SECURITY LAB EXPERIMENT 12

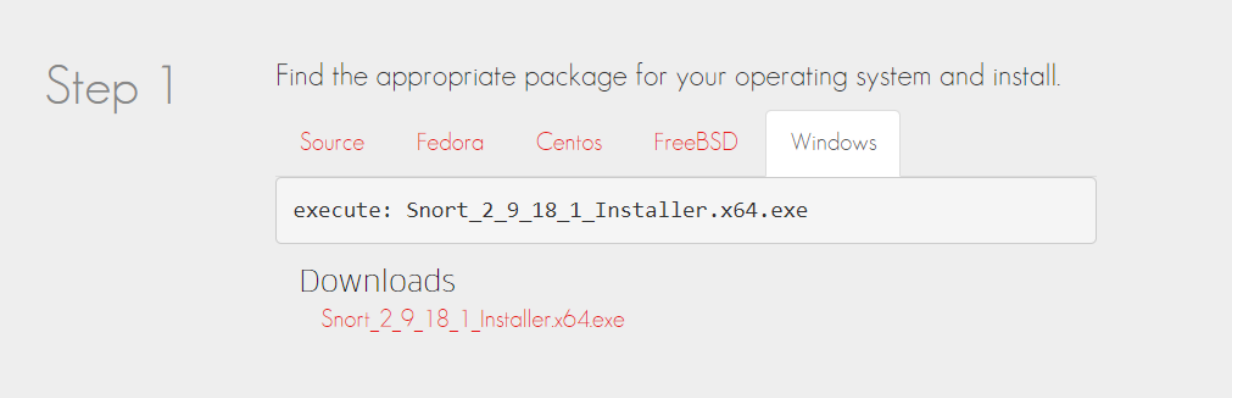
Name: Venkatesh Reddy Roll no:59 Class: D15A

Aim: Set up Snort and study the logs.

Snort is an open source and popular Intrusion Detection System (IDS). It works by actively monitoring network traffic parsing each packet and alerting system administrators of any anomalous behavior that goes against the snort rules configured by the administrator according to the security policies of an organization.

Let's begin with retrieving files from www.snort.org. There are two things we want to download: the Snort installer package and the rules files.

1. Get the latest version of Snort by browsing to https://www.snort.org/downloads and clicking on the link for the Windows installer.



2. Get the latest version of the rules by browsing to https://www.snort.org/downloads/#rule-downloads and clicking on the link for the current Registered User release.

Note that you must create an account (which is free) and log in to Snort.org in order to download the "*registered*" rules file or purchase an annual subscription to download the "subscriber" rules file. The "*community*" version of the rules is free and requires no user registration, but if you choose to use the community rules there are changes you must make to the snort.conf configuration file because the rules referenced in the configuration reflects the structure of the registered or subscriber rulesets.

3. Get the WinPcap installer by browsing to http://www.winpcap.org/install/default.htm and clicking on the link for the Version 4.1.3 installer for windows.

Now install the programs (in the case of WinPcap and Snort) and extract the rules files in the case of the Snort rules package). It is recommended that WinPcap is installed before Snort, but it is not required. At the end of the Snort installation process the program will prompt you to install WinPcap, whether or not the utility is already installed. If you have installed any other programs that rely on packet capture, such as Wireshark, then you will already have WinPcap installed and you can skip the first step below.

1. Double-click the WinPcap_4_1_3.exe installer file and follow the on-screen prompts. Typically no customization or configuration is required for this install, although on many systems a restart may be required to make sure the WinPcap netgroup packet filter (NPF) driver is running.

2. Double-click the Snort_2_9_18_1_Installer.exe file and follow the on-screen prompts.

    a. Accept the license agreement
    b. Choose the components (Snort, dynamic modules, documentation) you want to install. All are selected by default. Documentation is not strictly required for our purposes if space is at a premium (the space required to install is reduced by about 50% if documentation is unchecked).
    c. By default the installer creates a root directory for Snort at **c:\Snort**, although you can specify a different directory if desired. When you select "Next" the installation executes.
    d. At the end of the installation, the program displays a message that Snort has successfully been installed. The message includes a note that WinPcap is required (it refers to 4.1.1 although 4.1.3 is the current version), recommends tightening security on Snort, and directs you to edit the snort.conf file.

