Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Auditoría de Seguridad

Presentación

Daniel F. García

Introducción

Definición de Auditoría de Seguridad (*Security Audit*)

Revisión y examen independiente de los registros de las actividades de un sistema para:

- Determinar la **idoneidad** de los **controles** (de seguridad)
- Asegurar el **cumplimiento** de las **políticas** y procedimientos de seguridad establecidos
- Detectar **brechas** (*breaches*) en los servicios de seguridad
- Recomendar **cambios** que sean apropiados para las contramedidas (≈controles de seguridad)

Registro de Auditoría de Seguridad (RAS) (*Security Audit Trail*)

Un registro cronológico de las actividades del sistema que es suficiente para:
permitir la reconstrucción y el examen de la secuencia de entornos y actividades involucrados en una operación, procedimiento o evento de una transacción relevante para la seguridad desde el inicio hasta los resultados finales

RFC 4949 Internet Security Glossary, Version 2 August 2007

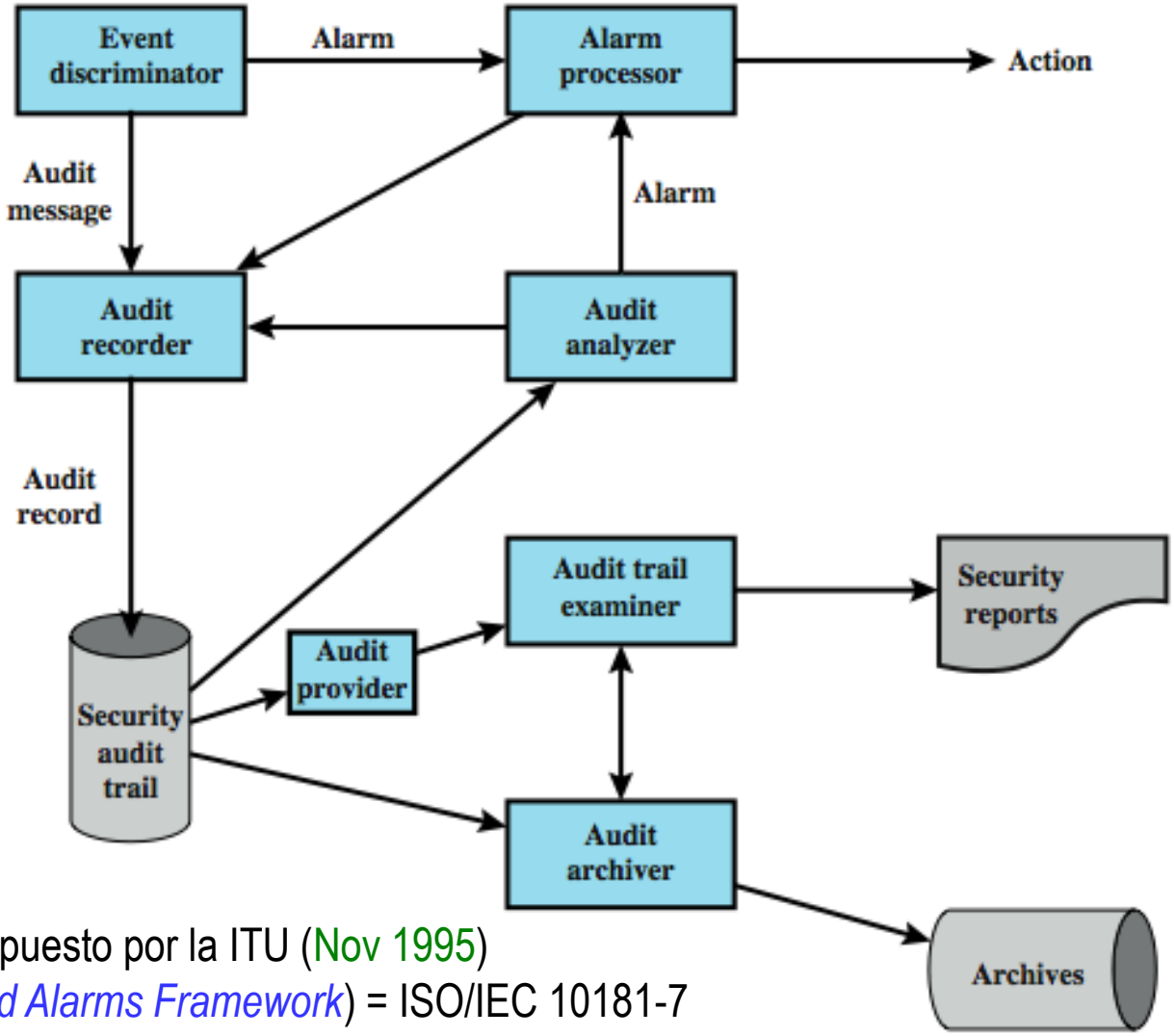
https://datatracker.ietf.org/doc/pdf/rfc4949.pdf

Objetivo de la Auditoría

Establecer la **responsabilidad** (*accountability*) de entidades que participan en acciones relevantes para la seguridad

Se necesitan mecanismos para: **(1)** generar y grabar RAS y **(2)** revisar y analizar RAS para descubrir y analizar violaciones de seguridad

