Assignment 2

Q. Provide a detailed comparison on commercial and open-source IDS available today. Compare them on the basis of various parameters.

Open Source Intrusion Detection System:

1. SNORT
2. BRO
3. OSSEC
4. TRIPWIRE

Snort:

Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

Features of Snort

- Real-time traffic monitor
- Packet logging
- Analysis of protocol
- Content matching
- OS fingerprinting
- Can be installed in any network environment.
- Creates logs
- Open Source

- Rules are easy to implement

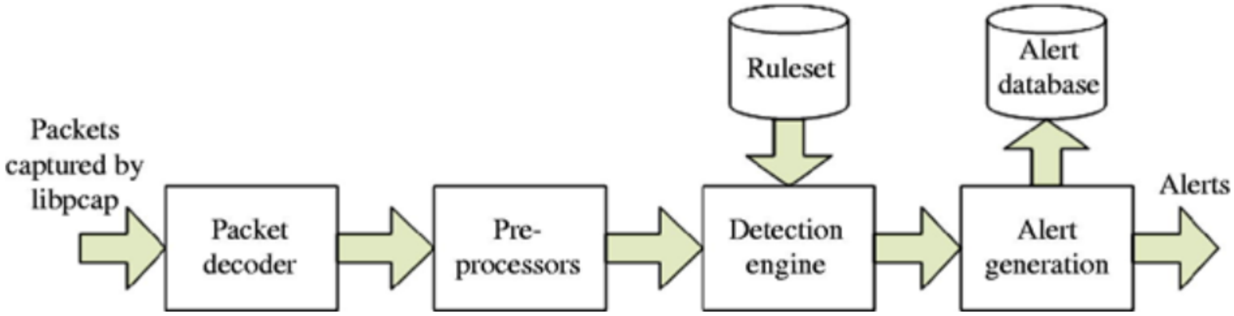
Purpose of Snort

The main purpose of Snort is to perform packet logging and traffic analysis on the network. In this case, Snort has three primary uses: As a packet sniffer, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system.

Snort Architectural Structure

Snort is made up of different components, and these components work together to identify attacks and generate output. Snort-based IDS systems mainly consist of the following components:

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



Some Advantages and Disadvantages

- Snort provides open source and free monitoring for networks and computers.
- Any alterations to files and directories on the system can be easily detected and reported.

- When deploying Snort, it’s important to make sure the used rules are relevant and up to date, otherwise the system will be much less efficient
- Although Snort is flexible, it does lack some features found in commercial intrusion detection systems.

Cyber Security Solutions Provided by Snort

It has some cyber security solutions provided to us.

- Snort is to do packet logging and traffic analysis on the network.
- Snort can detect many attacks and malicious / suspicious software.
- Snort can also be used to perform network/protocol analysis, content searching and matching.

Snort Alerts

Alerts are placed in the Alert file in the logging directory. Snort has 6 alert modes. These are fast, full, console, cmg, unsock and none. We applied cmg and console modes. Also, the mode Snort is run in depends on which flags are used with the Snort command.

Each alert carry the following information:

- IP address of the source
- IP address of the destination
- Packet type and useful header information

OSSEC:

OSSEC is fully open source and free. You can tailor OSSEC for your security needs through its extensive configuration options, adding custom alert rules and writing scripts to take action when alerts occur. OSSEC offers comprehensive host-based intrusion detection across multiple platforms including Linux, Solaris, AIX, HP-UX, BSD, Windows, Mac and VMware ESX.

Advantages:

- Analyze logs from multiple devices and formats. The devices can be Agents, Syslog devices, Routers, Switches, Printers, etc.,
- An active response system. This means OSSEC will not only monitor, but also respond to threats (ex. black list naughty IP addresses)

Disadvantages**:**

- Difficulty in upgrades between versions. OSSEC comes with default rules and they are overwritten on every upgrade.
- Coordinating pre-shared keys can be problematic. In OSSEC architecture Client and server communicate through encrypted channel using blowfish algorithm. Here pre- sharing keys before the communication establishment is a challenging issue.

TRIPWIRE:

Tripwire is a free and open-source Linux Intrusion Detection System. It is used to detect and report any unauthorized change in files and directories on Linux. It will also send you an alert on email on file/directory changes.

Advantages:

- Advantage of tripwire is that it encrypts its database and config file

Disadvantages:

- Tripwire does not generate real-time alerts upon an intrusion.

BRO:

In order to install Bro, one needs to install all the prerequisites. This included the following:

- C++ Actor Framework
- LibGeoIP Database
- Gperftools
- Ipsumdump
- PF_RING (needed for network throughput over 1 Gbps)
- And a few others

****

Commercial Intrusion Detection Systems

A Commercial Intrusion Detection System is a set of devices and alarms meant to safeguard business properties like commercial buildings, retail outlets, labs, schools, hospitals, clinics, industries, etc. Complete perimeter door protection, window or glass break protection, and interior motion detectors make up the most popular type of protective equipment.

Perimeter Door Protection (Commercial Intrusion Detection System):

The term Perimeter Door Protection could suggest the extent of measures used to brace entrances against doorway breaking, hammer striking, lock picking, and thwart bad behaviors like burglary and business interruptions. Entrance security is used in business and government structures, as well as in industries. All external entrances to be built of 16-measure steel or aluminum composite. Glass doorways to feature the impact of safety glass to obstruct crooks. Swinging entryways should be locked with unshakable, multi-point, long-flush bolts. Remember, that entrance frameworks ought to be essentially serious solid areas for as the genuine entrances or an intruder could have the choice to break in by evading the edge.

Glass Break Protection (Commercial Intrusion Detection System):

These are switches that should be physically enacted by a staff part when the person is threatened by an intruder. Normally, they are used in high-hazard or high-responsiveness regions and are stowed away from the overall population.

Interior Motion Detectors (Commercial Intrusion Detection System):

When we talk about Interior Motion Detectors in a commercial security system, we allude to Passive Infrared sensors. It generally detects temperature changes; when an Intruder raises the temperature by strolling through the safeguarded region, the sensor sets off an alarm. They are just responding to the radiation or intensity exuding from strong items in their field of view. However, the present movement sensors are significantly more intelligent than you suspect. They have algorithms to separate between a false alarm like a little mouse movement and an individual strolling through the safeguarded region.

Panic and duress alarms (Commercial Intrusion Detection System):

The term Perimeter Door Protection could suggest the extent of measures used to brace entrances against doorway breaking, hammer striking, lock picking, and thwart bad behaviors like burglary and business interruptions. Entrance security is used in business and government structures, as well as in industries. All external entrances to be built of 16-measure steel or aluminum composite. Glass doorways to feature the impact of safety glass to obstruct crooks. Swinging entryways should be locked with unshakable, multi-point, long-flush bolts. Remember, that entrance frameworks ought to be essentially serious solid areas for as the genuine entrances or an intruder could have the choice to break in by evading the edge.

****