Chapter 6: Intrusion Detection

Information Security

Nguyễn Đăng Quang

Fall 2017

Goals

- Distinguish among various types of intruder behavior patterns.
- Understand the basic principles of and requirements for intrusion detection.
- Discuss the key features of host-based intrusion detection.
- Discuss the key features network-based intrusion detection.
- Define the intrusion detection exchange format.
- Explain the purpose of honeypots.
- Present an overview of Snort.

Defense in Depth

- Multiple layers of defense mechanisms

Intruder

- Who is likely intruder?
  - May be outsider who got thru firewall
  - May be evil insider
- What do intruders do?
  - Launch well-known attacks
  - Launch variations on well-known attacks
  - Launch new/little-known attacks
  - “Borrow” system resources
  - Use compromised system to attack others. etc.

Example of intrusion

- Remote root compromise
- Web server defacement
- Guessing/cracking passwords
- Copying databases containing credit card numbers
- Viewing sensitive data without authorization
- Running a packet sniffer
- Distributing pirated software
- Using an unsecured modem to access internal network
- Impersonating an executive to get information
- Using an unattended workstation

Intruder behavior

- Target acquisition and information gathering
- Initial access
- Privilege escalation
- Information gathering or system exploit
- Maintaining access
- Covering tracks

Example of Intruders behavior

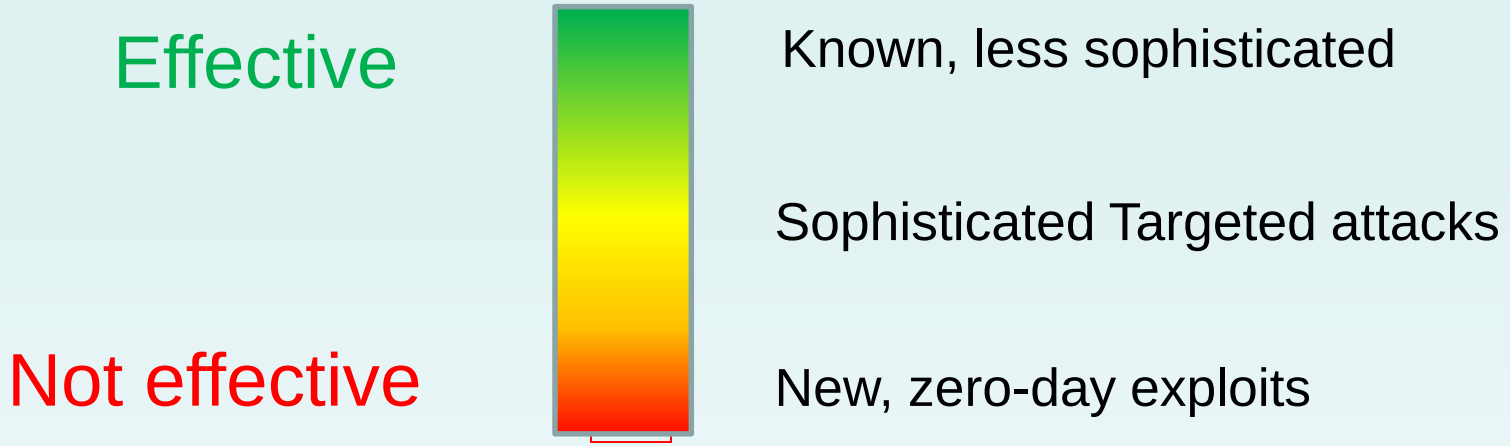
- Student read textbook p.271, 272

Intrusion Detection

- In spite of intrusion prevention, bad guys will sometime get in.
- Intrusion detection systems (**IDS**)
  - Detect attacks in progress (or soon after)
  - Look for unusual or suspicious activity
- IDS evolved from log file analysis.
- IDS is currently a **hot** research topic.
- How to respond when intrusion detected?

Intrusion Detection System

- As attack techniques become more sophisticated, IDS will become less effective. For example, attackers can blend attack traffic with normal activities so that it is very hard to detect such attacks.



IDS - Logical Components

Sensors:

- Sensors are responsible for collecting data. The input for a sensor may be any part of a system that could contain evidence of an intrusion.
- Types of input to a sensor includes network packets, log files, and system call traces. Sensors collect and forward this information to the analyzer.

