

Alumno: José Lourido Plata

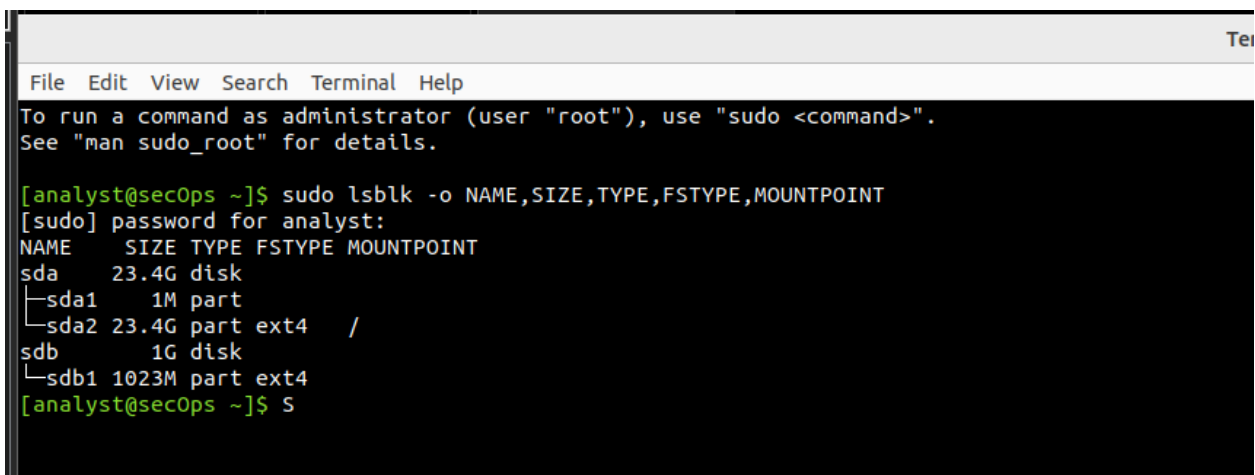
AYUDA A REALIZAR LA ACTIVIDAD 1 : ADMINISTRACIÓN BÁSICA LINUX

- Recurso: VM CyberOps Workstation
- Instrucciones: Entregar en la plataforma de Netacad un único documento en formato .pdf con una captura de pantalla y los comentarios correspondientes por cada uno de los puntos del enunciado.

Usando como la máquina virtual CyberOps Workstation del curso resolver las siguientes cuestiones:

1. ¿Qué tamaño tienen los dispositivos de bloques que referencian a particiones de los discos duros que tiene la máquina virtual CyberOps?

Se utilizan los comandos: lsblk o fdisk -l



```
File Edit View Search Terminal Help
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

[analyst@secOps ~]$ sudo lsblk -o NAME,SIZE,TYPE,FSTYPE,MOUNTPOINT
[sudo] password for analyst:
NAME        SIZE TYPE FSTYPE MOUNTPOINT
sda          23.4G disk
├─sda1        1M part
└─sda2 23.4G part ext4  /
sdb           1G disk
└─sdb1 1023M part ext4
```

