PAGE NO.
DATE / /

Algorithm -4

Roll NO :- 43236

Aim :- SNORT table

Objective :- To install, configure and define rules in SNORT

Theory :- SNORT is an open source intrusion prevention system (IPS) It uses a series of rules that help define malicious network activity and uses those rules to find packet that match against them and quarantine about for users

Features :-

- Real time traffic monitoring
- Packet logging
- Analysis protocol
- Content matching
- Open source
- Rules are easy to implement

Rules :-

- Detect TCP packets
- Alert tcp any - any -> any any (msg: "TCP detected"; sid +0000002;)

Detect VoIP Packet

Alert UDP any any -> any any (msg
"VAP detd"
sid + 0000003);

Conclusion :-

This successfully studied SNORT
to detect VoIP installed it and tested
it within rules.