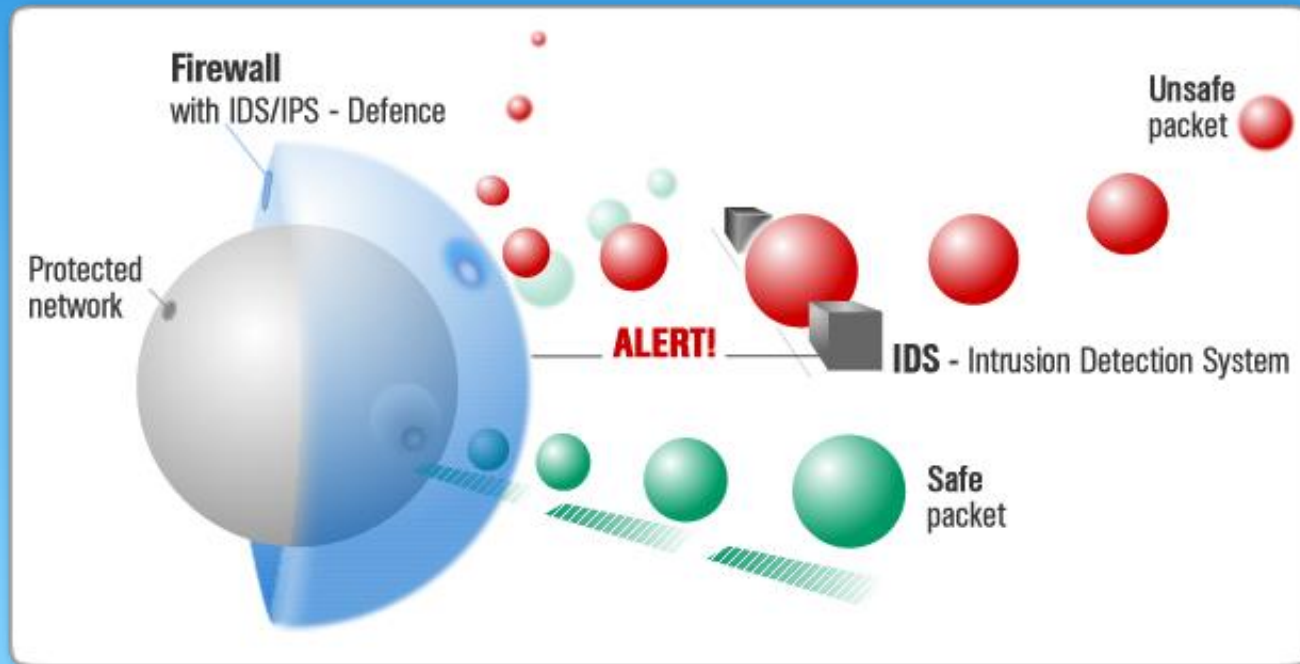


T1. Sistemas de detección y prevención de intrusiones (IDS/IPS)




