Intrusion Detection Systems (IDS)

Dr. Asem Kitana

Introduction

- Firewalls currently represent the most widely used security mechanism in corporate networks.
  - Firewalls, however, can be compromised or bypassed, and do preciously little to protect against insider attacks.
  - So, it is very important to have additional protection mechanisms on the internal hosts and network.
- Intrusion detection systems fulfill such purpose by **monitoring** computing systems and **reporting** intrusive behaviors.

Intrusion

- ***Intrusion:*** attempt to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a system. (attempt to breaking into a system).

- Intrusions have many causes:
  - Malware (viruses, worms, trojan horses, etc…).
  - Attackers gaining unauthorized access.
  - Authorized users who misuse their privileges.
  - Authorized users who attempt to gain additional privileges.

- Although many intrusions are malicious in nature, many others are not; for example: a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization.

Intrusion Detection

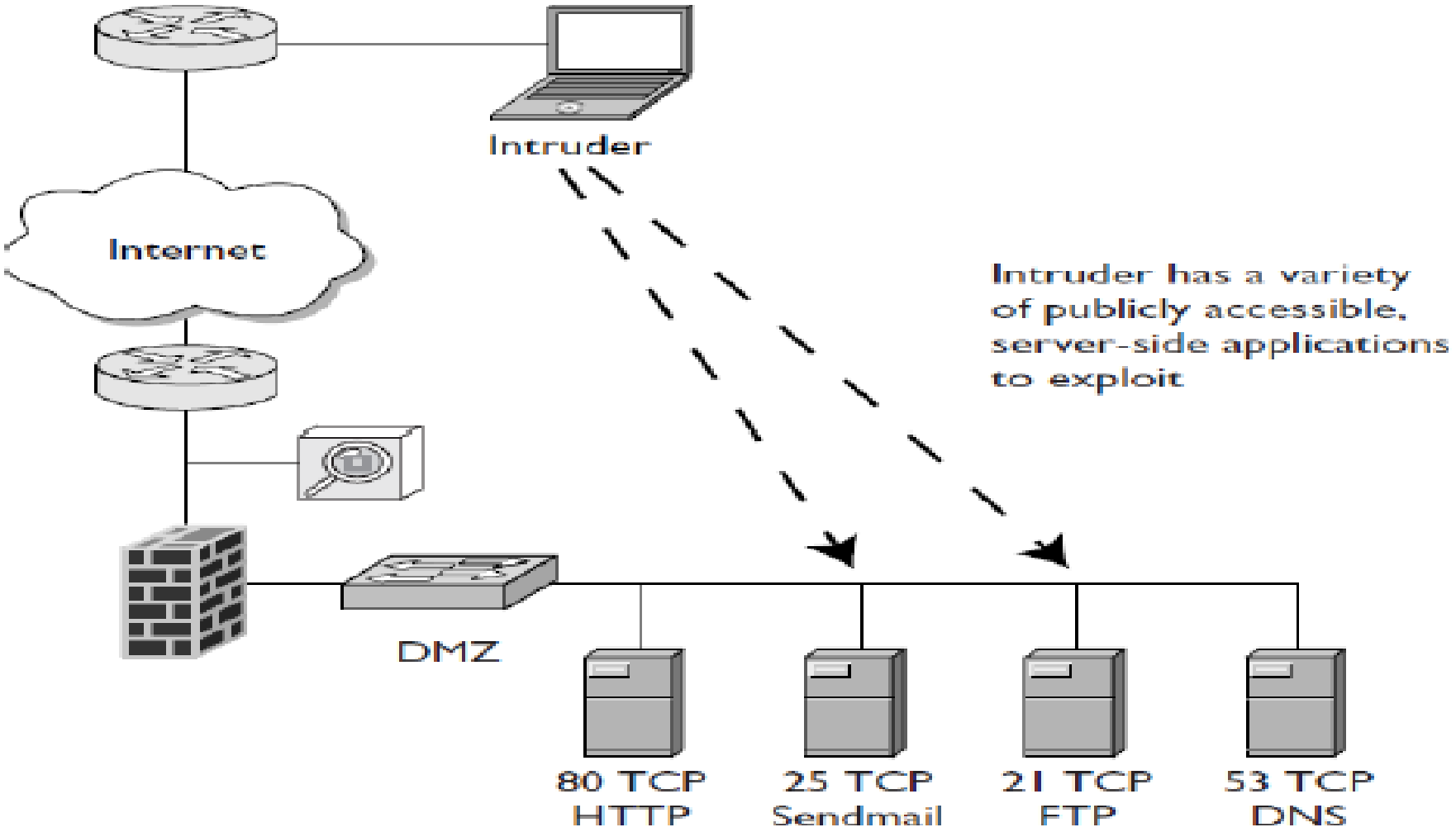
- ***Intrusion detection:*** is the process of monitoring the network traffic in order to identify unauthorized activities.
- ***Intrusion detection system (IDS):*** is a system that automates the intrusion detection process. The primary responsibility of an IDS is to detect unwanted and malicious activities.
- ***Intrusion prevention system (IPS***): is a system that has all the capabilities of an intrusion detection system, in addition to the ability of stopping possible incidents.
- ***Intruders*** may be from outside the network or legitimate users of the network.

