



APUNTES 08

**CONFIGURACIÓN DE
DISPOSITIVOS PARA LA
INSTALACIÓN DE
SISTEMAS INFORMÁTICOS**

BASTIONADO DE REDES Y SISTEMAS

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

1. Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, otros.
 - 1.1. Control de configuración BIOS/UEFI.
 - 1.2. Secuencia de arranque.
 - 1.3. Puertos de conexión: Ethernet, Wifi, Bluetooth,...
2. Puertos de conexión: USB.
3. Seguridad en el arranque del sistema informático, configuración del arranque seguro.
4. Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.

Caso práctico

El CISO de la compañía ACME S.L. quiere que se investigue si los sistemas donde se guarda información sensible y crítica son seguros. Por lo que ha pedido que se revisen las medidas de seguridad relativas a estos sistemas poniendo el foco en aspectos tales como:

- Configuración segura de la BIOS/UEFI.
- Riesgos asociados a los puertos de conexión y los puertos en los que se pueden conectar dispositivos para el intercambio de información u otros periféricos.
- Seguridad de los sistemas de ficheros: SUID de los ficheros, permisos de directorios, compartición de directorios,...

Objetivos:

En este módulo estudiaremos la importancia de preparar los equipos con los elementos que provee el fabricante.

Configurando de manera segura la BIOS/UEFI, y todos los riesgos asociados a los puertos de conexión y los puertos en los que se pueden conectar dispositivos para el intercambio de información u otros periféricos.

Mostraremos los aspectos de seguridad en el proceso de arranque del sistema, configurando el arranque seguro del mismo y aquellos medios que permiten vigilar el arranque y los cambios de configuración del mismo.

Finalizamos el módulo con la configuración segura de los sistemas de ficheros, particiones y la manera de establecer el cifrado en reposo para la información, sobre todo si el dispositivo está destinado a albergar información sensible.

1.- PRECAUCIONES PREVIAS A LA INSTALACIÓN DE UN SISTEMA INFORMÁTICO: AISLAMIENTO, CONFIGURACIÓN DEL CONTROL DE ACCESO A LA BIOS, BLOQUEO DEL ORDEN DE ARRANQUE DE LOS DISPOSITIVOS, OTROS.

Caso práctico

En la oficina de Mario algunos trabajadores se tienen que quedar más tiempo en la oficina para acabar el proyecto en el que están inmersos. La pasada semana aparecieron en Internet documentos confidenciales que estaban en su ordenador personal. Nadie sabe qué ha podido pasar ya que la política de la empresa tiene contraseñas robustas de acceso al dominio y los USB están deshabilitados para que no pueda haber fugas de información ni infecciones por malware por la utilización de USBs personales que los trabajadores pueden conectar a los ordenadores.

La empresa decide contratar a un consultor para que analice el ordenador de Mario y ver si tiene algún virus, pero no han encontrado software malicioso. Por lo que deciden analizar cada uno de los parámetros de configuración del PC y se dan cuenta que el acceso a la BIOS no dispone de contraseña. ¿Pudo ser el vector de entrada?

Protege la BIOS: El acceso a la BIOS permite habilitar 2 opciones que permitió a un compañero de Mario habilitar los USB y cambiar la secuencia de arranque del equipo, para que lo hiciera desde un USB y a partir de ahí acceder a la información del disco duro, que no estaba cifrada.

La protección de los dispositivos que van a formar parte de los sistemas también constituye un elemento de protección de cara al bastionado de los sistemas. La normativa relativa a los requisitos de seguridad de los sistemas (CCN-STIC, ENS, NIST) indica que es necesario llevar a cabo una configuración segura de la BIOS bajo los siguientes criterios:

- Mínima funcionalidad
- Acceso por contraseña
- Se activará el arranque seguro
- Actualización del firmware
- Comprobación de la integridad de firmware
- Revisión del proceso de arranque
- Revisión de los dispositivos conectados (puertos)

Analizando los elementos propios de los sistemas, habrá que tener en cuenta la configuración segura de los siguientes elementos de los equipos:

- Control de configuración de BIOS y UEFI
- Orden de arranque.
- Puertos de conexión: Bluetooth, wifi, NFC, ...
- Dispositivos de almacenamiento: USB, CD-ROM, tarjetas,...

Esta configuración está asociada al fabricante de los equipos. La mayoría de las recomendaciones y posibilidades de configuración desde el punto de vista de la seguridad vienen determinadas por sus manuales de usuario. Cada vez más fabricantes crean apartados específicos de configuración relativas a la seguridad.

