Intrusion Detection Systems

Objectives and Deliverable

- Understand the concept of IDS/IPS and the two major categorizations: by features/models, and by location. Understand the pros and cons of each approach
- Be able to write a snort rule when given the signature and other configuration info
- Understand the difference between exploits and vulnerabilities

Essential Reading

- The Practical Intrusion Detection Handbook by Paul E. Proctor, Printice Hall
- Intrusion Detection by Edward Amoroso, AT &T Laboratories
- Hacking Exposed: Malware & Rootkits, by Davis, Bodmer and Lemasters, McGraw-Hill

References

- Intrusion Detection by Rebecca G Bace, Macmillan Technical Publishing
- Intrusion Detection System with Snort by Rafeeq Ur Rehman, Prentice Hall
- Intrusion Detection and Prevention by C. Endorf, E Schultz, and J Mellander, Tata McGraw-Hill Edition

Definitions

- Intrusion
  - A set of actions aimed to compromise the security goals, namely
    - Integrity, confidentiality, or availability, of a computing and networking resource
- Intrusion detection
  - The process of identifying and responding to intrusion activities
- Intrusion prevention
  - Extension of ID with exercises of access control to protect computers from exploitation

- Intrusion-detection systems aim at detecting attacks against computer systems and networks or, in general, against information systems.

Why Use an IDS?

- Detection allows:
  - Finding and fixing the most serious security holes
  - Perhaps holding intruders responsible for their actions
  - Limiting the amount of damage an attacker can do

Goals of an IDS

- Run continually
- Be fault tolerant
- Minimize overhead
- Be easily configurable
- Cope with changing system behavior
- Minimize false positives and false negatives

First Line of Defense: The Firewall

- Primary means of securing a private network against penetration from a public network
- An access control device, performing perimeter security by deciding which packets are allowed or denied, and which must be modified before passing
- Can monitor all traffic entering and leaving the private network, and alert the staff to any attempts to circumvent security or patterns of inappropriate use

Firewalls Vs Intrusion Detection Systems

- A firewall monitors the system based on the rules that are set by the user and regulates the activity between the system and the Internet, and IDS monitors the system for unwanted entry and reports or alerts the same to the user.
- Firewall cannot detect security breaches associated with traffic that does not pass through it. Only IDS is aware of traffic in the internal network

Some of the benefits of IDS

- monitors the operation of firewalls, routers, key management servers and files critical to other security mechanisms
- allows administrator to tune, organize and comprehend often incomprehensible operating system audit trails and other logs
- comes with extensive attack signature database against which information from the customers system can be matched
- can recognize and report alterations to data files

The History of Intrusion Detection

- IDS has merged with traditional electronic data processing (EDP) and security audit with optimized pattern matching and statistical techniques
- Before Intrusion Detection , there was audit.
- Audit is defined as process of generating, recording, and reviewing a chronological record of system events.

- The goal of audit includes the following:
  - To assign and maintain personal accountability for system activities.
  - To reconstruct events
  - To access damage
  - To monitor problem areas of system
  - To allow efficient damage recovery
  - To deter improper use of system

Financial audit Vs Security audit

- Financial audit involves tracing the trail of evidences that link a chain of transactions to the summary figures in a financial statement
- Security audit requires additional features for protection of audit mechanism, the system on which it runs, and the audit trail generated by the mechanism.

- Audit trails supported the investigation of problems involving misuse of the system.
- In 1970, the US dept. of Defense (DOD) proposed the concept of trusted systems.
- The trusted systems are defined as systems that employ sufficient hardware and software assurance measures to allow their use for simultaneous processing of a range of sensitive of classified data.

- It imposed 5 security goals for audit mechanism.
  - To allow review of pattern of access and the use of protection mechanisms of the system.
  - To allow the discovery of both insider and outsider attempts to bypass protection mechanisms
  - To allow the discovery of transition of user lesser to greater privileged level
  - To serve as a deterrent to user's attempt to bypass protection mechanisms
  - To serve as a form of user assurance that attempt to bypass protection mechanisms can be recorded and discovered.

Birth of Intrusion Detection

- In 1980, James P Anderson proposed audit reduction, which eliminates redundant or irrelevant records from security audit trail.
- Anderson's report gave emphasis on strategy of a system attacker and optimization of audit trail contents to allow detection of problem. Also discovered some problem associated with masquerade.

