Правительство Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

Лабораторная работа № 3

по дисциплине «Проектный семинар по информационной безопасности»

|  |
| --- |
| Студент гр. БИБ211  \_\_\_\_\_\_\_\_\_\_\_\_\_ А.И. Семененя  «24» января 2022 г. |
| Руководитель  Заведующий кафедрой информационной безопасности киберфизических систем  канд. техн. наук, доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_О.О. Евсютин  «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2021 г. |

Москва 2021

**Цель:** изучение межсетевых экранов, приобретение навыков работы с Iptables и WAF.

**Атакующая машина (X):**

**IP-адрес:** 192.168.10.16/27

**MAC-адрес:** fe80::cf51::3130::cff0::797d/64

**Атакуемая машина (N):**

**IP-адрес:** 192.168.10.21/27

**MAC-адрес:** fe80::8dec::8525::5818::59c9/64

**Ход работы**

**Часть 1. Iptables**

1. Создадим две виртуальных машины и запустим их.
2. Устанавливаем на атакующую (X) и атакуемую (N) машины дополнительные пакеты (curl, apache2, libapache2-mod-security2).
3. Проверяем успешность установки пакетов на атакуемой машине с помощью команды:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 1

1. С атакующей машины сканируем атакуемую на порту 80 утилитой Xmas. Получаем такой результат:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 2

1. Приступаем к настройке защиты N. Смотрим список текущих правил:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3

1. С помощью команды *sudo iptables -A INPUT -i lo -j ACCEPT* вносим локальный интерфейс в разрешённые.
2. С помощью команд *sudo iptables -A INPUT -p tcp -m tcp –dport 22 -j ACCEPT* и *sudo iptables -A INPUT -p tcp -m tcp –dport 80 -j ACCEPT* разрешаем трафик на эти два порта – SSH и HTTP.
3. Однако в этой работе SSH не используется, поэтому лишнее правило удаляется командой *sudo iptables -D INPUT -p tcp -m tcp –dport 22 -j ACCEPT*.
4. Разрешаем устанавливать исходящие соединения: *sudo iptables -I INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT*.
5. Теперь мы можем заблокировать остальное и разрешить исходящие соединения командами *sudo iptables -P OUTPUT ACCEPT* и *sudo iptables -P INPUT DROP*.
6. Список правил после внесённых изменений выглядит так:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 4

1. Продолжаем укреплять защиту, на этот раз добавляя блокировку нулевых пакетов и отражение атак syn-пакетами без состояния NEW с помощью команд *sudo iptables -A INPUT -p tcp –tcp-flags ALL NONE -j DROP* и *sudo iptables -A INPUT -p tcp ! –syn -m state –state NEW -j DROP*, соответственно.
2. Защищаем сервер от разведывательных пакетов Xmas: *sudo iptables -A INPUT -p tcp –tcp-flags ALL ALL -j DROP*.
3. Для того, чтобы сохранить новые правила для следующих запусков, воспользуемся пакетом iptables-persistent.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 5

1. Проверяем наши настройки с атакующей машины с помощью Xmas-сканирования. Изображение выглядит как текст

   Автоматически созданное описание

Рисунок 6

**Часть 2. WAF**

1. Устанавливаем в модуль защиты атакуемой машины OWASP – готовый пакет правил.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 7

1. Для установки ModSecurity нужно переименовать файл с рекомендуемой конфигурацией, сделав его стандартным.
2. Меняем и содержимое файла:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 8

1. Открываем и меняем файл /etc/apache2/mods-enabled/security2.conf.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 9

1. *sudo service apache2 reload* – перезагрузка Apache.

**Тестирование модуля защиты WAF**

1. Открываем /etc/apache2/sites-available/000-default.conf, вносим изменения:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 10

1. В результате запрос curl приводит к ошибке 403 Forbidden.
2. Файл sudo nano /var/log/apache2/modsec\_audit.log фиксирует сканирование.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 11

**Ответы на вопросы:**

1. **Что такое межсетевой экран?** Комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.
2. **Для чего используется межсетевой экран?** Его основная задача — не пропускать пакеты, не подходящие под критерии, определённые в конфигурации.
3. **Принцип работы Netfilter:** сетевой пакет попадает в интерфейс => ряд проверок ядром => цепочка PREROUTING => кому адресован? => либо цепочка FORWARD, либо INPUT (=> отдаётся локальным демонам или процессам => при необходимости формируется ответ, который направляется в цепочку OUTPUT) => правило маршрутизации, цепочка POSTROUTING => в соответствии с пройденными проверками к пакету применяется определённое действие.
4. **Для чего используют таблицы межсетевого экрана Netfilter?** Raw: для маркировки пакетов, которые не должны обрабатываться системой определения состояний; mangle содержит правила модификации IP-пакетов; nat – для подмены адреса отправителя либо получателя; filter используется по умолчанию для фильтрации пакетов.
5. **Что такое правила межсетевого экрана?** Фильтры и критерии, которые определяют, какие пакеты пропускать, а какие блокировать.
6. **Как создавать правила для межсетевого экрана утилитой Iptables?** В терминале командой *sudo iptables* и параметр *-I* либо *-A.*
7. **Как сохранить правила для последующей автозагрузки?** *sudo apt-get install iptables-persistent*: во время установки пакет задаст вопрос, сохранять ли текущие правила для следующей автозагрузки.
8. **Что такое Web Application Firewall?** Межсетевые экраны, работающие на прикладном уровне и осуществляющие фильтрацию трафика web-приложений.
9. **Как настроить правила в WAF mod\_security?** С помощью изменения текстовых файлов /etc/modsecurity/modsecurity.conf и /etc/apache2/mods-enabled/security2.conf.

**Выводы по выполненной работе**: мы приобрели навыки работы с Iptables и WAF, а также изучили межсетевые экраны.