Государственное учреждение образования

“БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ”

Кафедра: Интеллектуальных информационных технологий

Дисциплина: Проектирование защищенных интеллектуальных информационных систем

Отчет по лабораторной работе №7-8

**Безопасность работы удаленных серверов в сети Internet.**

**Анализ запросов из сети Internet.**

**Усовершенствование системы безопасности удаленных серверов**

Выполнил:

студент гр.121702

Витковская С. И.

Проверил:

Захаров В. В.

Минск 2024

**Задание:**

1. Установить на удаленном сервере веб-сервер и разместить на нём тестовую страницу, доступную из сети Internet.

2. Настроить систему журналирования на веб-сервере.

3. Выполнить анализ данных логов различных подсистем, в том числе SSH, веб-сервера удаленного сервера за несколько дней.

4. Установить и настроить программное обеспечение, позволяющее

усовершенствовать защиту сервера, согласно варианту.

**Используемые инструментальные средства:**

1. ОС – Linux
2. Протокол SSH – протокол прикладного уровня для безопасного обмена информацией между двумя устройствами. При передаче по SSH информация шифруется, поэтому протокол используется для работы в незащищенных сетях, чтобы обеспечить высокий уровень защиты.
3. HTTP-сервер Apache – свободный веб-сервер. Apache является кроссплатформенным ПО. Основными достоинствами Apache считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д.
4. Snort – свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом, способная выполнять регистрацию пакетов и в реальном времени осуществлять анализ трафика в IP-сетях. Выполняет протоколирование, анализ, поиск по содержимому, а также широко используется для активного блокирования или пассивного обнаружения целого ряда нападений и зондирований, таких как попытки атак на переполнение буфера, скрытое сканирование портов, атаки на веб-приложения, SMB-зондирование и попытки определения операционной системы.
5. Fail2ban – локальный сервис, который отслеживает log–файлы запущенных программ, и на основании различных условий блокирует по IP найденных нарушителей. В первую очередь Fail2ban известен благодаря готовности «из коробки» к защите SSH–сервера от атак типа «bruteforce», то есть к защите SSH от перебора паролей.

**Ход работы:**

1. После установки сервера Apache, изменим приветственный файл по адресу /var/www/html/index.html, добавив туда текст Server is up and running!

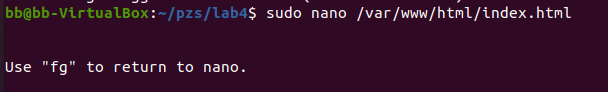


Рис.1 – Команда открытия файла для перезаписи

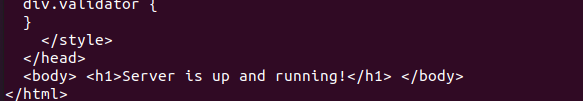


Рис.2 – Вставленный текст

1. Запустим сервер и откроем страницу по адресу http:/localhost с помощью команды curl.



