Don Bosco Institute of Technology, Mumbai 400070

Department of Information Technology

ITL502

Name:-Erica Bastyav DSouza Roll no.: 14 Subject :- Security Lab

Experiment No. : 12

Date: 20/09/2022

Title : SNORT and studying the logs.

Problem Definition : Study network security by installing an IDS, SNORT and study the logs.

Pre-requisite : IDS

Theory :

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.[1] IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content. SNORT Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in 1998. Snort is now developed by Sourcefire, of which Roesch is the founder and CTO. In 2009, Snort entered InfoWorld's Open Source Hall of Fame as one of the "greatest [pieces of] open source software of all time". Snort's open source network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching, and content matching. These basic services have many purposes including application-aware triggered quality of service, to de-prioritize bulk traffic when latency-sensitive applications are in use. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection.
In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

Packet capture library for windows :-

Npcap is the Nmap Project's packet capture (and sending) library for Microsoft Windows. It implements the open Pcap API using a custom Windows kernel driver alongside our Windows build of the excellent libpcap library. This allows Windows software to capture raw network traffic (including wireless networks, wired ethernet, localhost traffic, and many VPNs) using a simple, portable API. Npcap allows for sending raw packets as well. Mac and Linux systems already include the Pcap API, so Npcap allows popular software such as Nmap and Wireshark to run on all these platforms (and more) with a single codebase. Npcap began in 2013 as some improvements to the (now discontinued) WinPcap library, but has been largely rewritten since then with hundreds of releases improving Npcap's speed, portability, security, and efficiency.

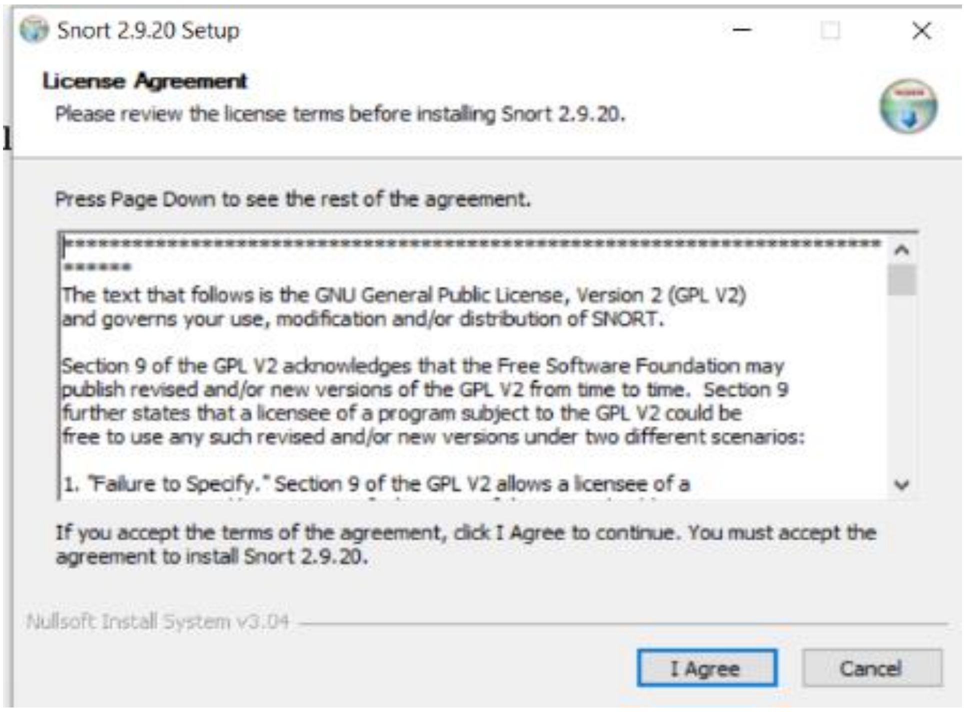
Procedure/ Algorithm :

Snort Installation:

- For Windows 10 64 bit supported SNORT's executable file can be downloaded from **here**.