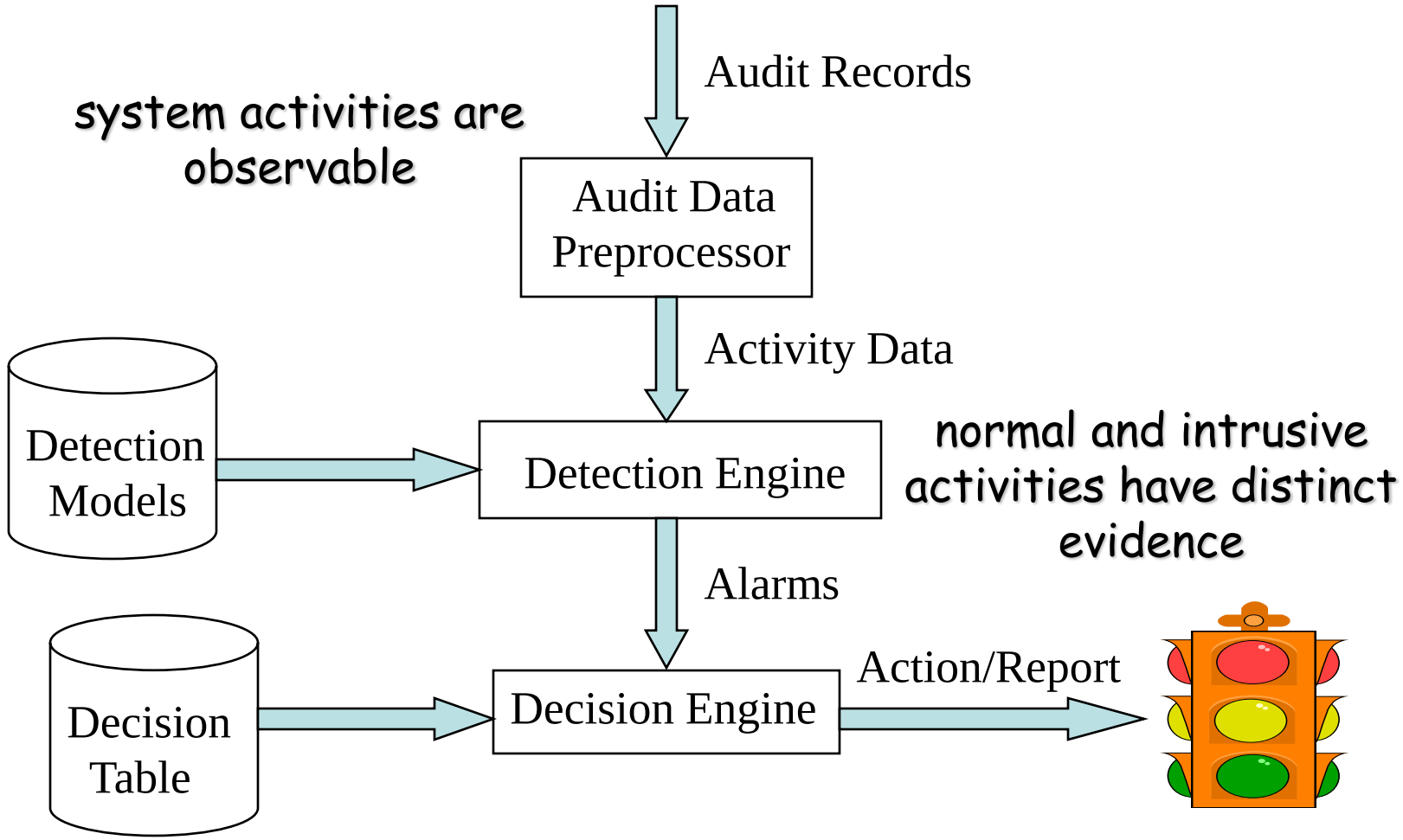
- In 1986, Intrusion Detection Expert System (IDES) was founded. IDES model is based on profiles, data structures that use statistical metrics and models to describe behaviors of system object.
- IDES model used a hybrid architecture, comprising of an anomaly detector and an expert system.

