

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **ESCENARIO - DESCRIPCIÓN DEL MODELO DE PROCESO DE MADURACIÓN DE SEGURIDAD DE UNA EMPRESA (GARTNER)**

### **▪ Fase 1: Cazador-recolector.**

- ✓ La empresa no tiene conciencia de la importancia de la seguridad de la información.
- ✓ No existe ni presupuesto ni organización dedicada a la seguridad.
- ✓ Sólo existen ciertas medidas rudimentarias de seguridad (ej.: password)

Lamentablemente, son muchas las pequeñas y medianas empresas que a día de hoy siguen en esta etapa prehistórica con nula concienciación en cuanto a seguridad.

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **ESCENARIO - DESCRIPCIÓN DEL MODELO DE PROCESO DE MADURACIÓN DE SEGURIDAD DE UNA EMPRESA (GARTNER)**

### **▪ Fase 2: Feudal.**

- ✓ La seguridad es vista como un problema técnico.
- ✓ El presupuesto de seguridad proviene prácticamente todo, del presupuesto de Informática.
- ✓ Existen medidas de protección tipo antivirus y firewalls.

Se cree equivocadamente que se ha adoptado una correcta política de seguridad enfocando el problema desde un punto de vista técnico y se olvida que la seguridad no es un producto. La seguridad en los sistemas de información ha de tener en cuenta varios aspectos: organizativos, físicos, normativos, legales, humanos y técnicos.

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **ESCENARIO - DESCRIPCIÓN DEL MODELO DE PROCESO DE MADURACIÓN DE SEGURIDAD DE UNA EMPRESA (GARTNER)**

### **▪ Fase 3: Renacimiento.**

- ✓ La Dirección reconoce la importancia de la seguridad sobre los procesos de negocio.
- ✓ Parte del presupuesto proviene de la parte no técnica del negocio aunque mayoritariamente se invierte en tecnología.
- ✓ Existen equipos de respuesta / emergencia informáticos.

Son pocas las empresas en general que han alcanzado esta etapa en la que existe un saltó cualitativo, ya que se enfoca el problema de la seguridad como un análisis de riesgos (riesgo enfocado a negocio).

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **ESCENARIO - DESCRIPCIÓN DEL MODELO DE PROCESO DE MADURACIÓN DE SEGURIDAD DE UNA EMPRESA (GARTNER)**

### **▪ Fase 4: Industrial.**

- ✓ La seguridad forma parte de la cultura corporativa de la empresa.
- ✓ La empresa reconoce que la seguridad es función de personas, procesos y herramientas.
- ✓ Existe la figura de CISO, responsable de la seguridad (Unidad independiente de informática ligada a negocio).

Esta es la etapa que se debería alcanzar. Las empresas de seguridad deben ayudar, generando modelos seguros que cubran los siguientes aspectos: organizativos, físicos, normativos, legales, humanos y técnicos de una entidad.

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## ORGANIZACIÓN DE LA SEGURIDAD



LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS

Albert Gabàs  
&  
M.I. Research Team  
18/09/2003

## MODELO DE PROTECCIÓN DE LA EMPRESA

Firewalls

Vulnerability Assessment

Network Intrusion Prevention

Host Intrusion Prevention

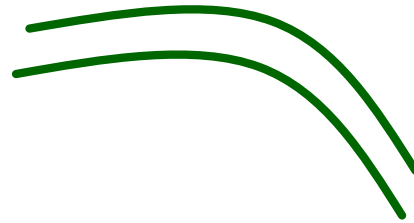
Antivirus

Security Management

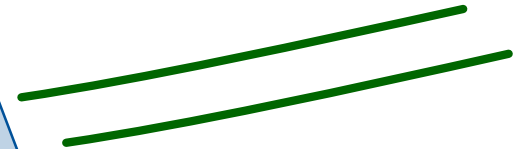
## NETWORK SECURITY NIRVANA

LOS IDS HAN  
MUERTO, LA  
PREVENCION DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS

