CS-552

CYBER FORENSICS

IDS

Intruders

significant problem of networked systems

- hostile/unwanted trespass
- from benign to serious

user trespass

- unauthorized logon, privilege abuse

software trespass

- virus, worm, or trojan horse

classes of intruders:

- masquerader, misfeasor, clandestine user

Security Intrusion and Intrusion Detection – Def’ns from RFC 2828

Security Intrusion

a security event, or combination of multiple security **events**, that constitutes a security **incident** in which an **intruder** gains, or attempts to gain, **access** to a system (or system resource) **without** having **authorization** to do so.

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 to access system resources in an unauthorized manner.

Examples of Intrusion

remote root compromise

web server defacement

guessing / cracking passwords

copying / viewing sensitive data / databases

running a packet sniffer to obtain username/passwords

impersonating a user to reset/learn password

- Mostly via social engineering, phishing

using an unattended and logged-in workstation

Intruder Types and Behaviors

Three broad categories

- Hackers
- Criminals
- Insiders

Hackers

- motivated by “thrill” and “status/reputation”
  - hacking community is a strong meritocracy
  - status is determined by level of competence
- benign intruders might be tolerable
  - do consume resources and may slow performance
  - can’t know in advance whether benign or malign
- What to do
  - IDS (Intrusion Detection Systems), IPS (Intrusion Prevention System), VPNs can help to counter
- Awareness of intruder problems led to establishment of CIRTs
  - Computer/Cyber Incident Response Teams
  - collect / disseminate vulnerability info / responses

Criminals / Criminal Enterprises

Here the main motivation is to make money

Now ~~the common threat is *organized groups of cyber criminals*~~

- May be employed by a corporation / government
- Most of the time, loosely affiliated gangs
- Typically young
- often Eastern European, Russian, Southeast Asian

common target is financial institutions, bank accounts and credit cards on e-commerce servers

criminal hackers usually have specific targets

once penetrated act quickly and get out

IDS may help but less effective due to quick-in-and-out strategy

sensitive data needs strong data protection (e.g. credit card numbers)

Strong authentication would also help (2-factor auth.)

Insider Attacks

Most difficult to detect and prevent

- employees have access & system knowledge

Attackers are motivated by revenge / feeling of entitlement

- when employment terminated
- taking customer data when moving to competitor

IDS/IPS may help but also need extra precautions

- least privilege (need-to-know basis)
- monitor logs
- DLP (data loss prevention) tools – sw agents monitoring user behaviors
- Upon termination revoke all rights and network access

Insider Behavior Example

1. create accounts for themselves and their friends
2. access accounts and applications they wouldn't normally use for their daily jobs
3. conduct furtive instant-messaging chats
4. visit web sites that cater to disgruntled employees
5. perform large downloads, file copying and printing
6. access the network during off hours.

Intrusion Detection Systems (IDS)

IDS classification

- Host-based IDS: monitor single host activity
- Network-based IDS: monitor network traffic

