ICS007 Industrial Control System Security Laboratory Project
Intrusion Detection with Snort

Lab Objective:
The objective of this project is to familiarize you with Intrusion Detection Systems (IDS), IDS Tools, IDS signatures and rules, the configuration and implementation of common open-source IDS tools, and the analysis and identification of possible system infections, compromises and other problems that will trigger an incident response process.

Lab Environment:
This lab requires a pre-configured USB drive with Kali Linux.

Lab Duration
20 minutes

Lab Tasks
Configure Snort for intrusion detection.

Background
Snort is an open source network intrusion prevention system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more (https://www.snort.org/faq/what-is-snort (Snort, 2016)).

Lab Scenario
Snort needs to be configured to be able to determine incoming attack packets and raise corresponding alerts. The protocols that need to be watched are modbus, icmp, ftp, http, and telnet.

Lab Procedure-Using Snort

To manually configure your wireless device on Kali Linux:

1. Open a browser on the desktop and type in 192.16.11.1 as the URL
2. Enter ***admin*** and ***password*** for the account name and password
3. Note the ***SSID*** and the ***Passphrase*** for the router.
4. Setup the wifi by clicking on the Dropdown Arrow on the rightmost top corner ofthe menu bar; Select Network and enter SSID and Passphrase
5. Open a command prompt/console and type the following commands:

```
ifconfig wlan0 192.168.11.124 netmask 255.255.255.0 up

route add default gw 192.168.11.1 wlan0
```

1. Using your favorite editor such as **nano** or **pico**, edit the snort configuration file:

```
nano /etc/snort/snort.conf
```

2. Configure your local network by replacing “***ipvar HOME_NET any***” with “***ipvar HOME_NET 192.168.11.0/24***”.

3. Save the configuration file by pressing "ctrl+x", "y" and "enter".

4. The core of Snort’s intrusion detection is on the catalog of signatures that are found in the rule sets. The predefined rules sets are found in ***/etc/snort/rules***. Those rule set files are properly named to indicate the family of signatures that each contains. Those rule sets are referenced in the snort configuration file. You are required to disable all references to the predefined rule sets (See the section labeled **Step #8** in the **snort.conf** file), except the one that references your own rules***:*** ***local.rules***, in the snort configuration file (***snort.conf***) by putting a hash (#) symbol at the start of the line. For example, the line:

```
include $RULE_PATH/bad-traffic.rules
```

should be edited to look like

```
#include $RULE_PATH/bad-traffic.rules
```

You should see all of the rule references in the snort configuration file by searching for a line that looks like:

```
# Step #7: Customize your rule set
```

Add a hash (#) mark at the beginning for all lines that start with this two- word pattern:

```
include $RULE_PATH
```

except, of course, the very first rule reference that looks like

```
include $RULE_PATH/local.rules
```

5. Next, you need to edit the file **/etc/snort/rules/local.rules** to include rules that will satisfy the following requirements:
    a. All rules must monitor activities coming from an attacking station in the local network.
    b. There must be at least one rule that will trigger an alert on each of the following activities:
        i. *modbus*
        ii. *system reconnaissance (like nmap);*
        iii. *ftp;*
        iv. *telnet;*
        v. *attempted attacks on the web server (on port 80 for instance)*

A sample rule for Modbus would look the following:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET (msg:”MODBUS attack warning”; sid:1379; )
```

Leave ***Snort*** running for at least **10 minutes**. One of the computers is configured to automatically run hacking/reconnaissance probes every 3 minutes on other machines. If you wrote your rules correctly on the ***local.rules*** file, you should see the expected results in the ***alert*** file. Gather the results. Note that the log file: ***alert*** is saved in the default directory: ***/var/log/snort***. You may need to start fresh by deleting and creating a new ***alert*** file using the following:

