* + 1. Mô hình



Hình - Mô hình cài đặt thực nghiệm

* + 1. Cài đặt mô hình
       1. Thực hiện Update Repository

|  |
| --- |
| # rpm -Uhv https://excellmedia.dl.sourceforge.net/project/snortsnortsam/rpmforge-release-0.5.2-2.el6.rf.i686.rpm |

* + - 1. Cài đặt DAQ

Cài đặt các gói cần thiết trước khi cài DAQ:

|  |
| --- |
| # yum -y install libdnet libdnet-devel libpcap libpcap-devel daq gcc make flex bison pcre pcredevel zlib zlib-devel  # yum install -y mysql-server mysql-devel php-mysql php-adodb php-pear php-gd httpd wget |

Tải và cài đặt gói DAQ:

|  |
| --- |
| # cd /tmp  # wget https://excellmedia.dl.sourceforge.net/project/snortsnortsam/daq-1.1.1.tar.gz  # tar -xzvf daq-1.1.1.tar.gz  # cd daq-1.1.1/  # ./configure  # make&& make install  # ldconfig -v |

* + - 1. Cài đặt Snort

Tạo user snort và các thư mục cần thiết:

|  |
| --- |
| # groupadd snort  # useradd -g snort snort  # mkdir /usr/local/snort  # mkdir /etc/snort  # mkdir /var/log/snort  # mkdir /var/run/snort  # chown snort:snort /var/log/snort  # chown snort:snort /var/run/snort  # mkdir -p /usr/local/lib/snort\_dynamicrules  # chown -R snort:snort /usr/local/lib/snort\_dynamicrules  # chmod -R 700 /usr/local/lib/snort\_dynamicrules |

Tải về và cài đặt Snort:

|  |
| --- |
| # cd /tmp ;  # wget https://excellmedia.dl.sourceforge.net/project/snortsnortsam/snort-2.8.4.1.tar.gz  # tar -xzvf snort-2.8.4.1.tar.gz  # cd snort-2.8.4.1/  #./configure --with-mysql --enable-dynamicplugin  # make&& make install  # cp /tmp/snort-2.8.4.1/etc/snort.conf /etc/snort/  # cp /tmp/snort-2.8.4.1/etc/unicode.map /etc/snort/  # cp /tmp/snort-2.8.4.1/etc/classification.config /etc/snort/  # cp /tmp/snort-2.8.4.1/etc/threshold.conf /etc/snort |

Download các rules cho Snort:

|  |
| --- |
| # cd /tmp  # wget https://svwh.dl.sourceforge.net/project/snortsnortsam/snortrules-snapshot-2.8.tar.gz  # tar -zxvf snortrules-snapshot-2.8.tar.gz  # cd snortrules-snapshot-2.8  # cp -R rules /etc/snort/  # chown -R snort:snort /etc/snort/ |

Sửa file cấu hình Snort:

|  |
| --- |
| # vi /etc/snort/snort.conf |

Cấu hình như sau:

|  |
| --- |
| var HOME\_NET 10.0.0.16/28 # dòng 46  var RULE\_PATH /etc/snort/rules # dòng 110 |

Lưu file lại và kiểm tra cấu hình đã thành công hay chưa bằng lệnh:

|  |
| --- |
| # sudo snort -T -i eth1 -c /etc/snort/snort.conf |

Nếu thành công:

|  |
| --- |
| user@snortserver:~$ sudo snort -T -i eth1 -c /etc/snort/snort.conf  (...)  Snort successfully validated the configuration!  Snort exiting |

Cấu hình init script cho Snort:

Tạo một liên kết mềm (symbolic link) của file snort binary đến /usr/sbin/snort:

|  |
| --- |
| # ln -s /usr/local/bin/snort /usr/sbin/snort |

Snort cung cấp các scrip để khởi động trong thư mục rpm/ ; (thư mục giải nén snort):

|  |
| --- |
| # cp /tmp/snort-2.8.4.1/rpm/snortd /etc/init.d/  # cp /tmp/snort-2.8.4.1/rpm/snort.sysconfig /etc/sysconfig/snort  # cp /tmp/snort-2.8.4.1/etc/reference.config /etc/snort/ |

