Intrusion Detection System (IDS)

# Intrusion and Intrusion Detecti

Intrusion : Attempting to brea or misuse your system.

Intruders may be from outside the network or legitimate users of the network.

Intrusion can be a physical, system or remote intrusion.

## Different ways to intrude

Buffer overflows Unexpected combinations Unhandled input

Race conditions

# Intrusion Detection Systems (IDS)

Different ways of classifying a ...-.. IDS based on

* anomaly detection
* signature based misuse
* host based
* network based

# Intrusion Detection Systems (IDS)

Different ways of classifying a ...-.. IDS based on

* anomaly detection
* signature based misuse
* host based
* network based

## Anomaly based IDS



This IDS models the normal us\_. network as a noise characterizatioh

Anything distinct from the noise is assumed to be an intrusion activity.

* E.g flooding a host with lots of packet.

The primary strength is its ability to recognize novel attacks.

**Drawbacks of Anomaly detection -S**

Assumes that intrusions will be acCOJl\ a ied by manifestations that are sufficiently unus a so as to permit detection.

These generate many false alarms and hence compromise the effectiveness of the **IDS.**

## Signature based IDS

This IDS possess an attacked ription that can be matched to sensed attaGk manifestations.

The question of what information is relevant to an IDS depends upon what it is trying to detect.

* E.g DNS, FTP etc.

## Signature based IDS (contd.)

ID system is programmed to interpret a c in series of packets, or a certain piece of data contained· n t ose packets,as an attack. For example, an IDS tha atches web servers might be programmed to look for th4string "phf' asan indicator of a CGI program attack.

Most signature analysis systems are based off of simple pattern matching algorithms. In most cases, the IDS simply looks for a sub string within a stream of data carried by network packets. When it finds this sub string (for example, the ''phf' in ''GET /cgi-bin/phf?"), it identifies those network packets as vehicles of an attack.

# Drawbacks of Signature based 1----------

They are unable to detect nave Suffer from false alarms

Have to programmed again for every new

'

pattern to be detected.

## Host/Applications based IDS

The host operating system or tr,, a; plication 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.

# Drawbacks of the host based

### IDS

The kind of information neede logged in is a matter of experience

Unselective logging of messages may greatly increase the audit and analysis burdens.

Selective logging runs the risk that attack manifestations could be missed.

# Strengths of the host based

### IDS

Attack verification System specific activity

Encrypted and switch environments

Monitoring key components

Near Real-Time detection and response. No additional hardware

## Stack based IDS



They are integrated closely wit he TCP/IP stack, allowing packets to be watc ea as

they traverse their way up the OSI layers. This allows the IDS to pull the packets from the stack before the OS or the application

have a chance to process the packets.

## Network based IDS

This IDS looks for attack signa i:es in network traffic via a promiscuous int i;face.

A filter is usually applied to determine which traffic will be discarded or passed on to an attack recognition module. This helps to filter out known un-malicious traffic.

# Strengths of Network based

### IDS

Cost of ownership reduced Packet analysis

Evidence removal

Real time detection and response Malicious intent detection Complement and verification Operating system independence

## Future of IDS

To integrate the network and h IDS for better detection.

Developing IDS schemes for detecting novel attacks rather than individual instantiations.

