Análisis e identificación de procesos y servicios sospechosos en Linux

1. Objetivo. – Analizar los procesos y servicios en ejecución del sistema operativo Linux con el fin de identificar acciones legítimas y sospechosas.

2. Herramientas. - Para este laboratorio se utilizaron:

- Oracle VirtualBox.
- Cliente Ubuntu (máquina virtual)

3. Metodología / Análisis realizado

Esta sección describe el análisis realizado sobre los procesos, servicios y puertos del sistema Linux utilizando comandos de línea, con el objetivo de obtener información relevante para la seguridad del sistema y diferenciar acciones sospechosas de las normales. Todos los comandos utilizados se presentan en el Anexo A (página 7).

3.1 Identificación de procesos activos

Se realizó la identificación de los procesos activos en el sistema operativo Linux, con el propósito diferenciar lo normal de lo sospechoso. Los resultados mostraron que el sistema no contiene usuarios raros, procesos con nombres extraños o que utilicen demasiados recursos. Dentro de un monitoreo de seguridad, esta acción es una de las principales que se ejecuta a la hora de investigar actividades sospechosas.

3.2 Monitoreo de procesos en tiempo real

Se analizaron los diferentes procesos en tiempo real, con el fin entender un comportamiento normal del sistema, diferenciando el ruido de los procesos importantes.

El análisis hecho evidenció varios procesos legítimos ejecutándose, ya que no existen usuarios desconocidos, ni procesos que consuman con excesividad recursos del sistema. Además de que no se utiliza la red de forma brusca y que no existen rutas potencialmente sospechosas. (Ver Figura 1)

Esta práctica es necesaria para un mejor monitoreo de la seguridad del sistema e identificar procesos potencialmente sospechosos.

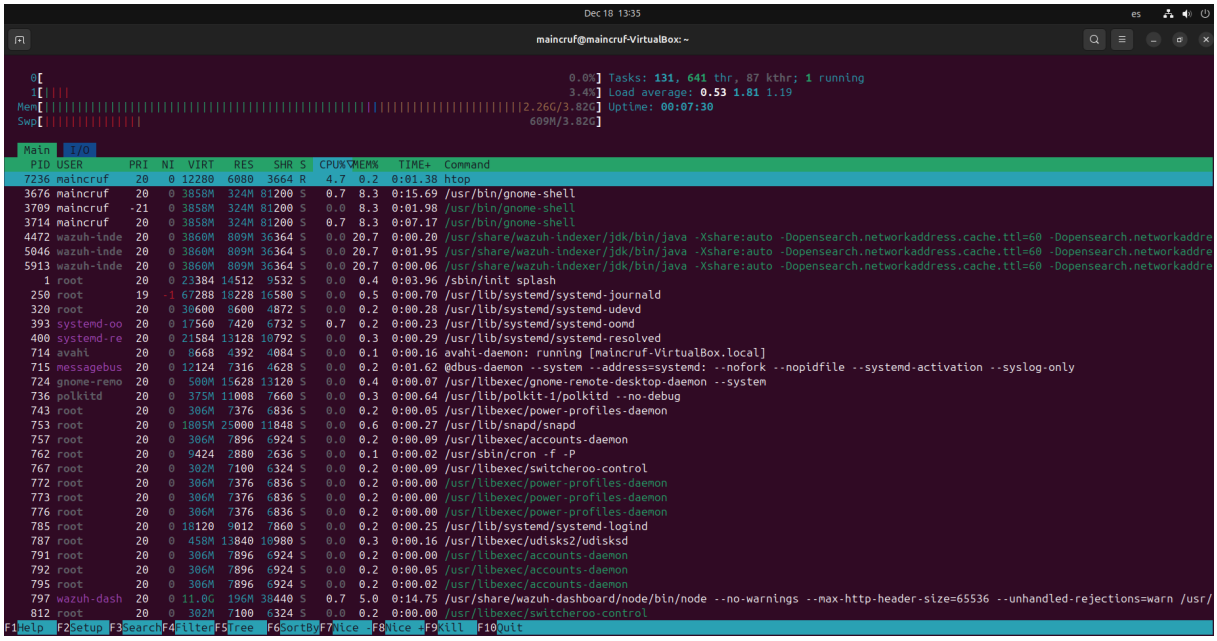

Figura 1. Procesos del sistema Linux en tiempo real

3.3 Servicios activos (systemd)

Se identificaron los servicios activos del sistema Linux, con el objetivo de determinar si existían servicios no legítimos.

