VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

Digital Assignment-I, MARCH 2021

B.Tech., Winter-2020-2021

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	CSE3502
COURSE NAME	INFORMATION SECURITY MANAGEMENT
SLOT	F1
FACULTY	Prof. I SUMAIYA THASEEN

Priyal Bhardwaj

Digitally signed by Priyal Bhardwaj
Date: 2021.03.31 23:23:45 +05'30'

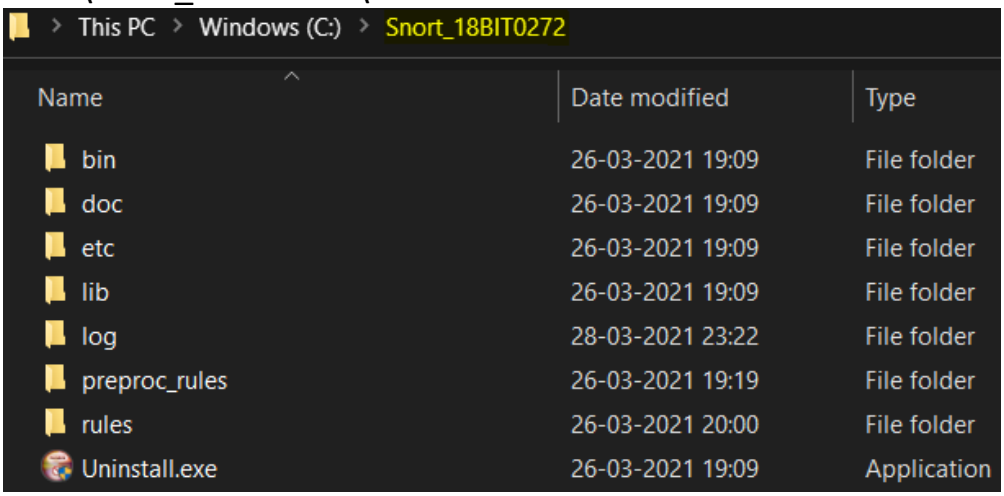
Any Open-Source IDS/IPS Installation and rule configuration: SNORT

1. Snapshot of your system IP address

```
C:\Users\PRIYAL BHARDWAJ>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::409:b1aa:4003:4def%16
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 13:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::20d7:3761:fb6a:3d8%9
   IPv4 Address. . . . . . . . . . . : 192.168.1.12
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

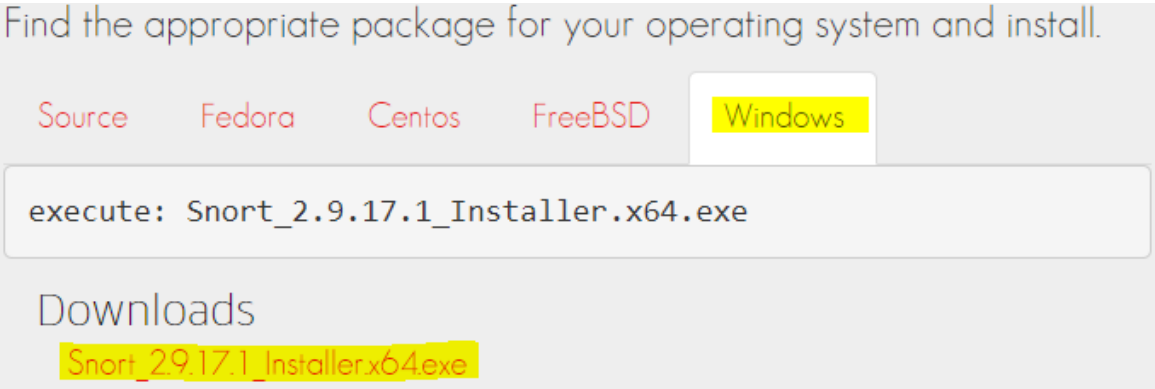
2. Installed open-source IDS/IPS location and steps for installation (Give your registration number in the location folder)

Location: C:\Snort_18BIT0272\



Snort Installation Steps: (Windows)

Step 1: Download and install setup file



Step 2: Download and install WinPcap.
I already had it installed for using Wireshark last semester.

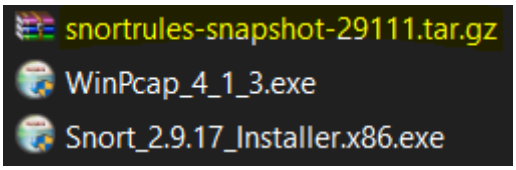
Step 3: Check directory structure of Snort.

