Assignment C-2

Aim:

To implement Intrusion Detection System to monitor network traffic.

Problem Statement:

Install and Use Latest IDS (Open Source).

Theory:

What is IDS

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 electronic 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. NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users). 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.

There are three primary components of an IDS:

1. **Network Intrusion Detection System (NIDS):**: This does analysis for traffic on a whole subnet and will make a match to the traffic passing by to the attacks already known in a library of known attacks.

2. **Network Node Intrusion Detection System (NNIDS):**: This is similar to NIDS, but the traffic is only monitored on a single host, not a whole subnet.

3. **Host Intrusion Detection System (HIDS):** This takes a âĂIJpictureâĂİ of an entire systemâĂŹs file set and compares it to a previous picture. If there are significant differences, such as missing files, it alerts the administrator.

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,and which has been owned by Cisco since 2013.

Uses

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 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.[11] 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.

Components of Snort

A Snort-based IDS contains the following components:

- Packet Decoder
- Preprocessors
- Detection Engine
- Logging and Alerting System
- Output Modules

Figure below shows how these components work together to detect particular attacks and to generate output. Any data packet coming from the Internet enters the packet decoder. On its way towards the output modules, it is either dropped, logged or an alert is generated.

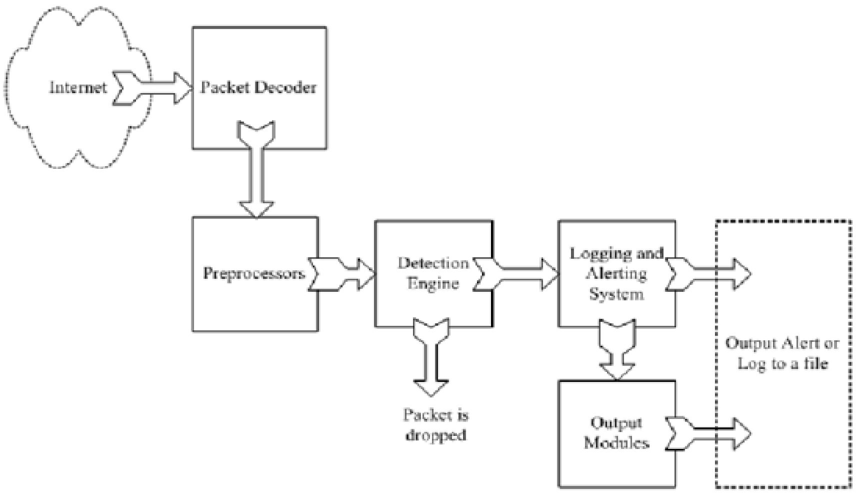
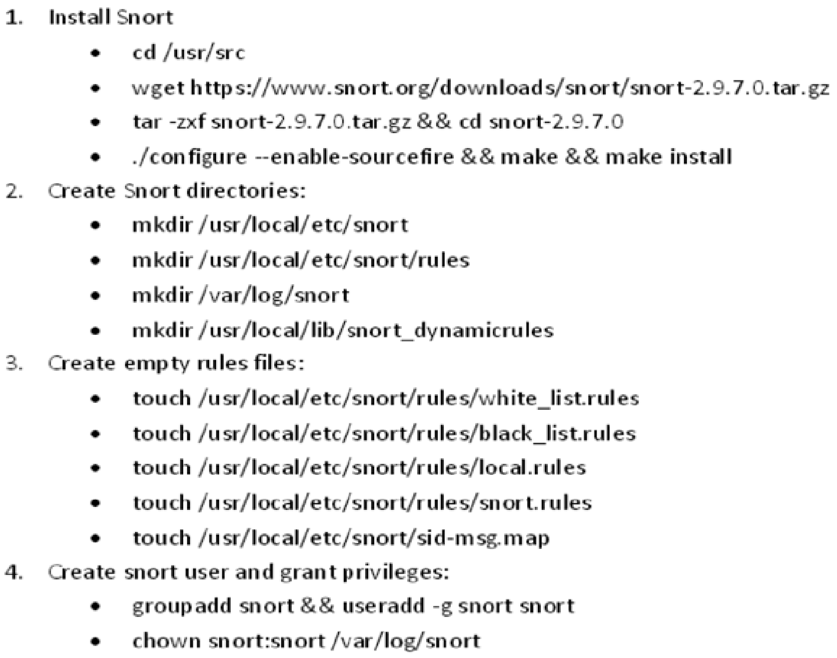


