**Practical 7**

**Objectives: To try out Intrusion Detection Systems**

**Part 1 : Network-Based Intrusion Detection Systems (NIDS)**

**Exercise Installing a Network Intrusion Detection System - Snort**

Description:

Snort is an open source Intrusion Detection System that's available for both Linux and Windows systems. We will be installing Snort on the web-server2 virtual machine.

In Kali VM:

1. As the web-server2 does not have a GUI, we will use Kali to download the Snort installation files first. Download the Snort installation zip file from Brightspace or from the download link under Topic 7 IDS.

You can also download the latest version of Snort from www.snort.org.

1. Start the SSH service on Kali.

sudo /etc/init.d/ssh start

In web-server2 VM:

1. Login as root. (or from Kali, you can SSH to web-server2 as user student00, and then do a su - to switch to user root)
2. Do a SCP to secure copy the Snort installation zip file from Kali to web-server2. For example, to copy the Snort installation zip file from Kali’s /home/kali directory to the web-server2’s current directory, then the command would be:

The full-stop represents the current directory

scp kali@*Kali-IP*:/home/kali/snort-centos7.zip .

1. Extract the Snort installation zip file.

unzip snort-centos7.zip

1. Run the following commands to install Snort and its dependencies and libraries.

rpm –ihv libdnet-1.12-13.1.el7.x86\_64.rpm

rpm –ihv daq- 2.0.6-1.el7.x86\_64.rpm

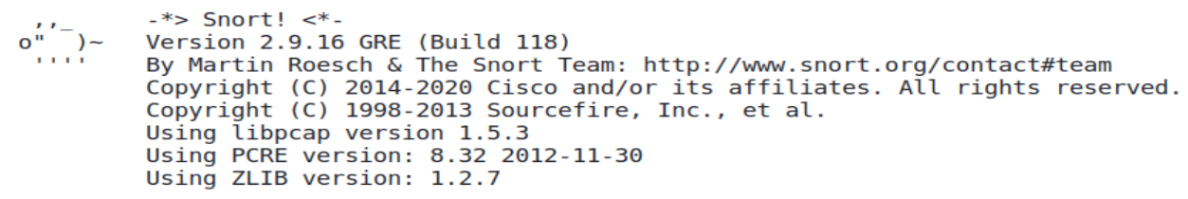
rpm –ihv snort- 2.9.16-1.centos7.x86\_64.rpm

1. Create a symbolic link to the libdnet library.

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

1. Run Snort with the capital V option to display its version number.

snort -V



**Exercise Configuring Snort**

Some common Snort options :

-i *<interface>* listen to that particular network interface device.

-v verbose mode.

-d dumping the application layer.

In web-server2 VM:

1. Run Snort to display the available options.

snort -h

1. Open the Snort config file /etc/snort/snort.conf with a text editor.
2. Edit the Snort config file and look for the following line containing HOME\_NET

ipvar HOME\_NET any

1. Change the word “any” to your web-server2 IP address.

Change to the IP address of your web-server2

ipvar HOME\_NET 192.168.13.100

This means Snort will treat your web-server2 as the “home network” that it will protect.

1. Check that EXTERNAL\_NET is set to the value “any”

ipvar EXTERNAL\_NET any

1. Check the value for RULE\_PATH. It is currently set to /etc/snort/rules, which means rule files should be placed in this folder.

var RULE\_PATH /etc/snort/rules

1. Set the values for SO\_RULE\_PATH, PREPROC\_RULE\_PATH, WHITE\_LIST\_PATH and BLACK\_LIST\_PATH.

var SO\_RULE\_PATH /etc/snort/so\_rules

var PREPROC\_RULE\_PATH /etc/snort/preproc\_rules

var WHITE\_LIST\_PATH /etc/snort/rules

var BLACK\_LIST\_PATH /etc/snort/rules

1. Scroll to the bottom of the file, where you see a list of rule files. Currently we do not have these rule files yet, so we need to comment them out. Add the hex sign to the front of each rule file.

# site specific rules

Add the hex sign to comment out the rule files.