```
C:\Snort_18BIT0272>dir
 Volume in drive C is Windows
 Volume Serial Number is 2E35-F7D8

 Directory of C:\Snort_18BIT0272

26-03-2021  19:09    <DIR>          .
26-03-2021  19:09    <DIR>          ..
26-03-2021  19:09    <DIR>          bin
26-03-2021  19:09    <DIR>          doc
31-03-2021  15:19    <DIR>          etc
26-03-2021  19:09    <DIR>          lib
31-03-2021  18:38    <DIR>          log
31-03-2021  15:33    <DIR>          preproc_rules
31-03-2021  15:35    <DIR>          rules
26-03-2021  19:09            50,108 Uninstall.exe
               1 File(s)         50,108 bytes
               9 Dir(s)   7,263,789,056 bytes free
```

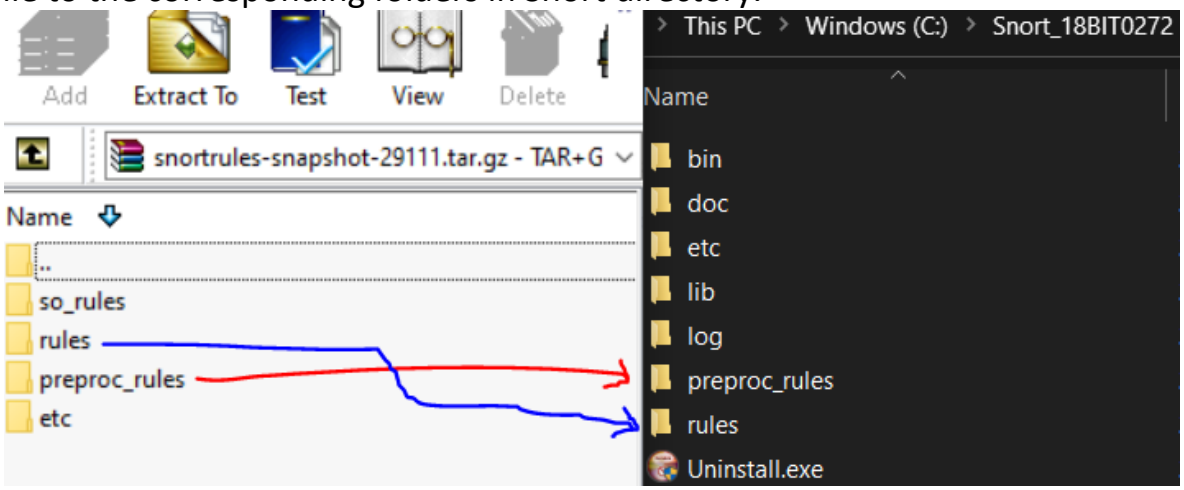
Step 4: Verify whether Snort installed correctly by checking the version.

```
C:\Snort_18BIT0272\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.17-WIN32 GRE (Build 199)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2020 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
```

Step 4: Download rules file (.tar.gz) after creating an account to get the Registered version.



Step 5: Extract files from “rules” and “preproc_rules” folders from the .tar.gz file to the corresponding folders in Snort directory.



Step 6: Make changes in C:\Snort_18BIT0272\etc\snort.conf file

- Set your IP address as HOME_NET (192.168.1.12).
- Use NOT operator(!) to set anything other than home network as external network.

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

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.12

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

Note: Since we are working in Windows we need to change the rule paths everywhere from / to \.

- Scroll down to RULE_PATH, and replace ../rules with C:\Snort_18BIT0272\rules and replace ../so_rules with C:\Snort_18BIT0272\so_rules. At last, replace ../preproc_rules with C:\Snort_18BIT0272\preproc_rules

