

# Ethical Hacking

## **Intrusion Detection Systems**

# Intrusion Detection Systems

- IDS: Intrusion Detection System
- Programa usado para detectar accesos no autorizados a un computador o a una red.
- El funcionamiento se basa en el análisis pormenorizado del tráfico de red
- Al entrar al analizador es comparado con ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, etc.

# Intrusion Detection Systems

- Normalmente esta herramienta se integra con un firewall.
- Pero no protege ni filtra, sólo detecta.
- Algunos productos de Firewall han incluido IDS pero se siguen llamando Firewalls.
- Los IDS suelen disponer de una base de datos de patrones o “firmas” de ataques conocidos.

# Intrusion Detection Systems

- Dos tipos:
  - Network Intrusion Detection System (NIDS)
  - Host-Based Intrusion Detection System (HIDS)
  - Distributed Intrusion Detection (DIDS)

# Network Intrusion Detection (NIDS)

- Uses “Packet Sniffers” to read and analyze packets exchanged between hosts.
- Los “sensores” suelen estar localizados en los puntos críticos de la red que tiene que ser monitorizada:
  - La DMZ
  - Puntos finales de la red:
- Los sensores (sniffers) capturan todo el tráfico de la red y analizan el contenido de cada paquete en busca de tráfico malicioso

# Network Intrusion Detection (NIDS)

- Ejemplo: Snort
- Funciona como un sniffer de red
- Detecta la peligrosidad o no gracias a una base de reglas → Configuración crítica.
- Guarda las alertas en una base de datos mysql y un módulo especial llamado snort-mysql



# Network Intrusion Detection (NIDS)

- Hay más de 2000 reglas, aunque uno puede escribir las suyas
- Formato de una regla
- Rule header (action, protocol, address, port, direction, address, port)
- Rule options



# Network Intrusion Detection (NIDS)

- Ejemplo: alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any (flags: SF; msg: “SYN-FIN Scan”);)
- Cabecera: alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any
- Opciones: (flags: SF; msg: “SYN-FIN Scan”);)



# Network Intrusion Detection (NIDS)

- Para acceder a esa base de datos se puede usar ACID, una consola muy completa en php
- Permite visualizar alertas y gráficas

ACID Alert Listing

Home Search AG Maintenance [Back]

Added 0 alert(s) to the Alert cache

Queried DB on : Thu June 06, 2002 00:01:19

Meta Criteria	any
IP Criteria	any
Layer 4 Criteria	none
Payload Criteria	any

Displaying alerts 1-3 of 3 total

<input type="checkbox"/>	< Signature >	< Classification >	< Total # >	Sensor #	< Src. Addr. >	< Dest. Addr. >	< First >	< Last >
<input type="checkbox"/>	[arachNIDS] ICMP PING NMAP	attempted-recon	1 (9%)	1	1	1	2002-06-05 23:55:00	2002-06-05 23:55:00
<input type="checkbox"/>	[arachNIDS] ICMP Large ICMP Packet	bad-unknown	2 (18%)	1	2	2	2002-06-05 23:54:59	2002-06-05 23:54:59
<input type="checkbox"/>	[bugtraq] [CVE] [arachNIDS] NETBIOS NT NULL session	attempted-recon	8 (73%)	1	2	4	2002-06-05 20:52:50	2002-06-05 23:32:28

Action:  Selected ALL on Screen

[Loaded in 0 seconds]

ACID v0.9.6b21 ( by Roman Danyliw as part of the AirCERT project )

# Host-Based Intrusion Detection System (HIDS)

- En este caso, el sensor consiste normalmente en un agente software que monitoriza toda la actividad en el host en el que está instalado.
- Busca en las fuentes de información local del host, como los logs del sistema.
  - Sesiones de usuarios
  - Actividades de los usuarios privilegiados
  - Cambios en el sistema de archivos
  - ...

# Host-Based Intrusion Detection System (HIDS)

- En este caso, el sensor consiste normalmente en un agente software que monitoriza toda la actividad en el host en el que está instalado.
- Busca en las fuentes de información local del host, como los logs del sistema.
  - Sesiones de usuarios
  - Actividades de los usuarios privilegiados
  - Cambios en el sistema de archivos
  - ...

# Host-Based Intrusion Detection System (HIDS)

- Un ejemplo es OSSEC
- Free, open source host-based intrusion detection system (IDS).
- Realiza análisis de logs, integrity checking, monitorización del registro de Windows.
- Disponible para Linux, OpenBSD, FreeBSD, Mac OS X, Solaris y Windows.
- <http://www.ossec.net/main/about/>



# Intrusion Detection System

- Problemas:
- Falsos positivos y falsos negativos
- Su eficacia depende mucho de su configuración
- No son fáciles de implementar

# Intrusion Detection System

- Problemas:
- Falsos positivos y falsos negativos
- Su eficacia depende mucho de su configuración
- No son fáciles de implementar