```
rm alert;  echo “START OF A NEW ALERT” > alert;   chmod 766 alert
```

6. Kill the running Snort process by the following commands:

   ```
   ps -A | grep snort
   ```

   This will give you the process ID (**pid**) of the running snort process. Stop the process by

   ```
   kill <pid>
   ```

   where <**pid**> is the process ID of the running snort process.

7. Manually start snort by the command:

   ```
   snort -i wlan0 -A full -q -c /etc/snort/snort.conf –g snort -D
   ```

8. Check whether snort is running by using the command:

   ```
   ps -A | grep snort
   ```

   This will give you the process ID (**pid**) of the running snort process. Stop the process by

   ```
   kill <pid>
   ```

   where <**pid**> is the process ID of the running snort process.

9. Check your ***alert*** file in the ***/var/log/snort*** directory to make sure it is being updated.

Lab Procedure- NIDS with Snort on Windows

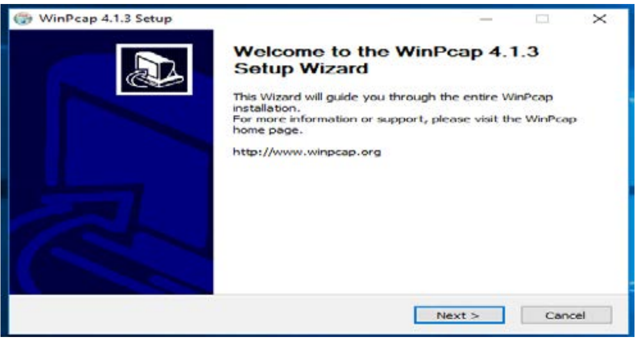
Download and Setup the Snort Application

Requirements:
Packages:

Snort: Snort_2_9_9_0_installer.exe (current latest version)
WinPcap: WinPcap_4_1_3.exe (current latest version)
Snort rules: snortrules-snapshot-2990.tar.gz (current updated rules)

Setup procedure:

1. Start by installing the WinPCap libraries. Accept all of the default settings. Download the winPacp (latest version: WinPcap_4_1_3.exe) from https://www.winpcap.org/install/default.htm .
2. Start the installation by right clicking the installation file and selecting "Run as Administrator". You will be presented a title screen.



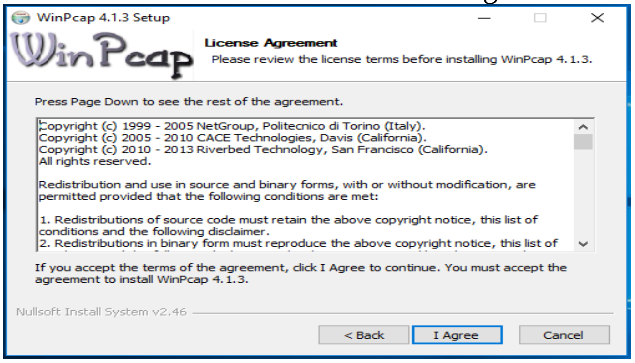
WinPcap 4.1.3 Setup

Welcome to the WinPcap 4.1.3 Setup Wizard

This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.

http://www.winpcap.org

A) Just click "Next" to continue to the License Agreement screen.



WinPcap 4.1.3 Setup

License Agreement
Please review the license terms before installing WinPcap 4.1.3.

Press Page Down to see the rest of the agreement.

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
Copyright (c) 2010 - 2013 Riverbed Technology, San Francisco (California).
All rights reserved.

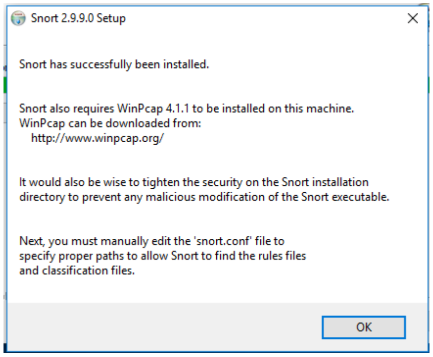
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.3.

Nullsoft Install System v2.46

3. Download Snort for Windows from www.snort.org and install.



Snort 2.9.9.0 Setup

Snort has successfully been installed.

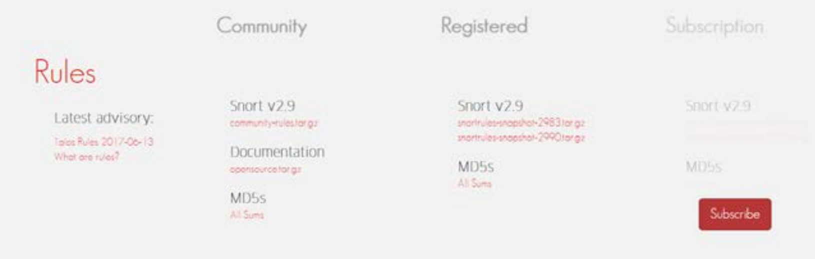
Snort also requires WinPcap 4.1.1 to be installed on this machine.
WinPcap can be downloaded from:
http://www.winpcap.org/

It would also be wise to tighten the security on the Snort installation directory to prevent any malicious modification of the Snort executable.

Next, you must manually edit the 'snort.conf' file to specify proper paths to allow Snort to find the rules files and classification files.

Click "OK" to acknowledge this and close the setup application.

