Intrusion Detection

Intrusion Detection

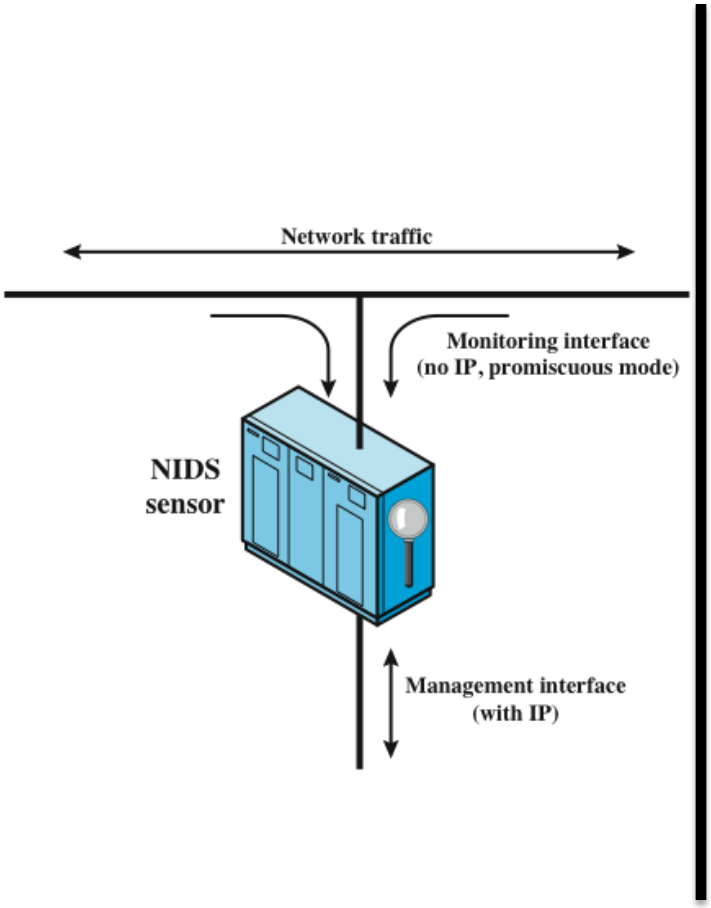
- Security Intrusion:
  - “a security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system”
- Intrusion Detection:
  - “A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts t access system resources in an unauthorized manner.”
- Components
  - Sensors – collect data (e.g., network packets, log files, system calls)
  - Analyzer – receives input from sensors and analyzes it for
  - User Interface – interface for user to view output of system and control its behavior

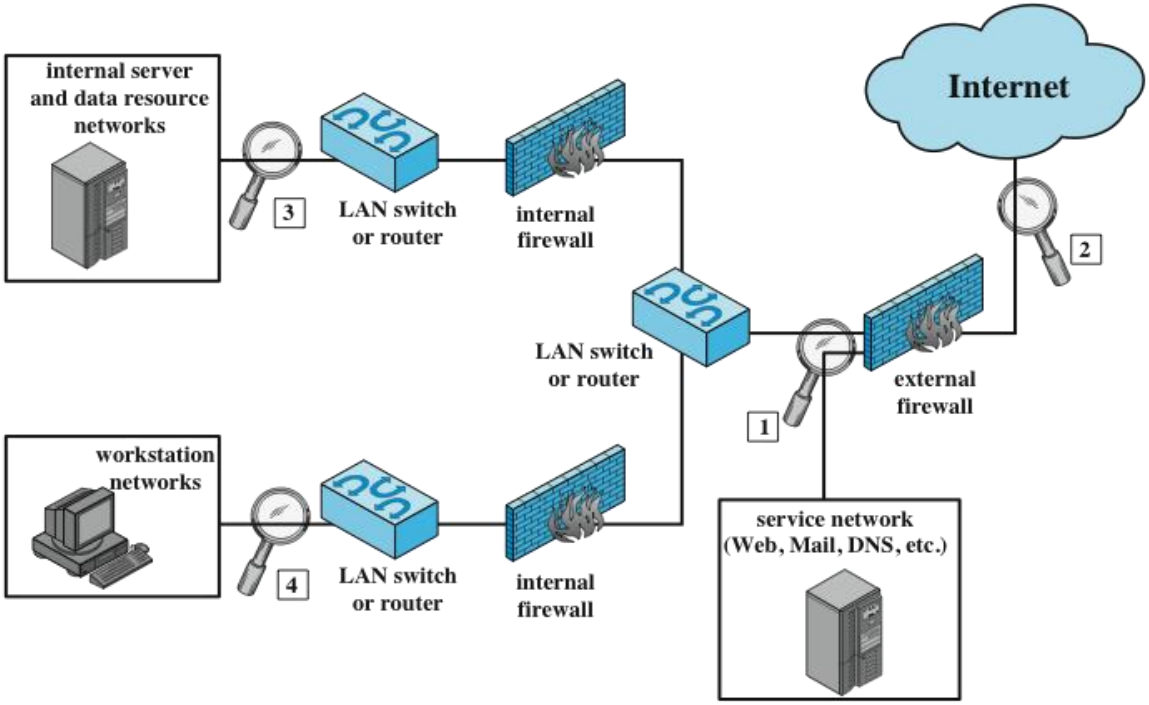
IDS Categories

- Sensor Types
  - Host-based (HIDS) – sensors collect data from hosts for malicious processes, network stack activity, modified files, etc.
  - Network-based (NIDS) – sensors collect data from network
  - Hybrid – combine information from both network and hosts