IDS – Logical Components

Analyzers:

- receive input from one or more sensors or from other analyzers.
- The output of this component is an indication or include evidence supporting the conclusion that an intrusion occurred.
- The analyzer may provide guidance about what actions to take as a result of the intrusion.

IDS - Logical Components

User interface:

The user interface to an IDS enables a user to view output from the system or control the behavior of the system.

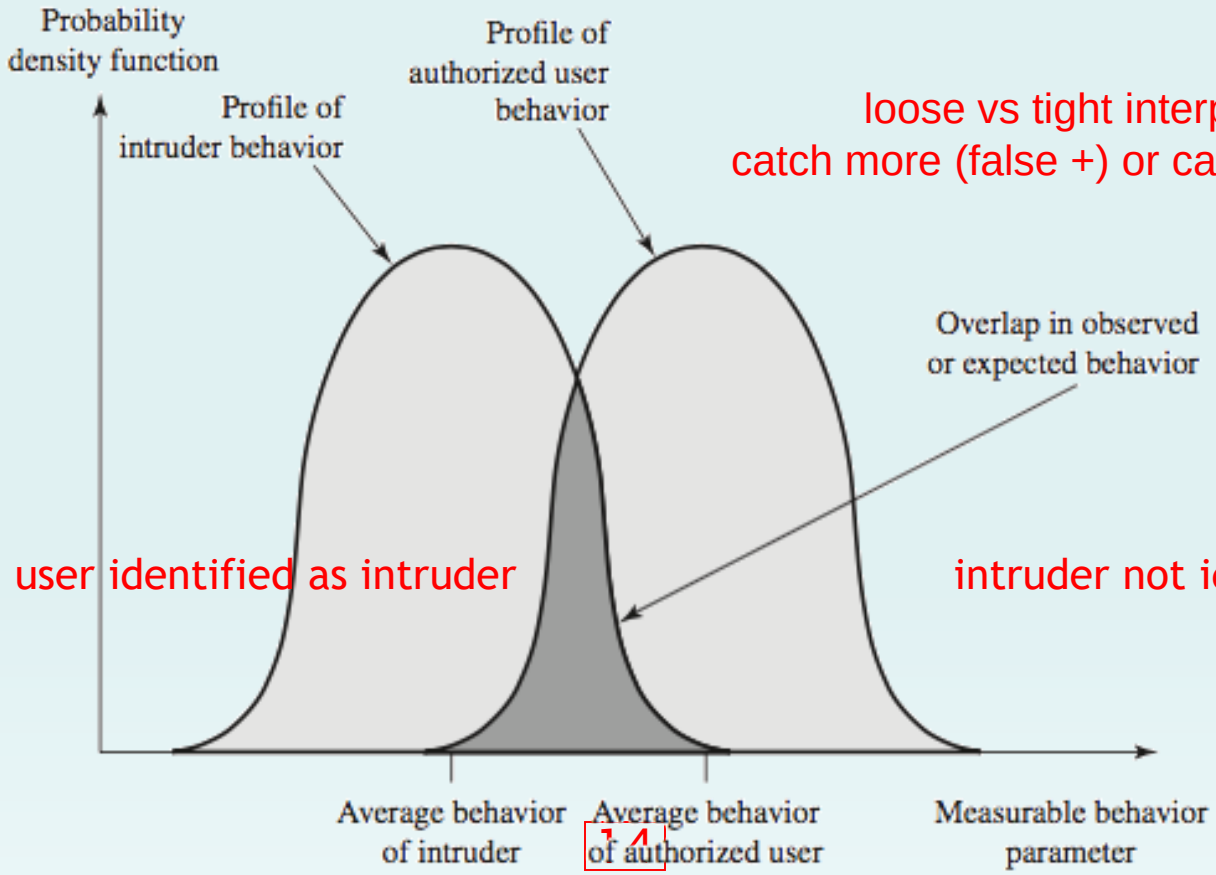
In some systems, the user interface may equate to a manager, director, or console component

HIDS vs NDIS

- **Host-based IDS**: monitor single host activity
- **Network-based IDS**: monitor network traffic
- **Distributed or hybrid**: Combines information from a number of sensors, often both host and network based, in a central analyzer that is able to better identify and respond to intrusion activity

