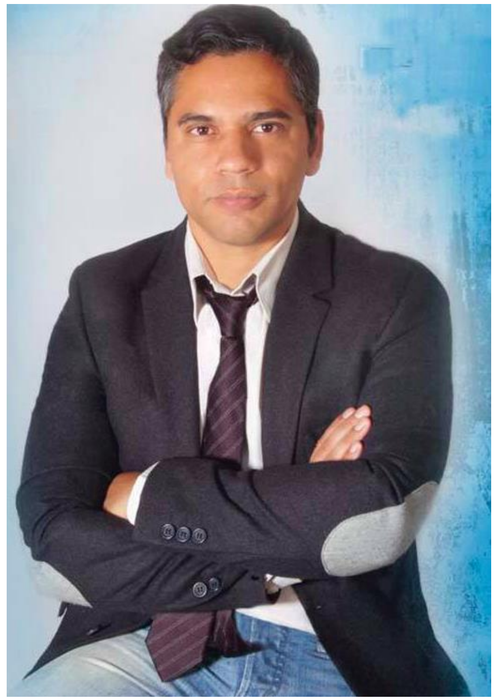
sedian

Seguridad Digital
de Andalucía

Respuesta ante Incidentes: despliegue y manejo de herramientas forense.

Junta de Andalucía

Adrián Ramírez (Dolbuck) >>



@adriandolbuck

adrian@dolbuck.net

Security Consultant
Data recovery
Computer forensics
Defense mitigation
Computer and networking Security
DPO
Social engineer
Graphic Design
Writer
Pentester
Organizer: SecAdmin

Introducción a DFIR

Qué es DFIR

DFIR es el acrónimo en inglés de Digital Forensics Incident Response. Dentro de la informática forense existe la rama conocida como respuesta a incidentes (Incident Response) y la disciplina conocida como análisis forense digital (Digital Forensics).

Los profesionales especializados en ambas disciplinas tienen como objetivo principal responder, de una forma rápida y efectiva, a un incidente de ciberseguridad de modo que tenga el menor impacto posible en las organizaciones.

¿Qué beneficios aporta un equipo de DFIR?

Contar con un equipo profesional en DFIR antes o durante la resolución de un incidente de seguridad aporta los siguientes beneficios:

- Ayuda a crear procedimientos y medidas de seguridad que preparen a la organización frente a un posible incidente de seguridad antes de que suceda, contribuyendo así a la resiliencia de esta.
- Garantiza un asesoramiento profesional, técnico y legal, durante un incidente de seguridad.
- Permite reducir el tiempo de respuesta frente a un incidente de ciberseguridad.
- Permite reducir el impacto de un ataque en la organización al contar con experiencia en este tipo de actuaciones.
- Garantiza un correcto análisis de las evidencias digitales y un correcto plan de mitigación de la amenaza.
- Ayuda a la elaboración de mecanismos de protección contra amenazas similares una vez superado el incidente de seguridad.

Respuesta a un incidente. Metodología de trabajo

El equipo de respuesta aplica una metodología de trabajo, cuyos puntos clave son los siguientes:

- **Detección:** Consiste en recopilar eventos, analizarlos y determinar si se está produciendo un incidente de ciberseguridad.
- **Análisis:** determinar el tipo de incidente, identificar los sistemas afectados, evaluar el impacto potencial, la criticidad y un plan para solucionarlo.
- **Contención:** Actuar rápido y con eficacia aplicando medidas para limitar el impacto del incidente en el negocio. Algunos ejemplos de acciones son cambiar un equipo a otra vlan, aplicar filtros en el firewall, etc.

- **Erradicación:** Se aplican medidas para eliminar la amenaza. Algunos ejemplos de acciones son eliminar ficheros maliciosos, aplicar actualizaciones de seguridad, etc.

- **Recuperación:** Contempla recobrar la actividad normal de la organización. Algunos ejemplos de acciones son restaurar sistemas, cambios de contraseñas, etc.

- **Lecciones aprendidas:** A través de todas las acciones anteriores se pretende responder a las siguientes preguntas: ¿Quién?, ¿Qué?, ¿Cuándo?, ¿Dónde?, ¿Por qué?, ¿Cómo? con el objetivo de prevenir que vuelva a suceder. Esto puede derivar en aplicar medidas de seguridad adicionales para seguridad los sistemas, dejar de utilizar una tecnología obsoleta, mejorar los procedimientos aplicados, etc.

Evento de ciberseguridad

En el contexto de la informática, un evento es una notificación o señal que indica que ha ocurrido algún tipo de acción o cambio en un sistema. Los eventos son fundamentales para el diseño de sistemas y aplicaciones interactivas, ya que permiten la interacción entre el usuario y el sistema, así como la respuesta automática del sistema a diferentes situaciones.

Los eventos pueden ser generados por diversas fuentes, como el usuario, el hardware, el software o incluso el propio sistema operativo. Algunos ejemplos comunes de eventos en informática incluyen:

Tipo de evento de ciberseguridad

Eventos de entrada: Estos eventos son generados por el usuario a través de dispositivos de entrada, como el teclado, el mouse o la pantalla táctil. Por ejemplo, cuando se presiona una tecla en el teclado, se genera un evento de teclado.

Eventos de temporizador: Estos eventos se generan después de transcurrir un período de tiempo específico. Se utilizan para realizar tareas programadas o para activar acciones periódicas en un sistema.

Tipo de evento de ciberseguridad

Eventos de red: Cuando se establece una conexión de red o se recibe un paquete de datos, se pueden generar eventos de red para notificar al sistema sobre la llegada de nuevos datos o cambios en la conexión.

Eventos del sistema operativo: El sistema operativo puede generar eventos para notificar sobre eventos importantes, como el inicio o cierre de aplicaciones, cambios en la configuración del sistema o errores.

Incidente:

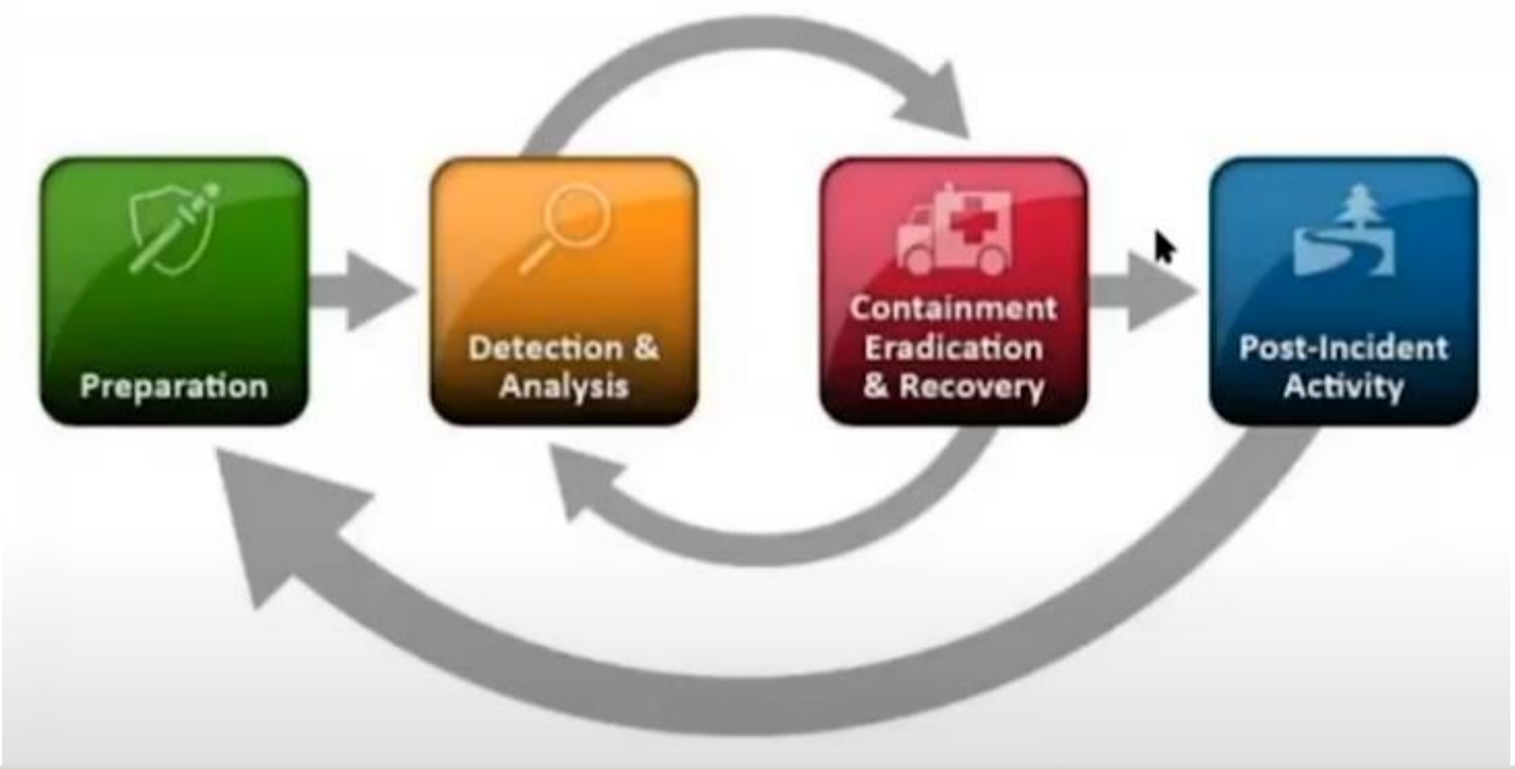
Aquel evento que de alguna manera es adverso a un sistema de información o una red, o alguna amenaza que aparece dentro de un evento.

¿Qué es un incidente de seguridad?

“Cualquier evento adverso, real o potencial, **vinculado a la seguridad de los sistemas de información** y sus redes. Así como el acto de **violar una política de seguridad** de forma implícita o explicita”.

Definición gráfica

Proceso de una respuesta a incidente simplificada



Incident response and handling steps

1. Preparation
2. Identification
3. Incident recording
4. Initial response
5. Communicating the incident
6. Containment
7. Formulating a response strategy
8. Incident clasification
9. Incident investigation
10. Data collection
11. Forensic analysis
12. Evidence protection
13. Notifying external agencies
14. Erradication
15. System recovery
16. Incident documentation
17. Incident damage and cost assessment
18. Review and update the response policies

Ciclo de Vida de la Gestión de incidentes de Ciber Seguridad

Recuperación

Esta fase tiene el objetivo de recuperar **completamente** las operaciones de la organización, a la vez que se analizan las vulnerabilidades y amenazas para **prevenir** que el incidente vuelva a presntarse.

- Coordinación para recuperación de operaciones
- Monitoreo a actividades de recuperación
- Lecciones aprendidas

Respuesta

Esta fase es crucial para **reducer** el **impacto** y contener la expansion del incidente, mediante un conjunto de acciones coordinadas para resolver el incidente en el menor tiempo possible. Las acciones de respuesta, el margen de tiempo y las **responsabilidaes**, serán diferentes segun el nivel de clasificación del incidente

- Coordinación para respuesta a incidentes
- Actividades de repuesta a incidentes
- Monitoreo de la respuesta a incidente

Preparación y prevención

Fase de preparación que tiene por objetivo estar listos antes de que ocurra un incidente. Permite a las organizaciones **Recuperar** los sistemas e inraestructuras mas rápidamente minimizando el impacto:

- Alertas preventivas, boletines informativos, noticias, etc
- Ejercicios y entrenamiento
- Concientización

Detección

Esta etapa esta enfocada detector oportuna de incidentes entendiendo la **tipología**, **magnitud** y **alcance**. Es crucial recopilar toda la información possible de las amenazas, así como **comunicar** e interactuar con otras unidades operativas para ofrecer una respuesta efectiva.

- Identificación y rastréo de eventos
- Flujos de gestión de incidentes
- Base de conomimiento del CERT

Análisis

Esta fase se enfoca en la identificaicón de los **activos** involucrados, **origen** del ataque, **motivación**, modo de **operación** y toda la **información** complementaria que sea de utilidad para el tratamiento. El resultado del análisis será la **clasificación** y **priorización**.