4. Download the Snort rules package and these are available in three categories. Community (free to download); Registered (free to download but need to register for it); Subscription (need to be paid). We would suggest you download Registered Snort Rules package.

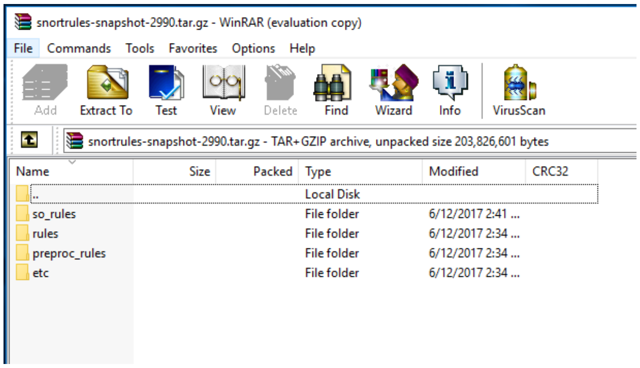


Rules

Latest advisory:
Talos Rules 2017-06-13
What are rules?

Community	Registered	Subscription
Snort v2.9 community-rules.tar.gz	Snort v2.9 snortrules-snapshot-2983.tar.gz snortrules-snapshot-2990.tar.gz	Snort v2.9
Documentation opensource.tar.gz	MD5s All Sums	MD5s
MD5s All Sums		Subscribe

5. Open the Snort rules package. Depending on your operating system, Windows may be able to open the zipped archive file automatically, or you can use a utility such as WinZip, 7Zip, or WinRAR to open it. Once opened the package, you can see the following window. For our Lab, we only extract “rules” and “preproc_rules” to snort.



snortrules-snapshot-2990.tar.gz - WinRAR (evaluation copy)

snortrules-snapshot-2990.tar.gz - TAR+GZIP archive, unpacked size 203,826,601 bytes

Name	Size	Packed	Type	Modified	CRC32
..			Local Disk		
so_rules			File folder	6/12/2017 2:41 ...	
rules			File folder	6/12/2017 2:34 ...	
preproc_rules			File folder	6/12/2017 2:34 ...	
etc			File folder	6/12/2017 2:34 ...	

a) Extract the contents of the “rules” folder in the archive to “C:\Snort\rules”

b) Extract the contents of the “preproc_rules” folder in the archive to “C:\Snort\preproc_rules”. If the extracted files already existed, just replace all the files with newly extracted files.

6. To check whether the Snort is installed, open command prompt in your computer and type following commands:

cd C:\Snort
cd bin
snort -V

Snort Configuration:

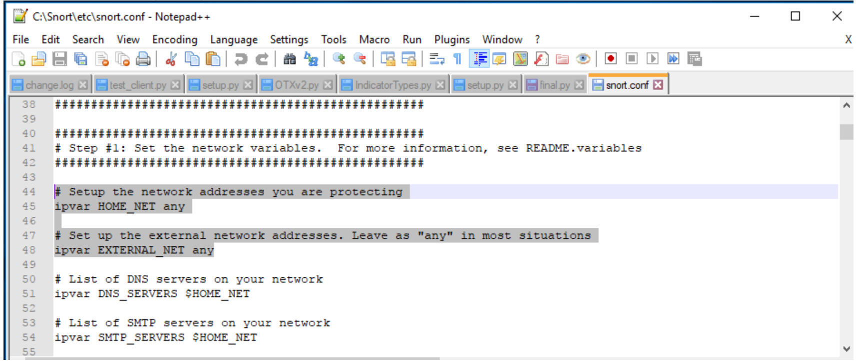
1. Now, we will need to change a couple of parameters in the “c:\Snort\etc\snort.conf” file. Snort.conf is plain text file, so we can use any text editor. To do so, let's use Notepad++ application. When you open the snort.conf file for viewing or editing, you will see it is organized into 9 steps:

1) Set the network variables.
2) Configure the decoder
3) Configure the base detection engine
4) Configure dynamic loaded libraries
5) Configure preprocessors
6) Configure output plugins
7) Customize your rule set
8) Customize preprocessor and decoder rule set
9) Customize shared object rule set

As you can see, there are a lot of ways to customize Snort, and making sense of the entire snort.conf file can be a little daunting. To get running for the first time, many of the defaults can be left alone. The following edits are recommended:

Step 1:

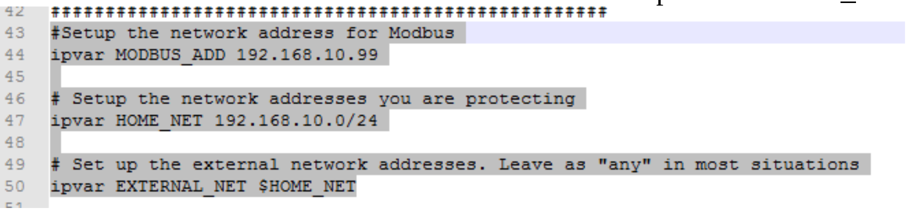
i. Edit the highlighted text is shown in below screen.


C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
test_client.py
setup.py
OTXv2.py
IndicatorTypes.py
setup.py
final.py
snort.conf

