

**University of Missouri-Kansas City**

**Information Security and Assurance**

**Key Loggers with Snort**

Under the guidance of Mahesh Maddumala

**By**

**Priyadarsini Nidadavolu**

**Tejkumar Yentrapragada**

**Contents**

[Introduction 3](#_Toc477830265)

[Snort 3](#_Toc477830266)

[Introduction: 3](#_Toc477830267)

[Features: 3](#_Toc477830268)

[Snort Architecture: 4](#_Toc477830269)

[Architecture of Snort: 4](#_Toc477830270)

[Key Loggers 5](#_Toc477830271)

[Introduction: 5](#_Toc477830272)

[Main Objective: 5](#_Toc477830273)

[Types 5](#_Toc477830274)

[Types of keyloggers: 5](#_Toc477830275)

[Software based: 5](#_Toc477830276)

[Hardware based : 6](#_Toc477830277)

[Kernel/Driver Key loggers : 6](#_Toc477830278)

[Detection: 6](#_Toc477830279)

[Prevention Methods: 6](#_Toc477830280)

[Flow Diagram 7](#_Toc477830281)

[Project Setup 8](#_Toc477830282)

[Requirements: 8](#_Toc477830283)

[Snort Installation: 8](#_Toc477830284)

[Snort rule 11](#_Toc477830285)

[Output screens 12](#_Toc477830286)

[How to run KeyLoggers: 12](#_Toc477830287)

[Storing the Logged keys in to a File: 12](#_Toc477830288)

[Text that is logged into log1.txt file 13](#_Toc477830289)

[Sending Log1.txt through SMTP mail: 13](#_Toc477830290)

[Snort Rule: 14](#_Toc477830291)

[Snort Execution: 14](#_Toc477830292)

[Running Snort: 15](#_Toc477830293)

[Generated Log files: 15](#_Toc477830294)

[Alert.ids file : 16](#_Toc477830295)

[References 16](#_Toc477830296)

# **Introduction**

Currently our world is enhancing with many new technologies to make the user tasks much easier. However, with these enrichments, it is not very easy to provide security in every corner as the user aims to get faster operations being performed. To achieve the fastness, developers neglect the security to some extent, which gives hackers an advantage.

Hackers are the one who gain access to our personal information without our prior knowledge. To avoid these, we need to have minimum security measures, so that we can detect the Worms, Trojans, Viruses etc. Snort is one of the tool that is used to detect the attacks made to gain access to our system. In this project, we aim to develop an application that stores the keystrokes on a system and logs them and send them to the attacker. The attack will be defended using Snort as another part.

# **Snort**

**Introduction:**

An open source tool developed by Sourcefire used to find network intrusion prevention system. By using Snort, we can defend the attack made by the attacker by defining our own rules. This tool is used to detect attach irrespective of the operating system and interfaces.

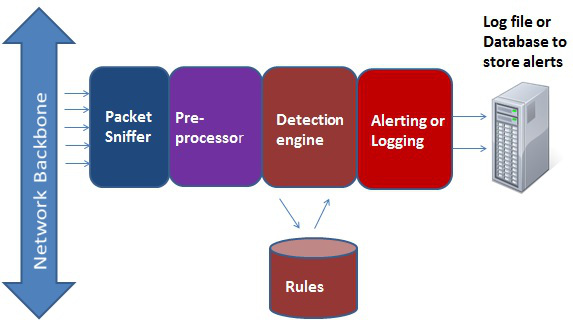
**Features:**

The following are the features of Snort:

* Real-time traffic analysis
* Packet logging
* Protocol analysis
* Content search
* Content match

**Snort Architecture:**

Architecture of Snort:



1. **Packet sniffer**: It collects or sniffs the network traffic and layer information. Then the collected packets are send to Preprocessors.
2. **The preprocessors**: It performs certain actions to determine the kind of behavior that snort is dealing. We use lot of plugins. After completing its job, it sends the information to the detection engine.
3. **The detection engine**: It performs the comparisons of each packets with the rules from the ruleset and if the rule matches with the packet then it is forwarded to the output.
4. **Alerting or Logging:** This will log and/or trigger alerts based on the rule action specified in the rule.

# **Key Loggers**

**Introduction:**

A system program that stores and records every keystroke typed on the user system and logs it. It may send the stored confidential information to the hackers. This may be done without permission or knowledge of the user.

**Main Objective**:

Business purpose: It is a tool used by employers to ensure that there employs use work systems only for work purpose.

Family purpose: Tool used by Head of the family to monitor the activities of the family members and restrict them to specific sites.

**Types**

Types of keyloggers:

* Software based
* Hardware based
* Kernel/driver key loggers.

### Software based:

These types of key loggers are software key loggers used on computer software in an organization to detect technical problems with systems, but Malicious users use key loggers on public machines to get confidential information of the user. Here are several categories:

* Hypervisor based : This type of key logger resides in a hypervisor malware which runs beneath the operating system.
  + Ex : Blue Pill
* Java Script based : A script program is deployed into the webpage and make it to listen for the key strokes
  + Ex : Cross Site Scripting , man in the browser.
* Memory injection based : These type of key loggers operates on the memory tables associated with the browsers.
  + Ex : Zeus and Spy Eye use these methods.
* Form grabbing based : These key loggers logs the data before the data is passed to through the internet when user completes the form and submits it.