Las actividades involucradas son:

- Correlación de eventos
- Análisis de ciber amenazas
- Análisis de impacto y triaje

Matriz de clasificación de incidentes

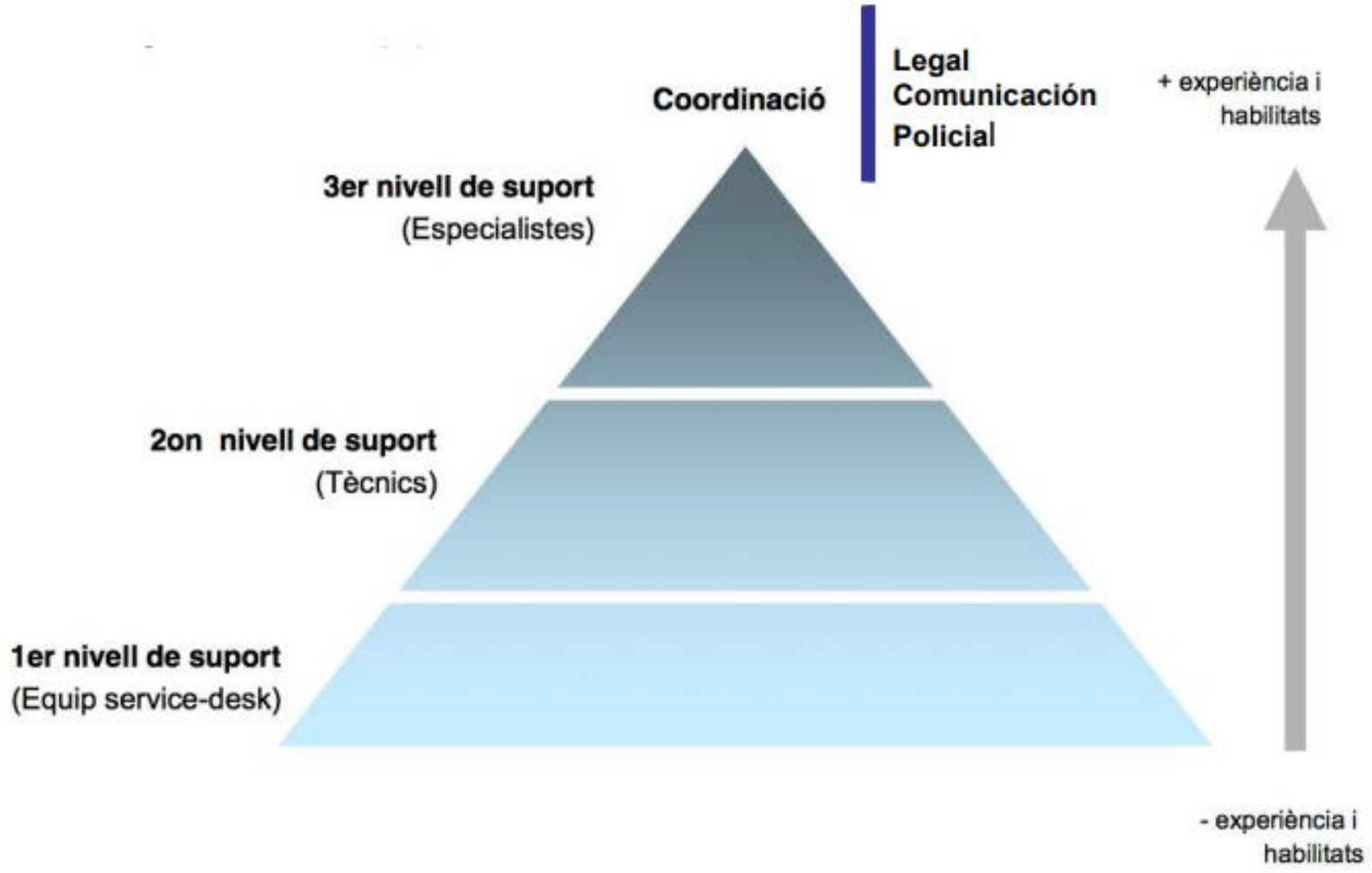
Matriz de clasificación de Incidentes			
N°	**Clase de Incidente**	**Tipo de Incidente**	**Descripción**
1	Contenido Abusivo	Pornografía Infantil – Sexual – Violencia	Pornografía infantil, glorificación de la violencia, otros.
		Spam	«Correo masivo no solicitado», lo que significa que el destinatario no ha otorgado permiso verificable para que el mensaje sea enviado y además el mensaje es enviado como parte de una grupo masivo de mensajes, todos teniendo un contenido similar
		Difamación	Desacreditación o discriminación de alguien
2	Código Malicioso	Malware, Virus, Gusanos, Troyanos, spyware, Dialler, rootkit	Software que se incluye o inserta intencionalmente en un sistema con propósito dañino. Normalmente, se necesita una interacción del usuario para activar el código.
3	Recopilación de Información	Scanning	Ataques que envían solicitudes a un sistema para descubrir puntos débiles. Se incluye también algún tipo de proceso de prueba para reunir información sobre hosts, servicios y cuentas. Ejemplos: fingerd, consultas DNS, ICMP, SMTP (EXPN, RCPT, …), escaneo de puertos.
		Sniffing	Observar y registrar el tráfico de la red (escuchas telefónicas o redes de datos).
		Ingeniería Social	Recopilación de información de un ser humano de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).

Creación y estructura de un ERI

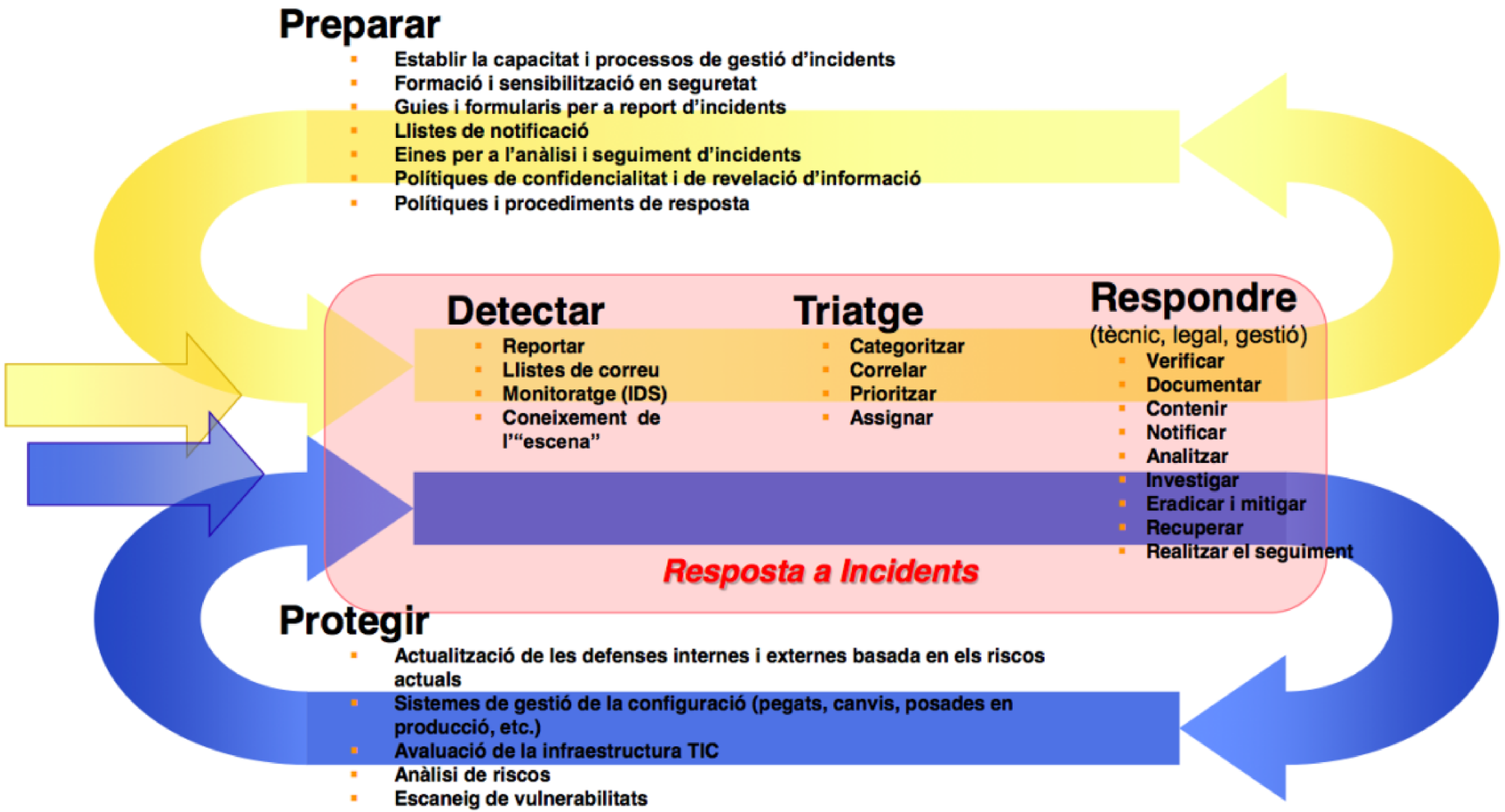
¿Qué es un Equipo de Respuesta a Incidentes?

Un Equipo de Respuesta a Incidentes (ERI) provee servicios y da soporte para prevenir, gestionar y responder ante los incidentes de seguridad de la información.

- Estructura Genérica del Equipo de Respuesta a Incidentes



Proceso del Equipo de Respuesta a Incidentes



Modelo documental del Equipo de Respuesta a Incidentes

Políticas y normas

Política para el intercambio de información con terceros.

Norma de uso de los dispositivos del laboratorio.

Procedimientos

Procedimiento para la adquisición de evidencias

Procedimiento para la clasificación de incidentes

Instrucciones operativas

Instrucciones para el clonado de discos duros

Instrucciones para el despliegue de contramedidas contra el incidente.

Servicios

Respuesta remota a incidentes

– Resolución de consultas.
– Avisos y alertas.
– Gestión de vulnerabilidades críticas.
– Coordinación con áreas internas de la organización y con terceros.
– Despliegue de sistemas de detección para ser más proactivos.
– Análisis y asesoramiento en la aplicación de contramedidas.

Servicios

- **Soporte in-situ**
  – Asesoramiento y coordinación en la gestión de un incidente.
  – Despliegue de contingencias
  – Adquisición de evidencias

Servicios

- **Análisis de laboratorio**
  – Análisis de artefactos
  – Investigación de vulnerabilidades y de la seguridad de nuevas tecnologías
  – Estudio de nuevas contramedidas..

En España existen actualmente 15 CERT’s

– 6 son del sector privado (e-LaCaixa, MAPFRE, s21sec, Telefonica, INCITA, CyberSOC CERT).

– 9 son del sector público (CCN, INTECO, CESICAT, esCERT, IRIS-CERT, **Andalucía-CERT**, CSIRT-CV, COSDEF, CESCA)

La red de CERT’s establece la voluntad, de las entidades adscritas, de compartir información y de ayudarse mutuamente para la resolución de incidentes.

Equipamiento de un DFIR

Herramientas de soporte

La gestión del ERI, se sustenta en dos herramientas:
– Gestión de tickets
– Gestión del conocimiento

Herramientas de soporte – Gestión de tickets

Herramienta de gestión de tickets
– Es el punto de entrada de información de cualquier incidente.
– Es la herramienta de comunicación con el afectado.
– Permite realizar un tracking de toda la gestión de la comunicación con los clientes y de las acciones que el Equipo realiza por cada incidente.
– Ayuda a entender que incidentes son mas prioritarios que el resto, cuáles deben ser atendidos, quién es la persona encargada de gestionar un incidente concreto, etc.
– La herramienta permite extraer automáticamente métricas e indicadores del servicio.

Herramientas de soporte – Gestión del conocimiento

Herramienta de gestión del conocimiento

– La herramienta es un sistema Wiki, que actúa como repositorio central de documentación del ERI.

– Encontramos todas las políticas, normas, procesos, instrucciones y documentación relativa a investigaciones.

– Al ser una Wiki, permite:

• Inter-relación de la información.

• Encontrar la información ágilmente (buscador, clasificación por categorías, tags, etc.).

• Colaboración en la creación y edición del contenido

• Comentarios y puntuación del contenido (I like it!)

• Restricción de acceso al contenido

Laboratorio

Infraestructura del laboratorio
– Red aislada
– Servidor ESXi per a la virtualización de sistemas.
– Caja fuerte y caja ignifuga.
– 2 Workstation de trabajo (con diferentes herramientas instaladas + bloqueador de escritura).
– 2 Maletines forense.
• Clonadora de discos
• Bloqueadores de escritura
• Disco duro para la adquisición de evidencias
• Lector de tarjetas
• Cámara de fotos
• Cables y adaptadores
• Etiquetadora
• Formularios de adquisición
– 1 Maletín TELCO (tarjeta wifi, antenas, funcube, pinapple, etc…)
– Bolsas de Faraday

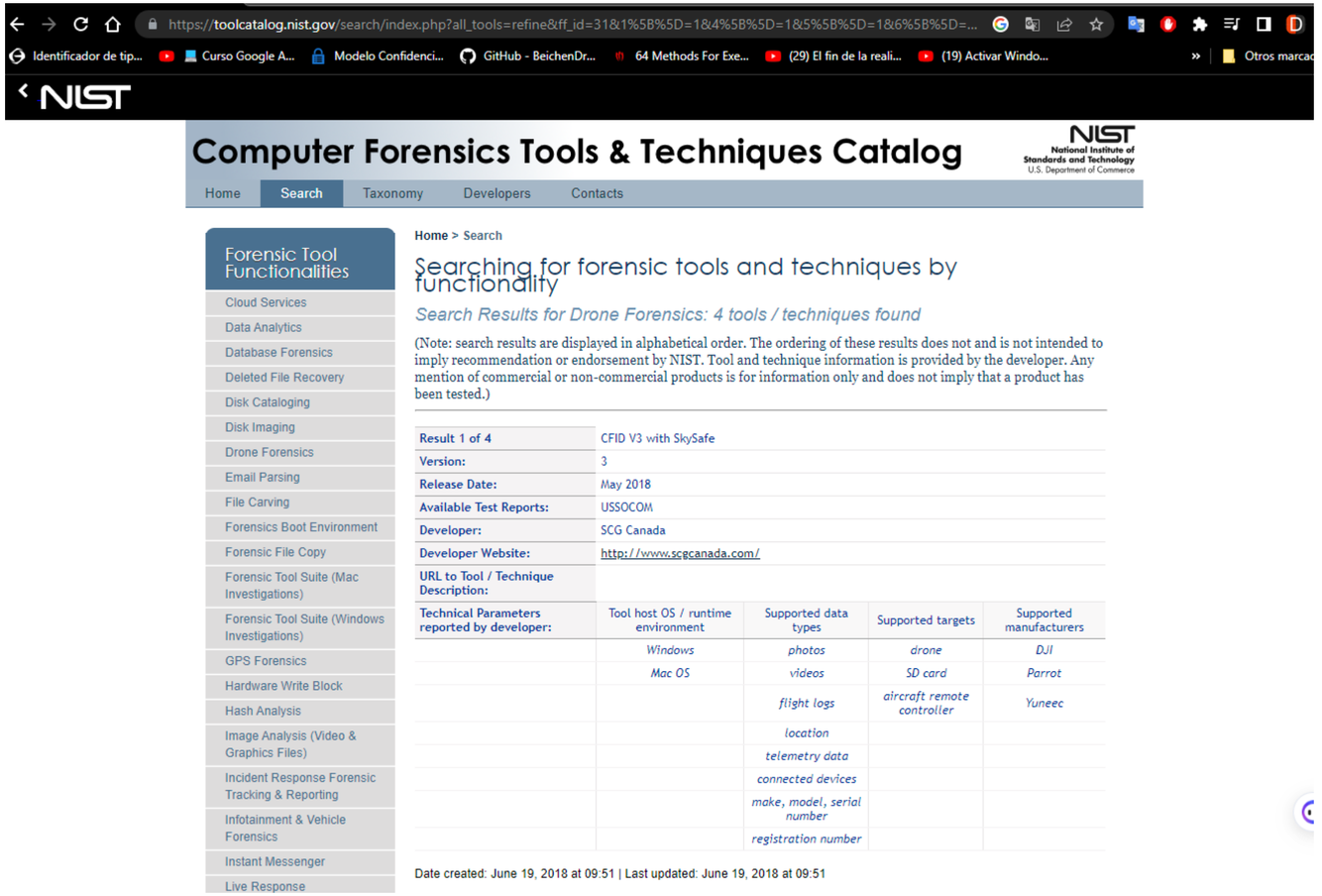
Laboratorio

Software del Laboratorio

Maquinas Virtuales de prueba (testbeds) :
• Windows XP (SP1, SP2, SP3), Windows 7-11, Windows 2003-2022, GNU/Linux, Caine, etc

Maquinas Virtuales con herramientas para:
• Búsqueda de información: Maltego
• Investigación de logs: Splunk, grep, sed, cut y awk... xD
• Análisis de intrusiones: Backtrack, Nessus, Accunteix, w3af
• Análisis de tráfico de red: Wireshark, NetworkMiner
• Análisis y captura de datos: Encase, Helix 3 pro, F-Response, VM Insectra, Paraben
• Análisis de comportamiento: Sysinternals, Norman Analyzer, FTK Analyzer
• Ingeniería inversa: HexRays IdaPro
• Ataques contra el cifrado: JTR, Hashcat, Rainbow tables, etc.