3. Open the Snort rules package. Depending on your operating system, Windows may be able to open the zipped archive automatically, or you can use a utility such as WinZip, 7Zip, or WinRAR to open it.

    a. Create a subfolder under **c:\Snort** called rules, and another called preproc_rules.
    b. Extract the contents of the rules folder in the archive to **c:\Snort rules**
    c. Extract the contents of the preproc_rules folder in the archive to **c:\Snort preproc_rules**
    d. Ignore the so_rules folder, while Sourcefire offers pre-compiled versions of the shared object rules for many Linux distributions, no such option exists for Windows. Compiling the Snort shared object rules to run on Windows is well beyond the technical scope of this course.
    e. Also ignore the contents of the etc folder in the archive.

Once you have completed installing these components, you can check to see if the program responds:

1. Change to the Snort program directory: **c:\>cd \Snort\bin**

```
D:\>cd Snort/bin

D:\Snort\bin>
```

2. Check the installed version for Snort: **c:\Snort\bin/snort -V**

```
D:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18.1-WIN64 GRE (Build 1005)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 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: 1.2.11
```

3. The - V option (it must be a capital V) simply returns the current installed version of the program. If Snort is installed on the system, you should see something similar to the screenshot below (which shows an installed version 2.9.18.1).

4. You should also check to see what network adapters are on your system, so you can tell Snort to listen on the appropriate interface when it runs. To see a list of interfaces, run the command:
   c:\Snort\bin/snort -W

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

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18.1-WIN64 GRE (Build 1005)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 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: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{2BC5C009-077C-4D97-A17C-20DC06F7084F}      WAN Miniport (Ne
twork Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{2468659C-3724-4D1D-8F68-B1E7C774660E}      WAN Miniport (IP
v6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{80AB6D61-E83D-446C-B0D7-A44F8A9748FA}      WAN Miniport (IP
)
    4   84:1B:77:2C:7C:20       0000:0000:fe80:0000:0000:0000:e8ad:3972 \Device\NPF_{6AD613EC-41F6-4240-BC02-FB88DD532CB
0}      Intel(R) Wi-Fi 6 AX200 160MHz
    5   86:1B:77:2C:7C:20       0000:0000:fe80:0000:0000:0000:e888:50ea \Device\NPF_{A3CCD546-43C6-496D-BD0B-7A325A744A7
6}      Microsoft Wi-Fi Direct Virtual Adapter #2
    6   84:1B:77:2C:7C:21       0000:0000:fe80:0000:0000:0000:009b:a7d0 \Device\NPF_{8F92B97F-C33C-4936-A5B7-3D0480E8750
5}      Microsoft Wi-Fi Direct Virtual Adapter
    7   0A:00:27:00:00:14       0000:0000:fe80:0000:0000:0000:e5eb:217b \Device\NPF_{FD2C9D2B-894F-4C82-81CF-A9BA20956AB
1}      VirtualBox Host-Only Ethernet Adapter
    8   00:00:00:00:00:00       disabled        \Device\NPF_Loopback    Adapter for loopback traffic capture
    9   00:FF:D6:BA:10:47       0000:0000:fe80:0000:0000:0000:20d7:2c3c \Device\NPF_{D6BA1047-AAB8-4A1D-A306-4D356F50451
5}      TAP-Windows Adapter V9
   10   00:FF:2A:4F:3D:D5       0000:0000:fe80:0000:0000:0000:dc62:67a5 \Device\NPF_{2A4F3DD5-B4CD-4FFA-94D0-0AB37156B81
3}      ExpressVPN TAP Adapter
   11   6C:02:E0:76:FF:DC       0000:0000:fe80:0000:0000:0000:6021:3e84 \Device\NPF_{11814494-ED98-48B0-9E30-BF9B79ECDCC
B}      Realtek Gaming GbE Family Controller
```

The next thing to do is to edit the snort.conf file to make it reflect the environment where your computer is running (see Configuring Snort with snort.conf). You should make sure that when you edit the file, you are working on the one in **c:\Snort\etc** (and not any other versions that may exist in temporary or download directories).

Now open the snort.conf file through the notepad++ editor or any other text editor to edit configurations of snort to make it work like we want it to.

1. Setup the network addresses you are protecting
   Note: Mention your own host IP addresses that you want to protect.

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.56.1/24
```

2. Setup the external network into anything that is not the home network. That is why ! is used in the command it denotes 'not'.

