

# Detección de Intrusos

*Artículo original en inglés:*

<http://www.itsecurity.com/features/intrusion-detection-030807/>

Por el Staff de IT Security, 8 de Marzo del 2007

*Traducción 21-04-2007: Marcelo Ponce Iñigo*

*Adaptación y publicación: Lic. Cristian Borghello - Director de [www.segu-info.com.ar](http://www.segu-info.com.ar)*

## Objetivo

Descubrir los principios de la detección de intrusos, que es, quienes lo hacen y que tecnologías existen para prevenirlo.

## ¿Qué es la Detección de Intrusos?

Si chequeas las recomendaciones de la mayoría de los artículos recientes acerca de la detección de intrusos, veras que algunas de las metodologías principales se remontan a fines de la década del 80, antes de la Internet publica. Eso estuvo de moda cuando la mayoría de los intrusos eran probablemente chicos de la escuela secundaria o estudiantes de la universidad, que solo ejercitaban sus mentes. Ellos podían entrar a una red y cambiar unos archivos o solo dejaban una especie de tarjeta de visita para atribuirse los derechos de alardear por lo hecho. Usualmente no hacían nada serio, excepto en las películas.

Eso rápidamente cambio cuando la Internet publica se hizo popular comercialmente en los comienzos de la década del 90. Hoy, las amenazas pasan por temas financieros y legales serios para las compañías mundiales, y como resultado, del desarrollo acelerado y la implementación de la detección de intrusos ha hecho que se vuelva cada vez más importante.

La [Detección de Intrusos](#) (alias DI) es la practica de amenazas para el capital IT, tal como computadoras, bases de datos, redes y dispositivos. Este articulo esta intentando ser un manual básico para los administradores de sistemas de negocios pequeños que están aprendiendo acerca de la detección de intrusos, quienes lo hacen y las tecnologías que existen para prevenirla.

## ¿Por qué los ataques o el mal empleo?

Con hackers diciendo que [atacan algún lugar cada 39 segundos](#), hay razones numerosas para que los bienes de su compañía IT podrían estar bajo vigilancia ahora mismo.

### 1. Beneficio Financiero

Si los hackers pueden comprometer su sistema, ellos podrían encontrar un beneficio económico, para el acceso a cuentas electrónicas de un banco, robando números de tarjeta de crédito de un cliente, o solo revendiendo sus datos. Este tipo de hacker es mas probable que sea empleado por una organización criminal formal.

### 2. Espionaje industrial

A veces los competidores solo quieren acceder a los secretos de la compañía, datos o información de un cliente.

### **3. Hacktivismo**

Algunas personas hackean para llamar la atención de otros hackers y algunas porque han defendido, un tema político, tecnológico, religioso u otro.

### **4. CopyCatting**

Algunos hackers lo hacen solo para protestar por el arresto de otros hackers.

### **5. Resentimiento**

Empleados disgustados o ex empleados que tengan acceso pueden hacerlo en venganza por algún incidente en el que sientan que han sufrido un daño a manos de la compañía. Esos "hackers" a veces hacen espionaje interno también.

### **6. Alarde**

Algunos individuos lo hacen solo por diversión. Este es el tipo original de hacker, y son relativamente menos numerosos que años anteriores, este hacker aun es una amenaza de seguridad seria.

### **7. Test de seguridad**

Una organización de seguridad que quiera probar un lugar (o desarrollo de un negocio nuevo) debe orquestar un ataque para mostrar las vulnerabilidades de una compañía.

## **¿Qué necesita para su protección?**

Las piezas de software no son perfectas, y siempre puedes contar con hackers que atenten para explotar esas vulnerabilidades. Afortunadamente, la mayoría de los ataques al capital IT son variaciones simples de métodos de piratería informática antiguos, y como consecuencia, es útil estar familiarizado con la mayoría de los tipos comunes de ataques:

#### **1) Buffer OverFlow**

Para sobrecargar un sistema y para causar la sobrecarga del buffer, los paquetes de datos adicionales pueden evitar o saltar la detección de intrusos y terminar modificando otros datos. Las [sobrecargas de buffer](#) son [frecuentemente causadas internamente por errores de programación](#) pero pueden también ser causados externamente por un sistema creciente artificialmente y por tipos de tráfico de red.