### Hardware based :

It doesn’t need any software, but instead of software the job is done by hardware connected to the system.

* Key Board Hardware: In this type a hardware is attached to the system some ware in between system and key board. This may be done by installing the device into the system so that user cannot know that there is a hardware connected to the system.
* Key Board Overlays: These are mostly used in ATM’s where hacker needs the PIN information of the user. These are designed such that they look like as if they are part of the ATM . Every key is registered by the criminals keyboard and keyboard of the ATM.
* Wireless Keyboard and Mouse Sniffers : These capture the information when it is transferred from the wireless keyboard to the receiver.

### Kernel/Driver Key loggers :

These receives data directly from the input device and these are present at the kernel level. These are very difficult to detect as the user need to have root permissions.

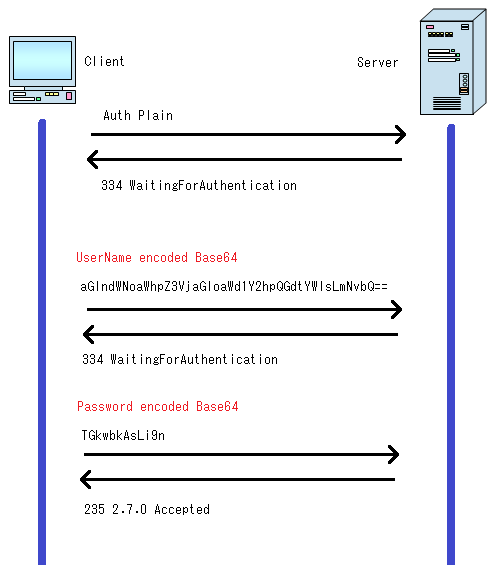
**Detection:**

Make sure that the operating system is fully patched with known vulnerabilities. The best way to prevent this is to educate the users not to install unnecessary software unless needed. Microsoft AntiSpyWare, Ad-Aware are some of the tools used to detect and remove the spywares.

**Prevention Methods:**

As we know that the key loggers are used to store the typed information from the keyboard either by hardware or by software. One way to avoid key stroke capture in web applications is to use of virtual keyboards rather than regular key boards. As by using these virtual key boards the keystrokes cannot be stored as if the keys are clicked instead of typed. As these is not 100% secure as some key loggers are designed in such a way that they stores the captured screenshots as for every mouse clicks.

# **Flow Diagram**





# **Project Setup**

## **Requirements:**

**Operating System:** Ubuntu

**Snort Version:** 2.9.9.0

**Ram:** 2 Gb (min)

## **Snort Installation:**

Before installing snort, we need to check the following

* sudo apt-get install build-essential -y
* sudo apt-get install libpcap-dev libpcre3-dev libdumbnet-dev -y
* mkdir ~/snort\_src
* cd ~/snort\_src/
* sudo apt-get install bison flex -y
* wget <https://www.snort.org/downloads/snort/daq-2.9.9.0.tar.gz>
* tar -zxvf daq-2.0.6.tar.gz
* cd daq-2.0.6/
* ./configure
* make
* sudo make install
* sudo apt-get install zlib1g-dev liblzma-dev openssl libssl-dev -y

**Install snort with below commands**

* cd ~/snort\_src
* wget <https://www.snort.org/downloads/snort/snort-2.9.8.2.tar.gz>
* tar -zxvf snort-2.9.8.2.tar.gz
* cd snort-2.9.8.2
* ./configure --enable-sourcefire
* make
* sudo make install

**Update shared libraries:**

* sudo ldconfig
* sudo ln -s /usr/local/bin/snort /usr/sbin/snort
* snort -V

**Snort Configuration steps:**

* sudo groupadd snort
* sudo useradd snort -r -s /sbin/nologin -c SNORT\_IDS -g snort
* sudo mkdir -p /etc/snort/rules/iplists
* sudo mkdir /etc/snort/preproc\_rules
* sudo mkdir /usr/local/lib/snort\_dynamicrules
* sudo mkdir /etc/snort/so\_rules
* sudo mkdir -p /var/log/snort/archived\_logs
* sudo touch /etc/snort/rules/iplists/black\_list.rules
* sudo touch /etc/snort/rules/iplists/white\_list.rules
* sudo touch /etc/snort/rules/local.rules
* sudo touch /etc/snort/sid-msg.map
* sudo chmod -R 5775 /etc/snort
* sudo chmod -R 5775 /var/log/snort
* sudo chmod -R 5775 /usr/local/lib/snort\_dynamicrules
* sudo chown -R snort:snort /etc/snort
* sudo chown -R snort:snort /var/log/snort
* sudo chown -R snort:snort /usr/local/lib/snort\_dynamicrules
* cd ~/snort\_src/snort-2.9.8.2/etc/
* sudo cp \*.conf\* /etc/snort
* sudo cp \*.map /etc/snort
* sudo cp \*.dtd /etc/snort
* cd ~/snort\_src/snort-2.9.8.2/src/dynamic-preprocessors/build/usr/local/lib/snort\_dynamicpreprocessor/
* sudo cp \* /usr/local/lib/snort\_dynamicpreprocessor/
* sudo sed -i "s/include \$RULE\\_PATH/#include \$RULE\\_PATH/" /etc/snort/snort.conf
* sudo gedit /etc/snort/snort.conf
* Change ‘ipvar HOME\_NET any’ to ipvar HOME\_NET 192.168.65.101
* Configure below parameters to :
  + var RULE\_PATH /etc/snort/rules
  + var SO\_RULE\_PATH /etc/snort/so\_rules
  + var PREPROC\_RULE\_PATH /etc/snort/preproc\_rules
  + var WHITE\_LIST\_PATH /etc/snort/rules/iplists
  + var BLACK\_LIST\_PATH /etc/snort/rules/iplists
* Un comment line ‘include $RULE\_PATH/local.rules’
* Test configuration with below command:
  + sudo snort -T -i ens160 -c /etc/snort/snort.conf
* Edit the local.rules file created under /etc/snort/rules/local.rules using the command:
  + Sudo gedit /etc/snort/rules/local.rules