IDS Basic Principles

Assumption: intruder behavior differs from legitimate users



loose vs tight interpretation:
catch more (false +) or catch less (false -)

valid user identified as intruder

intruder not identified

IDS requirements

- Run continually with minimal human supervision
- Be fault tolerant: recover from crashes
- Resist subversion: monitor itself from change by intruder
- Impose a minimal overhead on system
- Configured according to system security policies
- Adapt to changes in systems and users
- Scale to monitor large numbers of systems
- Provide graceful degradation of service: if one component fails, others should continue to work
- Allow dynamic reconfiguration

Detection techniques

- Anomaly (behavior) detection
- Signature/heuristic detection

Signature/heuristic detection

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior
- Also known as misuse detection
- Can only identify known attacks for which it has patterns or rules (signature)
  - Very similar to anti-virus (requires frequent updates)
  - Rule-based penetration identification
    - rules identify ***known*** penetrations/weaknesses
    - often by analyzing attack scripts from Internet (CERTs)

Example of rules in a signature detection IDS

- Users should not be logged in more than one session
- Users do not make copies of system, password files
- Users should not read in other users' directories
- Users must not write other users' files
- Users who log after hours often access the same files they used earlier
- Users do not generally open disk devices but rely on high-level OS utilities

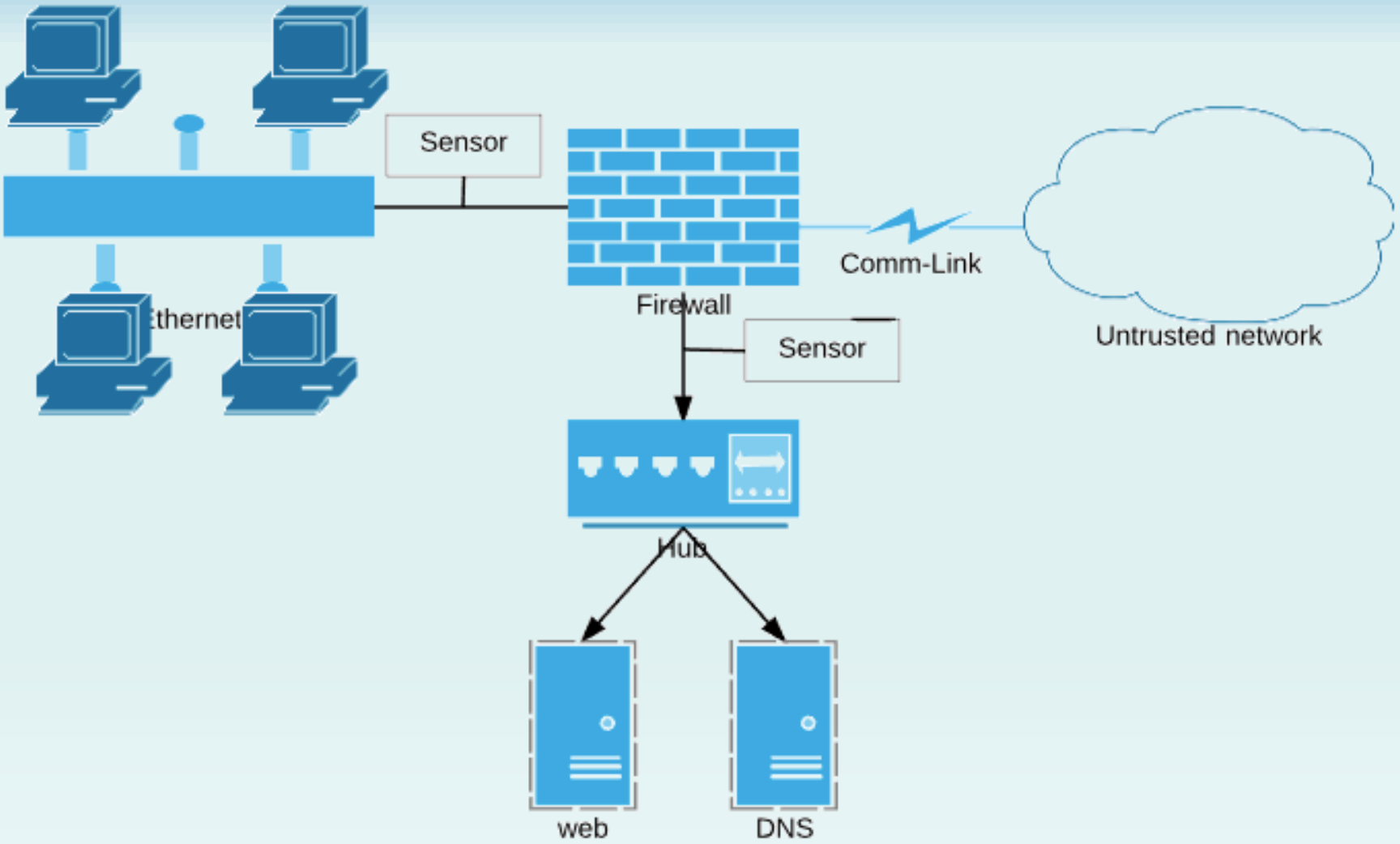
Rule-based Detection

- Use of rules for identifying known penetrations or penetrations that would exploit known weaknesses.
- Rules can also be defined that identify suspicious behavior.
- SNORT is an example of a rule-based NIDS

Network Based IDS (NDIS)

- Monitor traffic at a selected point in a network or subnet in real or close to real time so that it can react to intrusions in a timely manner.
- NDIS can analyze traffic in multiple layers of the network stack. A network IDS can include a number of sensors.

