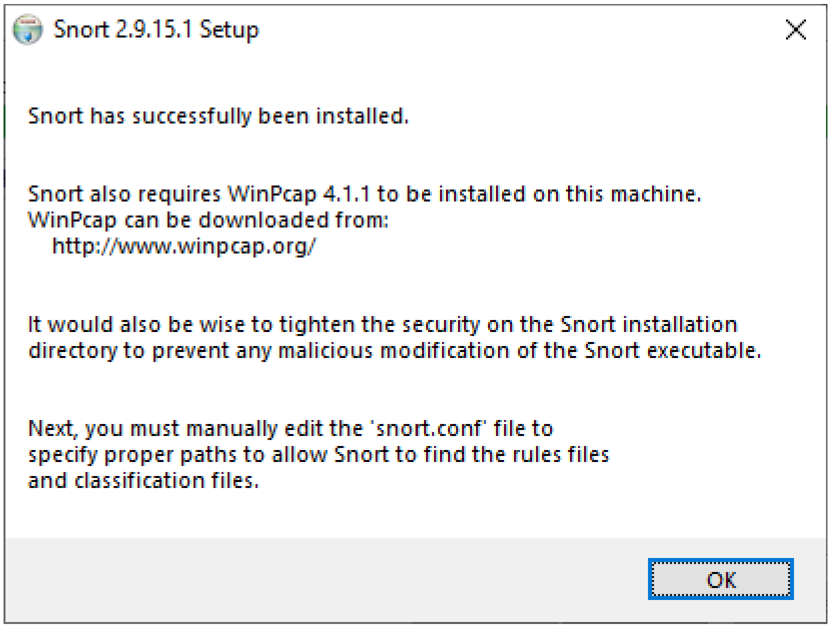
SNORT INSTALLATION GUIDE

Download snort and install on your computer.
https://www.snort.org/downloads#



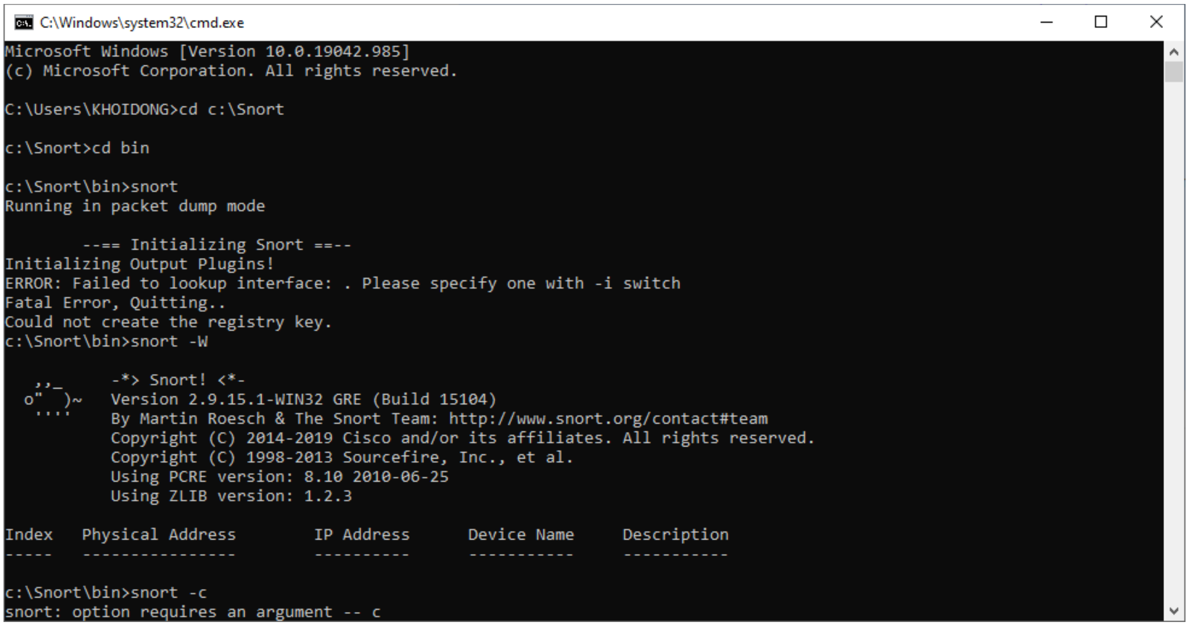
Snort has successfully been installed.