Durante el proceso de análisis, no se observaron servicios con nombres genéricos, descripciones poco claras ni servicios que no correspondieran al uso normal del sistema. Como resultado, se concluye que los servicios identificados corresponden a servicios legítimos. (ver Figura 2)

Dentro de un monitoreo de seguridad, la identificación temprana de los servicios fuera de lo común es fundamental para fortalecer la seguridad del sistema.

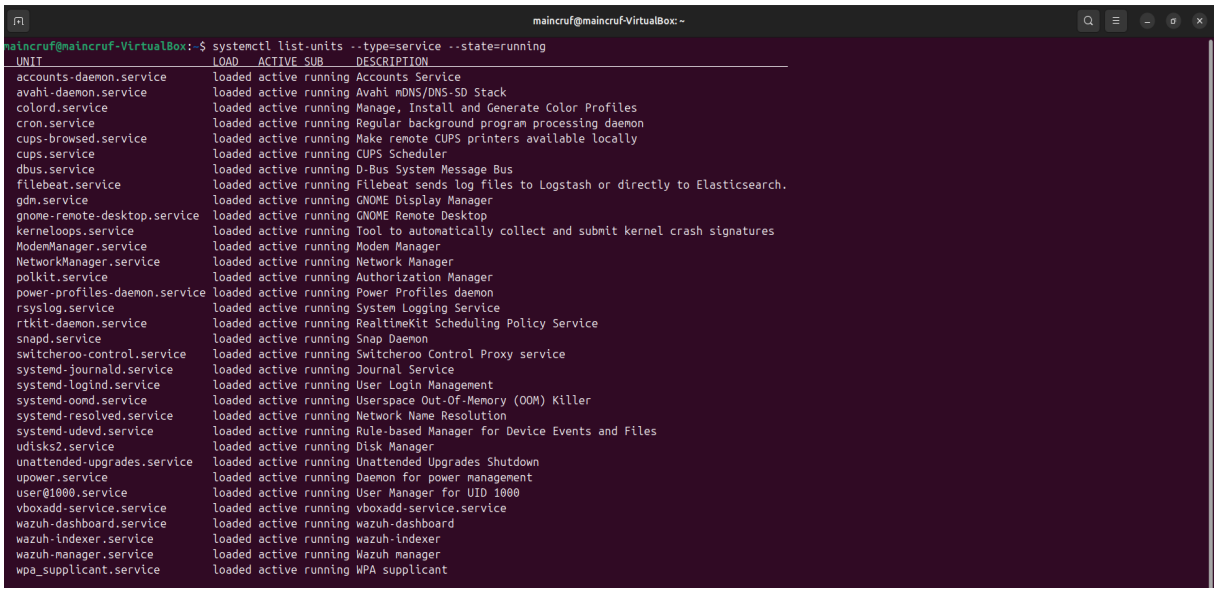

Figura 2. Servicios del sistema Linux.

3.4 Puertos y procesos asociados

Se realizó la revisión de los puertos existentes en el sistema Linux, con el propósito de identificar servicios expuestos que pueden representar un riesgo de seguridad.

El análisis reflejó varios puertos activos que corresponden a servicios legítimos como SSH, HTTP, HTTPS y componentes Wazuh. Sin embargo, se identificó que el puerto 5353 (mDNS) se encuentra habilitado y expuesto para todas las interfaces, tanto en TCP como UDP. En un entorno productivo, se recomienda restringirlo a redes locales o deshabilitarlo si no es necesario. (ver Figura 3)

Este tipo de verificación permite aplicar buenas prácticas de seguridad, minimizar el riesgo de accesos no autorizados, posibles ataques o la presencia de puertas traseras en el sistema.

