

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 03

**TRIỂN KHAI HỆ THỐNG PHÁT HIỆN XÂM
NHẬP SNORT**

Người xây dựng bài thực hành:

Th.S Cao Minh Tuấn

HÀ NỘI, 2018

MỤC LỤC

Mục lục	2
Thông tin chung về bài thực hành	3
Chuẩn bị bài thực hành	4
Đối với giảng viên	4
Đối với sinh viên	4
THIẾT LẬP VÀ CẤU HÌNH TƯỜNG LỬA IPTABLES	5
1.1. Mô tả.....	5
1.2. Chuẩn bị	5
1.3. Mô hình cài đặt.....	5
1.4. Cài đặt phần mềm phát hiện xâm nhập Snort	6
1.5. Các kịch bản thực hiện tấn công và phát hiện.....	10
1.5.1. Kịch bản 1. Phát hiện tấn công dò quét.....	10
1.5.2. Kịch bản 2. Phát hiện tấn công dò quét dịch vụ và cổng	12
1.5.3. Kịch bản 3. Phát hiện tấn công từ chối dịch vụ ICMP Ping of Death .	14

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Triển khai hệ thống phát hiện xâm nhập Snort.

Học phần: An toàn mạng máy tính

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

Máy tính vật lý có cấu hình tối thiểu: RAM 4GB, 50 HDD

- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

Công cụ được cung cấp cùng tài liệu này:

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

TRIỂN KHAI HỆ THỐNG PHÁT HIỆN XÂM NHẬP SNORT

1.1. Mô tả

Để đảm bảo an toàn cho mạng máy tính nhằm phát hiện các cuộc tấn công vào mạng nội bộ, cần triển khai hệ thống phát hiện xâm nhập. Hệ thống phát hiện xâm nhập có thể là thiết bị chuyên dụng hoặc dưới dạng phần mềm. Trong mô hình mạng thử nghiệm nghiên cứu và học tập thì phần mềm miễn phí Snort là phù hợp.

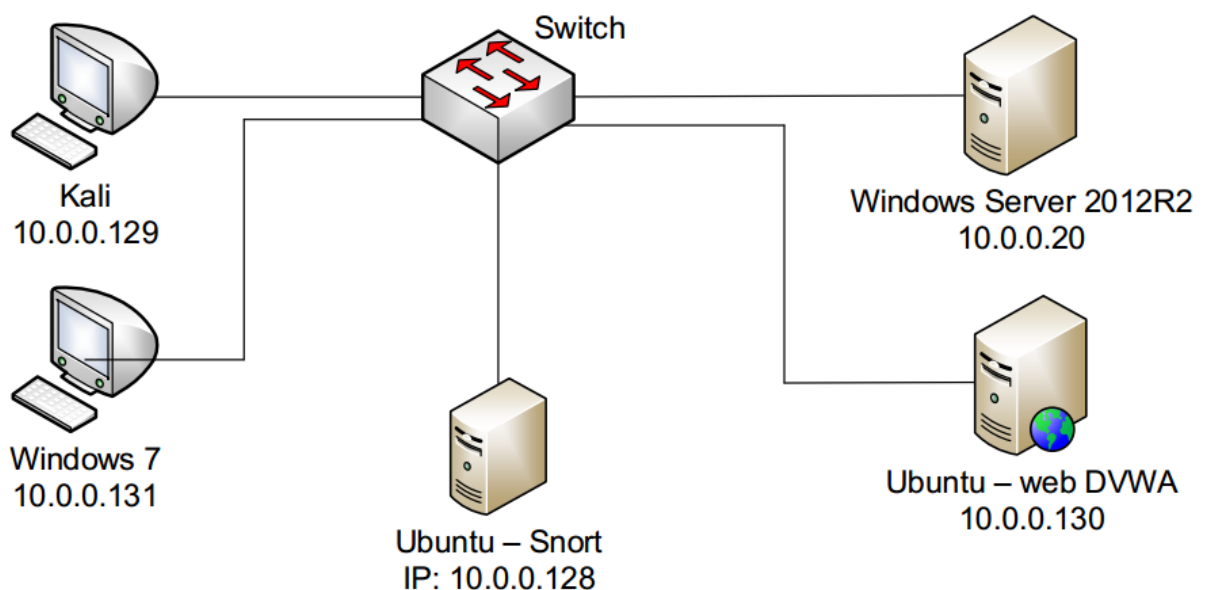
Yêu cầu của bài thực hành:

- Cài đặt phần mềm Snort
- Cấu hình các tham số cho Snort
- Sử dụng Snort để phát hiện một số dạng tấn công phổ biến

1.2. Chuẩn bị

- 01 máy ảo chạy Ubuntu 14.04
- 01 máy ảo hệ điều hành Windows 7
- 01 máy ảo hệ điều hành Windows Server 2012.
- 01 máy ảo hệ điều hành Linux chạy website DVWA.
- 01 máy ảo hệ điều hành Kali linux.

1.3. Mô hình cài đặt



1.4. Cài đặt phần mềm phát hiện xâm nhập Snort

Cấu hình giao diện mạng của máy ảo Ubuntu sao cho máy có thể kết nối được Internet (*chuyển card mạng sang chế độ NAT hoặc Bridged*).

Bước 1. Cài đặt các gói phần mềm hỗ trợ

Snort có bốn phần mềm hỗ trợ yêu cầu phải cài đặt trước:

- pcap (libpcap-dev)
- PCRE (libpcre3-dev)
- Libdnet (libdumbnet-dev)
- DAQ

Khởi động máy ảo Ubuntu, mở cửa sổ dòng lệnh bắt đầu cài đặt.

```
[attd@snort:~$]sudo apt-get install -y build-essential
[attd@snort:~$]sudo apt-get install -y libpcap-dev libpcre3-dev
libdumbnet-dev
[attd@snort:~$]sudo apt-get install -y bison flex
```

Tạo thư mục chứa mã nguồn Snort và các phần mềm liên quan:

```
[attd@snort:~$]mkdir ~/snort_src
[attd@snort:~$]cd ~/snort_src
[attd@snort:~$]sudo wget
https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
[attd@snort:~$]sudo tar -xvzf daq-2.0.6.tar.gz
[attd@snort:~$]cd daq-2.0.6
[attd@snort:~$]sudo ./configure
[attd@snort:~$]sudo make
[attd@snort:~$]sudo make install
[attd@snort:~$]sudo apt-get install -y zlib1g-dev liblzma-dev
openssl libssl-dev
```

Bước 2. Cài đặt Snort

```
[attd@snort:~$]cd ~/snort_src
[attd@snort:~$]wget https://snort.org/downloads/snort/snort-
2.9.12.tar.gz
```

Chú ý: Tại thời điểm 06/01/2019 là phiên bản 2.9.12, cần kiểm tra phiên bản trước khi chạy lệnh.

```
[attd@snort:~/snort_src$]sudo tar -zxf snort-2.9.12.tar.gz
```

```
[attt@snort:~/snort_src]$ cd snort-2.9.12/
[attt@snort:~/snort_src/snort-2.9.12]$ sudo ./configure --enable-
sourcefire --disable-open-appid
[attt@snort:~/snort_src/snort-2.9.12]$ sudo make
[attt@snort:~/snort_src/snort-2.9.12]$ sudo make install
[attt@snort:~/snort_src/snort-2.9.12]$ sudo ldconfig
[attt@snort:~/snort_src/snort-2.9.12]$ sudo ln -s
/usr/local/bin/snort /usr/sbin/snort
```

Chạy thử để kiểm tra Snort:

```
attt@snort:~$ snort -V

''_      -*> Snort! <*-
o" )~    Version 2.9.12 GRE (Build 325)
' ' '    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
        Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
        Copyright (C) 1998-2013 Sourcefire, Inc., et al.
        Using libpcap version 1.5.3
        Using PCRE version: 8.31 2012-07-06
        Using ZLIB version: 1.2.8
```

Snort đã được cài thành công.

