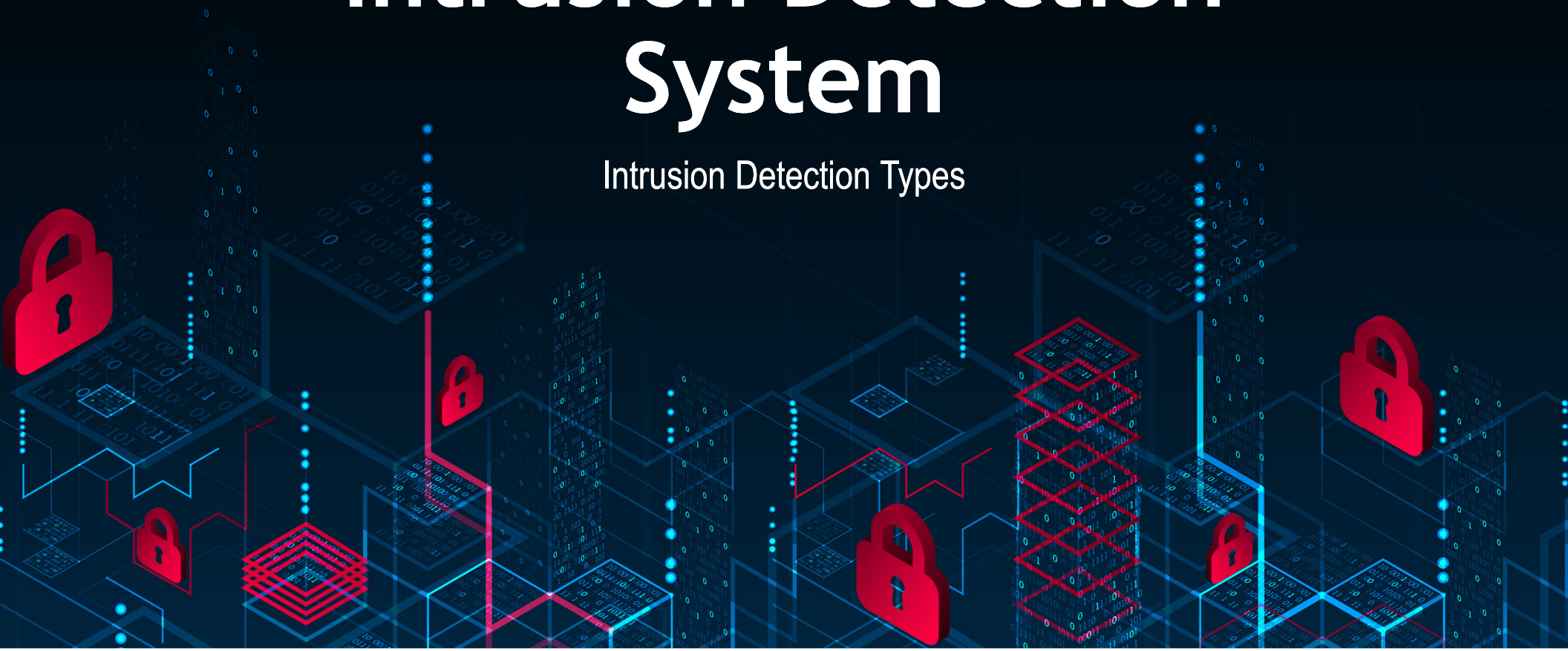
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Intrusion Detection System

Intrusion Detection Types



Video Summary

- IDS Components and Principles
- Example Measures for Intrusion Detection
- Example of Suspicious Activities
- Intrusion Detection Types → Host-based IDS
- Snort

Intrusion Detection Types

- **Host-based IDS**
  - Monitor characteristics of a single computer
- **Distributed host-based IDS**
  - Monitor characteristics on set of computers with central module detecting intrusions
- **Network-based IDS**
  - Monitor network traffic to identify suspicious activities