- Analysis Types
  - Signature based – use set of know attack patterns that are compared with current sensor data (e.g., Snort)
  - Anomaly based – compare current data to collection of past data, assumes deviation from past patterns (or anomalies) are attacks

NIDS Sensor Deployment





Anomaly vs Signature-based IDS

Anomaly Detection

- Overview:
  - Develop model of normal behavior and compare incoming events

- Approaches
  - Statistical – produce statistical profile of network traffic
  - Knowledge-based – use expert system to classify behavior according to rules
  - Machine learning – automatically determining classification based on traisning data

- Strength
  - Can detect new/unknown attacks!!!
- Weakness
  - Many benign anomalies (e.g., network reconfiguration, system upgrades, new programs)
  - Excessive False Positives
  - Attacks that are not anomalies?

Detection Categories

		Alarm Raised	
		Yes	No
Attack Present	Yes	True Positive	False Negative
	No	False Positive	True Negative

- IDS requires small
  - False positives
    - wastes money/resources investigating non-attack
  - False negatives
    - missed attack results in violation of security policy
  - Base Rate Fallacy
    - Small number of intrusions, vs large number of non-malicious traffic
    - Accurate IDS will still raise large number of false positives

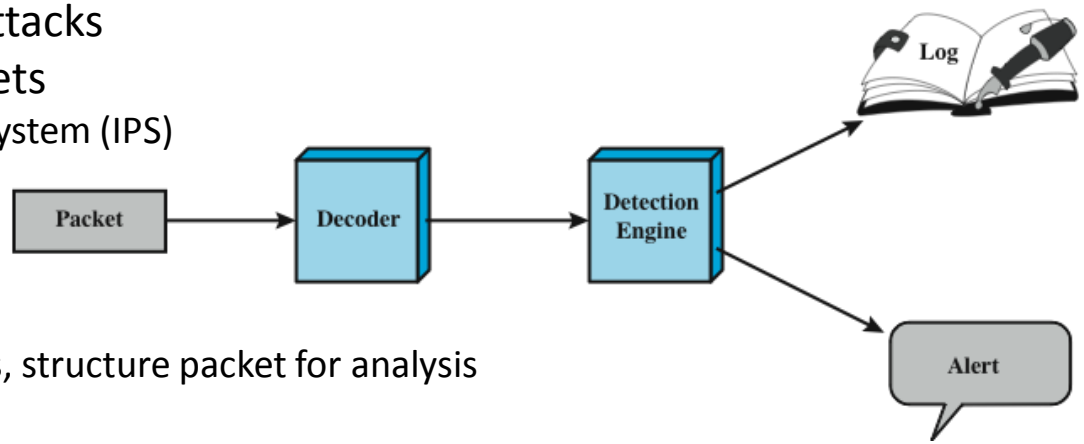
Signature Detection

- Overview:
  - maintain collection of known patterns of malicious data, compare incoming network traffic to patterns
- Strength
  - Low False Positive rate (if rules created correctly)
- Weakness
  - Can’t detect novel (0-day) attacks, detection only works when it has previous
- Example:
  - Snort IDS

Snort IDS

- Open- source signature based IDS
  - Based on large set of “rules”/signatures of known attacks

- Modes
  - Passive – only detect attacks
  - Inline – can block packets
    - Intrusion Prevention System (IPS)



- Architecture
  - Decoder
    - decode protocol layers, structure packet for analysis
  - Detection Engine
    - analyzes packet vs set of rules
  - Logger/Alerter
    - perform necessary response

Snort Rules

- Action: what do to when you identify a packet
  - Examples: alert, log, pass, drop, reject, activate, etc
- Protocol, Port, IP Address, Direction
  - Example: “tcp any any -> 192.168.1.0/24 111”
- Options
  - General – information without impact on detection
    - Examples: msg, ref(URL), classtype, priority
  - Payload – specify packet payload information
    - Example: content, offset, pcre, http_header,
  - Non-payload – specify non-payload data
    - Example: ttl, seq, ack,
  - Post-detection – specify rules for after rule operates
    - Example: resp, react, session
- More info here (http://manual.snort.org/node27.html)

Snort Rule Examples

```
Alert tcp $EXTERNAL_NET any -> $HOME_NET any\
        (mgs: “SCAN SYN FIN” flags: SF, 12;\
        reference: arachnids, 198; classtype: attempted recon;)
```

```
Alert tcp $EXTERNAL_NET any -> any any
        (msg:"Heartbleed Scan Detected - Metasploit - Pattern 1";
        flow:to_server,established; content:"|18 03 02 00 03 01|";  rawbytes;
        classtype:heartbleed-information-leak; sid:4560000005; rev:1;)
```

More Examples

- Port Scan
  - scan.rules
- Ping Scan
  - icmp.rules
- SQL Injection
  - community-sql-injection.rules