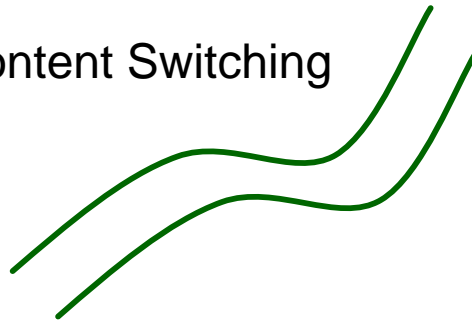
Application Defenses



Firewalls



Content Switching



IDS



Albert Gabàs  
&  
M.I. Research Team

18/09/2003

## LOS IDS NOS ENCAMINAN A LOS IPS

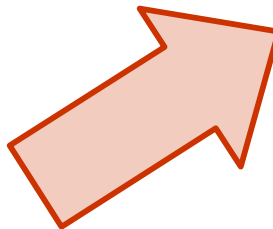
**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team**

**18/09/2003**

### **IDS**

- ✓ Montañas de datos
- ✓ Horas de control
- ✓ Multitud de alertas
- ✓ Falsos positivos
- ✓ Pesadillas ante la contestación de incidentes



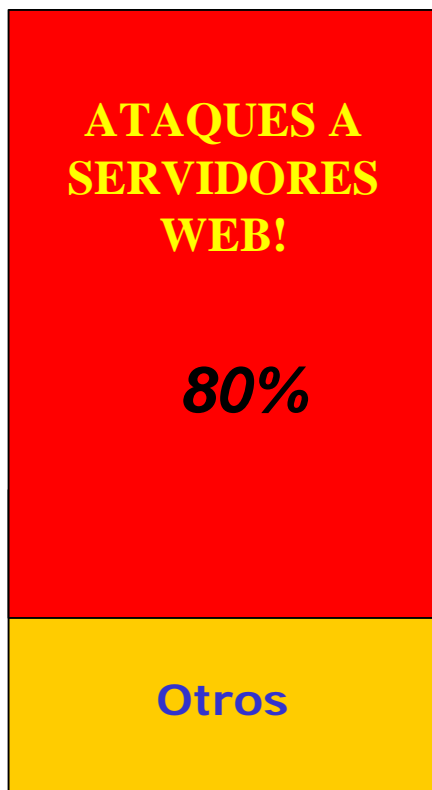
### **Intrusion Prevention**

- ✓ Repudia ataques de protocolo
- ✓ Bloquea ataques conocidos y desconocidos
- ✓ Menos pérdida de tiempo preguntando "qué pasó?"

LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS

Albert Gabàs  
&  
M.I. Research Team  
18/09/2003

## PROBLEMATICA



- La consultora americana Gartner estima que el 80% de los ataques con éxito se realizan a través de Aplicaciones Web.
- IBM estima una media de 65 vulnerabilidades por cada 10,000 líneas de código.

LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS

Albert Gabàs  
&  
M.I. Research Team  
18/09/2003

## TOP-10 VULNERABILIDADES DE APLICACIÓN

- **Parámetros no validados:** La información de una petición Web no se valida antes de ser utilizada por la aplicación Web. Un intruso podría usar este fallo para acceder a componentes del backend a través de la aplicación.
- **Control de accesos débil:** Se aprovechan restricciones débiles y permisos no implantados correctamente.
- **Cuentas débiles e identificación de sesión:** Las credenciales de una cuenta o de su sesión no están correctamente protegidas.
- **Cross-Site Scripting (XSS):** Los componentes de la aplicación Web podrían usarse para lanzar un ataque contra el navegador de un usuario final.

LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS

Albert Gabàs  
&  
M.I. Research Team  
18/09/2003

## TOP-10 VULNERABILIDADES DE APLICACIÓN

- **Buffer Overflows:** Los componentes de una aplicación Web, programados en diferentes entornos no validan ciertas entradas y se podrían explotar.
- **Command Injection:** Las aplicaciones Web, pueden pasar ciertos parámetros, cosa que podría ser aprovechada para ejecutar comandos, inyectar código SQL y tomar cierto control del servidor.
- **Problemas de errores de dirección:** Problemas que ocurren durante el uso normal de la aplicación por problemas de dirección. Pueden revelar datos del sistema o provocar DoS.

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

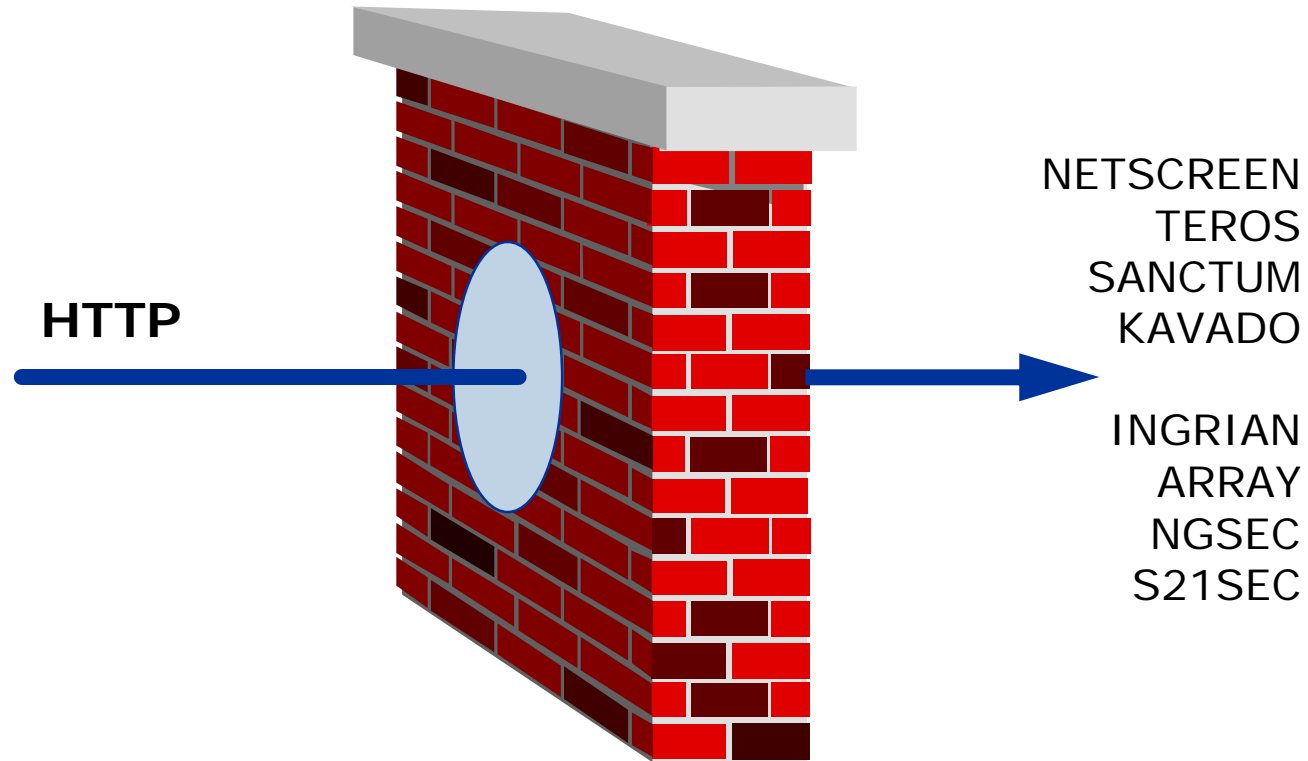
Albert Gabàs  
&  
M.I. Research Team  
18/09/2003