Distributed Host-Based Intrusion Detection

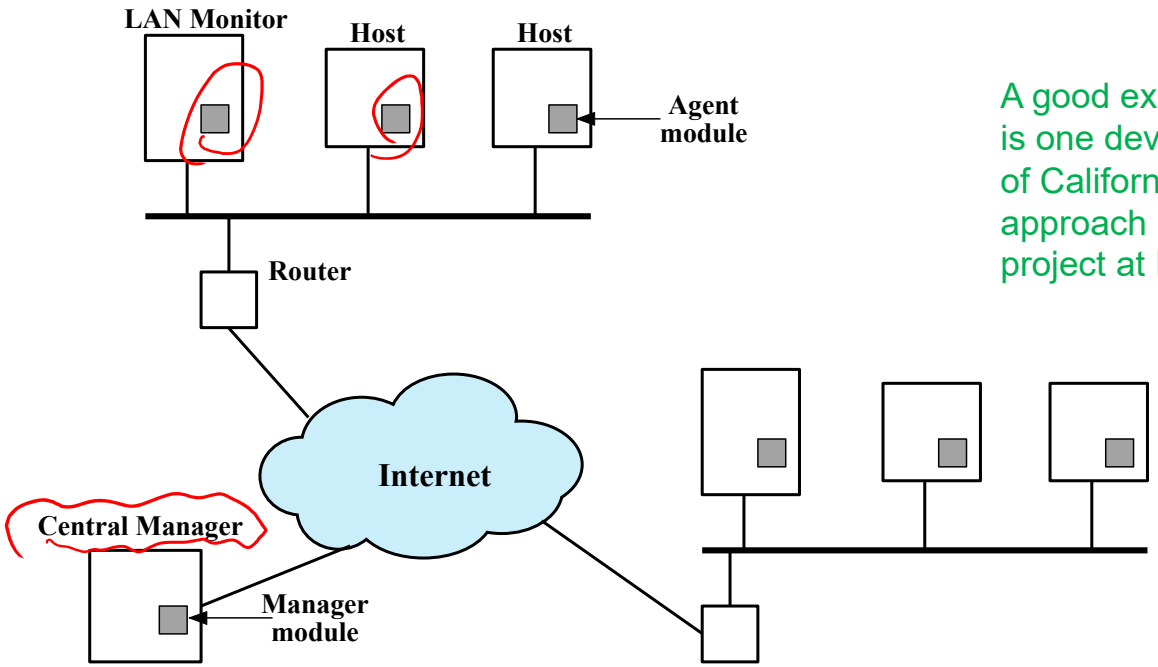
- **Host-based IDS on multiple computers with an organization LAN or internetwork**

  - Host agent collect and analyze audit records on individual hosts
  - LAN monitor agent analyzes LAN traffic
  - Host and LAN monitor agents send alerts to central manager
  - Central manager combines data to detect intrusion

- **Issues**

  - Deal with different audit record formats
  - Data transmitted over network by agents must be secured
  - With central architecture, single point of failure
  - With distributed architecture, complex coordination involved

Architecture for Distributed Intrusion Detection



A good example of a distributed IDS is one developed at the University of California at Davis; a similar approach has been taken for a project at Purdue.

Figure 8.2 Architecture for Distributed Intrusion Detection

Architecture for Distributed Intrusion Detection

- **Host agent module**

An audit collection module operating as a background process on a monitored system. Its purpose is to collect data on security-related events on the host and transmit these to the central manager.

- **LAN monitor agent module**

Operates in the same fashion as a host agent module except that it analyzes LAN traffic and reports the results to the central manager.

- **Central manager module**

Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion.

Architecture for Distributed Intrusion Detection

- **Host agent module**

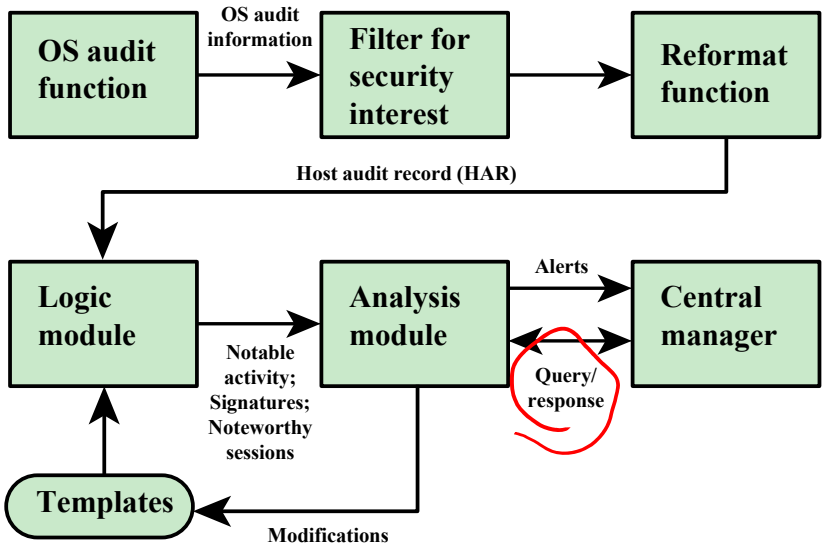
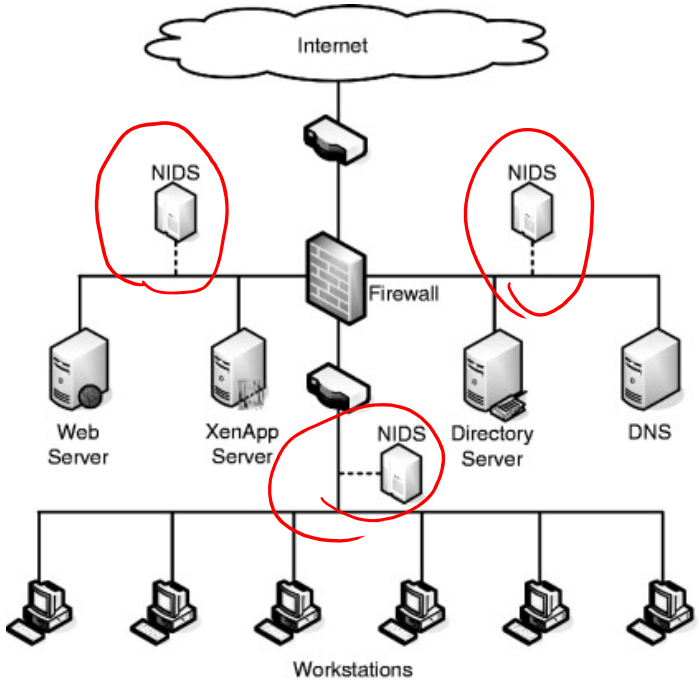