Cấu hình Snort khởi động cùng hệ thống:

|  |
| --- |
| # chmod +x /etc/init.d/snortd  # chkconfig snortd on  # service snortd start |

Khởi động snort ở chế độ debug nếu bạn muốn kiểm tra lỗi:

|  |
| --- |
| # snort -u snort -g snort -c /etc/snort/snort.conf -i eth1 |

* + - 1. Cài đặt Barnyard2

Barnyard2 là một ứng dụng được sử dụng để lưu việc xuất log và cảnh báo cho snort. Do đó, snort dành tài nguyên cho chức năng chính của nó.

Log và các cảnh báo của snort sẽ được lưu vào một hệ quản trị cơ sở dữ liệu. Trong khuôn khổ bài thực nghiệm này, chúng ta sử dụng PostgreSQL.

Cấu hình Snort để xuất các sự kiện dưới dạng nhị phân vào trong một thư mục, sau đó Barnyard2 đọc các sự kiện đó một cách không đồng bộ và chèn chúng vào cơ sở dữ liệu PostgreSQL.

Để kiểm tra khả năng phát hiện của Snort, chúng ta hãy tạo ra một quy tắc đơn giản để Snort tạo ra một cảnh báo bất cứ khi nào nó thấy một gói tin ICMP "Echo request" hoặc "Echo reply". Dán dòng sau vào file: */etc/snort/rules/local.rules*

|  |
| --- |
| alert icmp any any -> $HOME\_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;) |

Cài đặt các gói phụ thuộc:

|  |
| --- |
| # pear channel-update pear.php.net  # pear install Numbers\_Roman  # pear install channel://pear.php.net/Image\_Canvas-0.3.5  # pear install channel://pear.php.net/Image\_Graph-0.8.0 |

Cấu hình MySQL:

|  |
| --- |
| # mysqladmin -u root password 123456  # mysql -u root -p  mysql> create database snort;  Query OK, 1 row affected (0.00 sec)  mysql> grant select,insert,update,delete,create on snort.\* to snort@localhost;  Query OK, 0 rows affected (0.06 sec)  mysql> set password for snort@localhost=PASSWORD('123456');  Query OK, 0 rows affected (0.00 sec)  mysql>exit |

Chúng ta cần nói với snort rằng nó phải đưa các cảnh báo trong một định dạng nhị phân (vào một tập tin) mà Barnyard2 có thể xử lý. Để làm điều đó, ta chỉnh sửa tệp tin /etc/snort/snort.conf và thêm vào cuối file dòng sau:

|  |
| --- |
| #vi /etc/snort/snort.conf  # Thêm vào cuối file:  output unified2: filename snort.u2, limit 128 |

*Cài đặt Barnyard2:*

|  |
| --- |
| # cd /tmp ;  # wget https://excellmedia.dl.sourceforge.net/project/snortsnortsam/barnyard2-1.9.tar.gz  # tar -xzvf barnyard2-1.9.tar.gz  # cd barnyard2-1.9  # ./configure --with-mysql (nếu Cetnos 32bit)  #./configure -with-mysql-libraries=/usr/lib64/mysql/(nếu Cetnos 64bit)  # make&& make install  # cp etc/barnyard2.conf /etc/snort/  # mysql -u snort -p123456 snort < schemas/create\_mysql  # touch /etc/snort/barnyard2.waldo  # chmod 777 /etc/snort/barnyard2.waldo  # chown snort:snort /etc/snort/barnyard2.waldo |