#include $RULE\_PATH/local.rules

#include $RULE\_PATH/app-detect.rules

#include $RULE\_PATH/attack-responses.rules

Continue to comment out the rest of the rule files

1. Save the Snort config file.
2. Create the directory for Snort dynamic rules.

mkdir /usr/local/lib/snort\_dynamicrules

1. Create empty white and black lists.

touch /etc/snort/rules/white\_list.rules

touch /etc/snort/rules/black\_list.rules

1. Run Snort manually. The -i option is to specify the network interface card that Snort will listen on. The -l option means captured network packets will be logged into the specified directory.

snort –i eno16777736 –c /etc/snort/snort.conf –l /var/log/snort

The name of the web-server2 network interface card

1. Check that Snort can run without any errors.
2. Do a Control-C to end the Snort program.

**Exercise Creating a Snort rule file**

In web-server2 VM:

1. Look at the contents of /etc/snort/rules. There are no rules yet.
2. You will now create a rule that creates an alert every time there is TCP traffic from your Kali VM.
3. Create a file /etc/snort/rules/my.rules and enter the following rule in this file. Use a big SID (Snort ID for a rule) so that it will not clash with existing real SIDs from Snort.

Replace Kali\_IP with the IP address of your Kali VM

alert tcp *Kali\_IP* any -> $HOME\_NET any (msg:"TCP traffic from Kali!!"; sid:99999;)

1. Edit /etc/snort/snort.conf.
2. Scroll to the bottom of the file, where you see the list of rule files.
3. Add the rule file that you just created :

# site specific rules

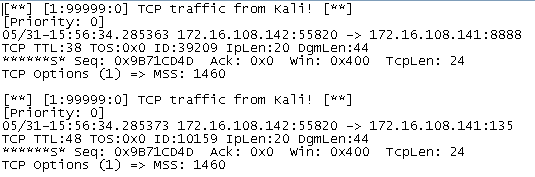
Specify the my.rules that you just created

include $RULE\_PATH/my.rules

1. Run Snort manually.

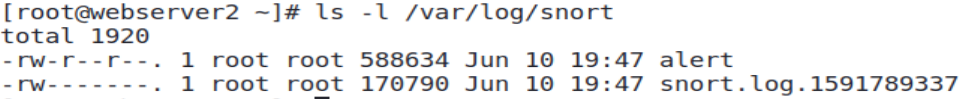
snort –i eno16777736 –c /etc/snort/snort.conf –l /var/log/snort

1. From your Kali VM, do a nmap scan against your web-server2.
2. When the scan is complete, stop Snort.
3. View the contents of the file /var/log/snort/alert. All the alerts messages due to TCP traffic from your Kali are captured here. (see following diagram)



1. In the /var/log/snort directory, there is another file snort.log.NNNNNNN. This file can be opened in Wireshark and contains the packets that generated the alerts. (see following diagram)

The generated alerts in a text file



Log file containing the packets that generated the alerts. Can be opened by Wireshark.

**Exercise Creating Snort rules to detect illegal TCP flags**

Description : A Null packet is a TCP packet that does not have any of the TCP flags set. This is an illegal packet. You will now create a Snort rule that detects such null packets.

In web-server2 :

1. Comment out any existing rules in /etc/snort/rules/my.rules. Create the following rule.

alert tcp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"Null packet detected!!"; flags:0; sid:99998;)

1. Run Snort manually.

snort –i eno16777736 –c /etc/snort/snort.conf –l /var/log/snort

In Kali:

1. Run a Null scan against some ports on your web-server2.

Change to your web-server2 IP

sudo nmap –sN –p21,22,23 192.168.13.100

In web-server2:

1. Check the /var/log/snort/alert file to view the alert messages about the null packets.
2. Stop Snort.

**Exercise Using the Snort community rules**

Description : To write from scratch all the rules to detect all possible known network attacks would be a time-consuming and difficult task. Fortunately, ready-made and up-to-date Snort rules are available for download.

In this example, we will use the Snort community rules which are free to use.