Ya se han detectado ataques a las infraestructuras ligados a la cadena de suministro de equipos que venía infectados desde el fabricante. Este es el motivo por el que los riesgos en la cadena de suministros se han elevado, ya que es necesario aumentar esa confianza entre el cliente y el proveedor de los dispositivos que van a formar parte de las redes. En algunos casos como el de redes clasificadas oficiales, los productos que forma parte de la red tienen que estar dentro del catálogo de productos acreditados que pasan una serie de controles y auditorías.

El CCN tiene publicado su catálogo de productos a través de su guía CCN-STIC 105.

Lo que se busca es tener productos en origen seguros desde el diseño y asegurar todo el ciclo de vida de los productos desde su inicio. En el siguiente enlace se puede ver una guía de referencia de certificación de productos basado en la metodología de certificación española de productos LINCE.

Otra referencia que hace mención a la utilización de productos seguros en las redes es el Esquema Nacional de Seguridad en su versión de Mayo de 2022.

1.1.- CONTROL DE CONFIGURACIÓN BIOS/UEFI.

La UEFI o BIOS(Basic Input/Output System) es el primer software que se ejecuta al arrancar el equipo, por lo que ya ha sido objetivo de atacantes, ya que la infección de este software aumenta el nivel de la persistencia en el sistema y la dificultad de detección. Por lo que es uno de los softwares críticos que debemos tener en cuenta en el plan de actualizaciones.

La BIOS suele estar desarrollada por el fabricante del equipo (original equipment manufacturer - OEM). Por lo que son ellos los que deben proporcionar el software original y sus actualizaciones.

El software UEFI (Unified Extensible Firmware Interface) surgió posteriormente, añadiendo nueva funcionalidades a BIOS como proporcionar acceso remoto, lo que abre un nuevo vector de ataque en el arranque del sistema. UEFI se define como una versión más moderna y segura, pero si la configuración se deja por defecto no será tan segura.

Suele estar guardado en memorias específicas: CMOS, EEPROM, ROM, Flash... por lo que su configuración permanece almacenada mientras exista una fuente de alimentación conectada, por ejemplo a través de una pila. Por lo que puede ser borrado quitando la pila o activado algún mecanismo que deje el sistema sin alimentación. Esto permite eliminar las modificaciones realizadas en la configuración de la BIOS, si se diera el caso que tuviéramos que resetear la configuración a valores de fábrica por algún error en la configuración u olvido de contraseña.

Este tipo de software también puede estar presente en tarjeta gráficas, controladores de tarjetas de red,...

La actualización de la BIOS vendrá marcada por el método que establezca el fabricante. Algunas de las actualizaciones de este firmware se realizará desde sistema ópticos, USB,...

La BIOS/UEFI realiza el proceso de inicio y carga de software:

- Comprobación del Hardware del equipo
- Iniciación del Hardware
- Inicio del sistema operativo.

Debido al impacto que tiene la BIOS en el arranque de los sistemas, se debe establecer el control de la configuración de la BIOS /UEFI a través de contraseña, para tener controlado el acceso a los cambios de configuración. Además, se debe establecer un procedimiento operativo que permita el cambio de configuración de cualquier elemento de la BIOS. Al no existir un control de usuarios, la contraseña debe ser custodiada y actualizada según los procedimientos de seguridad de la organización.

Para más información acerca de los ataques más comunes a las EUFI.

Además, es necesario considerar que las empresas proveedoras de software de UEFI tenga un plan de actualización y mitigación de vulnerabilidades y una metodología de desarrollo basado en la seguridad desde el desarrollo (security by-design).

Los organismos internacionales han publicado guías de configuración segura de este software:

- Guía NIST de protección de BIOS
- Guía NIST de protección de BIOS de servidores.

Entre los procedimientos de autenticación segura del EUFI y BIOS está el mecanismo de actualización protegido por contraseña, no permitiendo la realización de actualización remota o sólo desde dispositivos controlados. En caso de permitirlo, sería necesario monitorizar y controlar con los dispositivos de seguridad (firewalls) las conexiones que permiten la actualización de estos dispositivos, y sólo desde las redes internas.

