IDS(intrusion detection system)_**IPS**(intrusion prevention system)_Using_**SNORT**

What is IDS?

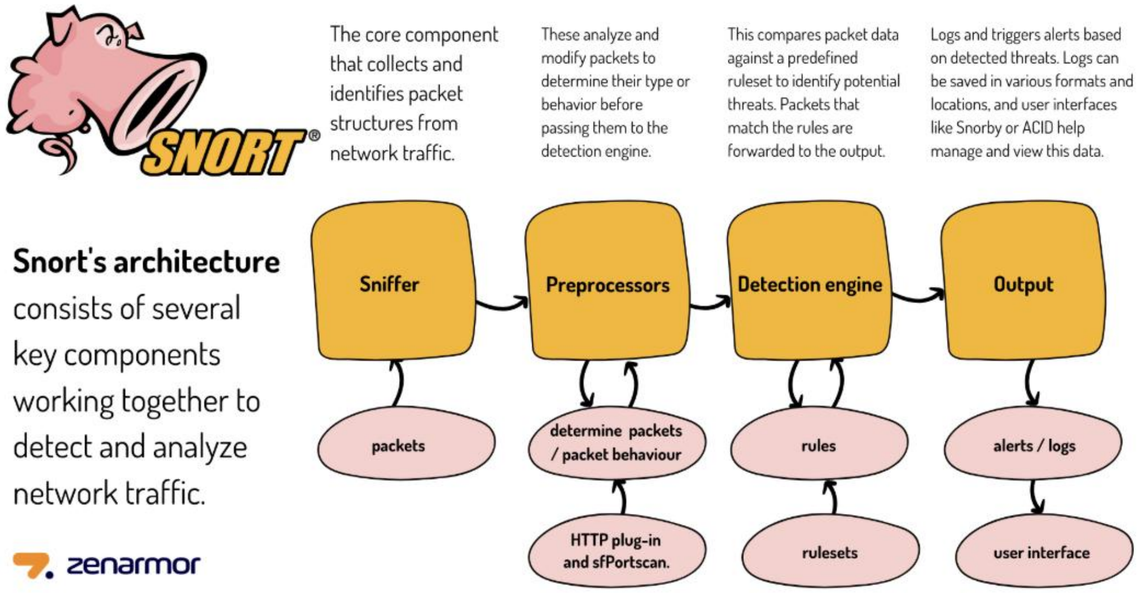
An intrusion detection system (IDS) is a device or software application that monitors a network for malicious activity or policy violations. Any malicious activity or violation is typically reported or collected centrally using a security information and event management system.

What is IPS?

An intrusion prevention system, or IPS, monitors real-time network activity for a deeper examination and identification of possible security concerns. IPS looks for traffic patterns or attack characteristics and when identified, IPS generates alerts and blocks detected attacks.

What is SNORT Tool?

SNORT is a powerful open-source intrusion detection system (IDS) and intrusion prevention system (IPS) that provides real-time network traffic analysis and data packet logging. SNORT uses a rule-based language that combines anomaly, protocol, and signature inspection methods to detect potentially malicious activity**.**


SNORT®
The core component that collects and identifies packet structures from network traffic.
These analyze and modify packets to determine their type or behavior before passing them to the detection engine.
This compares packet data against a predefined ruleset to identify potential threats. Packets that match the rules are forwarded to the output.
Logs and triggers alerts based on detected threats. Logs can be saved in various formats and locations, and user interfaces like Snorby or ACID help manage and view this data.
Snort's architecture consists of several key components working together to detect and analyze network traffic.
Sniffer
Preprocessors
Detection engine
Output
packets
determine packets / packet behaviour
rules
alerts / logs
HTTP plug-in and sfPortscan.
rulesets
user interface
zenarmor