#### **2) Ataques CGI**

Estos ataques explotan las fallos en los scripts CGI escritos para un servidor web. Los ataques típicamente comprenden explotar scripts estándar instalados y/o scripts escritos por programadores web sin experiencia.

#### **3) DoS/DDoS**

[DoS](#) (Denial of Service – Negación de Servicio) y [DDoS](#) (Distribuided Denial of Service – Negación de Servicio Distribuida) son esencialmente la misma cosa: un intento orquestado para sobrecargar una red o servicio (como un servidor web) para ponerlo fuera de servicio por un tiempo o para ganar un acceso por varias causas. DDoS usa puntos de ataque distribuidos en lugar de un punto simple. DoS son ataques realizados a veces como una [inundación de SYN](#) (SYN Flood)

#### **4) Uso indebido interno**

El [uso indebido](#) incluye el acceso a base de datos o adulterar un archivo por

empleados o ex empleados descontentos. Este ataque también puede ser motivado por competidores los cuales le pagan a empleados para realizar conductas de espionaje.

### **5) Tomar las huellas del Sistema Operativo (FingerPrinting)**

Estos son aptos para determinar [que tipo de](#) sistema operativo (SO) tiene su red, los hackers pueden determinar con mayor facilidad sus vulnerabilidades. Esto es frecuentemente usado cuando se [toma las huellas del stack TCP/IP](#).

### **6) Spoofing TCP/IP**

Esto típicamente son [direcciones IP que se falsifican](#) para luego pasar a ser uno o más sitios de confianza, servidores o computadoras. Esto a veces es hecho como parte de una inundación de SYN (SYN flooding)

### **7) Pruebas SMB**

Un [prueba de Server Message Block \(SMB\)](#) chequea un sistema para determinar que archivos compartidos están disponibles. Usándolo internamente, las pruebas pueden servir como un disparador de alertas. Usándolo externamente, a veces en la forma de un gusano, una prueba puede determinar las debilidades del un sistema. Las pruebas están también incluidas en la actividad de tomar las huellas del sistema operativo.

### **8) Escaneos de puerto oculto**

Los [escaneos de puerto oculto](#) chequea un sistema para verificar los [puertos usados comúnmente](#) (echo, ftp, ssh, telnet, domian, http) que pueden ser vulnerables. Esto es usado como una técnica de seguridad (usando herramientas libres como [Nmap](#)) así también como una [técnica de piratería informática](#).

## **¿Cuándo la Detección de Intrusos es necesaria?**

Ahora que tomo conocimiento de los principales ataques individuales, sus motivaciones para hacerlo, y alguna de la mayoría de los métodos comunes para atacar el capital IT, esto es importante para valorar si específicamente su compañía requiere de un sistema de detección de intrusos. La forma más rápida de saber si necesita un SDI – [Sistema de Detección de Intrusos](#) – es hacer una lista de control de las necesidades de seguridad como las siguientes:

1. ¿Tiene datos, que se encuentre en manos de gente errónea, con lo que pudo crear relaciones públicas que son una pesadilla para usted, y o perdió privacidad o financiamiento para sus clientes?
  - a. El cliente bancario, la tarjeta de crédito y otra información privada, la cual es protegida por la [ley Gramm-Leach-Bliley](#).
  - b. La salud de los registros del cliente, cuales deben estar protegidos de acuerdo con [HIPAA](#) (Ley para asegurar la salud de la Portabilidad y de la Contabilidad).
  - c. Grabaciones de las llamadas de los empleados, las cuales deben ser guardadas de acuerdo a la [ley Sarbanes-Oxley](#).
2. ¿Tiene datos, que si son robados pueden comprometer sus operaciones o credibilidad?