El no disponer de control de acceso a la BIOS/UEFI permitirá a un usuario no deseado cambiar:

1. Secuencia de arranque
2. Habilitar puertos y dispositivos de comunicación: bluetooth, wifi, nfc
3. Solicitud de contraseña con cada arranque del sistema

Recordar que es posible resetear la configuración por defecto de BIOS dejando sin energía a la memoria que almacena la configuración (CMOS) a través de una batería o pila que está dentro de placa. Este mecanismo requiere de acceso físico al equipo, por lo que se deberían establecer si se considera medidas de protección física de los dispositivos, con pegatinas anti tamper para comprobar que los dispositivos no han sido manipulados. En caso de detectar la manipulación, es necesario activar el procedimiento de cambio de contraseña de la BIOS.

Ilustración que muestra varias etiquetas antitampering

Hay dos métodos que pueden mitigar la infección de la BIOS, instalar la BIOS sin permisos de escritura y verificar su integridad en cada proceso de arranque.

La descarga del software de actualización de la BIOS sólo se debe realizar desde las páginas oficiales del fabricante. Es necesario controlar la integridad del software descargado y mantenerlo actualizado. Existen proyectos de software sobre la UEFI que incluyen la seguridad como uno de los aspectos a tener en cuenta. Es una manera de tener el control del código de la BIOS pero que necesita de mantenimiento, actualización y configuración con personal propio o con apoyo de la comunidad. Los dos proyectos más destacados son:

- <https://libreboot.org/>
- <https://www.coreboot.org/>

1.2.- SECUENCIA DE ARRANQUE.

La modificación de la secuencia de arranque permitirá iniciar el equipo con otro sistema operativo, que podrá tener acceso a los ficheros del sistema. Lo métodos más comunes del cambio de secuencia de arranque es cambiando la

configuración en la BIOS y utilizar un dispositivo externo con un arranque desde un sistema operativo que no tenga medidas de seguridad ni sea controlado por los administradores del sistema.

La forma más efectiva es deshabilitar los dispositivos externos o controlar la entrada y salida de información a través de puntos controlados en la red que se denominen ordenadores frontera o aduana.

El objetivo de este control de la configuración es impedir que la secuencia de arranque de los sistemas no sea manipulada por los usuarios sin control.

Existen varias herramientas para crear USBs de arranque, entre ellas está Rufus.

1.3. PUERTOS DE CONEXIÓN: ETHERNET, WIFI, BLUETOOTH,...

Minimizar los riesgos de conexiones incontroladas en los equipos, pasa por evitar las conexiones a redes wifi que no estén controladas por la organización (públicas, acceso libre, ...), dispositivos bluetooth, o conexiones a redes cableadas de otros sistemas.

Únicamente serán permitidas conexiones hacia puntos Wifi o de Ethernet de confianza, estableciendo una conexión VPN contra la organización, cuando esta se produzca desde fuera de las instalaciones (teletrabajo, viajes,...).

La organización permitirá únicamente estas 2 vías de conexión:

- Dispositivos controlados
- Conexiones a redes públicas protegidas por mecanismos de protección de la información a través de túneles VPN como extensión de su red.

Los dispositivos controlados son aquellos dispositivos que han sido configurados acorde a las políticas y normas de seguridad de la organización. Esto abarca todo tipo de conexiones: wifi, ethernet y bluetooth... y en caso de que los usuarios puedan establecer configuraciones hacia cualquier punto de acceso lo utilicen como vía de comunicación protegida por un túnel (VPN, HTTPS,...). De tal manera que no puedan realizar conexiones sin restricciones para por ejemplo poder navegar libremente, ... Estas medidas de seguridad deben ser implementadas de cara a tener un control de las conexiones, o minimizadas con la vigilancia y la respuesta rápida ante incidentes de seguridad.

Algunos fabricantes disponen de simuladores de BIOS en sus páginas web, como por ejemplo el fabricante de Lenovo. Lo que permite a los usuarios familiarizarse con las BIOS.

1.4.- PUERTOS DE CONEXIÓN: USB.

La conexión de dispositivos externos al equipo como norma general deben ser deshabilitados, ya que constituyen un elemento incontrolado de entrada y salida de información y por lo tanto de riesgos de infección y exfiltración de la información.

Algunas estaciones deben tener habilitada estos dispositivos por motivos de funcionalidad como la conexión de dispositivos periféricos. En este caso la instalación de los drivers del dispositivo tiene que estar controlado a través de restricción de permisos de administrador. Serán los administradores los que realizarán la instalación de los drivers y el control de las listas de dispositivos permitidos.