- In 1989, Haystack was designed to help security experts to detect insider abuse
- MIDAS (Multics Intrusion Detection and Alerting System) is the first IDS that monitored an operational system connected to Internet, gave a fascinating view of internet threats

Elements of Intrusion Detection

- Primary assumptions:
  - System activities are observable
  - Normal and intrusive activities have distinct evidence
- Components of intrusion detection systems:
  - From an algorithmic perspective:
    - Features - capture intrusion evidences
    - Models - piece evidences together
  - From a system architecture perspective:
    - Various components: audit data processor, knowledge base, decision engine, alarm generation and responses

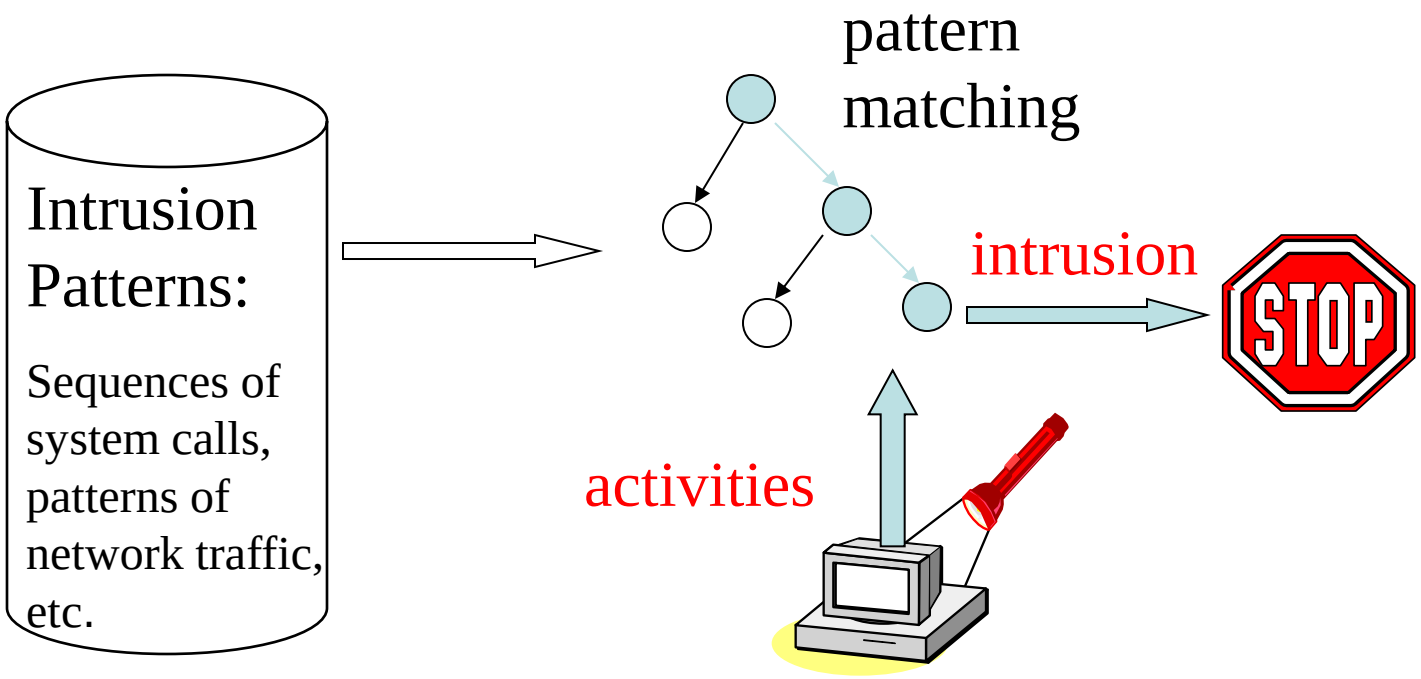
Components of Intrusion Detection System



Intrusion Detection Approaches

- Modeling
  - Features: evidences extracted from audit data
  - Analysis approach: piecing the evidences together
    - Misuse detection (signature-based)
    - Anomaly detection (statistical-based)
- Deployment: Network-based or Host-based
  - Network based: monitor network traffic
  - Host based: monitor computer processes

Misuse Detection



Example: ***if*** (traffic contains "x90+de[^\r\n]{30}") ***then*** "attack detected"

Problems?