Disco sda

Partición sda1 1MB

Partición sda2 23.4 GB

Disco sdb

Partición sdb1 1023M typo

```
[analyst@secOps ~]$ sudo fdisk -l
Disk /dev/sda: 23.44 GiB, 25165824000 bytes, 49152000 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 9C6E45E7-C049-4D5F-8D5E-8B1A593CF686

Device      Start      End  Sectors  Size Type
/dev/sda1    2048      4095     2048    1M BIOS boot
/dev/sda2    4096 49149951 49145856 23.4G Linux filesystem

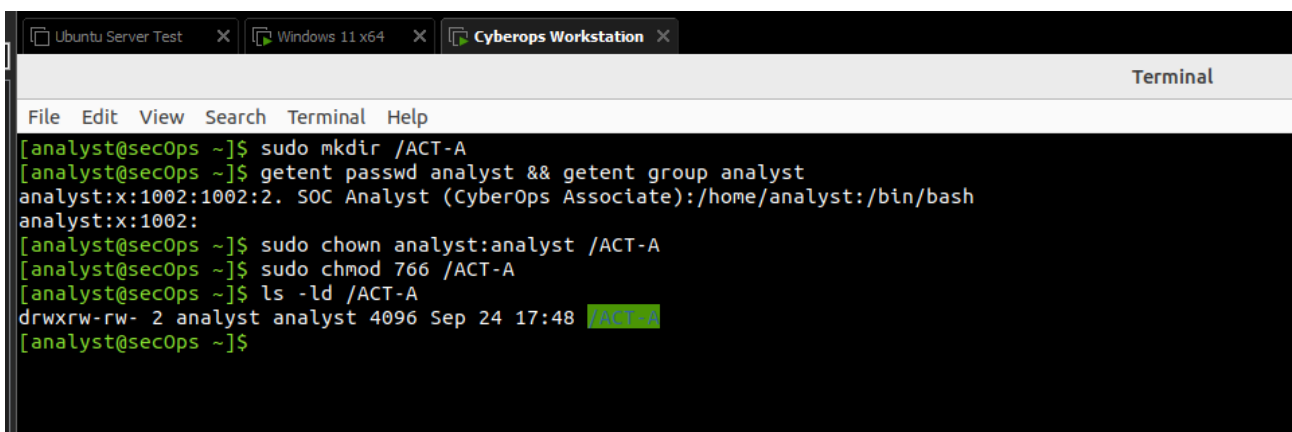
Disk /dev/sdb: 1 GiB, 1073741824 bytes, 2097152 sectors
Disk model: VMware Virtual S
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xe2894c0d

Device      Boot Start      End  Sectors  Size Id Type
/dev/sdb1                2048 2097151 2095104 1023M 83 Linux
[analyst@secOps ~]$
```

2. Crear el punto de montaje /ACT-A con los siguientes permisos:

- propietario: analyst
- grupo: analyst
- permisos:
 - propietario: rwx
 - grup: rw_
 - otros: rw_

NOTA: El directorio ACT-A ha de colgar de /



```
File Edit View Search Terminal Help
[analyst@secOps ~]$ sudo mkdir /ACT-A
[analyst@secOps ~]$ getent passwd analyst && getent group analyst
analyst:x:1002:1002:2. SOC Analyst (CyberOps Associate):/home/analyst:/bin/bash
analyst:x:1002:
[analyst@secOps ~]$ sudo chown analyst:analyst /ACT-A
[analyst@secOps ~]$ sudo chmod 766 /ACT-A
[analyst@secOps ~]$ ls -ld /ACT-A
drwxrw-rw- 2 analyst analyst 4096 Sep 24 17:48 /ACT-A
[analyst@secOps ~]$
```

Un punto de montaje no es más que una carpeta normal, donde se podrá mapear una unidad o volumen (como un disco) para poder acceder a sus contenidos a través de esa carpeta. Para crear una carpeta, usamos el comando `mkdir` seguido de la ruta y el nombre. Pero, dado que la vamos a crear en la raíz del sistema de archivos (/) necesitamos permisos de administrador con `sudo`.

Para cambiar el propietario, usamos el comando `chown` seguido del nombre de usuario y el archivo o carpeta. Para cambiar el grupo, se usa el comando `chgrp` junto con el nombre del grupo y la ruta.

Como la carpeta fue creada por el usuario administrador, este cambio de propietario debe hacerse con sudo.

En cuanto a los permisos, hay dos formas de asignarlos mediante el comando chmod:

- Simbólica o relativa: más intuitiva de entender, consiste en usar una combinación de 3 parámetros:
 - Clase de acceso: escogemos entre u (usuario), g (grupo) y o (otros).
 - Operador: escogemos entre + (añadir permisos), - (quitar permisos) y = (establecer permisos).
 - Tipo de acceso: escogemos entre r (lectura), w (escritura) y x (ejecución)

En un mismo comando se pueden dar los mismos permisos a distintas clases, y se pueden añadir unos permisos y quitar otros a la vez, pero no se puede dar distintos permisos a diferentes clases.

Por ejemplo, “ug+rw-x” añadiría permisos de lectura y escritura al usuario y al grupo, y quitaría el de ejecución. Este formato es más fácil de entender, pero puede requerir varias invocaciones para establecer muchos permisos.

- Absoluta: se especifica un número de 3 cifras, cada una en base octal (del 0 al 7). La primera cifra indica los permisos del usuario, la segunda los del grupo y la tercera los de otros. Cada cifra se obtiene sumando los posibles valores de 4 (lectura), 2 (escritura) y 1 (ejecución), siendo un 0 ningún permiso. Por ejemplo, “764” daría todos los permisos al usuario, los de lectura y escritura al grupo y sólo el de lectura a otros. Este formato es más difícil de entender, pero basta una única invocación para establecer todos los permisos.