No permitiéndose la conexión de dispositivos de manera incontrolada. Dichos dispositivos de intercambio (USB) deberán estar registrados como activos del sistema con un identificador único.

Entre los dispositivos que pueden constituir una amenaza para los sistemas, existen dispositivos específicos que permitirían una puerta de entrada al sistema, o de recopilación crítica.

- Rubber Ducky
- LAN Turtle
- Yard Stick One
- Key Logger
- USB Killer

Existen herramientas que permiten la gestión y control de los dispositivos conectados a los equipos mediante listas blancas, así como los ataques físicos a los equipos a los que se conecta el dispositivo.

Todos estos riesgos relativos a la utilización de dispositivos USB son elementos a considerar desde el punto de vista de la seguridad. Y se debe establecer en que equipos específicos se pueden utilizar. Una opción es utilizarlos sólo en equipo aislados de la red que cumplen las funciones de equipo de análisis de dispositivos USB, eliminando los riesgos a tener los USB activos en todos los equipos de la organización aumentando la probabilidad de:

- Infección
- Fuga de información
- Accesos remotos no controlados,...

Los equipos aislados que tenga como finalizada el intercambio de información a través de USB con los equipos de la red, utilizan el procedimiento de intercambio de información a través del medio que comúnmente se denomina air-gap. Aunque existen otros medios de intercambio de información entre dominios con diferentes grados de seguridad en el tratamiento de la información, como pueden ser pasarelas o diodos. Estos mecanismos son los se denominan dispositivos de protección de perímetro (DPP).

Estos procedimientos de seguridad minimizan los riesgos, pero no los eliminan al 100%, como sucedió con el famoso incidente de Stuxnet.

En estos dispositivos es necesario establecer procedimientos operativos de seguridad para la utilización de los dispositivos externos como USB en ciertas tareas como: actualizaciones del sistema operativo, actualizaciones de software de seguridad como las firmas del antivirus, ...

2.- SEGURIDAD EN EL ARRANQUE DEL SISTEMA INFORMÁTICO, CONFIGURACIÓN DEL ARRANQUE SEGURO

Caso práctico

Los administradores del sistema de la Universidad de Castilla-La Mancha utilizan PXE para facilitar la instalación de las imágenes de Windows a través de la red. Esto lleva asociado un servidor (WDS) que procesa las solicitudes y envía la imagen al equipo para instalarla.

Existen procesos asociados a la instalación de la imagen por PXE como son: DHCP, TFTP. Cuando los ficheros son transferidos al equipo comienza la instalación.

Lo importante es conocer los detalles de funcionamiento de PXE para saber cómo se puede explotar y que valores necesitamos configurar para que este proceso no suponga un riesgo.

PXE Seguro: Al utilizar el servicio TFTP para servir las imágenes se debería establecer una contraseña para no poder manipular los ficheros del servidor TFTP y subir una imagen manipulada conteniendo malware o un script que realice la conexión contra un servidor de control remoto.

También sería de utilidad analizar los ficheros que intercambia para automatizar la instalación, para saber si existen contraseñas en claro en esos ficheros y eliminarlas.

Para realizar un control sobre el arranque seguro del sistema operativo debemos conocer cómo se realiza un inicio normal de nuestro sistema operativo, para poder detectar cualquier anomalía que se produzca durante el arranque.

Debemos además tener en cuenta las amenazas de malware de rootkit que se instalan en el arranque del sistema que son difíciles de detectar y que provocan que muchas de las herramientas de seguridad no funcionen ante este tipo de amenazas.

Una de las labores de seguridad relativas al inicio del sistema, es realizar un análisis de la jerarquía de procesos que se ejecutan en Windows con el objetivo de poder determinar y analizar los posibles ataques en el inicio de un sistema operativo. En este caso de Windows este análisis nos ayudará a determinar si los atacantes se encuentran en la fase de persistencia en su Kill-Chain.

Estas son las medidas de seguridad que debemos establecer en el arranque:

- Comprobación de la integridad del sistema.
- Envío de logs de arranque al SOC para su análisis.

Existen herramientas que permiten controlar el arranque de los equipos. Para los sistemas operativos de Linux se pueden utilizar las siguientes herramientas:

- AppArmor
- SELinux

Para un análisis seguro de un equipo se puede utilizar un arranque con un dispositivo externo (liveCD o liveDVD) que permita la ejecución de un sistema operativo certificado y configurado de manera segura. De tal manera que podemos partir de un modo seguro para analizar el equipo. Aunque esta medida tiene que estar controlada solo para casos de análisis de equipos o equipos que tengan una funcionalidad específica y queremos que el equipo permanezca inmutable.