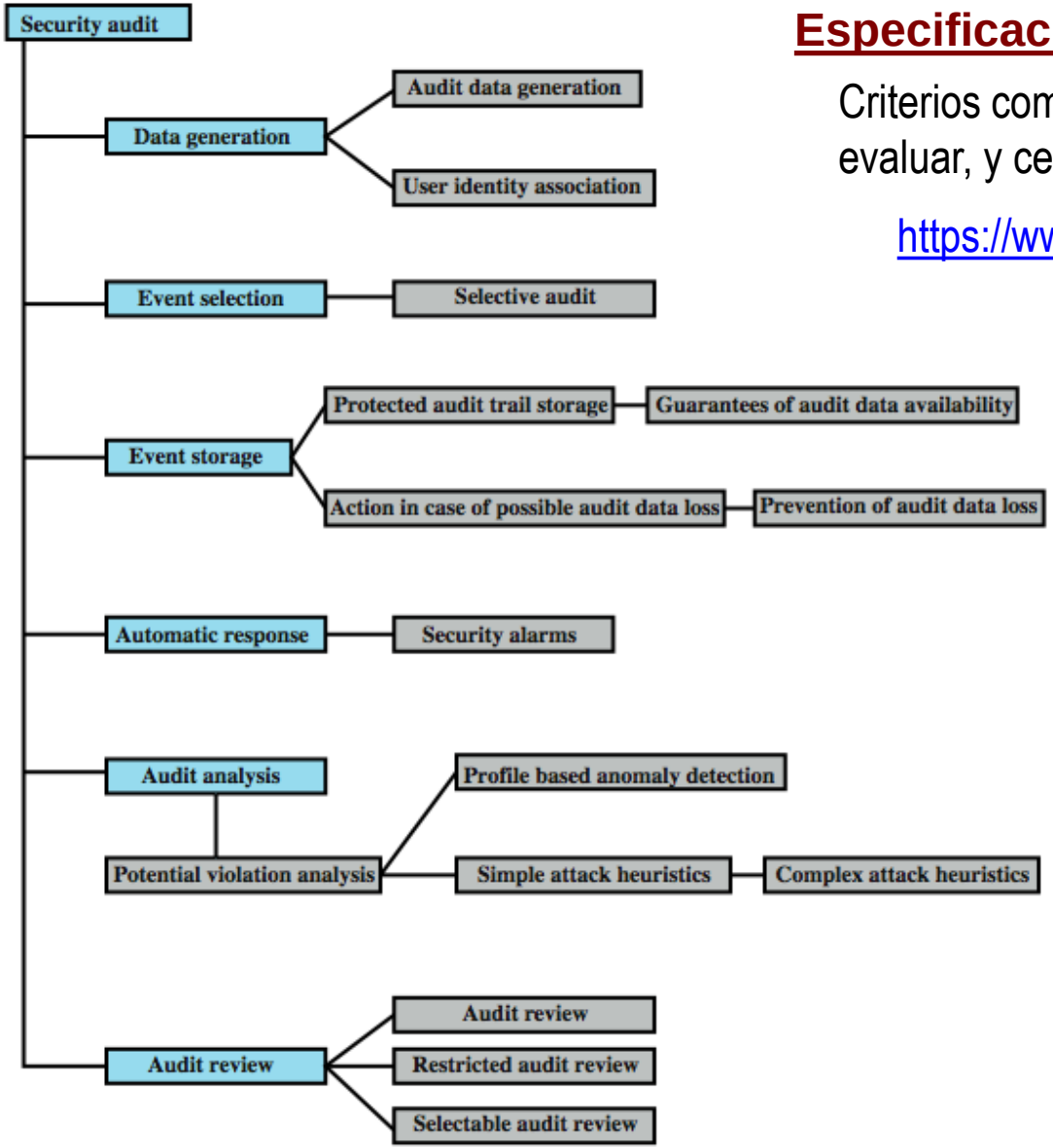
Modelo de auditoría de seguridad



Modelo **X.816** propuesto por la ITU (Nov 1995)
(*Security Audit and Alarms Framework*) = ISO/IEC 10181-7

https://www.itu.int/rec/T-REC-X.816/es https://www.iso.org/standard/18200.html

Funciones de la auditoría de seguridad



Especificación de Common Criteria (CC)

Criterios comunes para especificar, desarrollar, evaluar, y certificar productos de seguridad

https://www.commoncriteriaportal.org/

CC2022 Release 1 → Nov 2022

Documentos CC2022R1

Part 1: Introduction and general model
Part 2: Security functional requirements
Part 3: Security assurance requirements
Part 4: Framework for the specification of evaluation methods and activities
Part 5: Pre-defined packages of security requirements
CEM: Common evaluation methodology

Registros de Auditoría (1) Que capturar

1 Requisitos que determinan los datos a capturar

Cantidad de datos = F (rango de áreas de interés, granularidad de la captura)

Compromiso: Cantidad - Eficiencia

Cantidad alta → Degradación de prestaciones mayor
Sobrecarga de análisis
Tendencia a generar muchos informes y muy largos

2 Selección de datos a capturar

- Eventos relacionados con el uso del software de auditoría
- Eventos relacionados con los mecanismos de seguridad del sistema
- Eventos generados por mecanismos de seguridad (ej. Firewalls)
- Eventos relacionados con la gestión y el funcionamiento del sistema
- Accesos al sistema operativo (ej. vía system calls)
- Accesos a aplicaciones seleccionadas
- Accesos remotos

Registros de Auditoría (2) Que capturar – ISO 27002

Áreas de monitorización sugeridas en ISO 27002

a) Accesos autorizados, incluyendo detalles como:

1) Identificador del usuario
2) La fecha y el instante de los eventos clave
3) Los tipos de eventos
4) Los ficheros a los que se ha accedido
5) El programa o los servicios utilizados

b) Todas las operaciones realizadas usando privilegios, tales como:

1) Uso de cuentas con privilegios (administrador)
2) Arranques y paradas del sistema

c) Intentos de acceso no autorizados, tales como:

1) Acciones de usuario fallidas o rechazadas
2) Acciones fallidas o rechazadas que implican datos y otros recursos
3) Violaciones de la política de acceso y notificaciones para pasarelas de red y cortafuegos
4) Alertas provenientes de los sistemas de detección de intrusión

d) Alertas por fallos, tales como:

1) Alertas o mensajes de consola
2) Excepciones al registro del sistema
3) Alarmas de gestión de la red
4) Alarmas del sistema de control de acceso

e) Cambios e intentos de cambio en las configuraciones y los controles de seguridad del sistema

Registros de Auditoría (3) Ejemplos a varios niveles

Registros a nivel de sistema

```
Jan 27  17:14:04   host1  login: ROOT LOGIN console
Jan 27  17:15:04   host1  shutdown: reboot by root
Jan 27  17:18:38   host1  login: ROOT LOGIN console
Jan 27  17:19:37   host1  reboot: rebooted by root
Jan 28  09:46:53   host1  su: 'su root' succeeded for user1 on /dev/ttyp0
Jan 28  09:47:35   host1  shutdown: reboot by user1
Jan 28  09:53:24   host1  su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 12  08:53:22   host1  su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 17  08:57:50   host1  date: set by user1
Feb 17  13:22:52   host1  su: 'su root' succeeded for user1 on /dev/ttyp0
```

Generalmente usados para optimizar las prestaciones de un sistema …

Pueden usarse para auditar seguridad viendo accesos, operaciones, …

Registros a nivel de aplicación

```
Apr 9 11:20:22   host1    AA06370:  from=<user2@host2>, size=3355, class=0
Apr 9 11:20:23   host1    AA06370:  to=<user1@host1>, delay=00:00:02,stat=Sent
Apr 9 11:59:51   host1    AA06436:  from=<user4@host3>, size=1424, class=0
Apr 9 11:59:52   host1    AA06436:  to=<user1@host1>, delay=00:00:02, stat=Sent
Apr 9 12:43:52   host1    AA06441:  from=<user2@host2>, size=2077, class=0
Apr 9 12:43:53   host1    AA06441:  to=<user1@host1>, delay=00:00:01, stat=Sent
```

Para detectar violaciones de seguridad en aplicaciones

Ej. E-Mail, Bases de Datos

Registros a nivel de usuario

```
rcp        user1    ttyp0     0.02 secs Fri Apr 8 16:02
ls         user1    ttyp0     0.14 secs Fri Apr 8 16:01
clear      user1    ttyp0     0.05 secs Fri Apr 8 16:01
rpcinfo    user1    ttyp0     0.20 secs Fri Apr 8 16:01
nroff      user2    ttyp2     0.75 secs Fri Apr 8 16:00
sh         user2    ttyp2     0.02 secs Fri Apr 8 16:00
mv         user2    ttyp2     0.02 secs Fri Apr 8 16:00
sh         user2    ttyp2     0.03 secs Fri Apr 8 16:00
col        user2    ttyp2     0.09 secs Fri Apr 8 16:00
man        user2    ttyp2     0.14 secs Fri Apr 8 15:57
```

Usados para rastrear la actividad de un usuario

- Asignar responsabilidades a usuarios
- Detectar comportamientos anómalos
- Contabilizar la utilización de aplicaciones

Registros de Auditoría (4) Protección de los registros

Los registros de auditoría deben ser protegidos para garantizar:

Confidencialidad → Los registros contienen información sensible de los usuarios
Integridad → Un intruso no debe alterar los registros borrando evidencias de una intrusión

Alternativas típicas para almacenar los registros de auditoría

Según RFC 2196 Site Security Handbook Sept 1997 https://datatracker.ietf.org/doc/pdf/rfc2196.pdf

Fichero de lectura/escritura en un host
- Fácil de configurar, acceso rápido
- Vulnerable al ataque de un intruso

Dispositivo de una escritura / múltiples lecturas (Ej. CD ó DVD)
- Necesita un suministro continuo de discos
- El acceso no es inmediato y puede retrasarse notablemente
- Es más seguro que el anterior pero quizás menos conveniente

Dispositivo de solo escritura (Ej. Impresora)
- Proporciona registros impresos directamente
- No es práctico para almacenar muchos datos y/o muchos detalles
- Es útil cuando se necesita un registro permanente de forma inmediata

Implementación de la función de registro

Para obtener los registros en los que basar la auditoría de seguridad hay que implementar funciones que registren los datos necesarios

El software del computador debe contener sondas (*hooks*) que activen (*trigger*) la captura y el almacenamiento de datos cuando ocurren eventos preseleccionados

Las funciones de registro se suelen implementar a múltiples niveles

- **A nivel del sistema operativo**
  - Ej. El registro de eventos de Windows
  - Ej. El sistema syslog para UNIX
- **A nivel de software de soporte:**
  - Ej. Sistemas de Gestión de Bases de Datos
  - Ej. Servidores Web
- **A nivel de aplicación de usuario**

El registro de eventos de Windows (1)

El SO Windows incluye un sistema de captura y almacenamiento de eventos

Windows proporciona un Visor de Eventos (*event viewer*)

Hay 2 categorías de registros →
- Registros de Windows
- Registros de aplicaciones y servicios

Registros de Windows

Almacenan eventos del sistema y aplicaciones antiguas →
- Aplicación
- Seguridad
- Instalación
- Sistema
- Eventos reenviados