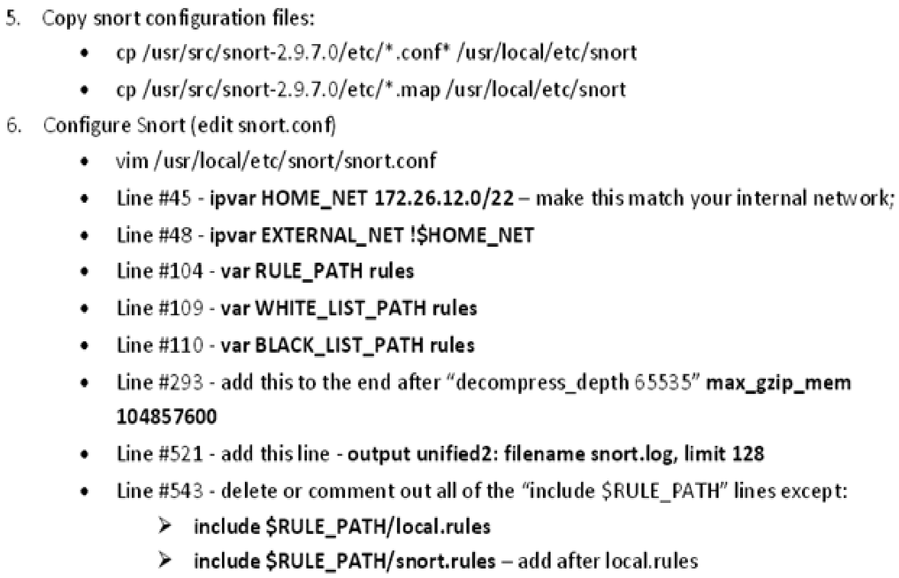
Figure 1: Round 1 of SHA-1

Installation and configuration

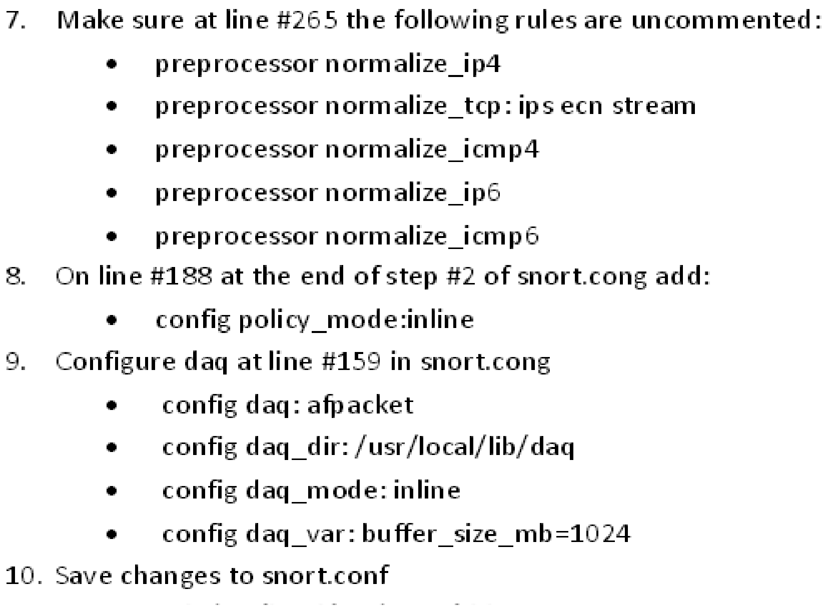
Before installing Snort make sure you have following packages installed namely libpcap,flex,bison,g++,tcpdump etc. installed on your machine. If any of the packages are missing it will prompt you to install those packages.Once your are done with the dependencies you can start installing snort.