Esta es una lista de control muy simplista, hay otras actividades maliciosas las cuales pueden ocurrir como resultado de ataques que de otro modo necesitan de un sistema DI para la prevención. No obstante si pasando a través de la lista anterior, las respuestas dentro de su compañía son afirmativas es probable que necesite de un sistema de detección de intrusos.

## ¿Cómo trabaja la detección de intrusos?

Hablando de manera general, la detección de intrusos (DI) funciona mediante [la unión de información de un sistema](#) y el análisis de la misma ante eventos inusuales o inesperados. La información histórica se usa luego para la [prevención, apropiación, disuasión o desviación](#) del tráfico de red y el acceso a una computadora.

Para tener un entendimiento básico de los pasos específicos que la detección de intrusos realiza para mejorar la seguridad, aquí se tiene una lista de ejemplo de las acciones de DI (algunos ítems son específicos del sistema):

### 1. Actividad de monitoreo

Este es un monitoreo general de cualquier acceso de usuario y eventos del sistema. Parte de esta tarea es la localización de las violaciones a las normas de un usuario como así también la detección de patrones de actividad normal y patrones de ataque detectables. Una variedad de técnicas de análisis diseñadas para la detección de intrusos puede aplicarse para determinar si fueron realizadas intrusiones.

### 2. Chequeo de la configuración

¿Sus sistemas y redes están configurados correctamente? ¿Hay alguna vulnerabilidad detectable en los archivos de configuración del sistema? ¿Hay algún host listado en el archivo de nodos de red que no debería estar?

Cada máquina dentro de una red debería ser chequeada periódicamente. Los escaneos de puertos son una tarea, otra es asegurarse que los archivos de configuración no son accesibles para cualquiera.

### 3. Chequeo general de la máquina

Cada máquina en una red debería ser chequeada periódicamente por una variedad de problemas potenciales como se tratan en esta lista. Si una máquina en su red ha sido alterada todas las otras máquinas en la red deberían ser chequeadas.

### 4. Chequeo del archivo de autorizaciones

Los archivos deberían ser chequeados para determinar si las configuraciones de autorización de un grupo y de un usuario han sido alteradas. Una manera es tener un mapa de las configuraciones del archivo de accesos desde afuera de la red de los sistemas que están siendo protegidos y compararlo periódicamente con los accesos actuales.

### 5. Chequeo de los archivos ocultos

¿Hay algún archivo oculto o inesperado en algún lugar? Podrían ser virus, keyloggers, crackeadores de contraseñas, spyware, etc. Dependiendo del sistema operativo en uso, los archivos pueden estar ocultos mediante el uso de una cierta convención.

### 6. Examen del archivo log

El servidor, el proceso, el router y otros logs de seguridad pueden mostrar intrusiones mediante la extracción de datos o de eventos grabados. Los archivos log pueden mostrar el agrupamiento de los accesos desde ubicaciones específicas y/o patrones de frecuencia. Tenga en mente que este tipo de DI no sucede en tiempo real.

### 7. Chequeo de sniffer de paquetes

¿Sus sistemas están corriendo programas de monitoreo de red no autorizados, alias sniffers de paquetes? Estos pueden estar grabando los datos de la cuenta de un usuario.

## **8. Chequeo de los archivos de contraseñas**

Las cuentas no autorizadas/puerta traseras (backdoor) puede ser encontradas en los archivos de contraseñas del sistema. Simplemente borrando una cuenta autorizada no es suficiente, ya que puede haber otros archivos comprometidos. En este punto debe cambiar todas las contraseñas del sistema.

## **9. Procesos programados**

Chequee tanto los procesos no autorizados como los que parezcan ser procesos autorizados que utilizan archivos inusuales. Por ejemplo, si un [keylogger](#) ha sido instalado y esta grabando contraseñas y nombres de usuario, estos serán actualizados en algún momento, usualmente en un momento específico.