```
104  var RULE_PATH C:\Snort_18BIT0272\rules
105  var SO_RULE_PATH C:\Snort_18BIT0272\rules
106  var PREPROC_RULE_PATH C:\Snort_18BIT0272\preproc_rules
```

- Change the WHITE_LIST_PATH and BLACK_LIST_PATH from ../rules to C:\Snort_18BIT0272\rules
- Navigate to C:\Snort_18BIT0272\rules and create two text files named **whitelist** and **blacklist** and change their file extension from **.txt** to **.rules.**

```
113  var WHITE_LIST_PATH C:\Snort_18BIT0272\rules
114  var BLACK_LIST_PATH C:\Snort_18BIT0272\rules
```

- Set #config logdir: to config logdir: C:\Snort_18BIT0272\log. This will help Snort write the output in a particular location.

```
187      config logdir: C:\Snort_18BIT0272\log
```

- At path to dynamic preprocessor libraries, replace usr/local/lib/snort_dynamicpreprocessor with your dynamic preprocessor, i.e. C:\Snort_18BIT0272\lib\snort_dynamicpreprocessor.
- Replace usr/local/lib/snort_dynamicengine/libsf_engine.so with base preprocessor engine, i.e. C:\Snort_18BIT0272\lib\snort_dynamicengine\sf_engine.dll.
- Comment (#) the dynamic rule libraries line, as we have already configured the libraries.

```
247  # path to dynamic preprocessor libraries
248  dynamicpreprocessor directory C:\Snort_18BIT0272\lib\snort_dynamicpreprocessor
249
250  # path to base preprocessor engine
251  dynamicengine C:\Snort_18BIT0272\lib\snort_dynamicengine\sf_engine.dll
252
253  # path to dynamic rules libraries
254  #dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

- Add a comment(#) before all the listed preprocessors under inline packet normalization. They do nothing but generate errors at the runtime.

```
266  #preprocessor normalize_ip4
267  #preprocessor normalize_tcp: ips ecn stream
268  #preprocessor normalize_icmp4
269  #preprocessor normalize_ip6
270  #preprocessor normalize_icmp6
```

- Give the location of the classification.config and replace it with C:\Snort_18BIT0272\etc\classification.config. Similarly, give location of reference.config & replace it with C:\Snort_18BIT0272\etc\reference.config.
- In the next line, add output alert_fast: alert.ids for snort to dump all logs in alert.ids

```
535  include C:\Snort_18BIT0272\etc\classification.config
536  include C:\Snort_18BIT0272\etc\reference.config
537  output alert_fast: alert.ids
```

- Remove the backslash and add comment characters # under preprocessor reputation.

```
508  #preprocessor reputation: \
509  #   memcap 500, \
510  #   priority whitelist, \
511  #   nested_ip inner, \
512  #   whitelist $WHITE_LIST_PATH\white_list.rules, \
513  #   blacklist $BLACK_LIST_PATH\black_list.rules
```

3. Any two rules configured and executed on distinct protocols like FTP, telnet, http (Give your registration number in the console/terminal prompt where you are executing the rules)

Write the rules in local.rules file and run the following command in terminal:
Snort -i 3 -c C:\Snort_18BIT0272\etc\snort.conf -A console

Rule 1: SSH Port connection
Before running Snort I connected to ssh port (22) from Windows Powershell
ssh abc@google.com

```
PS C:\Users\PRIYAL BHARDWAJ> ssh abc@google.com
ssh: connect to host google.com port 22: Connection timed out
```

alert tcp any any -> any 22 (msg: "SSH Connection detected"; GID:1; sid:100270; rev:1;)

