

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.

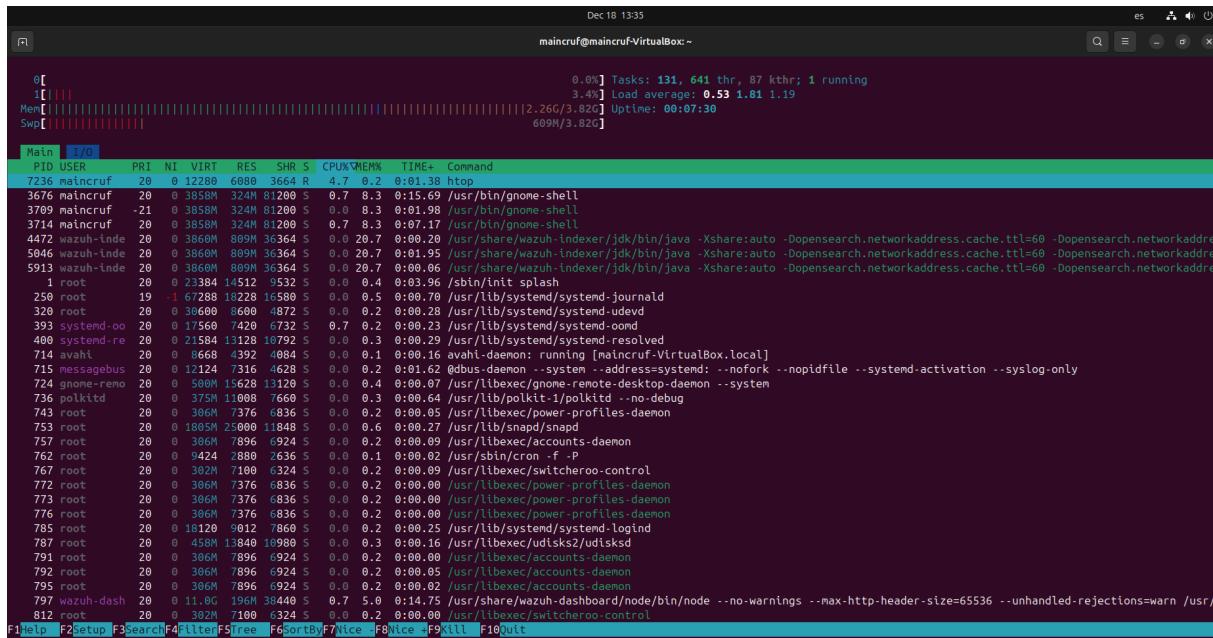


Figura 1. Procesos del sistema Linux en tiempo real

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.

```
maincruf@maincruf-VirtualBox:~$ systemctl list-units --type=service --state=running
UNIT          LOAD  ACTIVE SUB   DESCRIPTION
accounts-daemon.service loaded active running Accounts Service
avahi-daemon.service loaded active running Avahi mDNS/DNS-SD Stack
colorl.service loaded active running Manage, Install and Generate Color Profiles
cron.service loaded active running Regular background program processing daemon
cups-browsed.service loaded active running Make remote CUPS printers available locally
cups.service loaded active running CUPS Scheduler
dbus.service loaded active running D-Bus System Message Bus
filebeat.service loaded active running Filebeat sends log files to Logstash or directly to Elasticsearch.
gdm.service loaded active running GNOME Display Manager
gnome-remote-desktop.service loaded active running GNOME Remote Desktop
kerneloops.service loaded active running Tool to automatically collect and submit kernel crash signatures
ModemManager.service loaded active running Modem Manager
NetworkManager.service loaded active running Network Manager
polkit.service loaded active running Authorization Manager
power-profiles-daemon.service loaded active running Power Profiles daemon
rsyslog.service loaded active running System Logging Service
rtkit-daemon.service loaded active running RealtimeKit Scheduling Policy Service
snapd.service loaded active running Snap Daemon
switcheroo-control.service loaded active running switcheroo Control Proxy service
systemd-journal.service loaded active running Journal Service
systemd-logind.service loaded active running User Login Management
systemd-oond.service loaded active running Userspace Out-Of-Memory (OOM) Killer
systemd-resolved.service loaded active running Network Name Resolution
systemd-udevd.service loaded active running Rule-based Manager for Device Events and Files
udisks2.service loaded active running Disk Manager
unattended-upgrades.service loaded active running Unattended Upgrades Shutdown
upower.service loaded active running Daemon for power management
user@1000.service loaded active running User Manager for UID 1000
vboxadd-service.service loaded active running vboxadd-service.service
wazuh-dashboard.service loaded active running wazuh-dashboard
wazuh-indexer.service loaded active running wazuh-indexer
wazuh-manager.service loaded active running Wazuh manager
wpa_supplicant.service loaded active running WPA supplicant
```