Can't detect new attacks

Misuse detection - recognize known attacks

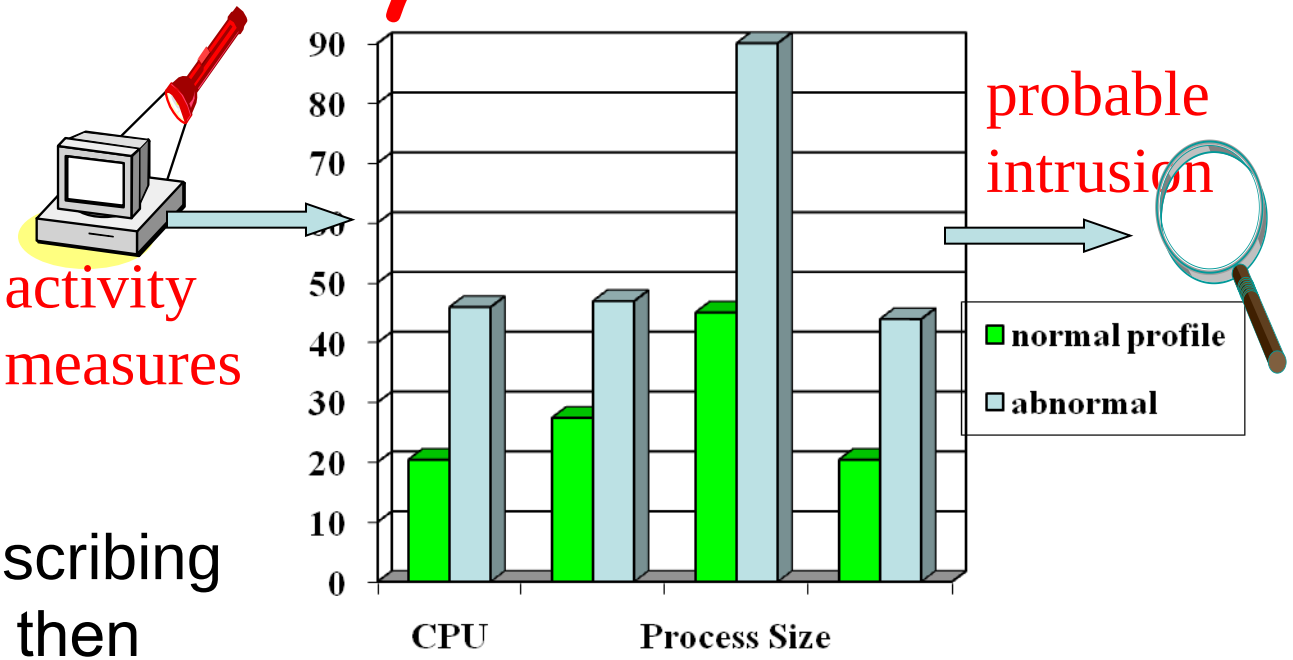
- Define a set of attack *signatures*

- Detect actions that match a signature

Add new signatures often

Examples: ARMD, ASIM, Bro, CSM, CyberCop, GRIDS, Stalker, Tripwire

Anomaly Detection



Define a profile describing "normal" behavior, then detects deviations.

Relatively high false positive rates

- Anomalies can just be new normal activities.
- Anomalies caused by other element faults
  - E.g., router failure or misconfiguration, P2P misconfigure

- Examples: AAFID, MIDAS, NADIR, UNICORN

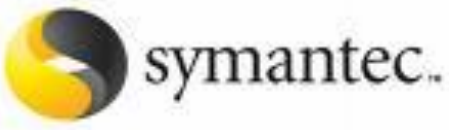
Types of Intrusion Detection System

Based on the sources of the audit information used by each IDS, the IDSs may be classified into