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

3. Now we have to define the directory for our rules and preproc rules folder

```
# 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 d:\Snort\rules
# var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH d:\Snort\preproc_rules
```

4. Now we have to set up our white list and black list path. It will be in our snorts' rule folder. Comment out the var WHITE_LIST_PATH ../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 d:\Snort\rules
```

5. Next we have to enable the log directory, so that we store logs in our log folder. Uncomment this line.

```
# Configure default log directory for snort to log to.  For more information see snort -h command line options (-l)
#
config logdir: d:\Snort\log
```

6. Now we will set the path to dynamic preprocessors and dynamic engine. Comment out the dynamic detection path.

```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory d:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine d:\Snort\lib\snort_dynamicengine\sf_engine.dll

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

7. Just comment out these lines. In doing so we are excluding packet normalization of different packets.

```
# 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
```

8. Scroll down to the reputation preprocessors. We will just change the name of the black list file and comment out the white list name path.

```
# Reputation preprocessor. For more information see README.reputation
preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   # whitelist $WHITE_LIST_PATH\white_list.rules, \
   blacklist $BLACK_LIST_PATH/blacklist.rules
```

9. Convert the backslashes to forward slashes in lines 546–651.

```
# site specific rules
include $RULE_PATH\local.rules

include $RULE_PATH\app-detect.rules
include $RULE_PATH\attack-responses.rules
include $RULE_PATH\backdoor.rules
include $RULE_PATH\bad-traffic.rules
include $RULE_PATH\blacklist.rules
include $RULE_PATH\botnet-cnc.rules
include $RULE_PATH\browser-chrome.rules
include $RULE_PATH\browser-firefox.rules
include $RULE_PATH\browser-ie.rules
include $RULE_PATH\browser-other.rules
include $RULE_PATH\browser-plugins.rules
include $RULE_PATH\browser-webkit.rules
include $RULE_PATH\chat.rules
include $RULE_PATH\content-replace.rules
include $RULE_PATH\ddos.rules
include $RULE_PATH\dns.rules
include $RULE_PATH\dos.rules
include $RULE_PATH\experimental.rules
include $RULE_PATH\exploit-kit.rules
include $RULE_PATH\exploit.rules
include $RULE_PATH\file-executable.rules
include $RULE_PATH\file-flash.rules
include $RULE_PATH\file-identify.rules
include $RULE_PATH\file-image.rules
include $RULE_PATH\file-multimedia.rules
include $RULE_PATH\file-office.rules
include $RULE_PATH\file-other.rules
include $RULE_PATH\file-pdf.rules
```

10. Again just convert forward slashes to backslashes and uncomment the lines below.

```
# decoder and preprocessor event rules
include $PREPROC_RULE_PATH\preprocessor.rules
include $PREPROC_RULE_PATH\decoder.rules
include $PREPROC_RULE_PATH\sensitive-data.rules
```

11. Now we just need to verify the presence of this command at the bottom of the snort.conf file.

```
# Event thresholding or suppression commands. See threshold.conf
include threshold.conf
```

12. Click on Save file and save all changes to save the configuration file (snort.conf).

Now we test snort again by running Command prompt as admin. To check if it's running fine after all the configurations.

```
D:\Snort\bin>snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18.1-WIN64 GRE (Build 1005)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 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: 1.2.11
```

We can also check the wireless interface cards from which we will be using snort by using the command below. We can see the list of our wireless interface cards through entering this command in the command prompt.

