

Escenario

COVID19 Corporation © ha sufrido un ciberataque que, por fortuna, sólo ha afectado a uno de sus servidores, pero de tal manera que el único disco con el que contaba el servidor ha quedado completamente inutilizado perdiéndose de forma irreversible toda la información que contenía.

Todos te han felicitado por la contención del ataque (queda demostrado que eres un buen sysadmin en materia de ciberseguridad) pero antes de que alguien eche de menos el servidor *hackeado* te dispones a ponerlo en servicio con un plan muy sencillo: Envías a reciclar el disco perdido (no lo tiras a la basura, tienes conciencia ecologista), adquieres dos nuevos de altas prestaciones, los conectas a la máquina y restauras sobre uno de ellos el sistema completo tirando de la copia de seguridad que tienes y todos tan contentos.

La práctica

El plan lo va a materializar el alumno aplicando/usando tres cosas:

1. Las especificaciones indicadas más abajo.
2. El material indicado más abajo.
3. Los recursos lógicos con los que ya cuenta en el DS de prácticas anteriores.

Especificaciones Hardware del servidor perdido:

- Tamaño de la memoria RAM: 1024 Mb.
- Firmware de la placa base: BIOS
- Núcleos de CPU: 1
- Arquitectura del procesador: x86_64
- Interfaces de red Ethernet: 2
- Controladora de dispositivos de almacenamiento: 1
- Tipo de controladora de dispositivos de almacenamiento: SATA
- Puertos de la controladora de dispositivos de almacenamiento: 5
- No cuenta con controladora multimedia.
- No cuenta con puertos serie.
- Discos Duros: 2 (recién comprados)
- DVD/CDROM: 1

Especificaciones lógicas de funcionamiento del servidor perdido:

- El sistema operativo es Debian GNU/Linux.
- El servidor debe estar conectado a una "red NAT" junto con otros servidores que prestan servicio de forma aislada a un segmento departamental de **COVID19 Corporation** ©. El servidor perdido tenía mapeado el puerto 22 a través de la mencionada "red NAT" para atender peticiones `ssh`. Esta es la única puerta de entrada desde el exterior a la red departamental..... **¡ALUMNO! tienes un recurso lógico de otras prácticas que debes usar aquí.**

Especificaciones de normalización para evitar colisiones entre los alumnos:

- El nombre de servidor perdido se construye concatenando el literal fijo "sysr-" y el nombre del usuario del alumno en el DS.

systemrescue_p00

Ubicación de la copia de seguridad del sistema completo:

- En el directorio `$HOME/practicas/systemrescue/p00/` reside todo el material de la copia de seguridad del sistema completo (¡no te despistes! `$HOME` es una variable de entorno, no el nombre de un directorio).

Información de apoyo a la operatoria de la práctica:

- Los archivos contenidos en `$HOME/practicas/systemrescue/p00/` son el resultado de aplicar el comando `dd` a cada una de las particiones del único disco del sistema perdido.
- El disco perdido tenía una tabla de particiones de tipo "dos" pero aprovechando que tenemos discos nuevos y que BIOS es compatible con "gpt", los vamos a formatear con tabla de partición "gpt" y así nos vamos introduciendo en los nuevos estándares. Habrá que averiguar cómo nos llevamos las copias de seguridad procedentes de un disco "dos" a un disco "gpt".
- La palabra de paso del usuario `root` del sistema perdido es "palabra"
- El cargador de arranque del sistema perdido es `extlinux`. En la copia de seguridad del sistema completo contamos con todo el material que este cargador de arranque depositó en los directorios correspondientes (`/boot`, etc.), pero no tenemos el MBR del disco perdido. Por otra parte, tampoco nos serviría tenerlo ya que se ha decidido cambiar de tabla de partición "dos" a "gpt". [Este documento](#) que en su día guardaste en favoritos de tu navegador te puede dar luz sobre como acometer esta circunstancia.

El contenido del fichero `/etc/fstab` del sistema perdido es este:

```
# / was on /dev/sda1 during installation
UUID=ca052427-2706-47e1-8d51-ca69570c73e3 / ext4 errors=remount-ro 0 1
# /boot was on /dev/sda2 during installation
UUID=b116c831-6615-40ef-8f03-43a9ad704a1d /boot ext4 defaults 0 2
# /home was on /dev/sda5 during installation
UUID=05b502bb-9921-40fb-87aa-7c5f79558fd1 /home ext4 defaults 0 2
# /opt was on /dev/sda8 during installation
UUID=c9cb5ee1-faf1-4a01-9415-9a0ff7d9081d /opt ext4 defaults 0 2
# /srv was on /dev/sda7 during installation
UUID=cb8eb99b-d612-4d45-9bb1-b90f5e46fbe2 /srv ext4 defaults 0 2
# /usr was on /dev/sda10 during installation
UUID=029c1b8e-0a8e-4c74-899c-81a8ea99203c /usr ext4 defaults 0 2
# /usr/local was on /dev/sda9 during installation
UUID=82c78ef9-b8dd-4612-8705-eeee3f83421d /usr/local ext4 defaults 0 2
# /var was on /dev/sda6 during installation
UUID=e7e43cd6-5d3b-4d23-95f2-9358f1e9dd8c /var ext4 defaults 0 2
# swap was on /dev/sda11 during installation
UUID=55190b06-c8dd-4f93-97d2-9217627d25fe none swap sw 0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
```