Network-Based IDS

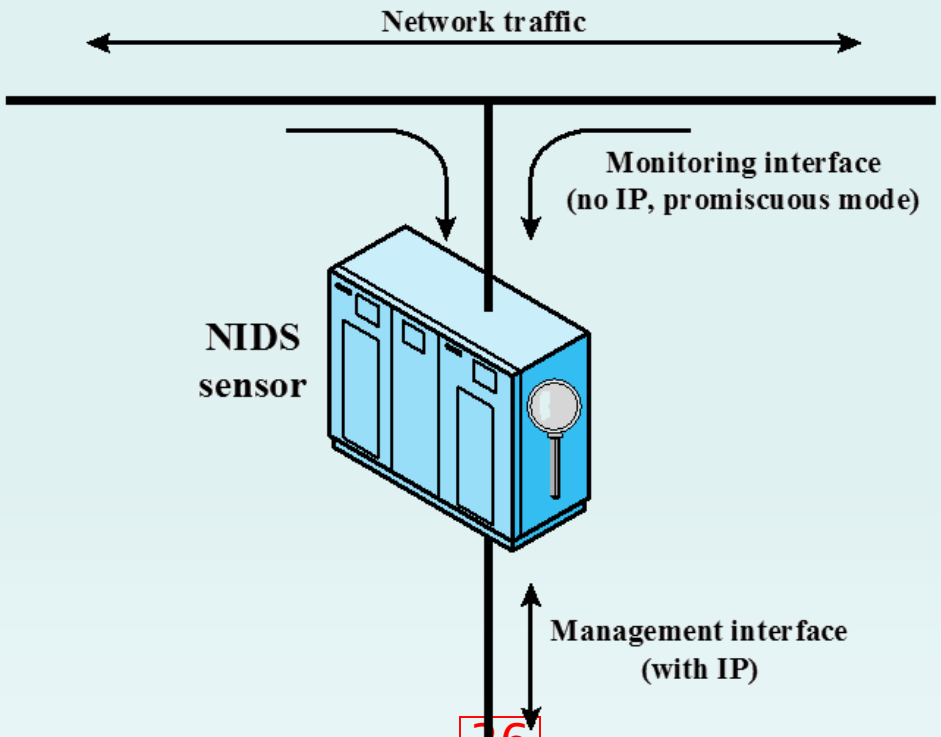


Inline Sensors

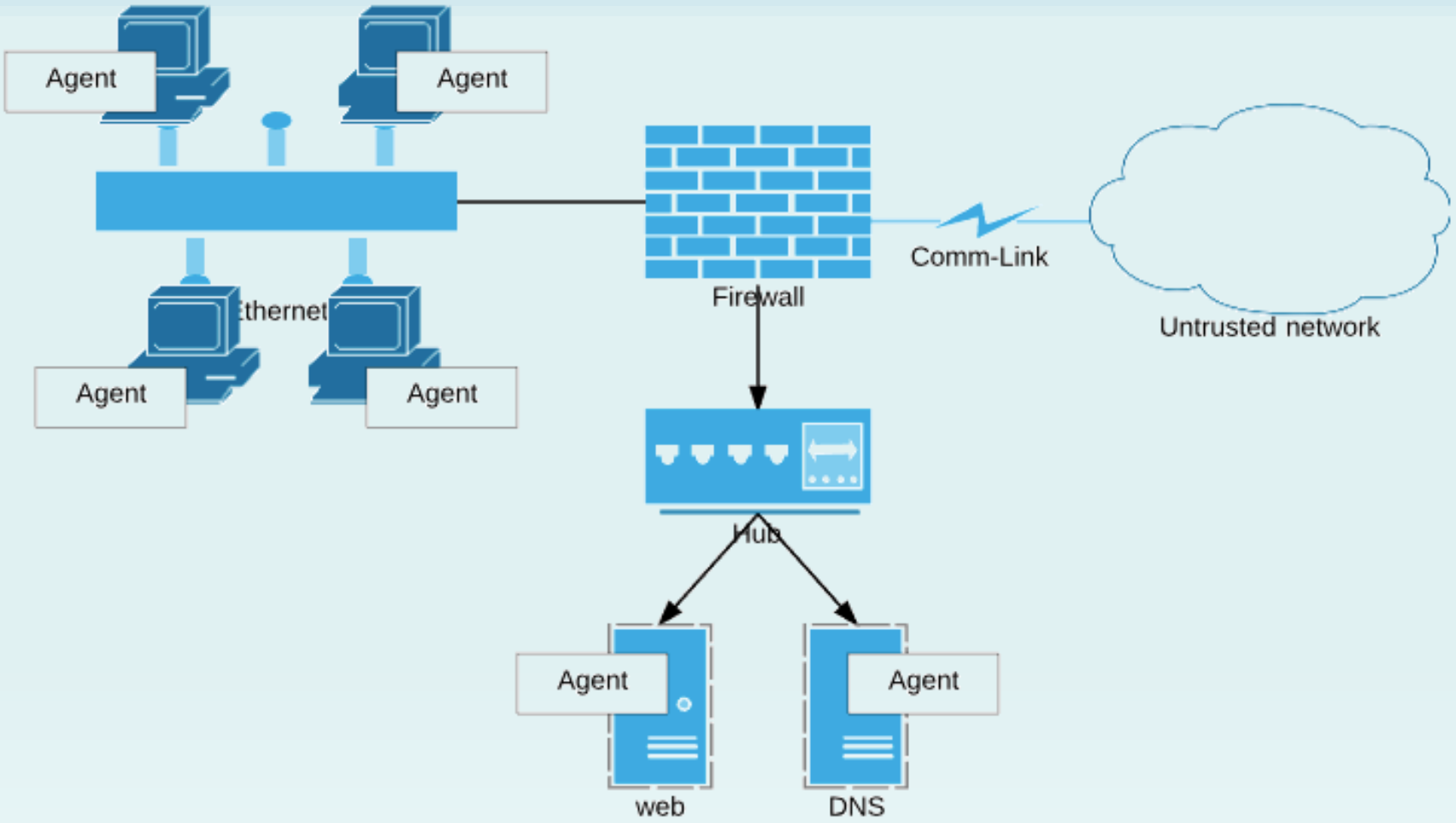
- The primary motivation for using inline sensors is to enable them to block an attack, when being detected.
- An inline sensor performs both intrusion detection and intrusion prevention.
- For an inline sensor to be effective, it must be placed at a network point where traffic must pass through it.

Passive Sensors

- A passive sensor only takes a copy of the traffic.
- That is, the traffic continues to reach its destination without passing through the device.



Host Based IDS (HIDS)



Logging of alerts (for all types)

Typical information logged by a NIDS sensor:

- Timestamp,
- Connection or session ID,
- Event or alert type,
- Rating,
- Network, transport, and application layer protocols,
- Source and destination IP addresses,
- Source and destination ports, ICMP types and codes,
- Number of bytes transmitted over the connection,
- Decoded payload data, such as application requests and responses,
- State-related information.