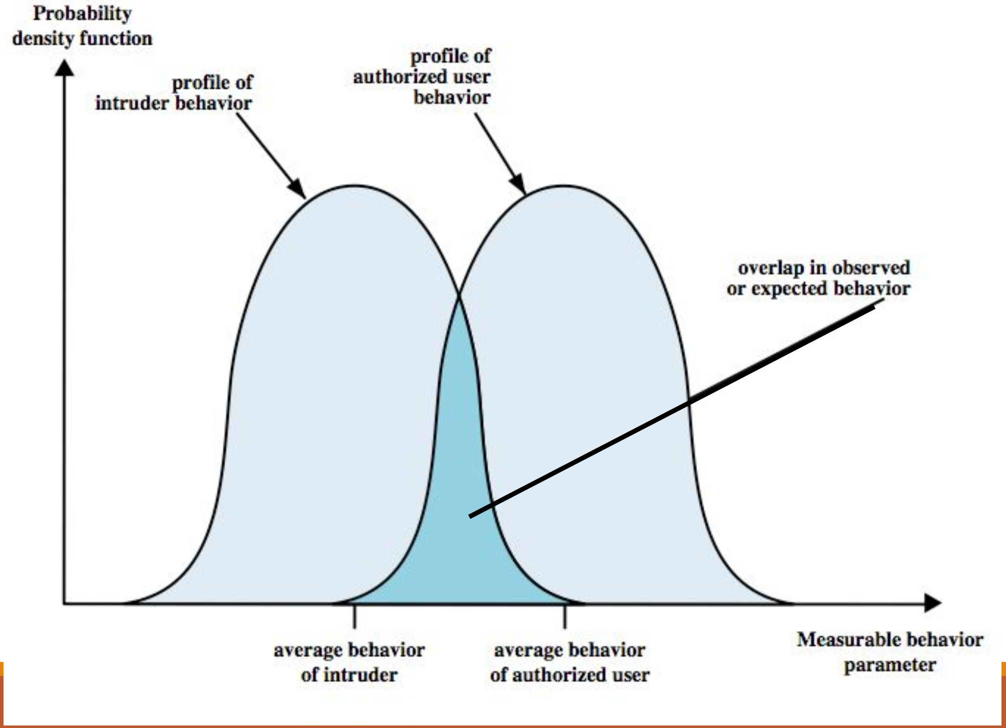
logical components:

- Sensors
  - collect data from various sources such as log files, network packets
  - sends them to the analyzer
- Analyzers
  - process data from sensors and determine if intrusion has occurred
  - may also provide guidance for the actions to take
- user interface
  - acts as a console
  - view the output and manage the behavior

IDS Principle

Main assumption: intruder behavior differs from legitimate user behavior

- expect overlaps as shown
- problems
  - false positives: authorized user identified as intruder
  - false negatives: intruder not identified as intruder


Probability density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter

IDS Requirements

run continually with minimal human supervision

be fault tolerant

resist subversion

minimal overhead on system

scalable, to serve a large numbe of users

configured according to system security policies

allow dynamic reconfiguration

Host-Based IDS

specialized software to monitor system activity to detect suspicious behavior

- primary purpose is to detect intrusions, log suspicious events, and send alerts
- can detect both external and internal intrusions

two approaches, often used in combination:

- signature detection
  - attack patterns are defined and they are used to decide on intrusion
- anomaly detection
  - collection of data related to the behavior of legitimate users
  - Statistical tests are applied to observed behavior
    - threshold detection – applies to all users
    - profile based – differs among the users

Audit Records

A fundamental tool for intrusion detection

Two variants:

- Native audit records - provided by OS
  - always available but may not contain enough info
- Detection-specific audit records
  - collects information required by IDS
  - additional overhead but specific to IDS task

Anomaly Detection

Threshold detection

- Checks excessive event occurrences over time
- Crude and ineffective intruder detector per se
- Creates lots of false positives/negatives due to
  - Variance in time
  - Variance accross users

Profile based

- Characterize past behavior of users and groups
- Then, detect significant deviations
- Based on analysis of audit records
  - example metrics: counter, guage, interval timer, resource utilization
  - analysis methods: mean and standard deviation, multivariate, markov process, time series (next slide)

Profile based Anomaly Detection - Analysis Methods

Mean and standard deviation

- of a particular parameter
- Not good (too crude)

Multivariate analysis

- Correlations among several parameters (ex. relation between login freq. and session time)

Markov process

- Considers transition probabilities

Time series analysis

- Analyze time intervals to see sequences of events happening rapidly or slowly

All statistical methods using AI, Mach. Learning and Data Mining techniques.

