In the Name of Allah

Intrusion Detection Systems

Outline

- Intrusion Concept
- Intrusion Detection Systems(IDS)
- Types of IDS
- Attacks to the IDS
- Snort Intrusion Detection System
- Host-based Intrusion Detection

What is an intrusion?

- An intrusion can be defined as “any set of actions that attempt to compromise the:
  - Integrity
  - confidentiality, or
  - availability

  of a resource”.

Intruders

- *Insider*: abuse by a person with authorized access to the system.
- *Hacker*: attack the via communication links (e.g. Internet).
- *Malicious software (`MalWare`, Trojan horse, Virus)*: attack on the system by software running on it.

Intrusion Examples

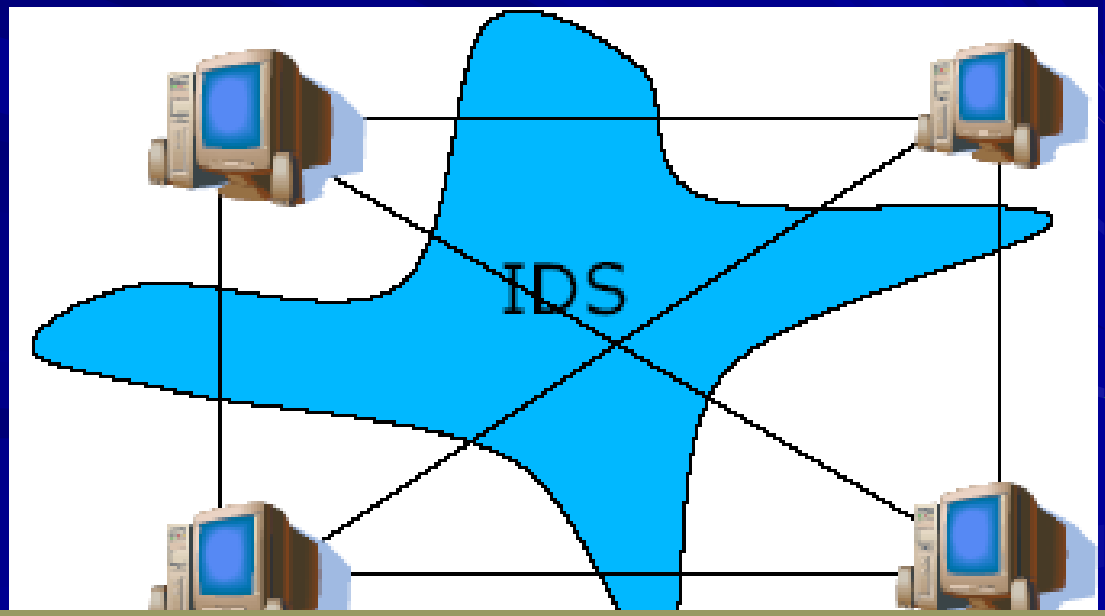
- **Virus**
- **Buffer-overflows**
  - 2000 Outlook Express vulnerability.
- **Denial of Service (DOS)**
  - explicit attempt by attackers to prevent legitimate users of a service from using that service.
- **Address spoofing**
  - a malicious user uses a fake IP address to send malicious packets to a target.
- **Many others**

Outline

- Intrusion Concept
- Intrusion Detection Systems(IDS)
- Types of IDS
- Attacks to the IDS
- Snort Intrusion Detection System
- Host-based Intrusion Detection

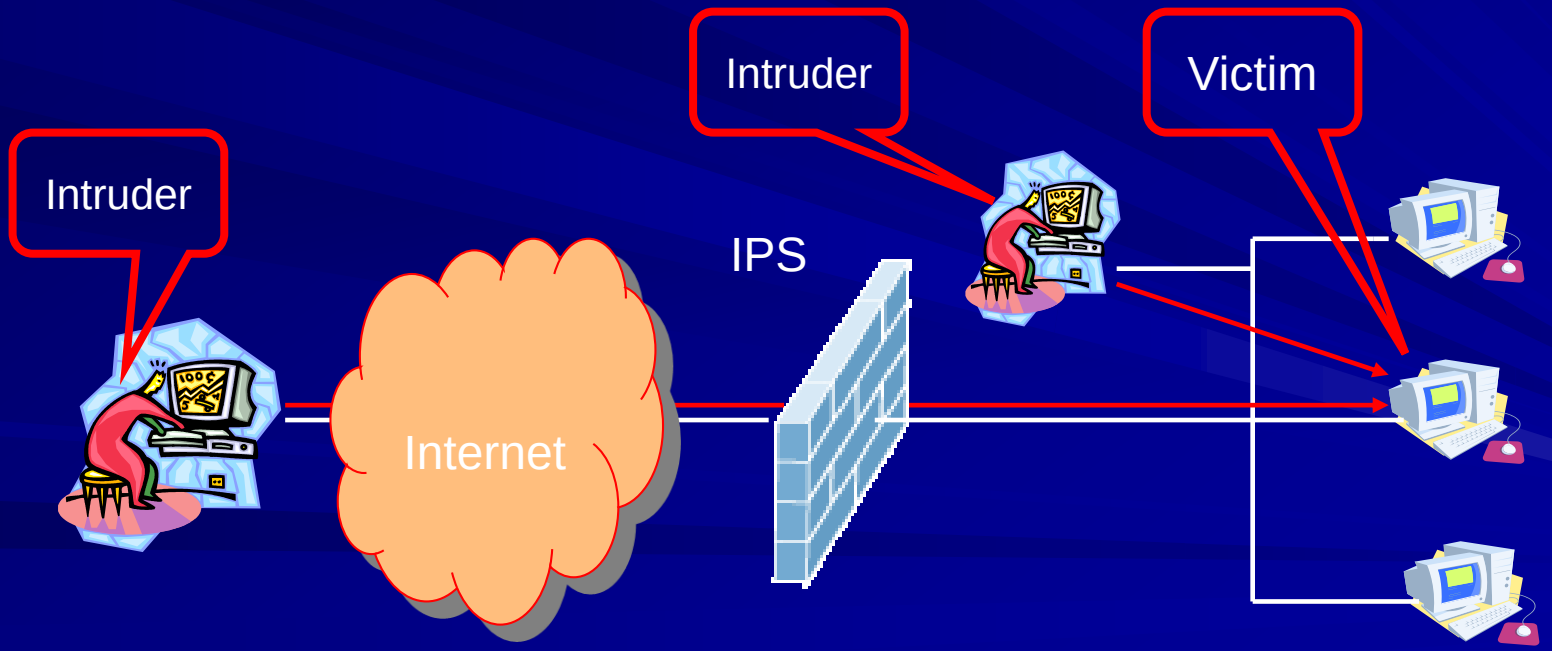
Intrusion Detection Systems

- Systems that detect attacks on computer systems.