Why IDS should be used?

- Identifying incidents, logging information about them, attempting to stop them, and reporting them to security administrators.
- Identifying problems with security policies
- Documenting existing threats
- Deterring individuals from violating security policies.

Intrusion Detection Systems

- Majority of intrusion detection systems rely on watching inbound traffic to a target.



IDS Models

There are three main categories of intrusion detection approaches:

- Anomaly detection

analyzes a set of characteristics of the system and compares their behavior with a set of expected values. It reports an intrusion when there is deviation from the expected behavior.

- Misuse detection

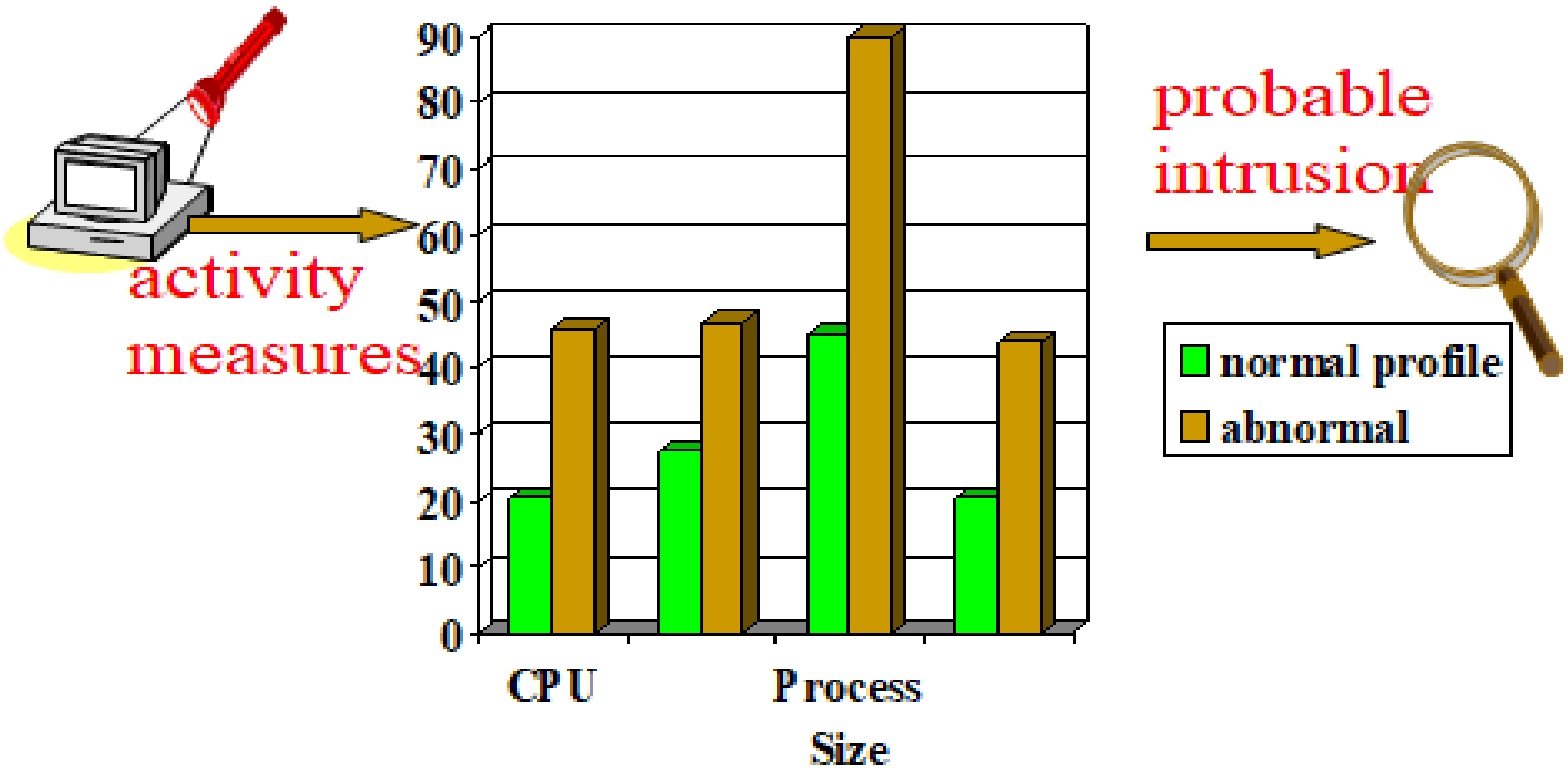
Also known as signature-based detection or Pattern Matching—Matches pattern of malicious activity.