Registros de aplicaciones y servicios

Almacenan eventos de una única aplicación o componente

Vistas personalizadas

Una VP almacena un **filtro** (conjunto de reglas) para mostrar solo los eventos de interés para resolver un problema – La vista permite reutilizar el filtro cuando se desee

Suscripciones

Una suscripción permite recopilar copias de eventos de varios equipos remotos y almacenarlas localmente → Luego el visor los trata como si fuesen eventos locales

El registro de eventos de Windows (2)

Propiedades de un evento

Origen: Software que registró el evento (Programa, Componente del sistema, Controlador, …)

Identificador: Número que identifica al evento

Nivel: Clasificación de la gravedad del evento (depende del registro)

Registros de Aplicación y Sistema	Registro de Seguridad
•Información •Advertencia •Error •Crítico	•Auditoría de aciertos •Auditoría de errores

Usuario: Nombre del usuario en cuya sesión (nombre) se produjo el evento

Código operativo: Valor numérico que indica la actividad de la aplicación que generó el evento

Registro: El nombre del registro en el que se registró el evento

Categoría de tarea: Representa un subcomponente o una actividad del publicador de eventos

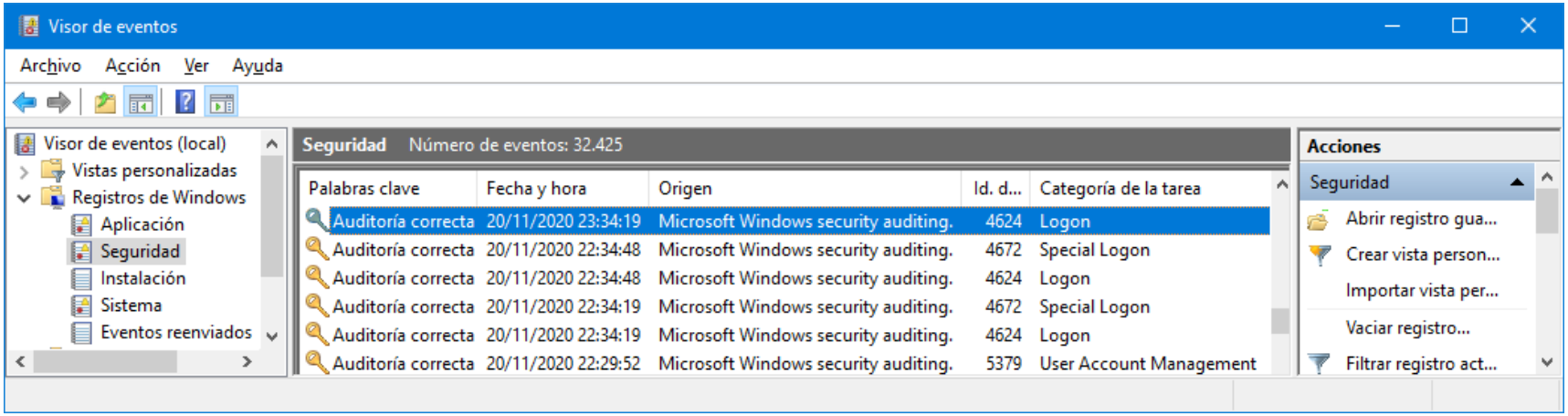
Palabras clave: Conjunto de categorías o etiquetas que se pueden usar para filtrar o buscar eventos

Equipo: Nombre del equipo en el que se produjo el evento

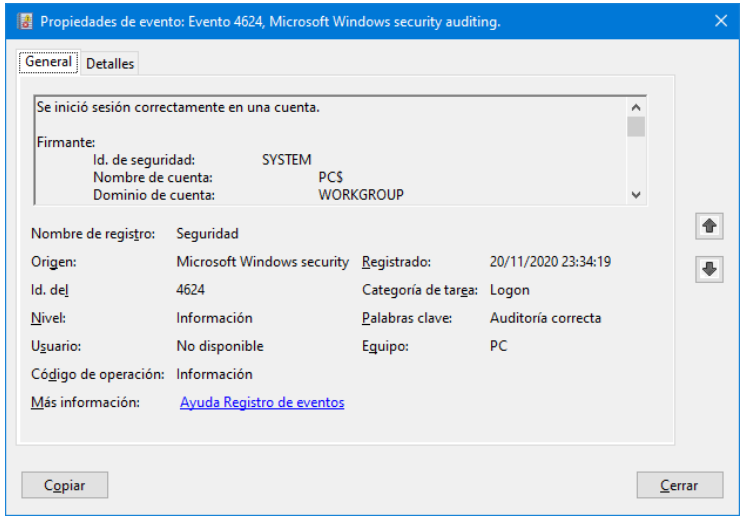
Fecha y hora: La fecha y la hora en la que se registró el evento

El registro de eventos de Windows (3)