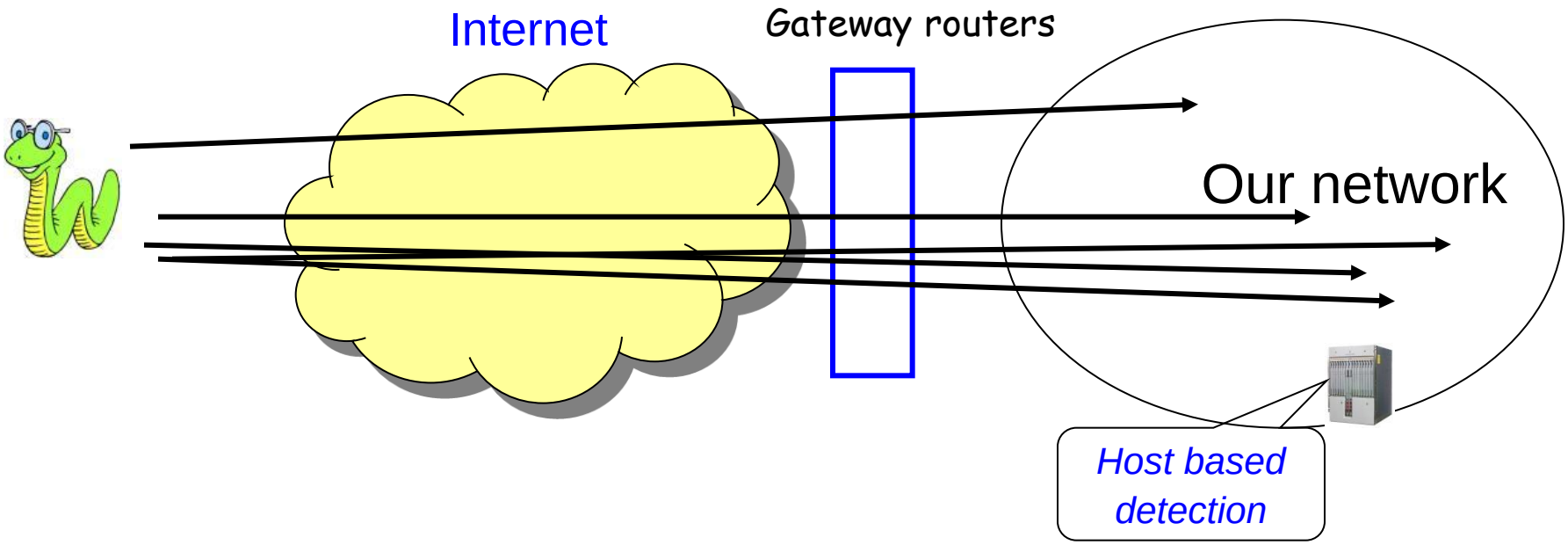
- Host-base IDSs
- Distributed IDSs
- Network-based IDSs

Host-Based IDSs

- Use OS auditing and monitoring mechanisms to find applications taken over by attacker
  - Log all relevant system events (e.g., file/device accesses)
  - Monitor shell commands and system calls executed by user applications and system programs
    - Pay a price in performance if every system call is filtered
- Problems:
  - User dependent: install/update IDS on all user machines!
  - If attacker takes over machine, can tamper with IDS binaries and modify audit logs
  - Only local view of the attack



