Практическое задание № 13.
Система обнаружения и предотвращения вторжений Snort

Опубликовано **26.11.2025**

Дедлайн **17.12.2025**

Лабораторная работа посвящена системе обнаружения вторжений Snort. Для выполнения работы понадобятся две виртуальные машины с Linux. Одна для защиты, другая для атаки.

1 Задания

1.1 Установка и настройка Snort

Для установки Snort нужно выполнить команду:

```
apt-get install snort
```

Настройка Snort осуществляется через файлы конфигурации (обычно из директории /etc/snort/).
Откройте /etc/snort/snort.conf в любом редакторе.
После каждого изменения необходимо перезапускать Snort, чтобы применить изменения:

```
service snort restart
```

1.2 Детектирование ping

Выполните с помощью утилиты ping запрос на целевую машину с запущенным Snort. Что находится в логах?

1.3 Детектирование сканирования портов

1. В файле snort.conf нужно раскомментировать строку, которая включает препроцессор sfportscan.
2. В настройках препроцессора укажите файл для логирования.
3. Перезапустите Snort, чтобы изменения вступили в силу.
4. Просканируйте машину с помощью nmap разными способами
5. Какие виды сканирования обнаруживает Snort?

1.4 Детектирование утечки данных

1. Запустите http-сервер на машине со Snort:

   service apache2 start

   или

   service nginx start

   Альтернативно: запустить nginx.

2. С другой машины попробуйте открыть адрес:
   http://IP_адрес/etc/shadow
   или
   http://IP_адрес/etc/passwd
3. Проверьте логи

1.5 Детектирование web-сканеров

1. Просканируйте защищаемую систему с помощью одного из web-сканеров, например:
   nikto -host 10.0.1.111
2. Что отображается в логах Snort?

1.6 Детектирование применения эксплойтов

1. Выявить применение эксплойта к Hearbleed
2. Проверить какие эксплойты-скрипты к Nmap выявляет Snort
3. При необходимости скачать и установить свежие версии правил (см. Материалы)
   Список: https://nmap.org/nsedoc/categories/exploit.html

1.7 Создание правил

1. Составьте правила, которые детектируют скачивание mp3-файла и доступ к запрещенному сайту.
2. Поместите его в файл /etc/snort/rules/local.rules и перезагрузите Snort.
3. Для проверки правила используйте браузер.

Подсказка: используйте uricontent

Материалы

1. Последняя версия community-правил:
   `https://www.snort.org/downloads/community/community-rules.tar.gz`