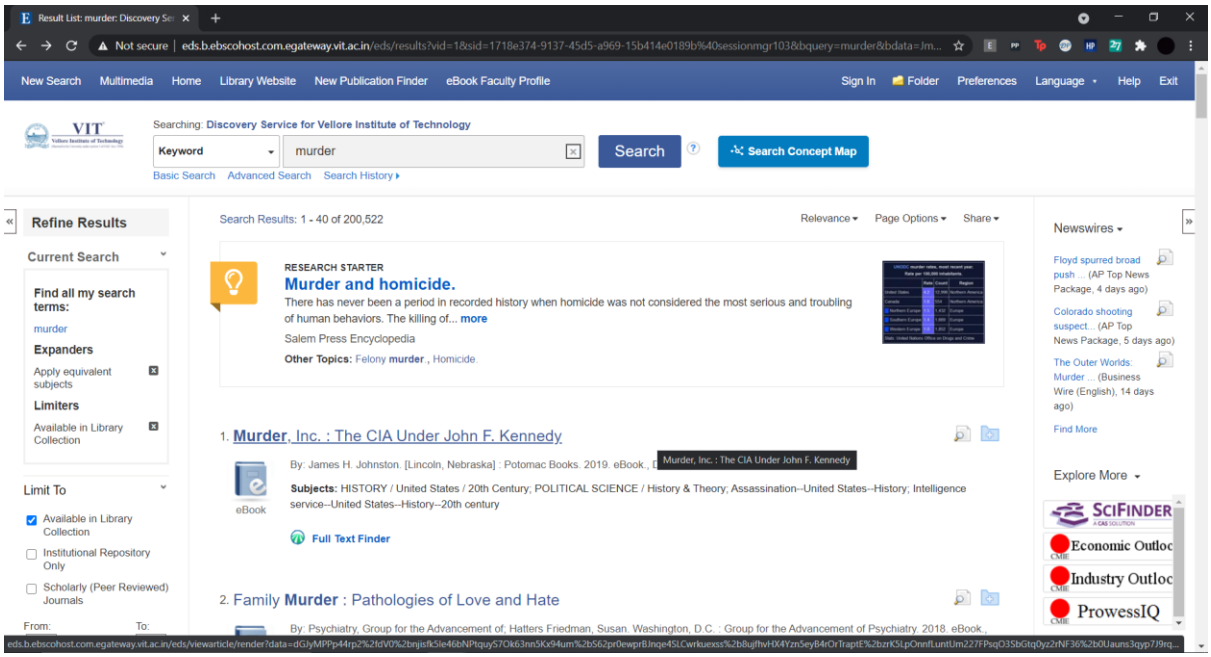
```
C:\Snort_18BIT0272\bin>snort -i3 -c C:\Snort_18BIT0272\etc\snort.conf -A console -q
03/31-22:59:03.319718  [**] [1:100270:1] SSH Connection detected [**] [Priority: 0] {TCP} 192.168.1.12:51157 -> 142.250.76.46:22
03/31-22:59:04.325897  [**] [1:100270:1] SSH Connection detected [**] [Priority: 0] {TCP} 192.168.1.12:51157 -> 142.250.76.46:22
03/31-22:59:06.326983  [**] [1:100270:1] SSH Connection detected [**] [Priority: 0] {TCP} 192.168.1.12:51157 -> 142.250.76.46:22
03/31-22:59:10.336651  [**] [1:100270:1] SSH Connection detected [**] [Priority: 0] {TCP} 192.168.1.12:51157 -> 142.250.76.46:22
03/31-22:59:18.345437  [**] [1:100270:1] SSH Connection detected [**] [Priority: 0] {TCP} 192.168.1.12:51157 -> 142.250.76.46:22
```

Rule 2: HTTP
When the word in content is searched on an http site snort gives the alert msg written in the rule.

