Build IPS Virtual Appliance

Based on

Vmware ESXi, Snort and Debian Linux

Step-by-step Tutorial

Vladimir Koychev

2015

Contents

I. Setup overview 3

II. Configuring the ESXi Host 3

III. Configuring the Virtual Machine 3

IV. Debian Installation and dependencies 4

V. Snort Installation 5

VI. PulledPork Installation 6

VII. Barnyard installation 7

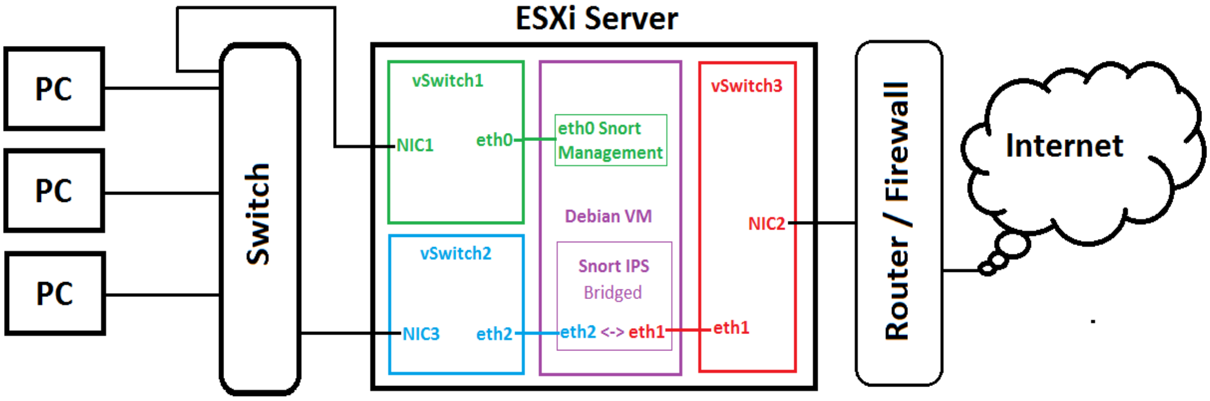
VIII. Using Snort 8

IX. Installing BASE 8

X. References 9

I. Setup overview

The tutorial aims to give general instructions on how to setup Intrusion Prevention System using VMware ESXi , Snort in IPS mode and Debian Linux. The main goal of such a setup is adding protection over a local network by passing all external traffic to IPS component for inspection. The setup sketch below:



II. Configuring the ESXi Host

1. ESXi requirements;
    - Protecting virtual network placed on the same host requires two physical NIC adapters, one for the management of Snort and another one for the egress traffic;
    - Protecting physical network requires three physical NIC adapters for Snort management, ingress and egress traffic;
2. EXSi configuration;
    a) Connect NIC1 and NIC3 to local network switch;
    b) Connect NIC2 to the router;
    c) Create three virtual switches each pointing to physical adapter (NIC);
        - vSwitch1 to NIC1 - Management network;
        - vSwitch2 to NIC2 – egress traffic;
        - vSwitch3 to NIC3 – ingress traffic
    d) Make sure vSwitch2 and vSwitch3 are in promiscuous mode;

III. Configuring the Virtual Machine

1. Create new virtual machine;
    - 1 virtual socket with 2 cores;
    - 4GB RAM;
    - 30GB HDD;
    - Three network adaptors;
2. Configure Network adaptors;
    - Assign Network adaptor 1 to vSwitch1;
    - Assign Network adaptor 2 to vSwitch2;
    - Assign Network adaptor 3 to vSwitch3;
3. Start the VM;