Recursos


https://toolcatalog.nist.gov/search/index.php?all_tools=refine&ff_id=31&1%5B%5D=1&4%5B%5D=1&5%5B%5D=1&6%5B%5D=...
Identificador de tip...
Curso Google A...
Modelo Confidenci...
GitHub - BeichenDr...
64 Methods For Exe...
(29) El fin de la reali...
(19) Activar Windo...
Otros marcad
NIST
Computer Forensics Tools & Techniques Catalog
NIST National Institute of Standards and Technology U.S. Department of Commerce
Home
Search
Taxonomy
Developers
Contacts
Forensic Tool Functionalities
Cloud Services
Data Analytics
Database Forensics
Deleted File Recovery
Disk Cataloging
Disk Imaging
Drone Forensics
Email Parsing
File Carving
Forensics Boot Environment
Forensic File Copy
Forensic Tool Suite (Mac Investigations)
Forensic Tool Suite (Windows Investigations)
GPS Forensics
Hardware Write Block
Hash Analysis
Image Analysis (Video & Graphics Files)
Incident Response Forensic Tracking & Reporting
Infotainment & Vehicle Forensics
Instant Messenger
Live Response
Home > Search
Searching for forensic tools and techniques by functionality
Search Results for Drone Forensics: 4 tools / techniques found
(Note: search results are displayed in alphabetical order. The ordering of these results does not and is not intended to imply recommendation or endorsement by NIST. Tool and technique information is provided by the developer. Any mention of commercial or non-commercial products is for information only and does not imply that a product has been tested.)
Result 1 of 4
CFID V3 with SkySafe
Version:
3
Release Date:
May 2018
Available Test Reports:
USSOCOM
Developer:
SCG Canada
Developer Website:
http://www.scgcanada.com/
URL to Tool / Technique Description:
Technical Parameters reported by developer:
Tool host OS / runtime environment
Supported data types
Supported targets
Supported manufacturers
Windows
Mac OS
photos
videos
flight logs
location
telemetry data
connected devices
make, model, serial number
registration number
drone
SD card
aircraft remote controller
DJI
Parrot
Yuneec
Date created: June 19, 2018 at 09:51 | Last updated: June 19, 2018 at 09:51

Adquisición de evidencias: La primer pregunta!!!

Máquina viva

- ✓ Adquisición de elementos volátiles de un sistema
- ✓ Memoria RAM
- ✓ Ejecución de comandos
- ✓ Artefactos de sistema
- ✓ Artefactos de usuario
- ✓ Artefactos de sistema de ficheros

Máquina apagada

- ✓ Imagen de disco duro

Principio de la volatilidad >>>

Clasificación de evidencias

- Registros CPU
- Memoria caché
- Memoria interna
  - Módulos S.O.
  - Controladores de dispositivos
  - Programas en ejecución
  - Conexiones activas
- Memoria externa
  - Discos
  - Soportes regrabables
  - Soportes no regrabables

Evidencia digital volátil

- Último arranque del sistema
- El histórico de comandos
- Procesos en ejecución
- Información del portapapeles («clipboard»)
- Usuarios conectados local o remótamente
- Conexiones abiertas y puertos
- Información de rutas
- Etc.

Evidencia digital persistente

- Metadatos (Prácticas con FOCA y Office)
- Ficheros modificados o accedidos
- Recuperar ficheros borrados (papelera reciclaje, sectores no reutilizados de ficheros borrados)
- Entradas en logs del sistema (histórico accesos)
- Ficheros temporales (Ej. cookies de navegación)
- Caché del navegador y URL recientes
- Registro de windows
- Correos enviados, recibidos o borrados
- Ficheros ocultos
- Ejecutables camuflados
- Usuarios y grupos de reciente creación

Herramientas forenses para entornos Windows

Acceso a objetos y tareas programadas

- Acceso a Objetos
  - 5140: Acceso a un recurso compartido
  - 5142: Se ha agregado un objeto de red compartido
  - 5143: Se ha modificado un objeto de red compartido
  - 5144: Se ha borrado un objeto de red compartido

- Tareas Programadas
  - 4698: Se ha creado una tarea programada
  - 4699: Se ha borrado una tarea programada
  - 4700: Se ha activado una tarea programada
  - 4701: Se ha deshabilitado una tarea programada
  - 4702: Se ha actualizado una tarea programada

- Auditoría de Cambios de Configuración del Sistema
  %SystemRoot%\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Operational
  - 106: Se ha creado una tarea programada
  - 140: Se ha actualizado una tarea programada
  - 141: Se ha borrado una tarea programada
  - 200: Tarea programada ejecutada
  - 201: Tarea programada completada

Eventos para monitorizar en Windows

4876	780	Bajo	La copia de seguridad de Servicios de servidor de certificados se ha iniciado.
4877	781	Bajo	Se ha completado la copia de seguridad de Servicios de servidor certificados.
4878	782	Bajo	Se inició la restauración de Servicios de servidor de certificados.
4879	783	Bajo	Se ha completado la restauración de Servicios de servidor de certificados.
4880	784	Bajo	Servicios de servidor de certificados iniciados.
4881	785	Bajo	Se detuvo Servicios de servidor de certificados.
4883	787	Bajo	Servicios de servidor de certificados recuperó una clave archivada.
4884	788	Bajo	Servicios de servidor de certificados importó un certificado en su base de datos.
4886	790	Bajo	Servicios de servidor de certificados recibió una solicitud de certificado.
4887	791	Bajo	Servicios de servidor de certificados aprobó una solicitud de certificado y emitió un certificado.
4888	792	Bajo	Servicios de servidor de certificados denegó una solicitud de certificado.

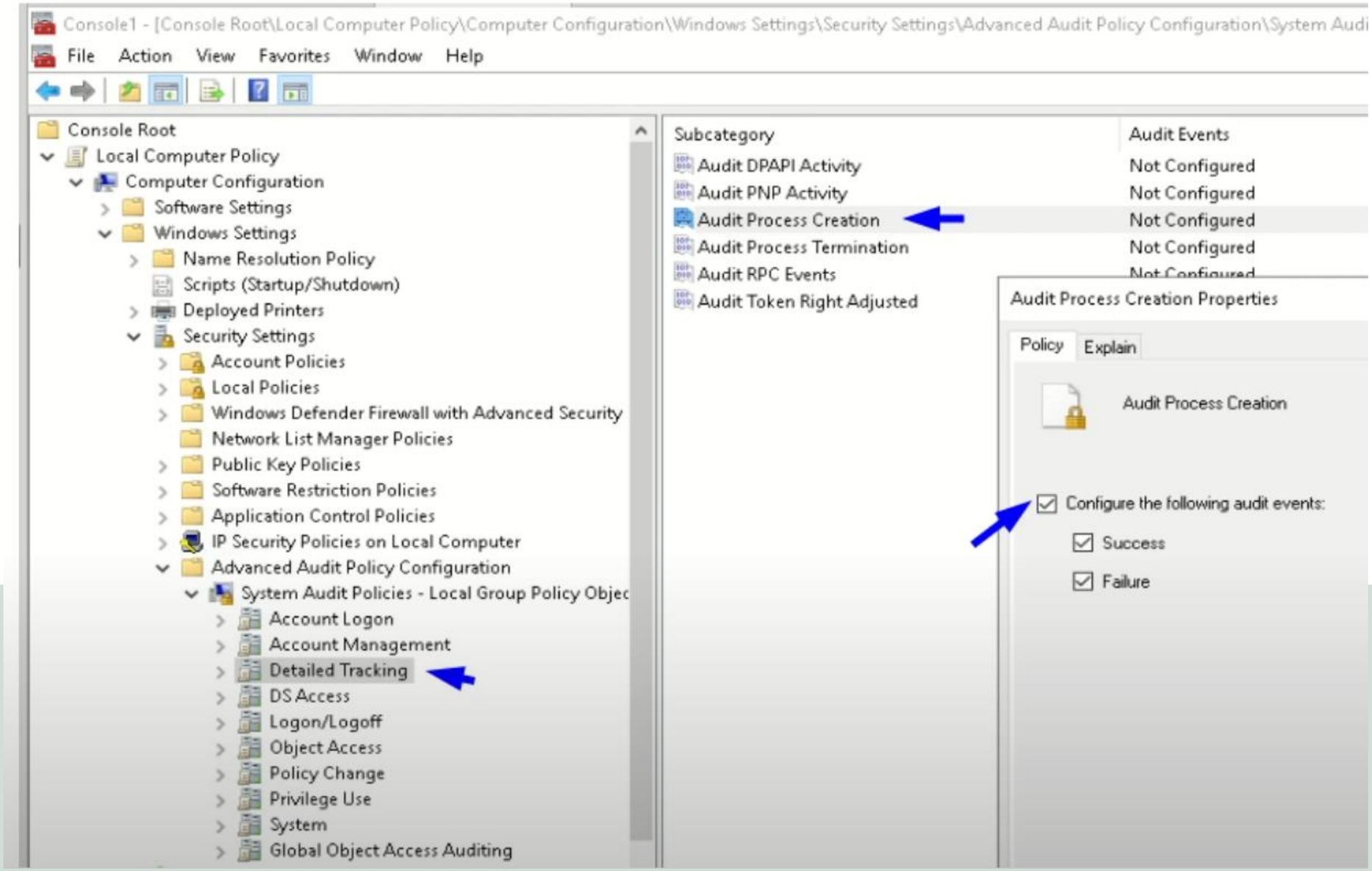
Fuente: https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

Windows Defender

- **%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4WHC.evtx**
- AMSI (Antimalware Scan Interface
  - 1006: El motor de antivirus ha encontrado malware
  - 1007: El antimalware ha realizado una acción para proteger el sistema
  - 1008: El antimalware ha intentado ejecutar una acción para proteger el sistema
  - 1015: El antimalware ha detectado un comportamiento sospechoso
  - 5001: Se ha detenido la protección en tiempo real
  - 5004: Se ha modificado la configuración de protección en tiempo real
  - 5007: Se ha modificado la configuración del antimalware
  - 5010: Se ha desactivado el escaneo de malware

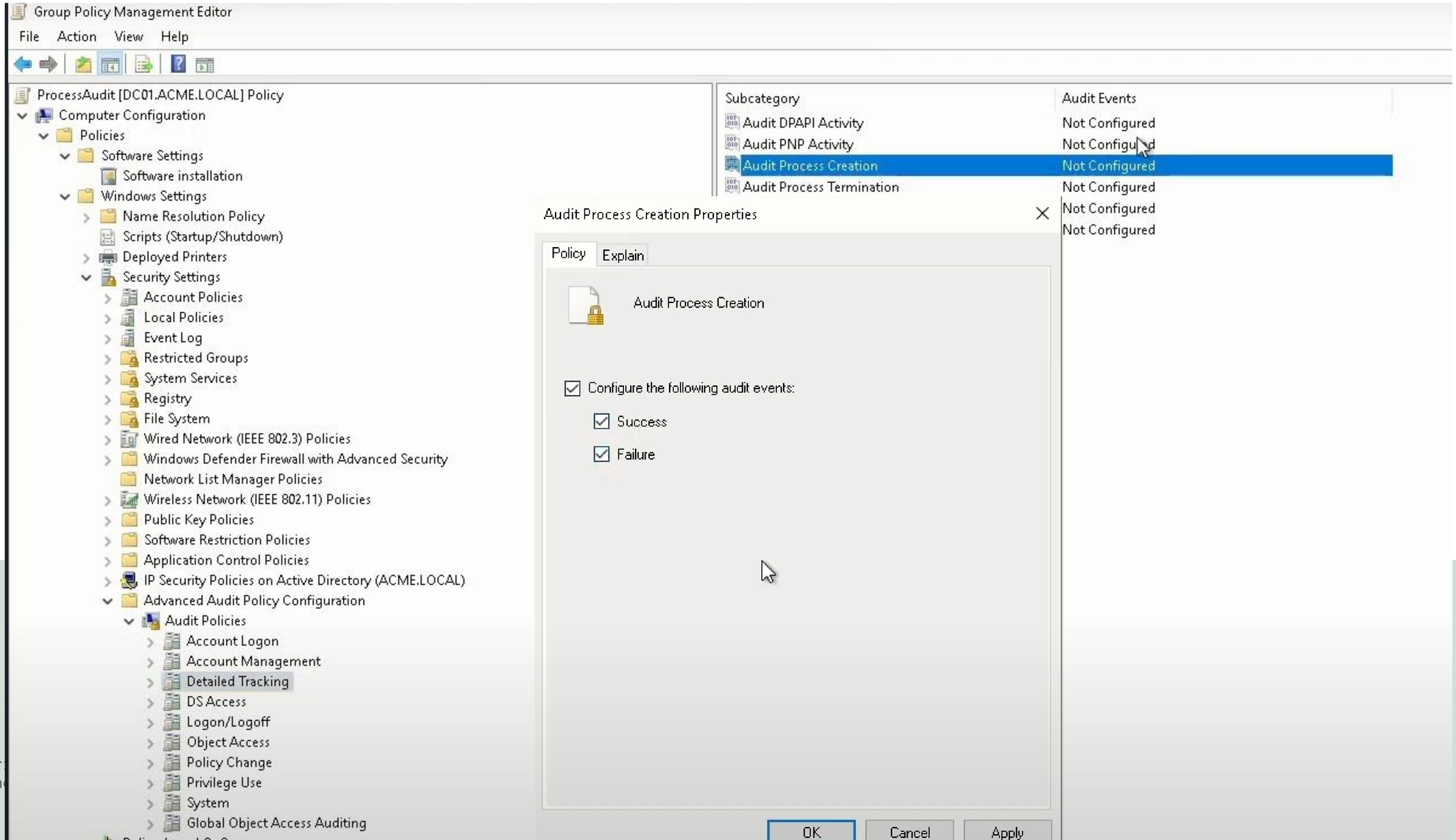
- Windows Exploit Protection
- **%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-Security-Mitigations%4KernelMode.evtx**
- **%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-Security-Mitigations%4UserMode.evtx**

