Snort Quick Guide **Scope:** Getting started with Snort for basic network intrusion prevention and SIEM. Assumes only basic Kali Linux skills (command line). Length: ≤3 pages.

1. What is Snort? Snort watches network traffic and checks it against rules. It can **alert** about suspicious activity (IDS mode) or **block** harmful traffic (IPS mode). Think of it as a security guard for your network.

2. Install Snort sudo apt update sudo apt install snort -y snort -V

3. Important Folders **Config:** /etc/snort/snort.conf **Rules:** /etc/snort/rules/ **Logs:** /var/log/snort/

4. First Test Run Edit HOME_NET in /etc/snort/snort.conf. Example: var HOME_NET 192.168.1.0/24 sudo snort -T -c /etc/snort/snort.conf

5. First Rule alert icmp any any -> $HOME_NET any (msg:"ICMP Ping Detected"; sid:1000001; rev:1;) Add this to /etc/snort/rules/local.rules and include in snort.conf.

6. Run & See Alerts sudo snort -c /etc/snort/snort.conf -i eth0 -A console Replace eth0 with your interface (check ip a). Try pinging the machine to see alerts.

7. Logs Snort saves alerts in /var/log/snort/.

8. Prevention (IPS) Snort can drop traffic using **drop** rules when inline. Start with IDS before IPS.

9. Sending Alerts to SIEM Enable JSON logs (EVE), then forward using Filebeat/Logstash to Splunk, Graylog, or ELK.

10. Troubleshooting Test config: snort -T -c /etc/snort/snort.conf No alerts? Ensure local.rules is included. Too many alerts? Comment noisy rules with #.

11. Quick Checklist Install Snort Confirm with snort -V Set HOME_NET Add simple rule Run and test traffic Check logs Forward to SIEM

Next Steps Download community rules at Snort.org. Try HTTP/DNS/SSH rules. Move to IPS once comfortable with IDS.

Start small, get one alert working, then expand step by step.