Kiểm tra xem Barnyard2 đã được cài đặt thành công hay chưa:

|  |
| --- |
| [root@localhost ~]# /usr/local/bin/barnyard2 -V  \_\_\_\_\_\_ -\*> Barnyard2 <\*-  / ,,\_ \ Version 2.1.9 (Build 263)  |o" )~| By the SecurixLive.com Team: http://www.securixlive.com/about.php  + '''' + (C) Copyright 2008-2010 SecurixLive.  Snort by Martin Roesch & The Snort Team: http://www.snort.org/team.html  (C) Copyright 1998-2007 Sourcefire Inc., et al. |

Chỉnh sửa file cấu hình barnyard2:

|  |
| --- |
| # mkdir /var/log/barnyard2  # chown snort:snort /var/log/barnyard2/  # vi /etc/snort/barnyard2.conf  29: config reference\_file: /etc/snort/reference.config  30: config classification\_file: /etc/snort/classification.config  31: config gen\_file: /etc/snort/etc/gen-msg.map  32: config sid\_file: /etc/snort/etc/sid-msg.map  44: config logdir: /var/log/barnyard2  60: config hostname: localhost  61: config interface: eth2  65: config alert\_with\_interface\_name  164: input unified2  318: output database: alert, mysql, user=snort password=123456 dbname=snort host=localhost |

Chỉnh sửa file init script cho barnyard2:

|  |
| --- |
| # vi /etc/init.d/snortd  # Thêm vào cuối file nội dung sau:  BARNYARD2=/usr/local/bin/barnyard2  start()  {  [ -x $SNORTD ] || exit 5  echo -n $"Starting $prog: "  daemon --pidfile=$PID\_FILE $SNORTD $LINK\_LAYER $NO\_PACKET\_LOG  $DUMP\_APP -D $PRINT\_INTERFACE $INTERFACE -u $USER -g $GROUP $CONF -l  $LOGDIR $PASS\_FIRST $BPFFILE $BPF && success || failure  RETVAL=$?  $BARNYARD2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -w  /etc/snort/barnyard2.waldo -u snort -g snort -D  [ $RETVAL -eq 0 ] && touch $lockfile  echo  return $RETVAL  }  stop()  {  echo -n $"Stopping $prog: "  killproc $SNORTD  killproc $BARNYARD2  if [ -e $PID\_FILE ]; then  chown -R $USER:$GROUP /var/run/snort\_eth0.\* && rm -f /var/run/snort\_eth0.pi\*  fi  RETVAL=$?  if [ "x$runlevel" = x0 -o "x$runlevel" = x6 ] ; then  trap TERM  killall $prog 2>/dev/null  trap TERM  fi  [ $RETVAL -eq 0 ] && rm -f $lockfile  echo  return $RETVAL  } |

Khởi động lại Snort:

|  |
| --- |
| # /etc/init.d/snortd restart |

Vì mật khẩu được lưu trữ trong dạng text trong tệp barnyard2.conf nên chúng ta nên ngăn người dùng khác đọc nó:

|  |
| --- |
| # sudo chmod o-r /etc/snort/barnyard2.conf |

Chạy Snort ở chế độ cảnh báo (eth1 là interface của máy thực nghiệm):

|  |
| --- |
| # sudo /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth1 |

Ping đến interface eth1 từ máy tính khác, chúng ta sẽ không thấy bất kỳ cảnh báo nào trên màn hình vì câu lệnh trên không có option *-A console*. Gõ Ctrl-C để dừng Snort. Một tập tin mới trong thư mục /var/log/snort được tạo ra với tên: snort.u2.nnnnnnnnnn (các con số sẽ khác nhau vì chúng dựa trên thời gian hiện tại).

|  |
| --- |
| [root@localhost ~]# ls -l /var/log/snort/  total 12  drwsrwxr-t 2 snort snort 4096 Nov 7 14:48 archived\_logs  -rw-r--r-- 1 snort snort 0 Nov 7 19:53 barnyard2.waldo  -rw------- 1 snort snort 708 Nov 7 14:53 snort.log.1446904397  -rw------- 1 snort snort 1552 Nov 7 19:56 snort.u2.1446922585 |