## **TOP-10 VULNERABILIDADES DE APLICACIÓN**

- **Uso inseguro de la criptografía:** Las aplicaciones Web suelen usar funciones criptográficas para proteger la información y sus credenciales. A veces puede ser complejo integrar estas funciones con la aplicación Web por lo que pueden dejar debilidades en la misma.
- **Problemas de Administración Remota:** Muchas aplicaciones Web permiten el acceso remoto de un administrador, si estas funciones no están protegidas correctamente, se puede lograr acceso como dicho administrador al sistema.
- **Falta de configuración del Web y/o del servidor de aplicación:** Debido a la no fácil securización de un servidor o sus servicios, equipos no securizados e instalados por defecto implican agujeros de seguridad fáciles de explotar.

## DEFENDIENDO APLICACIONES

LOS IDS HAN  
MUERTO, LA  
PREVENCION DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS



Albert Gabàs  
&  
M.I. Research Team

18/09/2003

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **DEFENDIENDO APLICACIONES**

### ▪ **NetScreen-IDP:**

Netscreen es una de las empresas más importantes en el mercado de Firewalls y de las pocas que han dado un salto cualitativo incorporando un producto IDP en sus soluciones.

Este IDP destaca por la robustez en cuanto al hardware y la sofisticada detección de ataques:

- ✓ Stateful Signature
- ✓ Protocol Anomaly
- ✓ Backdoor Traffic Anomaly
- ✓ IP Spoofing
- ✓ Layer 2 and SYNflood Detection

Dispone de una red Honeypot, que hace al producto casi perfecto a tener en cuenta en empresas de cierto calibre.

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **DEFENDIENDO APLICACIONES**

### ▪ **Sanctum-AppShield:**

Solución basada en Software (Windows, Solaris), es uno de los productos más maduros del mercado, gestado en parte en una unidad de élite del ejército Israelí.

Cabe destacar que en importantes instituciones de Estados Unidos usan AppShield y cuenta con un gran número de certificaciones, entre las que destacamos la certificación ICSA entre otras de terceros como IBM, CheckPoint, Sun, RSA, etc.

AppShield se basa en el endurecimiento de políticas de lo que considera "no aceptable" por una aplicación y reconociendo el cliente, genera ciertas reglas de tráfico que el cliente puede seguir.

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **DEFENDIENDO APLICACIONES**

### **▪ Sanctum-AppShield:**

Por defecto esta solución previene de los siguientes ataques:

- ✓ Contra campos de formulario agregados o borrados.
- ✓ Campos de formulario ocultos que tienen sus valores modificados por el cliente.
- ✓ Modificación de cookies por parte del cliente.

Es de los que mejor se adapta al concepto de automatización de políticas. Aunque es recomendable, en escenarios muy específicos puede presentar problemas con las páginas generadas dinámicamente. Es una solución destacable, pero no tan global como la propuesta por NetScreen.

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team**

**18/09/2003**

## **DEFENDIENDO APLICACIONES**

### **▪ Teros-100 APS:**

Es una solución basada en Hardware, el producto sólo ha estado en el mercado desde el pasado mayo, lo que no da garantías de su comportamiento en producción.

De las diferentes soluciones, Teros-100 APS mostró ser el más potente en cuanto a lo que se pretende que haga un Firewall de aplicación Web.

Su exclusiva capacidad para reconocer y controlar la transmisión de "objetos" comerciales, como los números de tarjetas de crédito y de Seguridad Social, proporciona un valor instantáneo a organizaciones que necesiten implementar rápidamente una solución fuerte de seguridad para afianzar la privacidad y el control de datos de sus clientes.

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **DEFENDIENDO APLICACIONES**

### **▪ Teros-100 APS:**

Proporciona seis características de alto nivel para la protección del contenido y, además, por defecto, el producto realiza chequeos a nivel del protocolo HTML.