- 2. Open the downloaded snort executable file.

- 3. Click On 'I Agree' on the license agreement



Snort 2.9.20 Setup

License Agreement

Please review the license terms before installing Snort 2.9.20.

Press Page Down to see the rest of the agreement.

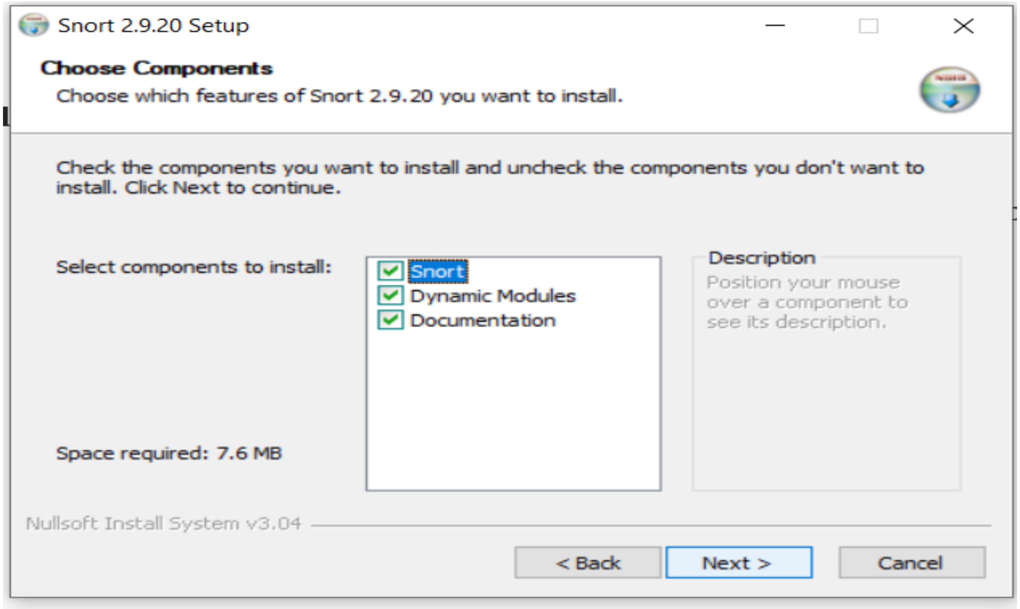
```
*****************************************************************************
******
The text that follows is the GNU General Public License, Version 2 (GPL V2)
and governs your use, modification and/or distribution of SNORT.

Section 9 of the GPL V2 acknowledges that the Free Software Foundation may
publish revised and/or new versions of the GPL V2 from time to time.  Section 9
further states that a licensee of a program subject to the GPL V2 could be
free to use any such revised and/or new versions under two different scenarios:

1. "Failure to Specify." Section 9 of the GPL V2 allows a licensee of a
```

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Snort 2.9.20.

4. Choose components of Snort to be installed.



Choose Components

Choose which features of Snort 2.9.20 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