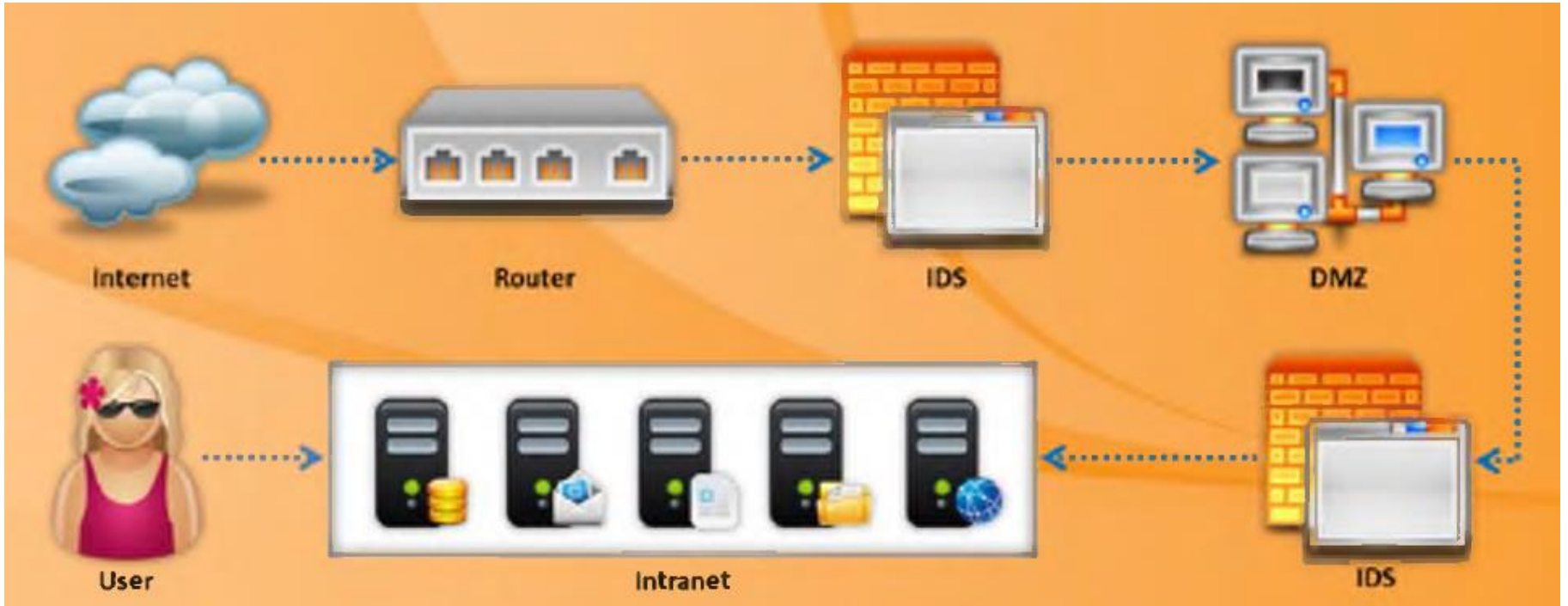
Apartados del BOE

- * Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
- * Identificación y caracterización de los datos de funcionamiento del sistema
- * Arquitecturas más frecuentes de los sistemas de detección de intrusos
- * Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
- * Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

Intrusion Detection System IDS

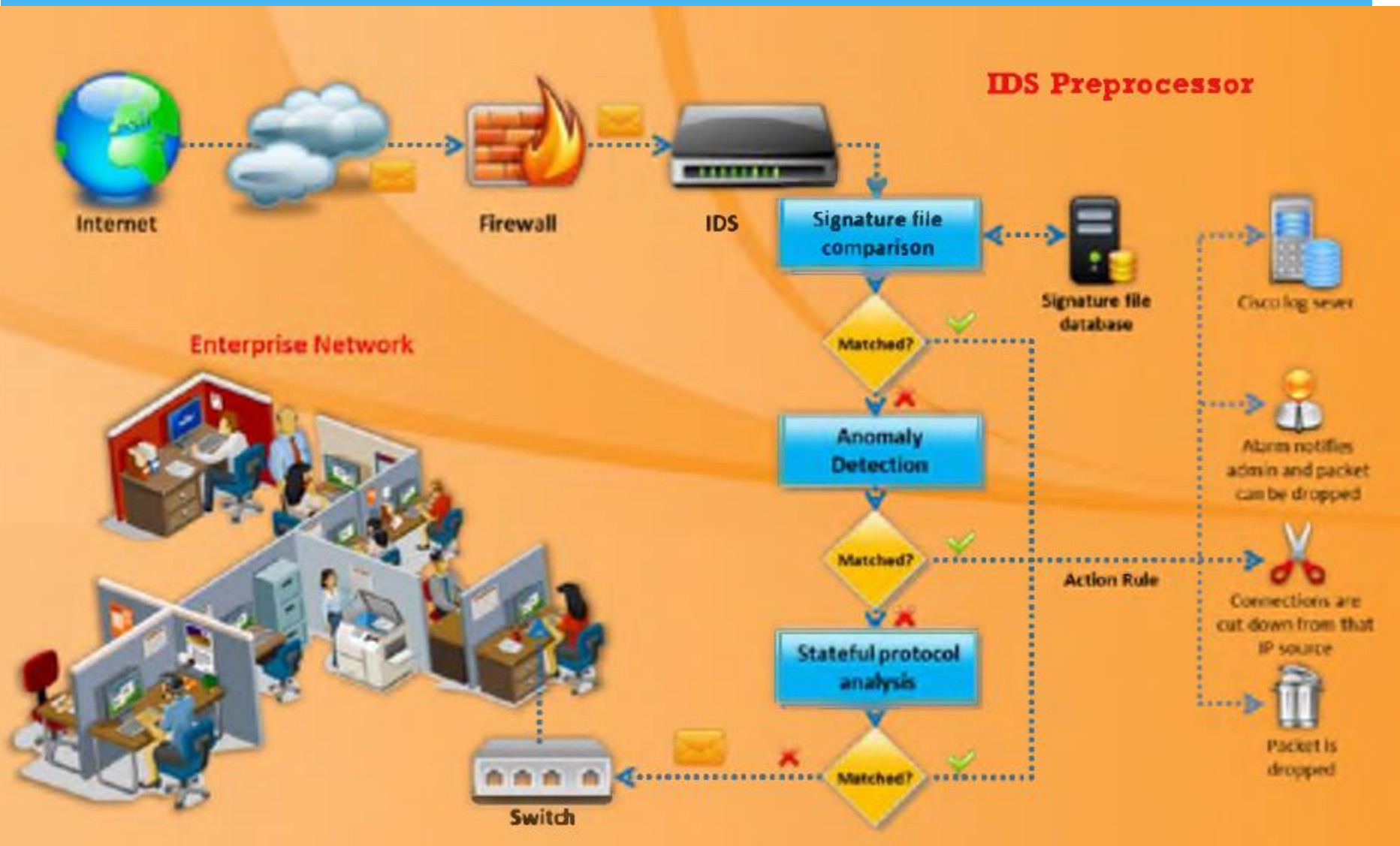
- * Un sistema de detección de intrusiones se utiliza para **monitorizar y proteger las redes** o sistemas debido a actividades maliciosas.
- * Para alertar al personal de seguridad acerca de las intrusiones, sistemas de detección de intrusiones son muy útiles.
- * Un IDS comprueba **actividades sospechosas y se notificarán** al administrador sobre las intrusiones de inmediato.

