

KHOA CÔNG NGHỆ THÔNG TIN

THỰC HÀNH HỆ THỐNG PHÁT HIỆN PHÒNG CHỐNG XÂM NHẬP

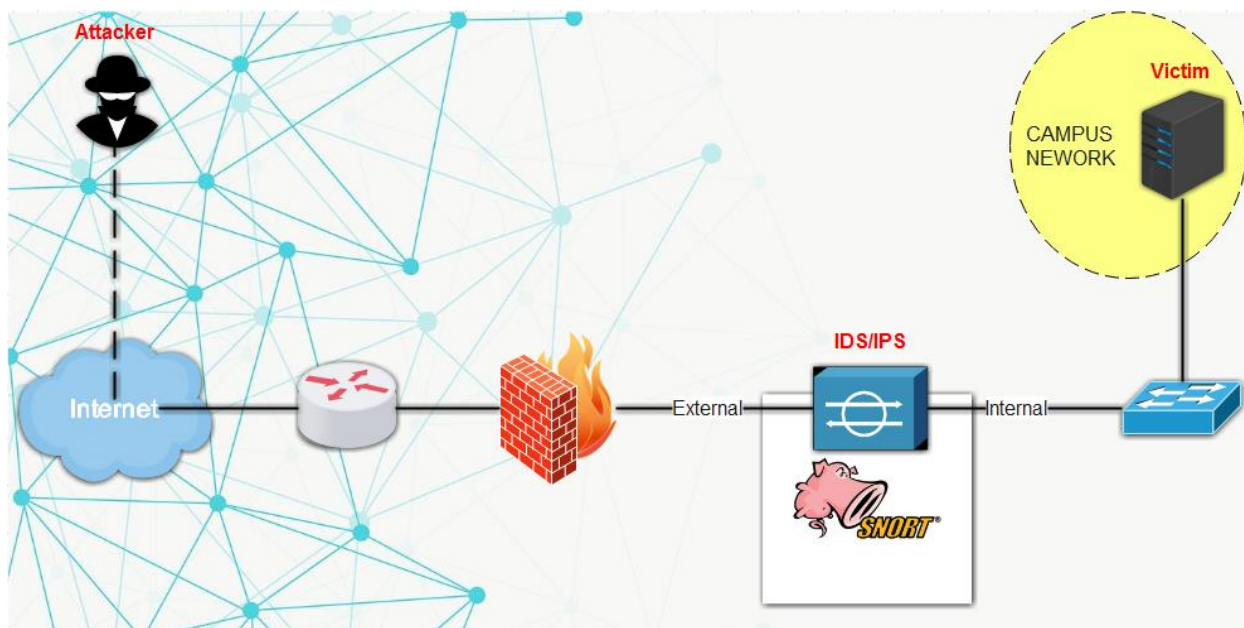
THỰC HÀNH 3 - CÀI ĐẶT VÀ THỰC NGHIỆM SNORT IDS/IPS



Nội dung:

1. Mô hình	3
2. Mục tiêu	3
3. Kịch bản	3
4. Thực hiện	4
4.1. Thiết lập các thông số kết nối mạng cho các máy	4
4.2. Cài đặt Snort trên CentOS	6
4.3. Cấu hình Snort NIDS mode.....	6
4.4. Cấu hình Snort Inline mode	9
4.5. Phát cảnh báo và ngăn chặn tấn công Ping of Death	9
Bài tập	11

1. Mô hình



Máy	Hệ điều hành	Địa chỉ IPv4	Interface
Attacker	Kali Linux	192.168.21.x/24	VMNet 1
IDS/IPS	CentOS 8 (đề xuất)	192.168.21.y/24 và 192.168.101.y/24	VMNet 1 (External) và VMNet 2 (Internal)
Victim	Windows Server 2008/2012	192.168.101.x/24	VMNet 2

Phần mềm triển khai: VMware Workstation, các hệ điều hành liên quan

2. Mục tiêu

- Cài đặt Snort trên CentOS
- Cấu hình Snort NIDS mode
- Cấu hình Snort Inline mode
- Cài đặt các package hỗ trợ Snort
- Xây dựng các tình huống/kịch bản cho việc khảo sát hệ thống Snort IDS/IPS