☑ Snort
☑ Dynamic Modules
☑ Documentation

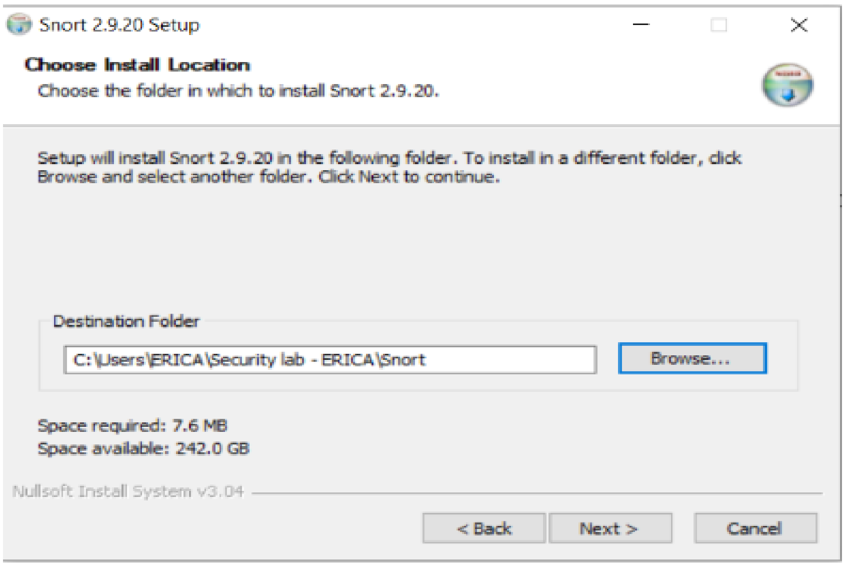
Description

Position your mouse over a component to see its description.

Space required: 7.6 MB

Nullsoft Install System v3.04

5. Click “Next” and then choose install location for snort preferably a separate folder in Windows C Drive.



Choose Install Location

Choose the folder in which to install Snort 2.9.20.

Setup will install Snort 2.9.20 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

