# Respuesta automática ante intrusiones

Antonio Villalón Huerta

avillalon@tissat.es

TISSAT, S.A.

# Índice de materias (I)

- Definiciones previas.
- Sistemas de detección de intrusos.
- Respuesta automática.
- Esquema de funcionamiento.
- Ejecución de la AR.
- Respuesta automática vs. manual.
- Tipos de respuesta.

# Índice de materias (II)

- Peligros de la AR.
- Minimización del riesgo.
- Algoritmo de activación.
- Algunos ejemplos.
- Conclusiones.
- Referencias.

# Definiciones previas

- **Intrusión:** Conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso.
- **Detección de intrusos:** Análisis automático de parámetros que modelan la actividad de un entorno con el propósito de detectar e identificar intrusiones.

# Sistemas de detección de intrusos

- El IDS no tiene por qué ser un programa o producto concreto.
- Habitualmente:
  - *Network–based IDS*, NIDS (vs. *Host–based IDS*, HIDS).
  - Detección de usos indebidos (vs. detección de anomalías).
  - Detección distribuida.

# Sistemas de detección de intrusos

¿Son necesarios? **SÍ**

- Los sistemas cortafuegos no son mágicos.
- Proporcionan conocimiento del entorno.
- Alertas ante actividades sospechosas.
- Registro adicional de incidentes. . . ¿Pruebas judiciales?
- . . .

# Sistemas de detección de intrusos

¿Son suficientes? **NO**

- Normalmente, sólo detectan ataques conocidos.
- Es posible (y a veces fácil) engañarlos.
- ¡IMPORTANTE!: Mecanismos de seguridad **pasivos**.
- . . .

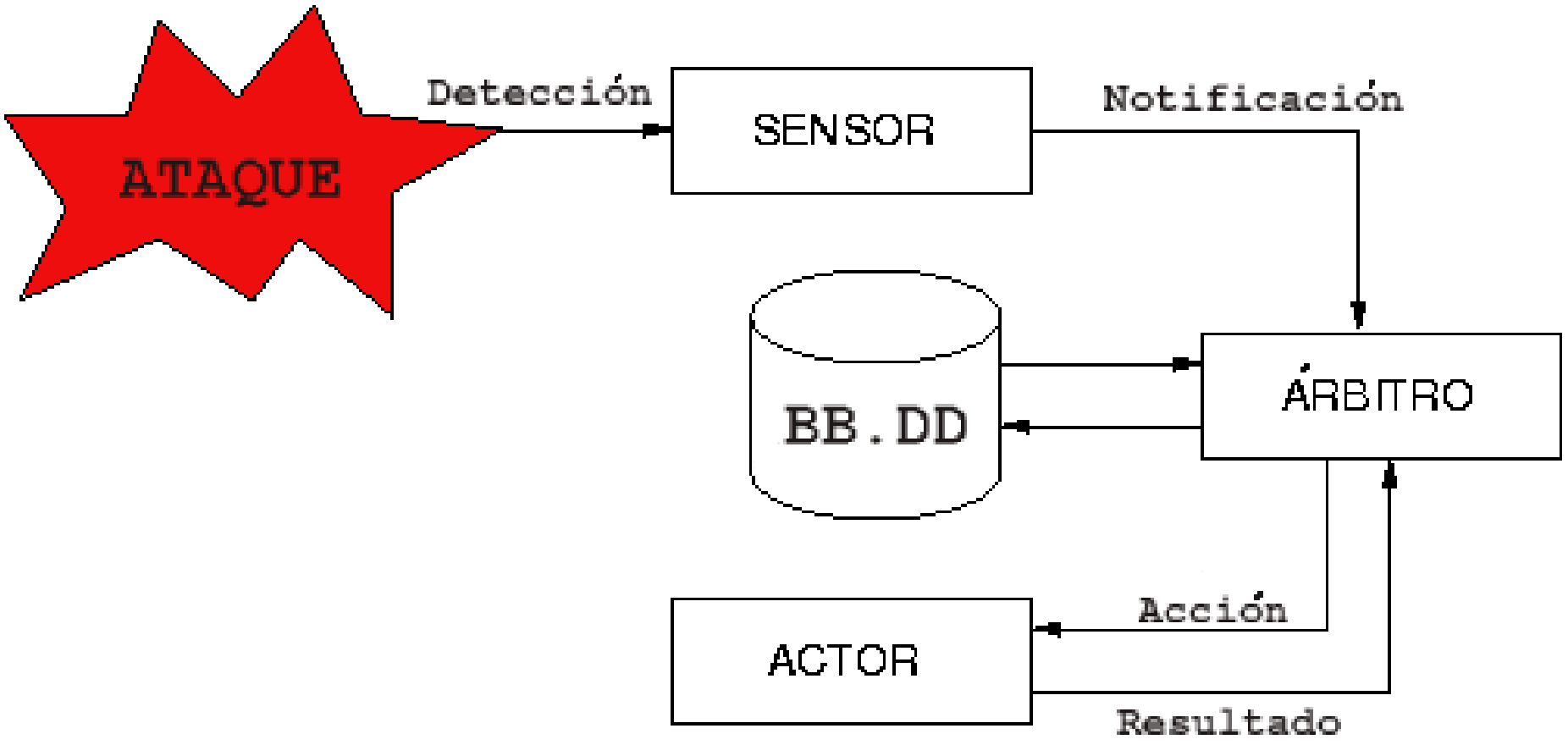
# Respuesta automática

- Nos interesa responder ante un ataque, transformando el esquema de IDS en un elemento **activo**.
- Dos tipos de respuesta: manual y automática.
- ¿Por qué responder ante un ataque muchas veces conocido?