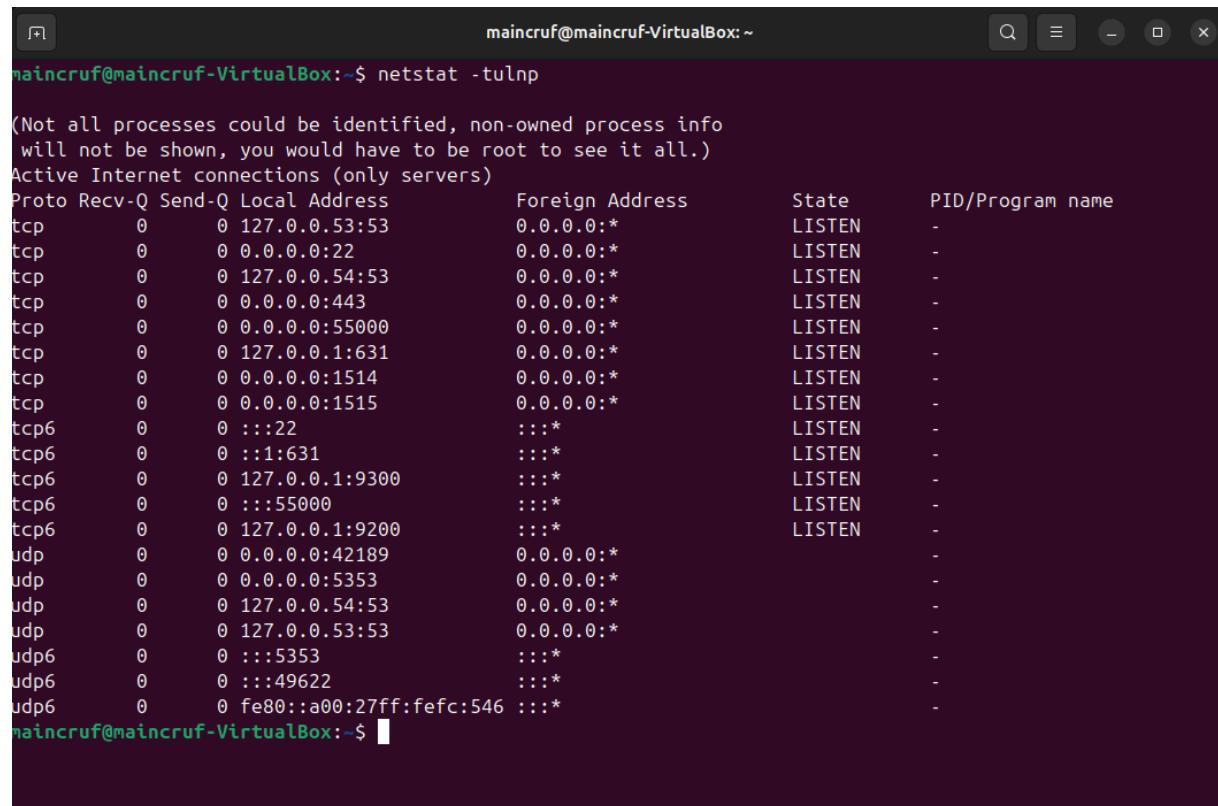
Figura 2. Servicios del sistema Linux.

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.