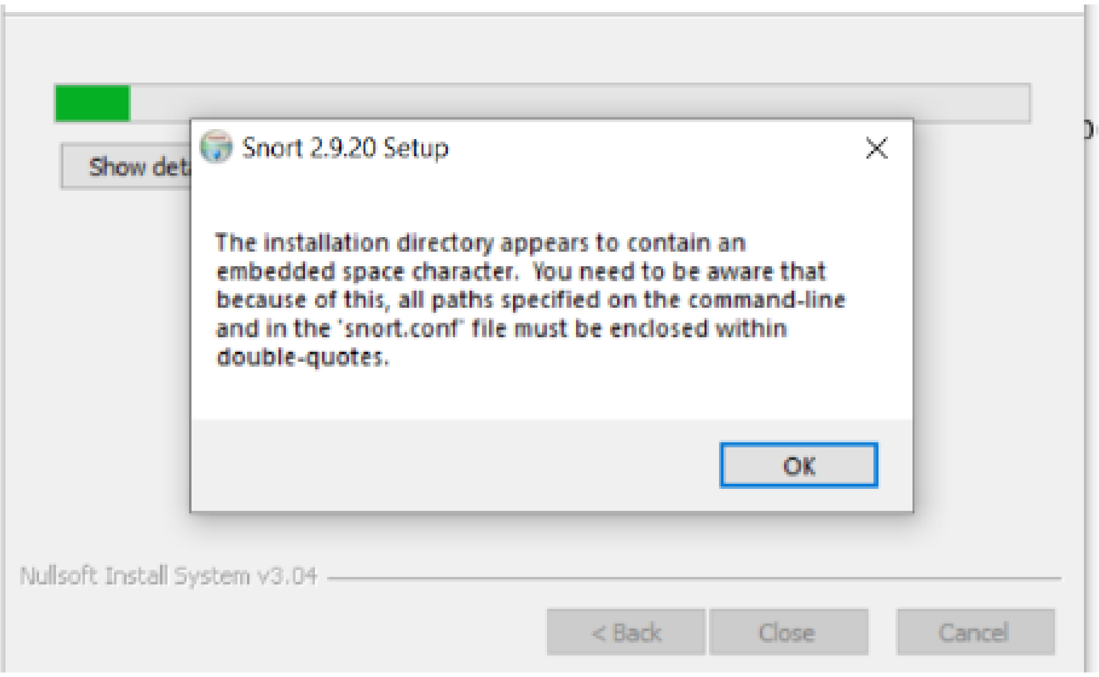
Destination Folder

C:\Users\ERICA\Security lab - ERICA\Snort

Space required: 7.6 MB
Space available: 242.0 GB

Nullsoft Install System v3.04

6. Click “Next” Installation process starts and then it completes as shown in figure 04:



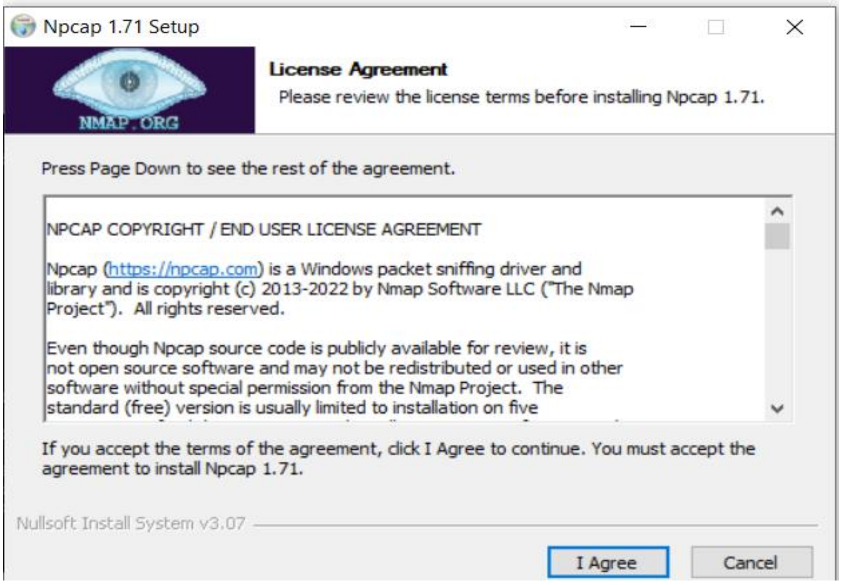
Snort 2.9.20 Setup

The installation directory appears to contain an embedded space character. You need to be aware that because of this, all paths specified on the command-line and in the 'snort.conf' file must be enclosed within double-quotes.

7. When you click " Close" you are prompted with this dialogue box.

8. Installing Npcap is required by snort for proper functioning.

9. Npcap for Windows 10 can be downloaded from **here**.



Npcap 1.71 Setup

License Agreement

Please review the license terms before installing Npcap 1.71.

Press Page Down to see the rest of the agreement.

NPCAP COPYRIGHT / END USER LICENSE AGREEMENT

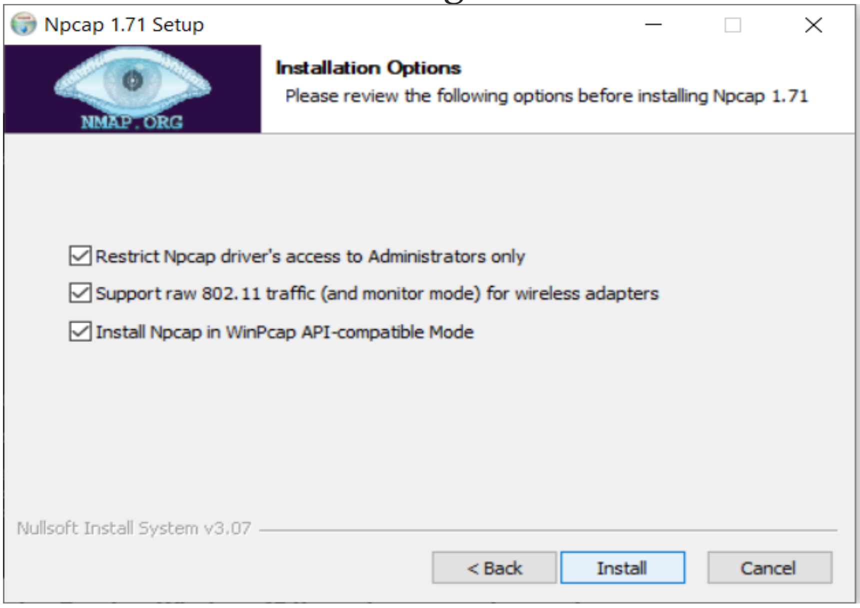
Npcap (https://npcap.com) is a Windows packet sniffing driver and library and is copyright (c) 2013-2022 by Nmap Software LLC ("The Nmap Project"). All rights reserved.

Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed or used in other software without special permission from the Nmap Project. The standard (free) version is usually limited to installation on five

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 1.71.

10. Opening Npcap setup file, Click on ‘I Agree’ To license agreement.

11. Now we proceed to choose which components of Npcap are to be installed and then clicking on “Install”.



Npcap 1.71 Setup

Installation Options

Please review the following options before installing Npcap 1.71

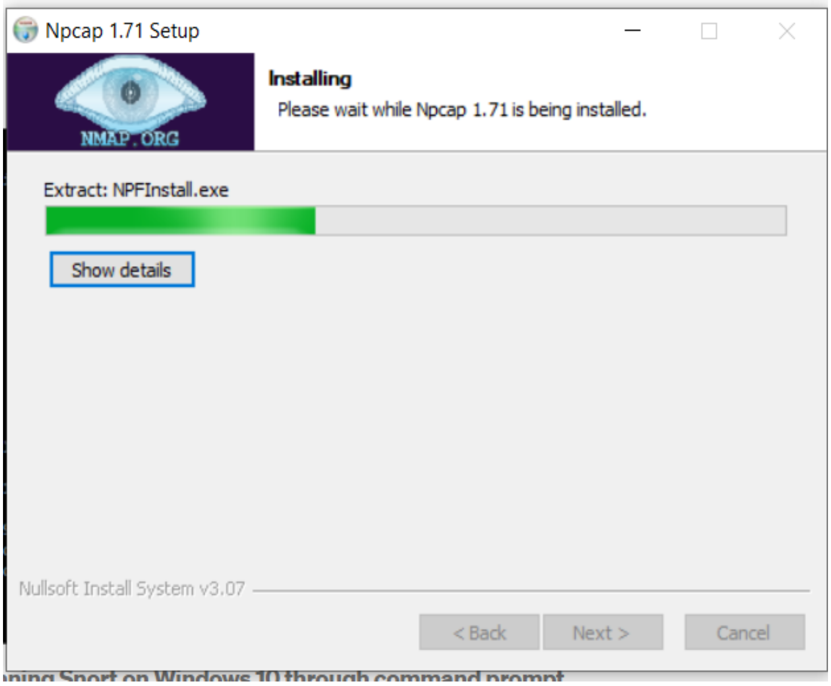
☑ Restrict Npcap driver's access to Administrators only

☑ Support raw 802.11 traffic (and monitor mode) for wireless adapters

☑ Install Npcap in WinPcap API-compatible Mode

Nullsoft Install System v3.07

13. Now the window for installation of Npcap shows it has been installed. Clicking “Finish”.



Npcap 1.71 Setup

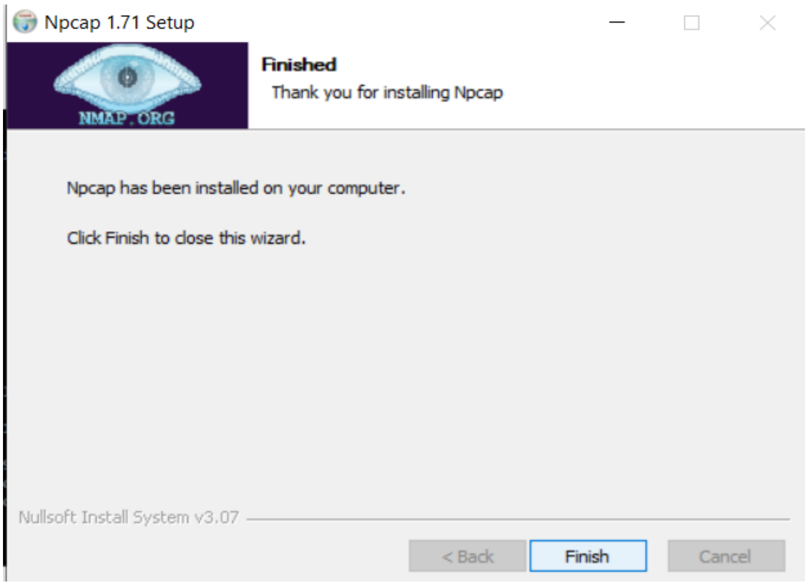
Installing

Please wait while Npcap 1.71 is being installed.