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

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18.1-WIN64 GRE (Build 1005)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 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: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{2BC5C009-077C-4D97-A17C-20DC06F7084F}      WAN Miniport (Ne
twork Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{2468659C-3724-4D1D-8F68-B1E7C774660E}      WAN Miniport (IP
v6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{80AB6D61-E83D-446C-B0D7-A44F8A9748FA}      WAN Miniport (IP
)
    4   84:1B:77:2C:7C:20       0000:0000:fe80:0000:0000:0000:e8ad:3972 \Device\NPF_{6AD613EC-41F6-4240-BC02-FB88DD532CB
0}      Intel(R) Wi-Fi 6 AX200 160MHz
    5   86:1B:77:2C:7C:20       0000:0000:fe80:0000:0000:0000:e888:50ea \Device\NPF_{A3CCD546-43C6-496D-BD0B-7A325A744A7
6}      Microsoft Wi-Fi Direct Virtual Adapter #2
    6   84:1B:77:2C:7C:21       0000:0000:fe80:0000:0000:0000:009b:a7d0 \Device\NPF_{8F92B97F-C33C-4936-A5B7-3D0480E8750
5}      Microsoft Wi-Fi Direct Virtual Adapter
    7   0A:00:27:00:00:14       0000:0000:fe80:0000:0000:0000:e5eb:217b \Device\NPF_{FD2C9D2B-894F-4C82-81CF-A9BA20956AB
1}      VirtualBox Host-Only Ethernet Adapter
    8   00:00:00:00:00:00       disabled        \Device\NPF_Loopback    Adapter for loopback traffic capture
    9   00:FF:D6:BA:10:47       0000:0000:fe80:0000:0000:0000:20d7:2c3c \Device\NPF_{D6BA1047-AAB8-4A1D-A306-4D356F50451
5}      TAP-Windows Adapter V9
   10   00:FF:2A:4F:3D:D5       0000:0000:fe80:0000:0000:0000:dc62:67a5 \Device\NPF_{2A4F3DD5-B4CD-4FFA-94D0-0AB37156B81
3}      ExpressVPN TAP Adapter
   11   6C:02:E0:76:FF:DC       0000:0000:fe80:0000:0000:0000:6021:3e84 \Device\NPF_{11814494-ED98-48B0-9E30-BF9B79ECDCC
B}      Realtek Gaming GbE Family Controller
```

Now we will enter a command to check validation of snort's configuration by choosing a specific wireless interface card (4) the rest of the command shows the config file path . The command is

```
D:\Snort\bin>snort -i 4 -c d:\Snort\etc\snort.conf -T
Running in Test mode
```

```
        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18.1-WIN64 GRE (Build 1005)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 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: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <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>

Total snort Fixed Memory Cost - MaxRss:975057680
Snort successfully validated the configuration!
Snort exiting
```

If you load these rules by starting Snort with the -A console option, you can see the output on the screen as it happens. Note that the startup command shown below uses an interface 4, which is often the correct choice, but many systems have multiple network interfaces so it is a good idea to determine which one you want Snort to monitor by running the command snort -W to see the available interfaces.

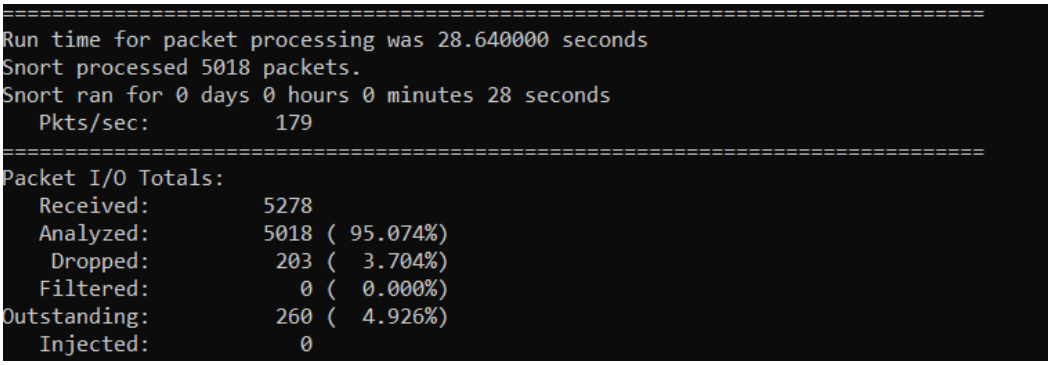
```
D:\Snort\bin>snort -i 4 -c d:\Snort\etc\snort.conf -A console
```

```
Acquiring network traffic from "\Device\NPF_{6AD613EC-41F6-4240-BC02-FB88DD532CB0}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18.1-WIN64 GRE (Build 1005)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 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: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <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>
Commencing packet processing (pid=764)
10/18-20:36:00.147449  [**] [1:1000003:1] Testing TCP alert [**] [Priority: 0] {TCP} 162.159.133.234:443 -> 192.168.29.1
44:1050
10/18-20:36:00.189047  [**] [1:1000003:1] Testing TCP alert [**] [Priority: 0] {TCP} 162.159.133.234:443 -> 192.168.29.1
44:1050
10/18-20:36:00.220147  [**] [1:1000003:1] Testing TCP alert [**] [Priority: 0] {TCP} 13.89.179.12:443 -> 192.168.29.144:
```



It can be seen in the given figure that Snort successfully validates our configuration. This brings us to the end of our installation and configuration tutorial.

Conclusion: Hence, we understood how to set up the Snort and study the logs.