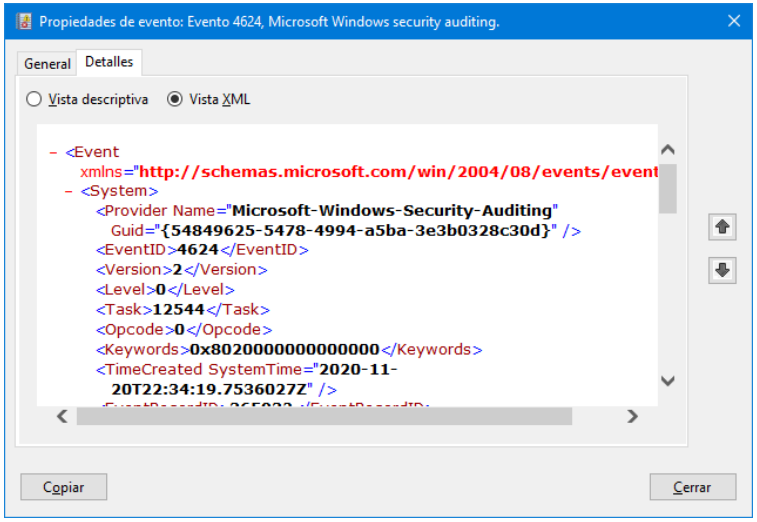
Inicio > Panel de control > Herramientas administrativas > Visor de eventos
Inicio > Cuadro de ejecución de programas: eventvwr.exe