Extract: NPFInstall.exe

Nullsoft Install System v3.07

ning Snort on Windows 10 through command prompt



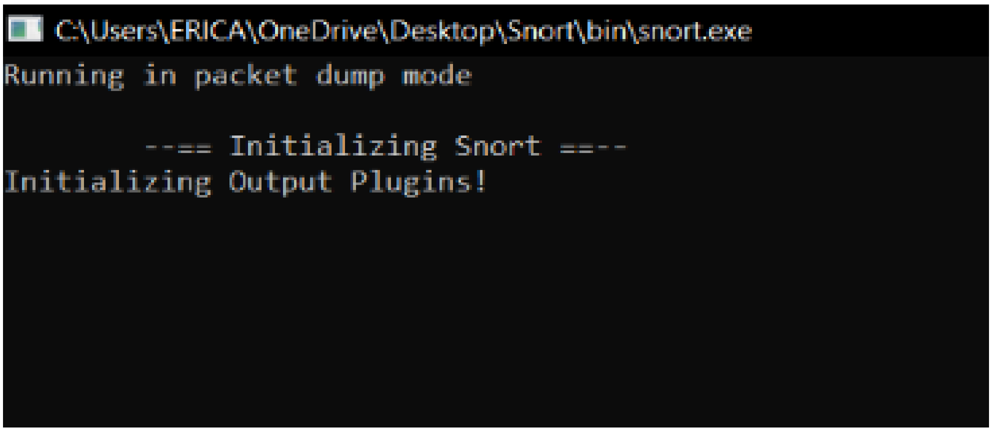
Finished

Thank you for installing Npcap

Npcap has been installed on your computer.

Click Finish to close this wizard.

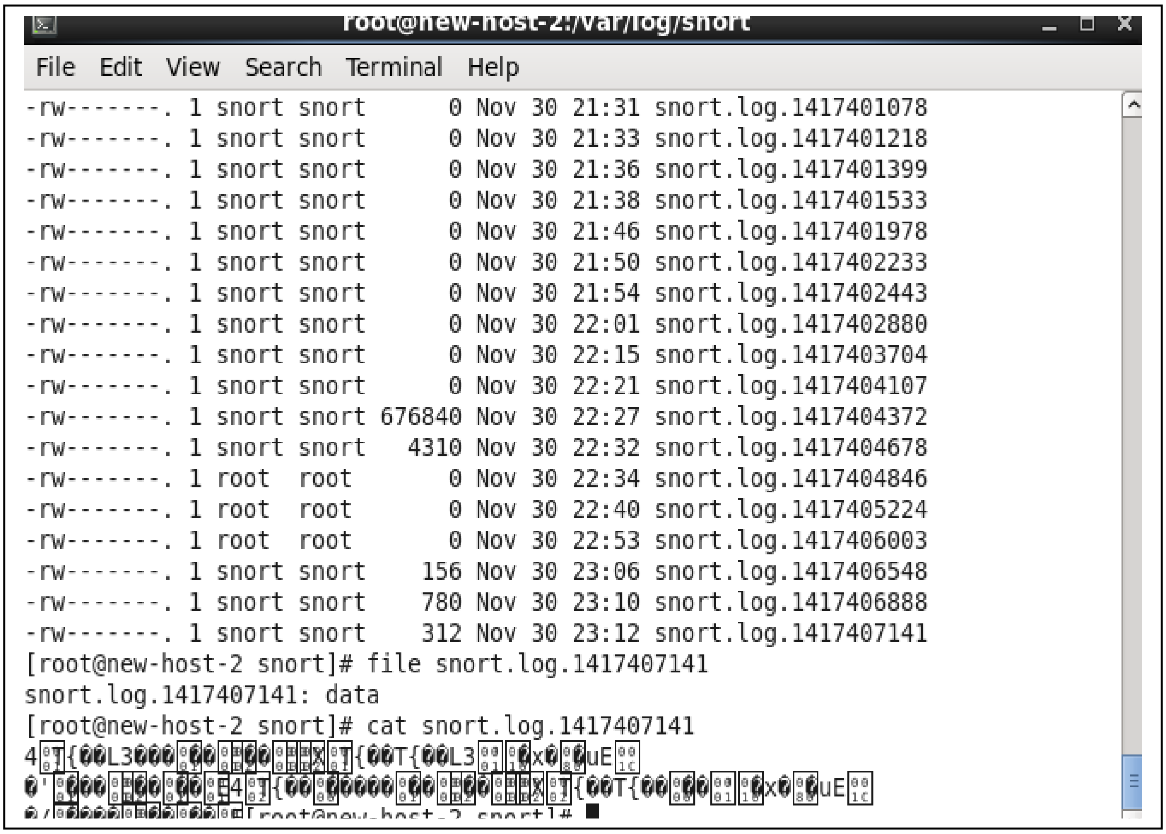
Results :



```
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
```