Bây giờ chúng ta chạy Barnyard2, xử lý các sự kiện trong snort.u2.nnnnnnnnnnn và nạp chúng vào cơ sở dữ liệu Snort. Sử dụng các cờ sau với Barnyard2:

|  |
| --- |
| -c /etc/snort/barnyard2.conf The path to the barnyard2.conf file  -d /var/log/snort The folder to look for Snort output files  -f snort.u2 The Filename to look for in the above directory (snort.u2.nnnnnnnnnn)  -w /var/log/snort/barnyard2.waldo The location of the waldo file (bookmark file)  -u snort Run Barnyard2 as the following user after startup  -g snort Run Barnyard2 as the following group after startup |

Chạy Barnyard2:

|  |
| --- |
| # sudo barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort -f snort.u2 -w /var/log/snort/barnyard2.waldo |

Kết quả:

|  |
| --- |
| (...)  Opened spool file '/var/log/snort/snort.u2.1389532785'  Closing spool file '/var/log/snort/snort.u2.1389532785'. Read 8 records  Opened spool file '/var/log/snort/snort.u2.1389535513'  12/06−12:14:28.908206 [∗∗] [1:10000001:1] ICMP test detected [∗∗] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 20.0.0.96 −> 10.0.0.19  12/06−12:14:28.908241 [∗∗] [1:10000001:1] ICMP test detected [∗∗] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.19 −> 20.0.0.96  12/06−12:14:29.905893 [∗∗] [1:10000001:1] ICMP test detected [∗∗] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 20.0.0.96 −> 10.0.0.19  12/06−12:14:29.905927 [∗∗] [1:10000001:1] ICMP test detected [∗∗] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 10.0.0.19 −> 20.0.0.96  Waiting for new data  ˆC∗∗∗ Caught Int−Signal |

Ctrl-C để dừng Barnyard2, sau đó kiểm tra trong MySQL:

|  |
| --- |
| # mysql -root -p  mysql> use snort;  mysql> select \* from event;  sid | cid | signature | timestamp  -----+-----+-----------+----------------------------  1 | 1 | 511 | 2017-10-10 01:40:40.891-07  1 | 2 | 511 | 2017-10-10 01:40:40.895-07  1 | 3 | 511 | 2017-10-10 01:40:41.894-07  1 | 4 | 511 | 2017-10-10 01:40:41.895-07  1 | 5 | 511 | 2017-10-10 01:40:42.895-07  1 | 29 | 511 | 2017-10-10 01:41:44.925-07  (29 rows) |

Cài đặt Barnyard2 thành công.

* + - 1. Cài đặt BASE - Web GUI for Snort

Tải về base:

|  |
| --- |
| # cd /tmp ;  # wget https://svwh.dl.sourceforge.net/project/snortsnortsam/base-1.4.5.tar.gz  # tar -xzvf base-1.4.5.tar.gz  # cp -r base-1.4.5/ /var/www/base  # cd /var/www/base/  # cp base\_conf.php.dist base\_conf.php |

Chỉnh sửa file cấu hình base\_conf:

|  |
| --- |
| # vi base\_conf.php  50: $BASE\_urlpath = '/base';  80: $DBlib\_path = ''/var/www/adodb';  102: $alert\_dbname = 'snort';  103: $alert\_host = 'localhost';  104: $alert\_port = '3306';  105: $alert\_user = 'snort';  106: $alert\_password = 123456''; |

Cấu hình Apache:

|  |
| --- |
| # vi /etc/httpd/conf.d/base.conf  # Thêm vào các dòng sau:  Alias /base /var/www/base/  <directory "/var/www/base/">  AllowOverride None  Order allow,deny  Allow from all  AuthName "Snort IDS"  AuthType Basic  AuthUserFile /etc/snort/base.passwd  Require valid-user  </directory> |

Tạo password truy cập vào web Base:

|  |
| --- |
| # htpasswd -c /etc/snort/base.passwd snortadmin |

Tạo file log barnyard2:

|  |
| --- |
| # mkdir /var/log/barnyard2/  # chown -R snort:snort /var/log/barnyard2/ |