```
###################################################

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

```

Include your home network address at “any” part in “ipvar HOME_NET any”. Ex: ipvar HOME_NET 192.168.10.0/24. Also change “ipvar EXTERNAL_NET any” to ipvar EXTERNAL_NET !$HOME_NET.

Also create another variable for MODBUS IP address: ipvar MODBUS_NET 192.168.10.99



```
###################################################
#Setup the network address for Modbus
ipvar MODBUS_ADD 192.168.10.99

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.10.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET $HOME_NET
```

Next, you need to make the following changes:

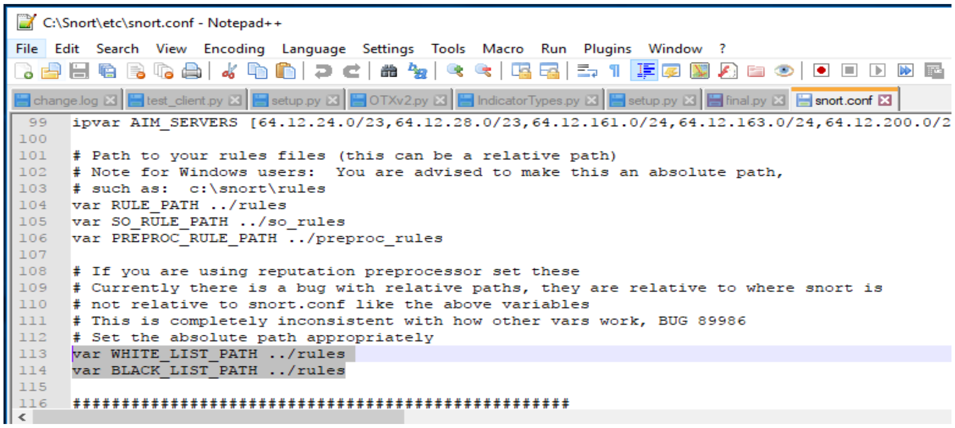
a) Change the var RULE_PATH declaration to var RULE_PATH C:\Snort\rules
b) Comment out (meaning put a # character in the first position in the line) the SO_RULE_PATH declaration
c) Change the var PREPROC_RULE_PATH declaration to var PREPROC_RULE_PATH C:\Snort\preproc_rules

Now in notepad++, create two empty files namely, white.list and black.list (when you are saving the file save it as ‘all types’ format) and add it to C:\Snort\rules.

It may look like this after adding the path:

```
var WHITE_LIST_PATH C:\Snort\rules
var BLACK_LIST_PATH C:\Snort\rules
```

After creating two files, add the location of files in snort.conf as shown below:

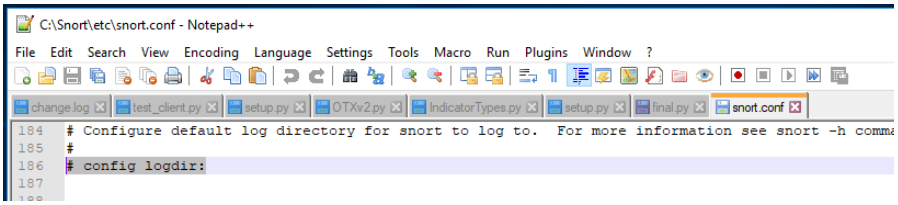

C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
test_client.py
setup.py
OTXv2.py
IndicatorTypes.py
setup.py
final.py
snort.conf

