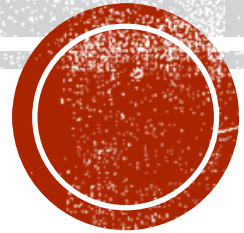
SNORT: INTRUSION DETECTION SYSTEM



WHAT IS SNORT?

- **SNORT** is a network based intrusion detection system which is written in C programming language. It was developed in 1998 by Martin Roesch. Now it is developed by Cisco. It is free open-source software.
- Snort is a network monitoring tool that watches traffic for signs of malicious activity (e.g., buffer overflows being executed against a service, command and control traffic from malware), suspicious activity (e.g., port scans and service enumeration) etc.
- Snort is a robust IDS that runs on Unix-based and Windows systems. It is also completely free.
- It is an open source intrusion prevention system capable of realtime traffic analysis and packet logging.

SNORT MODES

- **Sniffer**:- Simply reads the packets off of the network and displays them for you in a continuous stream on the console (screen).
- **Packet logger**:- Logs the packets to disk.
- **Network intrusion detection**:- Performs detection and analysis on network traffic. This is the most complex and configurable mode.

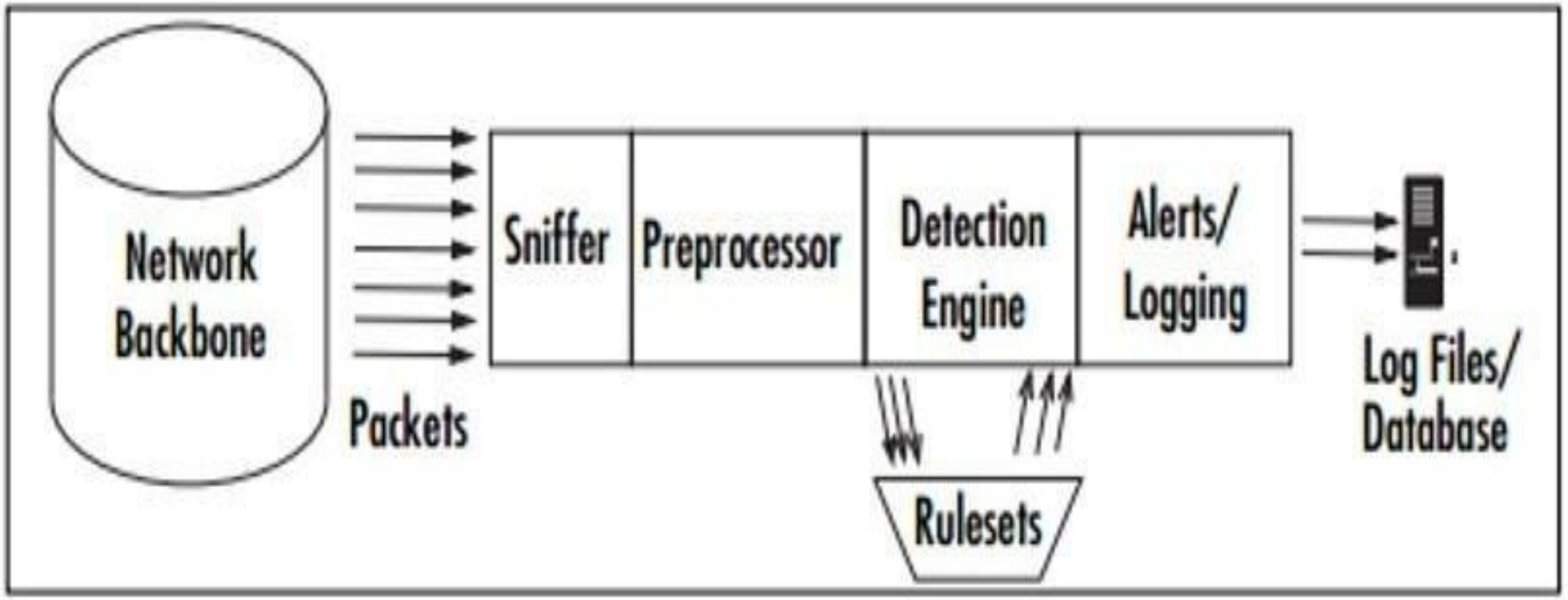
SNORT...