Intrusion Detection Systems

- Intrusion Prevention System can prevent the network from outside attacks.



IDS Basic Functions

- **Monitoring**
  - Collect the information from the network
- **Analyzing**
  - Determine what, if any thing, is of interest
- **Reporting**
  - Generate conclusions and otherwise act on analysis results

Intrusion Detection Systems

- Firewalls are typically placed on the network perimeter protecting against external attacks
- Firewalls allow traffic only to legitimate hosts and services
- Traffic to the legitimate hosts/services can have attacks
- Solution?
  - Intrusion Detection Systems
  - Monitor data and behavior
  - Report when identify attacks

Intrusion Detection Systems

- Traditional IDS response tends to be passive response
- Secondary investigation required because IDS is still imperfect

- These days, IDS can be set up to respond to events automatically – “active response”

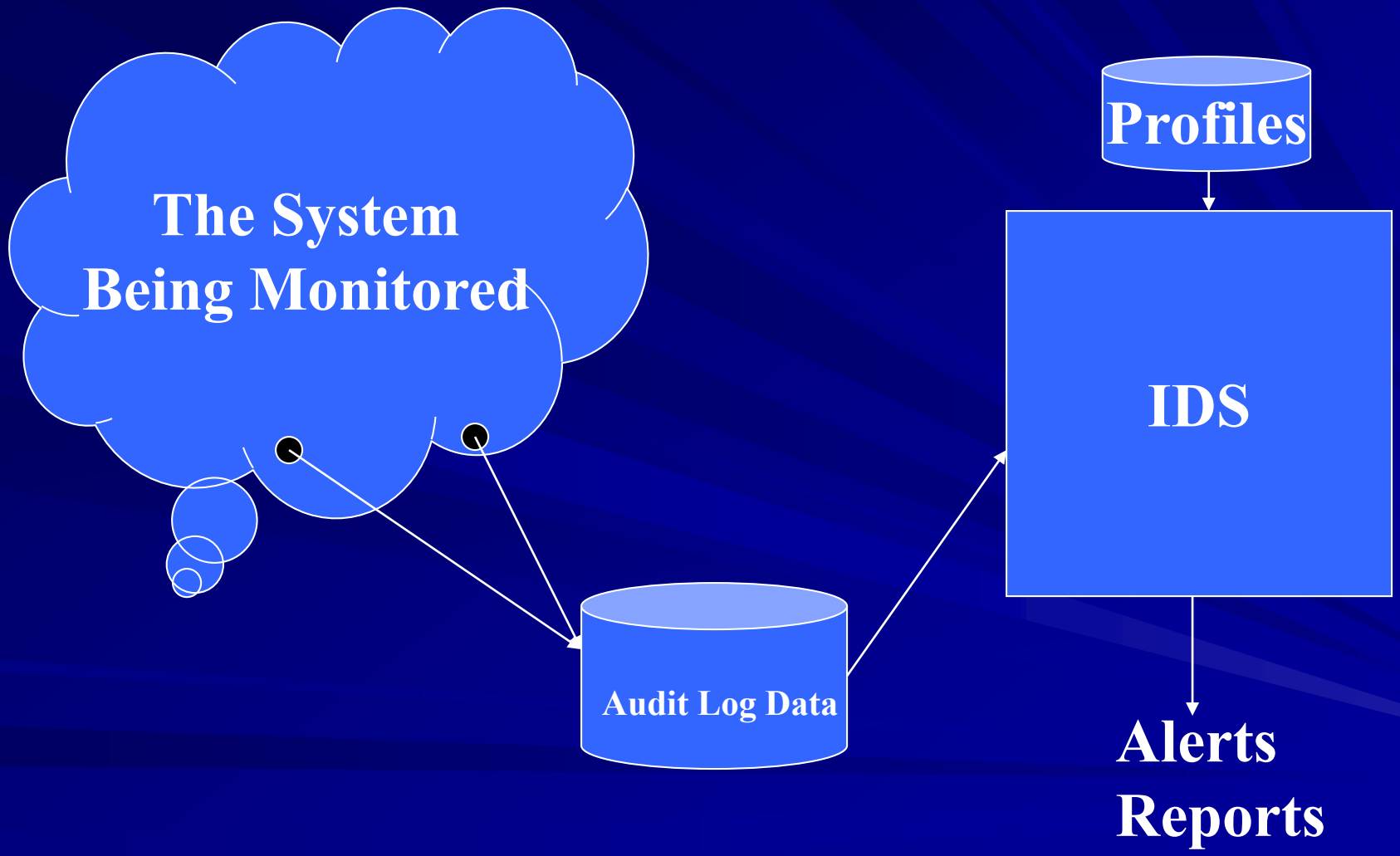
Intrusion Detection Systems

- Passive response
  - potential damage cost - resulting from alarmed events not investigated immediately
  - low false alarm costs since alarmed events are not disrupted

