Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Отчёт по лабораторной работе №8

По дисциплине “Средства и методы защиты информации в интеллектуальных системах”

Выполнил:
Мулярчик Д.С

Проверил:
Сальников Д.А

Минск 2023

Цель: изучение материала, а также применение на практике полученных знаний по теме: “**Наблюдение за стеком TCP/IP**”

Задачи:

1. На основном компьютере запустить Виртуальную машину. Измените имя компьютера на уникальное.
2. Установить Snort.
3. Запустите Snort в режиме Sniffer пакетов или протоколирования с различными параметрами детализации.
4. Обратитесь к локальной сети. Выполните команду ping, запустите броузер или проводник. Сохраните какой либо файл (не большой) на материнской машине.
5. Остановите Snort. Определите к каким IP-портам и адресам были выполнены обращения.
6. Пользуясь \windows\system32\etc\service, определите какие системные службы использовались.
7. Просмотрите содержимое перехваченных пакетов.
8. **Используя дополнительную литературу расшифруйте содержание вывода заголовка.** Оформите отчет. В отчет обязательно поместите примеры пакетов и список обнаруженных протоколов и служб.

Реализация:

Для запуска режима перехвата пакетов используется команда:

sudo snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/local.rules -i enp0s3 -A alert_fast -s 65535 -k none

Пример тревоги на пингование через родительское устройство:

```
11/28-11:10:25.738964 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
11/28-11:10:25.739030 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
11/28-11:10:26.741875 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
11/28-11:10:26.741893 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
11/28-11:10:27.745642 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
11/28-11:10:27.745693 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
11/28-11:10:28.749049 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.56.1 -> 192.168.56.101
11/28-11:10:28.749102 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} 192.168.56.101 -> 192.168.56.1
11/28-11:10:29.090189 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} fe80::24c:54c4:d2b8:ce2b -> ff02::2
11/28-11:10:29.184099 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} fe80::aaf2:59ca:385f:106f -> ff02::1:ff0
9:1
11/28-11:11:30.184550 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] {ICMP} fe80::aaf2:59ca:385f:106f -> ff02::1:ff0
9:1
```

```
11/28-12:28:54.023495 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [Priority: 3] [AppID: UTMPCD] {TCP} 198.16.74.44:431 -> 10.0.3.15:41054
11/28-12:28:54.030813 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [Priority: 3] [AppID: UTMPCD] {TCP} 198.16.74.44:431 -> 10.0.3.15:41056
11/28-12:28:59.389127 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [Priority: 3] [AppID: UTMPCD] {TCP} 198.16.74.44:431 -> 10.0.3.15:41070
11/28-12:29:00.435837 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [Priority: 3] [AppID: UTMPCD] {TCP} 198.16.74.44:431 -> 10.0.3.15:41156
11/28-12:29:20.337658 [**] [1:10000001:0] "ICMP Traffic Detected" [**] [Priority: 0] [AppID: ICMP for IPv6] {ICMP} fe80::1bb0:58fb:d71f:5401 -> ff02::2
11/28-12:29:27.735525 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [Priority: 3] [AppID: UTMPCD] {TCP} 198.16.74.44:431 -> 10.0.3.15:42592
11/28-12:29:27.735605 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [Priority: 3] [AppID: UTMPCD] {TCP} 198.16.74.44:431 -> 10.0.3.15:42602
11/28-12:29:39.283906 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [Priority: 3] [AppID: UTMPCD] {TCP} 198.16.74.44:431 -> 10.0.3.15:34244
11/28-12:29:39.285133 [**] [129:15:1] "(stream_tcp) reset outside window" [**] [Priority: 3] [AppID: UTMPCD] {TCP} 198.16.74.44:431 -> 10.0.3.15:34254
```

Пример установки оповещения при обнаружении трафика от хоста appid Facebook:

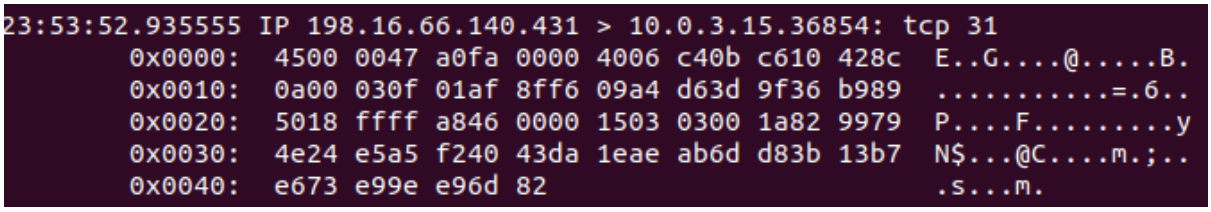
```
11/28-14:53:11.883881 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.883928 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
11/28-14:53:11.883881 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.883972 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
11/28-14:53:11.883966 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.884255 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
11/28-14:53:11.888011 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.889153 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
11/28-14:53:11.889343 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.889611 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
11/28-14:53:11.889784 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.890109 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
11/28-14:53:11.890309 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.897405 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.897884 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
11/28-14:53:11.898331 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.899119 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.899248 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
11/28-14:53:11.947813 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.948192 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
11/28-14:53:11.975631 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.976576 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
11/28-14:53:11.976959 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.977245 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
11/28-14:53:11.980446 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 31.13.81.36:443 -> 10.0.3.15:53534
11/28-14:53:11.993213 [**] [1:10000003:0] "Facebook Detected" [**] [Priority: 0] [AppID: Facebook] {TCP} 10.0.3.15:53534 -> 31.13.81.36:443
```

Список использованных служб:

```
Appid Statistics
-------------------------------------------------
detected apps and services
             Application: Services   Clients    Users      Payloads   Misc       Referred
                     dns: 31         31         0          0          0          0
                     ssl: 152        0          0          0          0          0
                   https: 1          0          0          0          0          0
                    mdns: 2          0          0          0          0          0
                  utmpcd: 185        0          0          0          0          0
           icmp_for_ipv6: 1          0          0          0          0          0
                 unknown: 7          0          0          153        0          0
-------------------------------------------------
```

Пример 2х пакетов, с данными и без соответственно:

```
23:53:28.425132 IP 10.0.3.15.36858 > 198.16.66.140.431: tcp 0
        0x0000:  4500 0028 c14a 4000 4006 63da 0a00 030f  E..(.J@.@.c.....
        0x0010:  c610 428c 8ffa 01af 43a6 1769 09ac c1b7  ..B.....C..i....
        0x0020:  5010 ffff 15c6 0000                      P.......
```



Разбор взятых пакетов:

1)

- Протокол: IP
- Исходный IP-адрес: 10.0.3.15
- Порт исходного узла: 36858
- Целевой IP-адрес: 198.16.66.140
- Порт целевого узла: 431
- Протокол внутри IP-пакета: TCP
- Длина пакета: 0

2)

- Протокол: IP
- Исходный IP-адрес: 198.16.66.140
- Порт исходного узла: 431
- Целевой IP-адрес: 10.0.3.15
- Порт целевого узла: 36854
- Протокол внутри IP-пакета: TCP
- Длина пакета: 31 байт

Вывод: в ходе выполнения лабораторной работы мною были получены практические знания по работе с утилитой Snort, её методами для перехвата пакетов, анализа данных отправляемых и получаемых устройством