Signature Detection

Observe events on system and applying a set of rules to decide if intruder

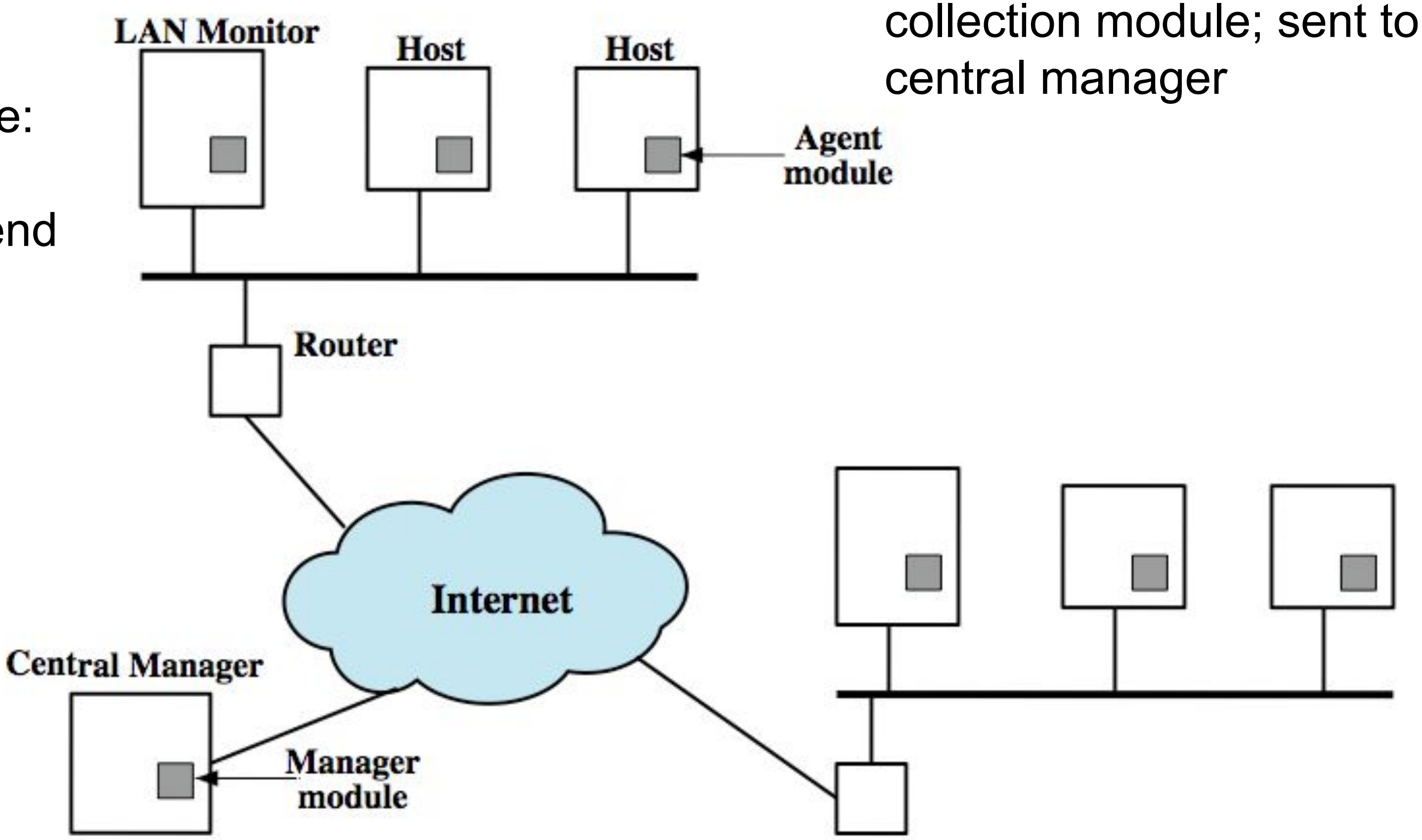
Approaches:

- rule-based anomaly detection
  - analyze historical audit records for expected behavior, then match with current behavior
- rule-based penetration identification
  - rules identify known penetrations or possible penetrations due to known weaknesses
  - rules are mostly OS specific
  - rules obtained by analyzing attack scripts from Internet
    - supplemented with rules from security experts of target system