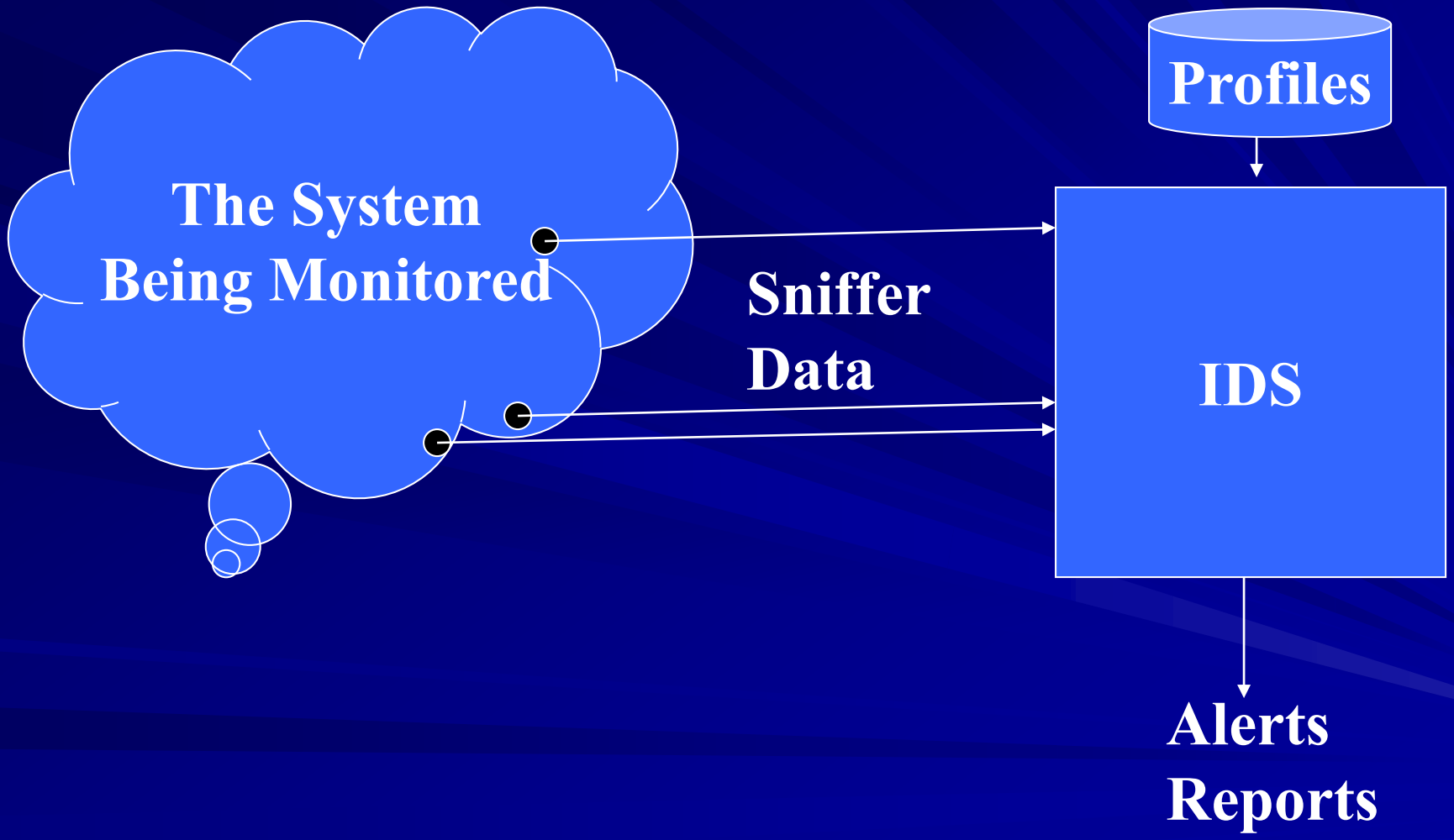
Intrusion Detection Systems

- Active response
  - It could prevent attack damage because the events are terminated immediately
  - higher false alarm costs contingent on the performance of the IDS