IV. Debian Installation and dependencies

1. Install Debian on the VM (For the current tutorial Debian-7-7-0-netinstall was used);
2. Install the following dependencies:
   - apt-get -y install ssh
   - apt-get -y install vim
   - apt-get -y install apache2
   - apt-get -y install apache2-doc
   - apt-get -y install libapache2-mod-php5
   - apt-get -y install autoconf
   - apt-get -y install automake
   - apt-get -y install bison
   - apt-get -y install ca-certificates
   - apt-get -y install ethtool
   - apt-get -y install flex
   - apt-get -y install g++
   - apt-get -y install gcc
   - apt-get -y install gcc-4.4
   - apt-get -y install libcrypt-ssleay-perl
   - apt-get -y install libmysqlclient-dev
   - apt-get -y install libnet1
   - apt-get -y install libnet1-dev
   - apt-get -y install libpcre3
   - apt-get -y install libpcre3-dev
   - apt-get -y install libphp-adodb
   - apt-get -y install libssl-dev
   - apt-get -y install libtool
   - apt-get -y install libwww-perl
   - apt-get -y install make
   - apt-get -y install mysql-client
   - apt-get -y install mysql-common
   - apt-get -y install mysql-server
   - apt-get -y install ntp
   - apt-get -y install php5-cli
   - apt-get -y install php5-gd
   - apt-get -y install php5-mysql
   - apt-get -y install php-pear
   - apt-get -y install sendmail-bin
   - apt-get -y install sendmail
   - apt-get -y install sysstat
   - apt-get -y install usbmount
   - apt-get -y libcrypt-ssleay-perl
   - apt-get -y liblwp-protocol-https-perl
3. Disable ”Large Receive Offload” and ”Generic Receive Offload” on eth3:
   - vim /etc/rc.local
   - Add before - exit0:

ethtool --offload eth3 rx off tx off
ethtool -K eth3 gso off
ethtool -K eth3 gro off

4. Install libpcap
   - cd /usr/src
   - wget http://www.tcpdump.org/release/libpcap-1.6.4.tar.gz
   - tar -zxf libpcap-1.6.4.tar.gz
   - cd libpcap-1.6.4
   - ./configure --prefix=/usr && make && make install
5. Install libdnet
   - cd /usr/src
   - wget http://libdnet.googlecode.com/files/libdnet-1.12.tgz
   - tar -zxf libdnet-1.12.tgz
   - cd libdnet-1.12
   - ./configure --prefix=/usr --enable-shared && make && make install
6. Install daq
   - cd /usr/src
   - wget https://www.snort.org/downloads/snort/daq-2.0.4.tar.gz
   - tar -zxf daq-2.0.4.tar.gz
   - cd daq-2.0.4
   - ./configure && make && make install
7. Update the shared library path
   - echo >> /etc/ld.so.conf /usr/lib
   - echo >> /etc/ld.so.conf /usr/local/lib && ldconfig

V. Snort Installation

1. Install Snort
   - cd /usr/src
   - wget https://www.snort.org/downloads/snort/snort-2.9.7.0.tar.gz
   - tar -zxf snort-2.9.7.0.tar.gz && cd snort-2.9.7.0
   - ./configure --enable-sourcefire && make && make install
2. Create Snort directories:
   - mkdir /usr/local/etc/snort
   - mkdir /usr/local/etc/snort/rules
   - mkdir /var/log/snort
   - mkdir /usr/local/lib/snort_dynamicrules
3. Create empty rules files:
   - touch /usr/local/etc/snort/rules/white_list.rules
   - touch /usr/local/etc/snort/rules/black_list.rules
   - touch /usr/local/etc/snort/rules/local.rules
   - touch /usr/local/etc/snort/rules/snort.rules
   - touch /usr/local/etc/snort/sid-msg.map
4. Create snort user and grant privileges:
   - groupadd snort && useradd -g snort snort
   - chown snort:snort /var/log/snort
5. Copy snort configuration files:

- cp /usr/src/snort-2.9.7.0/etc/*.conf* /usr/local/etc/snort
- cp /usr/src/snort-2.9.7.0/etc/*.map /usr/local/etc/snort

6. Configure Snort (edit snort.conf)
   - vim /usr/local/etc/snort/snort.conf
   - Line #45 - **ipvar HOME_NET 172.26.12.0/22** – make this match your internal network;
   - Line #48 - **ipvar EXTERNAL_NET !$HOME_NET**
   - Line #104 - **var RULE_PATH rules**
   - Line #109 - **var WHITE_LIST_PATH rules**
   - Line #110 - **var BLACK_LIST_PATH rules**
   - Line #293 - add this to the end after "decompress_depth 65535" **max_gzip_mem 104857600**
   - Line #521 - add this line - **output unified2: filename snort.log, limit 128**
   - Line #543 - delete or comment out all of the "include $RULE_PATH" lines except:
     - ➢ **include $RULE_PATH/local.rules**
     - ➢ **include $RULE_PATH/snort.rules** – add after local.rules
7. Make sure at line #265 the following rules are uncommented:
   - preprocessor normalize_ip4
   - preprocessor normalize_tcp: ips ecn stream
   - preprocessor normalize_icmp4
   - preprocessor normalize_ip6
   - preprocessor normalize_icmp6
8. On line #188 at the end of step #2 of snort.cong add:
   - config policy_mode:inline
9. Configure daq at line #159 in snort.cong
   - config daq: afpacket
   - config daq_dir: /usr/local/lib/daq
   - config daq_mode: inline
   - config daq_var: buffer_size_mb=1024
10. Save changes to snort.conf

VI. PulledPork Installation

Default Snort installation doesn't contain any rules/signatures. Snort rules can be created by the user (see https://www.snort.org/ for more information), downloaded manually or automatically using PulledPork. The following instructions describe the installation and configuration of PulledPork.