Distributed Host-Based IDS

main idea: coordination and cooperation among IDSs across the network

LAN Monitor agent module: analyze LAN traffic and send to Central Manager



Host agent module: audit collection module; sent to central manager

Central Manager Module: Analyze and correlate data received from other modules

Architecture

Network-Based IDS

network-based IDS (NIDS)

- monitor traffic at selected points on a network to detect intrusion patterns
  - in (near) real-time
- may examine network, transport and/or application level protocol activity directed toward the system to be protected
  - Only network packets, no software activity examined

System components

- A number of sensors to monitor packet traffic
- Management server(s) with console (GUI)

Analysis can be done at sensors, at management servers or both

Network-Based IDS

Types of sensors

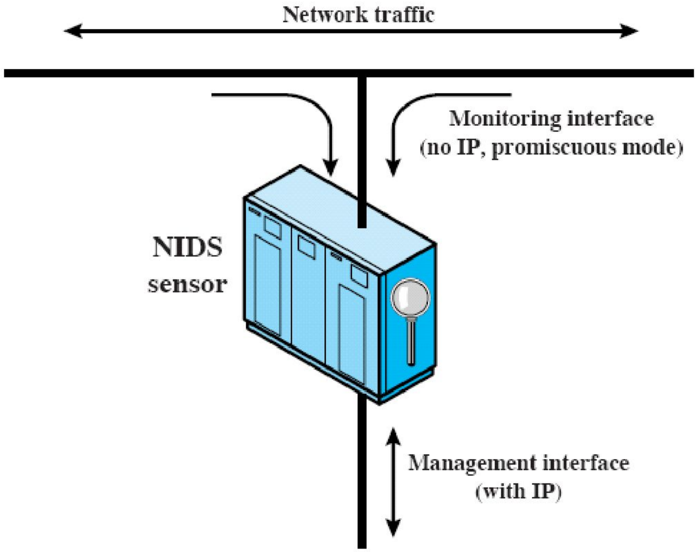
- inline and passive

Inline sensors

- Inserted into a network segment
- Traffic pass through
- possibly as part of other networking device (e.g. router, firewall)
  - No need for a new hardware; only new software
- May create extra delay
- Once attack is detected, traffic is blocked
  - Also a prevention technique