Study of snort logs


root@new-host-2:/var/log/snort
File Edit View Search Terminal Help

```
-rw-------. 1 snort snort      0 Nov 30 21:31 snort.log.1417401078
-rw-------. 1 snort snort      0 Nov 30 21:33 snort.log.1417401218
-rw-------. 1 snort snort      0 Nov 30 21:36 snort.log.1417401399
-rw-------. 1 snort snort      0 Nov 30 21:38 snort.log.1417401533
-rw-------. 1 snort snort      0 Nov 30 21:46 snort.log.1417401978
-rw-------. 1 snort snort      0 Nov 30 21:50 snort.log.1417402233
-rw-------. 1 snort snort      0 Nov 30 21:54 snort.log.1417402443
-rw-------. 1 snort snort      0 Nov 30 22:01 snort.log.1417402880
-rw-------. 1 snort snort      0 Nov 30 22:15 snort.log.1417403704
-rw-------. 1 snort snort      0 Nov 30 22:21 snort.log.1417404107
-rw-------. 1 snort snort 676840 Nov 30 22:27 snort.log.1417404372
-rw-------. 1 snort snort   4310 Nov 30 22:32 snort.log.1417404678
-rw-------. 1 root  root       0 Nov 30 22:34 snort.log.1417404846
-rw-------. 1 root  root       0 Nov 30 22:40 snort.log.1417405224
-rw-------. 1 root  root       0 Nov 30 22:53 snort.log.1417406003
-rw-------. 1 snort snort    156 Nov 30 23:06 snort.log.1417406548
-rw-------. 1 snort snort    780 Nov 30 23:10 snort.log.1417406888
-rw-------. 1 snort snort    312 Nov 30 23:12 snort.log.1417407141
[root@new-host-2 snort]# file snort.log.1417407141
snort.log.1417407141: data
[root@new-host-2 snort]# cat snort.log.1417407141
4□T{��L3���□��□□��□□□X□T{��T{��L3□□�x�□�uE□
�'□���□□��□��□□4□T{��□�����□��□□��□□□X□T{��T{��□��□□�x�□�uE□
�/□����□□��□��□[root@new-host-2 snort]# █
```

Snortlog.txt
Study of logfile

- investigate a suspicious program and user account.
- Monitor the command line traffic on the suspicious machine.
- Review the commands used to install an unauthorized program.

References

http://en.wikipedia.org/wiki/Snort_(software)
http://www.informit.com/articles/article.aspx?p=101171&seqNum=2
https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detectionsystem-ids
https://www.techopedia.com/definition/3988/intrusion-detection-system-ids https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799
http://searchmidmarketsecurity.techtarget.com/definition/Snort
Npcap: Windows Packet Capture Library & Driver