Por tanto, las dos posibilidades que tenemos son:

chmod usuario=permsos

/carpeta o bien:

chmod xyz /carpeta, siendo x,y,z los permisos en octal de x para el propietario, y para el grupo, y z para otros.

3. Montar el dispositivo de bloques que referencia al segundo disco en el directorio

/ACT-A/ Usaremos en comando:

mount particion carpeta

```

[analyst@secOps ~]$ sudo lsblk -o NAME,SIZE,TYPE,MOUNTPOINT
NAME        SIZE TYPE MOUNTPOINT
sda         23.4G disk 
├─sda1       1M part 
├─sda2      23.4G part /
└─sdb         1G disk 
   └─sdb1    1023M part 
[analyst@secOps ~]$ ls -ld /ACT-A || sudo mkdir -p /ACT-A
drwxr-xr-x 2 analyst analyst 4096 Sep 24 17:48 /ACT-A
[analyst@secOps ~]$ ls -ld /ACT-A
drwxr-xr-x 2 analyst analyst 4096 Sep 24 17:48 /ACT-A
[analyst@secOps ~]$ sudo file -s /dev/sdb1
/dev/sdb1: Linux rev 1.0 ext4 filesystem data, UUID=fc8b15ef-bc63-4ff3-bb6c-bc2bf3b742ba (extents) (64bit) (large files) (huge files)
[analyst@secOps ~]$ sudo mount /dev/sdb1 /ACT-A
[analyst@secOps ~]$ findmnt /ACT-A
TARGET SOURCE      FSTYPE OPTIONS
/ACT-A /dev/sdb1 ext4    rw,relatime
[analyst@secOps ~]$ df -h /ACT-A
Filesystem      Size  Used Avail Use% Mounted on
/dev/sdb1       989M   28K  922M   1% /ACT-A
[analyst@secOps ~]$ s

```

4. Hacer una copia del fichero existente en /ACT-A/ con el nombre saludo.txt

```

[analyst@secOps ~]$ cd /ACT-A
[analyst@secOps ACT-A]$ pwd
/ACT-A
[analyst@secOps ACT-A]$ ls -la
total 28
drwxr-xr-x 3 root root 4096 May 4 2020 .
drwxr-xr-x 19 root root 4096 Sep 24 17:48 ..
drwx----- 2 root root 16384 Mar 26 2018 lost+found
-rw-rw-r-x 1 1000 root 188 May 19 2020 myFile.txt
[analyst@secOps ACT-A]$ cp myFile.txt saludo.txt
cp: cannot create regular file 'saludo.txt': Permission denied
[analyst@secOps ACT-A]$ sudo chown -R analyst:analyst /ACT-A
[analyst@secOps ACT-A]$ sudo chown -R 766 /ACT-A
[analyst@secOps ACT-A]$ cp myFile.txt saludo.txt
cp: cannot create regular file 'saludo.txt': Permission denied
[analyst@secOps ACT-A]$ chmod -R 766 /ACT-A
chmod: changing permissions of '/ACT-A': Operation not permitted
chmod: changing permissions of '/ACT-A/myFile.txt': Operation not permitted
chmod: changing permissions of '/ACT-A/lost+found': Operation not permitted
chmod: cannot read directory '/ACT-A/lost+found': Permission denied
[analyst@secOps ACT-A]$ cp myFile.txt saludo.txt
cp: cannot create regular file 'saludo.txt': Permission denied
[analyst@secOps ACT-A]$
[analyst@secOps ACT-A]$ ls -la
total 28
drwxr-xr-x 3 766 analyst 4096 May 4 2020 .
drwxr-xr-x 19 root root 4096 Sep 24 17:48 ..
drwx----- 2 766 analyst 16384 Mar 26 2018 lost+found
-rw-rw-r-x 1 766 analyst 188 May 19 2020 myFile.txt
[analyst@secOps ACT-A]$ sudo chown -R analyst:analyst /ACT-A
[analyst@secOps ACT-A]$ ls -la
total 28
drwxr-xr-x 3 analyst analyst 4096 May 4 2020 .
drwxr-xr-x 19 root root 4096 Sep 24 17:48 ..
drwx----- 2 analyst analyst 16384 Mar 26 2018 lost+found
-rw-rw-r-x 1 analyst analyst 188 May 19 2020 myFile.txt
[analyst@secOps ACT-A]$ sudo chmod -R 766 /ACT-A
[analyst@secOps ACT-A]$ cp myFile.txt saludo.txt
[analyst@secOps ACT-A]$ ls
lost+found myFile.txt saludo.txt
[analyst@secOps ACT-A]$ ^C
[analyst@secOps ACT-A]$

