

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

# **«МИРЭА – Российский технологическ** **ий университет»**

# **РТУ МИРЭА**

|  |
| --- |
| Институт кибербезопасности и цифровых технологий |

|  |
| --- |
| Кафедра КБ-2 «Прикладные информационные технологии» |

Практическая работа № 6

по дисциплине «Безопасность Операционных систем»

«Netfilter, WAF»

|  |  |
| --- | --- |
|  | Выполнил:  Студент БББО-05-20  Кутьин З.С. |
|  | Проверил:  Абрамов Д.П. |

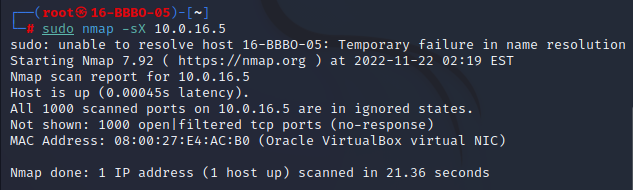
Москва

2022

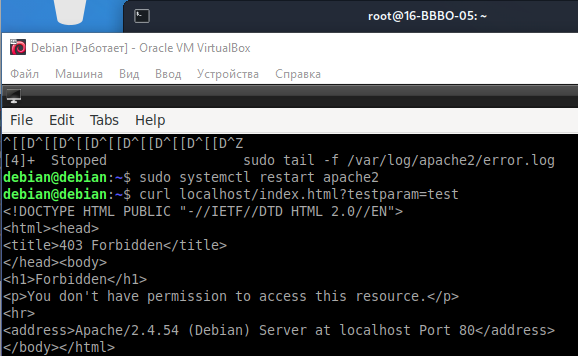
**Цель работы:** Изучение межсетевых экранов. Приобретение навыков работы с Iptables и WAF.