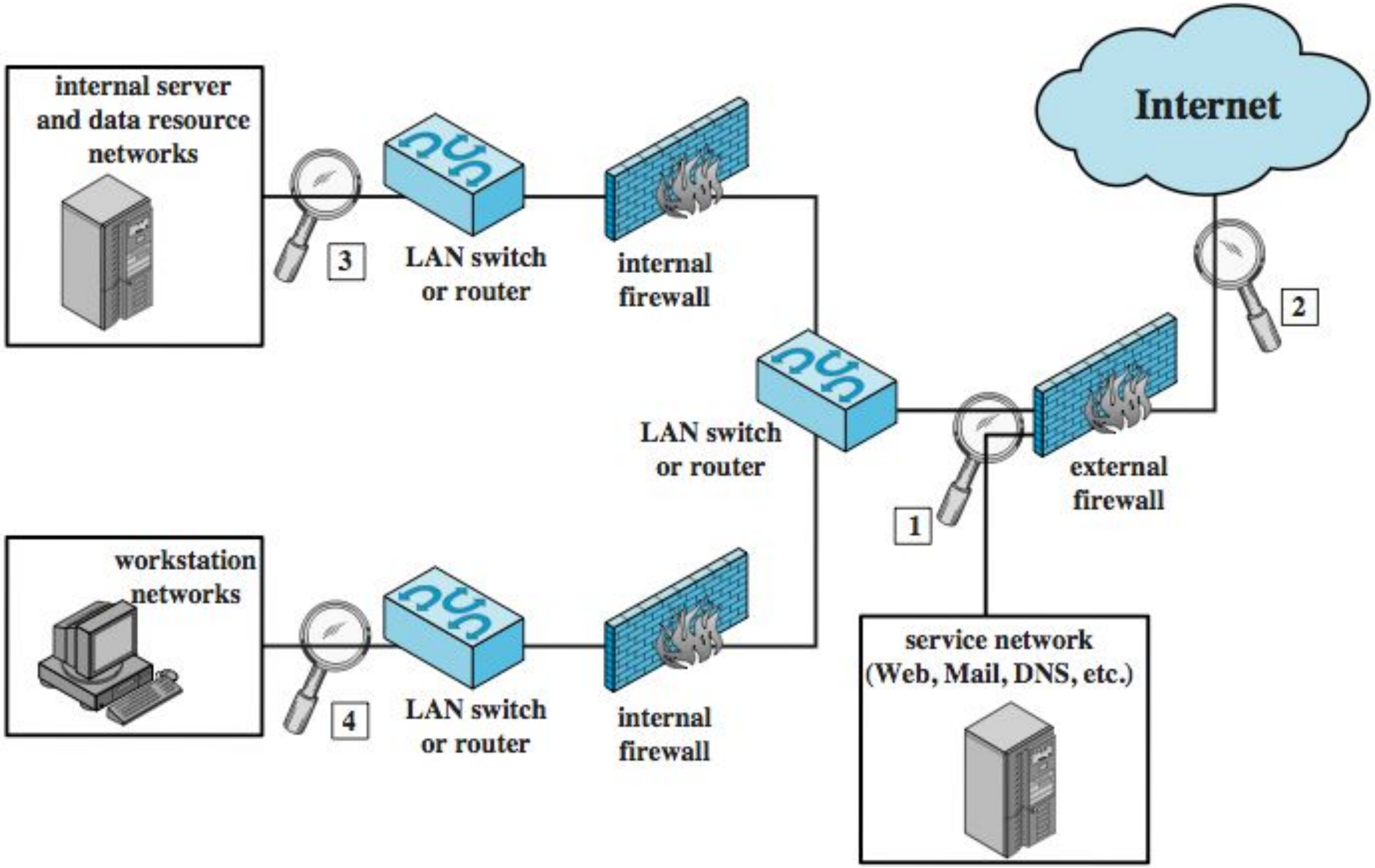
Passive sensors

- monitors copy of traffic at background
  - Traffic does not pass through it, so there is no blocking capability
- More efficient, therefore more common



Passive sensor

NIDS Sensor Deployment



Intrusion Detection Techniques in NIDS

signature detection

- at application (mostly), transport, and network layers
- Attack patterns are detected in packets

anomaly detection – attacks that cause abnormal behaviors are detected

- denial of service attacks, scanning attacks

when potential violation detected, sensor sends an alert and logs information

Honeypots

Decoy systems

- filled with fabricated info
  - appers to be the real system with valuable info
  - legitimate users would not access
- instrumented with monitors and event loggers
- divert and hold attacker to collect activity info
- without exposing production (real) systems

