

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ
КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Лабораторная работа №1

Выполнили студенты группы ИКТЗ-83:

Громов А.А., Миколаени М.С., Мазеин Д.С.

(Ф.И.О., № группы)

(подпись)

Проверил:

Казанцев А.А.

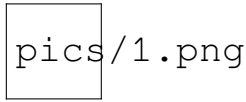
(уч. степень, уч. звание, Ф.И.О.)

(подпись)

Санкт-Петербург

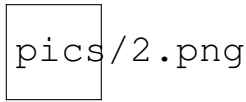
2021

Часть 1 - Настройка фильтрации пакетов (фаервол)



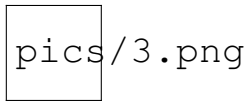
pics/1.png

Рис. 1 Выводим список правил iptables.



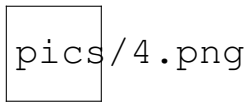
pics/2.png

Рис. 2 Выводим список правил iptables подробнее.



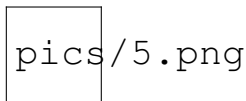
pics/3.png

Рис. 3 Выводим список команд необходимых для активации правил и политик.



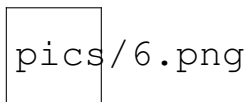
pics/4.png

Рис. 4 Разрешаем трафик на 80 и 22 порты для tcp протокола.



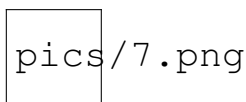
pics/5.png

Рис. 5 Удаляем разрешение для порта 22.



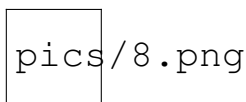
pics/6.png

Рис. 6 Правило, позволяющее устанавливать исходящее соединение.



pics/7.png

Рис. 7 Запрещаем все входящие и разрешаем все исходящие.



pics/8.png

Рис. 8 Правила для блокировки наиболее распространенных атак.

Часть 2 - Мониторинг журналов с использованием logcheck

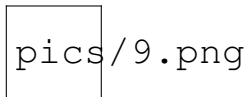


Рис. 9 logcheck успешно установлен.

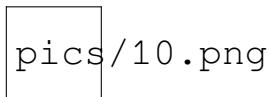


Рис. 10 Изменили REPORTLEVEL с server на paranoid.

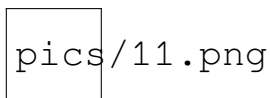


Рис. 11 Логи из файла /var/log/syslog.

Часть 3 - Установка и настройка netfilter

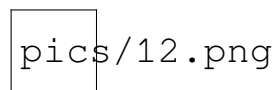


Рис. 12 Помечаем каждый пакет с помощью модуля conntrack.

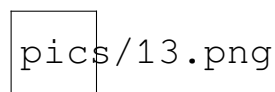


Рис. 13 Сопоставляем метки с состоянием битов.

Часть 4 - Осуществить защиту файловой системы.

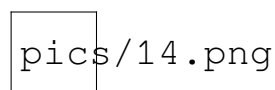


Рис. 14 Подменяем внутренний ip на внешний для всех пакетов, а также разрешаем перенаправлять пакеты между внутренними интерфейсами.

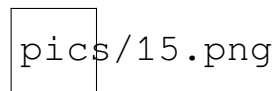


Рис. 15 Устанавливаем пакет iptables-persistent.

Часть 6 - Установка LOIC на Kali Linux.

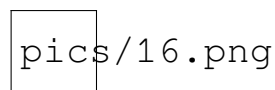


Рис. 16 Скачиваем git-core.

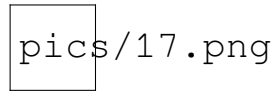


Рис. 17 Устанавливаем git-core с помощью утилиты dpkg.

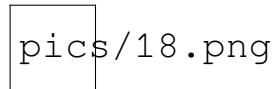


Рис. 18 Проверям установился ли пакет git-core.

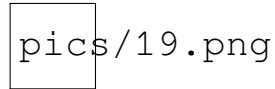


Рис. 19 Команда для установки MonoDevelop.

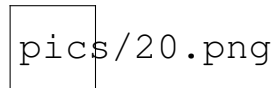


Рис. 20 Команда для установки MonoDevelop.

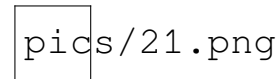


Рис. 21 Команда для установки MonoDevelop.

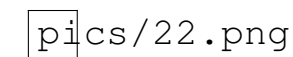


Рис. 22 Интерфейс программы MonoDevelop.

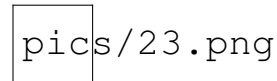


Рис. 23 Создаем папку и скачиваем скрипт для установки loic.

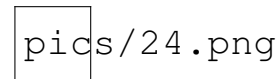


Рис. 24 Делаем скрипт исполняемым файлом.

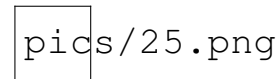


Рис. 25 Правим скрипт.

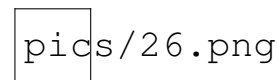


Рис. 26 Запускаем установку loic.

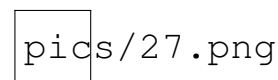


Рис. 27 Обновляем.

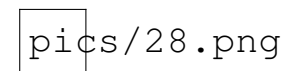


Рис. 28 Программа loic установлена, и запущена.

Часть 7 - Установка Wifi_Jammer на Kali Linux.

pics/29.png

Рис. 29 Клонировем из репозитория на github wifijammer.git.

pics/30.png

Рис. 30 Убеждаемся, что у нас не установелна библиотека scapy, для python 2.

pics/31.png

Рис. 31 wifijammer работает, после установки недостающего пакета.

Часть 8 - Использование SQLMAP на Kali Linux: взлом веб-сайтов и баз данных через SQL-инъекции

pics/32.png

Рис. 32 Производим SQL-инъекцию со стандартным поведением.

pics/33.png

Рис. 33 Производим SQL-инъекцию со стандартным поведением и случайным user-agent.

Часть 9 - Crunch — генератор паролей. Установка и тест.

pics/34.png

Рис. 34 Генерируем пароли от 1 до 9 цифр с использованием 0123456789abcdefg.

pics/35.png

Рис. 35 Пример паролей.

pics/36.png

Рис. 36 Генерируем пароли из 9 цифр с использованием 0123 и сохраняем их в файл passwords.txt.

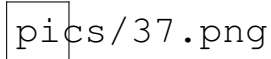


Рис. 37 Проверяем файл passwords.txt.

Вывод

В ходе данной лабораторной работы мы научились настраивать стандартный фаервол linux - iptables. Также установили мониторинг журналов logcheck и произвели его настройку. Установили программы MonoDevelop, Loic и wifijammer. Сделали попытку совершить SQL-инъекцию на сайт zss.sut.ru, и изучили работу консольной программы crunch.