PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

(All Branches NBA Accredited)

Department of Information Technology

Academic Year: 2022-23 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 6

Aim: To study Intrusion Detection system SNORT and its log analysis.

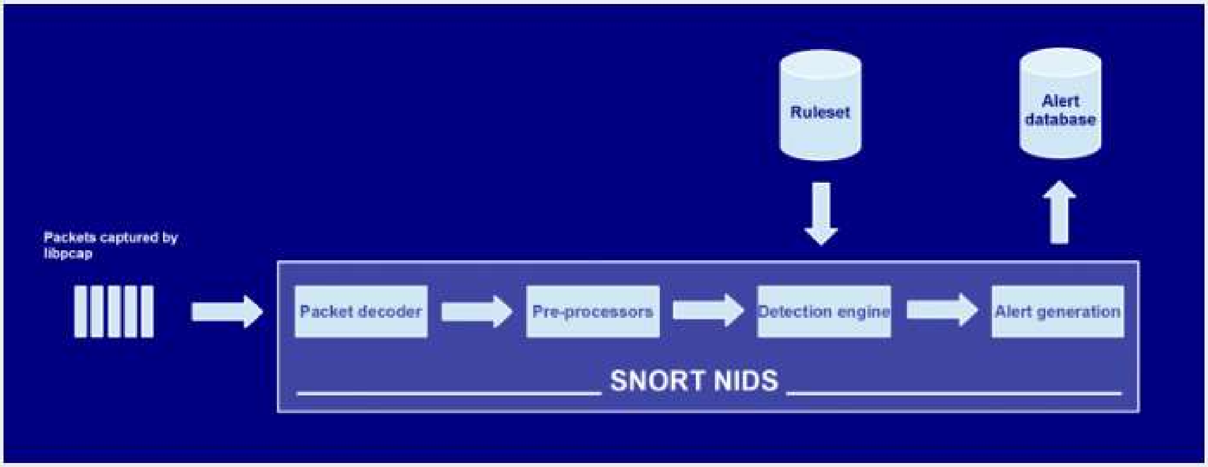
Theory :

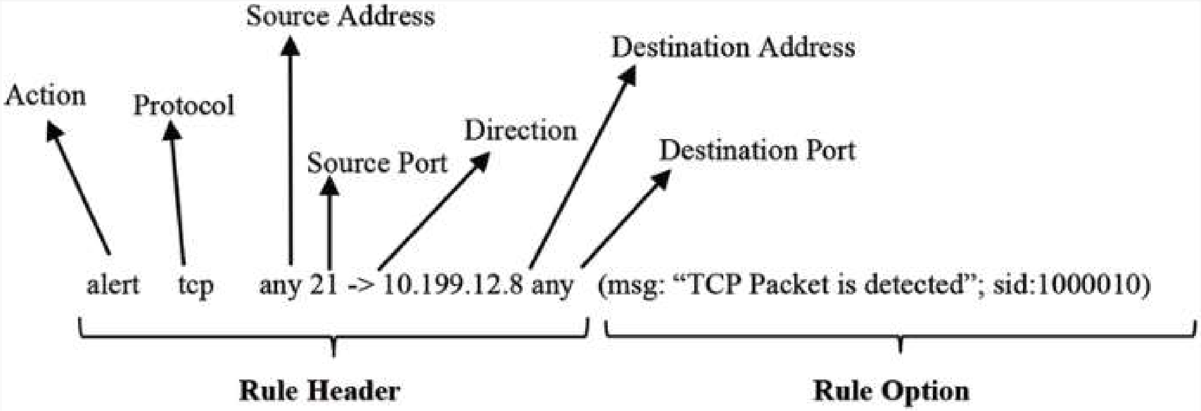
Snort is a popular choice for running a network intrusion detection systems or NIDS. It monitors the package data sent and received through a specific network interface. NIDS can catch threats targeting your system vulnerabilities using signature-based detection and protocol analysis technologies. NIDS software, when installed and configured appropriately, can identify the latest attacks, malware infections, compromised systems, and network policy violations.

Snort can run in two modes:

- Packet Sniffing :This mode have no special use, all you can do is just look at the traffic coming at the interface.

- Network Intrusion detection:This mode is the actual use of snort, in this mode snort monitor the traffic and block any unwanted traffic using the rules.





```
alert tcp any 21 -> 10.199.12.8 any (msg: “TCP Packet is detected”; sid:1000010)
```

Conclusion: Hence we have successfully studied Snort which is network intrusion prevention system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Also we have done analysis of log generated by snort.