Bước 3. Cấu hình Snort chạy ở chế độ phát hiện xâm nhập mạng

Tạo các thư mục cho Snort:

```
[attt@snort:~$] sudo mkdir /etc/snort
[attt@snort:~$] sudo mkdir /etc/snort/rules
[attt@snort:~$] sudo mkdir /etc/snort/rules/iplists
[attt@snort:~$] sudo mkdir /etc/snort/preproc_rules
[attt@snort:~$] sudo mkdir
/usr/local/lib/snort_dynamicrules
[attt@snort:~$] sudo mkdir /etc/snort/so_rules
```

Tạo các tệp tin chứa tập luật cơ bản cho Snort

```
[attt@snort:~$] sudo touch
/etc/snort/rules/iplists/black_list.rules
[attt@snort:~$] sudo touch
/etc/snort/rules/iplists/white_list.rules
[attt@snort:~$] sudo touch /etc/snort/rules/local.rules
[attt@snort:~$] sudo touch /etc/snort/sid-msg.map
```

Tạo thư mục chứa log:

```
[attt@snort:~$] sudo mkdir /var/log/snort
```

```
[attd@snort:~$]sudo mkdir /var/log/snort/archived_logs
```

#Tạo các bản sao tệp tin cấu hình của Snort

The configuration files are:

- classification.config
- file magic.conf
- reference.config
- snort.conf
- threshold.conf
- attribute table.dtd
- gen-msg.map
- unicode.map

```
[attd@snort:~$]cd snort_src/snort-2.9.12/etc
```

```
[attd@snort:~/snort_src/snort-2.9.12/etc$]sudo cp *.conf*  
/etc/snort
```

```
[attd@snort:~/snort_src/snort-2.9.12/etc$]sudo cp *.map  
/etc/snort
```

```
[attd@snort:~/snort_src/snort-2.9.12/etc$]sudo cp *.dtd  
/etc/snort
```

```
[attd@snort:~]cd ~/snort_src/snort-2.9.12/src/dynamic-  
preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/  
sudo cp * /usr/local/lib/snort_dynamicpreprocessor/
```

Bây giờ chúng ta có các thư mục và tệp tin của Snort theo các đường dẫn sau:

Tập thực thi của Snort: /usr/local/bin/snort

Tệp tin cấu hình: /etc/snort/snort.conf

Thư mục chứa log: /var/log/snort

Thư mục chứa tập luật: /etc/snort/rules

/etc/snort/so rules

/etc/snort/preproc rules

/usr/local/lib/snort dynamicrules

Thư mục chứa IP: /etc/snort/rules/iplists

Thư mục tiền xử lý động: /usr/local/lib/snort dynamicpreprocessor/

Tiếp theo cần sử dụng trình soạn thảo văn bản: nano hoặc vi để chỉnh sửa các tham số trong tệp tin: /etc/snort/snort.conf

```
[attt@snort:~]sudo nano /etc/snort/snort.conf
```

Tìm đến dòng 45, chỉnh sửa địa chỉ IP cho mạng nội bộ.

```
ipvar HOME_NET 10.0.0.0/24
ipvar EXTERNAL_NET !$HOME_NET (dòng 48)
```

Tìm đến các dòng sau chỉnh sửa đường dẫn chứa tập luật.

```
var RULE_PATH /etc/snort/rules (dòng 104)
var SO_RULE_PATH /etc/snort/so_rules (dòng 105)
var PREPROC_RULE_PATH /etc/snort/preproc_rules (dòng 106)
var WHITE_LIST_PATH /etc/snort/iplists (dòng 113)
var BLACK_LIST_PATH /etc/snort/iplists (dòng 114)
```

Đường dẫn tập luật:

```
include $RULE_PATH/local.rules (dòng 546)
```

Tệp tin này chứa tập luật sử dụng để kiểm tra sự hoạt động của Snort, cần bỏ dấu # trước dòng này.

