ЛАБОРАТОРНА РОБОТА №3
АНАЛІЗ БАЗОВОГО МЕРЕЖЕВОГО ТРАФІКУ

Мета роботи:

1. Ознайомлення з поняттям базової лінії (Baseline) мережевого трафіку та її значенням у процесі виявлення аномалій.

2. Отримання практичних навичок захоплення та аналізу мережевого трафіку за допомогою інструментів Kali Linux.

3. Дослідження можливості моніторингу подій у SIEM-системі Wazuh та аналіз мережевої активності, включаючи виявлення нетипових запитів.

Інструменти та ПЗ: Kali Linux, SIEM-система Wazuh.

Теоретичні відомості

Базова лінія (Baseline) – це сформований на основі спостережень еталонний профіль штатної мережевої активності інформаційної інфраструктури. Вона відображає характерні параметри функціонування мережі за умов відсутності інцидентів безпеки та виикористовується як точка відліку для виявлення аномалій, відхилень і потенційно шкідливої активності.

До структури базової лінії лінії входять такі компоненти:

1. Типові моделі трафіку – регулярні комунікації між системами.

2. Обсяги даних – звичайна кількість переданих даних за одиницю часу.

3. Часові патерни – періоди активності та спокою в мережі.

4. Протокольний склад – типові протоколи та порти, що використовуються.

Базова лінія критично важлива для:

1. Виявлення аномалій – відхилення від нормального трафіку можуть сигналізувати про загрози.

2. Налаштування SIEM – правильна конфігурація правил виявлення.

3. Зменшення хибних спрацьовувань.

Типи мережевого трафіку

У процесі аналізу мережевої активності трафік доцільно класифікувати на легітимний та підозрілий.

Легітимний трафік відповідає бізнес-процесам організації та очікуваним сценаріям використання мережі. До нього належать:

1. HTTP/HTTPS-запити до веб-додатків і корпоративнних сервісів (внутрішніх або зовнішніх)

2. DNS-запити для перетворення домениих імен у IP-адреси.

3. Процеси автентифікації користувачів у доменній інфраструктурі або корпоративних системах.

4. Оновлення програмного забезпечення з офіційних репозиторіїв або серверів вендорів.

Підозрілий трафік містить ознаки, що відхиляються від встановленої базової лінії та можуть свідчити про інцидент безпеки. До його характеристик належать:

1. Незвичайні обсяги переданих даних, зокрема різке зростання outbound-трафіку, що може вказувати на витік інформації.

2. Комунікації з невідомими або нетиповими IP-адресами, особливо з зовнішніми хостами, з якими раніше не було взаємодії.

3. Використання нестандартних портів або протоколів, які не застосовуються у звичайній роботі інфраструктури.

4. Активність у нетиповий час, наприклад, інтенсивний трафік у неробочі години.

Інструменти аналізу трафіку

Tcpdump – це консольний інструмент для перехоплення та аналізу мережевих пакетів на рівні мережевого інтерфейсу. Він широко використовується в середовищах Linux/Unix для оперативного моніторингу трафіку.

Основні можливості Tcpdump:

1. Захоплення трафіку в реальному часу безпосередньо з мережевого інтерфейсу.

2. Гнучка фільтрація пакетів за IP-адресами, портами, протоколами (BPF-фільтри).

3. Збереження перехоплених даних у файл (pcap) для подальшого аналізу в інших інструментах.

Wireshark – це графічний аналізатор мережевих протоколів, який дозволяє виконувати глибокий аналізу мережевих пакетів на різних рівнях моделі OSI.

Основні функції Wireshark:

1. Детальний розбір протоколів (Ethernet, IP, TCP, HTTP, DNS тощо) з декодуванням полів пакетів.

2. Візуалізація мережевих потоків і сесій, зокрема TCP-stream analysis.

3. Розширені механізми фільтрації та пошуку, що дозволяють точно виділяти релевантний трафік.

Netstat – це системна утиліта для відображення стану мережевих з'єднань і статистики мережевої підсистеми.

Основні можливості Netstat:

1. Перегляд активних TCP та UDP-з'єднань, включаючи локальні та віддалені адреси

2. Відображення станів сокетів (LISTEN, ESTABLISHED, TIME_WAIT тощо).

3. Отримання статистики мережевих інтерфейсів.

4. Перегляд таблиці маршрутизації.

Методологія створення базової лінії

Створення базової лінії здійснюється поетапно та включає такі основні кроки:

1. Збір даних протягом репрезентативного періоду.
2. Аналіз патернів трафіку різних типів.
3. Документунвання нормальної поведінки.
4. Створення правил для автоматизованого моніторингу.
5. Регулярне оновлення базової лінії.

Завдання на лабораторну роботу

Завдання 1. Запуск необхідних сервісів.