1. Install Snort
   - cd /usr/src
   - wget https://www.snort.org/downloads/snort/snort-2.9.7.0.tar.gz
   - tar -zxf snort-2.9.7.0.tar.gz && cd snort-2.9.7.0
   - ./configure --enable-sourcefire && make && make install
2. Create Snort directories:
   - mkdir /usr/local/etc/snort
   - mkdir /usr/local/etc/snort/rules
   - mkdir /var/log/snort
   - mkdir /usr/local/lib/snort_dynamicrules
3. Create empty rules files:
   - touch /usr/local/etc/snort/rules/white_list.rules
   - touch /usr/local/etc/snort/rules/black_list.rules
   - touch /usr/local/etc/snort/rules/local.rules
   - touch /usr/local/etc/snort/rules/snort.rules
   - touch /usr/local/etc/snort/sid-msg.map
4. Create snort user and grant privileges:
   - groupadd snort && useradd -g snort snort
   - chown snort:snort /var/log/snort



5. Copy snort configuration files:
    - cp /usr/src/snort-2.9.7.0/etc/*.conf* /usr/local/etc/snort
    - cp /usr/src/snort-2.9.7.0/etc/*.map /usr/local/etc/snort
6. Configure Snort (edit snort.conf)
    - vim /usr/local/etc/snort/snort.conf
    - Line #45 - **ipvar HOME_NET 172.26.12.0/22** – make this match your internal network;
    - Line #48 - **ipvar EXTERNAL_NET !$HOME_NET**
    - Line #104 - **var RULE_PATH rules**
    - Line #109 - **var WHITE_LIST_PATH rules**
    - Line #110 - **var BLACK_LIST_PATH rules**
    - Line #293 - add this to the end after "decompress_depth 65535" **max_gzip_mem 104857600**
    - Line #521 - add this line - **output unified2: filename snort.log, limit 128**
    - Line #543 - delete or comment out all of the "include $RULE_PATH" lines except:
        - **include $RULE_PATH/local.rules**
        - **include $RULE_PATH/snort.rules** – add after local.rules



7. Make sure at line #265 the following rules are uncommented:
    - preprocessor normalize_ip4
    - preprocessor normalize_tcp: ips ecn stream
    - preprocessor normalize_icmp4
    - preprocessor normalize_ip6
    - preprocessor normalize_icmp6
8. On line #188 at the end of step #2 of snort.cong add:
    - config policy_mode:inline
9. Configure daq at line #159 in snort.cong
    - config daq: afpacket
    - config daq_dir: /usr/local/lib/daq
    - config daq_mode: inline
    - config daq_var: buffer_size_mb=1024
10. Save changes to snort.conf

Snort Rules

A Snort rule can be broken down into two basic parts, the rule header and options for the rule. The rule header contains the action to perform, the protocol that the rule applies to, and the source and destination addresses and ports. Here's the general form of a Snort rule:

action proto src_ip src_port direction *dst_ipdst_port*

When a packet comes in, its source and destination IP addresses and ports are then compared to the rules in the ruleset. If any of them are applicable to the packet, then the options are compared to the packet. If all of these comparisons return a match, then the specified action is taken.

For instance, if you wanted to start recording packets once an exploit of a SSH daemon on 192.168.1.21 was noticed, you could use a couple of rules similar to these:

```
activate tcp any any -> 192.168.1.21 22 (content:"/bin/sh"; activates:1; \
msg:"Possible SSH buffer overflow"; )
dynamic tcp any any -> 192.168.1.21 22 (activated_by:1; count:100;)
```

Conclusion:

Thus, we have studied Intrusion Detection using Snort.