The terminal window shows the command `netstat -tulnp` being run by the user `maincruf` on a VirtualBox machine. The output lists active Internet connections (only servers) with columns for Proto, Recv-Q, Send-Q, Local Address, Foreign Address, State, and PID/Program name. The output shows numerous ports (e.g., 5353, 631, 9300, 55000, 49622) in LISTEN state, many of which are associated with the mDNS service.

```
maincruf@maincruf-VirtualBox:~$ netstat -tulnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp     0      0 127.0.0.53:53            0.0.0.0:*             LISTEN    
tcp     0      0 0.0.0.0:22              0.0.0.0:*             LISTEN    
tcp     0      0 127.0.0.54:53            0.0.0.0:*             LISTEN    
tcp     0      0 0.0.0.0:443             0.0.0.0:*             LISTEN    
tcp     0      0 0.0.0.0:55000           0.0.0.0:*             LISTEN    
tcp     0      0 127.0.0.1:631            0.0.0.0:*             LISTEN    
tcp     0      0 0.0.0.0:1514             0.0.0.0:*             LISTEN    
tcp     0      0 0.0.0.0:1515             0.0.0.0:*             LISTEN    
tcp6    0      0 :::22                  :::*                  LISTEN    
tcp6    0      0 ::1:631                :::*                  LISTEN    
tcp6    0      0 127.0.0.1:9300           :::*                  LISTEN    
tcp6    0      0 :::55000               :::*                  LISTEN    
tcp6    0      0 127.0.0.1:9200           :::*                  LISTEN    
udp     0      0 0.0.0.0:42189           0.0.0.0:*             -
udp     0      0 0.0.0.0:5353            0.0.0.0:*             -
udp     0      0 127.0.0.54:53            0.0.0.0:*             -
udp     0      0 127.0.0.53:53            0.0.0.0:*             -
udp6   0      0 :::5353                :::*                  -
udp6   0      0 :::49622               :::*                  -
udp6   0      0 fe80::a00:27ff:fefc:546  ::::*
```

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)

```
GNU nano 7.2                               maincruf@maincruf-VirtualBox: ~
#!/bin/bash

while true; do
    echo "Actividad maliciosa ejecutandose" >> /tmp/malicioso.log
    sleep 5
done
```

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)

```
Tasks: 133, 644 thr, 89 kthr; 2 running
Load average: 0.18 0.16 0.17
[2.67G/3.82G] Uptime: 00:54:39
296%[3.82G]

Main I/O
PID USER PRI NI VIRT RES SHR S CPU%SWREN% TIME+ Command
5254 maincruk 20 0 480M 28536 1624 5 0.0 0.7 0:00:00 /usr/bin/update-notifier
5268 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:37 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
5409 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:91 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
5410 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:91 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
5494 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:96 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
5495 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:93 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
5803 maincruk 20 0 617M 62324 48572 5 0.0 1.6 0:00:00 /usr/libexec/gnome-terminal-server
5828 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:31 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
5913 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:54 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
5916 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:57 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
5917 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:57 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
7056 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:00 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
7857 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:00 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
7237 wazuh-ind 20 0 3860M 1138M 36368 5 0.0 29.1 0:00:21 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.ttl=60
7288 maincruk 20 0 3986M 380M 87288 0 0.0 9.7 0:00:00 /usr/bin/gnome-shell
7387 root 20 0 541M 41380 35736 5 0.0 1.0 0:00:18 /usr/libexec/fwupd/fwupd
7400 root 20 0 541M 41380 35736 5 0.0 1.0 0:00:04 /usr/libexec/fwupd/fwupd
7406 root 20 0 541M 41380 35736 5 0.0 1.0 0:00:00 /usr/libexec/fwupd/fwupd
7407 root 20 0 541M 41380 35736 5 0.0 1.0 0:00:08 /usr/libexec/fwupd/fwupd
7408 root 20 0 541M 41380 35736 5 0.0 1.0 0:00:00 /usr/libexec/fwupd/fwupd
7410 root 20 0 541M 41380 35736 5 0.0 1.0 0:00:00 /usr/libexec/fwupd/fwupd
7603 maincruk 20 0 9940 3676 3484 5 0.0 0.1 0:00:21 /bin/bash /tmp/malicious.sh
7964 maincruk 20 0 2743M 64952 49966 5 0.0 1.6 0:00:52 qjs /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js -E -P /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js
7967 maincruk 20 0 2743M 64952 49966 5 0.0 1.6 0:00:00 qjs /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js -E -P /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js
7968 maincruk 20 0 2743M 64952 49966 5 0.0 1.6 0:00:00 qjs /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js -E -P /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js
7970 maincruk 20 0 2743M 64952 49966 5 0.0 1.6 0:00:02 qjs /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js -E -P /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js
7973 maincruk 20 0 2743M 64952 49966 5 0.0 1.6 0:00:09 qjs /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js -E -P /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js
7974 maincruk 20 0 2743M 64952 49966 5 0.0 1.6 0:00:00 qjs /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js -E -P /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js
7981 maincruk 20 0 2743M 64952 49966 5 0.0 1.6 0:00:00 qjs /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js -E -P /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js
7987 maincruk 20 0 2743M 64952 49966 5 0.0 1.6 0:00:01 qjs /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js -E -P /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js
8103 maincruk 20 0 8288 2100 1992 5 0.0 0.1 0:00:00 sleep 5
FakeLo F53t0n F3Sa7d F4l1t0n F6c5t0n B7t4F7t4 F9c5t0n F59 11_110ut
```