If there is somebody in, then there is an attack

- benign or malicious

Initially honeypots were single computer

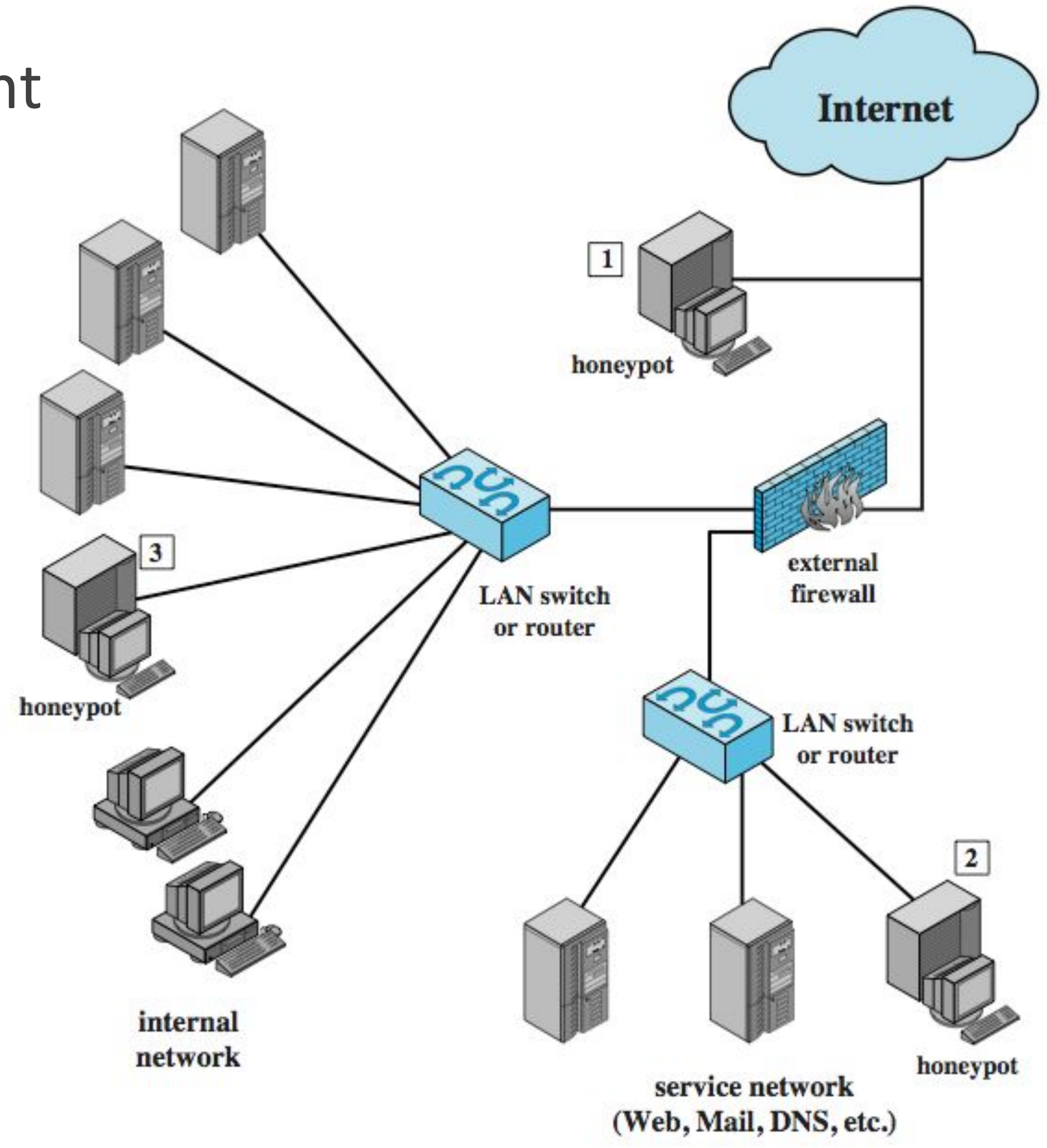
- now network of computers that emulate the entire enterprise network

Honeypot Deployment

1. Outside firewall: good to reduce the burden on the firewall; keeps the bad guys outside

2. As part of the service (DMZ) network: firewall must allow attack traffic to honeypot (risky)

3. As part of the internal network: same as 2; if compromised riskier; advantage is insider attacks can be caught



An Example IDS: Snort

Lightweight IDS

- open source
- Portable, efficient
- easy deployment and configuration
- May work in host-based and network-based manner