1. Install PulledPork:
   - cd /usr/src
   - wget https://pulledpork.googlecode.com/files/pulledpork-0.7.0.tar.gz
   - tar xzf pulledpork-0.7.0.tar.gz && cd pulledpork-0.7.0
   - cp pulledpork.pl /usr/local/bin/ && chmod +x /usr/local/bin/pulledpork.pl
   - cd etc && cp * /usr/local/etc/snort/
2. Snort can use community rules (freely available) and the "registered" rules. In order to use "registered " rules, it is necessary to be obtained "Oinkcode" via registration at: https://www.snort.org/
3. Configure PulledPork (edit /usr/local/etc/snort/pulledpork.cong):

- vim / usr/local/etc/snort/pulledpork.cong
- If “Oinkcode” available add it on line #19 and #26 e.g. rule_url=https://www.snort.org/reg-rules/|snortrules-snapshot-2970.tar.gz|1234123412313232132321321313113131312321 or comment out for community rules only;
- Leave line #27 uncommented to use the Emerging Threats rules;
- Line #71: change to: **rule_path=/usr/local/etc/snort/rules/snort.rules**
- Line #86: change to: **local_rules =/usr/local/etc/snort/rules/local.rules**
- Line #89: change to: **sid_msg=/usr/local/etc/snort/sid-msg.map**
- Line #112: change to: **config_path=/usr/local/etc/snort/snort.conf**
- Line #124: change to: **distro=Debian-7-7**
- Line #139: change to: **black_list=/usr/local/etc/snort/rules/black_list.rules**
- Line #200: make sure the following paths are available and uncommented:
    - ➢ enablesid=/usr/local/etc/snort/enablesid.conf
    - ➢ dropsid=/usr/local/etc/snort/dropsid.conf
    - ➢ disablesid=/usr/local/etc/snort/disablesid.conf
    - ➢ modifysid=/usr/local/etc/snort/modifysid.conf
- Save changes to pulledpork.conf

4. IMPORTANT: Default configuration only alerts upon rule/signature match, no matter if Snort configured in “Inline” mode. Therefore the action upon match should be changed from “alert” to “DROP”;
    - vim /usr/local/etc/snort/dropsid.conf (For more information: https://www.snort.org)
    - Make sure all lines are commented;
    - vim /usr/local/etc/snort/ modifysid.conf
    - Add to the end of the file: *** "^\s*alert" "DROP"**
    - Reboot the VM;
5. Run PulledPork
    - **/usr/local/bin/pulledpork.pl -c /usr/local/etc/snort/pulledpork.conf -T -l**
6. Create cronjob
    - *** */1 * * * /usr/local/bin/pulledpork.pl -c /usr/local/etc/snort/pulledpork.conf -T -l >/dev/null 2>&1**

VII. Barnyard installation

“Barnyard2 is an open source interpreter for Snort unified2 binary output files. Its primary use is allowing Snort to write to disk in an efficient manner and leaving the task of parsing binary data into various formats to a separate process that will not cause Snort to miss network traffic.” - https://github.com/firnsy/barnyard2

1. Install Barnyard2;
    - cd /usr/src
    - wget https://github.com/binf/barnyard2/tree/bug-fix-release
    - unzip bug-fix-release.zip
    - cd barnyard2-bug-fix-release
    - autoreconf -fvi -I ./m4 && ./configure --with-mysql --with-mysql-libraries=/usr/lib/x86_64-linux-gnu
    - make && make install
2. Configure Barnyard2
    - cd /etc && cp barnyard2.conf /usr/local/etc/snort
    - mkdir /var/log/barnyard2

- chown snort:snort /var/log/barnyard2
- vim usr/local/etc/snort/ barnyard2.conf
- Line #27 change to: **/usr/local/etc/snort/reference.config**
- Line #28 change to: **/usr/local/etc/snort/classification.config**
- Line #29 change to: **/usr/local/etc/snort/gen-msg.map**
- Line #30 change to: **/usr/local/etc/snort/sid-msg.map**
- Line #227 change to: **output alert_fast**
- At the end of the file: **output database: log, mysql, user=snort password=<mypassword> dbname=snort host=localhost**