Figura 5. Análisis y detección de scripto 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.

```
maincruf@maincruf-VirtualBox:~$ ls -l /tmp
total 68
-rw-rw-r-- 1 maincruf maincruf 11022 Dec 18 14:24 malicioso.log
-rwxrwxr-x 1 maincruf maincruf 108 Dec 18 13:56 malicioso.sh
drwx----- 3 root      root    4096 Dec 18 13:28 snap-private-tmp
drwx----- 3 root      root    4096 Dec 18 13:28 systemd-private-7ce27a5440d24a80960b787097ac79b4-colord.service-6sR7aa
drwx----- 3 root      root    4096 Dec 18 13:47 systemd-private-7ce27a5440d24a80960b787097ac79b4-fwupd.service-HZxaU5
drwx----- 3 root      root    4096 Dec 18 13:28 systemd-private-7ce27a5440d24a80960b787097ac79b4-ModemManager.service-rArD3Q
drwx----- 3 root      root    4096 Dec 18 13:28 systemd-private-7ce27a5440d24a80960b787097ac79b4-polkit.service-1aT2qd
drwx----- 3 root      root    4096 Dec 18 13:28 systemd-private-7ce27a5440d24a80960b787097ac79b4-power-profiles-daemon.service-XnU3FF
drwx----- 3 root      root    4096 Dec 18 13:28 systemd-private-7ce27a5440d24a80960b787097ac79b4-switcheroo-control.service-Tmw3NN
drwx----- 3 root      root    4096 Dec 18 13:28 systemd-private-7ce27a5440d24a80960b787097ac79b4-systemd-logind.service-ALCktC
drwx----- 3 root      root    4096 Dec 18 13:28 systemd-private-7ce27a5440d24a80960b787097ac79b4-systemd-oomd.service-TNc7pB
drwx----- 3 root      root    4096 Dec 18 13:28 systemd-private-7ce27a5440d24a80960b787097ac79b4-systemd-resolved.service-Vzl8Wm
drwx----- 3 root      root    4096 Dec 18 13:28 systemd-private-7ce27a5440d24a80960b787097ac79b4-upower.service-iCg4pp
drwx----- 3 root      root    4096 Dec 18 13:28 systemd-private-7ce27a5440d24a80960b787097ac79b4-wazuh-indexer.service-9NXa3T
drwxrwxrwt 2 root      root    4096 Dec 18 13:28 VMwareDnD
maincruf@maincruf-VirtualBox:~$ cat /tmp/malicioso.log
Actividad maliciosa ejecutandose
```

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
```