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

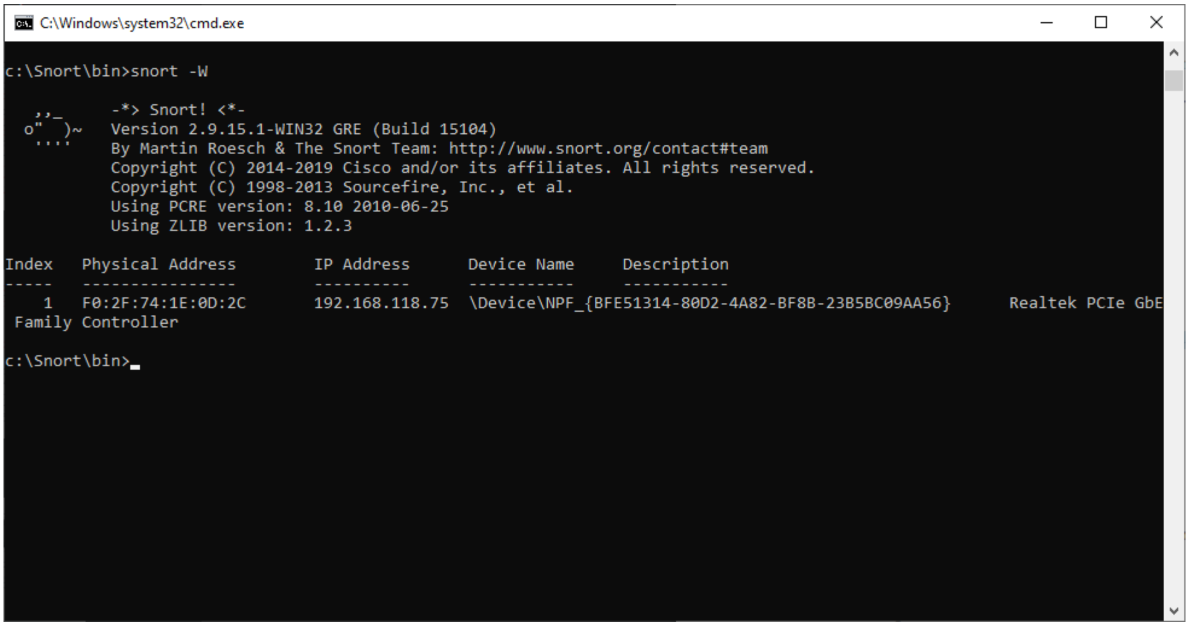
It would also be wise to tighten the security on the Snort installation directory to prevent any malicious modification of the Snort executable.