```
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/2

# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH ../rules
var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH ../preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH ../rules
var BLACK_LIST_PATH ../rules

###################################################
```

Step 2:

a. For most users, there are no changes needed to the decoder configurations.

b. At the end of this section, there is a configuration setting to indicate the default directory where Snort logs should be written. Uncomment the following marked line by deleting the # character in the first position and edit the line to include the C:\Snort\log default directory path.


C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
test_client.py
setup.py
OTXv2.py
IndicatorTypes.py
setup.py
final.py
snort.conf

```
# Configure default log directory for snort to log to.  For more information see snort -h comma
#
# config logdir:
```

It should look like this after edit:

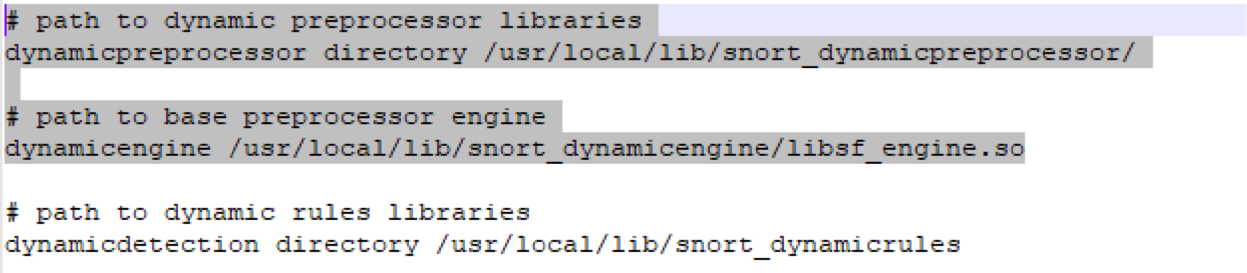
config logdir: C:\Snort\log

Step 3:

For most users, there are no changes needed to the base detection engine settings. Skip this step.

Step 4:

a) Change the dynamic loaded library path references to reflect their location in windows for the following highlighted text



```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory /usr/local/lib/snort_dynamicpreprocessor/

# path to base preprocessor engine
dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so

# path to dynamic rules libraries
dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

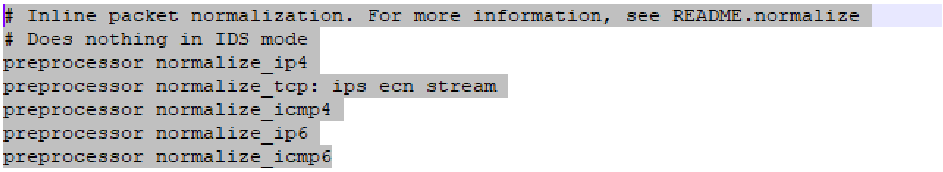
Ex: dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

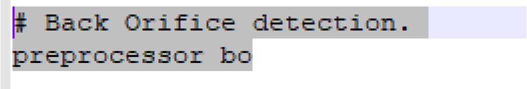
b) Comment out the **dynamicdetection directory** declaration

Step 5:

a) Comment out all the rows in the Inline packet normalization preprocessor (shown below).

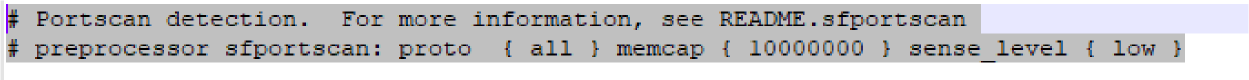


```
# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
preprocessor normalize_ip4
preprocessor normalize_tcp: ips ecn stream
preprocessor normalize_icmp4
preprocessor normalize_ip6
preprocessor normalize_icmp6
```



```
# Back Orifice detection.
preprocessor bo
```