```

Nota: Se presento varios problemas (solventados) de permisos – por eso tan largo la captura

Desde la terminal, copiar archivos es tan fácil como usar el comando cp seguido de la ruta completa del origen y el destino. Para facilitar las operaciones, cambiaremos primero al directorio /ACT-A con el comando cd seguido de la ruta (y comprobaremos con pwd y ls que se ha hecho correctamente). De ese modo, ya no tendremos que dar la ruta absoluta cuando trabajemos con archivos dentro de ese directorio, bastará con el nombre.

Si intentamos copiar el archivo ahora mismo, nos encontraremos con un error: al montar una unidad, Linux toma los permisos del sistema de archivos, no de la carpeta donde ha sido montada. Si lo comprobamos ahora veremos que el usuario “root” (administrador) es ahora el dueño de /ACT-A y se han cambiado los permisos a “rwxr-xr-x”. Tendremos que volver a cambiar el propietario, grupo y permisos, usando además el switch -R (recursivo) para que se aplique a todo el contenido del dispositivo. Esto sólo será necesario hacerlo una vez, si volvemos a montar la unidad en un futuro, se recordarán los permisos.

5. Editar el fichero saludo.txt y hacer que sólo aparezca el mensaje "HOLA MUNDO" en el contenido del fichero

```

re Workstation
Help  [Icons]
Ubuntu Server Test x Windows 11 x64 x Cyberops Workstation x
Terminal
File Edit View Search Terminal Help
[analyst@secOps ACT-A]$ pwd
/ACT-A
[analyst@secOps ACT-A]$ echo "HOLA MUNDO" > saludo.txt
[analyst@secOps ACT-A]$ cat saludo.txt
HOLA MUNDO
[analyst@secOps ACT-A]$

```

Existen dos maneras de hacerlo desde la terminal: la larga sería abrir el .txt con un editor de texto (como por ejemplo vi, vim o nano), hacer los cambios y guardarlo (en nano, sería mediante CTRL+O e INTRO para guardar, y CTRL+X para salir del editor).

Sin embargo hay otra manera más corta y directa, y es usar el comando echo para imprimir “HOLA MUNDO”, y el operador de redirección >, que hace que la terminal tome la salida del último comando y, en vez de imprimirlo en pantalla, lo guarde en un archivo sobrescribiendo los datos anteriores (el operador >> agregaría el texto al contenido previo ya existente en el .txt, pegándolo al final, en vez de sustituirlo todo).