Snort can perform

- real-time packet capture and rule analysis

Sensors can be inline or passive

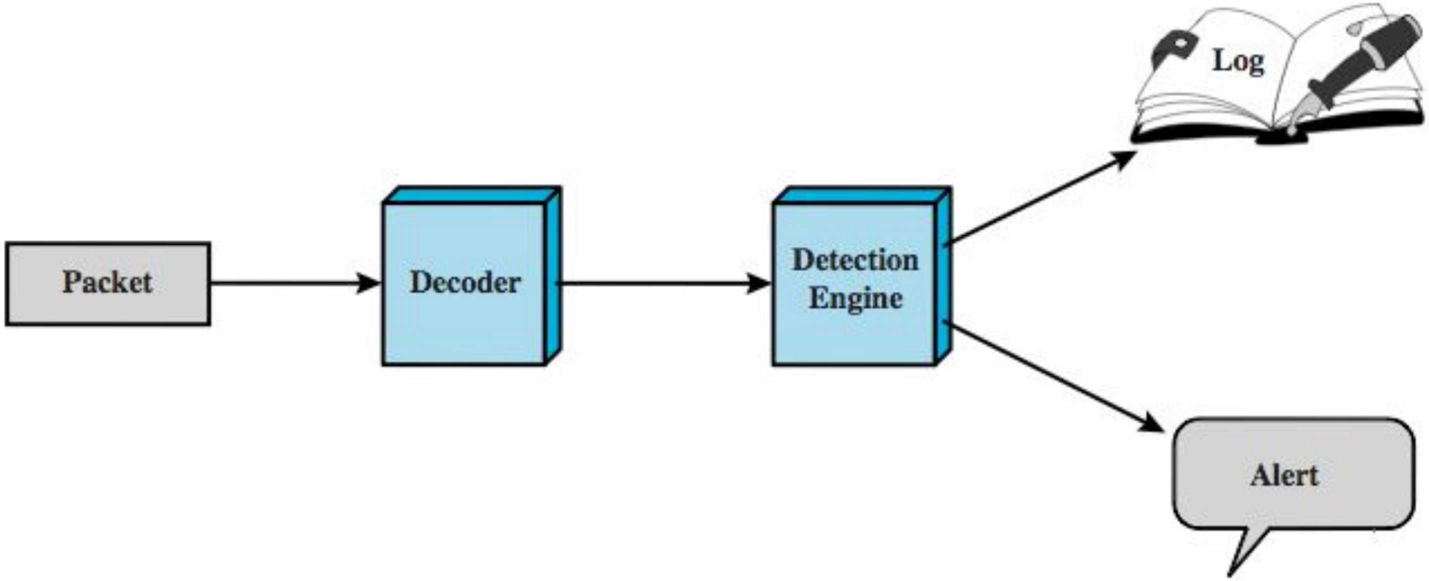
- In inline case, Snort can also be used as IPS

Snort Architecture

Packet Decoder: parses the packet headers in all layers

Detection Engine: actual IDS. Rule-based analysis.

If the packet matches a rule, the rule specifies logging and alerting options



SNORT Rules

Snort uses a simple, flexible and effective rule definition language

- But needs training to be an expert on it

Each rule has a fixed header and zero or more options

Header fields

- action: what to do if matches – alert, drop, pass, etc.
- protocol: analyze further if matches - IP, ICMP, TCP, UDP
- source IP: single, list, any, negation
- source port: TCP or UDP port; single, list, any, negation
- direction: unidirectional (->) or bidirectional (<->).
- dest IP, dest port: same format as sources

SNORT Rules

Many options

- Different categories, see table 6.5 for the list
- Other header fields can be checked using options

Option format

- *Keyword*: *arguments*;

Several options can be listed separated by semicolon

- Options are written in parentheses

example rule to detect TCP SYN-FIN attack:

```
Alert tcp $EXTERNAL_NET any -> $HOME_NET any \
(msg: "SCAN SYN FIN"; flags: SF;)
```

Intrusion Prevention Systems (IPS)

Later addition to terminology of security products

Two Interpretations of IPS

- inline network or host-based IDS that can block traffic
- functional addition IDS capabilities to firewalls

An IPS can block traffic like a firewall, but using IDS algorithms

- may be network or host based

Inline Snort is actually an IPS