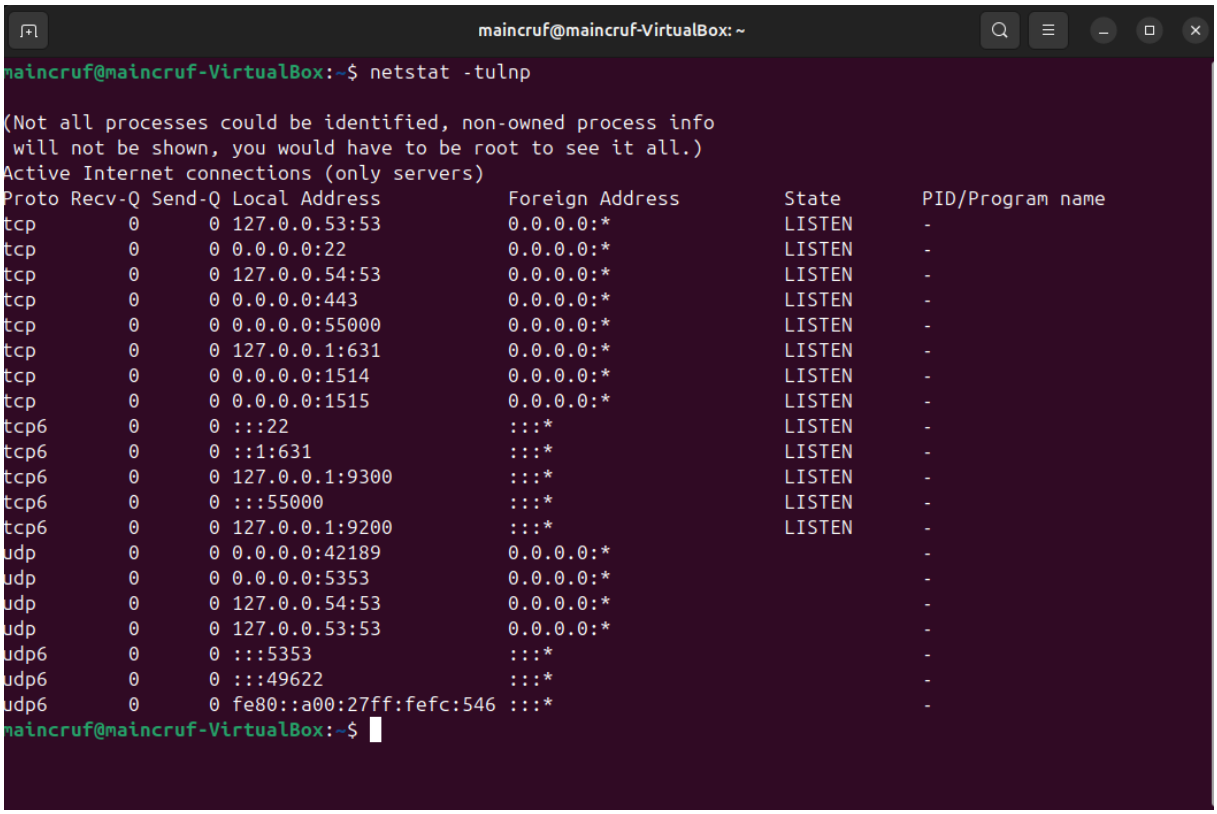

Figura 3. Puertos existentes en el sistema Linux.

3.5 Simulación de script malicioso

Se creó un script malicioso inofensivo con permisos de ejecución, configurado para ejecutarse en segundo plano de forma persistente. Con el fin de comprender como este tipo de archivos pueden operar en un entorno real y como pueden ser identificados mediante técnicas de análisis del sistema. (ver Figura 4)