- Specification-based detection

Examines the protocol and/or payload content to determine the validity of the specifications.

Anomaly Detection IDS

- Relatively high false positive rate - anomalies can just be new normal activities.



Anomaly Detection IDS

- This type of IDS models the normal usage of a network as a genuine behavior.
- Anything distinct from the genuine behavior is assumed to be an intrusion activity.
  - For instance, flooding a host with lots of packet.
- The primary strength is its ability to recognize novel (zero-day) attacks.

Example: Network Anomalies

- Normal traffic flowing to 142.104.112.106, the protected system

```
14345 03/23/2004 11:55:10 00:00:03 ftp  33291 20 142.104.112.115 142.104.112.106
14346 03/23/2004 11:55:13 00:00:04 smtp 32267 25 142.104.112.113 142.104.112.106
14347 03/23/2004 11:55:17 00:00:05 ftp  33547 20 142.104.113.10  142.104.112.106
14348 03/23/2004 11:55:22 00:00:03 http 32523 80 142.104.115.21  142.104.112.106
14349 03/23/2004 11:55:25 00:00:01 http 33035 20 142.104.124.110 142.104.112.106
14350 03/23/2004 11:55:25 00:00:02 http 32779 20 142.104.124.39  142.104.112.106
14351 03/23/2004 11:55:27 00:00:01 http 32011 20 142.104.124.78  142.104.112.106
14352 03/23/2004 11:55:27 00:00:03 http 34315 20 142.104.124.71  142.104.112.106
14353 03/23/2004 11:55:30 00:00:07 http 36107 20 142.104.124.80  142.104.112.106
14354 03/23/2004 11:55:37 00:00:01 ftp  35851 20 142.104.112.115 142.104.112.106
```