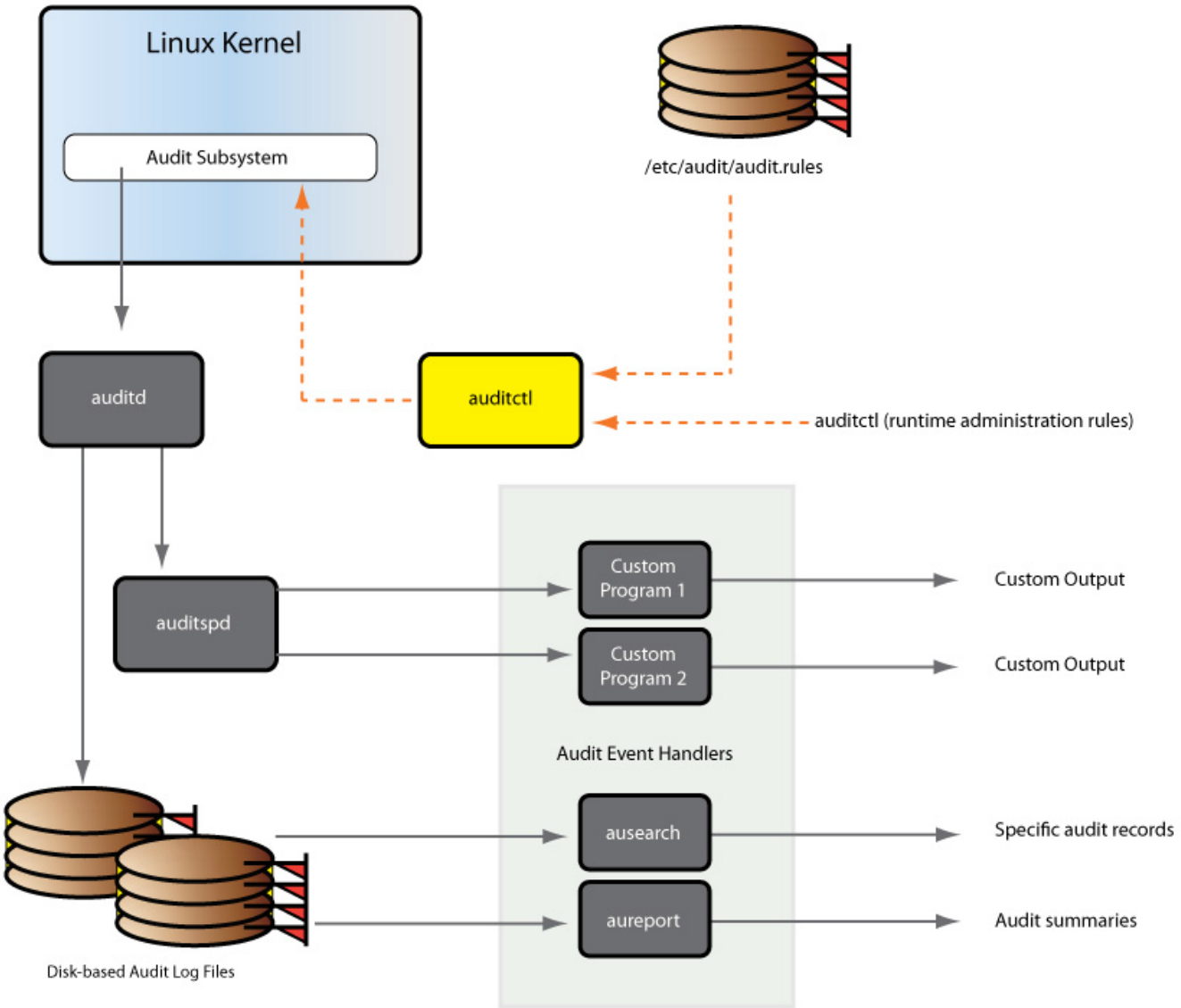
Ejemplo de un evento del registro



La información del evento en XML



El sistema de auditoría de Linux

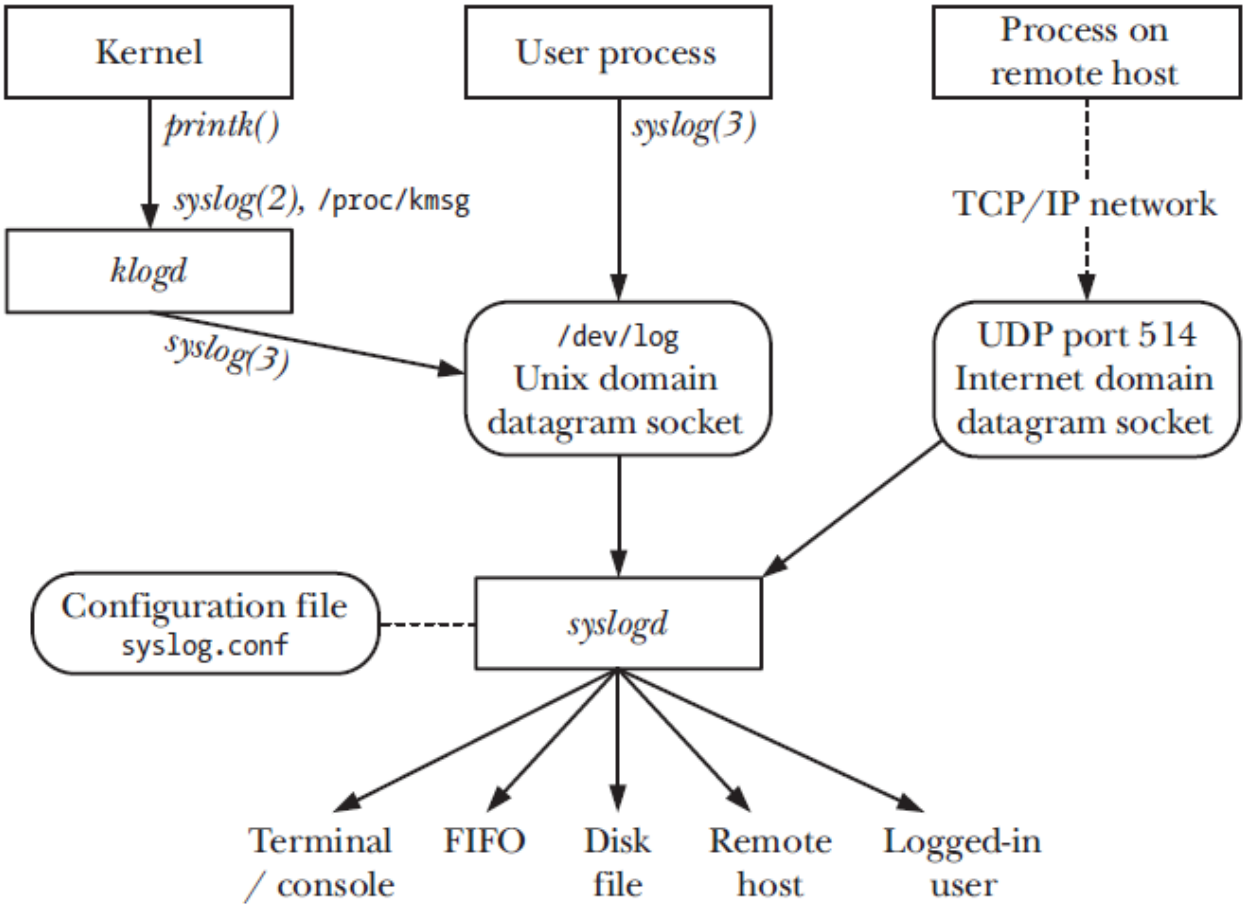


Herramienta syslog (1)

Syslog es un mecanismo de **registro de propósito general** que se encuentra en los sistemas UNIX

Se desarrolló en los años 80 para el programa sendmail en la Univ. de California en Berkeley

Se integró en las versiones de UNIX BSD (*Berkeley Software Distribution*) y luego en otros UNIX



Herramienta syslog (3)

Syslog empezó a utilizarse como colector para sistemas de registro distribuidos

A partir del año 2001 la **IETF** estandarizó el protocolo de comunicación usado en Syslog

2009 Marzo RFC 5424 The Syslog Protocol https://datatracker.ietf.org/doc/pdf/rfc5424.pdf

---

El protocolo Syslog es de tipo cliente/servidor Servidor == daemon

Los clientes envían mensajes de tamaño máximo 1024 bytes, generalmente vía UDP al puerto 514

Los mensajes se envían sin cifrar, pero hay implementaciones que admiten TCP y TLS/SSL

Problemas de seguridad:

- El envío mediante UDP no es fiable y se pueden perder mensajes
- Un equipo puede enviar mensajes representándose como otro diferente
- Un atacante puede enviar mensajes falsos que indican problemas en algunos equipos
- No se garantiza la entrega ordenada de paquetes → Facilita ataques de reenvío de paquetes

Cada paquete Syslog consta de 3 partes:

*Priority = 8 * Facility + Severity*

PRIORIDAD Combina el servicio (*facility*) - 5 bits + severidad (*severity*) - 3 bits

CABECERA Contiene el instante y el nombre del equipo que ha generado el mensaje

MENSAJE Consiste de dos campos: etiqueta (tag) y contenido (*content*)

Herramienta syslog (4)

Facility	Message Description (generated by)
kern	System kernel
user	User process
mail	e-mail system
daemon	System daemon, such as `ftpd`
auth	Authorization programs `login`, `su`, and `getty`
Syslogd	Messages generated internally by syslogd
lpr	Printing system
news	UseNet News system
uucp	UUCP subsystem
clock	Clock daemon
ftp	FTP deamon
ntp	NTP subsystem
log audit	Reserved for system use
log alert	Reserved for system use
Local use 0–7	Up to 8 locally defined categories