Audit Log Architecture



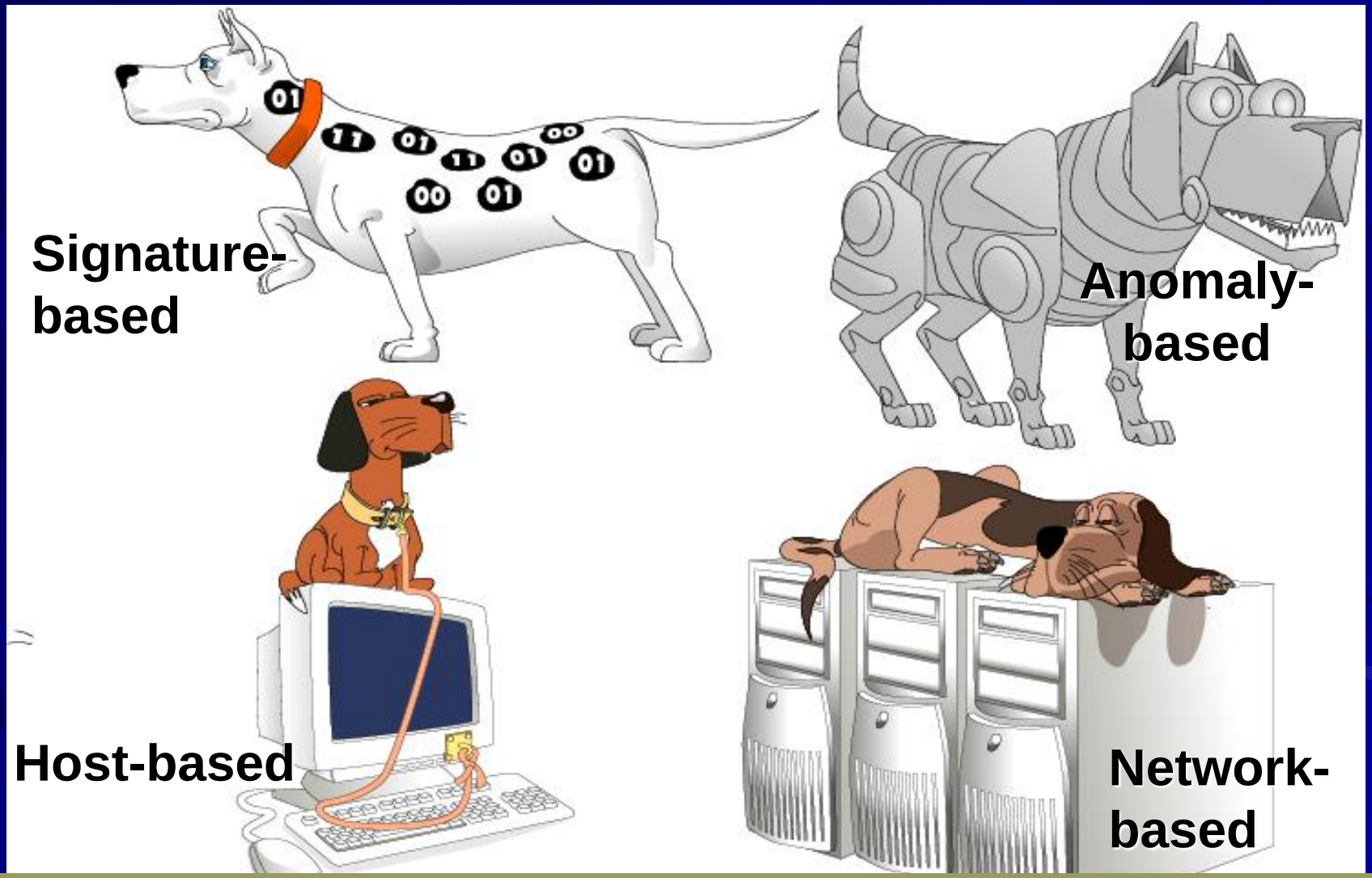
Inline Architecture



Outline

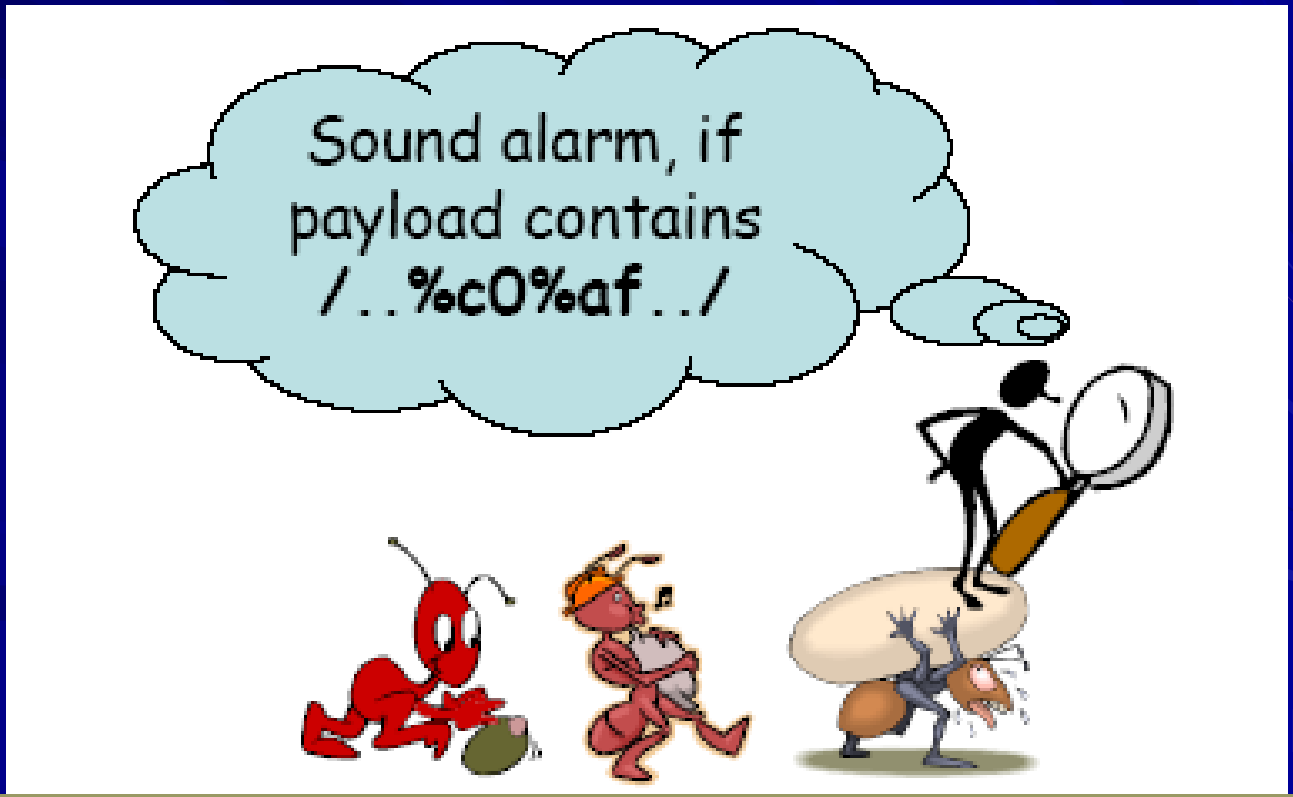
- **Intrusion Concept**
- **Intrusion Detection Systems(IDS)**
- **Types of IDS**
- **Attacks to the IDS**
- Snort Intrusion Detection System
- **Host-based Intrusion Detection**