In web-server2:

1. The Snort installation zip file contains a file called community-rules.tar.gz.
2. Untar and extract the Snort community rules.

tar –xvf community-rules.tar.gz

1. Copy the Snort community rules to /etc/snort/rules.

cp community-rules/community.rules /etc/snort/rules

1. Edit the community.rules to see the Snort community rules.

vi /etc/snort/rules/community.rules

You can use other text editors to edit the rules in the file community.rules

We will now try out one of the Snort community rules.

1. In the community.rules file, look for the following rule (sid:382) which will generate an alert whenever there is an ICMP packet sent by a Windows system. Remove the hex sign in front of the line to uncomment it.

alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"PROTOCOL-ICMP PING Windows"; itype:8; content:"abcdefghijklmnop"; depth:16; metadata:ruleset community; classtype:misc-activity; sid:382; rev:11;)

Remove the hex sign to uncomment this rule (sid:382)

1. Edit /etc/snort/snort.conf. Look for the section where you added my.rules.
2. Add the community.rules file :

# site specific rules

include $RULE\_PATH/my.rules

Specify the community.rules

include $RULE\_PATH/community.rules

1. Run Snort manually.

snort –i eno16777736 –c /etc/snort/snort.conf –l /var/log/snort

In Kali:

1. Ping to your web-server2.

In any Windows VM or Host PC:

1. Ping to your web-server2.

In web-server2:

1. Check the /var/log/snort/alert file to view the alert messages about the null packets. Only the ICMP packets from the Windows system have alert messages. The ICMP packets from Kali do not have alert messages.
2. Stop Snort.

**Exercise Running Snort as a service**

Description : So far we have been running Snort at the command line. Snort can also run as a service.

In web-server2:

1. Edit the file /etc/sysconfig/snort.
2. Look for the following INTERFACE line and update it to the name of the web-server2 network interface.