6. Cambiar el nombre del fichero saludo.txt a HOLA.txt

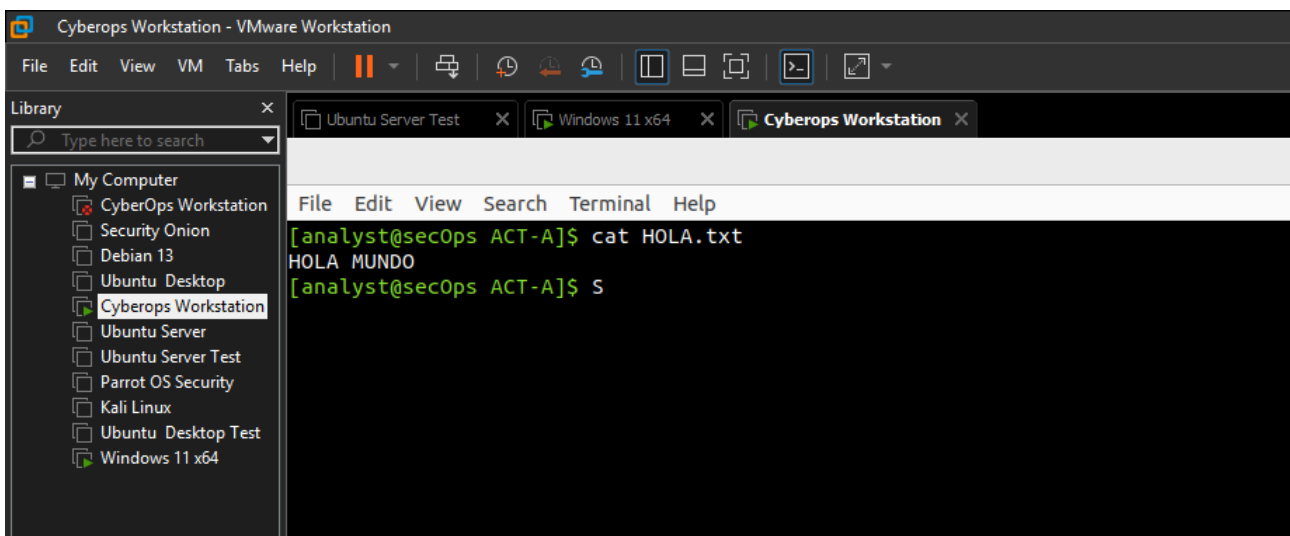
```

re Workstation
Help  [Icons]
Ubuntu Server Test x Windows 11 x64 x Cyberops Workstation x
Terminal
File Edit View Search Terminal Help
[analyst@secOps ACT-A]$ pwd
/ACT-A
[analyst@secOps ACT-A]$ mv saludo.txt HOLA.txt
[analyst@secOps ACT-A]$ ls -l
total 24
-rwxrw-r-- 1 analyst analyst  11 Sep 24 18:15 HOLA.txt
drwxrw-rw- 2 analyst analyst 16384 Mar 26 2018 lost+found
-rwxrw-rw- 1 analyst analyst  188 May 19 2020 myFile.txt
[analyst@secOps ACT-A]$ s

```

Como se ha visto en el punto 5 y el 6, el comando `cat` (concatenar) imprime en pantalla los contenidos de un archivo. La desventaja de este comando es que, si el fichero es muy largo, luego tendremos que desplazar la vista de la terminal para poder leerlo entero. Una alternativa mejor para estos archivos con mucho contenido es usar los comandos `more` o `less`, que no muestran más de una pantalla a la vez y permiten desplazarse con libertad por el contenido usando los cursores, la barra espaciadora, INTRO, retroceder y avanzar página, y Q para salir (“quit”). En este caso no es necesario pues HOLA.txt sólo tiene 1 línea.

7. Listar el contenido de HOLA.txt



```

Cyberops Workstation - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CyberOps Workstation
Security Onion
Debian 13
Ubuntu Desktop
Cyberops Workstation
Ubuntu Server
Ubuntu Server Test
Parrot OS Security
Kali Linux
Ubuntu Desktop Test
Windows 11 x64
File Edit View Search Terminal Help
[analyst@secOps ACT-A]$ cat HOLA.txt
HOLA MUNDO
[analyst@secOps ACT-A]$ s

```

Como se ha visto en el punto 5 y el 6, el comando **cat** (concatenar) imprime en pantalla los contenidos de un archivo. La desventaja de este comando es que, si el fichero es muy largo, luego tendremos que desplazar la vista de la terminal para poder leerlo entero. Una alternativa mejor para estos archivos con mucho contenido es usar los comandos `more` o `less`, que no muestran más de una pantalla a la vez y permiten desplazarse con libertad por el contenido usando los cursores, la barra espaciadora, INTRO, retroceder y avanzar página, y Q para salir (“quit”). En este caso no es necesario pues HOLA.txt sólo tiene 1 línea.

8. Comprobar si el servicio ssh está arrancado en el sistema para permitir el acceso en remoto a nuestro sistema.

Tenemos 2 formas de comprobar si el servicio de SSH (`sshd`, siendo la `d` por “daemon” o “demonio”, un proceso que se ejecuta de fondo y hacer sus tareas sin necesidad de entrada del usuario) está arrancado.

La primera es usar el comando `ps` para imprimir una lista de procesos en ejecución. Con los parámetros `a` (ver procesos de todos los usuarios), `u` (mostrar el usuario propietario de cada proceso) y `x` (mostrar también procesos que no se están ejecutando en una terminal), el comando nos imprimirá la lista completa, como el Administrador de tareas de Windows pero en texto. Para filtrar esta lista, usamos el comando `grep`, una herramienta muy útil de Linux que permite encontrar y mostrar lo que queremos en un archivo o salida de comando. Pidiéndole que busque el texto “`sshd`”, imprimirá sólo las líneas que contengan eso.