Các dòng từ 548 đến 651 chứa tập luật cho mỗi loại hình tấn công, trong quá trình kiểm tra cần đóng lại bằng cách đặt dấu # trước mỗi dòng.

Kết thúc quá trình cấu hình, lưu và thoát khỏi trình chỉnh sửa.

Bước 4. Kiểm tra sự hoạt động của Snort

Tại cửa sổ dòng lệnh chạy lệnh sau:

```
[attt@snort:~$] sudo snort -i eth0 -c /etc/snort/snort.conf -T
```

Kết quả như sau:

```

''-_*> Snort! <*-
o" )~ Version 2.9.12 GRE (Build 325)
    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.
    Using libpcap version 1.5.3
    Using PCRE version: 8.31 2012-07-06
    Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>

Snort successfully validated the configuration!
Snort exiting

```

Kết quả cài đặt và cấu hình Snort thành công.

1.5. Các kịch bản thực hiện tấn công và phát hiện

1.5.1. Kịch bản 1. Phát hiện tấn công dò quét

Bước 1. Sử dụng phần mềm Nmap dò quét các máy tính đang chạy

```

root@kali:~# nmap -sP 10.0.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-07 03:05 EST
Nmap scan report for 10.0.0.1
Host is up (0.0012s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 10.0.0.20
Host is up (0.0035s latency).
MAC Address: 00:0C:29:C2:85:69 (VMware)
Nmap scan report for 10.0.0.128
Host is up (0.00076s latency).
MAC Address: 00:0C:29:11:00:17 (VMware)
Nmap scan report for 10.0.0.130
Host is up (0.00057s latency).
MAC Address: 00:0C:29:E7:37:91 (VMware)
Nmap scan report for 10.0.0.254
Host is up (0.00019s latency).
MAC Address: 00:50:56:F9:76:5E (VMware)
Nmap scan report for 10.0.0.129
Host is up.

```

Nmap done: 256 IP addresses (6 hosts up) scanned in 28.29 seconds

Khi sử dụng phương pháp dò quét này, Nmap sẽ gửi các gói tin ARP tới địa chỉ broadcast để tìm địa chỉ IP các máy đang bật, sau đó nó gửi lại các gói ICMP để kiểm tra lại tình trạng hoạt động.

Do Snort chưa hỗ trợ phát hiện giao thức ARP nên chúng ta chỉ có thể phát hiện dò quét thông qua giao thức ICMP.

Bước 2. Phát hiện tấn công

Mã nguồn của luật phát hiện dò quét ICMP của Snort như sau:

```
alert icmp any any -> any any (msg:"Nmap ICMP scanning";
sid:10000001; rev:1;)
```

Chạy chương trình Snort ở chế độ lắng nghe và phát hiện:

```
[attt@snort:~$] sudo snort -i eth0 -c /etc/snort/snort.conf
```

Trong quá trình Snort chặn bắt gói tin và so sánh với tập luật, những sự kiện nào trùng khớp sẽ được lưu trong tệp tin theo đường dẫn: /var/log/snort/alert

Chúng ta có thể xem trực tiếp theo thời gian thực sử dụng lệnh:

```
[attt@snort:~$] tail -f /var/log/snort/alert
```