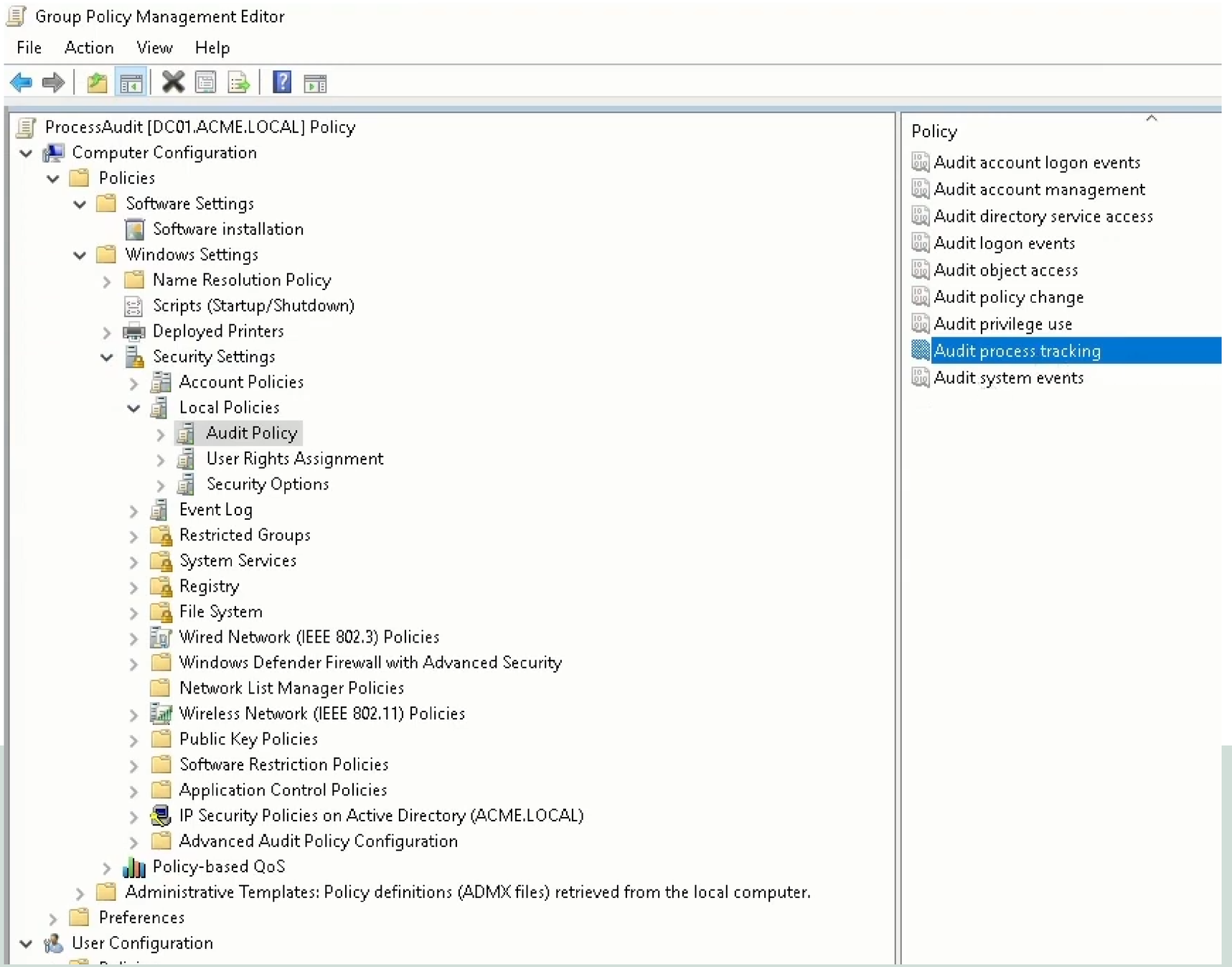
Auditorías de Procesos/ Sysmon



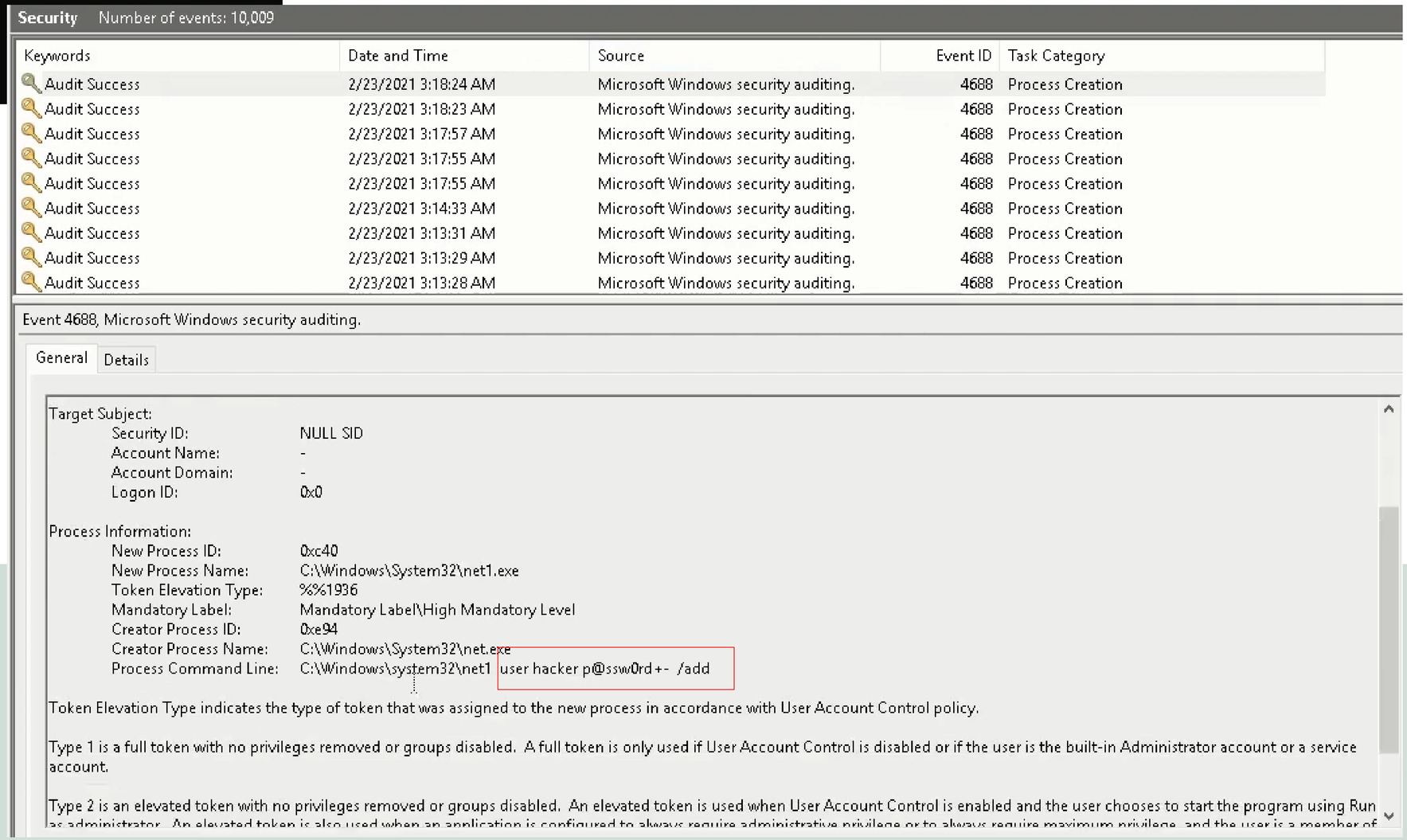
sepian Seguridad Digital de Andalucía

Auditorías de Procesos/ Sysmon (Hay que activarlo también!!)




Group Policy Management Editor
File Action View Help
ProcessAudit [DC01.ACME.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Software installation
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (ACME.LOCAL)
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer.
Preferences
User Configuration
Policy
Audit account logon events
Audit account management
Audit directory service access
Audit logon events
Audit object access
Audit policy change
Audit privilege use
Audit process tracking
Audit system events


Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>net user hacker p@ssw0rd+- /add
The command completed successfully.
C:\Users\Administrator>


Security Number of events: 10,009
Keywords Date and Time Source Event ID Task Category
Audit Success 2/23/2021 3:18:24 AM Microsoft Windows security auditing. 4688 Process Creation
Audit Success 2/23/2021 3:18:23 AM Microsoft Windows security auditing. 4688 Process Creation
Audit Success 2/23/2021 3:17:57 AM Microsoft Windows security auditing. 4688 Process Creation
Audit Success 2/23/2021 3:17:55 AM Microsoft Windows security auditing. 4688 Process Creation
Audit Success 2/23/2021 3:17:55 AM Microsoft Windows security auditing. 4688 Process Creation
Audit Success 2/23/2021 3:14:33 AM Microsoft Windows security auditing. 4688 Process Creation
Audit Success 2/23/2021 3:13:31 AM Microsoft Windows security auditing. 4688 Process Creation
Audit Success 2/23/2021 3:13:29 AM Microsoft Windows security auditing. 4688 Process Creation
Audit Success 2/23/2021 3:13:28 AM Microsoft Windows security auditing. 4688 Process Creation
Event 4688, Microsoft Windows security auditing.
General Details
Target Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Process Information:
New Process ID: 0xc40
New Process Name: C:\Windows\System32\net1.exe
Token Elevation Type: %%1936
Mandatory Label: Mandatory Label\High Mandatory Level
Creator Process ID: 0xe94
Creator Process Name: C:\Windows\System32\net.exe
Process Command Line: C:\Windows\system32\net1 user hacker p@ssw0rd+- /add
Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.
Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account.
Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run