3. Kịch bản

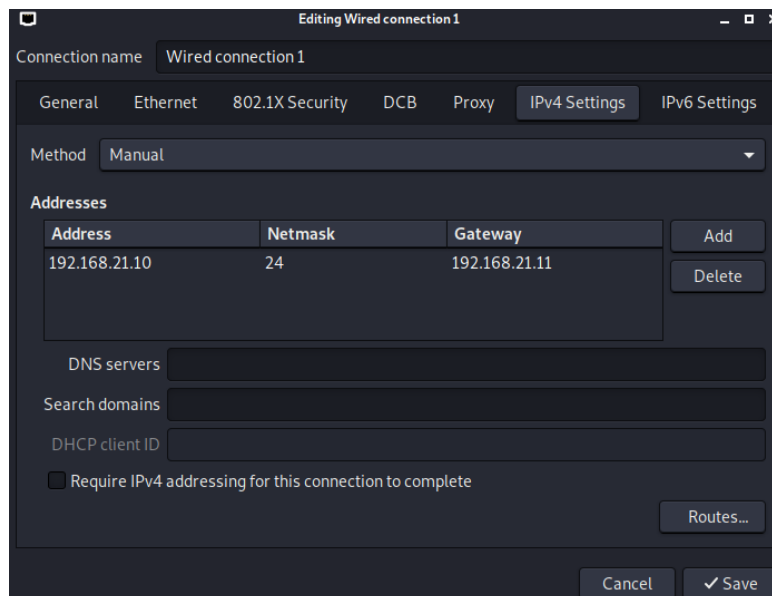
Giả lập một hệ thống Snort IDS/IPS, triển khai NIDS mode và Inline mode để phát hiện và ngăn chặn các xâm nhập của Attacker đến Victim trong môi trường mạng CAN. Từ đó, phát triển các kịch bản, tình huống khác nhau nhằm tìm hiểu, phân tích, khảo sát, thực nghiệm hệ thống Snort IDS/IPS.

4. Thực hiện

4.1. Thiết lập các thông số kết nối mạng cho các máy

- Attacker

→ Các thông số mạng



```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.21.10 netmask 255.255.255.0 broadcast 192.168.21.255
    inet6 fe80::20c:29ff:feb0:f70f prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:b0:f7:0f txqueuelen 1000 (Ethernet)
    RX packets 18 bytes 4468 (4.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 98 bytes 14460 (14.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 14 bytes 866 (866.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14 bytes 866 (866.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

→ Kiểm tra kết nối máy Victim

```
(kali@kali)-[~]
$ ping 192.168.101.10
PING 192.168.101.10 (192.168.101.10) 56(84) bytes of data.
64 bytes from 192.168.101.10: icmp_seq=1 ttl=127 time=1.43 ms
64 bytes from 192.168.101.10: icmp_seq=2 ttl=127 time=1.18 ms
64 bytes from 192.168.101.10: icmp_seq=3 ttl=127 time=0.683 ms
64 bytes from 192.168.101.10: icmp_seq=4 ttl=127 time=0.762 ms
64 bytes from 192.168.101.10: icmp_seq=5 ttl=127 time=0.762 ms
64 bytes from 192.168.101.10: icmp_seq=6 ttl=127 time=0.776 ms
64 bytes from 192.168.101.10: icmp_seq=7 ttl=127 time=0.843 ms
```

- Snort IDS/IPS

→ Các thông số mạng

```
[husky@localhost ~]$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.21.11 netmask 255.255.255.0 broadcast 192.168.21.255
    inet6 fe80::20c:29ff:fe12:e0de prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:12:e0:de txqueuelen 1000 (Ethernet)
    RX packets 15 bytes 3630 (3.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 79 bytes 11784 (11.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.101.11 netmask 255.255.255.0 broadcast 192.168.101.255
    inet6 fe80::fa4a:6384:9b55:75eb prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:47:82:1d txqueuelen 1000 (Ethernet)
    RX packets 10 bytes 1358 (1.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 83 bytes 11862 (11.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

→ Kiểm tra kết nối

```
[husky@localhost ~]$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.21.0 0.0.0.0 255.255.255.0 U 101 0 0 ens33
192.168.101.0 0.0.0.0 255.255.255.0 U 100 0 0 ens37
192.168.122.0 0.0.0.0 255.255.255.0 U 0 0 0 virbr0
```

- Victim

→ Các thông số mạng

```
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-81-19-6C
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::29e1:842d:c013:2f8f%12(Preferred)
IPv4 Address. . . . . : 192.168.101.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.101.11
DHCPv6 IAID . . . . . : 251661353
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-79-18-37-00-0C-29-81-19-6C

DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       : fec0:0:0:ffff::2%1
                       : fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
```