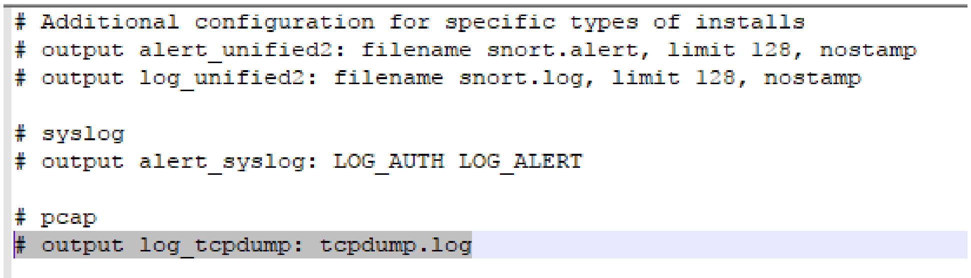
b) uncomment the marked text is shown in below



```
# Portscan detection.  For more information, see README.sfportscan
# preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }
```

c) change the file name of white list and black list rules, which are marked in the below screenshot.

Step 6:
a) Typically, only one of the output plugins is used with Snort at any one time. The default is unified2, which is not well supported on Windows platforms. For this lab, we use "pcap" plugin and uncomment the marked text is shown in below screenshot.



```
# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog
# output alert_syslog: LOG_AUTH LOG_ALERT

# pcap
# output log_tcpdump: tcpdump.log
```

Step 7 and Step 8:
In windows, the directory path represented with '\' rather than '/'. So just replace '/' with '\' in paths of site specific rules as well as decoder and preprocessor event rules.

Step 9: Save the file.

To see If Snort is working, beyond just getting it to load without errors, it is helpful to generate some alerts. The easiest way to do this to validate setup and configuration is to create a couple of testing rules, load them in Snort, and trigger them so you can check to see if they generate alerts as expected. Put your testing rules in the **local.rules** file that is located in the **C:\Snort\rules** directory.

Creating rules on Snort:

i. Open local.rules file with a text editor such as Notepad++ or Wordpad.
ii. write some rules such as:

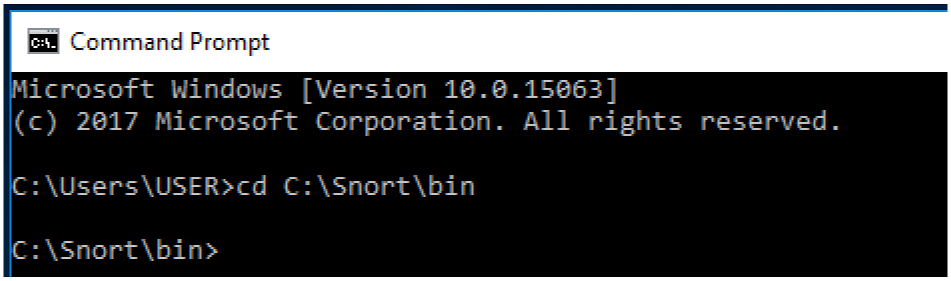
alert icmp any any -> any any (msg: "ICMP Testing Rule"; sid:1000001; rev:1;)
alert tcp any any -> any any (msg: "TCP Testing Rule"; sid:1000002; rev:1;)
alert udp any any -> any any (msg: "UDP Testing Rule"; sid:1000001; rev:1;)

iii. Now test these rules by performing the steps listed below so that you can see the output on the screen as it happens.

Generating alerts on Snort:

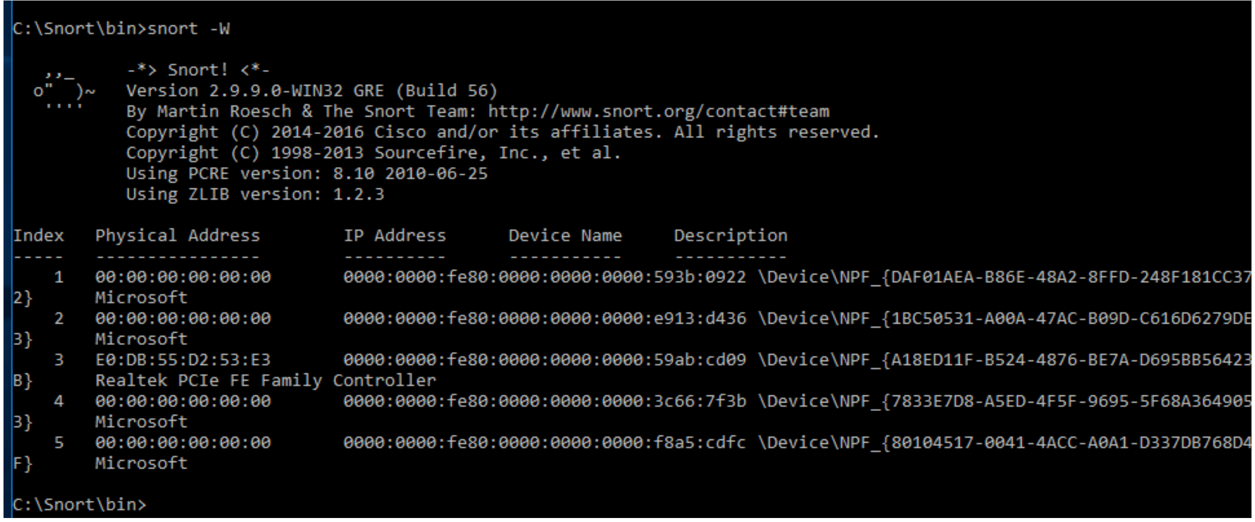
a) Locate command prompt and run it as administrator by right clicking on it.
b) Navigate to the directory where Snort is installed by typing following command:

cd C:\Snort\bin



```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\USER>cd C:\Snort\bin

C:\Snort\bin>
```

c) Before testing it is a good idea to determine which interface you want Snort to monitor. Since many systems have multiple network interfaces. Use **snort -W** to view the available interfaces.



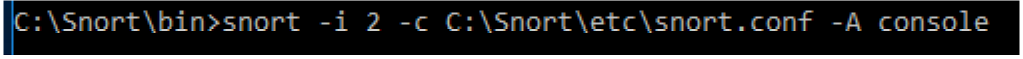
```
C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.9.0-WIN32 GRE (Build 56)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:593b:0922 \Device\NPF_{DAF01AEA-B86E-48A2-8FFD-248F181CC37
2}      Microsoft
    2   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:e913:d436 \Device\NPF_{1BC50531-A00A-47AC-B09D-C616D6279DE
3}      Microsoft
    3   E0:DB:55:D2:53:E3       0000:0000:fe80:0000:0000:0000:59ab:cd09 \Device\NPF_{A18ED11F-B524-4876-BE7A-D695BB56423
B}      Realtek PCIe FE Family Controller
    4   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:3c66:7f3b \Device\NPF_{7833E7D8-A5ED-4F5F-9695-5F68A364905
3}      Microsoft
    5   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:f8a5:cdfc \Device\NPF_{80104517-0041-4ACC-A0A1-D337DB768D4
F}      Microsoft

C:\Snort\bin>
```

Example 1:

i) Start snort with this command:

snort -i 2 -c C:\Snort\etc\snort.conf -A console

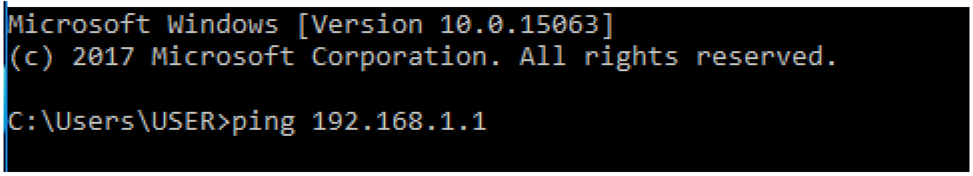
here -i is the system interface you want Snort to monitor.



```
C:\Snort\bin>snort -i 2 -c C:\Snort\etc\snort.conf -A console
```

ii) Now open another command prompt window and send a ping command to your local gateway (or any other host)

Ex: ping 192.168.1.1



```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\USER>ping 192.168.1.1
```

iii) Open a web browser and browse to any web page.

iv) You should see the alerts Snort produces in the first terminal shell where Snort is running.