Campos de la PRIORIDAD

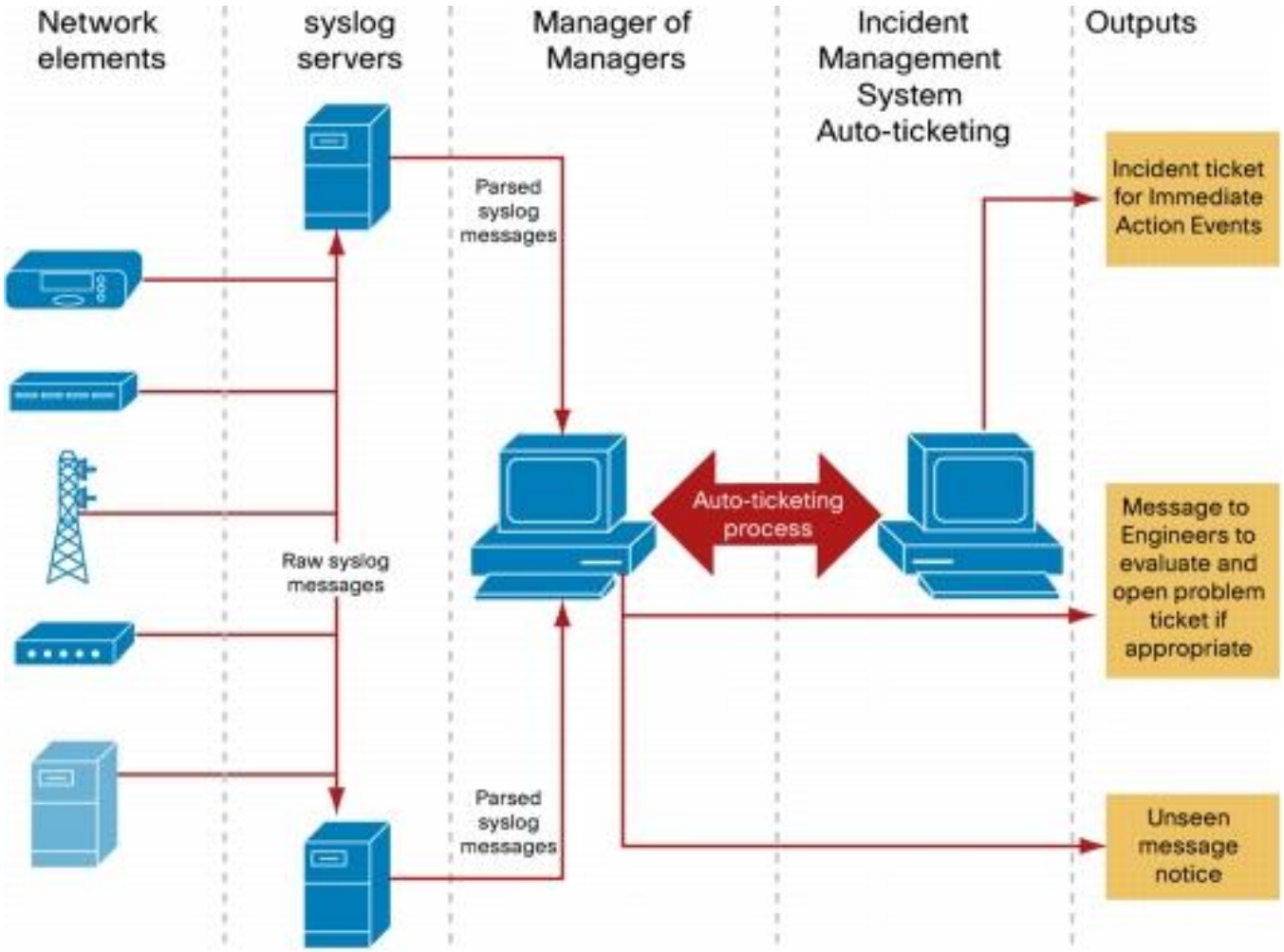
Severity	Description
emerg	Most severe messages, such as immediate system shutdown
alert	System conditions requiring immediate attention
crit	Critical system conditions, such as failing hardware or software
err	Other system errors; recoverable
warning	Warning messages; recoverable
notice	unusual situation that merits investigation; a significant event that is typically part of normal day-to-day operation
info	Informational messages
debug	Messages for debugging purposes

Ejemplos de mensajes

```
Mar 1 06:25:43 server1 sshd[23170]: Accepted publickey for server2 from
172.30.128.115 port 21011 ssh2

Mar 1 07:16:42 server1 sshd[9326]: Accepted password for murugiah from
10.20.30.108 port 1070 ssh2

Mar 1 07:16:53 server1 sshd[22938]: reverse mapping checking getaddrinfo for
ip10.165.nist.gov failed - POSSIBLE BREAKIN ATTEMPT!

Mar 1 07:26:28 server1 sshd[22572]: Accepted publickey for server2 from
172.30.128.115 port 30606 ssh2

Mar 1 07:28:33 server1 su: BAD SU kkent to root on /dev/ttyp2

Mar 1 07:28:41 server1 su: kkent to root on /dev/ttyp2
```

Herramienta syslog (5)

Ejemplos de utilización en entornos de red (CISCO Systems)



Análisis de registros de auditoría (1)

Los procedimientos para analizar los registros de auditoría son muy diversos

Dependen de muchos factores …

Pero hay aspectos generales a considerar en cualquier procedimiento de análisis

Preparación del analista

La clave para analizar registros es comprender la actividad típica asociada a cada sistema

Conocer bien los registros

La mayoría de los registros contienen una mezcla de texto plano y códigos

El analista debe conocer el significado de los códigos (Ej. Analizando registros regularmente)

Necesidad de contexto

Para valorar los registros el analista debe conocer el contexto en el que se generan y usan

- Las **políticas** de seguridad de la información
- Los **programas de seguridad** usados (eventos detectables, falsos positivos)
- Los **sistemas operativos** y **aplicaciones** usados por la organización
- Las técnicas de los **ataques comunes** y como se registran en cada sistema
- El **software** disponible para **analizar** los registros

Análisis de registros de auditoría (2)

¿Cuando se realiza el análisis?