→ Kiểm tra kết nối

```
C:\Users\corgi>ping 192.168.101.11

Pinging 192.168.101.11 with 32 bytes of data:
Reply from 192.168.101.11: bytes=32 time<1ms TTL=64
Reply from 192.168.101.11: bytes=32 time<1ms TTL=64
Reply from 192.168.101.11: bytes=32 time<1ms TTL=64
Reply from 192.168.101.11: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.101.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\corgi>_
```

4.2. Cài đặt Snort trên CentOS

Đảm bảo máy IDS/IPS kết nối được Internet

- Cập nhật hệ điều hành

```
dnf update -y
```

```
Installed:
  crun-0.18-2.module_el8.4.0+830+8027elc4.x86_64      kernel-4.18.0-305.7.1.el8_4.x86_64
  kernel-core-4.18.0-305.7.1.el8_4.x86_64            kernel-modules-4.18.0-305.7.1.el8_4.x86_64
```

```
dnf install -y epel-release
```

```
Installed:
  epel-release-8-11.el8.noarch
```

- Cài đặt các thư viện cần thiết

```
dnf install -y gcc flex bison zlib* libxml2 libpcap* pcre* tcpdump git
libtool curl daq libdnet
```

```
dnf --enablerepo=powertools install libdnet-devel
```

```
dnf groupinstall -y "Development Tools"
```

- Cài đặt các gói: libpcap-1.6.4, libdnet-1.12, daq-2.0.4

- Cập nhật các đường dẫn thư viện:

```
echo >>/etc/ld.so.conf /usr/lib
```

```
echo >> /etc/ld.so.conf /usr/local/lib && ldconfig
```

- Kiểm tra truy cập libdnet

```
ln -s /usr/lib64/libdnet.so.1.0.1 /lib64/libdnet.1
```

- Cài đặt Snort từ snort.org

```
dnf install https://www.snort.org/downloads/snort/snort-2.9.18-
1.centos8.x86_64.rpm
```

```
Installed:
  compat-openssl10-1:1.0.2o-3.el8.x86_64      libnsl-2.28-151.el8.x86_64      make-1:4.2.1-10.el8.x86_64
  snort-1:2.9.18-1.x86_64
```

4.3. Cấu hình Snort NIDS mode

- Tạo các thư mục cấu trúc cho việc lưu cấu hình Snort

```
mkdir -p /etc/snort/rules
```

```
mkdir /var/log/snort
```

```
mkdir /usr/local/lib/snort_dynamicrules
```

- Cấp quyền cho các thư mục cấu trúc

```
chmod -R 5775 /etc/snort
```

```
chmod -R 5775 /var/log/snort
```

```
chmod -R 5775 /usr/local/lib/snort_dynamicrules
```

```
chown -R snort:snort /etc/snort
```

```
chown -R snort:snort /var/log/snort
```

```
chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

- Tạo các tập tin cần thiết cho Snort

```
touch /etc/snort/rules/white_list.rules
```

```
touch /etc/snort/rules/black_list.rules
```

```
touch /etc/snort/rules/local.rules
```

```
touch /var/log/snort/snort.log
```

```
sed -i 's/include \${RULE_PATH}/#include \${RULE_PATH}/'  
/etc/snort/snort.conf
```

- Chỉnh sửa tập tin snort.conf

```
vi /etc/snort/snort.conf
```

```
44 # Setup the network addresses you are protecting  
45 ipvar HOME_NET 192.168.101.0/24  
46  
47 # Set up the external network addresses. Leave as "any" in most  
   situations  
48 ipvar EXTERNAL_NET !$HOME_NET  
49
```

```
104 var RULE_PATH /etc/snort/rules
105 var SO_RULE_PATH /etc/snort/so_rules
106 var PREPROC_RULE_PATH /etc/snort/preproc_rules
107
108 # If you are using reputation preprocessor set these
109 # Currently there is a bug with relative paths, they are relativ
   e to where snort is
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG
   89986
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH /etc/snort/rules
114 var BLACK_LIST_PATH /etc/snort/rules
```

```
520 # Recommended for most installs
521 output unified2: filename snort.log, limit 128
522 # output unified2: filename merged.log, limit 128, nostamp, mpls
   _event_types, vlan_event_types
```