**Additional Modifications for snort Configuration file to get the log files:**

In Step 2 : Config logdir:/var/log/snort.

In Step 6 : Configure the output pluging.

Output unified2:filename merged.log,limit 128,nostamp,npls\_types,vlan\_events\_types.

Output alert\_unified2:filename snort.alert,limit 128.

Output alert\_syslog:LOG\_ALERT.

Output alert\_fast:alert.

Output log\_tcpdump:tcpdump.log

# **Snort rule**

|  |
| --- |
| Alert tcp any any -> any 25 (msg:”KeyLogger Alert”;content:”smtp.gmail.com0”; [fast\_pattern:only;nocase;classtype:attempted-](mailto:Dunti.210@gmail.com%3e)recon;sid:1287;) |

**Description:**

**Alert** - It is an action. It generates an alert using the alert method and then log the packet.

**Tcp** - protocol that we use.

**Ip**: Then we have source ip followed by source port .Here we use any.

**direction**: -> gives the direction that it is coming from source and going to destination.

Followed by destination ip(any) and destination port(25 for checking outgoing mail server)

**content**: It allows the user to set rules that searchs for specific content in the packet payload.

**nocase:** I t allows the rule writer to specify that the snort should look for specific pattern, ignoring case.

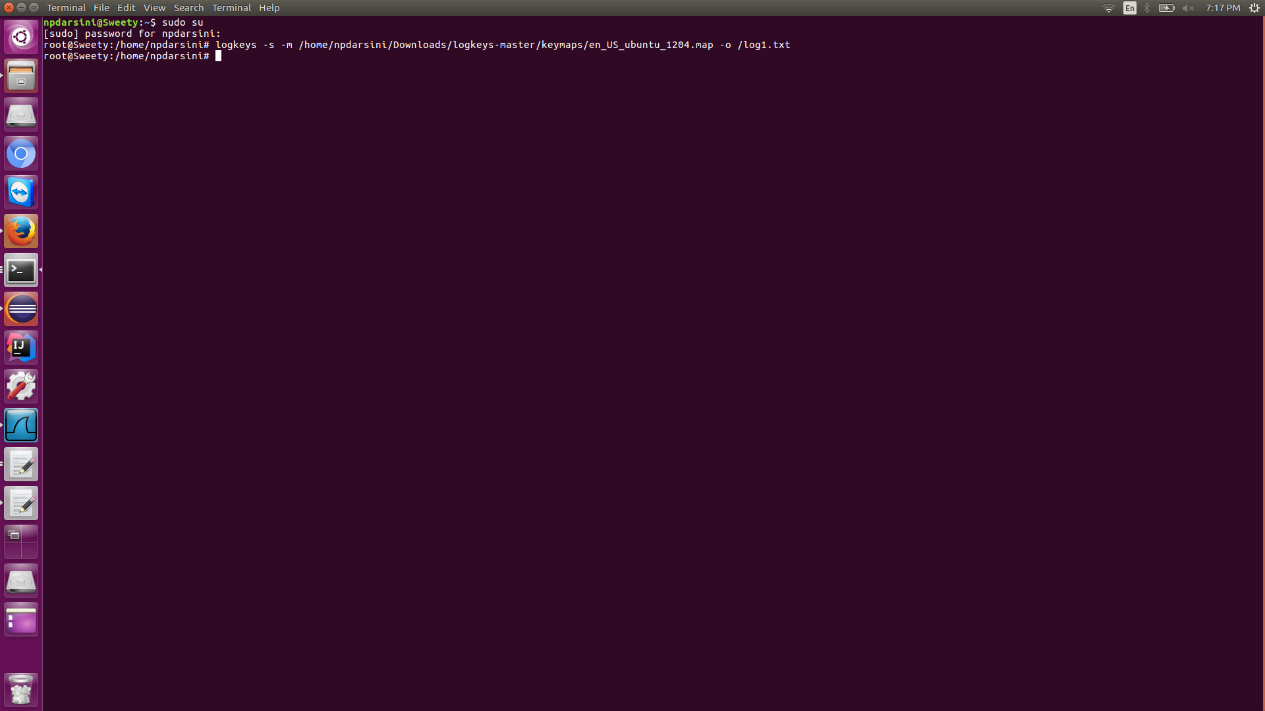
**Fast\_Pattern**: It is a content modifier that sets the content within a rule to be used with fast\_pattern matcher,by using this ,it select only those rules that have a chance of matching by using content in the rule for selection & only evaluating that rule if the content is found in payload. It reduces the number of rules that need to be evaluated and increases performance.