**Порядок работы:**

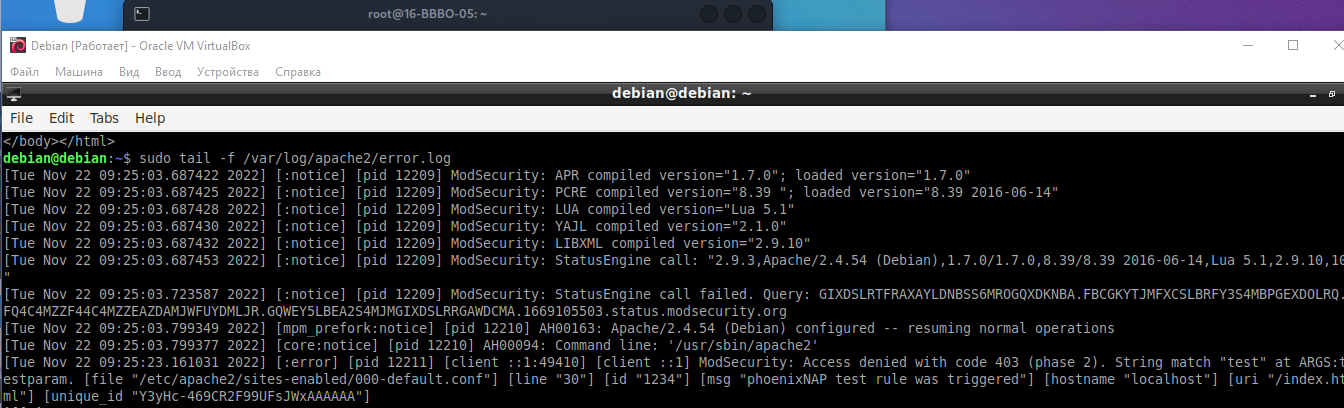
1. Сканирование(nmap) с Kali

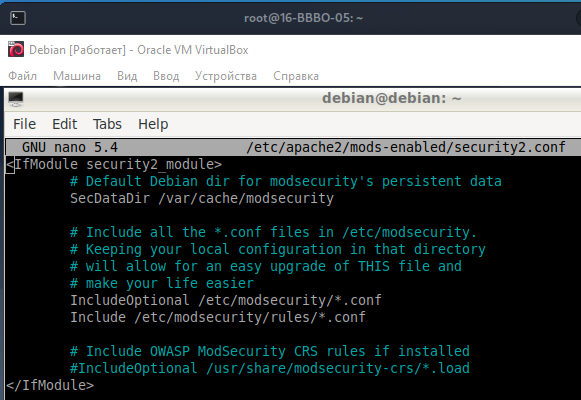


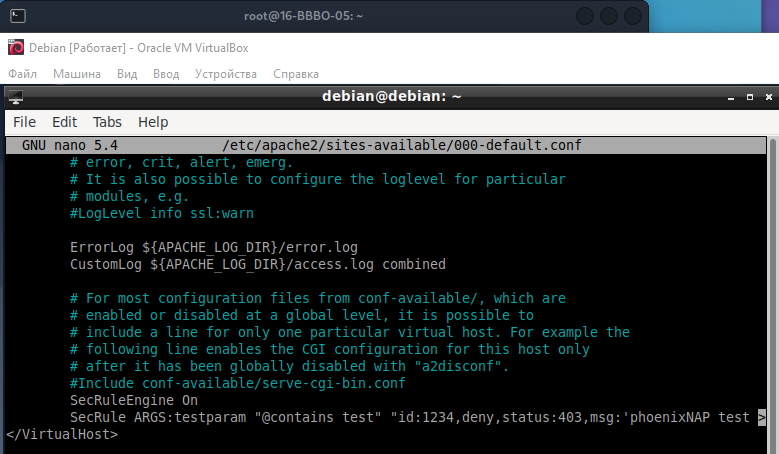
1. Открытие index.html

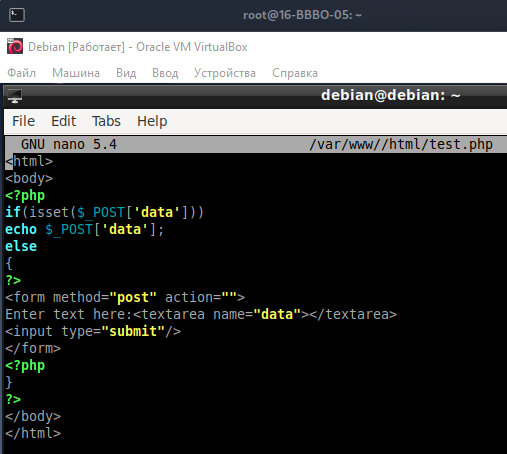


1. Логи ошибок

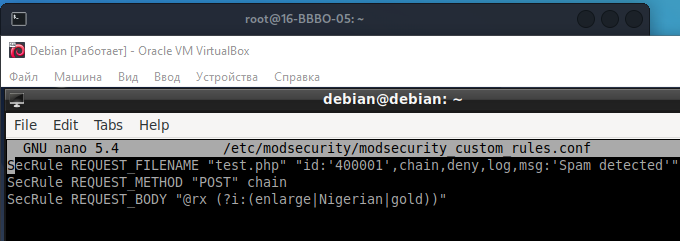


1. Проверяем security2.conf чтобы удостовериться, что правила ModSecurity загружены
2. Добавление строк в файл /etc/apache2/sites-available/000-default.conf

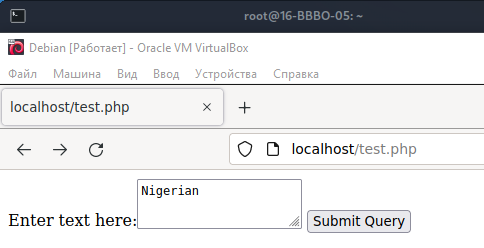


1. Создаем php файл в папке html с помощью команды sudo nano /var/www//html/test.php
2. Затем создайте свои правила для ModSecurity:

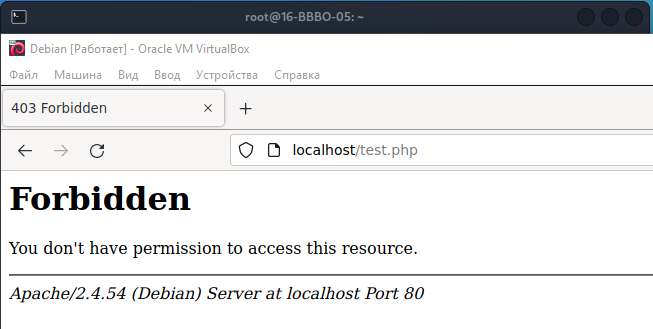
sudo nano /etc/modsecurity/modsecurity\_custom\_rules.conf



1. Открываем php-файл через Firefox



1. Результат ввода слова Nigerian



1. Вопросы к лабораторной работе

**Межсетевой экран (брандмауэр, файервол)** — технологический барьер, предназначенный для предотвращения несанкционированного или нежелательного сообщения между компьютерными сетями или хостами.