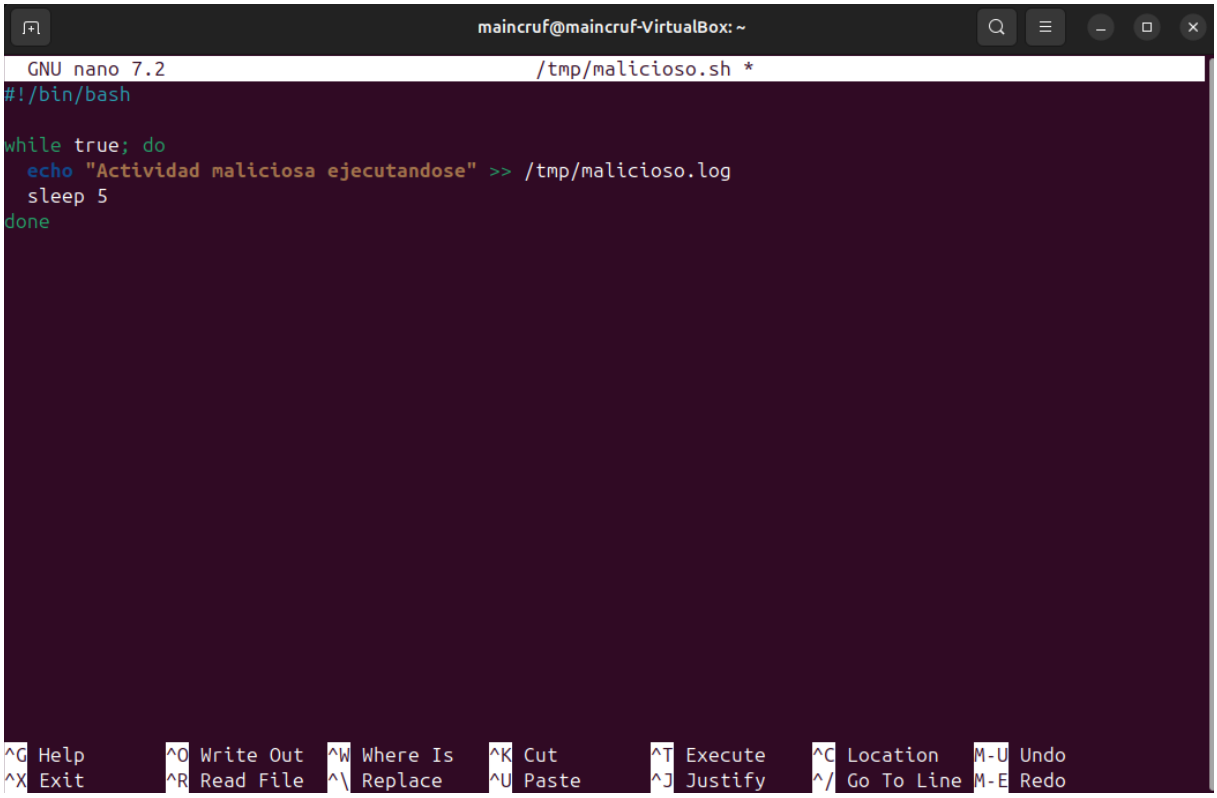

Figura 4. Creación de script no malicioso.

3.6 Detección de script malicioso

La identificación del archivo malicioso se realizó a través del monitor de procesos del sistema Linux, analizando el usuario al que pertenece, el consumo de recursos del sistema, el uso de red y la ruta en la que se encuentra. Aunque en un entorno real, los archivos maliciosos no suelen presentar nombres evidentes, se utilizaron estos criterios de análisis para identificar procesos sospechosos. (ver Figura 5)

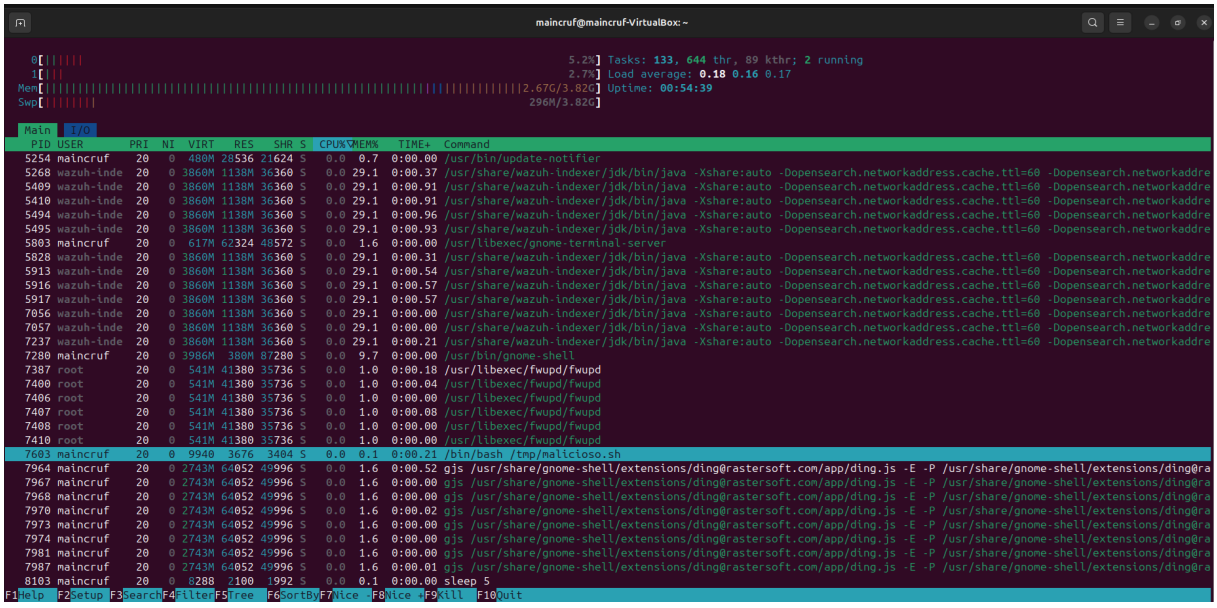

Figura 5. Análisis y detección de scritp malicioso

Una vez detectado el proceso, se empezó con la investigación accediendo al directorio /tmp, donde se obtuvo información detallada del archivo, incluyendo permisos, propietario, grupos, tamaño, fecha de modificación y nombre. Posteriormente, se logró visualizar el contenido del archivo sospechoso encontrado dentro del directorio temporal, confirmando la actividad maliciosa y deteniendo la ejecución del proceso. (ver Figura 6)

La identificación de un proceso o servicio anómalos dentro del sistema, es una parte fundamental y crítica en el ámbito de la seguridad, evitando ataques de mayor escala que podrían comprometer la integridad y disponibilidad del sistema.