**Classtype:** A keyword that is used to categorize a rule as detecting an attack that is part of more general type of attack class.

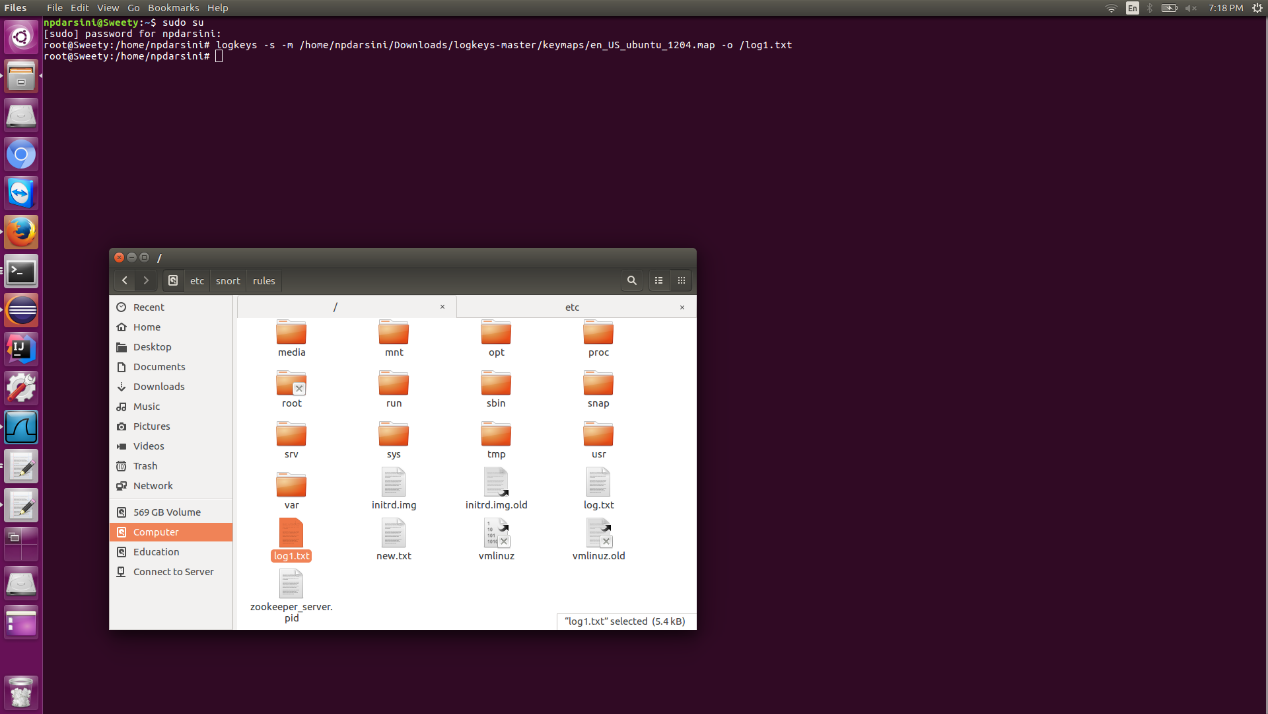
Ex : attempted-recon which deals with attempted info leak.