Sysmon v14.16

Artículo • 12/04/2023 • 9 colaboradores

Por Mark Russinovich y Thomas Garnier

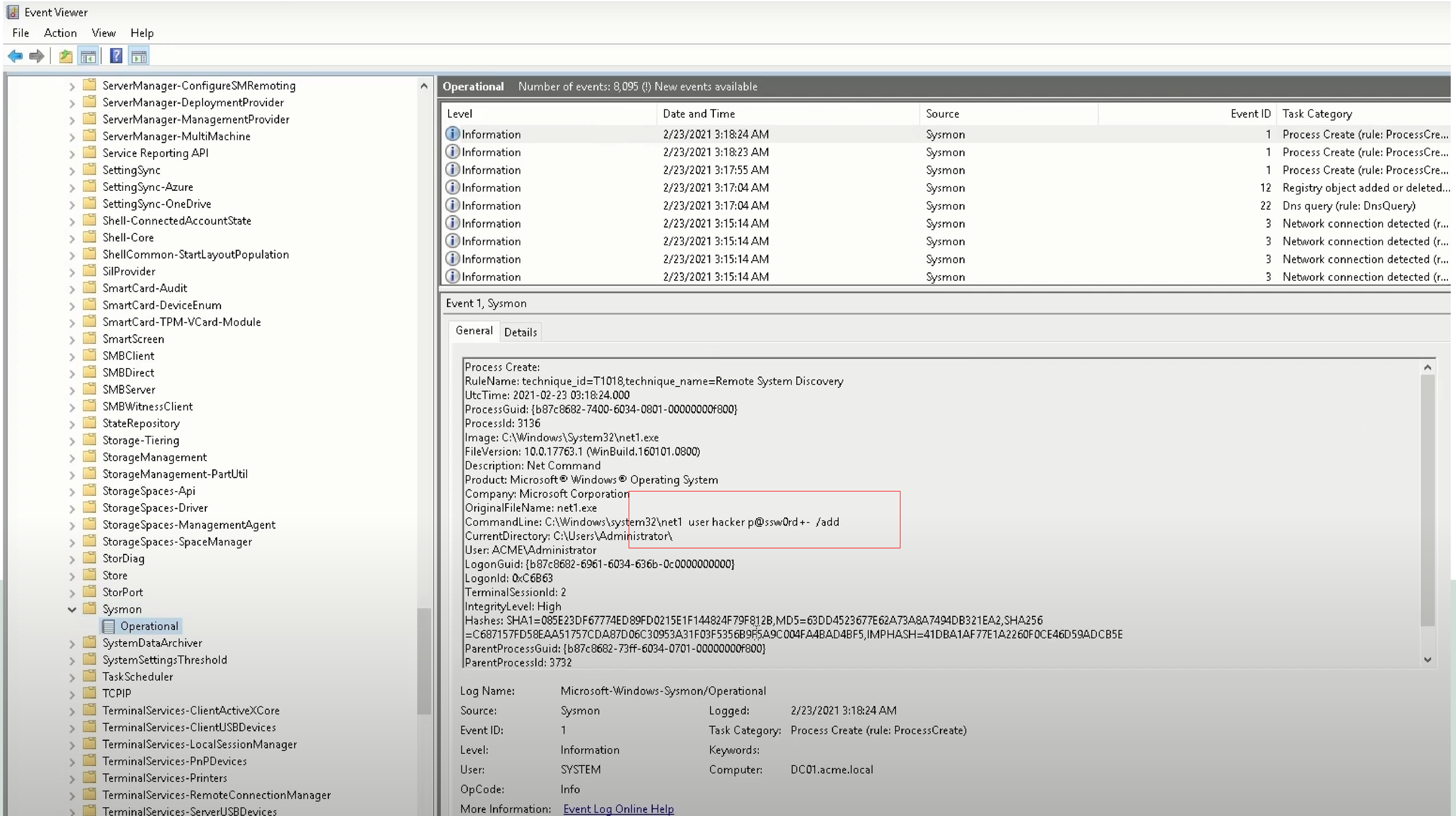
Publicado: 12 de abril de 2023

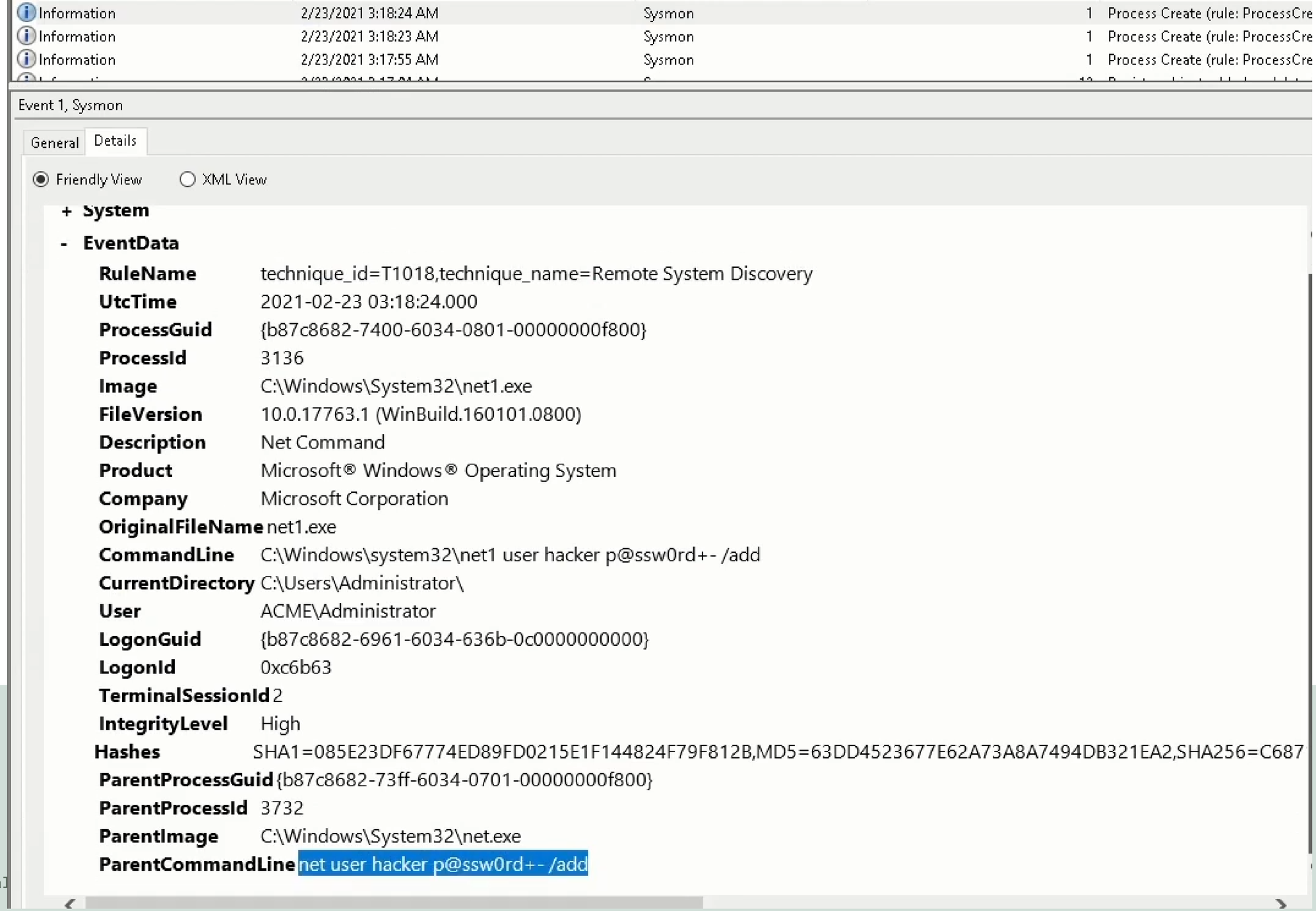
 Descargar Sysmon **(4.6 MB)**

Descarga de Sysmon para Linux (GitHub)

Sysmon incluye las siguientes funcionalidades:

- Registra la creación de procesos con línea de comandos completa para los procesos actuales y primarios.
- Registra el hash de los archivos de imagen de proceso mediante SHA1 (valor predeterminado), MD5, SHA256 o IMPHASH.
- Se pueden usar varios hash al mismo tiempo.
- Incluye un GUID de proceso en los eventos de creación de procesos para permitir la correlación de eventos incluso cuando Windows reutiliza los identificadores de proceso.
- Incluye un GUID de sesión en cada evento para permitir la correlación de eventos en la misma sesión de inicio de sesión.
- Registra la carga de controladores o archivos DLL con sus firmas y hashes.
- Los registros se abren para el acceso de lectura sin formato de los discos y volúmenes.
- Opcionalmente, registra las conexiones de red, incluido el proceso de origen de cada conexión, las direcciones IP, los números de puerto, los nombres de host y los nombres de puerto.
- Detecta los cambios en el tiempo de creación de archivos para comprender cuándo se creó realmente un archivo. La modificación de las marcas de tiempo de creación de archivos es una técnica que suele usar el malware para cubrir sus pistas.
- Vuelva a cargar automáticamente la configuración si se cambia en el Registro.
- Filtrado de reglas para incluir o excluir determinados eventos dinámicamente.
- Genera eventos desde el principio del proceso de arranque para capturar la actividad realizada por malware en modo kernel incluso sofisticado.


Event Viewer
File Action View Help
ServerManager-ConfigureSMRemoting
ServerManager-DeploymentProvider
ServerManager-ManagementProvider
ServerManager-MultiMachine
Service Reporting API
SettingSync
SettingSync-Azure
SettingSync-OneDrive
Shell-ConnectedAccountState
Shell-Core
ShellCommon-StartLayoutPopulation
SilProvider
SmartCard-Audit
SmartCard-DeviceEnum
SmartCard-TPM-VCard-Module
SmartScreen
SMBClient
SMBDirect
SMBServer
SMBWitnessClient
StateRepository
Storage-Tiering
StorageManagement
StorageManagement-PartUtil
StorageSpaces-Api
StorageSpaces-Driver
StorageSpaces-ManagementAgent
StorageSpaces-SpaceManager
StorDiag
Store
StorPort
Sysmon
Operational
SystemDataArchiver
SystemSettingsThreshold
TaskScheduler
TCPIP
TerminalServices-ClientActiveXCore
TerminalServices-ClientUSBDevices
TerminalServices-LocalSessionManager
TerminalServices-PnPDevices
TerminalServices-Printers
TerminalServices-RemoteConnectionManager
TerminalServices-ServerUSBDevices
Operational Number of events: 8,095 (!) New events available
Level Date and Time Source Event ID Task Category
Information 2/23/2021 3:18:24 AM Sysmon 1 Process Create (rule: ProcessCre...
Information 2/23/2021 3:18:23 AM Sysmon 1 Process Create (rule: ProcessCre...
Information 2/23/2021 3:17:55 AM Sysmon 1 Process Create (rule: ProcessCre...
Information 2/23/2021 3:17:04 AM Sysmon 12 Registry object added or deleted...
Information 2/23/2021 3:17:04 AM Sysmon 22 Dns query (rule: DnsQuery)
Information 2/23/2021 3:15:14 AM Sysmon 3 Network connection detected (r...
Information 2/23/2021 3:15:14 AM Sysmon 3 Network connection detected (r...
Information 2/23/2021 3:15:14 AM Sysmon 3 Network connection detected (r...
Information 2/23/2021 3:15:14 AM Sysmon 3 Network connection detected (r...
Event 1, Sysmon
General Details
Process Create:
RuleName: technique_id=T1018,technique_name=Remote System Discovery
UtcTime: 2021-02-23 03:18:24.000
ProcessGuid: {b87c8682-7400-6034-0801-00000000f800}
ProcessId: 3136
Image: C:\Windows\System32\net1.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Net Command
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: net1.exe
CommandLine: C:\Windows\system32\net1 user hacker p@ssw0rd+- /add
CurrentDirectory: C:\Users\Administrator\
User: ACME\Administrator
LogonGuid: {b87c8682-6961-6034-636b-0c0000000000}
LogonId: 0xC6B63
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=085E23DF67774ED89FD0215E1F144824F79F812B,MD5=63DD4523677E62A73A8A7494DB321EA2,SHA256
=C687157FD58EAA51757CDA87D06C30953A31F03F5356B9F5A9C004FA4BAD4BF5,IMPHASH=41DBA1AF77E1A2260F0CE46D59ADCB5E
ParentProcessGuid: {b87c8682-73ff-6034-0701-00000000f800}
ParentProcessId: 3732
Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 2/23/2021 3:18:24 AM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: DC01.acme.local
OpCode: Info
More Information: Event Log Online Help


Information 2/23/2021 3:18:24 AM Sysmon 1 Process Create (rule: ProcessCre
Information 2/23/2021 3:18:23 AM Sysmon 1 Process Create (rule: ProcessCre
Information 2/23/2021 3:17:55 AM Sysmon 1 Process Create (rule: ProcessCre
Event 1, Sysmon
General
Details
Friendly View
XML View
+ System
- EventData
RuleName technique_id=T1018,technique_name=Remote System Discovery
UtcTime 2021-02-23 03:18:24.000
ProcessGuid {b87c8682-7400-6034-0801-00000000f800}
ProcessId 3136
Image C:\Windows\System32\net1.exe
FileVersion 10.0.17763.1 (WinBuild.160101.0800)
Description Net Command
Product Microsoft® Windows® Operating System
Company Microsoft Corporation
OriginalFileName net1.exe
CommandLine C:\Windows\system32\net1 user hacker p@ssw0rd+- /add
CurrentDirectory C:\Users\Administrator\
User ACME\Administrator
LogonGuid {b87c8682-6961-6034-636b-0c0000000000}
LogonId 0xc6b63
TerminalSessionId 2
IntegrityLevel High
Hashes SHA1=085E23DF67774ED89FD0215E1F144824F79F812B,MD5=63DD4523677E62A73A8A7494DB321EA2,SHA256=C687
ParentProcessGuid {b87c8682-73ff-6034-0701-00000000f800}
ParentProcessId 3732
ParentImage C:\Windows\System32\net.exe
ParentCommandLine net user hacker p@ssw0rd+- /add