Set up SNORT for IDS and IPS →

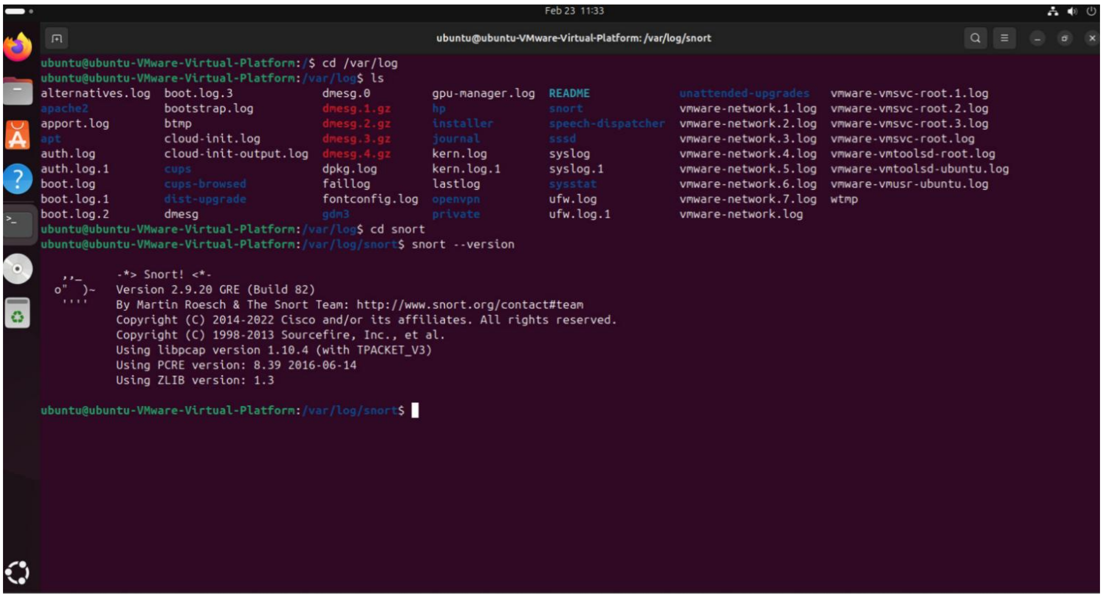
On ubuntu terminal:

Step-1: sudo apt-get install snort

Step -2: cd /var/log

Step-3: cd snort

Step-4: snort –version

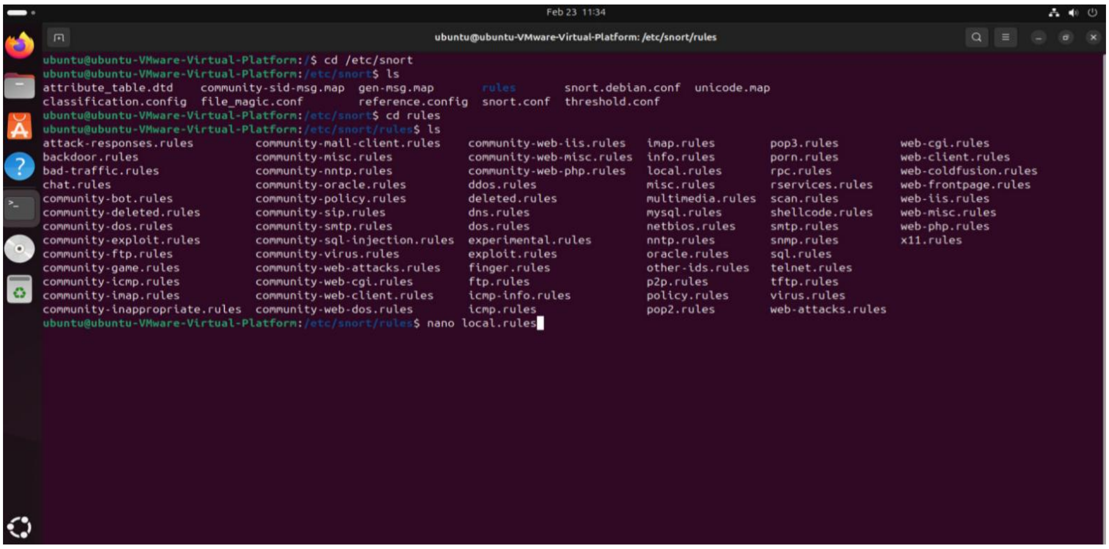


```
ubuntu@ubuntu-VMware-Virtual-Platform:/$ cd /var/log
ubuntu@ubuntu-VMware-Virtual-Platform:/var/log$ ls
alternatives.log  boot.log.3             dmesg.0         gpu-manager.log  README             unattended-upgrades   vmware-vmsvc-root.1.log
apache2           bootstrap.log          dmesg.1.gz      hp               snort              vmware-network.1.log  vmware-vmsvc-root.2.log
apport.log        btmp                   dmesg.2.gz      installer        speech-dispatcher  vmware-network.2.log  vmware-vmsvc-root.3.log
apt               cloud-init.log         dmesg.3.gz      journal          sssd               vmware-network.3.log  vmware-vmsvc-root.log
auth.log          cloud-init-output.log  dmesg.4.gz      kern.log         syslog             vmware-network.4.log  vmware-vmtoolsd-root.log
auth.log.1        cups                   dpkg.log        kern.log.1       syslog.1           vmware-network.5.log  vmware-vmtoolsd-ubuntu.log
boot.log          cups-browsed           faillog         lastlog          sysstat            vmware-network.6.log  vmware-vmusr-ubuntu.log
boot.log.1        dist-upgrade           fontconfig.log  openvpn          ufw.log            vmware-network.7.log  wtmp
boot.log.2        dmesg                  gdm3            private          ufw.log.1          vmware-network.log
ubuntu@ubuntu-VMware-Virtual-Platform:/var/log$ cd snort
ubuntu@ubuntu-VMware-Virtual-Platform:/var/log/snort$ snort --version

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

ubuntu@ubuntu-VMware-Virtual-Platform:/var/log/snort$ 
```