Bước 3. Kết quả

Giao diện hiển thị của lệnh **tail**:

```
[**] [1:10000001:1] Nmap ICMP scanning [**]
[Priority: 0]
01/06-22:52:44.949373 10.0.0.129 -> 10.0.0.255
ICMP TTL:43 TOS:0x0 ID:64780 IpLen:20 DgmLen:40
Type:13 Code:0 ID: 3608 Seq: 0 TIMESTAMP REQUEST

[**] [1:10000001:1] Nmap ICMP scanning [**]
[Priority: 0]
01/06-22:52:47.911250 10.0.0.129 -> 10.0.0.130
ICMP TTL:52 TOS:0x0 ID:20786 IpLen:20 DgmLen:28
Type:8 Code:0 ID:40419 Seq:0 ECHO

[**] [1:10000001:1] Nmap ICMP scanning [**]
[Priority: 0]
01/06-22:52:47.911696 10.0.0.130 -> 10.0.0.129
```

ICMP TTL:64 TOS:0x0 ID:57709 IpLen:20 DgmLen:28
Type:0 Code:0 ID:40419 Seq:0 ECHO REPLY

Đây là cảnh báo của Snort phát hiện tấn công dò quét. Ta thấy có rất nhiều tin ICMP xuất phát từ

Giao diện thống kê của Snort:

=====

Run time for packet processing was 84.182421 seconds

Snort processed 3670 packets.

Snort ran for 0 days 0 hours 1 minutes 24 seconds

Pkts/min: 3670

Pkts/sec: 43

=====

Memory usage summary:

Total non-mmapped bytes (arena): 6070272

Bytes in mapped regions (hblkhd): 30130176

Total allocated space (uordblks): 3466560

Total free space (fordblks): 2603712

Topmost releasable block (keepcost): 524656

=====

Packet I/O Totals:

Received: 3673

Analyzed: 3671 (99.946%)

Dropped: 0 (0.000%)

Filtered: 0 (0.000%)

Outstanding: 2 (0.054%)

Injected: 0

=====

Action Stats:

Alerts: 32 (0.871%)

Logged: 32 (0.871%)

Passed: 0 (0.000%)

1.5.2. Kịch bản 2. Phát hiện tấn công dò quét dịch vụ và cổng

Bước 1. Thực hiện tấn công

Tại bước này, sử dụng Nmap tại máy Kali để dò quét các dịch, cổng đang mở và hệ điều hành đang chạy đối với mỗi địa chỉ IP đã thu được ở kịch bản 1.

Tấn công dò quét tới máy chủ Windows Server 2012.

```
root@kali:~# nmap -sS -O 10.0.0.20
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-09 02:47 EST
Nmap scan report for 10.0.0.20
Host is up (0.00063s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1000/tcp  open  cadlock
MAC Address: 00:0C:29:C2:85:69 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2012|8.1
OS CPE: cpe:/o:microsoft:windows_7::ultimate
cpe:/o:microsoft:windows_2012 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7, Windows Server 2012, or Windows
8.1 Update 1
Network Distance: 1 hop
```

Bước 2. Thiết lập luật phát hiện tấn công dò quét cho Snort

Với hình thức tấn công trên Nmap gửi rất nhiều gói tin với cờ SYN với máy chủ Windows Server 2012 và Ubuntu web.

Sử dụng trình soạn thảo nano hoặc vi chỉnh sửa tệp tin local.rules và thêm vào luật phát hiện như sau:

```
alert tcp any any -> $HOME_NET any (msg:"SYN scan attack";
detection_filter:track by_src, count 100, seconds 2; flags:S;
classtype:network-scan; sid:10000002; rev:1;)
```

Với luật trên Snort sẽ theo dõi các gói tin với cờ SYN cùng xuất phát từ một nguồn gửi, đếm 100 gói trong 2 giây thì sẽ cảnh báo.