# **Output screens**

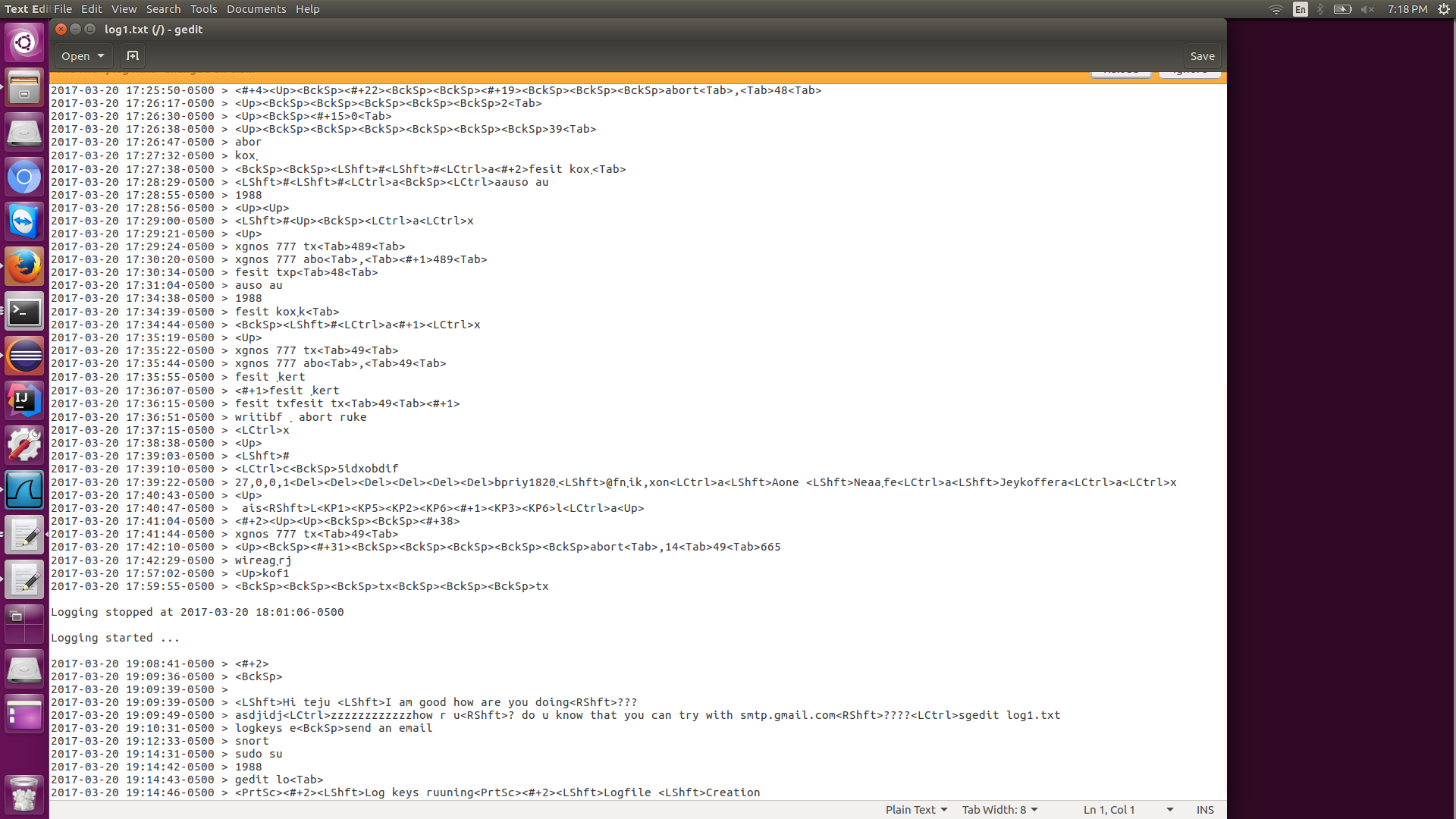
## **How to run KeyLoggers:**



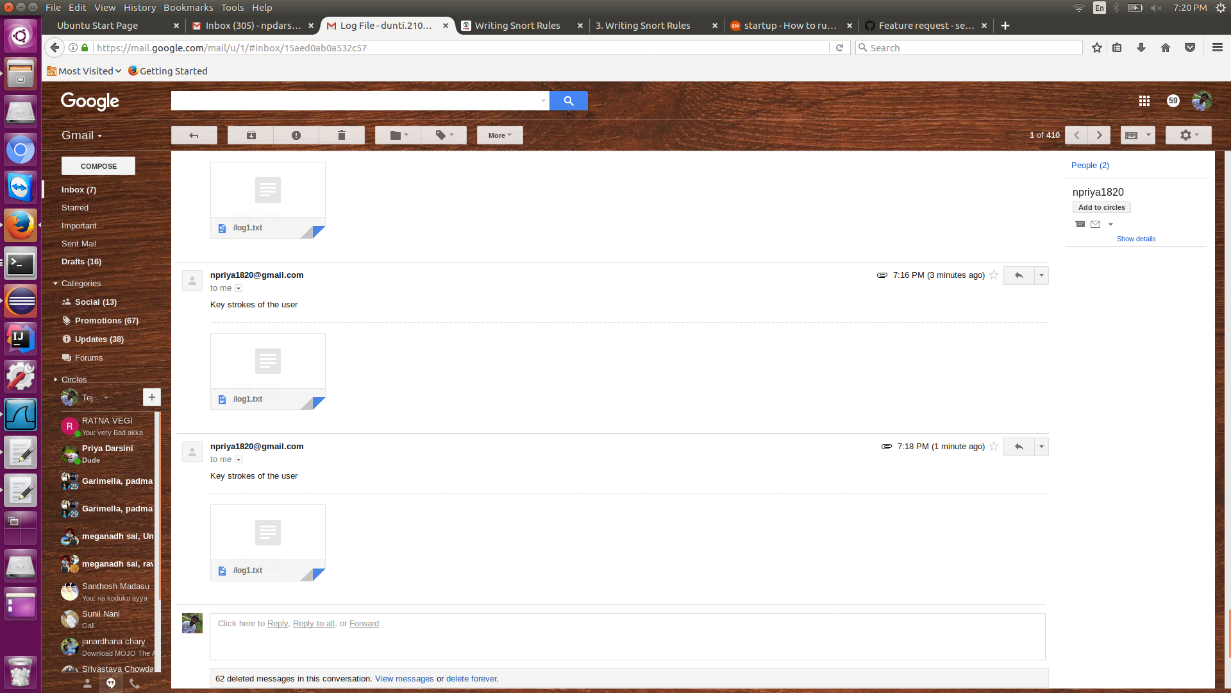
## **Storing the Logged keys in to a File:**