Firewall vs. Network IDS

Firewall

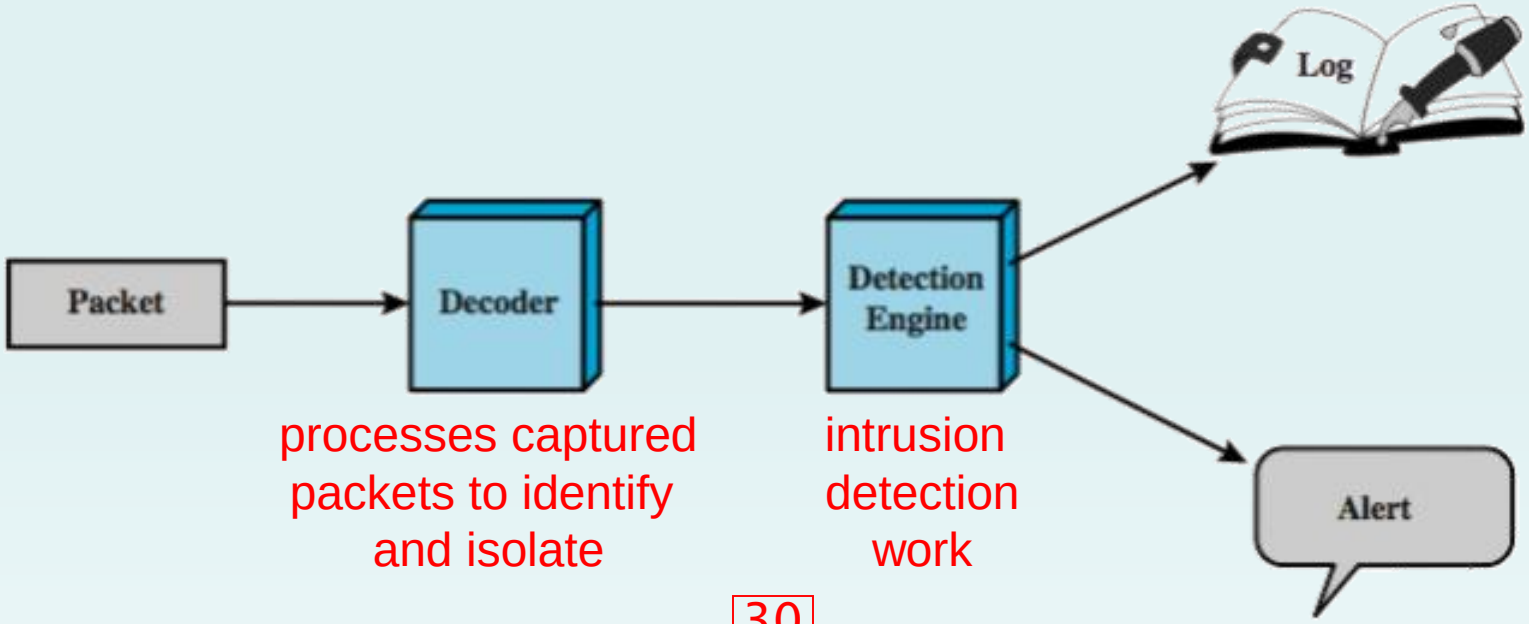
- Active filtering
- Fail-close

Network IDS

- Passive monitoring
- Fail-open

Snort IDS

- Lightweight IDS
  - Open source (rule-based)
  - Real-time packet capture and rule analysis
  - Passive or inline
  - Components: decoder, detector, logger, alerter



