***I.E.S. Fernando Aguilar Quignon*** 

*C/Conil de la Frontera, 3*

*CP 11010, Cádiz*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Administración de Sistemas Operativos - 1ª Evaluación (RA 2 – CE h, i) Unidad Didáctica 1. Arranque y procesos del sistema

**1. Responde las siguientes preguntas:**

**• ¿Qué herramientas específicas existen en los sistemas operativos Linux y Windows para la identificación y monitoreo de procesos no identificados, y cómo se comparan en términos de flexibilidad y control, interfaz de usuario, profundidad de información e integración con el sistema?**

**LINUX vs WINDOWS:**

1. **Flexibilidad y control**: En Linux, las herramientas como ps, htop y lsof suelen ser más flexibles porque permiten una mayor personalización y control sobre los procesos. En Windows, herramientas como Process Explorer también ofrecen bastante control, pero las opciones integradas, como el Administrador de Tareas, son más básicas y tienen menos opciones avanzadas.
2. **Interfaz de usuario**: Windows generalmente ofrece interfaces más fáciles de usar y gráficas, como el Administrador de Tareas, mientras que en Linux muchas de las herramientas avanzadas se manejan desde la línea de comandos, lo que puede ser menos intuitivo para algunos usuarios.
3. **Profundidad de información**: Ambos sistemas pueden ofrecer información muy detallada. En Linux, herramientas como ps y lsof proporcionan muchos datos técnicos sobre los procesos, mientras que en Windows, Process Explorer también ofrece un nivel similar de detalle.
4. **Integración con el sistema**: Las herramientas en ambos sistemas están bien conectadas al sistema operativo. En Linux, las herramientas suelen dar un control más profundo sobre los procesos y las configuraciones del sistema, mientras que en Windows las herramientas son más fáciles de usar para usuarios que no son tan técnicos.

**• ¿Cuáles son las implicaciones de seguridad asociadas con la aparición de procesos no identificados en un sistema operativo, y qué tipos de amenazas pueden representar para la integridad, confidencialidad y disponibilidad del sistema y de los datos?**

Las vulnerabilidades del sistema operativo son debilidades o fallas en un sistema operativo que los atacantes pueden aprovechar para obtener acceso no autorizado o causar daño. Estas vulnerabilidades pueden permitir a los atacantes robar datos, interrumpir servicios o tomar el control del sistema

Tenemos dos tipos de vulnerabilidades en el sistema operativo:

* **Errores de codificación:** Los errores cometidos durante el proceso de desarrollo de software pueden crear brechas de seguridad.
* **Problemas de configuración:** Las configuraciones incorrectas o los sistemas mal configurados pueden dejar un sistema operativo expuesto a ataques.

Uno de los impactos más significativos son las violaciones de datos, donde los atacantes pueden robar información confidencial, como datos de clientes o propiedad intelectual. Esto conduce a posibles pérdidas financieras y daña la confianza de la empresa y cliente. Aunque también existen más tipos de vulnerabilidades, como son:

* **Phishing**: Técnicas engañosas para obtener información confidencial, como contraseñas o datos bancarios, haciéndose pasar por entidades confiables
* **Inyecciones SQL**: Permiten la manipulación de datos almacenados, afectando su integridad.
* **Ataques de Denegación de Servicio**: Saturan los recursos del sistema para hacerlo inaccesible para usuarios legítimos

Es fundamental implementar medidas de seguridad adecuadas, como firewalls, sistemas de detección de intrusiones, encriptación, copias de seguridad y capacitación a usuarios, para mitigar estos riesgos y proteger la información crítica

**• Investigue y describa algunos casos reales en los que la aparición de procesos no identificados haya causado brechas de seguridad o interrupciones operativas. ¿Qué medidas de mitigación o prevención se implementaron para resolver o prevenir estos incidentes?**

* **WannaCry:** Encripta los archivos del equipo infectado, especialmente, los documentos y el contenido multimedia. En lugar de ser eliminada, la información es secuestrada, para pedir un rescate. La solución de este malware consiste en algunos pasos:

1. NO pagar el rescate, este virus solicita un rescate a cambio de una suma de dinero, la cual no debemos pagar
2. Mantener el sistema operativo actualizado
3. La solución más eficiente es utilizar un software que detecte y bloquee la infección del ransomware
4. No descargues archivos de sitios web que no sean de confianza

* **Ataque a Bank of America:** Un fallo de seguridad en Infosys McCamish, un proveedor de software financiero, llevó a la exposición de datos personales y de cuenta de 57,028 clientes del Bank of America. La información comprometida incluía nombres, direcciones, fechas de nacimiento, números de Seguro Social y otros detalles relevantes:

1. Realizar auditorías de seguridad
2. Reforzar la cadena de confianza y mejorar la comunicación durante incidentes para proteger los datos

* Ataque a Volkswagen: ataque cibernético que resultó en el robo de aproximadamente 19.000 documentos del servidor de la compañía. Este ataque, al parecer se originó en China y pudo estar vinculado con espionaje cibernético internacional. Los datos robados incluían información crítica sobre las tecnologías propietarias de VE de Volkswagen y estrategias de producción.

1. Proteger tus activos digitales y la propiedad intelectual de tu empresa
2. Contratar una estrategia de ciberseguridad clara, deberías poner como prioridad crear una que sea robusta y adaptable

**2. Teniendo los siguientes procesos:**

• Init/Systemd.

• Bash.

• Cron.

• Syslogd.

• Networkd.

• Sshd.

• Explorer.exe

• Svchost.exe

• Services.exe

• Winlogon.exe

• Dwm.exe

• SearchIndexer.exe

**Crea una tabla con los siguientes campos:**

• Nombre de proceso o proceso.

• Sistema operativo.

• Función.

• Esencial (Sí / No)

• Justificación.

| **Proceso** | **S.O** | **Función** | **Esencial** | **Justificación** |
| --- | --- | --- | --- | --- |
| **Init/systemd** | Linux | Es el primer proceso que se inicia durante el arranque del sistema y es responsable de iniciar y gestionar todos los demás servicios y procesos | Si | Sin él, el sistema no podría funcionar |
| **Bash** | Linux | Permite realizar tareas repetitivas, tantas veces como desees | NO | Aunque muy útil, no es esencial para el funcionamiento del sistema. |
| **Cron** | Linux | Permite ejecutar tareas programadas | NO | El sistema puede funcionar sin él. |
| **Syslog** | Linux | Daemon que gestiona los registros del sistema, permitiendo el almacenamiento y visualización de logs de eventos y errores | NO | Aunque es muy útil para la administración y solución de problemas, no es crítico para el funcionamiento del sistema |
| **Networkd** | Linux | Aunque facilita la configuración y administración de la red, | NO | El sistema puede operar sin él |
| **Sshd** | Linux | Útil para administraciones remotas | NO | No es esencial para el funcionamiento del sistema local. |
| **Explorer.exe** | Win | Sirve como shell para el escritorio, la barra de tareas y el menú Inicio, y también administra la organización y visualización de archivos y carpetas | SI | Le ayuda al sistema a obtener los archivos que necesita de forma rápida y sencilla |
| **Svchost.exe** | Linux | Este proceso es esencial ya que permite que muchos servicios de Windows se ejecuten en modo compartido | SI | Optimiza el uso de recursos del sistema |
| **Services.exe** | Win | Este proceso es el gestor de servicios en Windows, encargado de iniciar, detener y administrar los servicios del sistema | SI | Sin Services.exe, los servicios no funcionarán correctamente, lo que afectaría negativamente al sistema operativo. |
| **Winlogon.exe** | Win | Maneja las sesiones de usuario, incluyendo el inicio y cierre de sesión. | SI | Es fundamental para la autenticación y seguridad del sistema. |
| **Dwm.exe** | Win | Es responsable de los efectos visuales y la gestión de ventanas en Windows | NO | Mejora la experiencia visual pero windows puede operar sin el |
| **SearchIndexer.exe** | Win | Se encarga de indexar archivos para mejorar la búsqueda en Windows | NO | Aunque mejora la funcionalidad, no es esencial para el funcionamiento del sistema operativo |