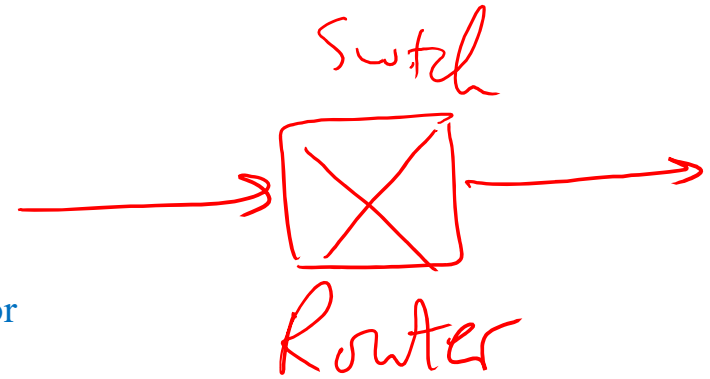
Figure 8.3 Agent Architecture

Network-Based Intrusion Detection (NIDS)

- Monitor traffic at selected points on network using sensors
- Analyze traffic to detect intrusion patterns (at sensors or management servers)



Network-Based Intrusion Detection (NIDS)

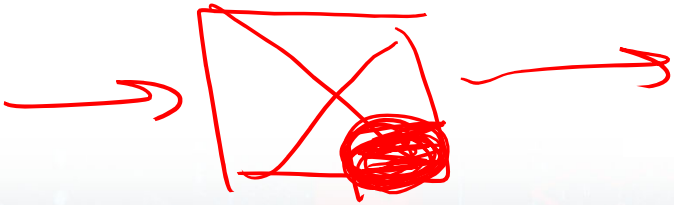


- **Inline sensor (online mode)**

- Inserted into network; analyze traffic as passes through sensor
- Runs as software on existing switch, router or firewall
- Can prevent an attack as soon as detected

- **Passive sensor (offline mode)**

- Monitors copy of traffic
- Extra device that receives copy of traffic, e.g. switch port mirroring
- Minimal impact on performance of traffic