Tại máy Snort sử dụng lệnh khởi tạo chương trình:

```
[attd@snort:~$] sudo snort -i eth0 -c /etc/snort/snort.conf
```

Bước 3. Kết quả phát hiện tấn công

Sử dụng lệnh tail như kịch bản 1 xem trực tiếp sự kiện phát hiện tại máy

Snort:

```
[**] [1:10000002:1] SYN scan attack [**]
[Classification: Detection of a Network Scan] [Priority: 3]
01/08-21:31:42.249952 10.0.0.129:50348 -> 10.0.0.20:1
TCP TTL:41 TOS:0x0 ID:10102 IpLen:20 DgmLen:60
*****S* Seq: 0xDC5D47FB Ack: 0xDB55837C Win: 0x7A69 TcpLen:
40
TCP Options (5) => WS: 10 NOP MSS: 265 TS: 4294967295 0 SackOK
[**] [1:10000002:1] SYN scan attack [**]
[Classification: Detection of a Network Scan] [Priority: 3]
01/08-21:31:42.042865 10.0.0.129:50336 -> 10.0.0.20:53
TCP TTL:56 TOS:0x0 ID:53142 IpLen:20 DgmLen:56
*****S* Seq: 0xDC5D4800 Ack: 0xDB55837C Win: 0x200 TcpLen:
36
TCP Options (3) => MSS: 265 SackOK TS: 4294967295 0
```

Với hiển thị này ta biết được một máy nào đó có địa chỉ IP 10.0.0.129 đang gửi gói SYN tới 10.0.0.20 với cổng đích là 53. Ngoài ra giao diện còn hiển thị rất nhiều gói tin với các cổng khác. Do vậy sử dụng Snort ta phát hiện được đang có cuộc tấn công dò quét.

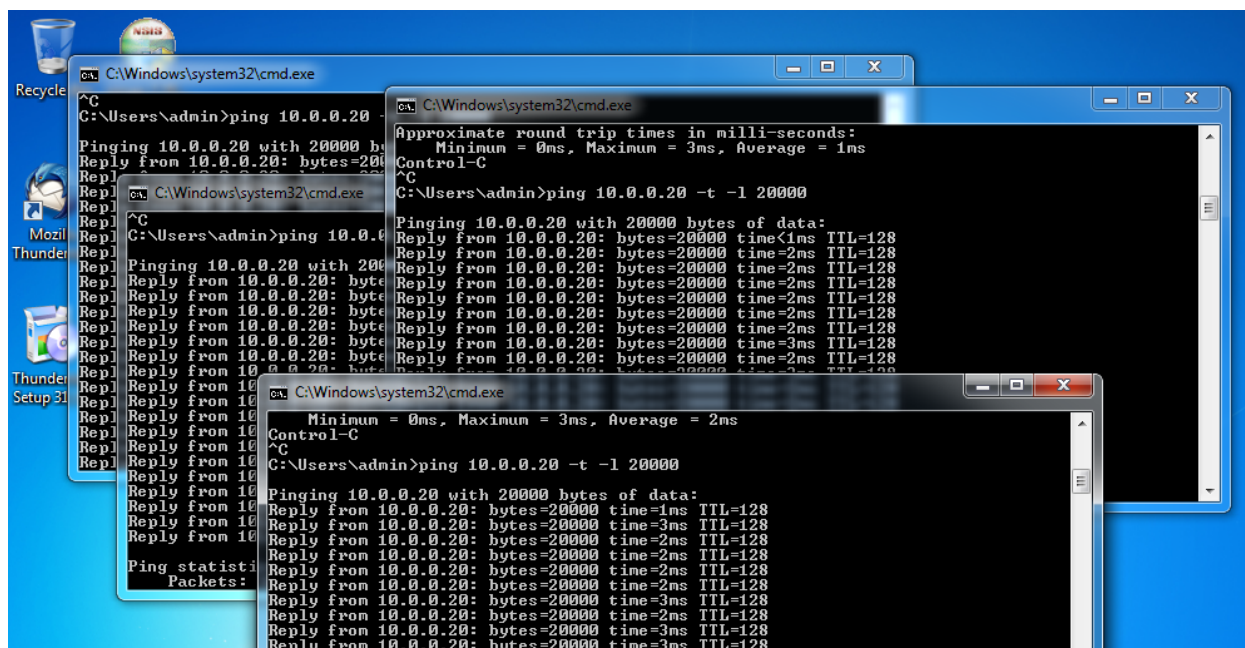
1.5.3. Kịch bản 3. Phát hiện tấn công từ chối dịch vụ ICMP Ping of Death