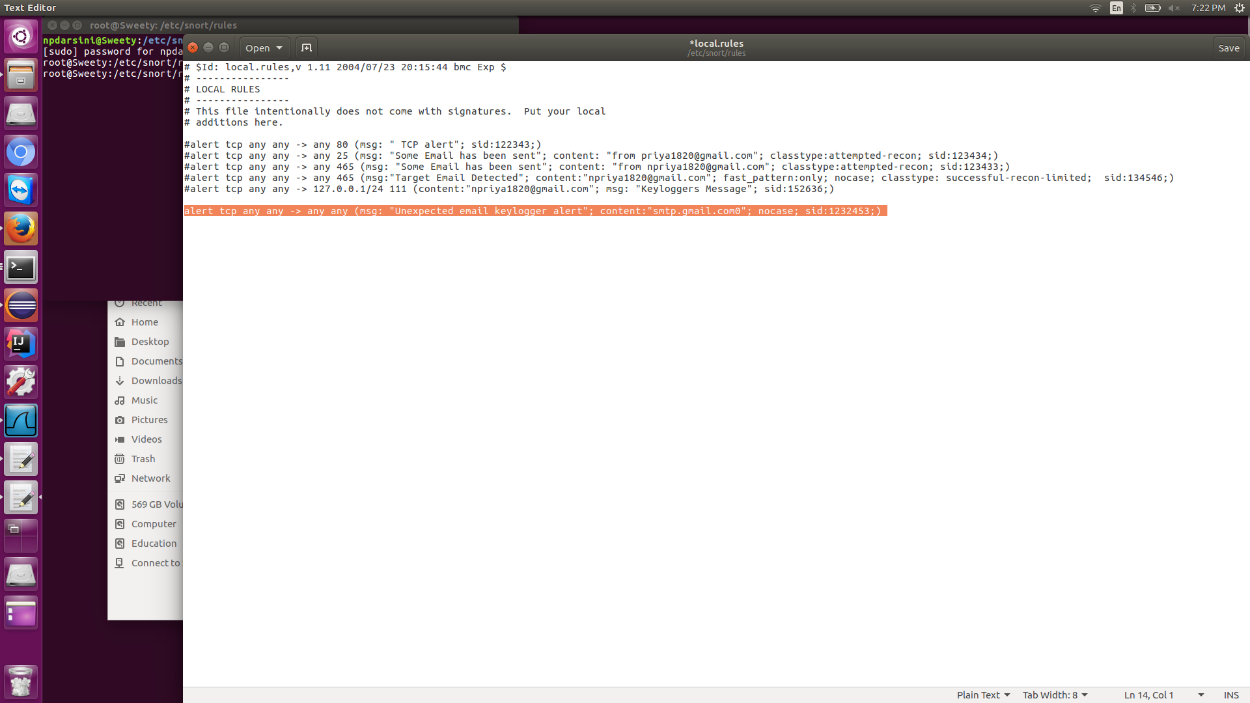
## **Text that is logged into log1.txt file**



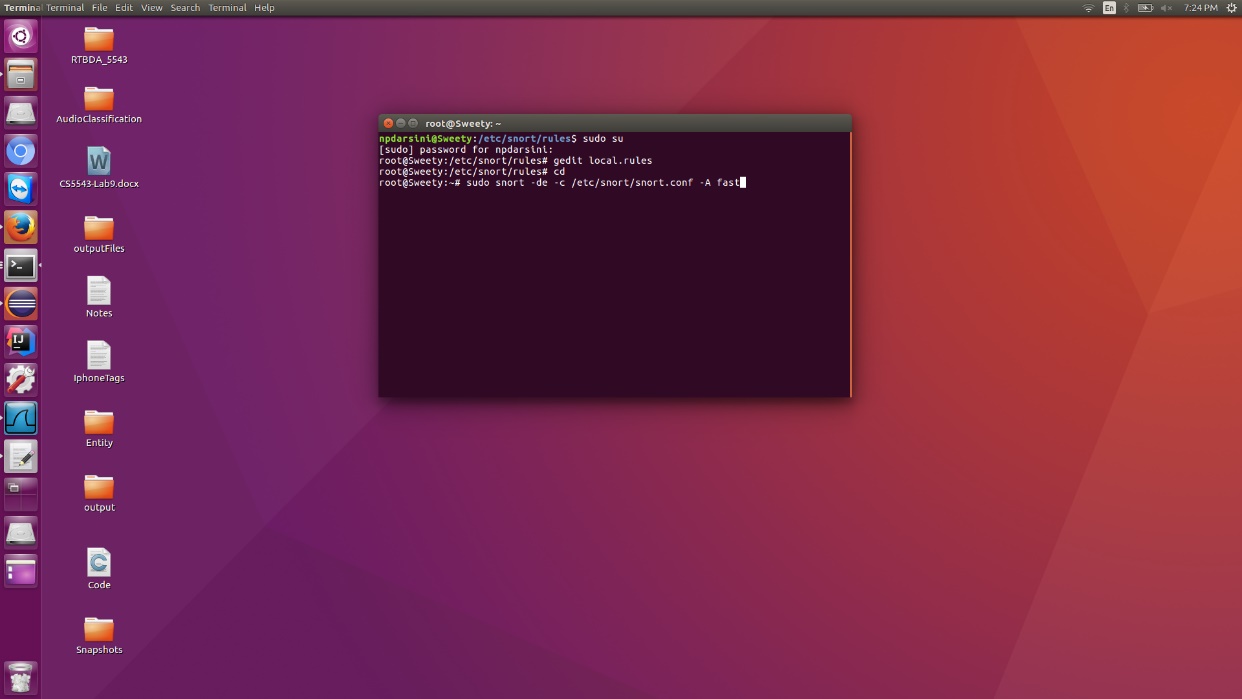
## **Sending Log1.txt through SMTP mail:**