Types of IDS



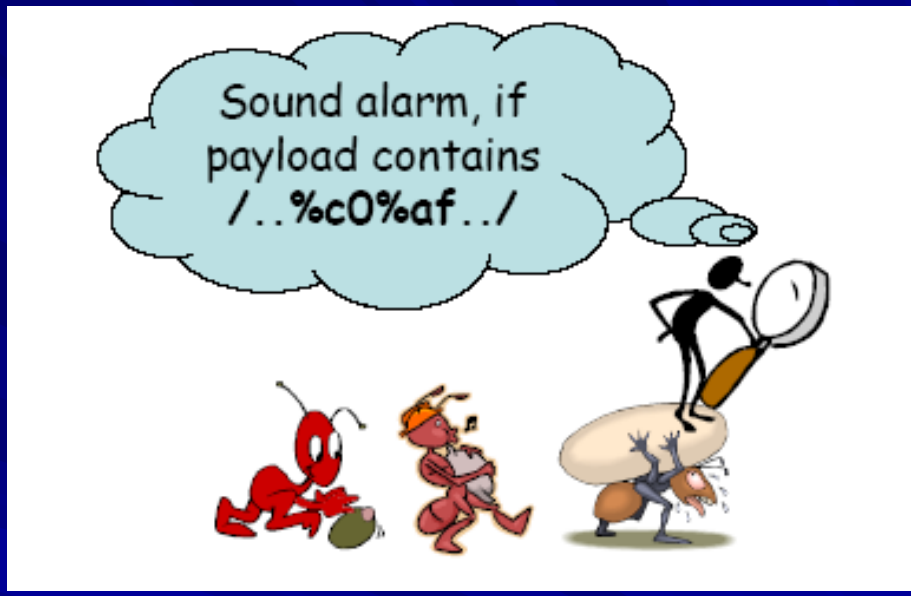
Signature-based IDS

- Characteristics
  - Uses known pattern matching to signify attack



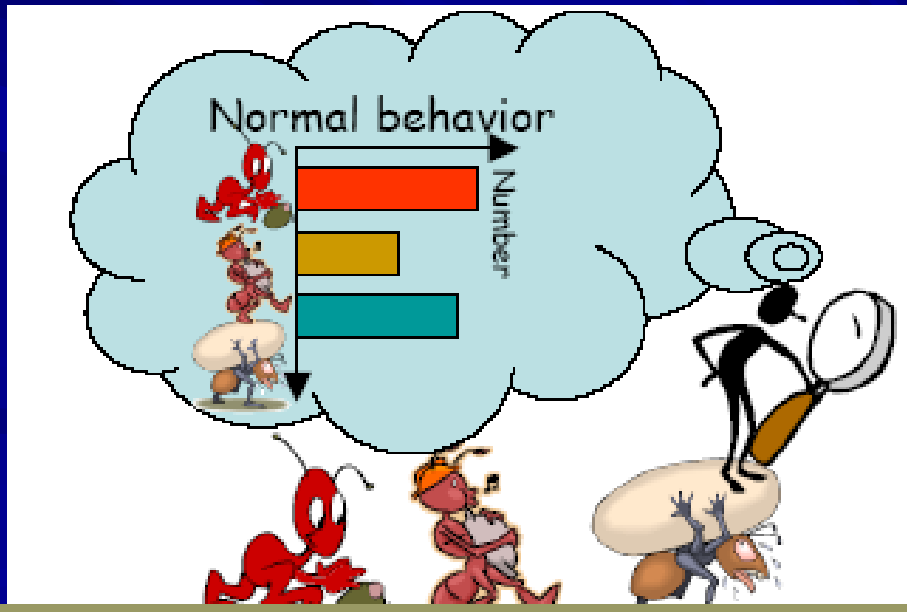
Signature-based IDS

- Advantages?
  - Widely available
  - Fairly fast
  - Easy to implement
  - Easy to update
- Disadvantages?
  - Cannot detect attacks for which it has no signature



Anomaly-based IDS

- Characteristics
  - –Uses statistical model or machine learning engine to characterize normal usage behaviors
  - –Recognizes departures from normal as potential intrusions



Anomaly-based IDS

- Advantages?
  - –Can detect attempts to exploit new and unforeseen vulnerabilities
  - –Can recognize authorized usage that falls outside the normal pattern
- Disadvantages?
  - –Generally slower, more resource intensive compared to signature-based IDS
  - –Greater complexity, difficult to configure
  - –Higher percentages of false alerts

More Problems with Anomaly Detection

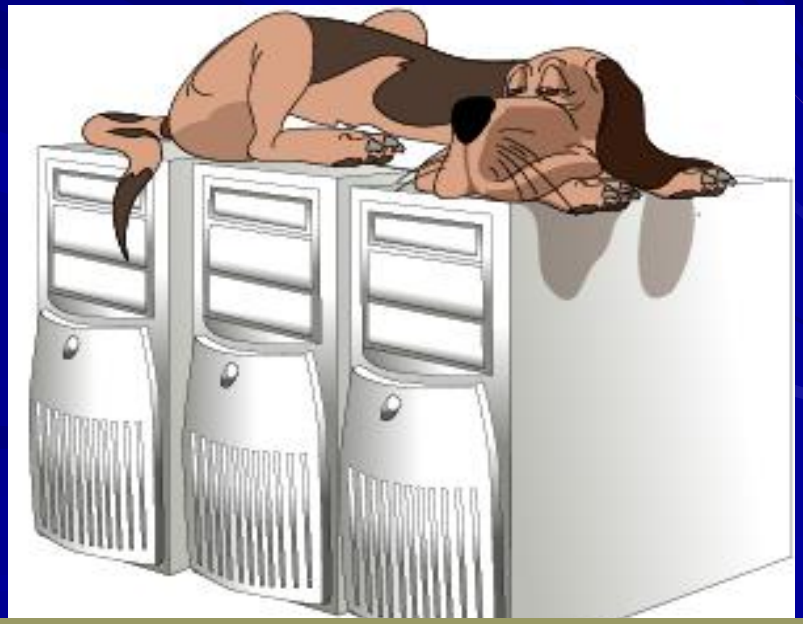
- The dynamic update problem is unsolved.
  - You can train these systems successfully to handle static environments, but computer networks are dynamic.
  - If you try to retrain an existing system to deal with new events, it will usually forget its old training. You have to give it the old training data as well as the new.

Possible Approaches to Anomaly Detection

- Neural networks
- Expert systems
- Statistical decision theory

Network-based IDS

- Characteristics
  - NIDS examine raw packets in the network passively and triggers alerts



Network-based IDS

- Advantages?
  - Easy deployment
  - Difficult to evade
- Disadvantages?
  - NIDS needs to create traffic seen at the end host
  - Need to have the complete network topology and complete host behavior

Host-based IDS

- Characteristics
  - Runs on single host
  - Can analyze logs, integrity of files and directories, etc.

Host-based IDS

- Advantages
  - More accurate than NIDS
  - Less volume of traffic so less overhead
- Disadvantages
  - Deployment is expensive
  - What happens when host get compromised?

Honey Pots and Burglar Alarms

- Burglar alarms are resources on the network that generate an alarm if accessed incorrectly.
- Honey pots are burglar alarms dressed up to look attractive.

