**Title: Intrusion Detection Systems (IDS): Snort and Suricata on Pop!\_OS**

**Slide 1: Title Slide**

* Title: Intrusion Detection Systems (IDS): Snort and Suricata
* Subtitle: Understanding, Installing & Using IDS on Pop!\_OS
* Your Name
* Date

**Slide 2: Introduction to IDS**

* **Definition**: An Intrusion Detection System (IDS) monitors network or system activities for malicious activities or policy violations.
* **Types**:
  + Host-Based IDS (HIDS)
  + Network-Based IDS (NIDS)
* **Function**: Alerts administrators about suspicious traffic, without blocking it.

**Slide 3: Importance of IDS**

* Detects security breaches in real-time
* Provides visibility into network traffic
* Helps in forensic analysis after an attack
* Enhances overall security posture
* Meets compliance requirements (e.g., PCI-DSS, HIPAA)

**Slide 4: Limitations of IDS**

* Cannot prevent attacks (only detects)
* False positives/negatives
* Requires constant updates of rule sets
* Needs skilled personnel to manage
* Can be resource-intensive

**Slide 5: Snort Overview**

* Open-source NIDS by Cisco
* Uses rules to detect threats
* Widely adopted, strong community support
* Outputs alerts in various formats

**Slide 6: Installing Snort on Pop!\_OS**

1. **Update system**:

* sudo apt update && sudo apt upgrade -y

1. **Install dependencies**:

* sudo apt install -y snort

1. **Configure Snort**:
   * Choose interface (e.g., wlp4s0)
   * Edit /etc/snort/snort.debian.conf
2. **Test**:

* sudo snort -T -c /etc/snort/snort.conf

**Slide 7: Suricata Overview**

* Developed by OISF
* Multi-threaded, high-performance IDS/IPS
* Can detect, log, and analyze traffic in depth
* Supports modern protocols (HTTP2, TLS, etc.)

**Slide 8: Installing Suricata on Pop!\_OS**

1. **Install Suricata**:

* sudo apt update  
  sudo apt install -y suricata

1. **Verify Installation**:

* suricata --build-info

1. **Run Suricata**:

* sudo suricata -i wlp4s0 -c /etc/suricata/suricata.yaml -v

1. **Install and Update Rules**:

* sudo apt install suricata-update  
  sudo suricata-update

1. **Test**:

* curl http://testmyids.com  
  sudo tail -f /var/log/suricata/fast.log

**Slide 9: Difference Between Snort and Suricata**

| Feature | Snort | Suricata |
| --- | --- | --- |
| Developer | Cisco (Sourcefire) | OISF |
| Performance | Single-threaded | Multi-threaded |
| Protocol Support | Limited | Advanced (HTTP2, TLS, etc.) |
| Output Format | Unified2, syslog | JSON (eve.json), fast.log |
| IPS Capabilities | Yes (with extra setup) | Built-in IDS/IPS mode |

**Slide 10: Testing Suricata with Nmap**

* **Install Nmap**:
* sudo apt install nmap
* **Run Basic Ping Scan**:
* nmap -sn <target\_ip>
* **Run Aggressive Scan**:
* sudo nmap -sS -T4 -A -v <target\_ip>
* **Trigger Suricata Rules**:
  + Watch alerts:
  + sudo tail -f /var/log/suricata/fast.log
  + Check logs:
  + grep -i nmap /var/log/suricata/eve.json

**Slide 11: Conclusion**

* IDS is vital for monitoring and defending networks
* Snort and Suricata are both powerful tools
* Suricata offers more performance and protocol support
* Easy to install and run on Pop!\_OS
* Regular updates and rule management are key to effectiveness

**Slide 12: Questions & Discussion**

* Thank You!
* Questions?