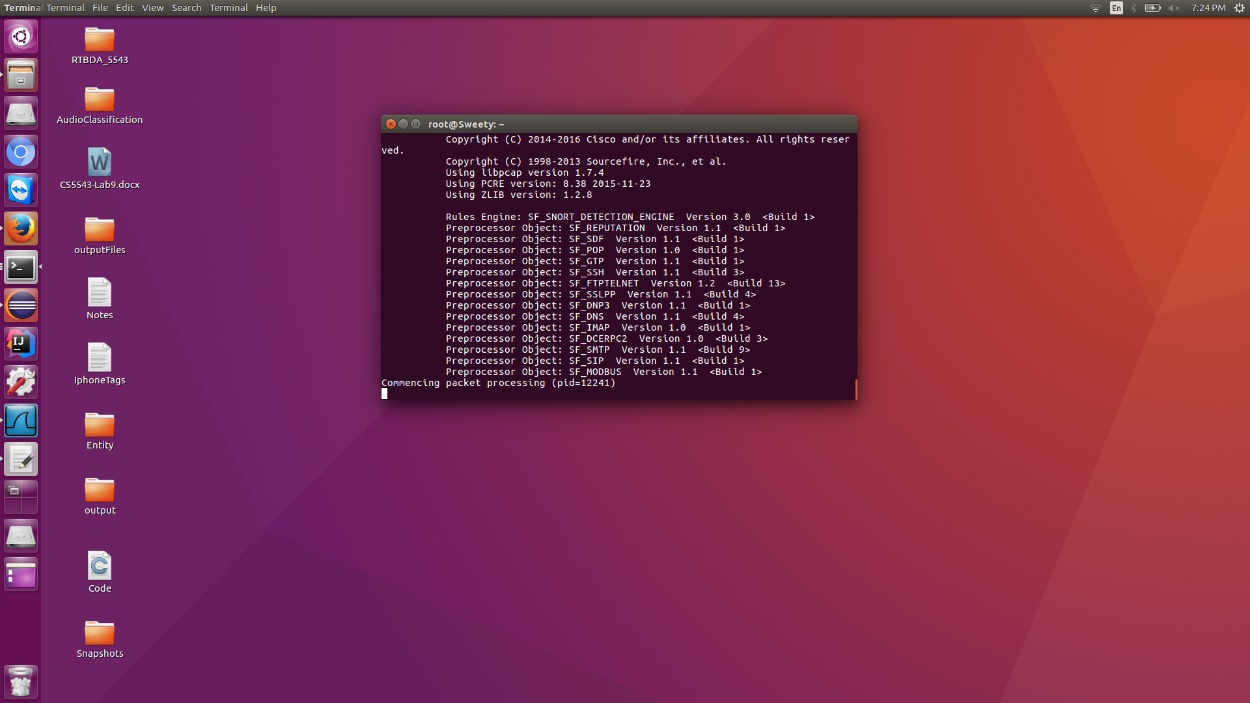
## **Snort Rule:**



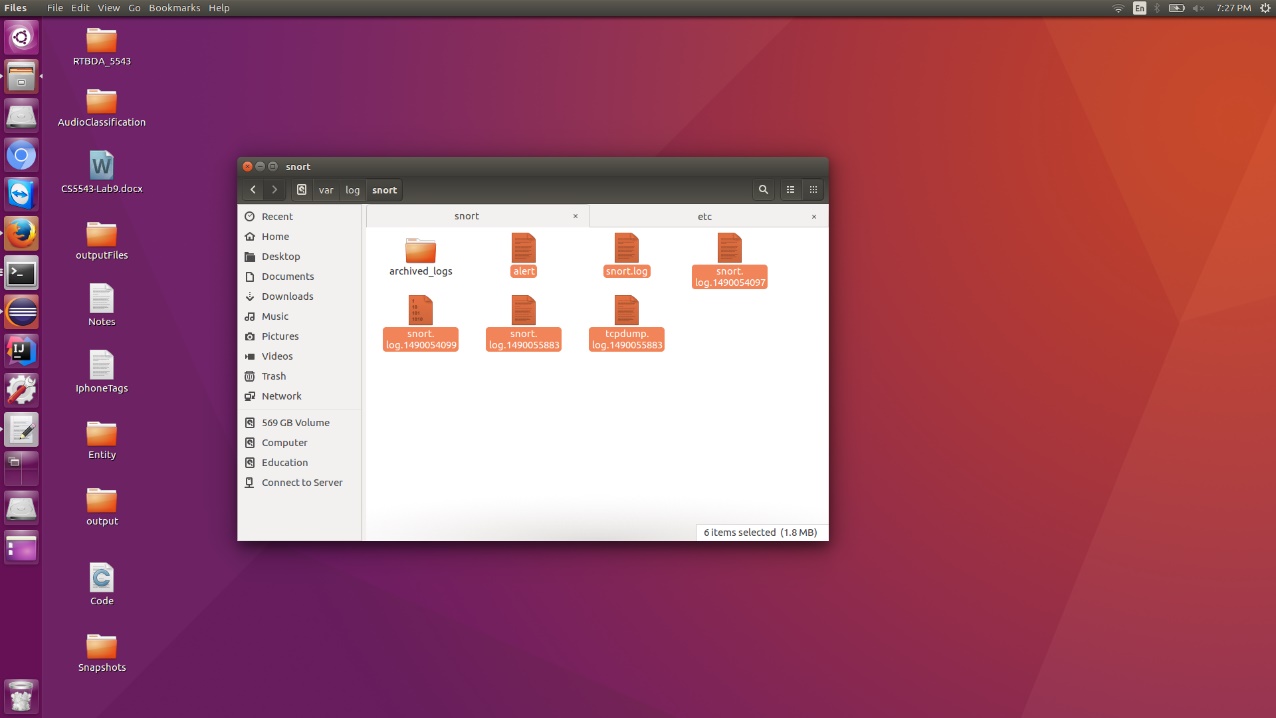
## **Snort Execution:**



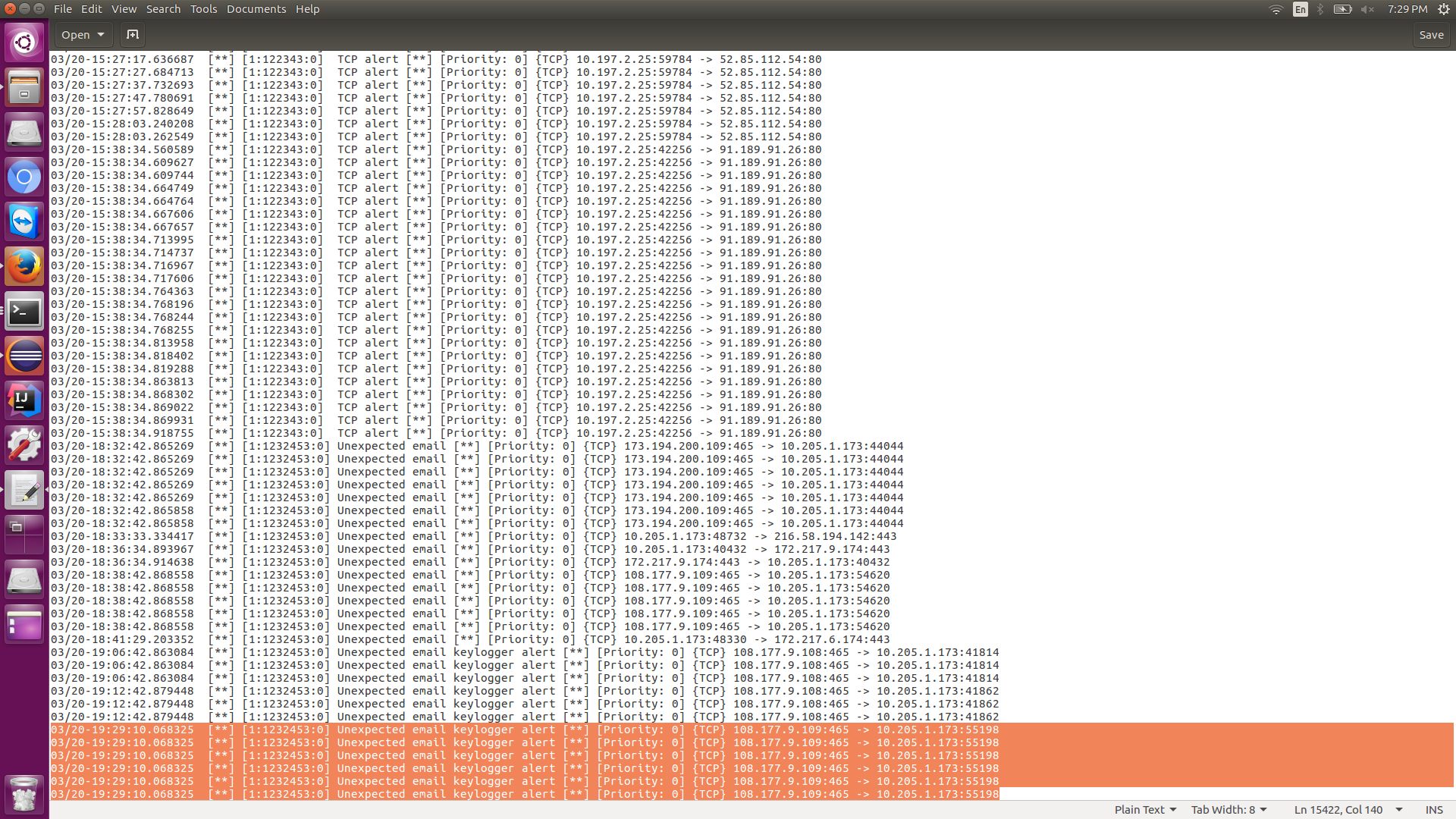
## **Running Snort:**



## **Generated Log files:**



## **Alert.ids file :**



# **References**

<https://www.symantec.com/connect/articles/introduction-spyware-keyloggers>

<http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node2.html>

<http://commons.oreilly.com/wiki/index.php/Snort_Cookbook/Rules_and_Signatures>

<https://www.snort.org/>

<http://opentodo.net/2012/10/snort-from-scratch-part-iii/>

<https://www.youtube.com/watch?v=RwWM0srLSg0>