Incorpora una protección anti-defacements, opción que previene al servidor Web de mostrar páginas no aprobadas.

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **DEFENDIENDO APLICACIONES**

### **▪ Interdo de Kavado:**

InterDo desde sus inicios ha seguido el camino del AppShield, aunque se aprecian notables diferencias en su arquitectura, que lo hacen más adecuado para usar en un cluster de balanceadores de carga.

Ofrece menos flexibilidad en su control sobre URLs arbitrarias y no tiene ninguna opción para definir un punto de entrada para sites.

En cambio AppShield y el Teros APS nos permiten definir unos puntos de entrada para construir una lista dinámica y cambiante de URL's permitidas para cada usuario conectado.

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **DEFENDIENDO APLICACIONES**

### **▪ Interdo de Kavado:**

El apoyo a servicios Web es una área de crecimiento importante para los cortafuegos de aplicación. InterDo tiene la primacía clara en este área ya que puede proteger el tráfico de servicios Web, capacidad ausente en Teros APS y AppShield.

Le avalan certificaciones de Sun, Radware, RSA, CheckPoint & OPSEC e Ingrian.

Se destaca de esta solución su gran flexibilidad, configurabilidad y extensibilidad, que la hacen práctica aunque puede considerarse una solución aún poco madura.

## DEFENDIENDO APLICACIONES

**LOS IDS HAN MUERTO, LA PREVENCIÓN DE INTRUSIONES ABRE NUEVAS EXPECTATIVAS**

Teros-100 APS		InterDo 3.0	AppShield 4.0
CAPACIDAD	EXCELENTE	BUENO	POBRE
RENDIMIENTO	BUENO	BUENO	BUENO
INTEROPERABILIDAD	BUENO	BUENO	EXCELENTE
MANEJABILIDAD	BUENO	BUENO	BUENO
FLEXIBILIDAD	BUENO	EXCELENTE	BUENO
SEGURIDAD	EXCELENTE	BUENO	BUENO

Evaluación por eWeek

Albert Gabàs  
&  
M.I. Research Team  
18/09/2003

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **DEFENDIENDO APLICACIONES**

### **▪ HIVE de S21SEC:**

Producto español comercializado como una solución en caja cerrada. Es el más inmaduro de los tratados en esta presentación, no cuenta con presencia internacional y el número de instalaciones es prácticamente nulo, por lo que son más recomendables soluciones que hayan demostrado sobradamente su funcionalidad en entornos de producción.

La información disponible sobre dicho producto es escasa y no se conocen los mecanismos que hacen que esta solución cumpla sus cometidos, por lo que es complicado contrastarlo con otras soluciones del mercado.

Para más información, S21SEC a día de hoy esta vendiendo dicha solución como un todo propietario. Se ha podido ver recientemente una noticia en un foro público de Internet que afirmaba que HIVE-OS, es una Slackware-Linux (GPL).

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## DEFENDIENDO APLICACIONES

### ▪ HIVE de S21SEC:

Intentamos contrastar esta noticia técnicamente y nos encontramos que la respuesta a un análisis de Fingerprinting con la herramienta Nmap 3.46 es:

(The 1210 ports scanned but not shown below are in state: filtered)

PORT STATE SERVICE

8080/tcp open http-proxy

Device type: general purpose

Running (JUST GUESSING) : **Linux** 2.2.X|2.1.X|2.3.X (93%)

Aggressive OS guesses: **Linux kernel** 2.2.22 (93%), **Linux** 2.2.21 SMP (X86)

(93%), **Linux** 2.2.12 - 2.2.19 (93%), **Linux** 2.1.19 - 2.2.25 (90%), **Linux**  
2.2.14 (89%), **Linux** 2.2.19 - 2.2.20 (87%), **Linux** 2.3.28-33 (86%), **Linux**  
2.2.5 - 2.2.13 SMP (86%), **Linux Kernel** 2.1.88 (86%)

No exact OS matches for host (test conditions non-ideal).