Example 2:

snort –d –e –v –l C:\Snort\log –c C:\Snort\etc\snort.conf (or)

snort –dev –l C:\Snort\log –c C:\Snort\etc\snort.conf (both are same)

ICS007 ICS Intrusion detection with Snort

Modbus specific Snort rules

Sample Snort rules that are Modbus specific are the following:

alert tcp $EXTERNAL_NET any -> $MODBUS_ADD 502 (content: "|05|"; offset:7; depth:1; flow:established, to_server; msg:"Modbus-write coil warning"; sid:1000001; rev:0; priority:6;)
alert tcp $EXTERNAL_NET any -> $MODBUS_ADD 502 (content: "|04|"; offset:7; depth:1; flow:established, to_server; msg:"Modbus-read input register warning"; sid:1000002; rev:0; priority:6;)
alert tcp $EXTERNAL_NET any -> $MODBUS_ADD 502 (content: "|01|"; offset:7; depth:1; flow:established, to_server; msg:"Modbus-read coils warning"; sid:1000003; rev:0; priority:6;)
alert tcp $EXTERNAL_NET any -> $MODBUS_ADD 502 (content: "|0f|"; offset:7; depth:1; flow:established, to_server; msg:"Modbus-write multiple coils warning"; sid:1000004; rev:0; priority:6;)

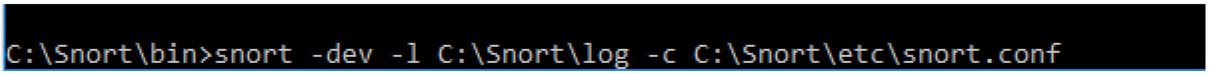
These rules are placed in the ***local.rules*** file (in the ***C:\Snort\rules*** folder) to monitor Modbus protocol activities.

Additional options for running Snort
i) if you use only **–d –e –v along with snort**, which means that you are running Snort in **sniffer mode**.

-v: printing the TCP/IP packet headers on the screen
-dv: shows the IP and TCP/ICMP/UDP/ headers as well as application transit data (packet data)
-dev: more descriptive display and shows the data link layer headers

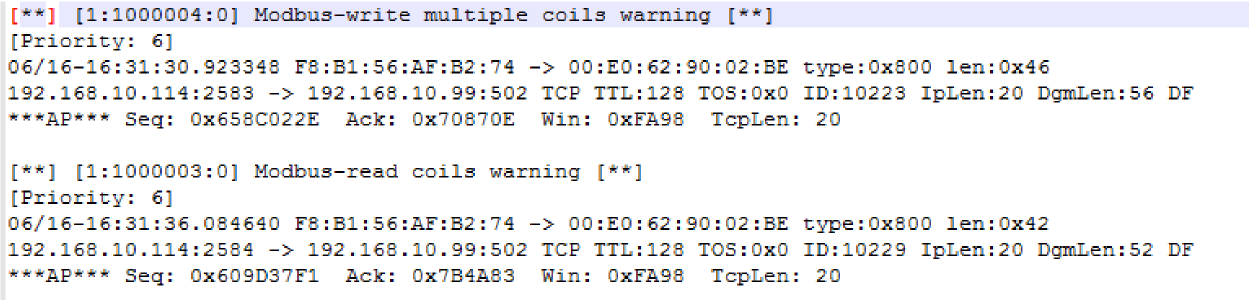
ii) If you use **–l (place log directory path) along with snort**, which means that you are running Snort in **packet logger mode**.

iii) if you use **–c (place snort.conf directory path) along with snort**, which means that you are Snort in **Network Intrusion Detection System mode**.



```
C:\Snort\bin>snort -dev -l C:\Snort\log -c C:\Snort\etc\snort.conf
```

After executing above command, we can see following type of alerts in log directory (C:\Snort\log)



```
[**] [1:1000004:0] Modbus-write multiple coils warning [**]
[Priority: 6]
06/16-16:31:30.923348 F8:B1:56:AF:B2:74 -> 00:E0:62:90:02:BE type:0x800 len:0x46
192.168.10.114:2583 -> 192.168.10.99:502 TCP TTL:128 TOS:0x0 ID:10223 IpLen:20 DgmLen:56 DF
***AP*** Seq: 0x658C022E  Ack: 0x70870E  Win: 0xFA98  TcpLen: 20

[**] [1:1000003:0] Modbus-read coils warning [**]
[Priority: 6]
06/16-16:31:36.084640 F8:B1:56:AF:B2:74 -> 00:E0:62:90:02:BE type:0x800 len:0x42
192.168.10.114:2584 -> 192.168.10.99:502 TCP TTL:128 TOS:0x0 ID:10229 IpLen:20 DgmLen:52 DF
***AP*** Seq: 0x609D37F1  Ack: 0x7B4A83  Win: 0xFA98  TcpLen: 20
```