# AIM:

PRACTICAL: 10

Identify the requirement of firewall/IDS in the system and perform firewall/IDS configuration.

# THEORY:

**Snort:** Snort is a free open source network intrusion detection system and intrusion prevention system. Snort is an intrusion detection and prevention system. It can be configured to simply log detected network events to both log and block them.Snort package enables application detection and filtering.Snort rules can be custom created by the user, or any of several pre-packaged rule sets can be enabled and downloaded.

Snort works by analyzing network traffic in real-time and comparing it against a set of predefined rules. When Snort detects traffic that matches one of its rules, it generates an alert that can be used to notify network administrators of potential security threats.

**Network sharing:** Network sharing refers to the process of making files and resources available to other computers on a network. This can be done using various protocols such as SMB, NFS, FTP, and others. Network sharing is a common practice in many organizations, as it allows users to access files and resources on different computers without having to physically transfer files.

**Detecting network sharing:** To detect network sharing, Snort looks for traffic associated with file sharing protocols such as SMB, NFS, and FTP. Snort analyzes the packets of these protocols and compares them against a set of predefined rules that are designed to identify the specific characteristics of network sharing traffic. For example, Snort might look for certain byte sequences in the packet payload that indicate the presence of an SMB session request, or it might look for certain file transfer commands in an FTP session.

Snort can be customized to detect specific types of network sharing activity by modifying the rules used to analyze network traffic. Network administrators can create custom Snort rules that look for specific byte sequences, commands, or other characteristics associated with network sharing protocols. By doing so, they can tailor Snort to detect network sharing activity that is specific to their organization and network environment.

# CODE(Rules):

**FTP Protocol verification:**

* alert tcp $EXTERNAL\_NET any -> $HOME\_NET 21 (msg:"FTP REST overflow attempt"; flow:to\_server,established; content:"REST"; nocase; isdataat:100,relative; pcre:"/^REST\s[^\n]{100}/smi"; reference:bugtraq,2972; reference:cve,2001-0826; classtype:attempted-admin; sid:1974; rev:6;)

**FTP Bad directories:**

* alert tcp $EXTERNAL\_NET any -> $HOME\_NET 21 (msg:"FTP CWD ~root attempt"; flow:to\_server,established; content:"CWD"; nocase; content:"~root"; distance:1; nocase; pcre:"/^CWD\s+~root/smi"; reference:arachnids,318; reference:cve,1999-0082; classtype:bad-unknown; sid:336; rev:10;)

## File detect:

* alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"FILE- IDENTIFY JAR/ZIP file magic detected"; flow:to\_client,established; file\_data; content:"PK|06 08|"; flowbits:set,file.zip; flowbits:set,file.jar; flowbits:noalert; metadata:policy max-detect-ips drop, service ftp-data, service http, service imap, service pop3; classtype:misc-activity; sid:20467; rev:15;)

## PDF-file detect:

* alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"FILE- PDF Adobe Flash Player memory corruption attempt"; flow:to\_client,established; flowbits:isset,file.pdf; file\_data; content:"|63 2F 55 46 28 70 6F 63 2E 73 77 66 29 3E 3E 0D|"; content:"|3C 2F 43 68 65 63 6B 53 75 6D 3C 31 36 43 44 45 32 43 39 44 38 41 44 37 37 30 35 46 41 32 31 36 46 31 33 34 46 41 46 37 38 35 30 3E 2F 43 72 65|"; within:48; distance:112; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service ftp-data, service http, service imap, service pop3; reference:cve,2011-0609; reference[:url,ww](http://www.adobe.com/support/security/bulletins/apsb11-)w.ado[be.com/support/security/bulletins/apsb11-](http://www.adobe.com/support/security/bulletins/apsb11-) 06.html; classtype:attempted-user; sid:19082; rev:11;)
* alert tcp $EXTERNAL\_NET $FILE\_DATA\_PORTS -> $HOME\_NET any (msg:"FILE- PDF Adobe Acrobat Reader embedded TTF bytecode memory corruption attempt"; flow:to\_client,established; flowbits:isset,file.pdf; file\_data; content:"|2C 23 4B 54 58 20 20 60 B0 01 60 25 8A 38 1B 23 21 59 B8 FF FF 62 2D|"; fast\_pattern:only; metadata:policy balanced-ips drop, policy connectivity-ips drop, policy security-ips drop, service ftp-data, service http, service imap, service pop3; reference:bugtraq,55015; reference:cve,2012-4154; reference[:url,ww](http://www.adobe.com/support/security/bulletins/apsb12-16.html%3B)w.a[dobe](http://www.adobe.com/support/security/bulletins/apsb12-16.html%3B).c[om/support/security/bulletins/apsb12-16.html;](http://www.adobe.com/support/security/bulletins/apsb12-16.html%3B) classtype:attempted-user; sid:24152; rev:4;)