- snort is based on libpcap(for library packet capture), a tool that is widely used in TCP/IP traffic sniffers and analyzers
- Through protocol analysis and content searching and matching , snort detects attacks methods including deniol of services, buffer overflow, CGI attacks, stealth port scans, and SMB probes. When suspicious behavipur is detected, snort sends a real-time alert to syslog, a separate 'alerts' file, or to a pop-up windows.
- A rule may be used to generate an alert message, log a message, or in terms of snort, pass the data packets drop it silently
- The word pass here is not equivalent to the traditional meaning of pass as used in firewalls and routers. In firewalls and routers, pass and drop are opposite to each other.

SNORT...

- Snort rules are written in an easy to understand syntax. Most of the rules are written in a single line. However you can also extend rules to multiple lines by using a backslash character at the end of lines.
- Rules are usually placed in configuration files, typically snort.conf.you can also use multiple files by including them in a main configuration file.
- A rule may be used to generate an alert message, log a message, or, in terms of snort , pass the data the packet ,i.e drop silently

SNORT


Network Backbone
Packets
Sniffer
Preprocessor
Detection Engine
Alerts/ Logging
Log Files/ Database
Rulesets

EXPLORING SNORT.CONF

- In the Snort source directory, there are 2 subdirectories of interest: etc and rules. The actual snort.conf file lives in etc.
- The first part of the snort.conf file lets you set some important global variables, indicating such things as your home subnet, your web servers, and your rule locations.
- The second part of the file lets us configure pre-processors. The pre-processors handle such things as fragmented packets, port scan detection, and stream reassembly.

SNORT RULES

- Snort has several types of rules that affect how it handles traffic:
- **Alert rules** - Log packets whose characteristics match a predefined suspicious pattern (e.g., generated by a common hacking tool, or contain a string indicative of a buffer overflow or web attack) or custom rules that monitor packets you determine to be prohibited or undesirable on your network (e.g., file sharing, gaming, etc.).
- **Pass rules** - Explicitly ignore packets. Traffic that matches these rules will not be logged.
- **Log rules** - Record packets but do not generate rules. This would be useful for diagnosing network problems, storing traffic for audits, or monitoring sensitive systems so that traffic can be analyzed in case a compromise is detected.

SNORT RULES...

- **Activate rules -** Generate an alert for traffic that matches this rule's trigger, then activate a subsequent dynamic rule. (Until it is activated, a dynamic rule will not generate an alert even if traffic matches it.)
- **Dynamic rules -** Triggered by activate rules. This enables you to chain rules together in a way that makes inspection more efficient (don't run rules needlessly) and more effective (create complex chains). These are great mechanisms for gathering more information during an attack.

SNORT RULES SYNTAX

- Snort comes with a standard ruleset that checks for activity such as Nmap stealth scans, vulnerability exploits, attempted buffer overflows, anonymous FTP access etc.
- By default, Snort checks the packet against alert rules first, followed by pass rules, and then log rules.
- Basic Snort rules consist of two parts: the header and the options.
- The first part of the header tells Snort what type of rule it is (such as alert, log, pass).
- The rest of the header indicates the protocol (ip, udp, icmp, or tcp), a directional operator (either -> to specify source to destination or <> to specify bidirectional), and the source and destination IP address and port.