```
546 include $RULE_PATH/local.rules
547 include $RULE_PATH/snort.rules
```

```
264 # Does nothing in IDS mode
265 preprocessor normalize_ip4
266 preprocessor normalize_tcp: ips ecn stream
267 preprocessor normalize_icmp4
268 preprocessor normalize_ip6
269 preprocessor normalize_icmp6
270
```

- Kiểm tra tập tin cấu hình snort

```
snort -T -c /etc/snort/snort.conf
```

```
Total snort Fixed Memory Cost - MaxRss:45820
Snort successfully validated the configuration!
Snort exiting
```


4.4. Cấu hình Snort Inline mode

Cập nhật vi /etc/snort/snort.conf

```
186 # config logdir:
187
188 config policy_mode:inline
189 #####
190 # Step #3: Configure the base detection engine. For more inform
    ation, see README.decode
191 #####
```

```
159 config daq:afpacket
160 config daq_dir: /usr/local/lib/daq
161 config daq_mode:inline
162 config daq_var: buffer_size_mb=1024
```

4.5. Phát cảnh báo và ngăn chặn tấn công Ping of Death

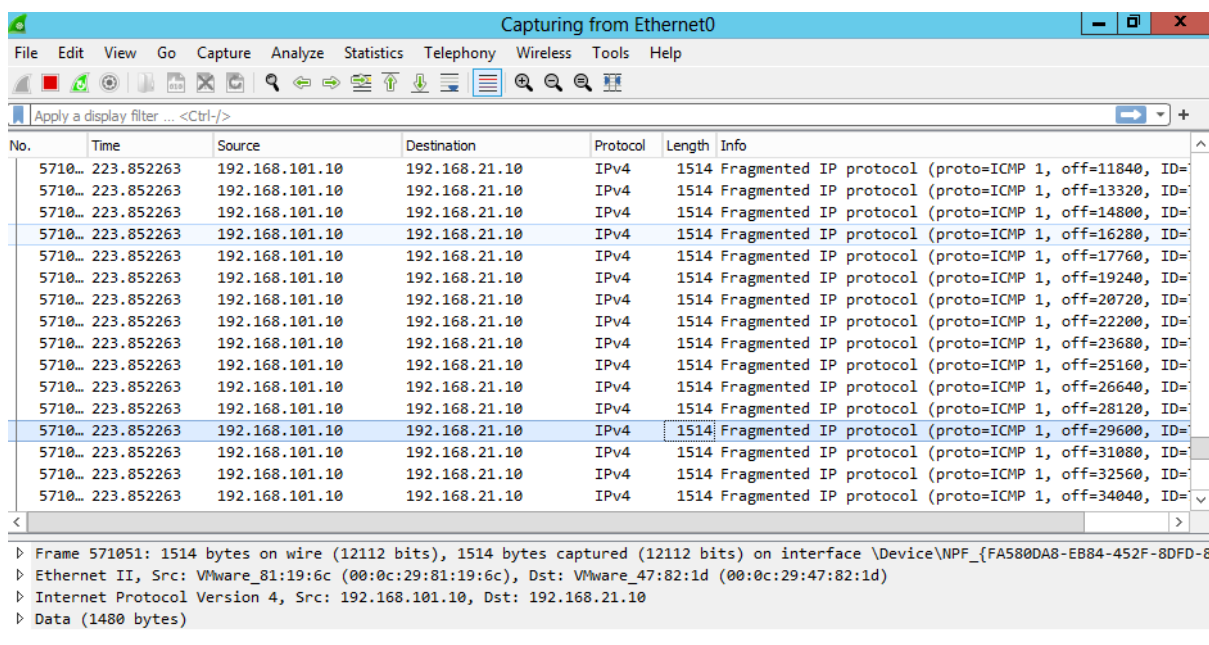
- Attack tấn công Victim

- Attack sử dụng Ping of Death thông qua lệnh:

ping <ip address> -s 65500 -t 1 -n 1

(Có thể sử dụng công cụ hping3 để tiến hành tấn công Ping of Death đến Victim)

- Lưu lượng ICMP trên Wireshark của máy Victim



No.	Time	Source	Destination	Protocol	Length	Info
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=11840, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=13320, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=14800, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=16280, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=17760, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=19240, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=20720, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=22200, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=23680, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=25160, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=26640, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=28120, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=29600, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=31080, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=32560, ID=)
5710...	223.852263	192.168.101.10	192.168.21.10	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=34040, ID=)

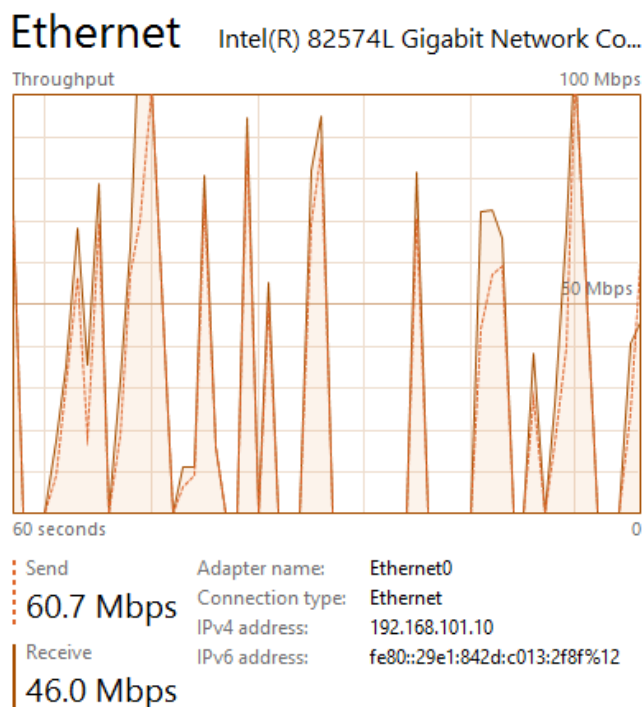
> Frame 571051: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{FA580DA8-E884-452F-8DFD-8...}

> Ethernet II, Src: VMware_81:19:6c (00:0c:29:81:19:6c), Dst: VMware_47:82:1d (00:0c:29:47:82:1d)

> Internet Protocol Version 4, Src: 192.168.101.10, Dst: 192.168.21.10

> Data (1480 bytes)

- Quan sát Throughput trong Task Manager của máy Victim tăng đột biến



- Viết rule phát cảnh báo khi gặp tấn công Ping of Death

- Truy cập tập tin local.rules:
vi /etc/snort/rules/local.rules
- Thêm nội dung rule vào tập tin:
alert icmp any any -> \$HOME_NET any (msg:"--> **Ping of death** attack!"; dsiz>10000; gid:1000001; sid:1000001; rev:1;)
- Chạy console giám sát của Snort
snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
- Console giám sát trên Snort phát cảnh báo khi bị tấn công **Ping of death**

