Intro to Anomaly-Based Intrusion Detection/Prevention Systems

Goal

- Provide a general introduction to anomaly-based intrusion detection / intrusion prevention systems.
- Assume that you are addressing students in an introductory cybersecurity course.

Objectives

- Define terminology
- Understand the four states of an IDS
- Discuss Signature Based IDS
- Discuss Anomaly Based IPS
- Demonstrate example of IDS & IPS

Terminology

- **Intrusion**
- **Detection**
- **Prevention**
- **States of IDS**
  - **Positive** – Alarm
  - **Negative –** No Alarm
  - **True** – Attack
  - **False** – No Attack

- **Signature**
- **Anomaly**
- **Intrusion Detection System** - Detects and Monitors only
- **Intrusion Prevention System** - Proactively Try's to stop
- **Signature based detection**
- **Anomaly based detection**

- **Question:** Which is better, anomaly or signature based detection?

Four IDS States

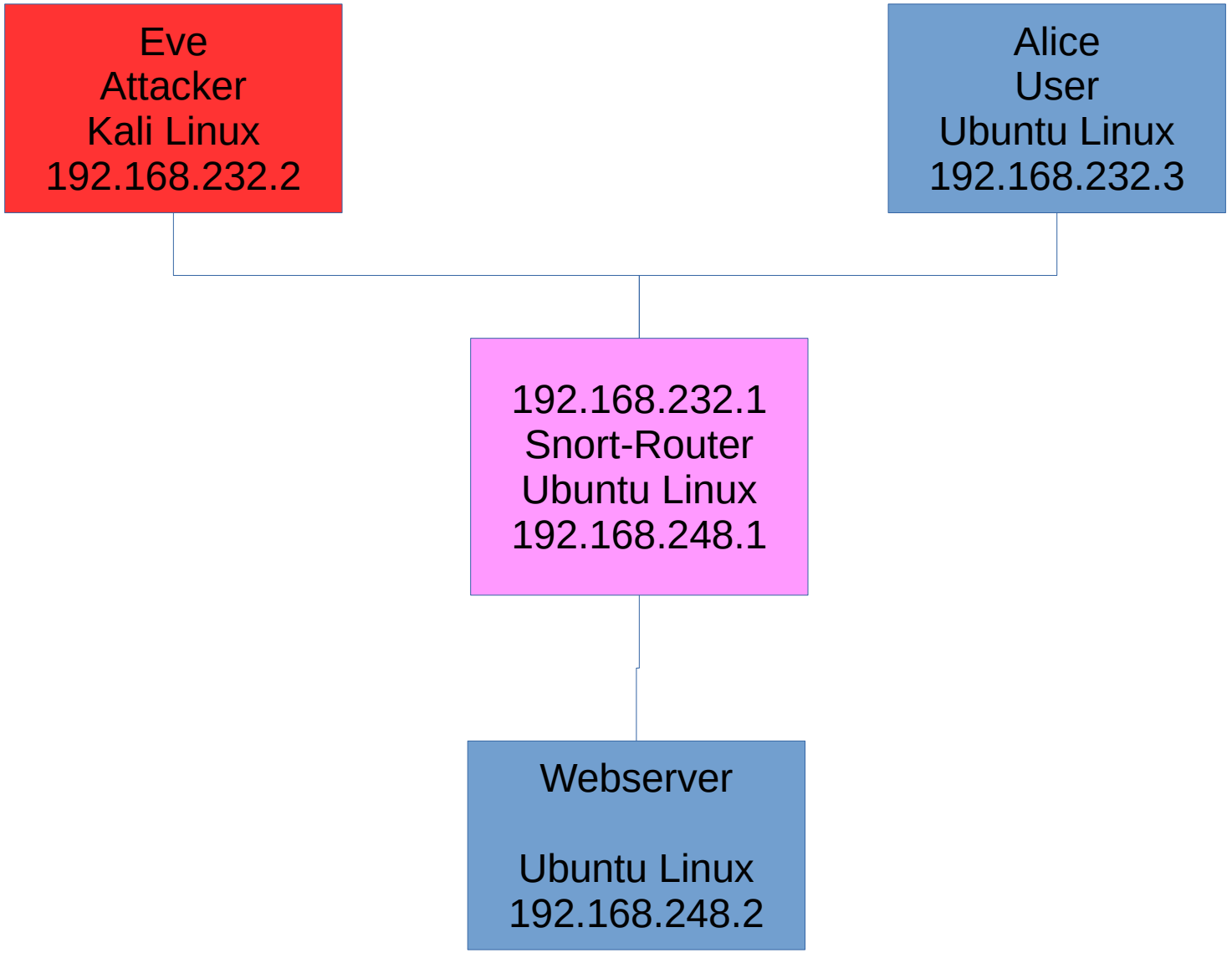
- **True Positive** - Intrusion & Alarm
- **False Negative -** Intrusion & No alarm (Fail to detect intrusion)
- **False Positive** - No Intrusion & Alarm (False alarm)
- **True Negative** - No Intrusion & No Alarm

- **Question:**

  Which is worse when dealing with IDS / IPS?

Four IDS States		
	Intrusion	No Intrusion
Alarm	True Positive	False Positive
No Alarm	False Negative	True Negative

Network Diagram



Example of Signature Based IDS

- Create a Snort rule to detect login attempts to the webserver
- `alert tcp !$HOME_NET any -> $WEBSERVER 80 (msg:”Login attempt on webserver”; content:”Authorization”; sid: 1000990)`

Anomaly Based IDS / IPS

- What is normal behavior for a webserver?
  - How many times a second should a normal user be attempting to login?
- What happens when an attacker tries to guess a users' password?
- Create a Snort rule to prevent brute force login attempts triggered from the IDS rule in the previous slide.
- `rate_filter gen_id 1, sig_id 1000990, track by_src, count 5, seconds 1, new_action drop, timeout 600`

Conclusion

- Defined terminology
- Understand the four states of an IDS
- Discussed Signature Based IDS
- Discussed Anomaly Based IPS
- Demonstrated an example of IDS & IPS