Network Based IDSs

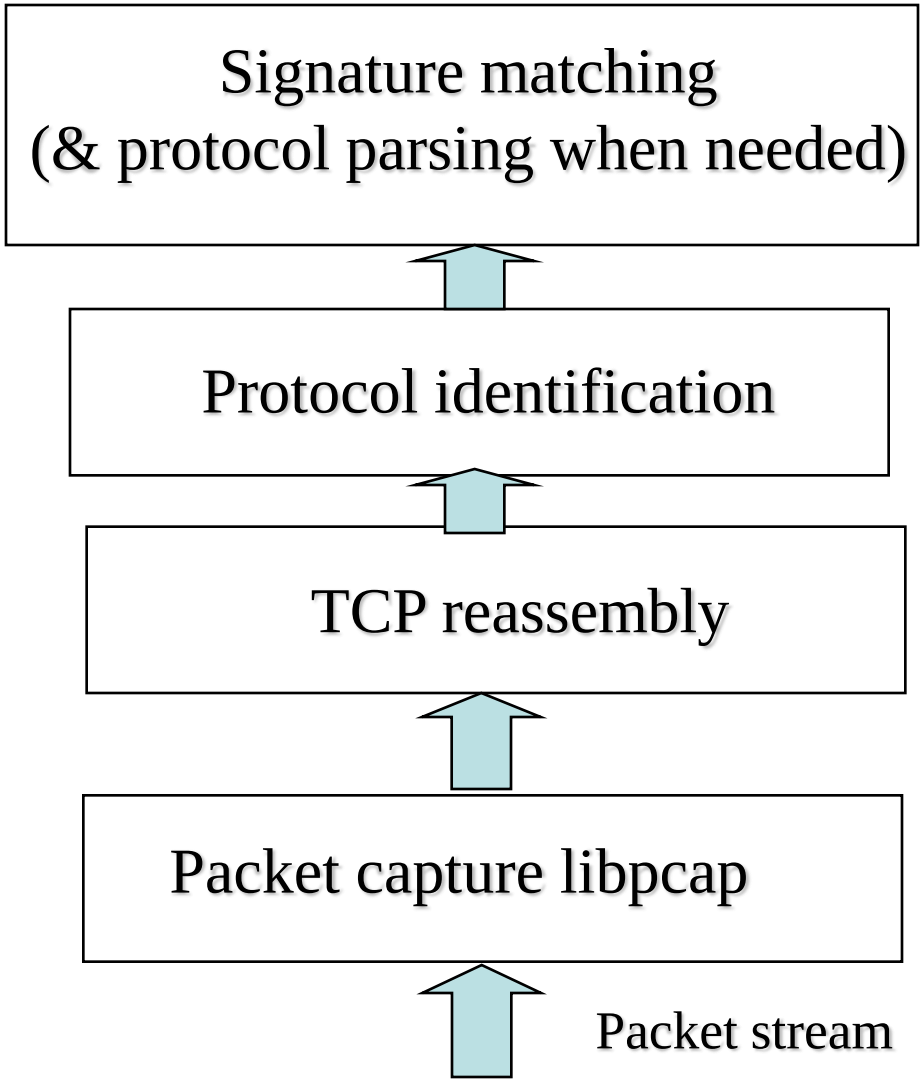


- At the early stage of the worm, only limited worm samples.
- Host based sensors can only cover limited IP space, which has scalability issues. Thus they might not be able to detect the worm in its early stage.

Network IDSs

- Deploying sensors at strategic locations
  - For example, Packet sniffing via *tcpdump* at routers
- Inspecting network traffic
  - Watch for violations of protocols and unusual connection patterns
  - Look into the packet payload for malicious code
- Limitations
  - Cannot execute the payload or do any code analysis !
  - Even DPI gives limited application-level semantic information
  - Record and process huge amount of traffic
  - May be easily defeated by encryption, but can be mitigated with encryption only at the gateway/proxy

Architecture of Network IDS



Requirements of Network IDS

- High-speed, large volume monitoring
  - No packet filter drops
- Real-time notification
- Mechanism separate from policy
- Extensible
- Broad detection coverage
- Economy in resource usage
- Resilience to stress
- Resilience to attacks upon the IDS itself!

Related Tools for Network IDS

- While not an element of Snort, wireshark (used to called Ethereal) is the best open source GUI-based packet viewer
- www.wireshark.org offers:
  - Support for various OS: windows, Mac OS.
- Included in standard packages of many different versions of Linux and UNIX
- For both wired and wireless networks

Related Tools for Network IDS

- Also not an element of Snort, tcpdump is a well-established CLI packet capture tool
  - www.tcpdump.org offers UNIX source
  - http://www.winpcap.org/windump/ offers windump, a Windows port of tcpdump

Problems with Current IDSs

- Inaccuracy for exploit based signatures
- Cannot recognize unknown anomalies/intrusions
- Cannot provide quality information for forensics or situational-aware analysis
  - Hard to differentiate malicious events with unintentional anomalies
    - Anomalies can be caused by network element faults, e.g., router misconfiguration, link failures, etc., or application (such as P2P) misconfiguration
  - Cannot tell the situational-aware info: attack scope/target/strategy, attacker (botnet) size, etc.

- cannot conduct investigations of attacks without human intervention
- cannot intuit the contents of organizational security policy
- cannot compensate for weaknesses in network protocols
- cannot compensate for weak identification and authentication mechanisms
- capable of monitoring network traffic but to a certain extent of traffic level