INTERFACE=eno16777736

1. Look for the following USER and GROUP lines and update them to run Snort as user root.

USER=root

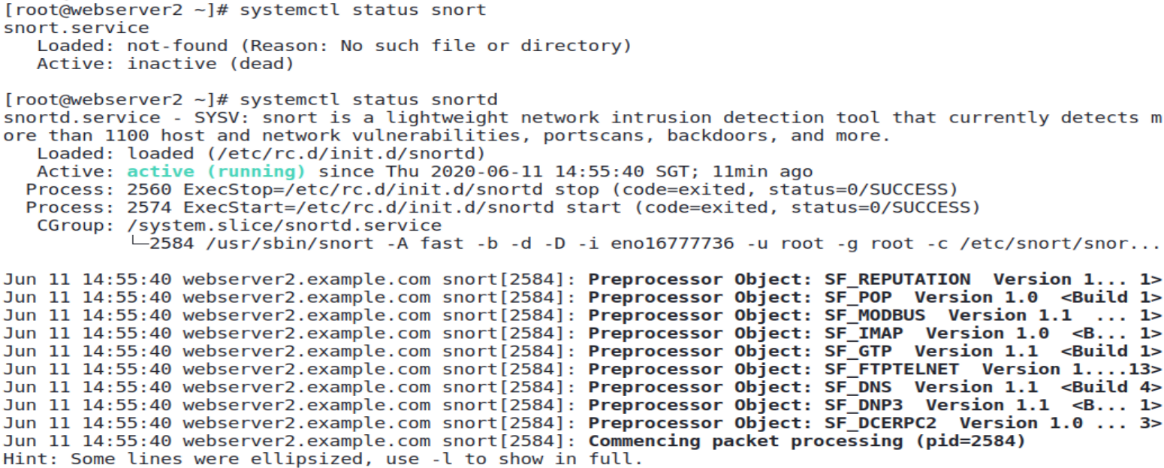
GROUP=root

1. Start the Snort service.

systemctl start snortd

1. Check that the Snort service is running.

systemctl status snortd



Snort is running

1. The following command will stop the Snort service.

systemctl stop snortd

**Part 2 : Host-Based Intrusion Detection Systems (HIDS)**

**Exercise Using Tripwire**

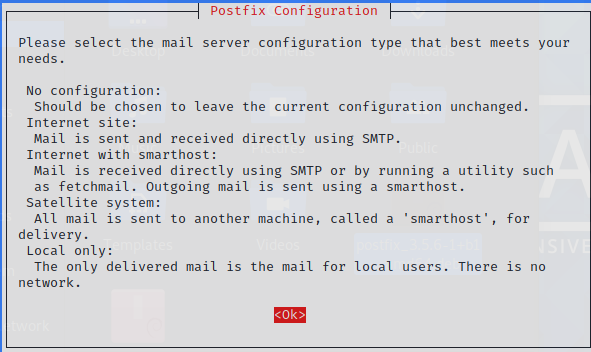
In Kali:

1. Download the Tripwire zip file from Brightspace or from the download link under Topic 7 IDS. You can also download from http.kali.org, or run “apt install tripwire”.
2. Extract the Tripwire zip file. There are two installation packages : Postfix and Tripwire.
3. If your Kali already has Postfix installed, or another mail transport agent like Exim installed, you do not need to install the Postfix package. You can proceed to install the Tripwire package.

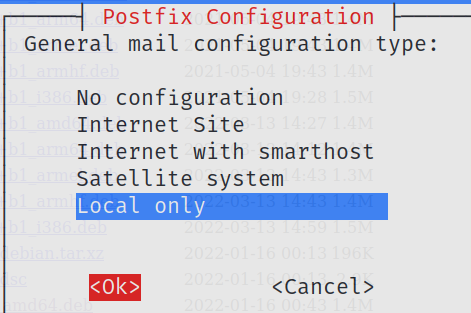
To install the Postfix package:

sudo dpkg -i postfix\_*NNNN*\_amd64.deb where NNNN is the version number

1. At the first screen of the Postfix installation, use the Tab key to move to OK and press OK.



1. The Postfix installation will then ask you to select a mail server configuration. Use the arrow keys to move to “Local only”. Use the Tab key to move to OK and press Enter. (see following diagram)



Use the arrow keys to move to “Local only”

Use the Tab key to move to “OK” and press Enter

1. When asked for System mail name, just accept the default value and press Enter.
2. Install the Tripwire package.

sudo dpkg -i tripwire\_*nnnnn*\_amd64.deb

1. Select the default settings during installation. Use the Tab or Enter key to select the OK button. When asked to create site and local passphrases, you can enter “password” as the passphrase. Note : you should use more secure passwords on real systems.
2. Tripwire will monitor files on the hard disk, and alert when any file is modified.

Next , as user root, edit the Tripwire Policy text file /etc/tripwire/twpol.txt to see which files are being monitored (use sudo if necessary, to edit as user root).

1. A number of files listed in the Tripwire Policy text file do not exist on the Kali image. We shall comment out these files so that Tripwire will not complain about missing files when it is run.

Look for the following lines and add a hex sign to comment them.

(

rulename = "Boot Scripts",

severity = $(SIG\_HI)

)

{

/etc/init.d -> $(SEC\_BIN) ;

Add a hex sign at the start of this line to comment it as /etc/rc.boot directory does not exist in our Kali

# /etc/rc.boot -> $(SEC\_BIN) ;

/etc/rcS.d -> $(SEC\_BIN) ;

(

rulename = "System boot changes",

severity = $(SIG\_HI)

)

Comment these lines /var/lock and /var/run as the files in these directories will keep changing so we are configuring Tripwire not to monitor them.

{

# /var/lock -> $(SEC\_CONFIG) ;

# /var/run -> $(SEC\_CONFIG) ;

/var/log -> $(SEC\_CONFIG) ;

}

(

rulename = "Root config files",

severity = 100

)

{

/root -> $(SEC\_CRIT) ;

