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

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.

THIẾT LẬP VÀ CẤU HÌNH TƯỜNG LỬA IPTABLES

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

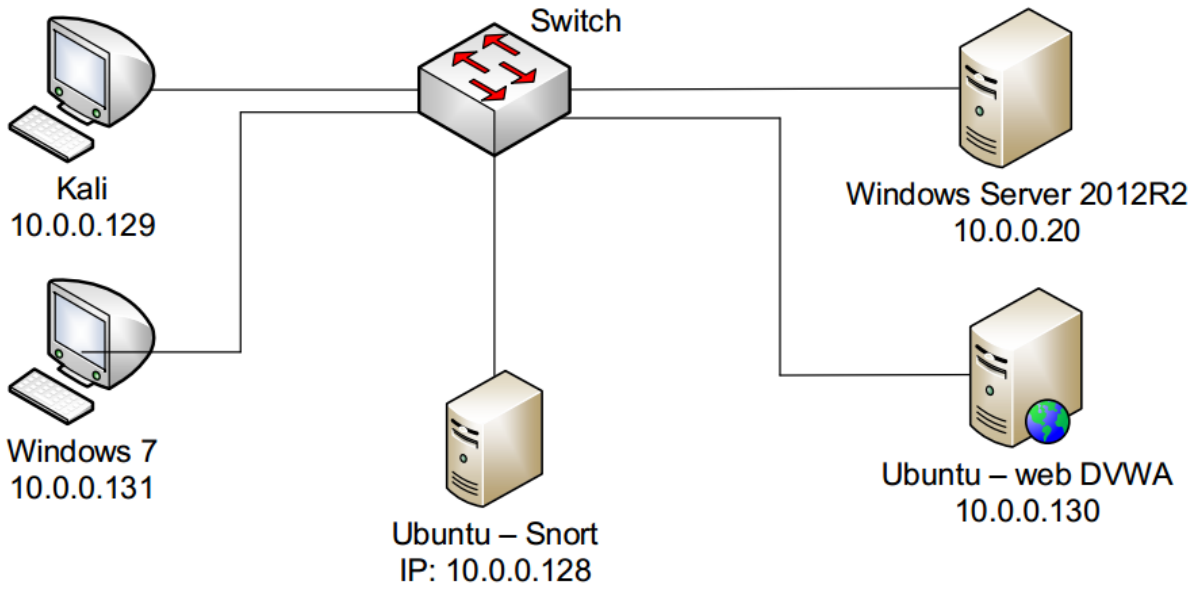
– 01 máy ảo hệ điều hành Windows 7

– 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 bổ trợ

Snort có bốn phần mềm bổ 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.

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

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

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

Bước 2. Cài đặt Snort

```
[attt@snort:~$]cd ~/snort_src
[attt@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.

```
[attt@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
```

```
[attt@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

```
[attt@snort:~$]cd snort_src/snort-2.9.12/etc
[attt@snort:~/snort_src/snort-2.9.12/etc$]sudo cp *.conf*
/etc/snort
[attt@snort:~/snort_src/snort-2.9.12/etc$]sudo cp *.map
/etc/snort
[attt@snort:~/snort_src/snort-2.9.12/etc$]sudo cp *.dtd
/etc/snort
[attt@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:

Tệp 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 của 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 scaning";
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 scaning [**]
[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 scaning [**]
[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 scaning [**]
[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 ICPM 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

Yêu cầu:

- Sử dụng phần mềm Nmap trên Kali tấn công dò quét dịch vụ và cổng tương ứng tới máy chủ Windows Server 2012 và Ubuntu web
- Thiết lập luật cho Snort để phát hiện tấn công dò quét dịch vụ và cổng
- Sử dụng các tính năng hiển thị và thống kê như trong kịch bản 1 để xem kết quả.

1.5.3. Kịch bản 3. Phát hiện tấn công từ chối dịch vụ

Yêu cầu:

- Tại máy tính Windows 7 sử dụng cửa sổ dòng lệnh CMD, Ping nhiều gói tin ICMP với kích thước lớn (2000byte) tới máy chủ Window Server 2012.
- Thiết lập luật cho Snort phát hiện tấn công này.
- Tại máy tính Kali sử dụng script Slowloris.pl tấn công từ chối dịch vụ vào máy chủ web Apache.
- Thiết lập luật cho Snort để phát hiện tấn công này.