```
[root@localhost husky]# snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33
07/10-01:48:08.111549 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.112828 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.114039 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.115422 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.116809 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.118011 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.119243 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.120714 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.122054 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.123270 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.124507 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.125946 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-01:48:08.127273 [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
```

- Khảo sát tập tin log

```
tcpdump -r /var/log/snort/snort.log.xxxx
```

- Cập nhật thêm rule ngăn chặn tấn công **Ping of death**

- Cập nhật rule:

```
drop icmp any any -> $HOME_NET any (msg:"--> chan Ping of death attack!"; dsize:>10000; gid:1000002; sid:1000002; rev:1;)
```

- Chạy console giám sát của Snort

```
snort -i ens33:ens37 -A console -c /etc/snort/snort.conf -l /var/log/snort/ -Q
```

```
07/10-02:33:40.507190 [Drop] [**] [1000002:1000002:1] --> chan Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
07/10-02:33:40.507273 [Drop] [**] [1000001:1000001:1] --> Ping of death attack! [**] [Priority: 0] {ICMP} 192.168.21.10 -> 192.168.101.10
```

Hoàn thành nội dung trên được 4đ. Sinh viên có thể thực hiện dựng Snort trên pfSense (để thay thế cho môi trường CentOS) và tiến hành thực hiện tương tự, tuy nhiên chỉ được tính 3đ

Bài tập

1. Tìm hiểu, cài đặt và khảo sát các package hỗ trợ Snort: (1đ)

- a) Barnyard2: Phần mềm sao chép output của Snort và ghi vào csdl SQL
- b) PulledPork: Tự động tải các Snort rule miễn phí mới nhất
- c) BASE: một giao diện đồ họa nền web cho việc xem các Snort event

2. Tiến hành dựng các kịch bản dựa trên mô hình có sẵn sao cho phù hợp các rule sau: (2đ)

- a) alert icmp any any -> \$HOME_NET 81 (msg:"Scanning Port 81";sid:1000005;rev:1;)
- b) alert tcp any any -> any 22 (msg:"ssh connection=>Attempt";sid:1000004;)
- c) alert icmp any any -> any any (msg:"UDP Tesing Rule";sid:1000006;rev:1;)