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

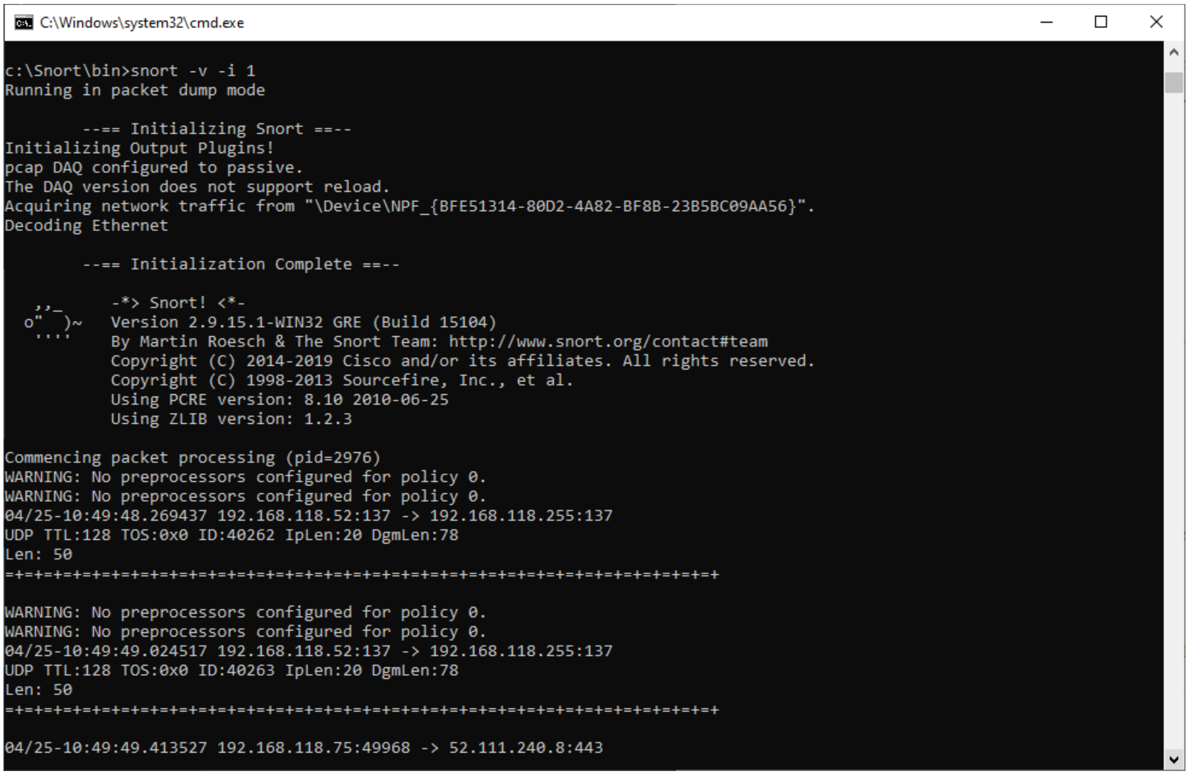
Download and install Winpcap before running snort:
https://www.winpcap.org/install/default.htm



```
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\KHOIDONG>cd c:\Snort

c:\Snort>cd bin

c:\Snort\bin>snort
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
ERROR: Failed to lookup interface: . Please specify one with -i switch
Fatal Error, Quitting..
Could not create the registry key.
c:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1-WIN32 GRE (Build 15104)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 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
-----   ----------------        ----------      -----------     -----------

c:\Snort\bin>snort -c
snort: option requires an argument -- c
```



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

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1-WIN32 GRE (Build 15104)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 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   F0:2F:74:1E:0D:2C       192.168.118.75  \Device\NPF_{BFE51314-80D2-4A82-BF8B-23B5BC09AA56}      Realtek PCIe GbE
 Family Controller

c:\Snort\bin>_
```



```
c:\Snort\bin>snort -v -i 1
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{BFE51314-80D2-4A82-BF8B-23B5BC09AA56}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1-WIN32 GRE (Build 15104)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 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

Commencing packet processing (pid=2976)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
04/25-10:49:48.269437 192.168.118.52:137 -> 192.168.118.255:137
UDP TTL:128 TOS:0x0 ID:40262 IpLen:20 DgmLen:78
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
04/25-10:49:49.024517 192.168.118.52:137 -> 192.168.118.255:137
UDP TTL:128 TOS:0x0 ID:40263 IpLen:20 DgmLen:78
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/25-10:49:49.413527 192.168.118.75:49968 -> 52.111.240.8:443
```

THEORY

A. SNORT COMMANDS AND TESTING

snort -W : to see your interfaces

Note that the order of interfaces to choose what interface to be detected by Snort.

For example, *-i1* means capture packets going through the first interface.

snort –c: Check configuration file

For example: *snort –c C:\Snort\etc\snort.conf*

–*i:* Select interface to listen

For example: *C:\Snort\bin>snort -v -i 1*

Choose interface 1 to listen

–v: set snort in verbose mode, where it highlights events.

–d: display data of application layer

–e: display layer 2 packets

–T: validate the configuration of Snort

-l: Specify the path to log

–A: set Snort into alert modes (fast, full or none)

-K = Logging mode [pcap (default), ascii, none]

For example:

C:\Snort\bin>snort -c C:\Snort\etc\snort.conf -i1 -l c:\Snort\log -A full -K ascii

Means: run snort using snort.conf file, listen on interface 1 and log captured packets into C:\Snort\log in ascii mode.

B. SNORT MODES

- Sniffer mode: snort will read the network traffic and print them to the screen
- Packet logger mode: snort will record the network traffic on a file
- IDS mode: network traffic matching security rules will be recorded

PRACTICE

C. ENVIRONMENT PREPARATION

Install Snort. Copy and extract snortrules-snapshot-2962.tar.gz to C:\Snort\

D. ERROR CORRECTION

Go to *C:\Snort\etc\snort.conf.* Open file using Notepad++.

Run: *C:\Snort\bin> snort.exe –c C:\Snort\etc\snort.conf -i 1 - T to* test Snort configuration file

ERROR: C:\Snort\etc\snort.conf(243) Could not stat dynamic module path

"/usr/local/lib/snort_dynamicpreprocessor/": No such file or directory.

Go to line 243. Change path into

