Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**ЛАБОРАТОРНАЯ РАБОТА №10**

**Дисциплина: Информационная безопасность**

Работу выполнил: Романов В.В.

Направление подготовки: 02.03.02 Фундаментальная информатика и информационные технологии

Преподаватель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Шиян В.И.

**Цель:** Получение теоретических и практических навыков работы с песочницами и файловыми антивирусами. Изучить работу почтового сервера, получить практические навыки работы по защите от спама.

**Ход работы:**

**Часть 1**

Проведем исследование сети и определим публичный IP-адрес компьютера с использованием команды ifconfig.На рисунке 1 представлен результат.

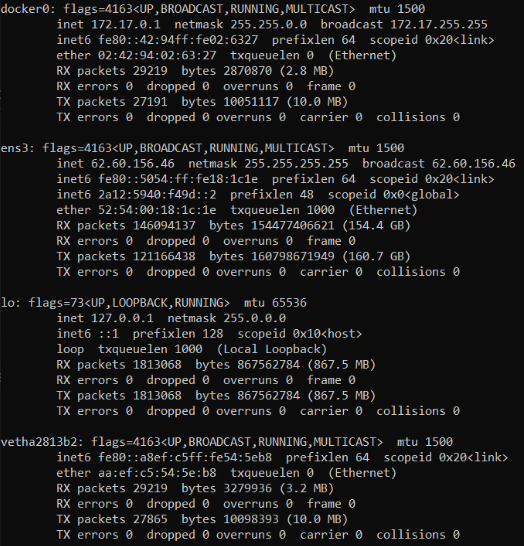


Рисунок 1 – Вывод команды ifconfig

**После этого установим Snort и настроим защиту сети**:

sudo apt-get install snort.

В процессе установки укажем диапазон защищаемой сети в формате X.X.X.0/24, где X.X.X соответствует первым 3-ем числам IP-адреса.

Инициализировал работу Snort с помощью команды sudo service snort start. Программа успешно запущена и готова к обработке трафика.

**Настроим правило для отслеживания посещений сайта Google.**  
В файле test.rules создал правило:

alert tcp any any -> any any (content:"https://www.google.ru/"; msg:"Someone open Google website"; sid:12312313;)

Данное правило генерирует оповещение при обнаружении трафика, связанного с открытием сайта Google. Подключил файл с правилом в конфигурации Snort и подтвердил его корректность.

**Добавил правило для обнаружения NULL-сканирования.** В тот же файл добавил следующее правило:

alert tcp any any -> any any (msg:"NULL Scan"; flags:0; sid:322222;)

Это правило отслеживает сканирование с нулевыми флагами в TCP-пакетах. Перезапустил Snort для применения нового правила.

**Проведем сканирование null-пакетами с другой ВМ.**С помощью программы nmap на второй виртуальной машине выполнил NULL-сканирование (sudo nmap -sN) защищаемой сети. Snort успешно зафиксировал данное действие и сгенерировал оповещение в логах. На рисунке 2 представлен результат.

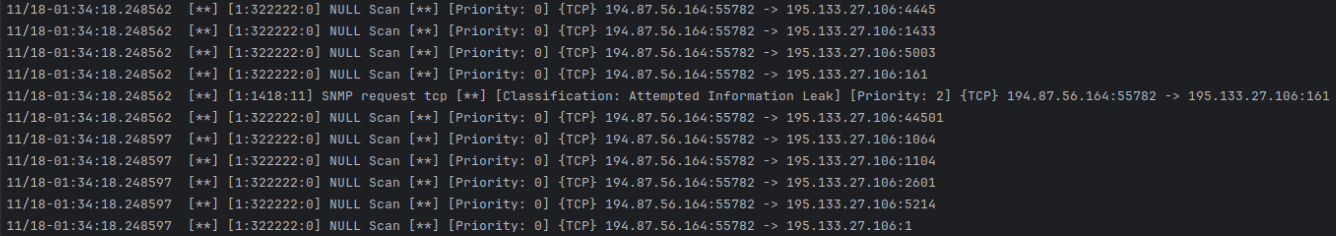


Рисунок 2 – Сканирование null-пакетами

**Проведём дополнительные сканирования, включая XMAS-сканирование.**  
Используем разные методы сканирования (nmap -sX для XMAS-сканирования) для проверки устойчивости сети и реакции Snort. В логах были зафиксированы соответствующие предупреждения. На рисунке 3 представлен результат.

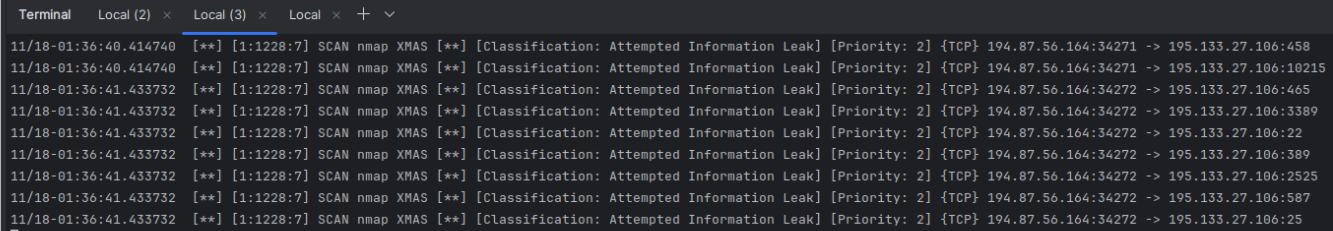


Рисунок 3 – Сканирование XMAS

### **Часть 2**

Так как программа Splunk недоступна для скачивания, то выполнить практические шаги из этой части не удалось. Но несмотря на это, теоретически выполним следующие действия:

1. Загрузить и установить платформу Splunk Enterprise.  
   Загрузить дистрибутив с официального сайта, установить программу с использованием команды dpkg -i splunk\_package\_name.deb (или иной соответствующей команды для вашей операционной системы).
2. Настроить Splunk для работы с журналами событий.  
   После установки запустить Splunk с помощью команды /opt/splunk/bin/splunk start, а затем войти в веб-интерфейс системы для настройки. В разделе **Settings → Data Inputs** подключить файл журнала /var/log/auth.log и указать его для непрерывного мониторинга.
3. Импортировать логи Snort в Splunk.  
   Убедиться, что Snort работает в режиме логирования (sudo snort -A console -i eth0 -c snort.conf -l /var/log/snort/). Затем настроить Splunk на мониторинг созданных логов, что позволит анализировать данные в удобном интерфейсе.
4. Проверить интеграцию Snort и Splunk.  
   Сгенерировать события с помощью сканирования сети и убедиться, что логи Snort корректно отображаются в Splunk. Дополнительно можно было бы установить приложение Snort для Splunk из официального каталога приложений.

**Вывод:** изучил и использовал системы обнаружения вторжений Snort, а также установил и настроил правила для мониторинга сетевого трафика и реагирования на определённые события, такие как посещение сайта Google и NULL-сканирование.