También es importante proteger el arranque por PXE. En el siguiente enlace se puede ver una forma de atacar un equipo redirigiendo el arranque PXE hacia un servidor malicioso. Este procedimiento de instalación y arranque de sistemas suele tener contraseñas guardadas en ficheros de scripts que están en claro. Es necesario proteger estas contraseñas en claro.

En el siguiente enlace se muestran algunos modos de arranque seguro para diagnosticar el sistema.

Los gestores de arranque también presentan vulnerabilidades, por lo que es necesario realizar la actualización de este software. Los gestores de arranque deben tener configurado la contraseña para el acceder a la configuración y poder cambiarla. Como es el caso del gestor de arranque del grub.

3.- SEGURIDAD DE LOS SISTEMAS DE FICHEROS, CIFRADO, PARTICIONADO, ENTRE OTROS.

Caso práctico

Los comerciales de la empresa de Ricardo, viajan por toda Europa y muchas veces tienen que llevar el portátil a todos lados. El riesgo de robo del portátil es alto porque un pequeño descuido, dejarlo en el hotel encima de la cama, olvidarlo en una cafetería,...puede suponer que desaparezca. Pero a veces es inevitable.

El portátil es algo material que supone un coste para la empresa, pero tiene más valor la información. Así que tenemos que ponerle una capa de protección a esa información y aunque el portátil se vea expuesto a sustracción. Hay que intentar que se lleven una caja fuerte, pero sin la llave.

Protege la información: Los usuarios deberían alojar la información en los servicios de ficheros corporativos y no en sus equipos personales. Pero a veces no es posible y por eso debemos aplicar mecanismos de cifrado de la información en reposo. Por si se diera el caso de que tuvieran acceso físico al disco duro la información esté cifrada y protegida por una contraseña robusta y que no permita extraer la información. Esto se deberá aplicar también a dispositivos como USBs, discos duros externos, etc.

Los sistemas son importantes por la información que almacenan. Ya que el sistema en sí sólo soporta los mecanismos necesarios para el tratamiento de la información. Por lo que debemos proteger o proporcionar al sistema de los mecanismos de protección del dato.

Entre los mecanismos de protección está el cifrado de la información, que es la medida de seguridad que en caso de robo de la información permite proteger la información y que esta no sea utilizada por personas que no deberían tener acceso a ella y que puedan perjudicar a la organización o ser utilizadas con otros fines para las que fueron creadas. Esta información debería ser cifrada en todos los niveles del sistema, tanto a nivel de sistema de ficheros, como de los dispositivos extraíbles: USB, memorystick, CD, DVD, También deben aplicarse estos mecanismos de protección para la información almacenada en la nube.

Uno de los mecanismos más utilizados por Windows es el cifrado de información a través de BitLocker. Para los sistemas Linux existe el cifrado a través de la herramienta gpg, teniendo los modos de clave simétrica y asimétrica. También dentro del ciclo de vida de la información está el borrado seguro de la misma, de tal manera que no pueda ser recuperada por métodos forenses y que permita recuperar la información. Estas son algunas de las referencias a herramientas de borrado seguro:

- Herramientas de borrado seguro de INCIBE.
- Olvido Herramienta de Borrado Seguro de CCN.

Los mecanismos de borrado seguro de la información deberá estar aplicado a todos los dispositivos: ordenadores, portátiles, servidores, discos duros, USB, móviles,...

Los usuarios deben estar concienciados de no almacenar la información en sus dispositivos locales, sino que se deben almacenar en servidores de ficheros, bases de datos, ... que tengan un bastionado de la información y del sistema. Ya que dichos servicios se pueden proteger con otro nivel adicional de seguridad y se centrarían los esfuerzos en generar una protección adicional sobre el servicio. Además de que estos servicios estarán protegidos por el plan de recuperación ante desastres o por incidentes de seguridad como el Ransomware como son las copias de seguridad.

Existe una tendencia a la utilización de sistemas virtualizados con el despliegue de las máquinas virtuales (VDI/VGI) en el momento que el usuario solicita el despliegue de su máquina mediante sistemas de virtualización. Y una vez que el usuario deja de utilizar el sistema la información se borrará del equipo, esto permite proteger la información ante el robo de dispositivos. Además, las tecnologías de comunicaciones actuales con anchos de banda altos nos permiten obtener esa información de una manera rápida sin necesidad de disponer de un equipo potente.