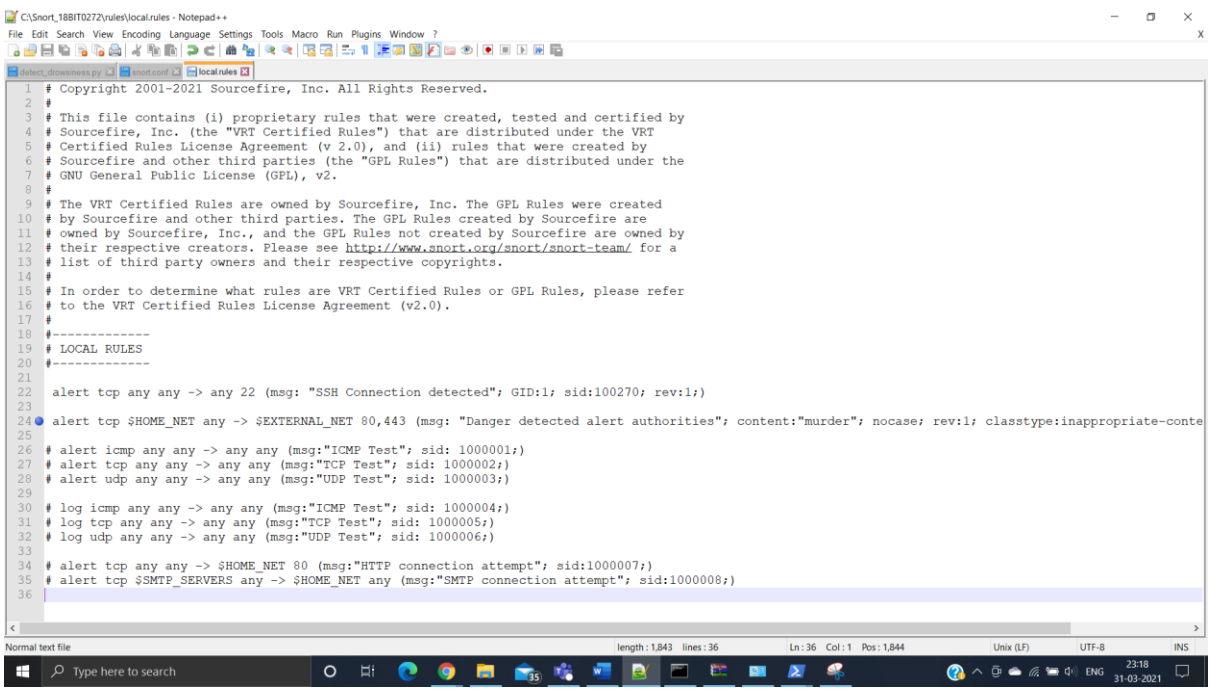
alert tcp $HOME_NET any -> $EXTERNAL_NET 80,443 (msg: "Danger detected alert authorities"; content:"murder"; nocase; classtype:inappropriate-content; sid:100272; rev:1;)

```
C:\Snort_18BIT0272\bin>snort -i3 -c C:\Snort_18BIT0272\etc\snort.conf -A console -q
03/31-23:12:21.716141  [**] [1:100272:1] Danger detected alert authorities [**] [Classification: Inappropriate Content was Detected] [Priority: 1] {TCP} 192.168.1.12:51235 -> 35.154.217.189:80
03/31-23:12:21.716221  [**] [1:100272:1] Danger detected alert authorities [**] [Classification: Inappropriate Content was Detected] [Priority: 1] {TCP} 192.168.1.12:51235 -> 35.154.217.189:80
03/31-23:12:21.716141  [**] [119:19:2] (http_inspect) LONG HEADER [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.12:51235 -> 35.154.217.189:80
03/31-23:12:23.845921  [**] [119:19:2] (http_inspect) LONG HEADER [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.12:51244 -> 35.154.217.189:80
03/31-23:12:26.326278  [**] [119:19:2] (http_inspect) LONG HEADER [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.12:51246 -> 35.154.217.189:80
03/31-23:12:26.328044  [**] [119:19:2] (http_inspect) LONG HEADER [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.12:51245 -> 35.154.217.189:80
03/31-23:12:27.551077  [**] [119:19:2] (http_inspect) LONG HEADER [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.12:51247 -> 35.154.217.189:80
```

I searched “murder” on a http site (not secure): vit.egateway after running the Snort command.



local.rules file:



Rule Header:

alert – part of rule actions, generates an alert using the selected alert method, and then log the packet.

tcp – protocol
any – Range of source port numbers
$HOME_NET – Home IP address
$EXTERNAL_NET – Range of source IP addresses
msg - message to print along with a packet dump or to an alert
content - option pattern match is performed
sid - uniquely identify Snort rules
rev - uniquely identify revisions of Snort rules
classtype - categorize a rule as detecting an attack that is part of a more general type of attack class.