SNORT Rules

- Use a simple, flexible rule definition language
- Fixed header and zero or more options
- Header includes: action, protocol, source IP, source port, direction, dest IP, dest port
- Many options
- Example rule to detect TCP SYN-FIN attack:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any \
(msg: "SCAN SYN FIN"; flags: SF, 12; \
reference: arachnids, 198; classtype: attempted-recon;)
```

  - detects an attack at the TCP level; $strings are variables with defined values; any source or dest port is considered; checks to see if SYN and FIN bits are set

Honeypots

- Decoy systems
  - Filled with fabricated info and instrumented with monitors/event loggers
  - Lure a potential attacker away from critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to respond
  - Divert and hold attacker to collect activity info without exposing production systems
- Initially were single systems
- More recently are/emulate entire networks

Honeypot classification

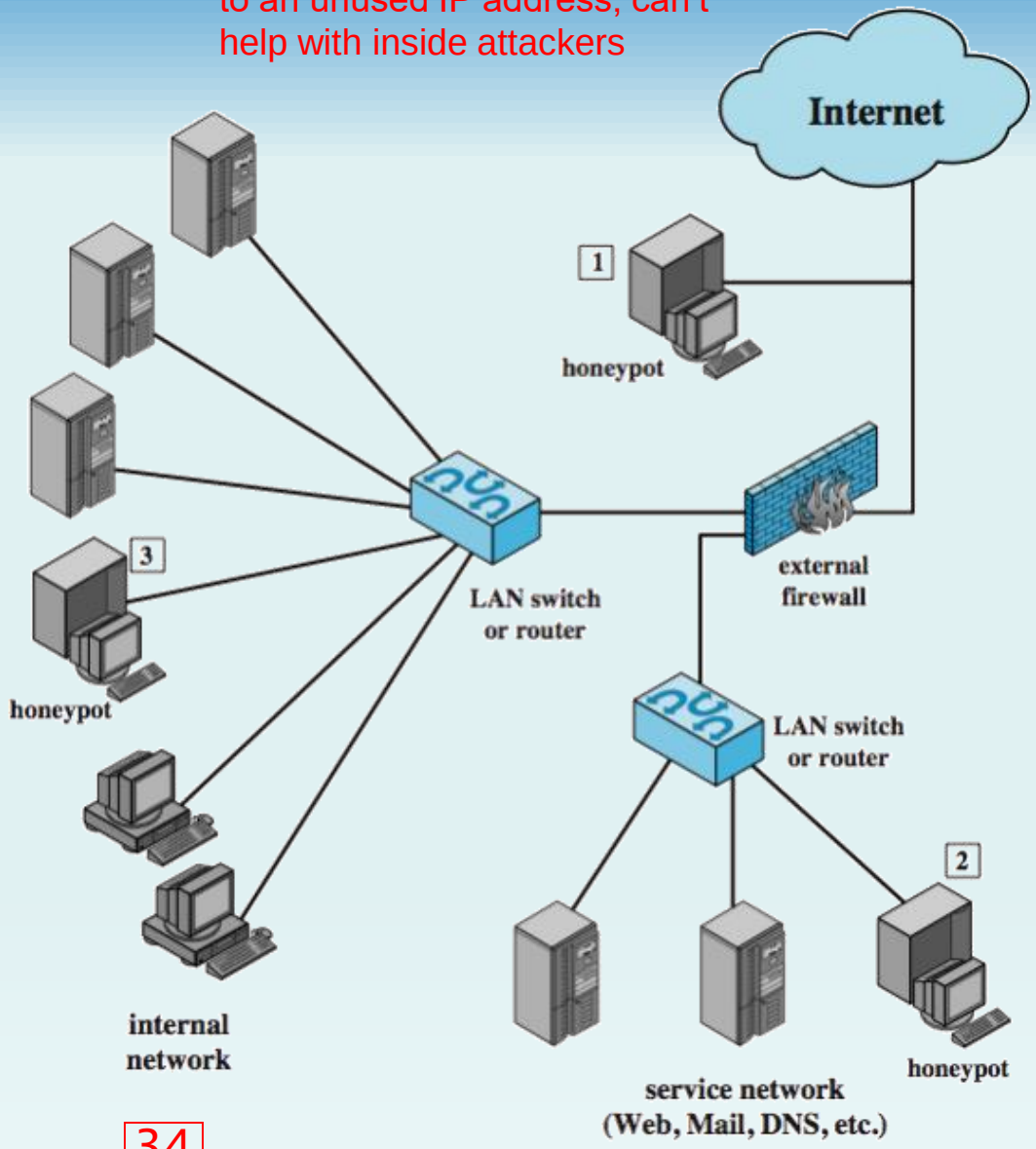
- Low interaction honeypot
  - Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems
  - Provides a less realistic target
  - Often sufficient for use as a component of a distributed IDS to warn of imminent attack
- High interaction honeypot
  - A real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers

Honeypot deployment

1. Tracks attempts to connect to an unused IP address; can't help with inside attackers

3. Full internal honeypot; can detect internal attacks

2. In DMZ; must make sure the other systems in the DMZ are secure; firewalls may block traffic to the honeypot



Intrusion Prevention System (IPS)