Comment these lines as these files/directories do not exist on our Kali

# /root/mail -> $(SEC\_CONFIG) ;

# /root/Mail -> $(SEC\_CONFIG) ;

# /root/.xsession-errors -> $(SEC\_CONFIG) ;

# /root/.xauth -> $(SEC\_CONFIG) ;

# /root/.tcshrc -> $(SEC\_CONFIG) ;

# /root/.sawfish -> $(SEC\_CONFIG) ;

# /root/.pinerc -> $(SEC\_CONFIG) ;

# /root/.tcshrc -> $(SEC\_CONFIG) ;

# /root/.mc -> $(SEC\_CONFIG) ;

# /root/.gnome\_private -> $(SEC\_CONFIG) ;

# /root/.gnome\_desktop -> $(SEC\_CONFIG) ;

# /root/.gnome -> $(SEC\_CONFIG) ;

# /root/.esd\_auth -> $(SEC\_CONFIG) ;

# /root/.elm -> $(SEC\_CONFIG) ;

# /root/.cshrc -> $(SEC\_CONFIG) ;

/root/.bashrc -> $(SEC\_CONFIG) ;

# /root/.bash\_profile -> $(SEC\_CONFIG) ;

# /root/.bash\_logout -> $(SEC\_CONFIG) ;

# /root/.bash\_history -> $(SEC\_CONFIG) ;

# /root/.amandahosts -> $(SEC\_CONFIG) ;

# /root/.addressbook.lu -> $(SEC\_CONFIG) ;

# /root/.addressbook -> $(SEC\_CONFIG) ;

# /root/.Xresources -> $(SEC\_CONFIG) ;

# /root/.Xauthority -> $(SEC\_CONFIG) ;

# /root/.ICEauthority -> $(SEC\_CONFIG) ;

}

(

rulename = "Devices & Kernel information",

severity = $(SIG\_HI)

)

{

Comment this line /proc as the files in this directory change very frequently

/dev -> $(Device) ;

# /proc -> $(Device) ;

You can always customise this Tripwire Policy file to specify the files/directories you want to monitor

1. Save the Tripwire Policy text file.
2. Recreate the encrypted Tripwire Policy file by running the following command :

sudo twadmin -m P /etc/tripwire/twpol.txt

If you are asked to enter the site passphrase, enter the passphrase that you have just set.

1. Create the baseline database (snapshot of the current system) by running

sudo tripwire –-init

If you are asked to enter the local passphrase, enter the passphrase that you have just set.

(This may take a few minutes. There may be a few error messages as there may be other files and directories specified in the default policy file that do not match our Kali environment)

1. When it is complete, run the following command to list the contents of the directory /var/lib/tripwire to view the baseline database created. The database file usually ends with a .twd extension.

ls /var/lib/tripwire



The baseline database file is “kali.twd” in this example

1. Create a change in the system by creating a new user. This will cause changes to files like /etc/passwd and /etc/group.

sudo useradd mary

1. Check for any changes in your system by running a Tripwire check.

sudo tripwire --check

1. A report will be generated and stored in /var/lib/tripwire/report. Change directory to the /var/lib/tripwire/report directory and list the contents of the directory to view the report file. The report file usually ends with a .twr extension.

cd /var/lib/tripwire/report

ls

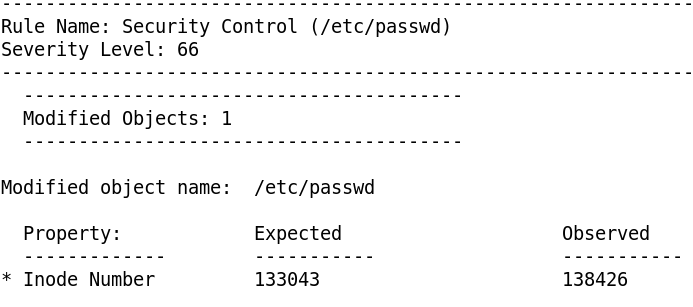


The Tripwire report

1. View the report by running twprint, replacing *report\_filename* with the actual filename.

sudo twprint --print-report -r *report\_filename* | less

1. Use the PageUp and PageDown keys to scroll through the report. Spot the changes reported to files like /etc/passwd and /etc/group. Press the q key to quit the viewer.



Sample extract from Tripwire report on /etc/passwd being modified

Other popular Host-Intrusion Detection Systems (HIDS) include AIDE, OSSEC and Osiris.

*End of Practical*