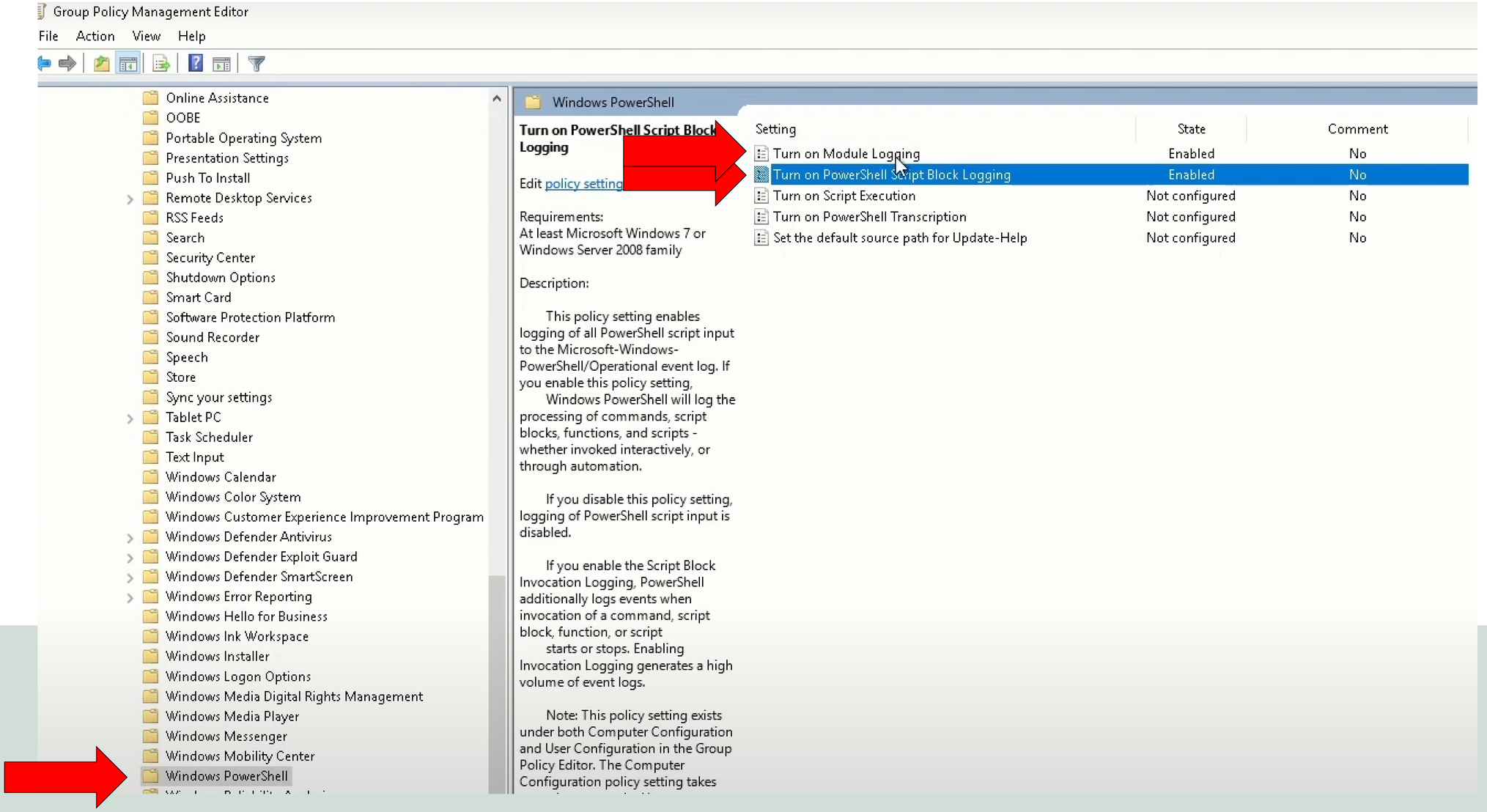
LOGS RDP

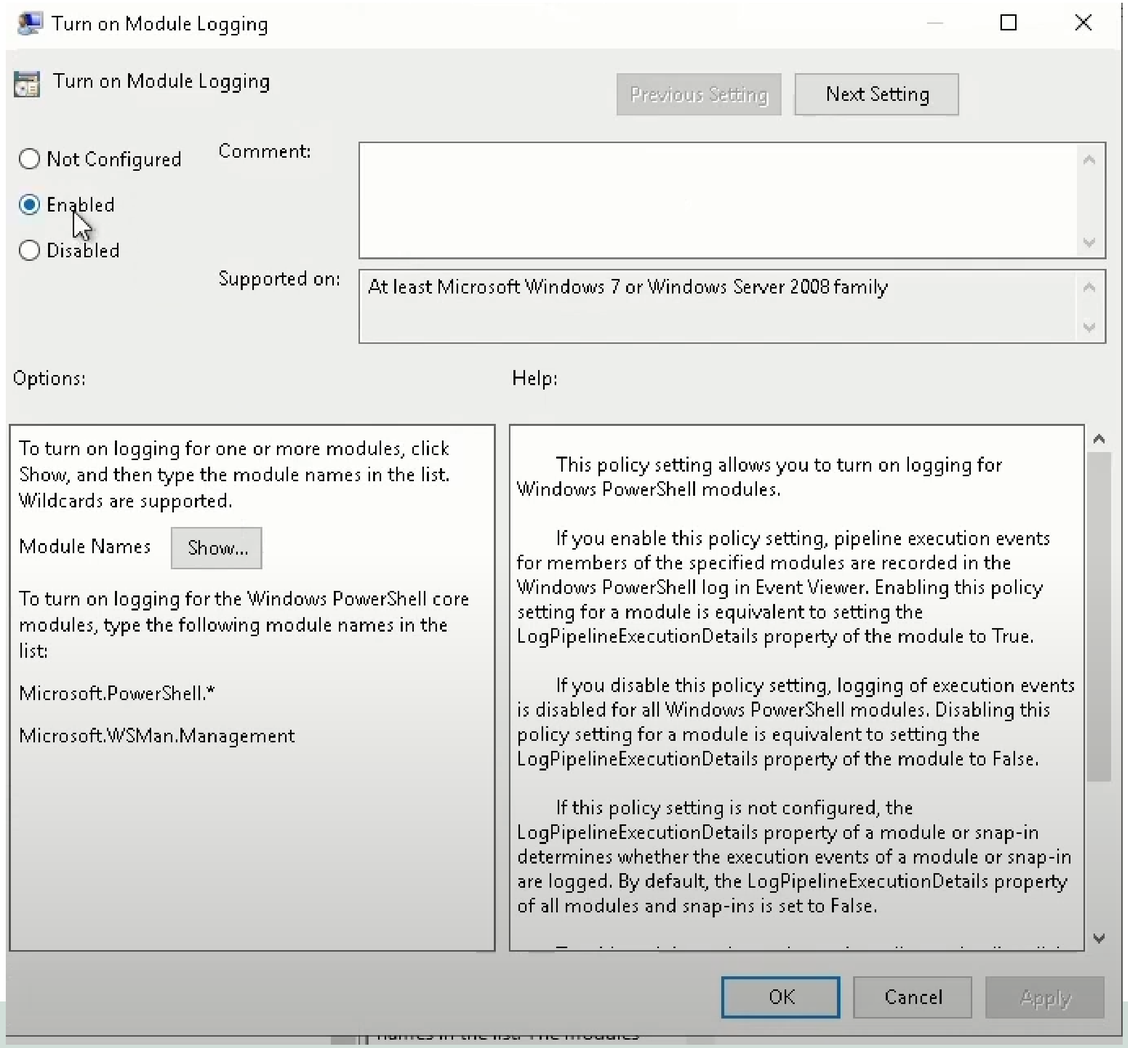
- Sesiones RDP:
  - **%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSesiónManager%4Operational**
    - Event ID 21: Conexiones
    - Event ID 24: Desconexiones
  - **%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational**
    - EventID: 1149

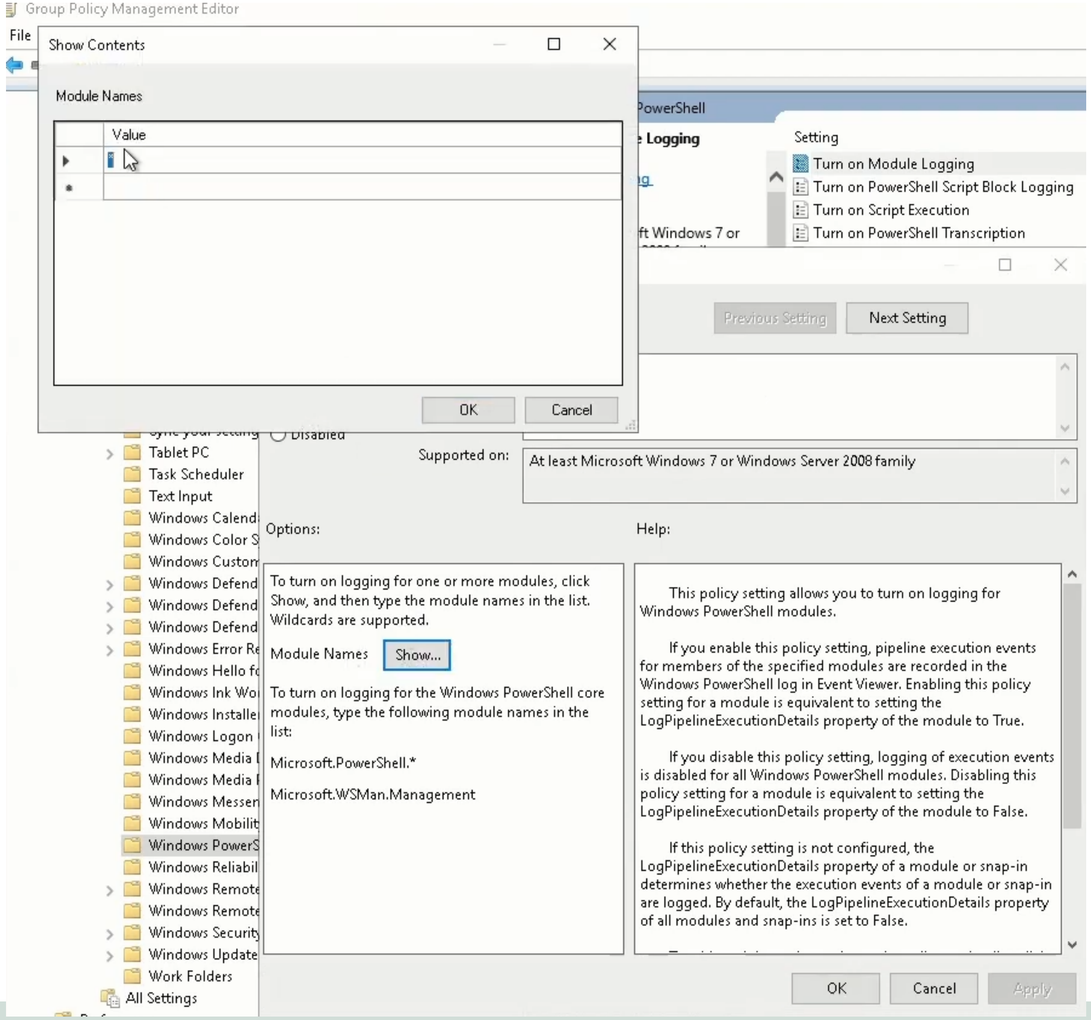
Ejecución de PowerShell

- **%SystemRoot%\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx**
  - **4103:** Muestra el comando de powershell ejecutado
  - **4104**: Muestra el bloque de script ejecutado. Captura los comandos enviados a powershell
  - **400**: Indica el inicio de la ejecución o inicio de sesión de powershell
  - **800**: Muestra información adicional

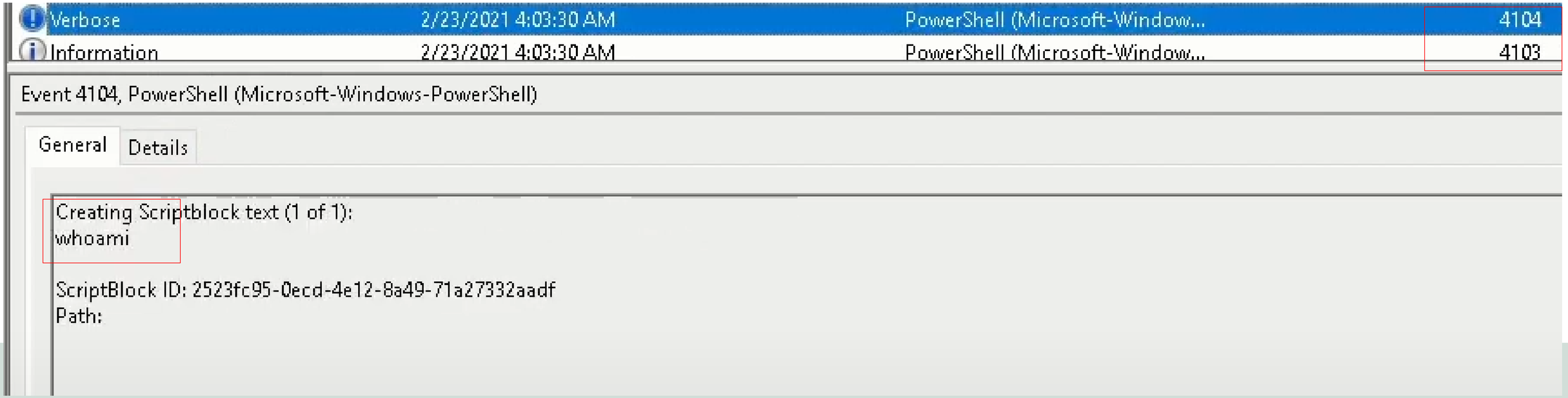
Atención no vienen activas, hay que activarlas !!!




Turn on Module Logging
Turn on Module Logging
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Microsoft Windows 7 or Windows Server 2008 family
Options:
Help:
To turn on logging for one or more modules, click Show, and then type the module names in the list. Wildcards are supported.
Module Names
Show...
To turn on logging for the Windows PowerShell core modules, type the following module names in the list:
Microsoft.PowerShell.*
Microsoft.WSMan.Management
This policy setting allows you to turn on logging for Windows PowerShell modules.
If you enable this policy setting, pipeline execution events for members of the specified modules are recorded in the Windows PowerShell log in Event Viewer. Enabling this policy setting for a module is equivalent to setting the LogPipelineExecutionDetails property of the module to True.
If you disable this policy setting, logging of execution events is disabled for all Windows PowerShell modules. Disabling this policy setting for a module is equivalent to setting the LogPipelineExecutionDetails property of the module to False.
If this policy setting is not configured, the LogPipelineExecutionDetails property of a module or snap-in determines whether the execution events of a module or snap-in are logged. By default, the LogPipelineExecutionDetails property of all modules and snap-ins is set to False.
OK
Cancel
Apply


Group Policy Management Editor
File
Show Contents
Module Names
Value
OK
Cancel
PowerShell
Logging
Setting
Turn on Module Logging
Turn on PowerShell Script Block Logging
Turn on Script Execution
Turn on PowerShell Transcription
Previous Setting
Next Setting
Disabled
Supported on:
At least Microsoft Windows 7 or Windows Server 2008 family
Options:
Help:
To turn on logging for one or more modules, click Show, and then type the module names in the list. Wildcards are supported.
Module Names
Show...
To turn on logging for the Windows PowerShell core modules, type the following module names in the list:
Microsoft.PowerShell.*
Microsoft.WSMan.Management
This policy setting allows you to turn on logging for Windows PowerShell modules.
If you enable this policy setting, pipeline execution events for members of the specified modules are recorded in the Windows PowerShell log in Event Viewer. Enabling this policy setting for a module is equivalent to setting the LogPipelineExecutionDetails property of the module to True.
If you disable this policy setting, logging of execution events is disabled for all Windows PowerShell modules. Disabling this policy setting for a module is equivalent to setting the LogPipelineExecutionDetails property of the module to False.
If this policy setting is not configured, the LogPipelineExecutionDetails property of a module or snap-in determines whether the execution events of a module or snap-in are logged. By default, the LogPipelineExecutionDetails property of all modules and snap-ins is set to False.
Tablet PC
Task Scheduler
Text Input
Windows Color S
Windows Custom
Windows Defend
Windows Error Re
Windows Hello fo
Windows Ink Wo
Windows Installe
Windows Logon
Windows Media
Windows Messen
Windows Mobilit
Windows PowerS
Windows Reliabil
Windows Remote
Windows Remote
Windows Security
Windows Update
Work Folders
All Settings
OK
Cancel
Apply

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/

PS C:\Users\Adrián> whoami
desktop-hihmn89\adrián
PS C:\Users\Adrián>
```



Wevtutil

```
C:\Users\Adrián>wevtutil
No se especificó el comando.
Utilidad de línea de comandos de eventos de Windows.

Permite recuperar información acerca de registros de eventos y publicadores,
instalar y desinstalar manifiestos de eventos, ejecutar consultas y exportar,
archivar y borrar registros.

Uso:

Puede usar la versión corta (por ejemplo, ep /uni) o larga (por ejemplo,
enum-publishers /unicode) de los nombres de opciones y comandos. Los
comandos, las opciones y los valores de las opciones no distinguen
mayúsculas de minúsculas.