- Anomalous traffic flowing to 142.104.112.106

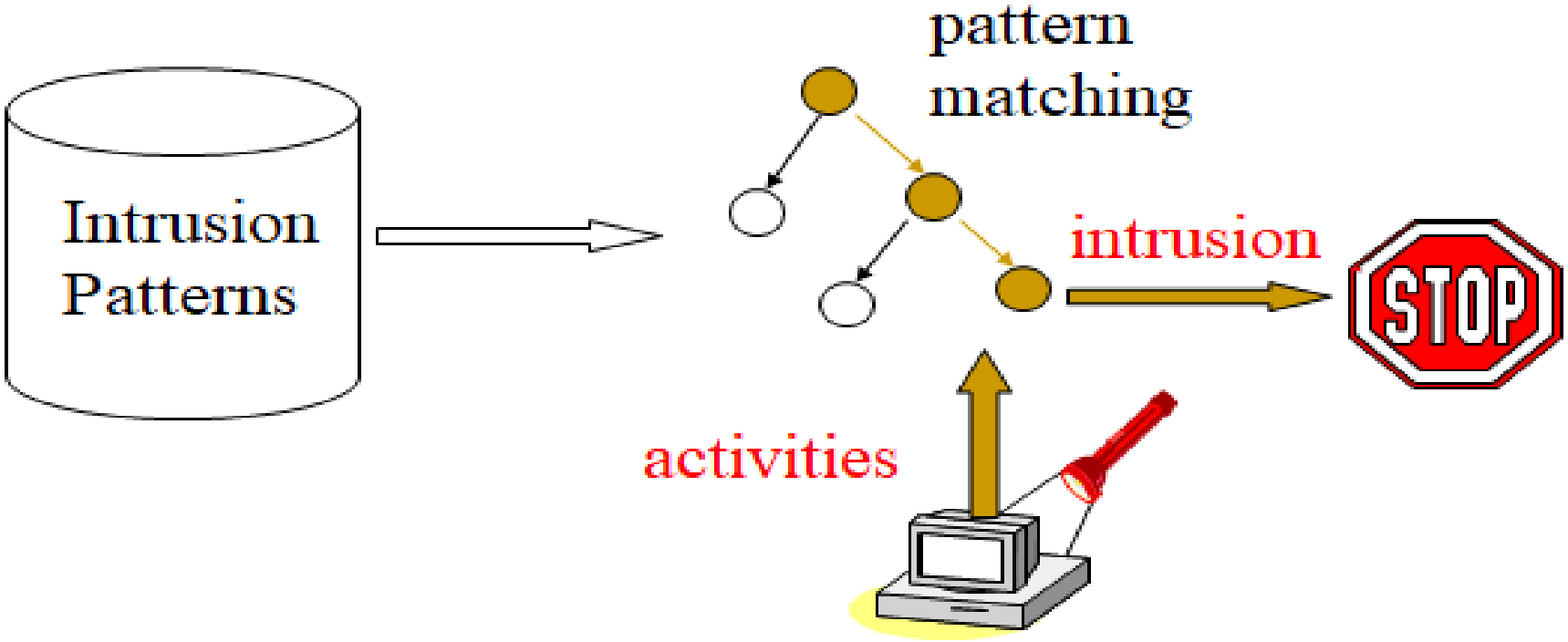
```
14355 03/23/2004 11:55:38 00:00:01 http 26891 80 009.009.009.009 142.104.112.106
14356 03/23/2004 11:55:38 00:00:01 http 26635 80 009.009.009.009 142.104.112.106
14357 03/23/2004 11:55:38 00:00:01 http 27403 80 009.009.009.009 142.104.112.106
14358 03/23/2004 11:55:38 00:00:01 http 26427 80 009.009.009.009 142.104.112.106
14359 03/23/2004 11:55:38 00:00:01 http 27659 80 009.009.009.009 142.104.112.106
14360 03/23/2004 11:55:38 00:00:01 http 27147 80 009.009.009.009 142.104.112.106
14361 03/23/2004 11:55:38 00:00:01 http 27915 80 009.009.009.009 142.104.112.106
14362 03/23/2004 11:55:38 00:00:01 http 28171 80 009.009.009.009 142.104.112.106
14364 03/23/2004 11:55:39 00:00:01 http 28939 80 009.009.009.009 142.104.112.106
14365 03/23/2004 11:55:39 00:00:01 http 31499 80 009.009.009.009 142.104.112.106
14366 03/23/2004 11:55:39 00:00:01 http 30219 80 009.009.009.009 142.104.112.106
14367 03/23/2004 11:55:39 00:00:01 http 29963 80 009.009.009.009 142.104.112.106
14368 03/23/2004 11:55:39 00:00:01 http 30475 80 009.009.009.009 142.104.112.106
14369 03/23/2004 11:55:39 00:00:01 http 29195 80 009.009.009.009 142.104.112.106
14370 03/23/2004 11:55:39 00:00:01 http 29451 80 009.009.009.009 142.104.112.106
14371 03/23/2004 11:55:39 00:00:01 http 30731 80 009.009.009.009 142.104.112.106
14372 03/23/2004 11:55:39 00:00:01 http 29707 80 009.009.009.009 142.104.112.106
14373 03/23/2004 11:55:39 00:00:01 http 28683 80 009.009.009.009 142.104.112.106
14374 03/23/2004 11:55:39 00:00:01 http 31243 80 009.009.009.009 142.104.112.106
14375 03/23/2004 11:55:39 00:00:01 http 30987 80 009.009.009.009 142.104.112.106
```

Drawbacks of Anomaly Detection IDS

- Relatively high false positive rate.
- Anomalies can just be new normal activities.