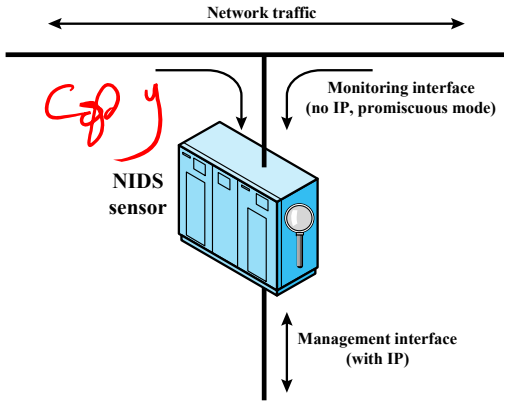


Figure 8.4 Passive NIDS Sensor

Example of NIDS

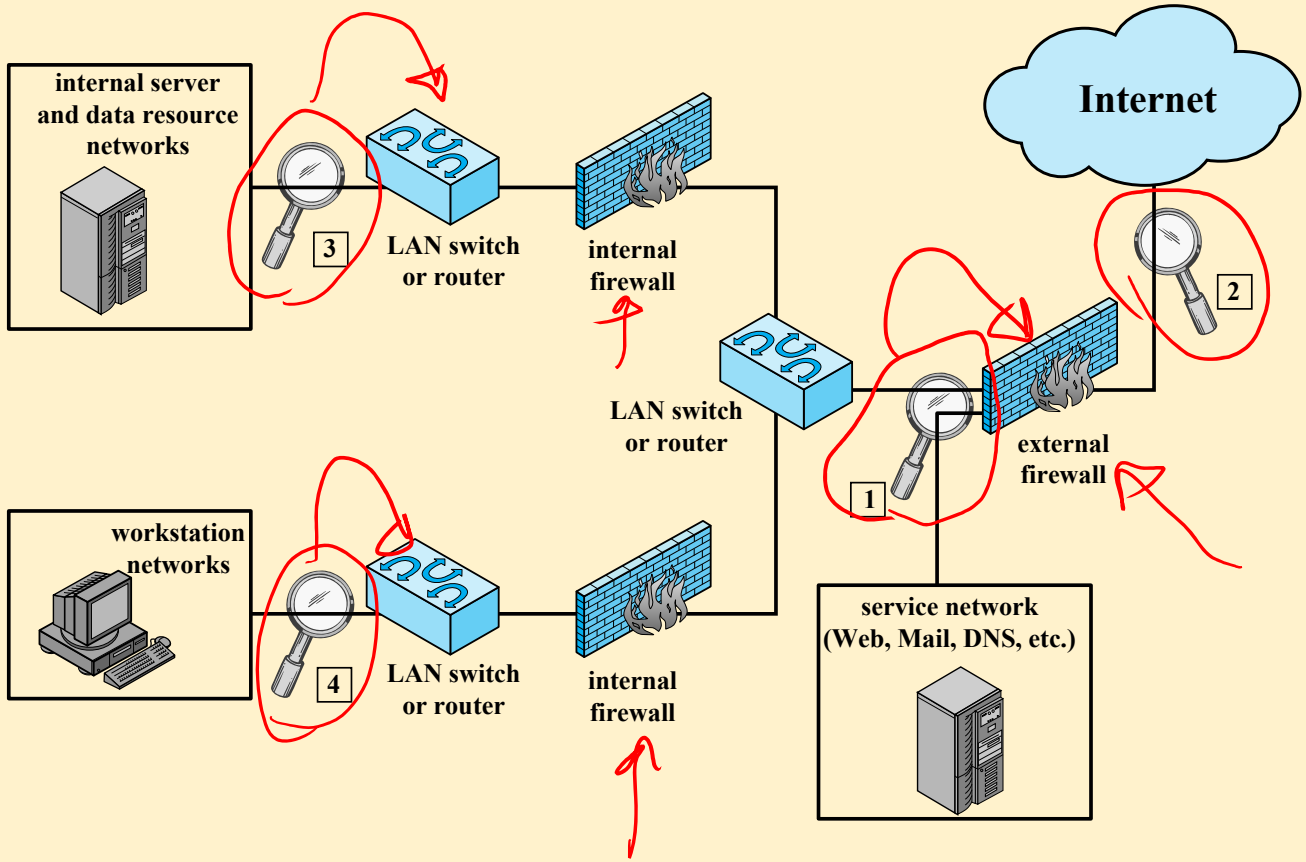


Figure 8.5 Example of NIDS Sensor Deployment

https://www.snort.org

Search... | Rule Doc Search

Documents | Downloads | Products | Community | Talos | Resources | Contact

Sign In

Get started with the world's most powerful detection software

Download Snort and the rules you need to stay ahead of the latest threats

Keep up-to-date with the latest changes and documentation

Get Started

Rules

Documents

Snort 3.0 Beta Available...

Free and open source
Realtime traffic analysis
Packet logging

New to Snort?

Check out the videos and labs on the redesigned Resources page here.

Snort Software (IDS/IPS)

- **Snort is a free open source network IDS/IPS**

✓ Created in 1998 by SourceFire

✓ Acquired and developed by Cisco (purchased SourceFire in 2013)

✓ has the ability to perform real-time traffic analysis and packet logging/analyzer on Internet Protocol (IP) networks.

✓ The program can also be used to detect attacks, including operating system fingerprinting attempts, URL attacks, buffer overflows, server message block probes, and port scans.

Snort Software (IDS/IPS)

- **Snort can be configured as sniffer, packet logger and NID**

- Sniffer: it will read network packets and display them on the console
- Packet logger: it logs packets to the disk
- Network Intrusion Detection: it monitors the network traffic and analyze it against a rule set defined by the user

- Other free IDSes: https://www.upguard.com/blog/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise

Snort Rule Actions

Action	Description
alert	Generate an alert using the selected alert method, and then log the packet.
log	Log the packet.
pass	Ignore the packet.
activate	Alert and then turn on another dynamic rule.
dynamic	Remain idle until activated by an activate rule , then act as a log rule.
drop	Make iptables drop the packet and log the packet.
reject	Make iptables drop the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
sdrop	Make iptables drop the packet but does not log it.

Video Summary

- IDS Components and Principles
- Example Measures for Intrusion Detection
- Example of Suspicious Activities
- Intrusion Detection Types → DIDS & NIDS
- Snort