Análisis del registro de auditoría después de un evento

Activado por el evento observado (ej. problema en una aplicación)

El analista usa información para diagnosticar la causa del problema y sugerir un remedio

El análisis **se centra en las entradas** del registro que son relevantes para el evento observado

Análisis periódico del registro de auditoría

Activado por el usuario (diariamente, semanalmente, mensualmente, …)

El análisis **usa todas las entradas** del registro o conjuntos de entradas predefinidos

Los objetivos del análisis pueden ser diversos:

- Buscar eventos o patrones de eventos que indican que hay un problema de seguridad
- Desarrollar un perfil de comportamiento normal y buscar comportamientos anómalos
- Desarrollar perfiles para usuarios individuales y mantener registros por usuario

Análisis de auditoría en tiempo real

El análisis se realiza continuamente, generalmente como parte de la detección de intrusiones

Análisis de registros de auditoría (3)

Estrategias para el análisis de los datos

Usar Alertas (*Alerting*)

Solicitar al software de análisis que de una indicación de que ha ocurrido un evento de interés

Usar Bases de Referencia (*Baselining*)

Baselining ←→ Proceso de definir los eventos y patrones normales versus los inusuales

Los nuevos valores se **comparan** con los valores base para detectar desviaciones inusuales

Estrategias de comparación →
- Detección de anomalías (*Never Before Seen*)
- Uso de umbrales (*Thresholding*)
- Uso de ventanas (*Windowing*)

Buscar correlaciones (*Correlation*)

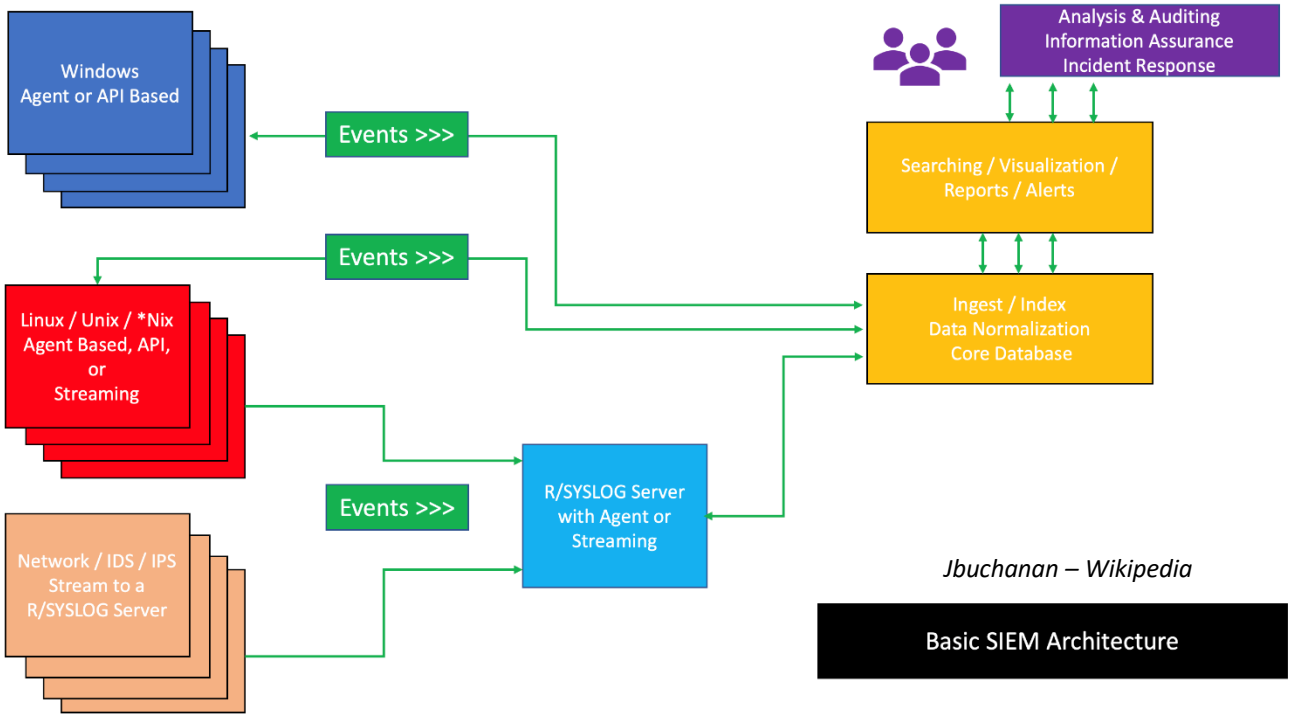
Consiste en buscar posibles relaciones entre eventos

Una vez detectado un mensaje particular → Alertar de la presencia de otros mensajes concretos

Herramientas de análisis: SIEM

El enorme volumen de datos para auditar la seguridad que se generan continuamente en una organización obliga a usar herramientas…

SIEM == **S**ecurity **I**nformation and **E**ven **M**anagement



Jbuchanan – Wikipedia

Basic SIEM Architecture

Capacidades

- Agregación de datos
- Correlación
- Alertas
- Dashboards
- Cumplimiento
- Retención de datos
- Análisis forense

https://www.ibm.com/es-es/qradar https://www.splunk.com/en_us/products/enterprise-security.html

https://cybersecurity.att.com/products/ossim https://www.solarwinds.com/solutions/it-security-solutions