Download adodb và thực hiện gán quyền truy cập:

|  |
| --- |
| # cd /tmp  # wget https://svwh.dl.sourceforge.net/project/snortsnortsam/adodb519.tar.gz  # tar -zxvf adodb519.tar.gz  # mv adodb5 /var/www/adodb  # chown -R snort:snort /var/www/adodb  # chmod -R 775 /var/www/adodb |

Khởi động lại Apache, MySQL:

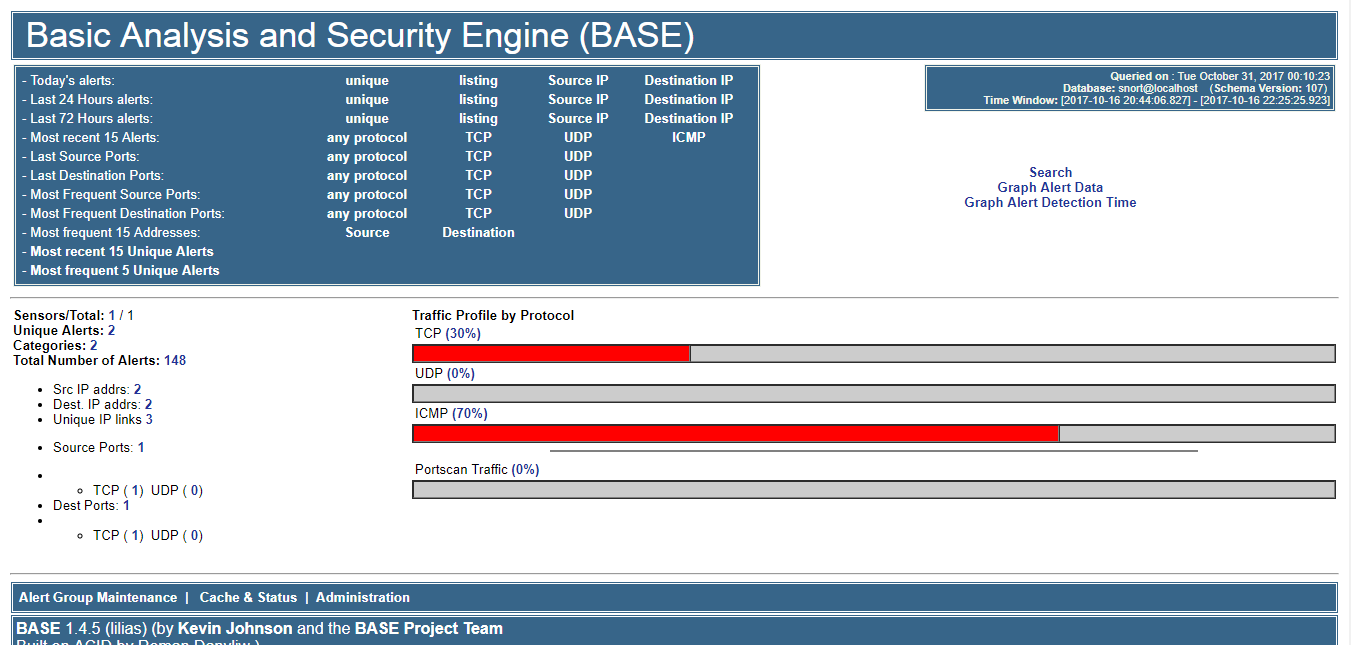
|  |
| --- |
| # service httpd restart  # service mysqld restart |

Chạy snort và barnyard:

|  |
| --- |
| # snort -u snort -g snort -c /etc/snort/snort.conf -i eth1  # barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort/ -f snort.u2 |

Đăng nhập vào web *https://10.0.0.19/base/base\_db\_setup.php*

User đăng nhập snortadmin password 123456. Click create BASE AG.



Hình - Giao diện BASE sau khi cài đặt thành công