Las variables se escriben en mayúsculas.

wevtutil COMANDO [ARGUMENTO [ARGUMENTO] ...] [/OPCIÓN:VALOR
[/OPCIÓN:VALOR] ...]
```

Ejercicio:

Crear un comando para que me muestre los 10 últimos eventos de seguridad

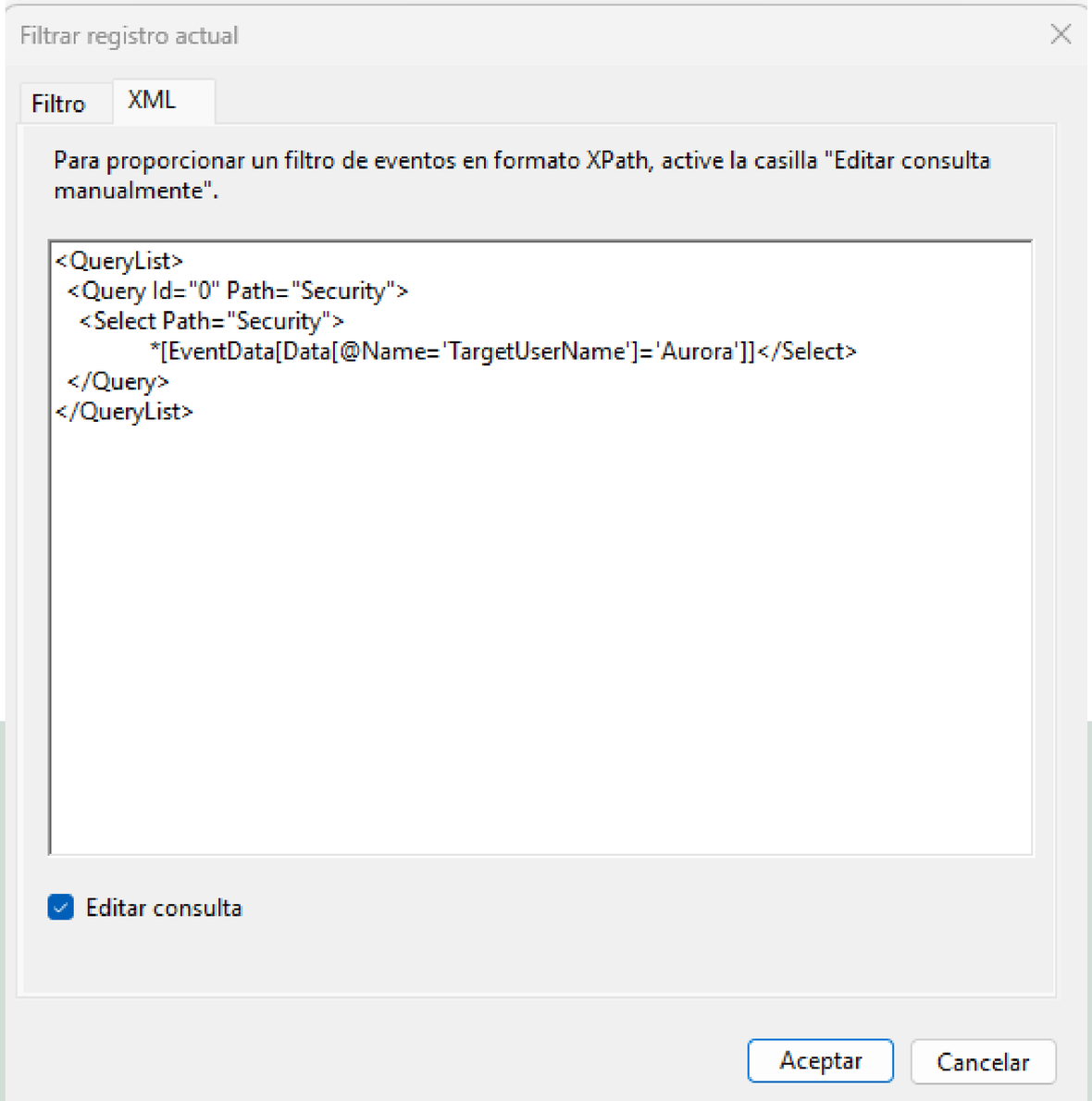
```
C:\Users\Adrián>wevtutil query-events Security /c:10 /f:text
Event[0]
  Log Name: Security
  Source: Microsoft-Windows-Security-Auditing
  Date: 2023-05-16T05:56:00.6620000Z
  Event ID: 5379
  Task: User Account Management
  Level: Información
  Opcode: Información
  Keyword: Auditoría correcta
  User: N/A
```

Ejercicio:

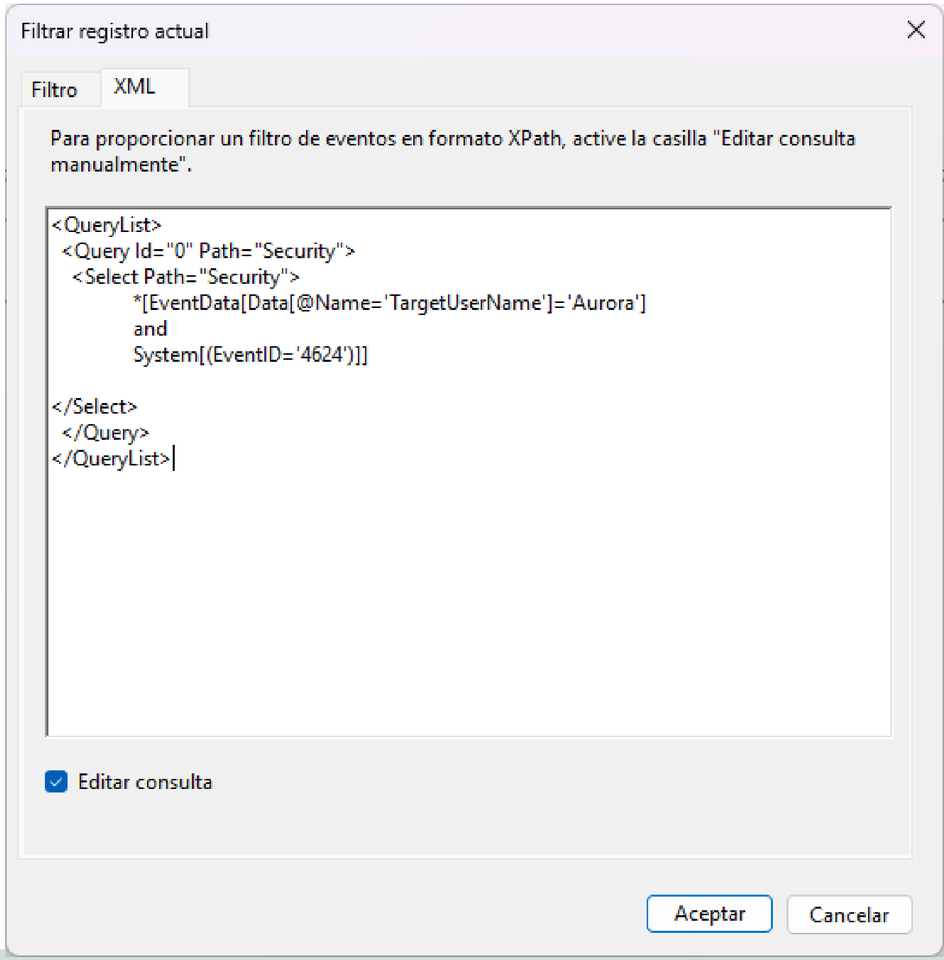
¿Qué hace este comando?

```
C:\Users\Adrián>wevtutil query-events Security /c:10 /f:text /q:"Event[System[EventID=4624]]"
```

Visor de eventos: Filtrando inicio de sesión con XML



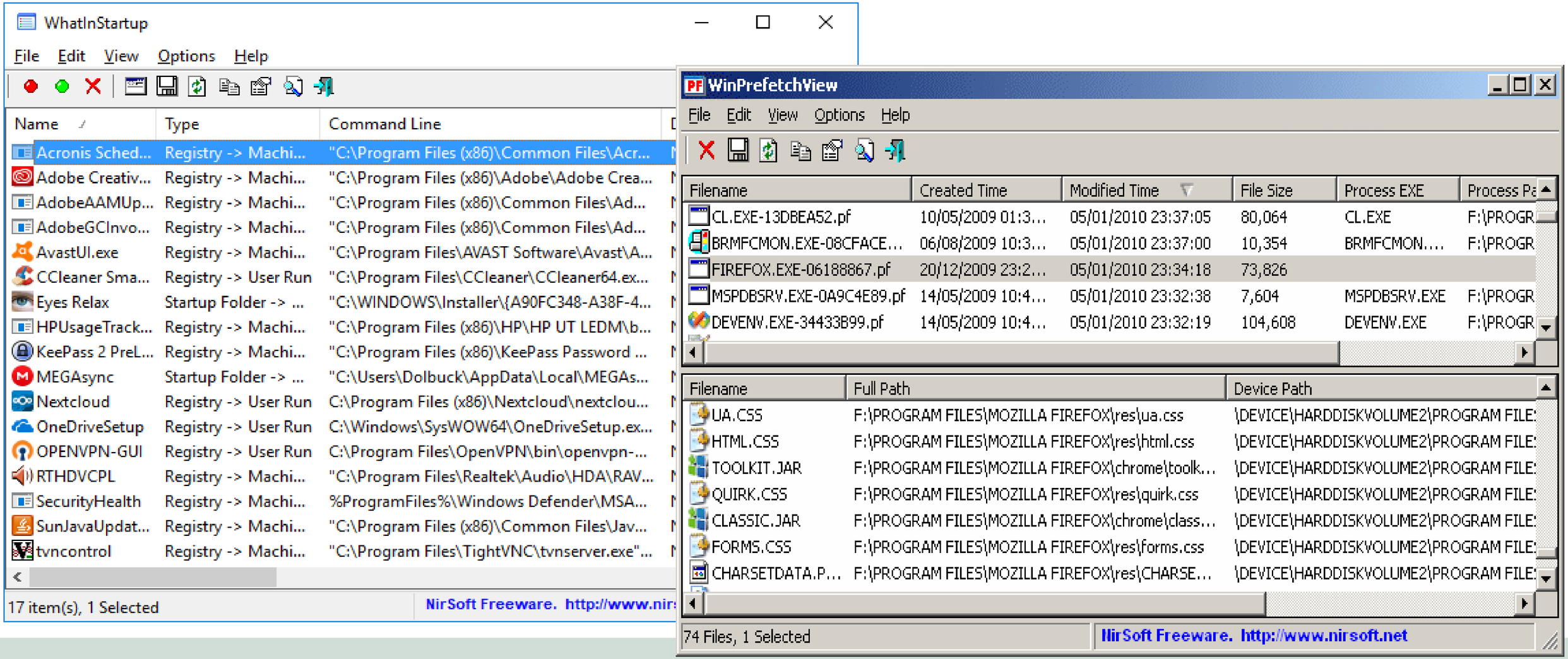
```
<QueryList>
  <Query Id="0" Path="Security">
   <Select Path="Security">
   *[EventData[Data[@Name='TargetUserName']='Aurora']
   and
   System[(EventID='4624')]]

</Select>
  </Query>
</QueryList>
```



Programas que se ejecutan al iniciar Windows

Las principales entradas de registro donde se almacenan el listado de programas que se ejecutan al iniciar el sistema operativo son las siguientes:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager


WhatInStartup
File Edit View Options Help
Name Type Command Line
Acronis Sched... Registry -> Machi... "C:\Program Files (x86)\Common Files\Acr...
Adobe Creativ... Registry -> Machi... "C:\Program Files (x86)\Adobe\Adobe Crea...
AdobeAAMUp... Registry -> Machi... "C:\Program Files (x86)\Common Files\Ad...
AdobeGCInvo... Registry -> Machi... "C:\Program Files (x86)\Common Files\Ad...
AvastUI.exe Registry -> Machi... "C:\Program Files\AVAST Software\Avast\A...
CCleaner Sma... Registry -> User Run "C:\Program Files\CCleaner\CCleaner64.ex...
Eyes Relax Startup Folder -> ... "C:\WINDOWS\Installer\{A90FC348-A38F-4...
HPUsageTrack... Registry -> Machi... "C:\Program Files (x86)\HP\HP UT LEDM\b...
KeePass 2 PreL... Registry -> Machi... "C:\Program Files (x86)\KeePass Password ...
MEGAsync Startup Folder -> ... "C:\Users\Dolbuck\AppData\Local\MEGAs...
Nextcloud Registry -> User Run C:\Program Files (x86)\Nextcloud\nextclou...
OneDriveSetup Registry -> User Run C:\Windows\SysWOW64\OneDriveSetup.ex...
OPENVPN-GUI Registry -> User Run C:\Program Files\OpenVPN\bin\openvpn-...
RTHDVCPL Registry -> Machi... "C:\Program Files\Realtek\Audio\HDA\RAV...
SecurityHealth Registry -> Machi... %ProgramFiles%\Windows Defender\MSA...
SunJavaUpdat... Registry -> Machi... "C:\Program Files (x86)\Common Files\Jav...
tvncontrol Registry -> Machi... "C:\Program Files\TightVNC\tvnserver.exe"...
17 item(s), 1 Selected
NirSoft Freeware. http://www.nir
WinPrefetchView
File Edit View Options Help
Filename Created Time Modified Time File Size Process EXE Process Pa
CL.EXE-13DBEA52.pf 10/05/2009 01:3... 05/01/2010 23:37:05 80,064 CL.EXE F:\PROGR
BRMFCMON.EXE-08CFACE... 06/08/2009 10:3... 05/01/2010 23:37:00 10,354 BRMFCMON.... F:\PROGR
FIREFOX.EXE-06188867.pf 20/12/2009 23:2... 05/01/2010 23:34:18 73,826
MSPDBSRV.EXE-0A9C4E89.pf 14/05/2009 10:4... 05/01/2010 23:32:38 7,604 MSPDBSRV.EXE F:\PROGR
DEVENV.EXE-34433B99.pf 14/05/2009 10:4... 05/01/2010 23:32:19 104,608 DEVENV.EXE F:\PROGR
Filename Full Path Device Path
UA.CSS F:\PROGRAM FILES\MOZILLA FIREFOX\res\ua.css \DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
HTML.CSS F:\PROGRAM FILES\MOZILLA FIREFOX\res\html.css \DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
TOOLKIT.JAR F:\PROGRAM FILES\MOZILLA FIREFOX\chrome\toolk... \DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
QUIRK.CSS F:\PROGRAM FILES\MOZILLA FIREFOX\res\quirk.css \DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
CLASSIC.JAR F:\PROGRAM FILES\MOZILLA FIREFOX\chrome\class... \DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
FORMS.CSS F:\PROGRAM FILES\MOZILLA FIREFOX\res\forms.css \DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
CHARSETDATA.P... F:\PROGRAM FILES\MOZILLA FIREFOX\res\CHARSE... \DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
74 Files, 1 Selected
NirSoft Freeware. http://www.nirsoft.net

Recursos para Windows

- Nirsoft >> https://www.nirsoft.net/
- Zibermman >> https://ericzimmerman.github.io/#!index.md
- KAPE >> https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape

- Autopsy >> https://www.autopsy.com/
- FTK Imager >> https://www.exterro.com/ftk-imager
- Process Hacker >> https://processhacker.sourceforge.io/github.php

Herramientas forenses para entornos GNU/Linux

Enfoque:

- Procesos
- Red
- Directorios
- Archivos
- Usuarios y sesiones
- Logs

Todo es un archivo!!

Procesos y red

Procesos extraños, ejecutándose con usuarios del proceso “switch”
Procesos extraños ejecutándose con “root”
Sockets abiertos, conexiones tcp (established) y correlacionar con PIDs

#netstat -antupo

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name     Timer
tcp        0      0 0.0.0.0:587             0.0.0.0:*               LISTEN      983/openvpn          off (0.00/0/0)
tcp        0      0 0.0.0.0:10443           0.0.0.0:*               LISTEN      998/openvpn          off (0.00/0/0)
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      768/systemd-resolve  off (0.00/0/0)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1032/sshd            off (0.00/0/0)
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      1068/stunnel4        off (0.00/0/0)
```