* 1. Для чего используется межсетвой экран?

Для фильтрации трафика, поступающего на устройство со всех или конкретных зон, защиты участка сети, корпоративной сети, сайта или устройства от нежелательного сетевого доступа.

* 1. Принцип работы Netfilter.

Все пакеты пропускаются через цепочки правил. При прохождении к нему последовательно применяются правила этой цепочки, если он соответствует указанному критерию, применяется действие (в т. ч. переход к другой цепочке, например пользовательской).

* 1. Таблицы межсетевого экрана Netfilter. Для чего они используются?

**raw** - используется для маркировки пакетов, которые не должны обрабатываться системой определения состояний. Содержится в цепочках PREROUTING и OUTPUT.

**mangle**— содержит правила модификации IP-пакетов.

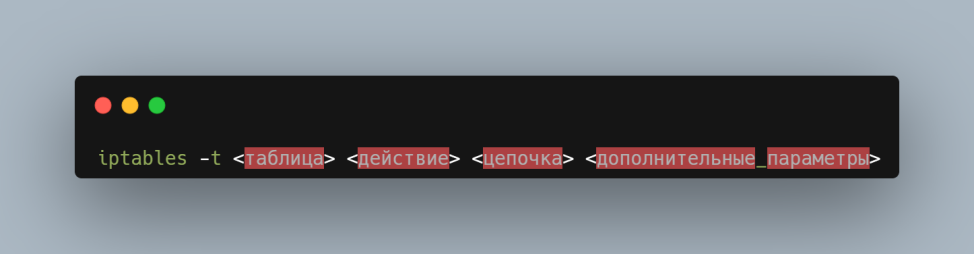
**nat**- предназначена для подмены адреса отправителя или получателя. Данную таблицу проходят только первые пакеты из потока - трансляция адресов или маскировка (подмена адреса отправителя или получателя) применяются ко всем последующим пакетам в потоке автоматически. Поддерживает действия DNAT, SNAT, MASQUERADE, REDIRECT. Содержится в цепочках PREROUTING, OUTPUT, и POSTROUTING.

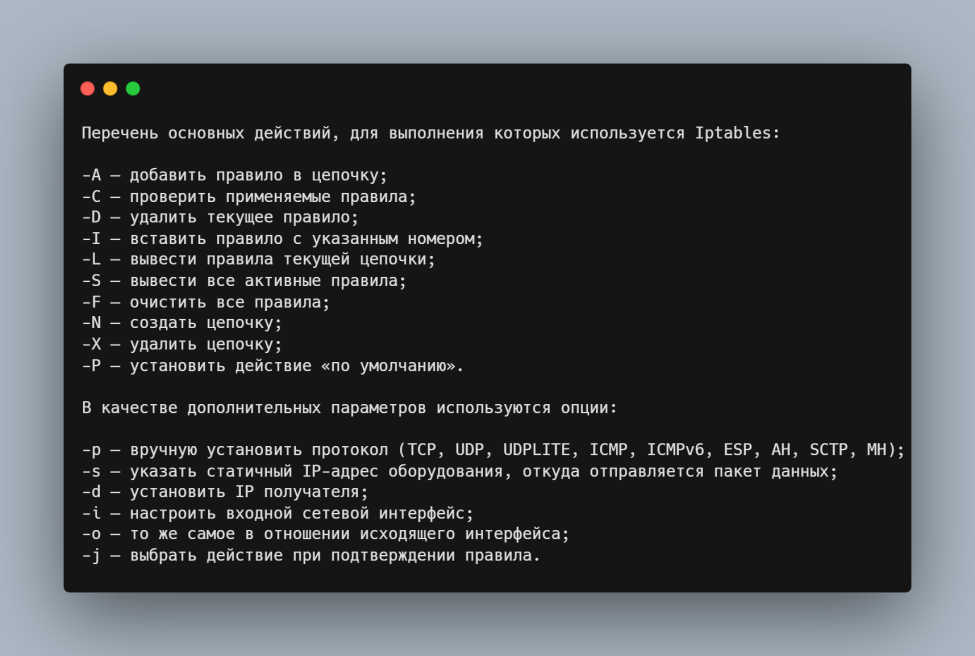
**filter**— основная таблица, используется по умолчанию если название таблицы не указано. Используется для фильтрации пакетов. Содержится в цепочках INPUT, FORWARD, и OUTPUT.