Nmap run completed -- 1 IP address (1 host up) scanned in 399.763 seconds

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **DEFENDIENDO APLICACIONES**

### ▪ **HIVE de S21SEC:**

No satisfechos, contactamos con ex-técnicos/becarios de desarrollo de S21SEC, que afirman lo expuesto con anterioridad.

Slackware y paquetes como Apache, Lilo y el propio Kernel de Linux, supuestamente usados y modificados por S21SEC **tienen LICENCIA GPL**, que prohíbe prácticas comerciales con software bajo esta licencia, si la solución no es "libre".

Este hecho podría ocasionar problemas en cuanto a propiedad intelectual, por lo que desaconsejamos esta solución. Es curioso que no se preguntaran porque Nokia usa BSD.

Más información sobre violación de la Licencia GPL:

<http://es.gnu.org/Licencias/viol.html>

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **DEFENDIENDO APLICACIONES**

### **▪ NGSecureWeb-NGSEC:**

Producto distribuido como solución host o general instalándose en un Firewall Microsoft ISA Server.

Es la solución más enfocada a la practicidad y cuenta en su última versión con una herramienta de gestión remota a destacar.

NGSEC es una empresa española pionera en el desarrollo de soluciones de prevención de intrusiones, con una creciente y destacable proyección internacional.

NGSecureWeb cubre un gran abanico de servicios y sistemas operativos, que lo hacen instalable en prácticamente todos los escenarios posibles.

Esta solución, protege los sistemas ante vulnerabilidades conocidas, y algunas que aún están por descubrir.

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## DEFENDIENDO APLICACIONES

### ▪ NGSecureWeb-NGSEC:

Se destaca la eficaz protección ante diversos métodos que enumeramos a continuación:

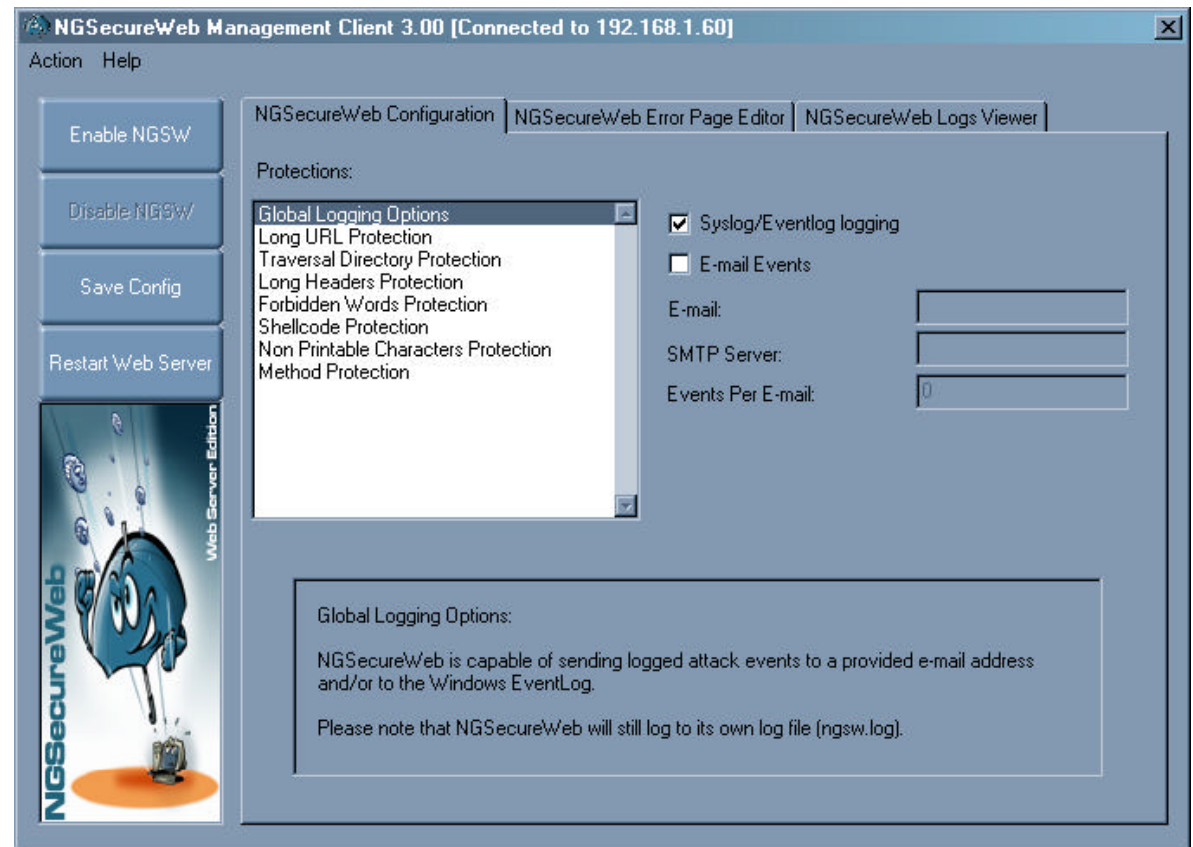
- ✓ Directory traversal attacks
- ✓ Forbidden Words
- ✓ Shellcode
- ✓ Long Headers (buffer overflows)
- ✓ Long GET (buffer overflows)
- ✓ Long POST (buffer overflows)
- ✓ Long URL (buffer overflows)
- ✓ Non printable Characters
- ✓ SQL injection (xp\_cmdshell , UNION, ...)