- Have to look real to the attackers

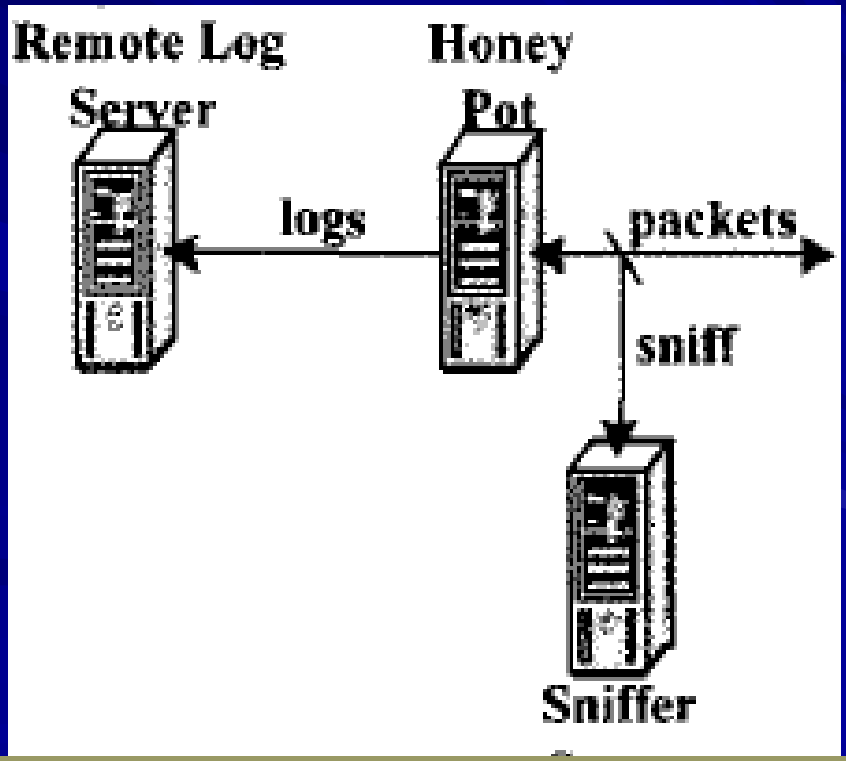
Intrusion Detection Using Honey Pot

- Honey pot is a “decoy” system that appears to have several vulnerabilities for easy access to its resources.
- It provides a mechanism so that intrusions can be trapped before attack is made on real assets.

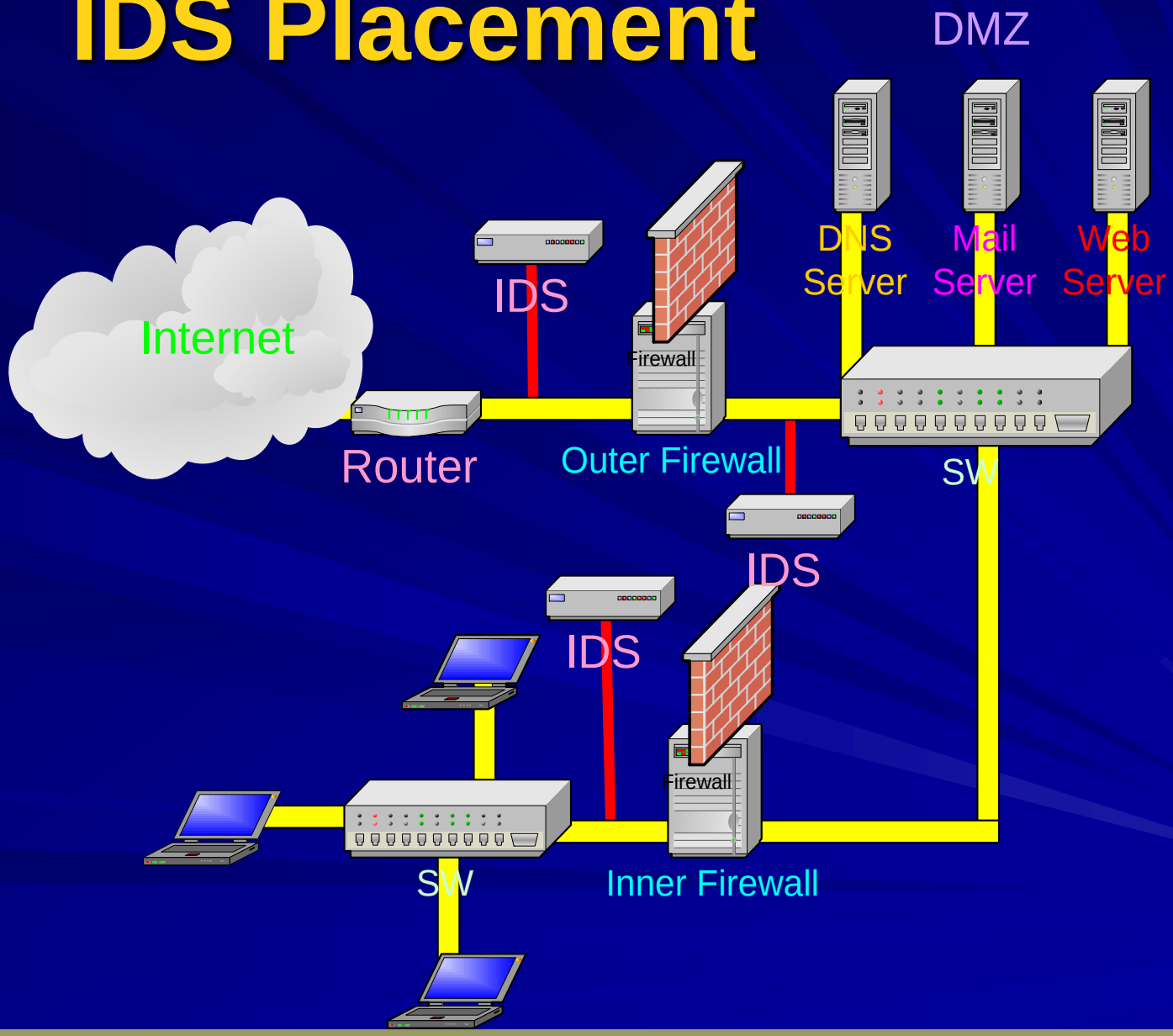
Intrusion Detection Using Honey Pot (cont.)