Misuse Detection IDS

- Can't detect new attacks



Example: ***if*** (src_ip == dst_ip) ***then*** "land attack"

Misuse Detection IDS

- Misuse detection IDSs are rely on pattern matching algorithms. IDS is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets, as an attack. For example, an IDS that watches web servers might be programmed to look for the string “phf” " in (“GET /cgi-bin/phf?”), as an indicator of a CGI program attack.

Drawbacks of Misuse Detection IDS

- They are unable to detect novel attacks (zero-day attacks).
- Have to programmed again for every new pattern to be detected.

IDS Architecture

- Basic architecture of an intrusion detection system involves 3 components: *Agent*, *Director*, and *Notifier*.
- ***Agent:***
  - Obtains information from data sources such as log files, system calls, or network traffic. The information is sent to the director possibly after preprocessing.
  - The information may be collected from a single host, a set of hosts, from the network, or from a combination of all these sources.

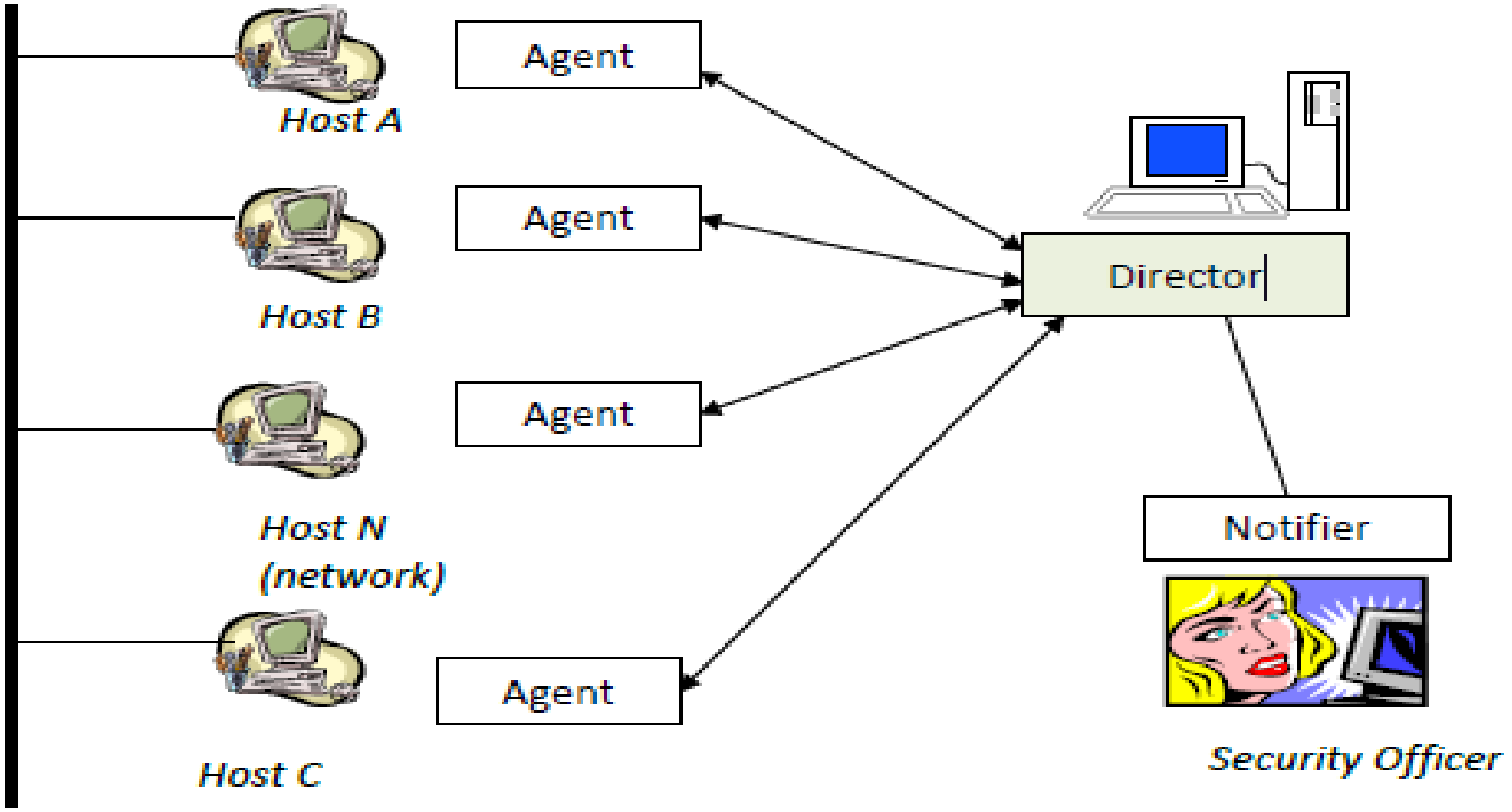
IDS Architecture

- ***Director:***
  - Analyzes the data from the agents to determine if an attack is in progress or has occurred.
  - To do so, the director reduces the incoming log entries to eliminate unnecessary records, and then uses an analysis engine to determine evidence of an attack.

IDS Architecture

- ***Notifier:***
  - Receives attack notifications from the director and takes some actions.
  - The notifier may display attack information on a GUI and/or send electronic mail to the cybersecurity officer.

IDS Architecture



Host based IDS

- The host operating system or the application logs in the audit information.
- These audit information includes events like the use of identification and authentication mechanisms (logins etc.) , file opens and program executions, admin activities etc.
- This audit is then analyzed to detect trails of intrusion.

Network based IDS

- This IDS looks for attack signatures in network traffic via a promiscuous interface.
- a commonly used data source consists of network traffic sniffer.

IDS Placement

- Multiple
  - Per segment / per traffic /per application
- Between main firewall and external firewall
  - Capture attack plans
  - But exposed IDS to attack, performance issues, lots of logs to view
- Between main firewall and internal network
  - Capture all attacks getting through the firewall
  - IDS less vulnerable to attacks
  - But limited views of attacks
- Both inside and outside the firewall?
- What if only can afford either inside or outside the firewall?

Honeypot

- Honeypots are decoy systems that designed to redirect a potential attacker away from critical systems.