```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
# path to base preprocessor engine
dynamicengine directory C:\Snort\lib\snort_dynamicengine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
# path to dynamic rules libraries
#dynamicdetection directory C:\Snort\lib\snort_dynamicrules
```

Notice: Be careful at this step. Everything must be exact.

Go to line 261 and comment the following lines

```
#preprocessor normalize_ip4
#preprocessor normalize_tcp: ips ecn stream #preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6
```

Go to line 101, and change to:

```
var RULE_PATH C:\Snort\rules
var SO_RULE_PATH C:\Snort\so_rules

var PREPROC_RULE_PATH C:\Snort\preproc_rules

# If you are using reputation preprocessor set these

#var WHITE_LIST_PATH ../rules

#var BLACK_LIST_PATH ../rules
```

Go to line 501 and change to

```
#preprocessor reputation: \

  #memcap 500, \

  #priority whitelist, \

  #nested_ip inner, \

  #whitelist $WHITE_LIST_PATH/white_list.rules, \

  #blacklist $BLACK_LIST_PATH/black_list.rules
```

Find and replace “ipvar” with “var”

Go to line 290 and change to

```
preprocessor http_inspect_server: server default profile apache ports { 80 }
```

Maybe there are more errors, please try to search and debug to run Snort successfully.

If you can’t do it successfully, please download snort.conf file from LMS and copy that file to C:\Snort\etc\ to replace C:\Snort\etc\snort.conf.

Go to C:\Snort\rules\local.rules. Open and add new rules

```
alert icmp any any -> any any (msg:"PING PING PING"; sid:10000003;)
```

E. SNORT TESTING AND DEPLOYMENT

a. Validate snort settings

Open cmd (run as administrator)

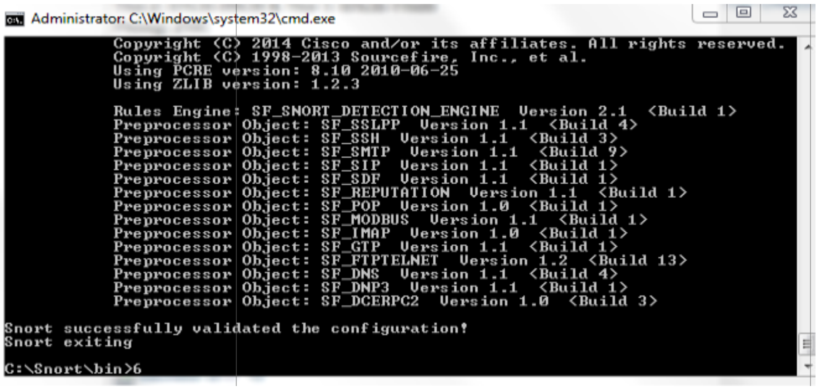
Type in CMD: *cd C:\Snort\bin*

Type *Snort -W* to check your interface.

Choose appropriate interface for Snort to detect packets. Keep in mind to choose your physical interface. For example, my physical interface is the first to be listed (when you commanded snort -W), I will use *-i 1* to specify my interface in snort command later on.

```
C:\Snort\bin>snort.exe -c C:\Snort\etc\snort.conf –l C:\Snort\log -i 1 –T
```

Check if it’s validated. If it print outs like this:



```
           Copyright (C) 2014 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

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>

Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>6
```

means you have finished error c**o**rrection. Now let’s run it.

b. Run in sniffer mode

*C:\Snort\bin>snort.exe -c C:\Snort\**e**tc\snort.conf -dev -i1 -l C:\Snort\log*

To see packets captured in sniff**e**r modes

c. Run snort in alert mode

Run: *C:\Snort\bin>snort.exe -c C:\Snort\etc\snort.conf -i1 -l C:\Snort\log -A full*

Open new CMD. **Ping** another c**o**mputer.

and open *alert.ids* to see the log**g**ing.