Procesos y red

Procesos extraños, ejecutándose con usuarios del proceso “switch”
Procesos extraños ejecutándose con “root”
Sockets abiertos, conexiones tcp (established) y correlacionar con PIDs

#ps –ef | grep 983

```
root       983     1  0 Feb16 ?        00:02:02 /usr/sbin/openvpn --status /run/openvpn-server
```

El directorio /proc/

El kernel de Linux tiene dos funciones primarias: controlar el acceso a los dispositivos físicos del ordenador y establecer cuándo y cómo los procesos interactuarán con estos dispositivos. El directorio /proc/ (o sistema de archivos proc) contiene una jerarquía de archivos especiales que representan el estado actual del kernel. Esto permite a las aplicaciones y usuarios mirar detenidamente en la vista del kernel del sistema.

Dentro del directorio /proc/, se puede encontrar una gran cantidad de información con detalles sobre el hardware del sistema y cualquier proceso que se esté ejecutando actualmente. Además, algunos de los archivos dentro del árbol de directorios /proc/ pueden ser manipulados por los usuarios y aplicaciones para comunicar al kernel cambios en la configuración.

Aquí les dejo algunos archivos de los cuales se puede obtener información importante del sistema.

Buscar en el directorio proc

#ls –al /proc/983

cmdline

cwd > /etc/openvpn/server

environ

exe -> /usr/sbin/openvpn

fd

maps

stack

status

AUDIT

¿Qué es el comando Auditd (Linux Audit Framework)?
Brevemente, pudiéramos describir a dicho comando Auditd como, una herramienta de software (framework) de auditoría para Linux, la cual, proporciona un sistema de auditoría compatible con CAPP (Controlled Access Protection Profile, en inglés, o Perfil de Protección de Acceso Controlado, en español). Por lo que, es capaz de recopilar información de manera confiable sobre cualquier evento relevante (o no) para la seguridad en un sistema operativo Linux.

En consecuencia, es ideal para apoyarnos a la hora de hacer seguimientos de las acciones realizadas en un SO. De esta forma, el comando Auditd o el Framework de Auditoria Linux (Linux Audit Framework o LAF) es capaz de ayudarnos a mantener nuestro SO más seguro, gracias a proveernos de los medios necesarios para analizar lo que sucede en el mismo con un gran nivel de detalle.

Por ejemplo, en Debian GNU/Linux y derivados sería:

sudo apt install auditd
Mientras que, en Fedora GNU/Linux y Red Hat, y sus similares sería:

sudo dnf install auditd
sudo yum install audit
Y para su uso básico y predeterminado solo hace falta ejecutar las órdenes de comando siguientes:

Chequear estado de ejecución
sudo systemctl status audit

Ver las reglas configuradas actualmente

sudo auditctl –l

Creación de reglas de visualización (watch) o control (syscall)

sudo auditctl -w /carpeta/archivo -p permisos-otorgados

sudo auditctl -a action,filter -S syscall -F field=value -k keyword

Gestionar todas las reglas creadas

sudo vim /etc/audit/audit.rules

Listar todos los eventos que tengan que ver con un proceso concreto según su PID, palabra clave asociada, ruta o archivo o llamadas al sistema.

sudo ausearch -p PID

sudo ausearch -k keyword

sudo ausearch -f ruta

sudo ausearch -sc syscall

LSOF

Lsof es una potente herramienta disponible en la shell de Linux que lista los ficheros abiertos en el sistema. Partiendo de esta base, podemos conocer rápidamente que ficheros mantiene abiertos un determinado proceso (PID) o usuario e información adicional como el puerto utilizado por dichos servicios/ficheros, sockets en uso, etc.

Lanzando el comando lsof sin ningún parámetro listará todos los ficheros abiertos en la máquina en ese momento, no es recomendable ya que como imaginaréis saldrá una cantidad enorme.

Algunos de los ejemplos de uso más comunes son los siguientes:

Listar ficheros abiertos por un determinado PID

```
# lsof -p PID
```

Listar ficheros abiertos de un determinado usuario:

```
# lsof –u adrian
```

Ver actividad de red en tiempo real

```
#lsof –i
```

Ver archivos abiertos por un proceso o programa concreto

Con el parámetro «-c» podemos visualizar los archivos abiertos por un proceso en ejecución así como los puertos en los que está escuchando y sus conexiones establecida

```
#lsof –c programa
```

Ver archivos abiertos en un directorio concreto

El parámetro «+D» seguido de un path muestra los archivos abiertos de esa ruta especificada. Por ejemplo, para mostrar los archivos abiertos y por quien en /etc:

Archivos interesantes para analizar

/var/log/messages
Aquí encontraremos los logs que llegan con prioridad *info* (información), *notice* (notificación) o *warn* (aviso).

/var/log/secure
Registra los accesos al servidor que tienen relación con procesos de autentificación.

/var/log/auth.log
En este log se registran los login en el sistema, las veces que hacemos *su*, etc. Los intentos fallidos se registran en líneas con información del tipo *invalid password* o *authentication failure*.

/var/log/maillog
Registro del servidor de emails.

/var/log/cron
Registro de tareas del cron.

Archivos interesantes para analizar

/var/log/user.log
Registro de avisos enviados a usuarios del sistema, por ejemplo “shutdown”
Además podemos ver los archivos de algunos servicios importantes:

Ficheros de acceso web: (cambia httpd por apache2 en caso de la nueva versión de apache)
/var/log/httpd/access_log

Acceso de “login”:
/var/log/btmp -> logins fallidos (lastb)
/var/log/wtmp -> logias y logouts (last)
/var/log/lastlog -> logias en el sistema (lastlog)
/var/run/utmp -> usuarios en el sistema (who /w)
/var/run/dmesg-> logs del Kernel (dmesg)

Archivos interesantes para analizar

Comando de Shell.
$HOME/<user>/ .bash_history
$HOME/ <user>/.sh_history
$HOME/<user>/ .history

Comando less:
$HOME/ .lesshst

Equipos a los que se ha conectado con SSH:
$HOME/ .ssh/known_hosts

Comandos para obtener información básica

Obtener un listado de usuarios: /etc/passwd /etc/shadow

Grupos del sistema: /etc/group

Versión: /etc/*release /etc/*version

Kernel: uname –a

Modulos del Kernel cargados: lsmod

Procesos: ps axufwww

Puertos: netstat –tanp

Hora: date

Software: dpkg –l / rpm –qa

CPU: lspci

Memoria: free –m

Interfaces de red: ifconfig –a

Rutas: route –n / netstat –nr

Tabla arp: arp –n

Detectar herramientas de Malware y rootkits

Instalamos los paquetes necesarios para ejecutar ClamAV, el demonio del mismo y la documentación de este:

```
# apt-get install clamav-base clamav-docs clamav-daemon daemon
```

Si se prefiere instalar desde las fuentes, descargar la versión stable, desinstalar la versión antigua:

```
# dpkg - remove clamav *
```

verificando que no quedan bibliotecas instaladas y que solo había una versión de Clamav instalada.

Whereis freshclam

Whereis clamscan

Ubicación de Archivos Principales

/etc/clamav/, ubicación de los ficheros de configuración:

cd /etc/clamav/

/var/lib, aquí es donde se ubicará la base de datos de ClamAV.

ls -ltr /var/lib/clamav

/var/log, ubicación de los logs de ClamAV.

ls -ltr /var/log/clamav

Detección de rootkits

Antes que nada, deberíamos de empezar definiendo que es un rootkits.

Rootkit es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

RKUNTER: Es una herramienta de Unix que detecta los rootkits, los backdoors y los exploit locales mediante la comparación de los hashes MD5 de ficheros importantes con su firma correcta en una base de datos en línea, buscando los directorios por defecto (de rootkits), los permisos incorrectos, los archivos ocultos, las cadenas sospechosas en los módulos del kernel, y las pruebas especiales para Linux y FreeBSD.

Fuente: Wikipedia.

Rkhunter: http://www.rootkit.nl

Para instalarlo podemos ejecutar:

```
# apt-get install rkhunter
```

En la primera ejecución usaremos:

#rkhunter - -update

#rkhunter --propupd

Y luego lanzaremos la aplicación

```
rkhunter - - check
```

Herramientas forenses para entornos redes

Capturas de tráfico de red

Modo Promiscuo

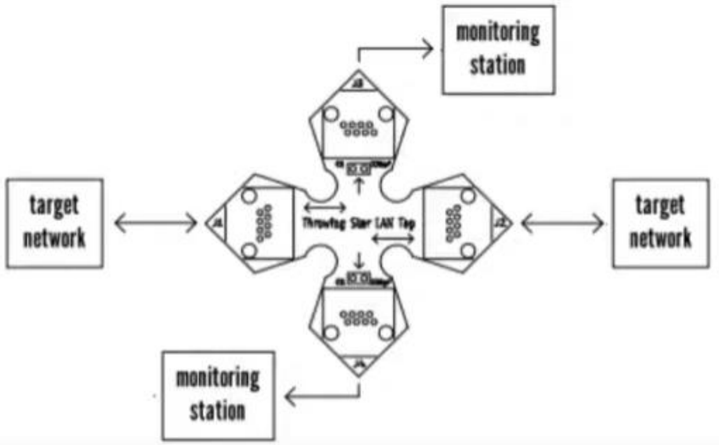
HUB

Port Mirroring

TAP de Red

Envenenamiento ARP

Capturas de tráfico de red



Qué mirar en cada caso

- **Switches**
  - Tablas CAM (Content Addressable Memory)
  - Capturas de tráfico a través de puerto espejo
  - Logs
- **Routers**
  - Tablas de enrutamiento
  - Logs
  - Flujo de datos
- **Firewalls**
  - Logs
  - Capturas de Tráfico
  - Flujos de datos

Qué mirar en cada caso

- **Sistemas de Detección y Prevención de Usuarios**
  - Logs
  - Capturas de Tráfico
- **Servidores Proxy**
  - Logs
- **Servidores DNS**
  - Logs
- **Servidores DHCP**
  - Logs
- **Servidores de Autenticación**
  - Logs

Caso práctico de un análisis forense sobre entorno Windows

Reto forense: El despacho de Lionel

El prestigioso bufete del abogado Lionel Hutz sufrió una fuga de información de importantes casos mediáticos que llevaba.

Tras años de fracaso el abogado Lionel logró por fin la fama tras ganar los importantes casos como el caso de Round Springfield en donde representó a Bart en la demanda contra Corporación de Cereales Krusty. Gracias a una serie de contradicciones de Krusty en la rueda de prensa.

¿Podrás ayudar a Lionel Hutz a encontrar al que robó la información de su despacho y poner en “entredicho” el prestigio del bufete?

Para resolver este difícil reto partirás de las evidencias obtenidas por Clancy Wiggum.

¿Podrías indicar quién ha sido el ladrón?

Desafío 1:

- Quién fue el último usuario en iniciar sesión
- Qué día se instaló el sistema operativo (formato: ddmmyy)
- ¿Sabiendo que la contraseña Lionel tiene 4 caracteres, sabrías indicar cuál es?
- ¿Sabrías localizar la IP del posible ladrón?
- ¿Sabrías indicar la marca del pendrive introducido más veces en el sistema?
- Qué tipo de CMS es la web del bufete.
- ¿Cuál es el nombre de usuario de la bbdd de la web?
- ¿Podrías indicar el día del ataque?
- Qué dirección entró más veces a la web del bufete
- ¿Sabrías indicar el número de serie del volumen?
- ¿Cuándo se apagó el equipo por última vez?
- Si Lionel actualizaba la web, ¿sabrías decirnos la clave del WordPress?
- ¿Sabrías identificar el autor del robo?

Regístrate aquí

Conclusiones y preguntas abiertas para discusión

Recursos

1. https://www.youtube.com/watch?v=laT-jfy4mII&ab_channel=hackplayers
2. https://www.youtube.com/watch?v=GhCZfCzn2l0&ab_channel=SANSDigitalForensicsandIncidentResponse
3. https://www.youtube.com/watch?v=SjDH_vTuefM&ab_channel=SANSDigitalForensicsandIncidentResponse
4. https://www.youtube.com/watch?v=dsQdbvquBr8&ab_channel=CCN

sedian Seguridad Digital de Andalucía