Bước 1. Tấn công

Tại máy tính Windows 7, sử dụng chương trình dòng lệnh CMD để ping với số lượng lớn các gói tin ICMP có kích thước lớn tới máy chủ Windows Server.

Sử dụng lệnh:

```
C:\Users\admin>ping 10.0.0.20 -t -l 20000
```



Chú ý: Đây là cách tấn công thử nghiệm để kiểm tra luật phát hiện của Snort, gây ảnh hưởng rất ít tới máy chủ.

Bước 2. Thiết lập tập luật phát hiện cho Snort

Sử dụng trình soạn thảo văn bản nano hoặc vi thêm vào luật phát hiện cho Snort trong tệp tin: `/etc/snort/rules/local.rules`

```
alert icmp any any -> $HOME_NET any (msg:"ICMP Ping of Death";
itype:8; dsize:>1000; detection_filter:track by_src, count 1000,
seconds 10; classtype:denial-of-service; sid:10000003; rev:1;)
```

Với luật này Snort sẽ lắng nghe và theo dõi những gói tin với giao thức ICMP echo request có kích thước lớn hơn 1000, xuất phát từ một nguồn và trong 10 giây có 1000 gói tin gửi đến thì Snort sẽ đưa ra cảnh báo.

Tại máy Snort sử dụng lệnh khởi tạo chương trình lắng nghe:

```
[attt@snort:~$] sudo snort -i eth0 -c /etc/snort/snort.conf
```

Bước 3. Phát hiện tấn công

Tại máy Snort sử dụng cửa sổ dòng lệnh và chạy lệnh tail như trên:

Kết quả:

```
[**] [1:10000003:2] ICMP Ping of Death [**]
[Classification: Detection of a Denial of Service Attack]
[Priority: 2]
01/09-00:58:51.713816 10.0.0.131 -> 10.0.0.20
ICMP TTL:128 TOS:0x0 ID:317 IpLen:20 DgmLen:20028
Type:8 Code:0 ID:1 Seq:232 ECHO
```

```
[**] [1:10000003:2] ICMP Ping of Death [**]  
[Classification: Detection of a Denial of Service Attack]  
[Priority: 2]  
01/09-00:58:52.540265 10.0.0.131 -> 10.0.0.20  
ICMP TTL:128 TOS:0x0 ID:318 IpLen:20 DgmLen:20028  
Type:8 Code:0 ID:1 Seq:233 ECHO
```

```
[**] [1:10000003:2] ICMP Ping of Death [**]  
[Classification: Detection of a Denial of Service Attack]  
[Priority: 2]  
01/09-00:58:52.712217 10.0.0.131 -> 10.0.0.20  
ICMP TTL:128 TOS:0x0 ID:319 IpLen:20 DgmLen:20028  
Type:8 Code:0 ID:1 Seq:234 ECHO
```

Với cảnh báo này người quản trị biết được rằng đang có cuộc tấn công dạng từ chối dịch vụ sử dụng giao thức ICMP có nguồn xuất phát từ máy có địa chỉ IP 10.0.0.131 tới máy đích 10.0.0.20.

(Sinh viên cần thiết lập nhiều luật thêm cho Snort để phát hiện các kiểu tấn công khác.)

Kết luận:

Với bài thực hành này đã hướng dẫn cài đặt phần mềm phát hiện xâm nhập Snort, cấu hình và chạy các tập luật để phát hiện một số dạng tấn công cơ bản lên tài nguyên mạng.

Kết thúc bài thực hành./.