- a honeypot is a system designed to teach how intruders probe for and exploit a system. By learning their tools and methods, you can then better protect your network and systems.

Honeypots are Designed To

- Divert an attacker from accessing critical systems.
- Collect information about the attacker's activity.
- Encourage the attacker to stay on the system long enough for administrators to respond.

Building a Honeypot

- There are a variety of different approaches to building a honeypot:
  - You can just easily use any other operating system. Don't do anything special to this system, build it as you would any other. Then put the system on the Internet and wait.
  - Emulate variety of different systems. A commercial product called “CyberCopSting” Designed to run on NT, this product can emulate variety of different systems at the same time

The plan

- The simple plan is to build a box I wanted to learn about, put it on the network, and then wait.
  - How do I track the intruders moves?
  - How do I alert myself when the system is probed or compromised?
  - how do I stop the intruder from compromising other systems?
- The solution to this was simple, put the honeypot on its own network behind a firewall.

Tracking Their Moves

- Do not want to depend on a single source of information, track in layers.
- Do not log information on the honeypot itself.
  - The fewer modification you make to the honeypot, the better. The more changes you make, the better the chance a black-hat will discover something is up.
  - You can easily lose the information.

Tracking Their Moves

- first layer of tracking is the firewall logs.
- A second layer is the system logs!!!
- third layer of tracking is to use a sniffer.
  - The advantage of a sniffer is it picks up all keystrokes and screen captures.
- run tripwire on the honeypot.
  - what binaries have been altered on a compromised system

The Sting

- We want to attract the intruders, monitor them, let them gain root, and then eventually put them off the system, all without them getting suspicious.
  - Rebooting the machine.
- To attract intruders, you can name honeypot enticing names:
  - “ns1.example.com” (name server).
  - “mail.example.com” (mail server).
  - “intranet.example.com” (internal web server).

Security Information Management (SIM)

- SIM provides a simple mechanism that allows security teams to collect and analyze vast amounts of security alert data.

  More specifically, SIM solutions collect, analyze and correlate – in real-time – all security device information across an entire enterprise.

- Correlated results are then displayed on a centralized real-time console that is part of an intuitive graphical user interface.