# Respuesta automática

**Respuesta automática (AR):** Conjunto de acciones que se ejecutan sin intervención humana al detectar un evento, generalmente con el objetivo de salvaguardar la integridad, disponibilidad o confidencialidad de un determinado recurso.

# Esquema de funcionamiento



# Ejecución de la AR

- Una intrusión – una respuesta.
- Una intrusión – varias respuestas.
- Varias intrusiones – una respuesta.
- Varias intrusiones – varias respuestas.
- . . .

# Respuesta automática vs. manual

- Rapidez.

# Respuesta automática vs. manual

- Rapidez.
- Escalabilidad.

# Respuesta automática vs. manual

- Rapidez.
- Escalabilidad.
- Registro.

# Respuesta automática vs. manual

- Rapidez.
- Escalabilidad.
- Registro.
- Integración.

# Respuesta automática vs. manual

- Rapidez.
- Escalabilidad.
- Registro.
- Integración.
- Precio.

# Respuesta automática vs. manual

- Rapidez.
- Escalabilidad.
- Registro.
- Integración.
- Precio.
- ¿Fiabilidad?

# Tipos de respuesta

- Registro
- Bloqueo
- Ataque
- Recuperación
- Decepción

# Registro

- Activación de registros adicionales.
- Todavía es un mecanismo pasivo.
- Útil para monitorización.
- Ejemplo: activación del sistema de auditoría de Unix ante un acceso sospechoso a `/etc/passwd`

# Bloqueo

- Suprime interacciones entre atacante y atacado.
- El esquema más habitual.
- Mecanismos **activos**.
- Ejemplos: bloqueo en cortafuegos intermedio, suspensión de trabajos en un *host*. . .

# Ataque

- Acciones agresivas contra el pirata.
- Mecanismos **activos**.
- ¿Es ética esta respuesta?
- Ejemplo: lanzamiento de negación de servicio contra el pirata ante un intento de intrusión.

# Recuperación

- Detectan cambio en el estado de un recurso atacado y lo devuelven a su estado anterior.
- Mecanismos **activos**.
- Ejemplo: sistema que restaura el contenido de una página *web* si detecta una modificación.
- En muchas ocasiones, difíciles de implantar (p.e. actualización frecuente de páginas *web*).

# Decepción

- ‘Decepcionan’ al atacante.
- Mecanismos **activos**.
- Partidarios vs. detractores: ¿Sirve de algo la decepción?
- Ejemplos: *‘Sonria a la cámara oculta*’, PHF. . .

# Peligros de la AR

- Subversión del sistema.
- Respuestas inadecuadas.
- . . .

**Negación de servicio**

# Minimización del riesgo (I)

Diferentes aproximaciones. Tres de ellas (**básicas**):

- Limitación de respuestas por u.t.
- Actores protegidos.
- Probabilidad de falso positivo.

# Minimización del riesgo (II)

## Limitación de respuestas por u.t.

- IDEA: Determinar un número máximo de respuestas por unidad de tiempo, superado el cual el sistema no actúa.
- OBJETIVO: Evitar negaciones de servicio masivas.

¡∄ umbral universal!

# Minimización del riesgo (III)

## Actores ‘protegidos’

- IDEA: Establecer elementos contra los que **nunca** se actúa.
- OBJETIVO: No dañar recursos controlados o vitales para el correcto funcionamiento de una plataforma.

# Minimización del riesgo (IV)

## Probabilidad de falso positivo

- IDEA: No todos los eventos son igual de ‘sospechosos’.
- OBJETIVO: Ponderar cada actividad sospechosa en función de su probabilidad de ser un ataque real.
- PROBLEMA: ¿Quién determina la probabilidad de que una actividad ‘sospechosa’ sea realmente un ataque?

# Algoritmo de activación

ESTADO: {Detección ataque}
SI umbral de respuestas superado: FIN
SI NO
    Comprobación actor atacante
    SI es actor protegido: FIN
    SI NO
        Ponderación histórica de gravedad
        SI umbral de gravedad superado: **ACTUAR**
        SI NO
            **REGISTRAR**
        FSI
    FSI
FSI

# Algunos ejemplos (I)

SNORT

- `http://www.snort.org/`
- NIDS, *misuse detection* (sistema experto), tiempo real. . .
- Sistema abierto: muchas herramientas de terceros, incluida AR.

¡Libre (GNU)!

# Algunos ejemplos (II)

## TripWire

- Tripwire, Inc. (http://www.tripwire.com/).
- Verificador de integridad basado en máquina.
- No incorpora AR ‘de serie’, pero es fácil integrarla en el sistema.

# Algunos ejemplos (III)

PHF

- Sistema de decepción (*honeypot*) simple.
- Emula vulnerabilidad BID #629 en el CGI `phf` (1996), que permite ejecución remota.
- Proporciona información falsa (pero creíble) al atacante, mientras registra sus actividades.
- Fichero único en PERL: efectivo, fácil de instalar y gestionar.

# Conclusiones

- La detección de intrusos es necesaria, pero no suficiente.
- La respuesta automática es necesaria, pero peligrosa.
- Se puede (y debe) minimizar el riesgo a la hora de aplicar cualquier esquema de respuesta automática.

# Finalmente. . .

Ni la detección de intrusos,
ni la respuesta automática,
ni los cortafuegos,
ni. . .

Al hablar de seguridad, no existe la panacea

# Referencias


- Intrusion Detection: Network Security beyond the Firewall. Terry Escamilla. John Wiley & Sons, 1998.
- Network Intrusion Detection: An Analyst´s Handbook. Stephen Northcutt, Donald McLachlan, Judy Novak. New Riders Publishing, 2000 (2nd Edition).
- Intrusion Detection: Generics and State of the Art. NATO Research & Technology Organisation. Technical Report RTO–TR–049. NATO, 2002.

# ¡Muchas gracias!