1. Запустіть усі необхідні сервіси (якщо раніше не було запущено):

   sudo ./lab-management.sh start wazuh

   sudo ./lab-management.sh start vuln-lab

2. Переконайтеся, що веб-додатки доступні:

   DVWA: http://localhost:80

   Juice Shop: http://localhost:3000

3. Відкрийте термінал у Kali Linux
4. У терміналі Kali виконайте сканування мережі:

   nmap -sn 172.20.0.0/24

5. Визначте активні хости та запишіть їх IP-адреси:

   nmap -sS -O 172.20.0.0/24

6. Ідентифікуйте основні сервіси:

   nmap -sV -p 1-1000 172.20.0.0/24

Завдання 2. Захоплення базового трафіку.

1. У Kali Linux запустіть tcpdump для захоплення трафіку:

   sudo tcpdump -i any -w baseline_traffic.pcap -v

2. Відкрийте новий термінал (залиште tcpdump працювати в першому).
3. Відкрийте Firefox у Kali Linux.
4. Поступово перейдіть до кожного веб-додатку та виконайте типові дії:

   DVWA (http://172.20.0.20):

   - Увійдіть з обліковими даними: admin/password.

   - Перегляньте головну сторінку.

   - Перейдіть до розділу "DVWA Security".

   - Змініть рівень безпеки на "Low".

   - Перегляньте різні уразливості без виконання атак.

Juice Shop (http://172.20.0.40:3000):

- Перегляньте головну сторінку.

- Перегляньте каталог товарів.

- Зареєструйте акаунт користувача.

- Увійдіть до системи.

- Перегляньте профіль користувача.

5. Дочекайтеся накопичення трафіку (мінімум 5-7 хвилин активності).
6. Зупиніть tcpdump (Ctrl+C у першому терміналі).
7. Перевірте розмір захопленого файлу:

```
ls -lh baseline_traffic.pcap
```

8. Отримайте базову статистику пакетів:

```
tcpdump -r baseline_traffic.pcap | wc -l
```

Завдання 3. Аналіз захопленого трафіку.

1. Проаналізуйте розподіл протоколів:

```
tcpdump -r baseline_traffic.pcap -n | awk '{print $3}' | cut -d: -f1 | sort | uniq -c | sort -nr
```

2. Визначте найпопулярніші порти:

```
(echo -e "COUNT\tDEST_PORT"; tcpdump -r baseline_traffic.pcap -n 'tcp or udp' 2>/dev/null | awk '{split($5,a,"."); split(a[length(a)],b,":"); print b[1]}' | sort | uniq -c | sort -nr | head -20) | column -t
```

3. Ідентифікуйте основні напрямки трафіку:

```
tcpdump -r baseline_traffic.pcap -n | awk '{print $3 " -> " $5}' | sort | uniq -c | sort -nr | head -20
```

4. Виділіть HTTP запити:

```
tcpdump -r baseline_traffic.pcap -A | grep -E "(GET|POST|PUT|DELETE)" | head -20
```

5. Ідентифікуйте User-Agent рядки:

```
tcpdump -r baseline_traffic.pcap -A | grep -i "user-agent" | sort | uniq
```

6. Проаналізуйте HTTP статус коди:

```
tcpdump -r baseline_traffic.pcap -A | grep -E "HTTP/[0-9]\.[0-9] [0-9]{3}" | sort | uniq -c
```

7. Визначте пікові періоди активності:

```
tcpdump -r baseline_traffic.pcap -tt | awk '{print strftime("%H:%M", $1)}' | sort | uniq -c | sort -nr
```

Завдання 4. Розширений аналіз з Wireshark.

1. Відкрийте файл baseline_traffic.pcap у Wireshark:

```
xhost +local:root
sudo -E wireshark baseline_traffic.pcap
```

2. Використайте фільтри Wireshark для детального аналізу.

```
tcp.port == 80
ip.addr == 172.20.0.20
```

Завдання 5. Моніторинг у Wazuh (сканування Nmap).

1. Відкрийте Wazuh Dashboard:

```
https://localhost:443
```

2. Увійдіть з обліковими даними:

```
admin/SecretPassword
```

3. У Wazuh Dashboard перейдіть до “Discover”.
4. Встановіть фільтр за останню годину (або час виконання сканування за допомогою Nmap).
5. Знайдіть події, пов’язані зі скануванням Nmap.
6. Виберіть одну з подій та зафіксуйте:

   - IP-адреса джерела.

   - IP-адреса цілі.

   - HTTP-запит, який Nmap автоматично відправляє через свій NSE (Nmap Scripting Engine) для виявлення сервісів.

   - User-Agent в HTTP запиті від Nmap.

Завдання 6. Завершення роботи.

```
sudo ./lab-management.sh stop vuln-lab
```

Контрольні запитання

1. Що таке базова лінія (Baseline) мережевого трафіку?
2. Яка ознака найбільш імовірно свідчить про витік даних?
3. Яка команда використовується для перехоплення трафіку у Kali Linux?
4. У якому форматі зазвичай зберігається захоплений трафік?
5. Який інструмент використовується для графічного аналізу мережевих пакетів?
6. Яка команда дозволяє визначити активні хости в мережі?
7. Який стан TCP-з’єднання означає активну встановлену сесію?
8. Чому базову лінію потрібно регулярно оновлювати?