Sistemas de Detección de Intrusos

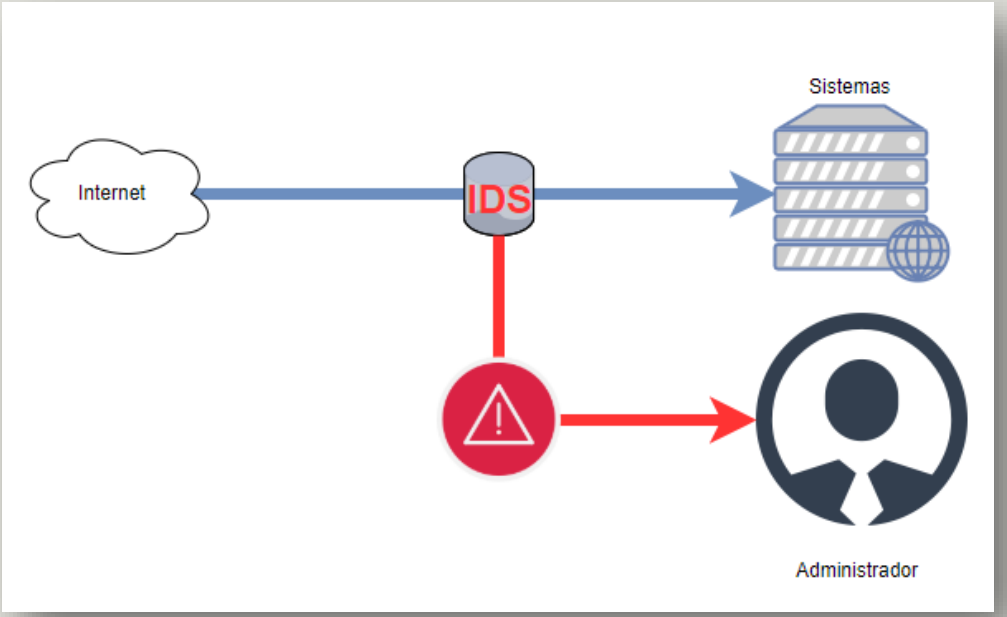
MARTA ARENAS MARTÍNEZ

PABLO REY PEDROSA

¿Qué es un IDS?

Programa que monitoriza la actividad de un sistema o una red en busca de intentos de **intrusión.**

Una intrusión es cualquier **acción** que intente **comprometer** la **integridad**, **co nfidencialidad** o **disponibilidad** de un recurso.



Características

1. ~~Supervisión~~
2. Tolerancia a fallos
3. Resistencia a perturbaciones
4. Sobrecarga ↓
5. Detectar desviaciones en el comportamiento estándar y hacer frente a cambios en él
6. Adaptabilidad al sistema
7. Ser difícil de engañar

Motivación

Aumento del número de incidentes de ciberseguridad año tras año.

Solo en 2017 casi **160.000.**

El **93%** podrían haberse evitado.

2017 Incident Highlights

159,700 total cyber incidents in 2017 (OTA)

93% of breaches could have been prevented (OTA)

18.2% increase in reported breach incidents (RBS)