**LOS IDS HAN  
MUERTO, LA  
PREVENCION DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## DEFENDIENDO APLICACIONES

### ■ NGSecureWeb-NGSEC:



NGSecureWeb Management Client 3.00 [Connected to 192.168.1.60]

Action Help

Enable NGSW

Disable NGSW

Save Config

Restart Web Server

NGSecureWeb Configuration | NGSecureWeb Error Page Editor | NGSecureWeb Logs Viewer

Protections:

Global Logging Options  
Long URL Protection  
Traversal Directory Protection  
Long Headers Protection  
Forbidden Words Protection  
Shellcode Protection  
Non Printable Characters Protection  
Method Protection

Syslog/Eventlog logging  
 E-mail Events

E-mail:

SMTP Server:

Events Per E-mail:

Global Logging Options:  
NGSecureWeb is capable of sending logged attack events to a provided e-mail address and/or to the Windows EventLog.  
Please note that NGSecureWeb will still log to its own log file (ngsw.log).

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **DEFENDIENDO APLICACIONES**

### **▪ NGSecureWeb-NGSEC:**

La trayectoria profesional de su equipo de desarrollo, equipo que ha implementando una solución práctica más que suficiente en muchos entornos, hace que en relación calidad precio, esta solución, sea una de las más recomendables.

<http://www.ngsec.com>

**LOS IDS HAN  
MUERTO, LA  
PREVENCIÓN DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**Albert Gabàs  
&  
M.I. Research Team  
18/09/2003**

## **RECOMENDACIONES**

Desde Mentres Inquietas se recomienda:

- Retrasar grandes inversiones en IDS.
- Realizar pruebas piloto con productos IPS.
- Endurecer servidores críticos y analizar el impacto ante posibles vulnerabilidades de aplicación.



"Computers are useless. They can only give you answers." Picasso

**LOS IDS HAN  
MUERTO, LA  
PREVENCION DE  
INTRUSIONES  
ABRE NUEVAS  
EXPECTATIVAS**

**GRACIAS**

**Albert Gabàs  
&  
M.I. Research Team**

**18/09/2003**

Referencias: Richard Stiennon (Gartner)