Multi-level Log Mechanism (MLLM)

- MLLM logs the attacker's activities into
  - Remote Log Server
  - Sniffer Server



IDS Placement



Outline

- **Intrusion Concept**
- **Intrusion Detection Systems(IDS)**
- **Types of IDS**
- **Attacks to the IDS**
- Gateway Intrusion Detection System
- **Host-based Intrusion Detection**

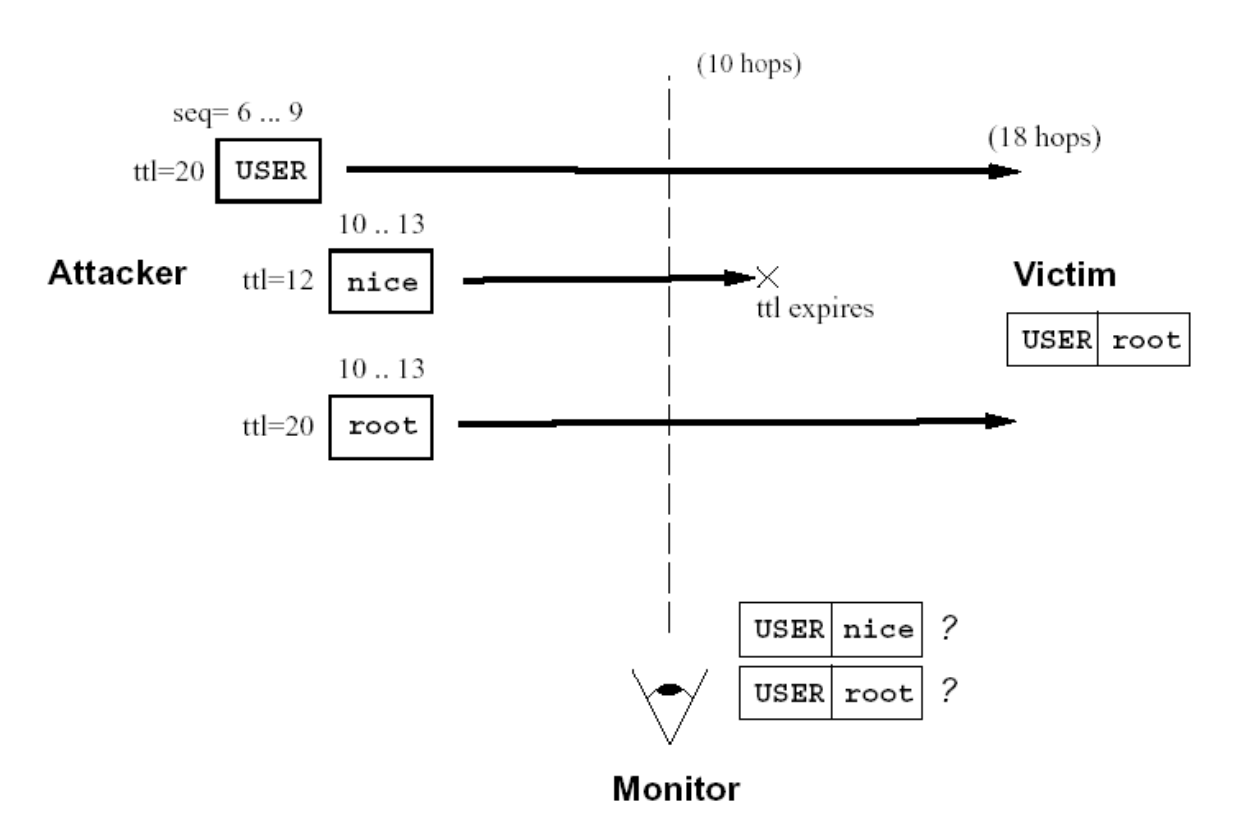
Attacks to the IDS

Overload until IDS fails to keep up with the data

- ✓ Overload packet filter (easy)
- ✓ Overload event engine (difficult because events are light weighted and attacker doesn’t know policy script)
- ✓ Overload Logging/Recording mechanism

Attacks to the IDS

An Subterfuge attack attempts to mislead the IDS to the meaning of the analyzed traffic



IDS Software

- **Snort** Free, libpcap based, rules driven **IDS** package. Many add-on components available.
- **...**

Outline

- Intrusion Concept
- Intrusion Detection Systems(IDS)
- Types of IDS
- Attacks to the IDS
- Snort Intrusion Detection System
- Host-based Intrusion Detection