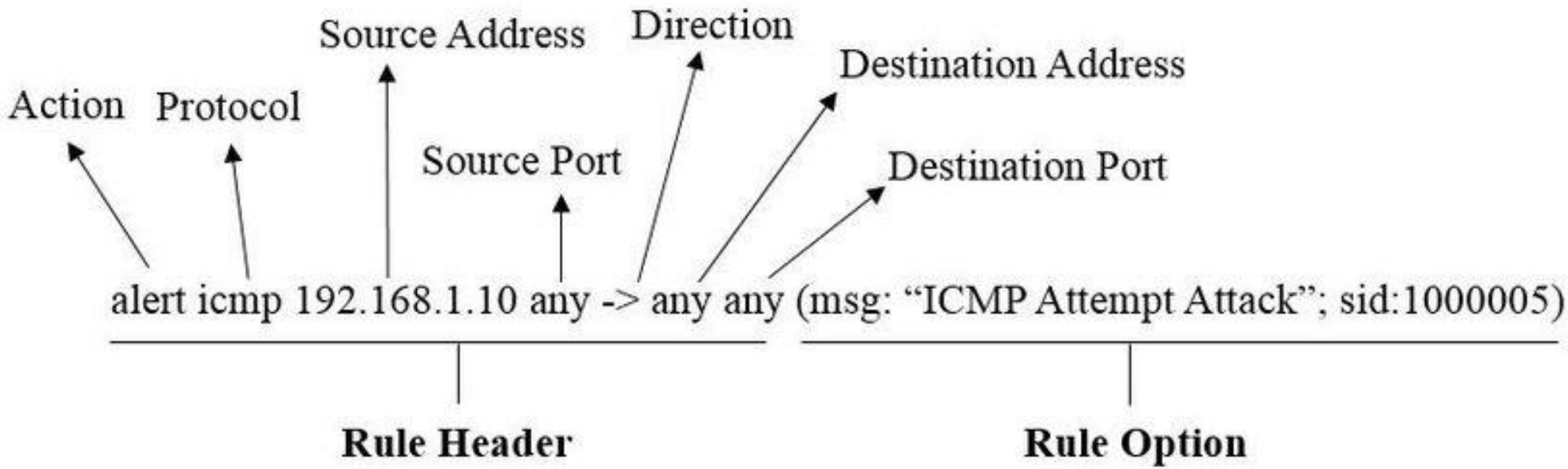
TESTING RULE (TO CHECK)

- **Rule:-**
  - **Alert ip any any → any any (msg;ip"ip packet detected';)**
- This is the worst rule ever written, but it dose a very good job of testing if snort is working well and is able to generate alerts.
- You can use this rule at the end of the snort.conf file the first time you install snort. The rule will generate an alert message for every captured IP packet.
- This rule is bad because it does not convey any information. This should be your first test to make sure that snort is installed properly.

STRUCTURE OF A RULE

- All snort rules have two logical parts: rule header and rule options.
- The rule header contains information about what action a rule takes. It also contains criteria for matching a rule against data packets.
- The rule options part usually contains an alert message and information about which part of the packets should be used to generate the alert message.
- The options part contains additional criteria for matching a rule against data packets.
- A rule may detect one type or multiple types of intrusion activity

SNORT RULE


Source Address
Direction
Destination Address
Action
Protocol
Source Port
Destination Port
alert icmp 192.168.1.10 any -> any any (msg: “ICMP Attempt Attack”; sid:1000005)
Rule Header
Rule Option

SNORT PLUG-INS

- **Pre-processors :-** Pre-processors are set up in the snort.conf file using the pre-processor command. They operate on packets after they've been received and decoded by Snort but before it starts trying to match rules.
- **Output Modules:-**Output modules are also set up in the snort.conf file using the output command, which controls how, where, and in what format Snort stores the data it receives. Any rule types we define can be specified to use a particular kind of output plug-in

BASIC USAGE

- **Packet Sniffing:** The way traffic is being transmitted can be thoroughly examined by gathering the individual packets that travel to and from devices on the network.
- **Generates Alerts:** It generates warnings based on the configuration file's rules when it discovers unusual or malicious activity, the possibility of a vulnerability being exploited, or a network threat that compromises the organization's security policy.
- **Debug Traffic:** After the traffic has been logged, any malicious packets and configuration problems are checked.

FEATURES

- 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

THANK YOU