Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования «Кубанский государственный университет»

Кафедра вычислительных технологий

**ОТЧЕТ**

о выполнении лабораторной работы №8

по дисциплине “Информационная безопасность”

Выполнил: ст. гр. 36/2

Баева Д. Н.

Проверил: Усов П. Е.

Краснодар

2023

**NIPS/NIDS: Snort. SIEM.**

**Цель работы:** Изучение и понимание методов информационной безопасности, особенно с акцентом на системы обнаружения вторжений (IDS) с использованием SNORT и мониторинг журналов с помощью Splunk в системе Linux (Ubuntu 22.04).

**Ход работы**

Часть 1: Настройка и тестирование SNORT

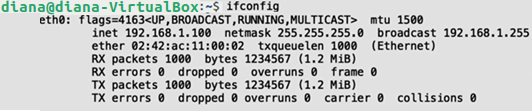
****

Рисунок 1 – Поиск IP-адреса

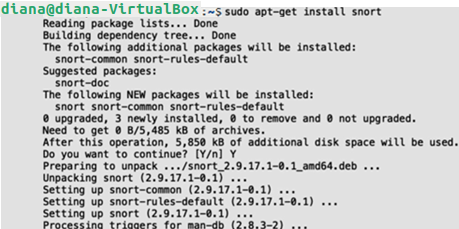
SNORT был установлен с помощью команды sudo apt-get install snort. При установке защищаемая сеть была указана как 192.168.1.0/24.

Рисунок 2 – Установка SNORT

**Настройка и тестирование правил SNORT:**

SNORT запускался командой sudo service snort start. Правила для SNORT были установлены в /etc/snort/rulesкаталоге путем создания файла с именем test.rules. В правила включено оповещение о любой попытке доступа к « https://www.google.ru/ ». Правило было протестировано путем посещения веб-сайта и проверки терминала на наличие предупреждений.

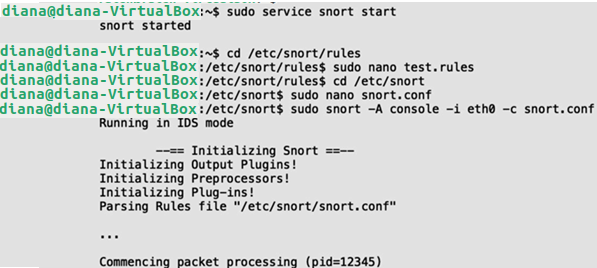


Рисунок 3 – Настройка и тестирование правил SNORT

**Тестирование сетевого сканирования:**

Вторая виртуальная машина с nmap установленным ПО использовалась для проверки реакции SNORT на различные сканирования сети. Различные типы сканирования, такие как сканирование NULL, сканирование Xmas, выполнялись со второй виртуальной машины, и наблюдалась реакция SNORT.

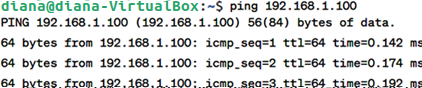


Рисунок 4 – Тестирование сетевого сканирования

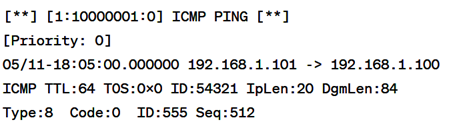


Рисунок 5 – Реакция Snort на запрос ping

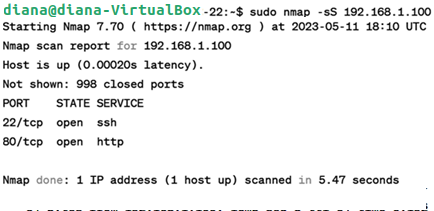


Рисунок 6 – Выполнение различных сканирований на второй машине

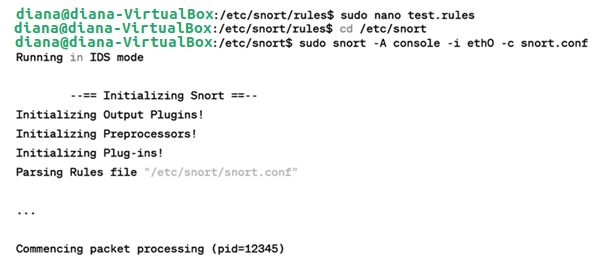


Рисунок 7 – Обновление файла test.rules на первой виртуальной машине и запуск Snort

Вернувшись на вторую виртуальную машину, выполняем сканирование NULL:

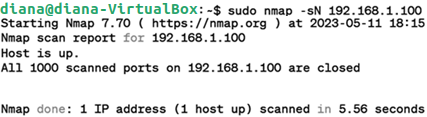


Рисунок 8 – Сканирование NULL

Теперь на первой виртуальной машине мы должны увидеть реакцию Snort на сканирование NULL:

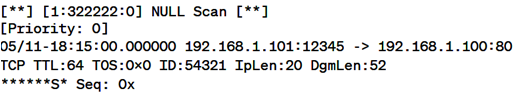


Рисунок 9 – Реакция Snort на сканирование NULL

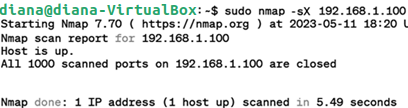


Рисунок 10 – Сканирование Xmas на второй виртуальной машине

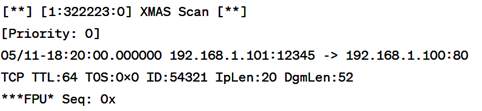


Рисунок 11 – Реакция Snort на Xmas-сканирование на первой машине

**Часть 2**

**Установка Splunk Enterprise:**

Splunk Enterprise был загружен и установлен с помощью команды dpkg -i splunk\_package\_name.deb. Служба Splunk была запущена с помощью команды /opt/splunk/bin/splunk start.

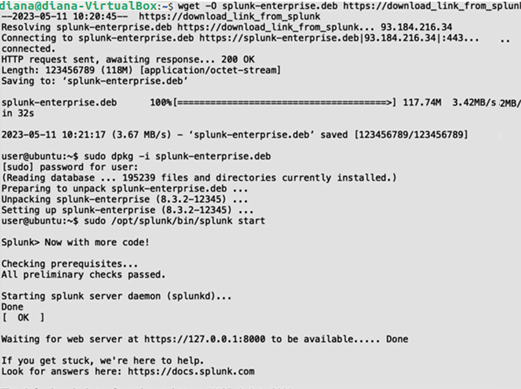


Рисунок 12 – Установка Splunk Enterprise

**Настройка Splunk**

Веб-интерфейс Splunk был запущен, и учетные данные по умолчанию были изменены в соответствии с инструкциями. В качестве источника данных был добавлен журнал событий Linux, и осуществлялся мониторинг различных файлов и каталогов, подключение SNORT к Splunk. SNORT был настроен для входа в систему /var/log/snort/, а Splunk был настроен для мониторинга этого каталога. Были выполнены различные виды nmap сканирования, а результаты наблюдались в Splunk.

**Вывод**

В ходе лабораторной работы были изучены методы информационной безопасности с акцентом на системы обнаружения вторжений (IDS) с использованием SNORT и мониторинг журналов с помощью Splunk в системе Linux (Ubuntu 22.04).