Лабораторная работа №2

Тема: Методы детектирования и блокировки сканирования сети (Nmap) с помощью Suricata.

Теория

Port scanning — это метод анализа состояния сетевых портов (открытый/закрытый) для поиска сервисов и потенциальных уязвимостей.

nmap — один из самых популярных инструментов для обнаружения хостов, сервисов и ОС в сети. Среди вариантов сканирования — SYN scan (`-sS`), TCP Connect (`-sT`), UDP scan (`-sU`), XMAS scan (`-sX`), OS fingerprinting (`-O`), и др.

Suricata — современная IPS/IDS, умеющая обнаруживать и блокировать сетевые сканирования по сигнатурам (пакетным признакам).

Методология защиты от сканирования включает:

- Сигнатурный анализ (правила Suricata)
- Блокировку опасных или подозрительных соединений (IPS режим)
- Ведение журналов для расследования

Практическая часть

1. Подготовка лабораторного стенда

Аналогично ЛР1, используется docker-compose:

- `attacker` — контейнер с Kali Linux (kalilinux/kali-rolling:latest)
- `victim` — контейнер на Alpine с запущенными базовыми сервисами (например, HTTP)
- Suricata IPS/IDS подключён к bridge-сети Docker, анализирует трафик между контейнерами
- EveBox - инструмент управления оповещениями и событиями Suricata

Для конфигурации EveBox (https://evebox.org/) воспользуйтесь официальной документацией

2. Базовые правила для блокировки и детектирования nmap scans

2.1. Синтаксис правил Suricata

```
# Пример сигнатуры scan SYN (nmap -sS)
drop tcp any any -> any any (flags:S; msg:"[IPS] NMAP SYN Scan Blocked";
threshold: type both, track by_src, count 10, seconds 6; sid:1001001;
rev:1;)

# Пример детектирования Xmas scan (nmap -sX)
alert tcp any any -> any any (flags:FPU; msg:"[IDS] NMAP XMAS Scan
Detected"; threshold: type both, track by_src, count 5, seconds 6;
sid:1001002; rev:1;)

# Пример блокировки UDP scan
drop udp any any -> any any (msg:"[IPS] NMAP UDP Scan Blocked"; threshold:
type both, track by_src, count 10, seconds 10; sid:1001003; rev:1;)

# Пример детектирования OS-фингерпринтинга (nmap -O)
alert ip any any -> any any (msg:"[IDS] Possible OS Fingerprinting Attempt";
ipopts: any; threshold: type both, track by_src, count 5, seconds 20;
sid:1001101; rev:1;)
```

Пояснения к элементам правила:

- `drop` — блокировать соединение
- `alert` — только логировать
- `flags:` — TCP-флаги, специфичные для типа сканирования
- `msg:` — текст сообщения
- `threshold:` — срабатывайте на серию событий
- `sid:` — уникальный идентификатор
- `rev:` — ревизия

3. Добавление и активация правил

Отредактируйте файл `/etc/suricata/rules/local.rules` и внесите сигнатуры.

Проверьте/отредактируйте раздел rule-files в `suricata.yaml`:

```
rule-files:
  - local.rules
```

Перезагрузите Suricata:

```
systemctl restart suricata
```

4. Генерация тестового трафика

Запустите сканирование с attacker:

- SYN scan: `nmap -sS victim_ip`
- Xmas scan: `nmap -sX victim_ip`
- UDP scan: `nmap -sU victim_ip`
- OS fingerprinting: `nmap -O victim_ip`

Проверьте логи:

- `/var/log/suricata/eve.json` — события блокировки/детектирования
- Проверьте результаты в EveBox

---

5. Блокировка всех nmap-сканирований

IPS-режим позволяет не просто выявлять, но и блокировать попытки сканирования:

- Для критических сценариев (например, SYN/UDP scans с броскими пакетными паттернами) используйте `drop`.
- Для OS-фингерпринтинга и редких техник лучше логировать с помощью `alert` для обзора событий.
- Блокировка осуществится на уровне iptables + NFQUEUE (как в ЛР1).

Пример проверки:

- После запуска сканирования убедитесь, что соединения прерываются, а попытки сканирования не доходят до victim.
- В логах Suricata вы должны увидеть события drop для заблокированных попыток (например, "NMAP SYN Scan Blocked") и alert для детектированных, но не заблокированных техник.

6. Работа с ложными срабатываниями и оптимизация

- При большом количестве ложных срабатываний корректируйте threshold/count/seconds — увеличивайте порог или задавайте исключения по src_ip.
- Для production-сетей рекомендуется отрабатывать каждую выявленную сигнатуру на реальном трафике и корректировать конфигурацию.

7. Примеры правил для других техник nmap

```
# ACK scan (nmap -sA)
alert tcp any any -> any any (flags:A; msg:"[IDS] NMAP ACK Scan Detected";
threshold: type both, track by_src, count 5, seconds 10; sid:1001004;
rev:1;)

# Фин-флаг портсканирование (nmap -sF)
alert tcp any any -> any any (flags:F; msg:"[IDS] NMAP FIN Scan Detected";
threshold: type both, track by_src, count 3, seconds 10; sid:1001005;
rev:1;)

# Null scan (nmap -sN)
alert tcp any any -> any any (flags:0; msg:"[IDS] NMAP NULL Scan Detected";
threshold: type both, track by_src, count 2, seconds 10; sid:1001006;
rev:1;)
```

Вопросы по работе

- Почему важно блокировать сканирование сети?
- Чем опасны техники фингерпринтинга и что такое OS Fingerprinting?
- Какие проблемы могут возникать при избыточной блокировке?
- Как корректировать сигнатуры для уменьшения ложных срабатываний?

Дополнительное задание со звездочкой

Реализуйте детальное логирование попыток сканирования, привяжите алерты к отдельным src_ip, выведите статистику по самим алертам (например, используя jq по

eve.json). Протестируйте стойкость правил к обходу (фрагментации, медленным сканам).