- 
- * Un sistema de detección de intrusiones (IDS) recoge y analiza la información desde un ordenador o una red, para identificar los posibles violaciones de la política de seguridad, incluyendo el **acceso no autorizado**, así como el uso malicioso.
 - * Un IDS también se conoce como un "**packet-sniffer**", que intercepta los paquetes que viajan a lo largo de varios medios y protocolos de comunicación, por lo general TCP / IP
 - * Los paquetes son analizados después de ser capturados
 - * Un IDS evalúa una intrusión sospechosa una vez que ha tenido lugar y da la señal de alarma



¿Cómo funciona un IDS?


- * Los principales **objetivos** de IDS's son que no sólo **impiden intrusiones** sino que también **alertan al administrador inmediatamente** si el ataque sigue en curso.
- * El administrador podría identificar métodos y técnicas utilizadas por el intruso y también la fuente de ataque.






* Un IDS funciona de la siguiente manera:

1. IDS's tienen sensores para **detectar firmas** y algunos IDS's avanzados tienen la detección de actividad de comportamiento para determinar el comportamiento malicioso. Incluso si las firmas no coinciden con este sistema de detección de actividad puede alertar a los administradores acerca de posibles ataques.

- 
2. Si la firma coincide, entonces se mueve al siguiente paso o las **conexiones son cortados de esa fuente IP**, el paquete se descarta, y la alarma notifica al administrador por lo que el paquete se puede descartar.
 3. Una vez que la firma es contrastada, entonces los sensores transmiten la **detección de anomalía**

- 
4. Si el paquete pasa a la etapa de anomalía, el estado del análisis de protocolo sería correcto. Después pasará a través del switch y pasarán los paquetes por la red. Si hubiera un desajuste de nuevo, las conexiones se cortarían de esa fuente IP, el paquete se descartaría, y la alarma se notificaría al administrador y el paquete se podría descartar.

Maneras de detectar una intrusión

- * **Reconocimiento de firmas**

- * También conocidas como **detecciones de abuso**, esto trata de identificar sucesos que indican un abuso en el sistema.

- * **Detección de anomalías**

- * Esta también es llamada “not– use detection”. El modelo consiste en una base de datos de anomalías. Cualquier suceso identificado en la base de datos y cualquier derivación del ataque será considerada como una anomalía. Crear el modelo es la tarea más difícil en un detector de anomalías.

- * **Protocolo de detección de anomalías**

- * Este protocolo está basado en las anomalías de un protocolo específico. Integra modelos de IDS recientes y también identifica protocolos TCP/IP específicos de la red.