## FTP bad files:

* alert tcp $EXTERNAL\_NET any -> $HOME\_NET 21 (msg:"FTP authorized\_keys"; flow:to\_server,established; content:"authorized\_keys"; classtype:suspicious-filename-detect; sid:1927; rev:2;)

## File identify:

* alert tcp $EXTERNAL\_NET any -> $SMTP\_SERVERS 25 (msg:"FILE-IDENTIFY Microsoft Office PowerPoint file attachment detected"; flow:to\_server,established; content:".ppt"; fast\_pattern:only; content:"Content-Disposition: attachment|3B|"; content:"filename="; nocase; pcre:"/filename=[^\n]\*\x2eppt/i"; flowbits:set,file.ppt; flowbits:noalert; metadata:policy max-detect-ips drop, service smtp; classtype:misc-activity; sid:20983; rev:8;)

# OUTPUT:



Figure 10.1 checking snort version

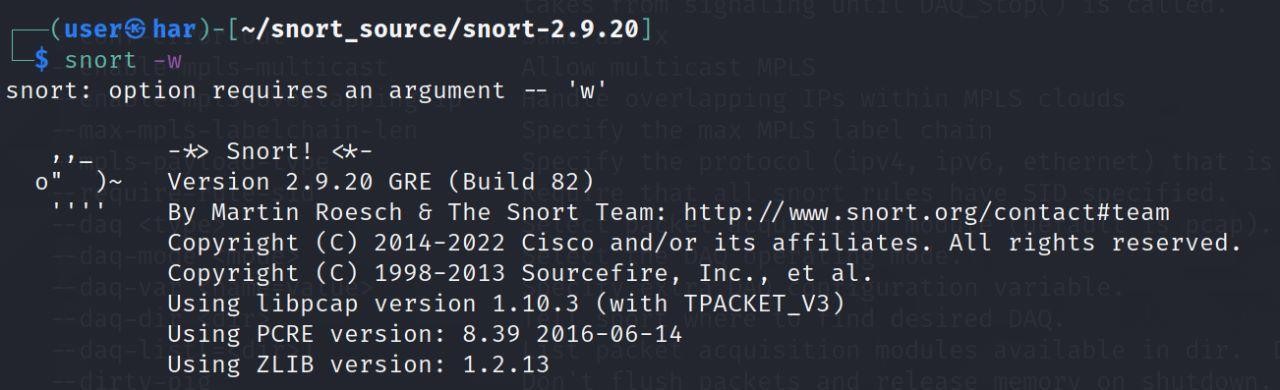
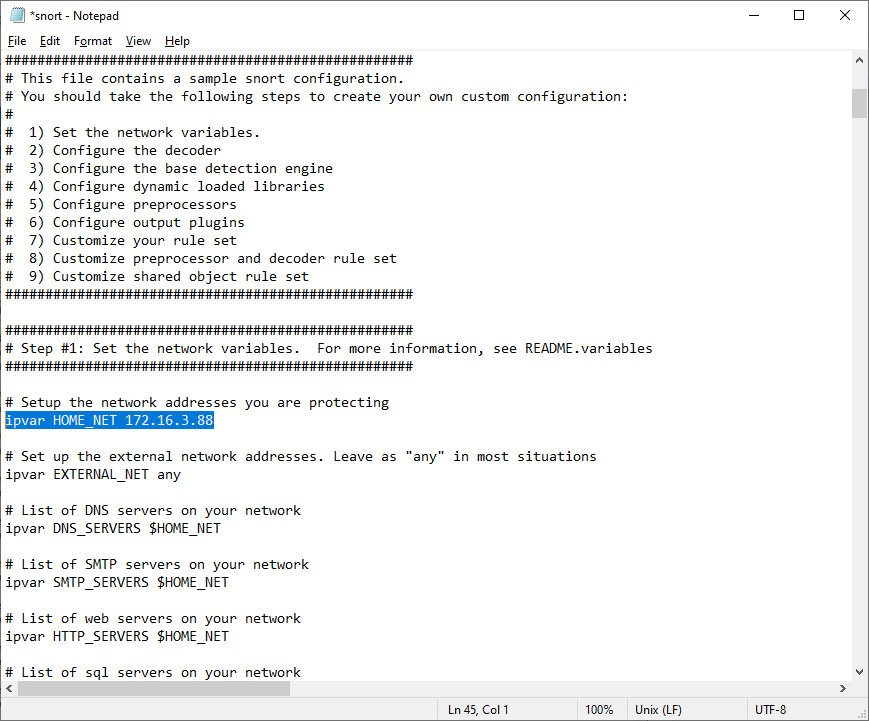
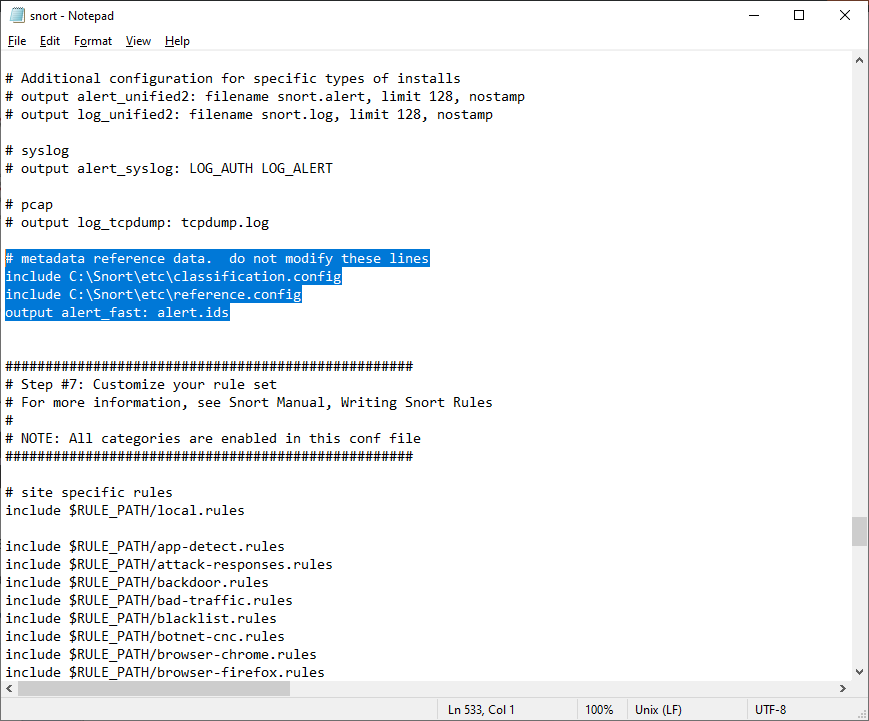
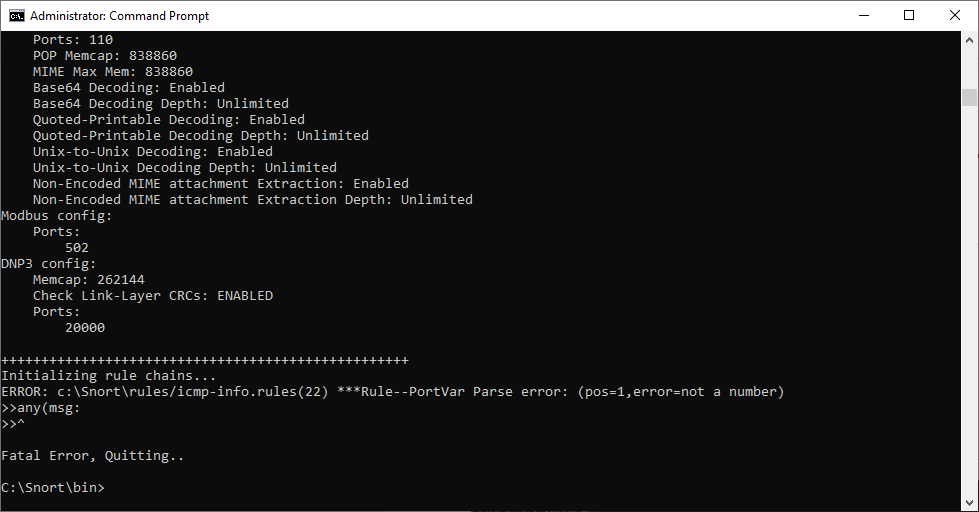


Figure 10.2 interfaces detection using snort

****

Configuring the variables and specifying the HOME\_NET variable with my ip

****

 error occured in the rule’s execution.

# LATEST APPLICATIONS:

* Snort's open-source network-based intrusion detection/prevention system (IDS/IPS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching.
* The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, semantic URL attacks, buffer overflows, server message block probes, and stealth port scans.
* Snort can be configured in three main modes:
  1. sniffer,
  2. packet logger, and
  3. network intrusion detection.

# LEARNING OUTCOME:

In this practical, I learnt about intrusion detection system using snort, installing and configuring snort, detecting network sharing using snort rules.

# REFERENCES:

1. Snort: <https://www.snort.org/>
2. Snort Theory & applications:
   * <https://en.wikipedia.org/wiki/Snort_(software)>
   * <https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html>