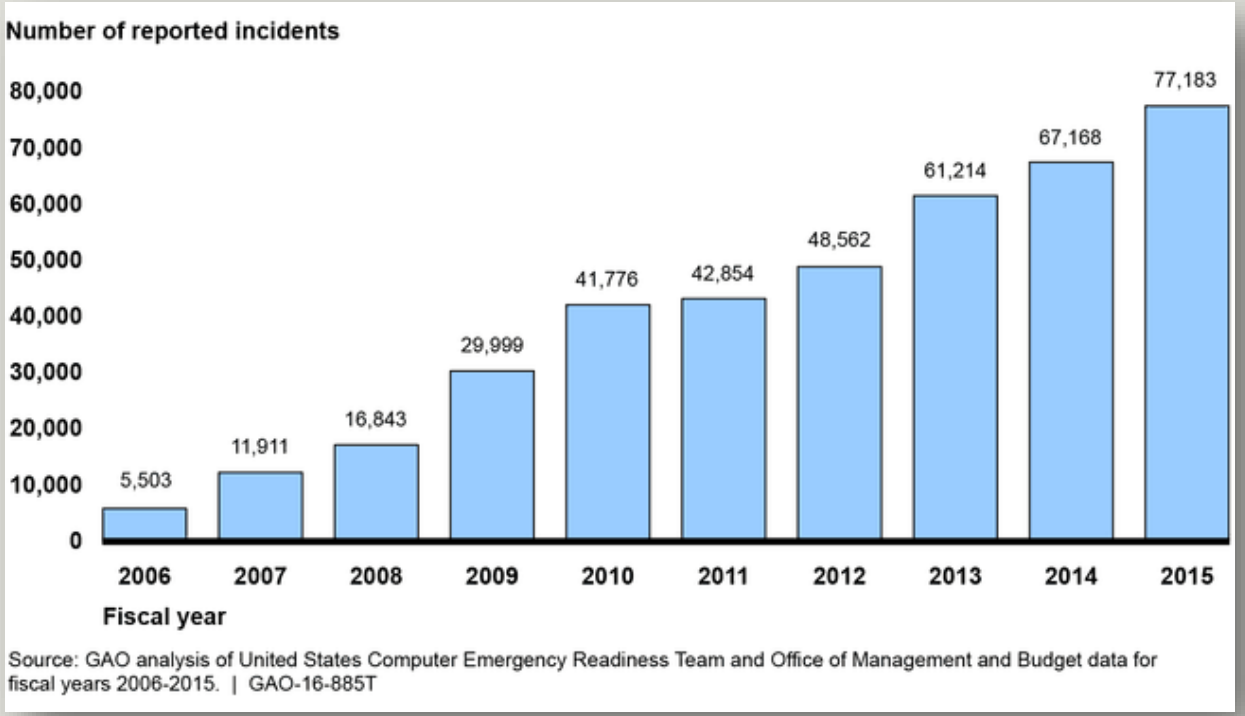
7 billion records exposed in first 3 quarters (RBS)

$5 billion financial impact of ransomware (CV)

90% rise in business targeted ransomware (Symantec)

$5.3 billion in global BEC losses (FBI)

Worldwide estimates. Sources: (OTA) Online Trust Alliance, (RBS) Risk Based Security, Cybersecurity Ventures (CV)



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

Motivación

Aumento no solo en número sino también de gravedad.

- Ransomeware
- DDOS

Clasificación

Hay dos grandes grupos, y cada uno de ellos está a su vez dividido en otros dos:

1. En función de qué sistemas vigilan:
   a) IDSes basados en red.
   b) IDSes basados en host.
2. En función de cómo vigilan:
   a) Detección de anomalías.
   b) Detección de usos indebidos.

En función de qué sistemas vigilan

1. IDSes basados en red: monitorizan los paquetes que circulan por una red buscando elementos que denoten un ataque.
2. IDSes basados en host: protegen un único sistema. Busca patrones que puedan denotar un intento de intrusión. Se dividen en tres subgrupos:
   a) Verificadores de integridad del sistema.
   b) Monitores de registros
   c) Sistemas de decepción

En función de cómo vigilan

1. Detección de anomalías: el sistema supone que una intrusión se puede ver como una anomalía.
2. Detección de usos indebidos: el sistema presupone que podemos establecer patrones para los diferentes ataques conocidos y sus variaciones.

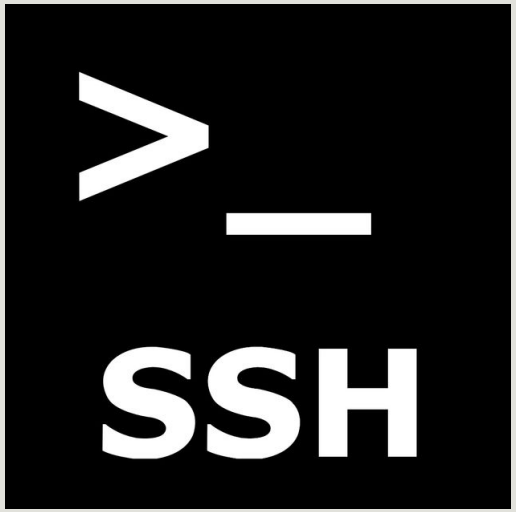
Técnicas para detectar intrusiones

1. Verificación de la lista de protocolos.
2. Verificación de los protocolos de la capa de aplicación.
3. Reconocimiento de ataques de comparación de patrones.

Demo

Demo

70 HTTP ≤ 10 s



5 SSH ≤ 30 s