La segunda opción es, aprovechando que SSH es un servicio dado de alta en `systemd` (el sistema de gestión de servicios de Linux usado por distribuciones modernas), interrogar por su estado actual con la herramienta `systemctl` (control de `systemd`).

```

[analyst@secOps ACT-A]$ ps
  PID TTY          TIME CMD
 1919 pts/0    00:00:00 bash
 2130 pts/0    00:00:00 ps
[analyst@secOps ACT-A]$ ps aux | grep sshd
root      1202  0.0  0.1 15424  8736 ?        Ss   17:29   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
analyst   2132  0.0  0.0  6476  2324 pts/0    S+   18:22   0:00 grep sshd
[analyst@secOps ACT-A]$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-09-24 17:29:04 UTC; 54min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 1202 (sshd)
      Tasks: 1 (limit: 8809)
     Memory: 2.6M
        CPU: 22ms
    CGroup: /system.slice/ssh.service
            └─1202 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Warning: some journal files were not opened due to insufficient permissions.
[analyst@secOps ACT-A]$

```

9. Simular una acceso remoto, haciendo un ssh desde la máquina virtual hacia nuestra propia máquina virtual. Acceder con el usuario analyst. Mostrar el contenido del directorio /ACT-A

Tenemos 2 formas de comprobar si el servicio de SSH (sshd, siendo la d por “daemon” o “demonio”, un proceso que se ejecuta de fondo y hacer sus tareas sin necesidad de entrada del usuario) está arrancado.

La primera es usar el comando ps para imprimir una lista de procesos en ejecución. Con los parámetros a (ver procesos de todos los usuarios), u (mostrar el usuario propietario de cada proceso) y x (mostrar también procesos que no se están ejecutando en una terminal), el comando nos imprimirá la lista completa, como el Administrador de tareas de Windows pero en texto. Para filtrar esta lista, usamos el comando grep, una herramienta muy útil de Linux que permite encontrar y mostrar lo que queremos en un archivo o salida de comando. Pidiéndole que busque el texto “sshd”, imprimirá sólo las líneas que contengan eso.

La segunda opción es, aprovechando que SSH es un servicio dado de alta en systemd (el sistema de gestión de servicios de Linux usado por distribuciones modernas), interrogar por su estado actual con la herramienta systemctl (control de systemd).


```

File Edit View Search Terminal Help
[analyst@secOps ACT-A]$ ps
  PID TTY          TIME CMD
  1919 pts/0    00:00:00 bash
  2130 pts/0    00:00:00 ps
[analyst@secOps ACT-A]$ ps aux | grep sshd
root      1202  0.0  0.1 15424  8736 ?        Ss   17:29   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
analyst    2132  0.0  0.0  6476  2324 pts/0    S+   18:22   0:00 grep sshd
[analyst@secOps ACT-A]$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-09-24 17:29:04 UTC; 54min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 1202 (sshd)
     Tasks: 1 (limit: 8809)
    Memory: 2.6M
       CPU: 22ms
   CGroup: /system.slice/ssh.service
           └─1202 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Warning: some journal files were not opened due to insufficient permissions.
[analyst@secOps ACT-A]$ ssh analyst@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:criHpZzp2Yjg6kuEKXsugSKmDJxR3HUKUJAGSfOn8Yo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
analyst@localhost's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-60-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Sep 24 06:25:25 PM UTC 2025

System load:  0.0               Processes:    232
Usage of /:   34.6% of 22.9GB    Users logged in: 1
Memory usage: 6%               IPv4 address for ens32: 192.168.1.134
Swap usage:   0%

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

https://ubuntu.com/pro

```

135 updates can be applied immediately.
 73 of these updates are standard security updates.
 To see these additional updates run: `apt list --upgradable`

The list of available updates is more than a week old.
 To check for new updates run: `sudo apt update`

The programs included with the Ubuntu system are free software;
 the exact distribution terms for each program are described in the
 individual files in `/usr/share/doc/*/copyright`.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
 applicable law.

```

[analyst@secOps ~]$ ls -l /ACT-A
total 24
-rwxrwx-r-- 1 analyst analyst   11 Sep 24 18:15 HOLA.txt
drwxrwx-rw- 2 analyst analyst 16384 Mar 26 2018 Lost+Found
-rwxrwx-rw- 1 analyst analyst   188 May 19 2020 myFile.txt
[analyst@secOps ~]$

```