**Лабораторная работа №1**

**Цель:**

Произвести атаку на ОС Metasploitable2 с помощью ОС Kali Linux и ее инструментария.

**Задачи:**

1. Настроить инфраструктуру для выполнения лабораторной работы.
2. Определить доступные сервисы на исследуемой машине.
3. Получить удаленный доступ, путем эксплуатации уязвимостей 3-х различных сервисов.
4. Оформить отчет по лабораторной работе.

**Порядок выполнения лабораторной работы:**

1. Скачать и установить на виртуальную машину образы жертвы (Metasploitable2) и атакующего (Kali Linux).
2. В настройках виртуальной машины, для каждой из них установить тип подключения «NAT» (Network Adress Translation — механизм в сетях, построенных с использованием TCP/IP протокола, преобразующий IP-адреса транзитных пакетов). Проверить соединение с помощью команды «ping»
3. Определить запущенные на машине-жертве сетевые сервисы с машины «атакующего» при помощи утилиты nmap (Рисунок 1)

Изображение выглядит как текст, меню, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 1 – утилита nmap

1. Получаем удаленный доступ, путем эксплуатации уязвимостей 3-х различных сервисов с помощью программы **OpenVAS** и **Metasploit Framework**

**Теория:**

Итак, найден сервер, к которому можно получить доступ. Обычно для несанкционированного подключения используют уязвимости в установленном программном обеспечении. Поиск уязвимостей можно осуществлять вручную, используя полученную информацию и базы данных уязвимостей. Однако это очень долгий и трудоемкий процесс. А можно воспользоваться сканерами уязвимостей. Самые популярные из них — Nessus, OpenVAS, Retina и Nexpose. Они позволяют не только находить открытые уязвимости в установленном программном обеспечении и операционных системах, но и определять устаревшие протоколы шифрования, зараженные компьютеры и многое другое. OpenVAS входит в состав Kali Linux.

Kali Linux является передовым Linux-дистрибутивом для проведения тестирования на проникновение и аудита безопасности. Kali включает более 600 инструментов, ориентированных на различные задачи информационной безопасности, такие как тестирование на проникновение, сбор информации, форензика и обратная инженерия. Kali Linux разрабатывается, финансируется и поддерживается Offensive Security, лидирующей компанией в сфере обучения информационной безопасности. В качестве основы для создания Kali Linux был выбран распространенный дистрибутив – Debian, что делает его использование простым для широкого круга пользователей Ubuntu, Knoppix и других дистрибутивов, основанных на Debian.

Все действия, проводимые на данном этапе в ходе проведения тестирования на проникновение, могут быть замечены администраторами целевой системы. Если это случится, то они наверняка попробуют помешать проведению дальнейших действий.

Для разработки, тестирования и применения эксплойтов была создана программная платформа Metasploit Framework.

Эксплойт — это специальная программа, использующая известные уязвимости в программном обеспечении для проведения атаки с целью получения контроля над системой или вывода ее из строя (отказа в обслуживании). Эксплойты бывают удаленными, работающими через компьютерную сеть, и локальными, запускающимися непосредственно в самой системе. В Metasploit эксплоиты делятся на активные и пассивные. Активные начинают эксплуатировать определенную уязвимость в программном обеспечении сразу же после запуска и закачивают свою работу в случае удачи или провала. Пассивные ждут подключения удаленного хоста и только после этого начинают свою работу. Например, можно запустить эксплойт, отправив жертве клиентскую часть по электронной почте. После того, как получатель откроет приложение к письму, клиентская часть соединится с запущенным ранее эксплойтом, и тот начнет атаку. Просмотреть все доступные эксплойты можно, используя команду show exploits, однако, учитывая их огромное количество, это не всегда удобно.