Tipos de IDS

- * NIDS (Network-based IDS)
- * HIDS (Host-based IDS)
- * Log File Monitors
- * File Integrity Checking

NIDS Network-based IDS

- * Los NIDS revisan cada paquete que entra a la red en busca de anomalías o información incorrecta.
- * A diferencia de los firewall que son limitados para filtrar paquetes con contenido malicioso.
- * Los NIDS revisan cada paquete que atraviesa la red sin importar si son permitidos o no. Ya sea a nivel de IP o aplicación se genera una alerta.
- * Los NIDS tienden a ser mas distribuidos que los host-based IDS.
- * Básicamente son diseñados para encontrar anomalías en el router y a nivel de host.
- * Auditan la información contenida en los paquetes y guardan información de los paquetes maliciosos.
- * Un nivel de amenaza se asigna a cada riesgo después de que los paquetes de datos son recibidos. El nivel de amenaza permite al equipo de seguridad estar en alerta

HIDS Host-based IDS

- * En este caso los IDS analizan el comportamiento del sistema.
- * Los HIDS pueden ser instalados sobre cualquier sistema alcanzando desde un PC de escritorio hasta un servidor.
- * Es mas **versátil** que el NIDS. Un ejemplo de un HIDS es un programa que opera sobre un sistema y recibe las solicitudes de auditoría que operan los registros del sistema.
- * Son altamente efectivos detectando abusos internos. Residen sobre la confianza de las redes.
- * Están cerca de ser usuarios autenticados de la red. Si uno de estos usuarios intenta ingresar sin autorización, estos lo detectan y recolectan la información más importante.
- * Estos también son efectivos detectando modificaciones en archivos sin autorización (por aquello que el delincuente lo modifique). Se enfocan más en cambios específicos en los sistemas y son multi plataformas.

Log File Monitors (LFMs)

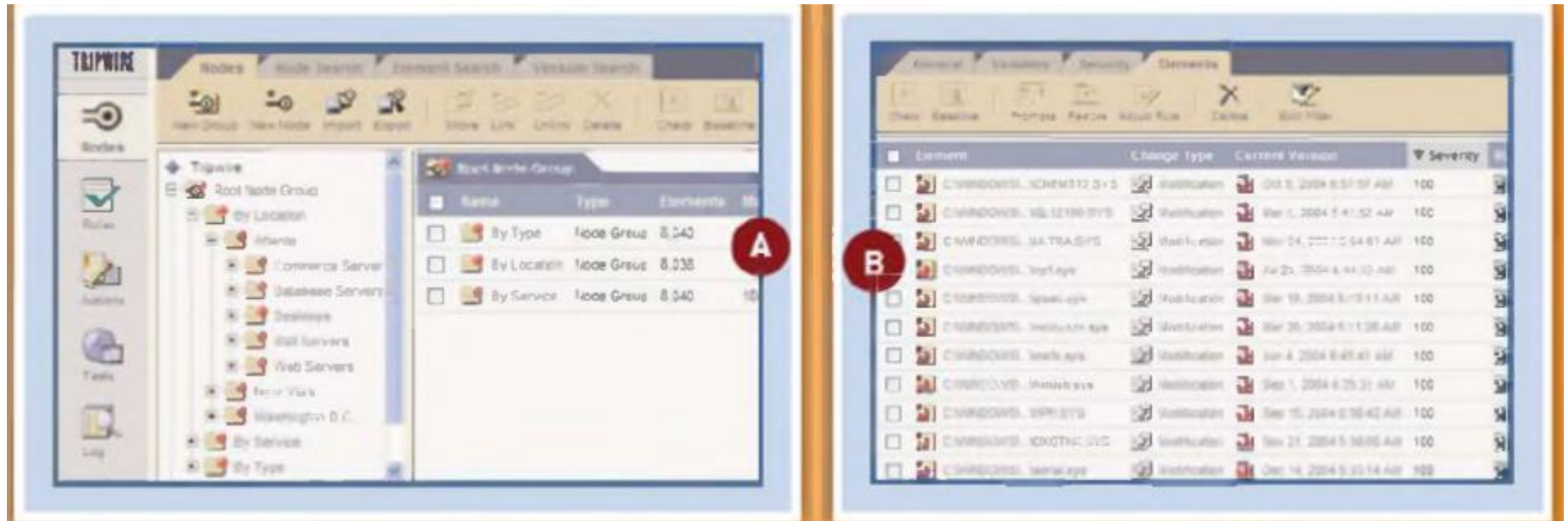
- * Estos monitorean los archivos logs creados por los servicios en la red.
- * Buscan a través de los archivos log e identifican sucesos maliciosos.
- * En manera similar a los NIDS , miran por patrones en los archivos log para ver si hubo una intrusión.
- * Un ejemplo típico podría ser analizar el log de un HTTP server , ya que cuando los intrusos usan técnicas o herramientas para encontrar fallos , si hacen peticiones a este server , toda petición queda registrada.