* 1. Что такое правила межсетевого экрана?

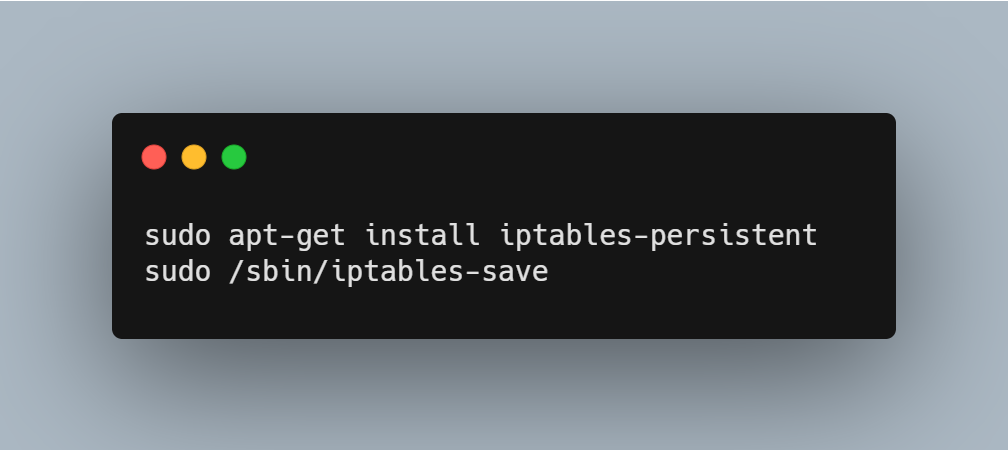
Правило межсетевого экрана состоит из условия (IP-адрес, порт) и действия, которое необходимо применить к пакетами, подходящим под заданное условие. К действиям относятся команды разрешить (accept), отклонить (reject) и отбросить (drop). Эти условия указывают МЭ, что именно нужно совершить с трафиком:

* Accept — пропустить трафик;
* Reject — не пропускать трафик, а пользователю выдать сообщение-ошибку «недоступно»;
* Drop — заблокировать передачу и не выдавать ответного сообщения.
  1. Как создавать правила для межсетевого экрана утилитой Iptables?





* 1. Как сохранить правила для последующей автозагрузки?



* 1. Что такое Web Application Firewall?

WAF (Web Application Firewall) – межсетевой экран для веб-приложений. Это инструмент для фильтрации трафика, работающий на прикладном уровне и защищающий веб-приложения методом анализа трафика HTTP/HTTPS и семантики XML/SOAP. WAF может устанавливаться на физический или виртуальный сервер и выявляет самые разнообразные виды атак.

* 1. Как настроить правила в WAF mod\_security?

Установите mod\_security

<sudo apt install libapache2-mod-security2>

Стандартный конфигурационный файл настроен на DetectionOnly, то есть, фаервол только отслеживает логи, при этом ничего не блокируя. Чтобы изменить это поведение, сначала перейдите в папку /etc/modsecurity

<cd /etc/modsecurity>

затем отредактируйте файл modsecurity.conf:

<sudo nano /etc/modsecurity/modsecurity.conf>

<sudo nano modsecurity.conf>

Найдите в файле строку: «SecRuleEngine DetectionOnly». И измените

ее так: «SecRuleEngine On».

Перезапустите Apache

<sudosystemctl restart apache2>