунке 6. Ниже более подробно рассмотрим, что означает каждая команда.

“Router#conf t” – переход в конфигурационный режим (Global Configuration Mode). Все последующие команды изменяют конфигурацию устройства. Без данного режима невозможно вносить изменения.

“Router(config)#enable secret cisco” – установка секретного пароля для привилегированного режима.

“Router(config)#username admin privilege 15 secret cisco” **–** создание локального пользователя в базе данных роутера. Рассмотрим более подробно аргументы команды. “username admin” – создается пользователь с логином admin. “privilege 15” – пользователю присваивается максимальный уровень привилегий, что эквивалентно режиму enable. Он сможет выполнять все команды без необходимости вводить enable отдельно. “secret cisco” – устанавливается зашифрованный пароль cisco для этого пользователя.

“Router(config)#aaa new-model” – включение системы ААА на роутере.

“Router(config)#aaa authentication login default local” **–** настройка метода аутентификации для входа на устройство (login).

“Router(config)#ex” **–** выход из конфигурационного режима обратно в привилегированный режим.

В итоге общий смысл всей конфигурации:

1. Включается система AAA (aaa new-model).
2. Настраивается: для входа на устройство (login) по *умолчанию* (на всех линиях) должна использоваться локальная база данных пользователей (aaa authentication login default local).
3. В локальную БД добавляется пользователь admin с максимальными правами (privilege 15) и паролем cisco (username admin privilege 15 secret cisco).
4. Устанавливается пароль для входа в привилегированный режим (enable secret cisco). (Пользователь admin с privilege 15 может сразу в него попадать без этого пароля, но другим пользователям с меньшими правами или для прямого входа в enable он понадобится).

Изображение выглядит как текст, снимок экрана, Шрифт, алгебра

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 6 – настройка Local Database для роутера

**Задание 6**. Попробовать подключиться к роутеру через telnet с PC0.

Для выполнения задания нужно на PC0 перейти в Command Prompt и ввести команды, которые представлены на рисунке 7. Логин здесь admin, а пароль – cisco. На рисунке 7 показано, что подключение успешно произошло.

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 7 – подключение через telnet c PC0 к Router

**Задание 7.** Настроить AAA-сервер.

Для выполнения задания нужно зайти на устройство Server-PT и выбрать во вкладке Services “AAA”. В результате должно получиться то, что представлено на рисунке 8.

Изображение выглядит как текст, снимок экрана, дисплей, число

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 8 – конфигурация сервиса “AAA” на Server-PT

**Задание 8.** Настроить роутер для аутентификации через Radius сервер.

Для выполнения задания будем использовать команды, которые представлены на рисунке 9. Рассмотрим более подробно, что эти команды выполняют.

“conf t” - вход в глобальный конфигурационный режим.

“no aaa authentication login default local” - удаление предыдущей настройки метода аутентификации по умолчанию. Эта команда стирает старую конфигурацию aaa authentication login default local, которая использовала только локальную базу данных. Это подготовка к новой настройке.

“aaa authentication login default group radius local” - настройка нового метода аутентификации для входа по умолчанию.

“radius-server host 192.168.1.4 key cisco” **-** назначение: Конфигурация параметров конкретного RADIUS-сервера. Эта команда добавляет RADIUS-сервер с адресом 192.168.1.4 в группу RADIUS-серверов по умолчанию. Именно к этому серверу роутер будет обращаться, когда в методе аутентификации (aaa authentication login default group radius local) дойдет очередь до group radius.

Изображение выглядит как текст, снимок экрана, Шрифт, документ

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 9 – настройка Radius сервера для Router0

**Задание 9.** Подключиться из-под Router0 под старым пользователем - admin и новым - cooper.

На рисунке 10 представлено, что из-под пользователя admin не получилось подключиться.

Изображение выглядит как текст, Прямоугольник, снимок экрана, доска

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 10 – подключение к роутеру из-под пользователя “admin”.

Попробуем теперь подключиться из-под консоли за пользователя “cooper”. Результат представлен на рисунке 11.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 11 – подключение за пользователя cooper

**Вывод:** в данной лабораторной работе мы успешно настроили аутентификацию.

# **Контрольные вопросы**

1. **Сформируйте определение AAA-сервера.**

**AAA-сервер** (Authentication, Authorization, Accounting) — это сервер, который обеспечивает централизованное управление доступом к сетевым ресурсам и устройствам. AAA-сервер выполняет три основные функции:

* **Аутентификация (Authentication)**: Проверка подлинности пользователя или устройства, пытающегося получить доступ к сетевым ресурсам. Это включает в себя проверку учетных данных (например, логина и пароля) для подтверждения личности.
* **Авторизация (Authorization)**: Определение прав доступа пользователя или устройства после успешной аутентификации. Авторизация определяет, какие ресурсы и действия доступны пользователю или устройству.
* **Учет (Accounting)**: Сбор и запись информации о действиях пользователя или устройства, таких как время доступа, использованные ресурсы и выполненные команды. Эта информация используется для мониторинга, аудита и биллинга.