## **10. Chequeo de servicios**

¿Hay algún servicio no autorizado corriendo? La mayoría de los sistemas operativos tiene archivos de configuración de servicios, que pueden ser chequeados bastante rápido y pueden ser la señal de una intrusión.

## **11. Chequeo binario de archivos**

¿Alguno de sus binarios ha sido alterado? Debn chequearse los time/date stamp y los checksums de los archivos –el último no siempre es suficiente si un hacker ha emulado el checksum. Deberían utilizarse herramientas de checksum con criptografía fuerte para los archivos del sistema.

## **12. Evaluación del sistema y del archivo de integridad**

Cualquier cosa que no haya sido listada mas arriba como tests de integridad de su sistema y de sus archivos eson importantes para la detección de todo tipo de intrusión.

Mientras muchas de las funciones de la detección de intrusos nombradas anteriormente pueden ser realizadas manualmente es más seguro y fácil automatizar los chequeos mediante un sistema de detección de intrusos. Los sistemas de detección de intrusos automatizados son más poderosos ya que pueden realizar los chequeos necesarios de la integridad del archivo y hacer los análisis estadísticos con relativa facilidad. El análisis es una necesidad importante en la detección de intrusos, porque solo a través de las estadísticas de las anomalías es que los ataques se manifiestan. Los ejemplos de análisis de la detección de intrusos incluyen:

1. Igualar patrones y comparación de la firma de contenidos para detectar malware.
2. Análisis del comportamiento del tráfico para prevenir posibles ataques DoS/DDos u otras anomalías.
3. Análisis del agrupamiento IP para determinar la ubicación geográfica de los ataques.
4. Análisis del protocolo para examinar el tráfico de red en general.

Dentro del paraguas de los SDIs automatizados, hay dos tipos principales, los basados en host, y los basados en la red. Los SDI basados en host [monitorean](#) las llamadas al sistema, los logs y el tráfico de la red, y protegen solo a una máquina. Los SDI basados en la red monitorean los paquetes de red, las velocidades y hace un análisis estadístico de los patrones de tráfico.

## **Herramientas para la detección de intrusos**

Cada sistema de detección de intrusos emplea herramientas para hacer alguna o todas las funcionalidades antes mencionadas. Esta una lista de algunos SDI así como algunas de las herramientas mencionadas. Asegúrese de revisar las páginas blancas de [IT Security](#) para comparar algunos de los SDI mencionados anteriormente.

1. [AIDE](#)
2. [AirDefense](#) - Guard Enterprise (wireless solution)
3. [Arbor Networks](#) - Peakflow X
4. [Bro](#)
5. [CERIAS](#)
6. [CounterStorm](#) - Counterstorm-1
7. [Enterasys](#) - Dragon 7
8. [GFI Network Security](#) - GFI LANguard S.E.L.M
9. [ISS \(Internet Security Systems\)](#) - Real Secure Network
10. [Juniper Networks](#)
11. [Lancope](#) - Stealthwatch
12. [Netpoke](#)
13. [nmap](#)
14. [Prelude-IDS](#)
15. [SinFP](#)
16. [Snort](#)
17. [SonicWALL](#) - Gateway Intrusion Prevention
18. [StillSecure](#) - Strata Guard

A pesar de lo maravilloso, un sistema de detección de intrusos no es suficiente para proteger su capital IT, los sistemas DI no remueven las intrusiones totalmente, solo las identifican. Como consecuencia, los SDI trabajan mejor cuando están acoplados con un SPI ([Sistema de Prevención de Intrusos](#)).

Para aprender mas acerca de la detección de intrusos, vea Georgia Teach's [Lecturas en la Detección de Intrusos](#), las cuales aunque desactualizadas, incluyen cerca de 45 referencias más para la lectura. Para terminar, la Seguridad IT tiene un [Glosario SDI](#) el cual clarificara la terminología desconocida relatada para la detección de intrusos.