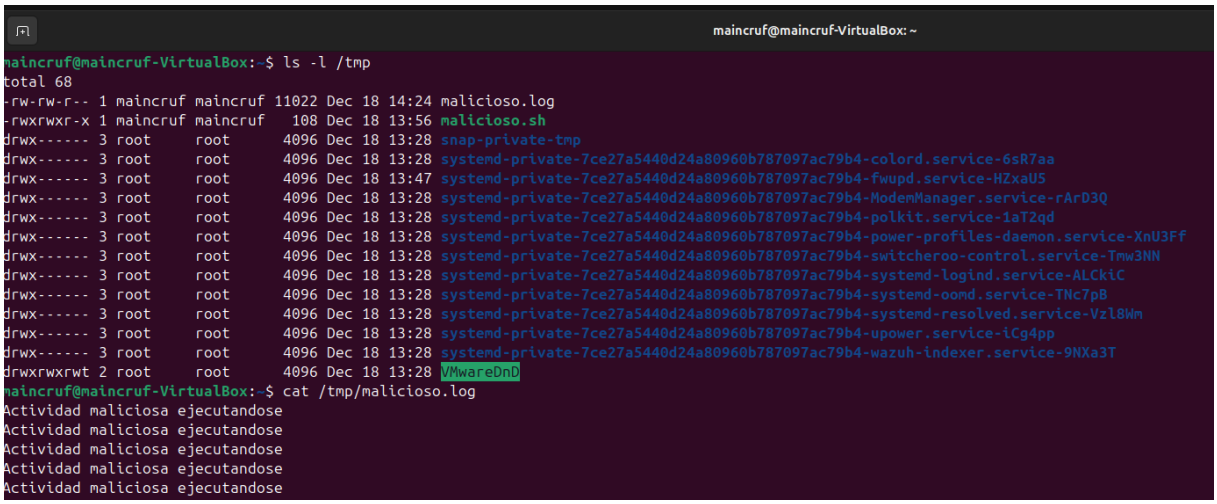

Figura 6. Identificación de archivo malicioso a través de la ruta de ejecución

4. Acciones recomendadas

Ante la detección de procesos sospechosos ejecutándose en segundo plano con persistencia en el sistema, se recomienda seguir las siguientes medidas:

- Aislar temporalmente el sistema de la red para evitar posible comunicación externa.
- Detener y eliminar el proceso malicioso identificado.
- Verificar conexiones de red activas asociadas al proceso.
- Calcular el hash del archivo malicioso y conservarlo para su análisis posterior.
- Revisar otros posibles archivos o usuarios comprometidos en el sistema.
- Cambiar credenciales si existe sospecha de compromiso.
- Realizar escaneo adicional del sistema para descartar otras amenazas.

5. Resultados obtenidos

En este laboratorio se utilizaron distintos comandos en Linux con el fin de identificar procesos y servicios tanto legítimos como sospechosos, así como los puertos vulnerables en el sistema. Mediante el análisis realizado, se logró diferenciar procesos y servicios normales de aquellos potencialmente maliciosos, por medio de una simulación de un proceso sospechoso. En conjunto, estas actividades permitieron conocer y aplicar medidas básicas de seguridad en entornos Linux y reforzar la comprensión sobre la importancia del monitoreo constante del sistema.

6. Reflexión final

Este laboratorio permitió comprender la importancia de diferenciar procesos y servicios comunes de los sospechosos, ya que estos últimos se ocultan haciéndose pasar por elementos legítimos del sistema. Además, se evidenció la relevancia de identificar puertos que se encuentran escuchando en todas las interfaces de red, así como aquellos pueden representar un riesgo de seguridad al permanecer habilitados sin alguna justificación. El análisis de procesos y servicios requiere tiempo y una gran dedicación con un trabajo detallado. No obstante, este esfuerzo es fundamental en el ámbito de la seguridad, donde identificar, investigar y emitir un veredicto sobre la legitimidad de un proceso resulta clave para mantener la seguridad y estabilidad del sistema.

Anexo A – Comandos Utilizados

```
ps aux

htop

systemctl list-units –type=service --state=running

netstat -tulnp

nano /tmp/malicioso.sh

chmod +x /tmp/malicioso.sh

/tmp/malicioso.sh &

ps aux | grep malicioso

top

ls -l /tmp

cat /tmp/maliciosos.log

pkill -f malicioso.sh
```