1. **Что такое аутентификация и авторизация?**

**Аутентификация** — это процесс проверки подлинности личности пользователя или устройства, пытающегося получить доступ к системе или ресурсу. Цель аутентификации — убедиться, что пользователь или устройство действительно являются теми, за кого себя выдают.

**Основные методы аутентификации:**

1. **Пароль**: Пользователь предоставляет секретный пароль, который соответствует заранее заданному.
2. **Биометрия**: Использование уникальных физических характеристик, таких как отпечатки пальцев, распознавание лица или сетчатки глаза.
3. **Токены**: Устройства, генерирующие одноразовые пароли или коды, которые пользователь должен ввести для аутентификации.
4. **Многофакторная аутентификация (MFA)**: Комбинация нескольких методов аутентификации, например, пароль + SMS-код.
5. **Сертификаты**: Использование цифровых сертификатов, подтверждающих подлинность пользователя или устройства.

**Авторизация** — это процесс определения прав доступа пользователя или устройства к определенным ресурсам или действиям после успешной аутентификации. Авторизация определяет, какие действия и ресурсы доступны пользователю или устройству.

**Основные аспекты авторизации:**

1. **Роли**: Пользователи могут быть сгруппированы в роли (например, администратор, пользователь), каждая из которых имеет определенные права доступа.
2. **Политики доступа**: Определяют, какие ресурсы и действия доступны для каждой роли или пользователя.
3. **Разрешения**: Явное предоставление или ограничение прав доступа к определенным ресурсам или функциям.
4. **Контроль доступа на основе атрибутов (ABAC)**: Авторизация основана на атрибутах пользователя, ресурса и контекста доступа.

3**. Что такое telnet?**

Telnet (Телетайп-сеть) в системе Cisco и других сетевых устройствах — это протокол удаленного доступа, который позволяет администраторам управлять сетевыми устройствами через сеть. Он используется для удаленного подключения к устройству и выполнения команд, настройки и мониторинга.

**4. Перечислите методы аутентификации в AAA.**

В контексте AAA (Authentication, Authorization, Accounting), аутентификация — это первый этап, на котором проверяется подлинность пользователя или устройства, пытающегося получить доступ к сетевым ресурсам. Существует несколько методов аутентификации, которые могут использоваться в AAA-системах. Вот основные из них:

### 1. **Парольная аутентификация (Password Authentication)**

* **Описание**: Пользователь предоставляет секретный пароль, который соответствует заранее заданному.
* **Пример**: Ввод логина и пароля при входе в систему.

### 2. **Биометрическая аутентификация (Biometric Authentication)**

* **Описание**: Использование уникальных физических характеристик, таких как отпечатки пальцев, распознавание лица или сетчатки глаза.
* **Пример**: Считывание отпечатка пальца для доступа к устройству.

### 3. **Аутентификация с использованием токенов (Token-Based Authentication)**

* **Описание**: Устройства, генерирующие одноразовые пароли или коды, которые пользователь должен ввести для аутентификации.
* **Пример**: Использование аппаратного или программного токена для генерации OTP (одноразового пароля).

### 4. **Многофакторная аутентификация (Multi-Factor Authentication, MFA)**

* **Описание**: Комбинация нескольких методов аутентификации, например, пароль + SMS-код.
* **Пример**: Ввод пароля и получение SMS-кода на мобильный телефон для дополнительной проверки.

### 5. **Аутентификация на основе сертификатов (Certificate-Based Authentication)**

* **Описание**: Использование цифровых сертификатов, подтверждающих подлинность пользователя или устройства.
* **Пример**: Использование сертификата клиента для аутентификации в VPN.

### 6. **Аутентификация на основе Kerberos (Kerberos Authentication)**

* **Описание**: Протокол аутентификации, который использует билеты для проверки подлинности пользователя.
* **Пример**: Использование Kerberos для аутентификации в среде Windows Active Directory.

### 7. **Аутентификация на основе RADIUS (RADIUS Authentication)**

* **Описание**: Использование протокола RADIUS для централизованной аутентификации пользователей.
* **Пример**: Аутентификация пользователей, подключающихся к беспроводной сети через RADIUS-сервер.

### 8. **Аутентификация на основе TACACS+ (TACACS+ Authentication)**

* **Описание**: Использование протокола TACACS+ для централизованной аутентификации пользователей на сетевых устройствах.
* **Пример**: Аутентификация администраторов, подключающихся к маршрутизаторам и коммутаторам Cisco.

### 9. **Аутентификация на основе LDAP (LDAP Authentication)**

* **Описание**: Использование протокола LDAP для аутентификации пользователей на основе данных в каталоге.
* **Пример**: Аутентификация пользователей в веб-приложении с использованием LDAP-сервера.

### 10. **Аутентификация на основе OAuth (OAuth Authentication)**

* **Описание**: Использование протокола OAuth для делегирования доступа к ресурсам без передачи учетных данных.
* **Пример**: Вход в веб-приложение через учетную запись Google или Facebook.