Content Replacement

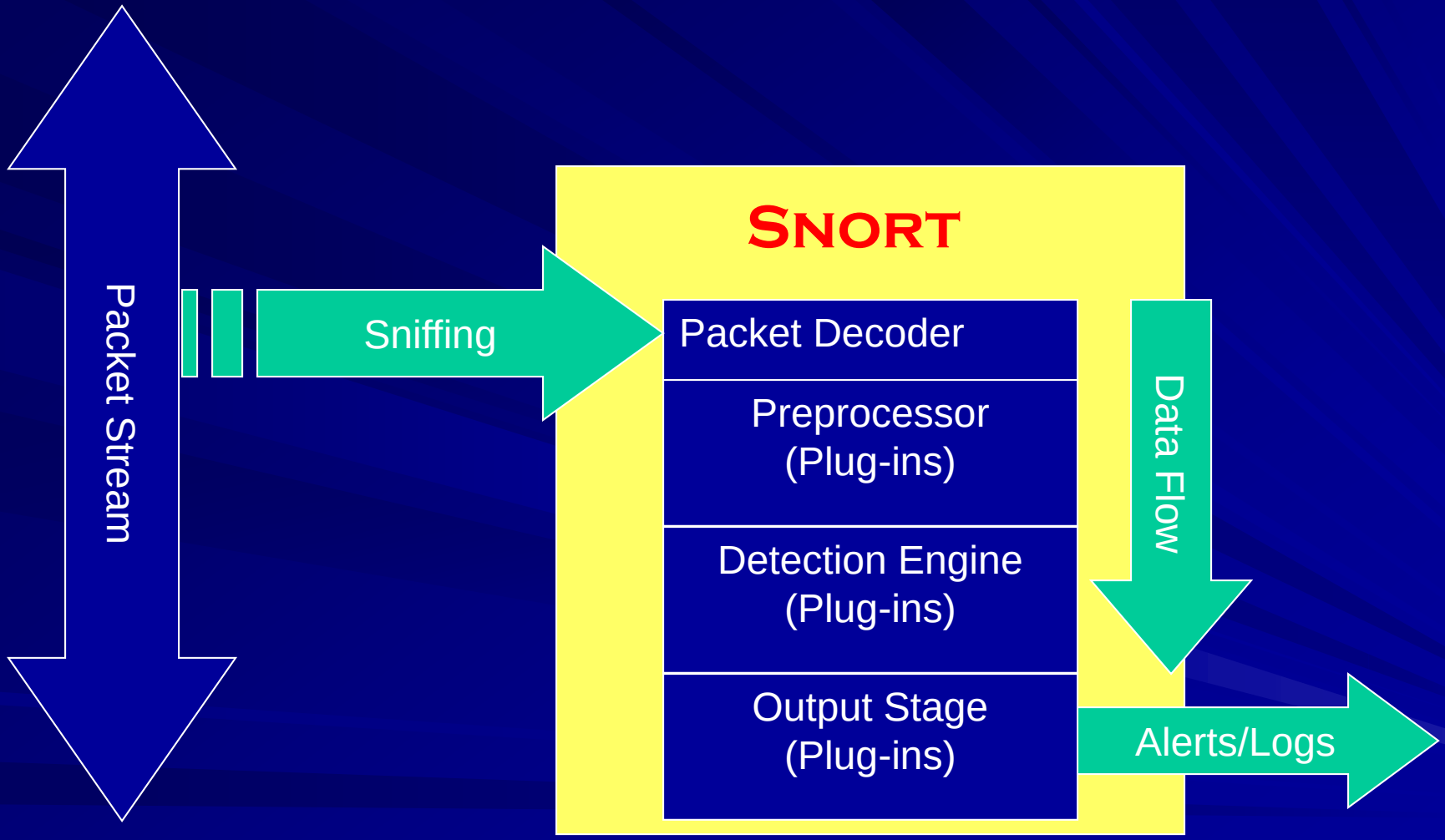
It can replace content in a packet

- "replace" keyword tells snort to replace a detected string with another string.
- Example:

alert tcp any any -> $IIS_SERVERS 80 (content:"cmd.exe"; replace:"yyy.yyy";)

- Any content in the packet payload can be replaced.
- A great way to break an exploit without dropping the packet!!

Snort Data Flow



Detection Engine: Rules

Rule Header	Rule Options
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: SF; msg: “SYN-FIN Scan”;)
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: Nil; msg: “Null Scan”;)
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: F; msg: “FIN Scan”;)

About Inline Snort

- Based on the Snort intrusion detection system
- Operation is similar to some bridging firewalls
- Uses snort rules with some additional keywords to make forward/drop decisions
- Compatible with most snort plugins
- Freely available under the GPL

Sample snort Rules

- To drop incoming port 80 connections:

```
drop tcp any any -> $HOMENET 80 (msg:"Port 80 tcp")
```

- To drop cmd.exe calls to your webservers:

```
drop tcp any any -> $HOMENET 80 (msg:"cmd.exe
attempt"; content: "cmd.exe")
```

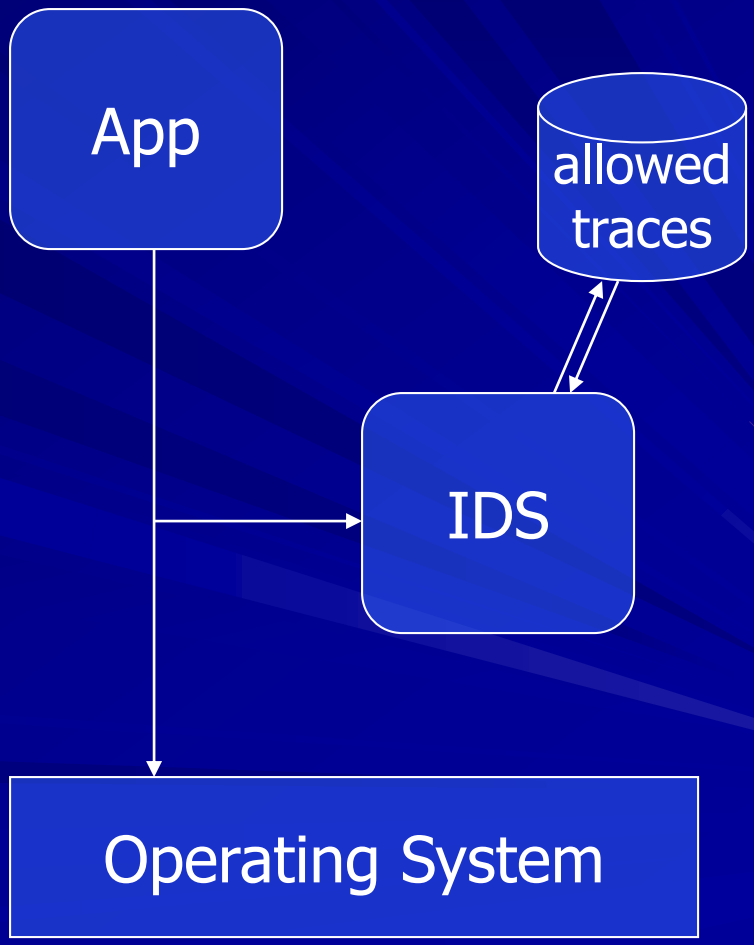
Outline

- **Intrusion Concept**
- **Intrusion Detection Systems(IDS)**
- **Types of IDS**
- **Attacks to the IDS**
- Snort Intrusion Detection System
- **Host-based Intrusion Detection**

Host-based Intrusion Detection

Anomaly detection:

- IDS monitors system call trace from the app
- DB contains a list of subtraces that are allowed to appear
- Any observed subtrace not in DB sets off alarms



HIDS' Advantages over NIDS

- HIDS can monitor user-specific activity of the system
  - Check process listing, local log files, system calls.
  - It is difficult for NIDS to associate packets to specific users (except when content switch-based NIDS is used!) and to determine if the commands in the packets violate specific user's access privilege.