El particionado del sistema de archivos se realizará según la funcionalidad del sistema. Esto permitirá asignar permisos a cada una de las particiones para proporcionar el mínimo privilegio a cada una de ellas. Estableciendo permisos por particiones así como la gestión de permisos de los ficheros que se alojan en las particiones.

La elección de cada uno de los sistemas de archivos estará relacionada con las características que proporcionen cada uno de los sistemas de archivos.

Para sistemas operativos Linux se indican algunos de los modificadores del fichero de configuración de las particiones (/etc/fstab) y sus características de montaje inicial asociadas al sistema de ficheros:

- noauto: montaje automático.
- noexec: no admitirá la ejecución de ficheros.
- nodev: no admitirá la instalación de dispositivos.
- Permisos: permisos de solo lectura(ro) y lectura y escritura (rw).
- defaults: opciones para esta configuración (rw, suid, dev, exec, auto, nouser, async)

Además, se deberá proteger aquellas particiones que alberguen información de los usuarios y configuraciones del sistema, para que en caso de recuperación del sistema se haga de una manera rápida y eficaz. A continuación, se indica la guía de referencia del CCN relativo al bastionado de sistemas Linux con la configuración de las particiones (la guía tiene una errata en el epígrafe 6.2.4.1. donde dice default debe decir defaults).

Respuesta

Autoevaluación I: a)

Autoevaluación II: b)

Autoevaluación III: a)

TEST I: 1a), 2b), 3c), 4b), 5c), 6c), 7b), 8b), 9b), 10a)

TEST II: 1c), 2a), 3a), 4b), 5c), 6c), 7a), 8b), 9a), 10b)

Autoevaluación I

¿Es necesario actualizar el software de la BIOS?

- a) Verdadero
- b) Falso

Autoevaluación II

Tener el Bluetooth activado en los equipos para que los usuarios conecten sus dispositivos inalámbricos de audio no supone un riesgo.

- a) Verdadero
- b) Falso

Autoevaluación III

¿Qué es el air-gap?

- a) Mecanismo para tempetizar los equipos
- b) Un nuevo malware
- c) Mecanismo para intercambiar información entre dos equipos aislados a través de un dispositivo externo: USB key, disco duro portátil, CD, ...

TEST I

1. Por defecto y atendiéndonos a los principios de seguridad el CDROM debería estar desactivado en la BIOS.

¿Verdadero o falso?

- a. Verdadero
- b. Falso

2. ¿Cuál de los siguientes no es un riesgo de tener los USB activados?

- a. Eleva el riesgo de fuga de información y de infección
- b. Aumenta la concienciación de los usuarios
- c. Permite conectar dispositivos "rogue" para captura de información, líneas de conexión no controladas, despliegue de malware,...

3. Desde el punto de vista de la seguridad, el particionado del disco duro nos permite

- a. No será necesario actualizar el sistema tan frecuentemente
- b. Tener más organizado el disco duro
- c. Proteger la información más sensible

4. Cual de lo siguientes es el puerto que menos riesgo tiene dejar habilitado en un equipo a través de la BIOS:

- a. Bluetooth
- b. Audio
- c. USB

5. En los sistema linux, ¿qué mecanismo nos permite proteger la secuencia de arranque?:

- a. Ansible
- b. Network Deception
- c. GRUB

6. ¿Qué parámetro de la configuración de particiones de Linux en /etc/fstab permite protege al sistema de la ejecución de ficheros en dicha partición?.

- a. nodev
- b. default
- c. noexec

7. ¿Es seguro habilitar por defecto las nuevas funcionalidades de actualización remota de la UEFI? ¿Verdadero o falso?

- a. Verdadero
- b. Falso

8. Qué tecnología nos proporciona el acceso más segura al sistema de manera remota sin que la información tenga que almacenarse en el dispositivo desde el que nos conectamos.

- a. Telnet
- b. VDI/VGI
- c. RDP

9. ¿Qué mecanismo de seguridad permite proteger el acceso la BIOS?