3. Setup Database
   - Login to MySQL: mysql -u root –p
   - mysql> **create database snort;**
   - mysql> **grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;**
   - mysql> **SET PASSWORD FOR snort@localhost=PASSWORD('mypassword');** set user password for snort database user;
   - mysql> **use snort;**
   - mysql> source /usr/src/barnyard2-bug-fix-release/schemas/create_mysql
   - mysql> **show tables;** - the list of new tables should be displayed;
   - mysql> **exit;**

VIII. Using Snort

1. Snort in inline mode no database logging (console alerts):
   - snort -d -A console -u snort -g snort -c /usr/local/etc/snort/snort.conf -i eth1:eth2 -Q
2. Snort in inline mode no database logging (Logged alerts):
   - snort -d -A full -u snort -g snort -c /usr/local/etc/snort/snort.conf -i eth1:eth2 -Q
3. Snort in inline mode and database logging (console alerts):
   - snort -d -A console -u snort -g snort -c /usr/local/etc/snort/snort.conf -i eth1:eth2 -Q & /usr/local/bin/barnyard2 -c /usr/local/etc/snort/barnyard2.conf -d /var/log/snort -f snort.log -w /usr/local/etc/snort/bylog.waldo -C /usr/local/etc/snort/classification.config
4. Snort in inline mode and database logging (Logged alerts):
   - snort -d -A full -u snort -g snort -c /usr/local/etc/snort/snort.conf -i eth1:eth2 -Q & /usr/local/bin/barnyard2 -c /usr/local/etc/snort/barnyard2.conf -d /var/log/snort -f snort.log -w /usr/local/etc/snort/bylog.waldo -C /usr/local/etc/snort/classification.config
5. Snort in inline mode no database logging no snort status (console alerts):
   - snort -q -d -A console -u snort -g snort -c /usr/local/etc/snort/snort.conf -i eth1:eth2 -Q

IX. Installing BASE

"BASE is the Basic Analysis and Security Engine. It is based on the code from the Analysis Console for Intrusion Databases (ACID) project. This application provides a web front-end to query and analyze the alerts coming from a SNORT IDS system." - http://sourceforge.net/projects/secureideas/

1. Configure Apache & PHP
   - cp /etc/apache2/sites-available/default-ssl /etc/apache2/sites-enabled
   - vim /etc/php5/apache2/php.ini
   - Line #452: change to: error_reporting = E_ALL & ~E_NOTICE
   - a2enmod ssl

- pear config-set preferred_state alpha
- pear channel-update pear.php.net
- pear install --alldeps Image_Color2 Image_Canvas Image_Graph
- /etc/init.d/apache2 restart

2. Install BASE
   - cd /usr/src
   - wget http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz
   - tar xzf base-1.4.5.tar.gz
   - cp -r base-1.4.5 /var/www/base
   - chmod 777 -R /var/www/base
3. Configure Base
   - Open the Browser console: **https://<host ip address>/base**
   - Click **Continue**, choose **English**
   - Path to adodb: /usr/share/php/adodb
   - Click **Continue**
   - Database Name: **snort**
   - Database Host: **localhost**
   - Database Port: **leave blank**
   - Database User Name: **snort**
   - Database Password: **pass for snort database user**
   - Put in values for the authentication and click submit.
   - Click "create baseag" which extends the DB to support BASE.
   - Continue to “step 5” to login.
4. Configure privileges
   - rm /var/www/index.html
   - chmod 755 /var/www/base

X. References

1. ^ https://www.snort.org/
2. ^ Jason Weir, Snort 2.9.6.x on Debian 7.6, https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/049/original/Debian_Snort_based_Intrusion_Detection_System.pdf?AWSAccessKeyId=AKIAIXACIED2SPMSC7GA&Expires=1426706767&Signature=EBDoAqabQuhmyzrOI2EqkPXjccc%3D
3. ^ Yaser Mansour, Snort IPS using DAQ AFPacket, https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/013/original/Snort_IPS_using_DAQ_AFPacket.pdf?AWSAccessKeyId=AKIAIXACIED2SPMSC7GA&Expires=1426706931&Signature=J5vvL1BXS1lJYBngaNeu%2F70Ssvo%3D
4. ^ http://sourceforge.net/projects/secureideas/
5. ^ https://github.com/firnsy/barnyard2