Рис.3 – Запуск сервера

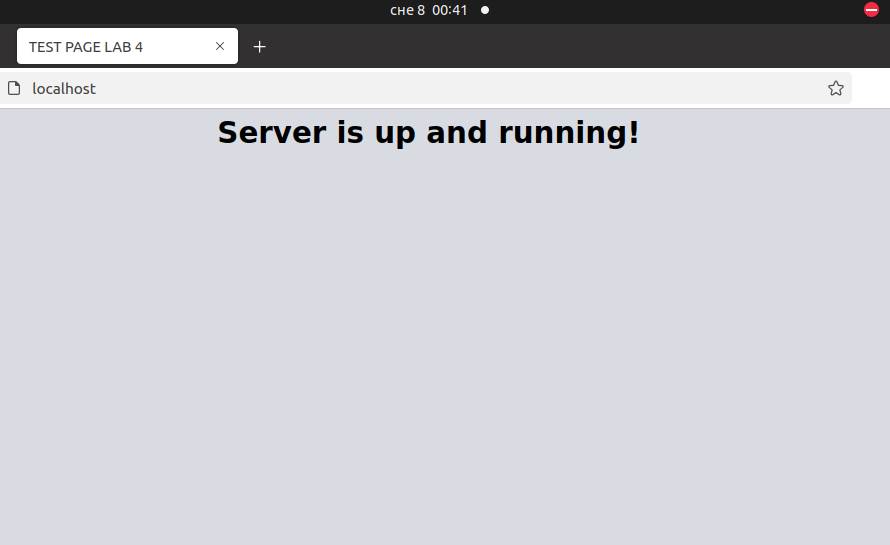


Рис. 4 – Просмотр страницы

1. Просмотрим файлы логов, определим период просмотра действий

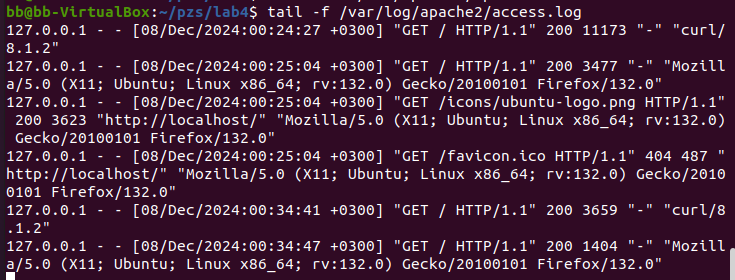


Рис. 5 – Логи запросов

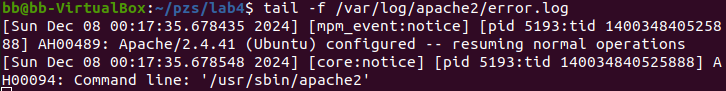
Как видим, все запросы производились с помощью локального веб-браузера Mozila, и производились успешно, т.к. все коды ответа являются 200. Т.к. на странице присутствует только текстовая строка, все запросы относятся к типу GET.

Рис. 6 – Логи ошибок



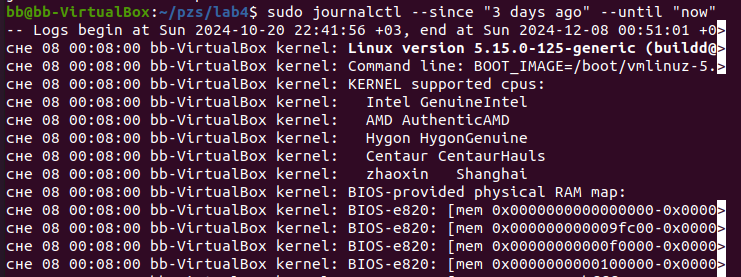
Рис.7 – Настройка системы журналирования SSH

Рис.8 – Просмотр журнала за последние 3 дня

1. Усовершенствуем защиту сервера с помощью Snort.



Рис.9 – Команда установки

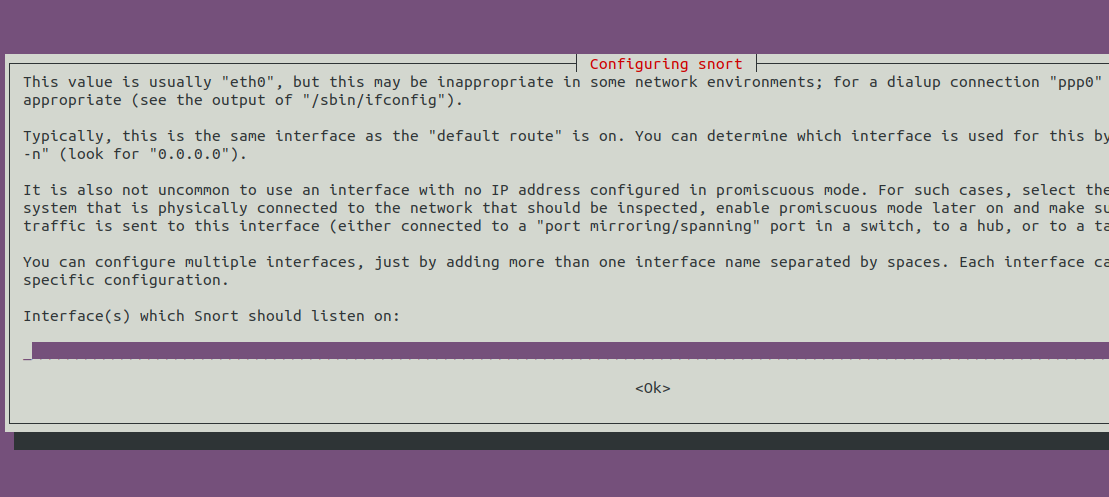


Рис.10 – Процесс конфигурации

1. Добавим дополнительную защиту от брутфорс-атак с помощью Fail2ban

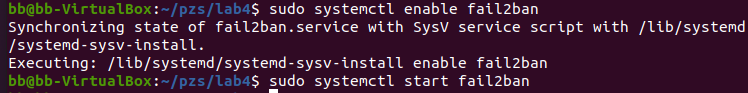


Рис. 11 – Запуск Fail2ban

**Вывод:**

В ходе лабораторной работы был установлен веб-сервер Apache, создана веб-страница, проверена работа сервера, проанализированы логи запросов и ошибок, в том числе за несколько дней. Была усовершенствована защита сервера с помощью Snort и Fail2ban.