- a. Cambiar la secuencia de arranque
- b. Contraseña
- c. Actualizarla

10. La comprobación de integridad de la nueva versión de la BIOS nos asegura:

- a. Autenticidad del software por parte del fabricante
- b. Que no tiene vulnerabilidades
- c. La correcta funcionalidad

TEST II

1. ¿Cómo se denomina el modo de arranque del sistema que nos permite realizar un diagnóstico de un problema?
 - a. Arranque antihacking
 - b. Arranque TOR
 - c. Arranque seguro
2. El método de intercambio de ficheros entre dos equipos a través de un dispositivo externo se denomina:
 - a. Air Gap
 - b. Hand Disk
 - c. USB transporting
3. El Bluetooth activado constituye un riesgo para la fuga de información del sistema. ¿Verdadero o falso?
 - a. Verdadero
 - b. Falso
4. Qué herramienta de Windows permite el cifrado de la información del sistema de archivos:
 - a. CipherWin
 - b. BitLocker
 - c. AppLocker
5. Por qué se ha tenido en consideración la utilización de productos ciberseguros acreditados
 - a. Por el continuo negocio de las blockchain
 - b. El alto coste que tienen los productos de software libre
 - c. Ataques a la cadena de suministros
6. ¿Qué debemos monitorizar en el arranque del sistema?
 - a. Consumo de disco
 - b. Número de usuarios
 - c. Jerarquía de procesos
7. ¿Qué tipo de malware se instala en el arranque del sistema:
 - a. rootkit
 - b. adware
 - c. spoofing
8. La descarga de la actualización firmware de BIOS/UEFI se debe hacer desde:
 - a. La página que aglutina más software relativo a BIOS/UEFI.
 - b. Página oficial del fabricante.
 - c. Página web del Ministerio de Industria.
9. ¿Qué herramienta permite cifrar archivos en Linux?
 - a. gpg
 - b. ppp
 - c. man
10. ¿Es considerada segura la UEFI de un fabricante que no publica actualizaciones de seguridad de su firmware? ¿Verdadero o falso?
 - a. Verdadero
 - b. Falso

El departamento de I+D tiene unos resultados extraordinarios por lo logros conseguidos en el descubrimiento de un nuevo sistema de propulsión eléctrica en los coches fabricados por la compañía. Existen intereses económico de empresas de la competencia y actores externos por hacerse con esta información para poder aplicarla a sus modelos.

El CISO de la compañía quiere que se investigue si el sistema donde se guarda la información sensible y crítica es segura. Por lo que ha pedido que se revisen las medidas de seguridad relativas a estos sistemas.

Buscando:

- Los directorios que tienen permisos de escritura.
- Los directorios que tienen permisos de ejecución.
- Ficheros con el SUID o SGID activado, que permitan ejecutar los ficheros con permisos de root, incluyendo si existe algún fichero con permisos de root entre los de la siguiente lista: <https://gtfobins.github.io>
- Los ficheros de la variable PATH, comprobando qué usuarios tienen acceso de escritura en esos directorios.
- Las carpetas compartidas mal configuradas que permiten realizar acciones no controladas.
- Las particiones que tienen permisos para ejecutar ficheros y otras características que tienen impacto sobre la seguridad.
- Borrado seguro de archivos.

El escenario se puede realizar con un sistema operativo Linux Ubuntu.

1. Los directorios que tienen permisos de escritura

`find / -type d -perm /o+w`

buscamos (find) los directorios (-type d) que tienen permisos de escritura para otros usuarios (-perm /o+w)

```
albamorejon@albamorejon:~$ sudo find / -type d -perm /o+w
[sudo] contraseña para albamorejon:
/snap/core22/1722/run/lock
/snap/core22/1722/tmp
/snap/core22/1722/var/tmp
/snap/core22/1748/run/lock
/snap/core22/1748/tmp
/snap/core22/1748/var/tmp
/snap/core20/2496/run/lock
/snap/core20/2496/tmp
/snap/core20/2496/var/tmp
/snap/core20/2434/run/lock
/snap/core20/2434/tmp
/snap/core20/2434/var/tmp
/dev/nqueue
/dev/shm
find: /run/user/1000/gvfs: Permisos denegados
/run/lock
/tmp
/tmp/systemd-private-66e05a29ac2c4bc595815c423229e78d-fwupd.service-9e5Maj/tmp
/tmp/systemd-private-66e05a29ac2c4bc595815c423229e78d-swiftcontrol.service-M384jl/tmp
/tmp/systemd-private-66e05a29ac2c4bc595815c423229e78d-colord.service-myHY7g/tmp
/tmp/.X11-unix
/tmp/.Test-unix
```