File Integrity Checking

- * Estos mecanismos buscan por troyanos o archivos que tienden a ser modificados, indicando que un intruso estuvo en el sistema. Ej: Tripwire
- * <http://www.tripwire.com/>

Verificadores de Integridad del sistema (SIV)

- * Monitorean archivos del sistema para determinar si un intruso ha **modificado los archivos**. Un monitor de integridad mira los objetos claves del sistema en busca de cambios.
- * Ej: Un básico monitor de integridad usa archivos del sistema o claves del registro para rastrear los cambios que hizo un atacante.
- * Aunque tienen funcionalidad limitada, estos pueden añadir una capa de protección a otras formas de detección de intrusos.
- * Una Herramienta es Tripwire.




Indicadores generales de intrusiones en el sistema

- * Para revisar si el sistema fue víctima de un ataque , debemos revisar ciertas cosas que indican que hubo presencia de un intruso en el sistema.
- * Cuando un intruso trata romper al sistema, estos intentos modifican archivos y configuraciones que indican una intrusión.




* Indicadores:


- * Intentos fallidos en la autenticación de usuarios.
- * Acceso activo de logins sin uso.
- * Logins en horas no laborales.
- * Nuevas cuentas de usuario.
- * Modificaciones en el sistema o archivos de configuración usando como acceso una cuenta administrador y la presencia de archivos ocultos.
- * Reducción del rendimiento del sistema.
- * Caídas del sistema, se reinicia solo.

- 
- * Los logs del sistema son cortos e incompletos.
 - * Fechas de los logs están modificados.
 - * Permisos sobre los logs están modificados.
 - * Los logs son borrados.
 - * El rendimiento del sistema es anormal.
 - * Nuevos procesos desconocidos en el sistema.
 - * Mensajes, ventanas se abren solas.
 - * Intentos de borrar los logs.

Indicadores en los archivos del sistema

- * Observando los files system puedes detectar si hubo presencia de un intruso.
- * Estos archivos guardan actividades del sistema.
- * Cualquier modificación o borrado en los atributos de un archivo o en estos, se considera que el sistema fue un blanco de ataque.

- 
- * Si encuentras nuevos archivos o programas en tu sistema, es una posibilidad de que hubo una intrusión, además este puede ser un punto para atacar otros sistemas (Como lo hace metasploit, una vez adentro se puede intentar acceder a otros).
 - * Cuando un intruso entra en el sistema, este trata de escalar privilegios hasta ser administrador, y cuando es administrador él puede cambiar los permisos de los archivos. Ej: si hay un archivo que no pudo modificar (logs , configuraciones) con la cuenta que tuvo acceso , ahora al ser admin podrá hacer lo que quiera.

- 
- * Cambio en el tamaño de los archivos son indicaciones de un ataque, por lo que habrá que analizarlos a fondo.
 - * Archivos perdidos es una posibilidad de una intrusión.
 - * Nombres extraños en directorios, que incluyen ejecutables con doble extensión.

Indicadores en la red

- * Incremento en el consumo de ancho de banda.
- * Identificación de intentos de logeo desde maquinas remotas.
- * Escaneos
- * Intentos de DOS conexiones masivas.

IDS Tools



**IBM Security Network
Intrusion Prevention System**

<http://www-01.ibm.com>



Peek & Spy

<http://networkingdynamics.com>



**INTOUCH INSA-Network
Security Agent**

<http://www.ttinet.com>



Strata Guard

<http://www.stillsecure.com>



**IDP8200 Intrusion Detection
and Prevention Appliances**

<https://www.juniper.net>



OSSEC

<http://www.ossec.net>



**Cisco Intrusion Prevention
Systems**

<http://www.cisco.com>



**AIDE (Advanced Intrusion
Detection Environment)**

<http://aide.sourceforge.net>



**SNARE (System iNtrusion Analysis
& Reporting Environment)**

<http://www.intersectalliance.com>



Vanguard Enforcer

<http://www.go2vanguard.com>



Check Point Threat Prevention Appliance

<http://www.checkpoint.com>



FortiGate

<http://www.fortinet.com>



fragroute

<http://www.monkey.org>



Enterasys® Intrusion Prevention System

<http://www.enterasys.com>



Next-Generation Intrusion Prevention System (NGIPS)

<http://www.sourcefire.com>



StoneGate Virtual IPS Appliance

<http://www.stonesoft.com>



Outpost Network Security

<http://www.agnitum.com>



Cyberoam Intrusion Prevention System

<http://www.cyberoam.com>



Check Point IPS-1

<http://www.checkpoint.com>



McAfee Host Intrusion Prevention for Desktops

<http://www.mcafee.com>