Step-5: cd /etc/snort

Step-6: ls

Step-7: cd /etc/snort/rules



```
ubuntu@ubuntu-VMware-Virtual-Platform:/$ cd /etc/snort
ubuntu@ubuntu-VMware-Virtual-Platform:/etc/snort$ ls
attribute_table.dtd    community-sid-msg.map  gen-msg.map       rules       snort.debian.conf  unicode.map
classification.config  file_magic.conf        reference.config  snort.conf  threshold.conf
ubuntu@ubuntu-VMware-Virtual-Platform:/etc/snort$ cd rules
ubuntu@ubuntu-VMware-Virtual-Platform:/etc/snort/rules$ ls
attack-responses.rules         community-mail-client.rules    community-web-iis.rules   imap.rules        pop3.rules       web-cgi.rules
backdoor.rules                 community-misc.rules           community-web-misc.rules  info.rules        porn.rules       web-client.rules
bad-traffic.rules              community-nntp.rules           community-web-php.rules   local.rules       rpc.rules        web-coldfusion.rules
chat.rules                     community-oracle.rules         ddos.rules                misc.rules        rservices.rules  web-frontpage.rules
community-bot.rules            community-policy.rules         deleted.rules             multimedia.rules  scan.rules       web-iis.rules
community-deleted.rules        community-sip.rules            dns.rules                 mysql.rules       shellcode.rules  web-misc.rules
community-dos.rules            community-smtp.rules           dos.rules                 netbios.rules     smtp.rules       web-php.rules
community-exploit.rules        community-sql-injection.rules  experimental.rules        nntp.rules        snmp.rules       x11.rules
community-ftp.rules            community-virus.rules          exploit.rules             oracle.rules      sql.rules
community-game.rules           community-web-attacks.rules    finger.rules              other-ids.rules   telnet.rules
community-icmp.rules           community-web-cgi.rules        ftp.rules                 p2p.rules         tftp.rules
community-imap.rules           community-web-client.rules     icmp-info.rules           policy.rules      virus.rules
community-inappropriate.rules  community-web-dos.rules        icmp.rules                pop2.rules        web-attacks.rules
ubuntu@ubuntu-VMware-Virtual-Platform:/etc/snort/rules$ nano local.rules
```

SET UP OF RULES ->

STEP-8: cd rules

After the step-7 several rules appers , we have to configure the rules according to the alert message.

For example: nano local.rules