2. Los directorios que tienen permisos de ejecución.

`find / -type d -perm -o+x`

buscamos (find) los directorios (-type d) que tienen permisos de ejecución para otros usuarios (-perm -o+x)

```
albamorejon@albamorejon:~$ find / -type d -perm -o+x
/opt
/opt/VBoxGuestAdditions-7.1.4
/opt/VBoxGuestAdditions-7.1.4/sbin
/opt/VBoxGuestAdditions-7.1.4/bin
/opt/VBoxGuestAdditions-7.1.4/init
/opt/VBoxGuestAdditions-7.1.4/other
/opt/VBoxGuestAdditions-7.1.4/src
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/generic
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/common
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/common/alloc
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/common/math/gcc
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/common/string
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/common/err
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/common/log
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/common/table
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/common/risc
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/common/checksum
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/common/time
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/common/asm
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/VBox
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/rdrv
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/rdrv/generic
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/rdrv/linux
/opt/VBoxGuestAdditions-7.1.4/src/vboxguest-7.1.4/vboxguest/include
```

3. Ficheros con el SUID o SGID activado, que permitan ejecutar los ficheros con permisos de root, incluyendo si existe algún fichero con permisos de root entre los de la siguiente lista: <https://gtfobins.github.io>

SUID (/u+s)=4000

SGID (/g+s)=2000

`sudo find / -type f \(-perm -4000 -o -perm -2000 \) -user root`

```
albamorejon@albamorejon:~$ sudo find / -type f \( -perm -4000 -o -perm -2000 \) -user root
[sudo] contraseña para albamorejon:
/opt/VBoxGuestAdditions-7.1.4/bin/VBoxDRMClient
/snap/core22/1722/usr/bin/chage
/snap/core22/1722/usr/bin/chfn
/snap/core22/1722/usr/bin/chsh
/snap/core22/1722/usr/bin/expiry
/snap/core22/1722/usr/bin/gpasswd
/snap/core22/1722/usr/bin/mount
/snap/core22/1722/usr/bin/newgrp
/snap/core22/1722/usr/bin/passwd
/snap/core22/1722/usr/bin/ssh-agent
/snap/core22/1722/usr/bin/su
/snap/core22/1722/usr/bin/sudo
/snap/core22/1722/usr/bin/unmount
/snap/core22/1722/usr/bin/dbus-daemon-launch-helper
/snap/core22/1722/usr/bin/openssh/ssh-keysign
/snap/core22/1722/usr/bin/libexect/polkkit-agent-helper-1
/snap/core22/1722/usr/bin/pan_extrausers_chkpwd
/snap/core22/1722/usr/bin/umix_chkpwd
/snap/core22/1748/usr/bin/chage
/snap/core22/1748/usr/bin/chfn
/snap/core22/1748/usr/bin/chsh
/snap/core22/1748/usr/bin/expiry
/snap/core22/1748/usr/bin/gpasswd
```

Se podrían buscar los ficheros, suid o sgid por separado

```

root@albamorejon:~# sudo find / -type f -perm /4000
/opt/VBoxGuestAdditions-7.1.4/btn/VBoxDRMClient
/snap/core22/1722/usr/bin/chfn
/snap/core22/1722/usr/bin/chsh
/snap/core22/1722/usr/bin/gpasswd
/snap/core22/1722/usr/bin/mount
/snap/core22/1722/usr/bin/newgrp
/snap/core22/1722/usr/bin/passwd
/snap/core22/1722/usr/bin/su
/snap/core22/1722/usr/bin/sudo
/snap/core22/1722/usr/bin/umount
/snap/core22/1722/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core22/1722/usr/lib/openssh/ssh-keysign
/snap/core22/1722/usr/libexec/polkit-agent-helper-1
/snap/core22/1748/usr/bin/chfn
/snap/core22/1748/usr/bin/chsh
/snap/core22/1748/usr/bin/gpasswd
/snap/core22/1748/usr/bin/mount
/snap/core22/1748/usr/bin/newgrp
/snap/core22/1748/usr/bin/passwd
/snap/core22/1748/usr/bin/su

```

```

root@albamorejon:~# sudo find / -type f -perm /2000
/snap/core22/1722/usr/bin/chage
/snap/core22/1722/usr/bin/expiry
/snap/core22/1722/usr/bin/ssh-agent
/snap/core22/1722/usr/sbin/pan_extrausers_chkpwd
/snap/core22/1722/usr/sbin/unix_chkpwd
/snap/core22/1748/usr/bin/chage
/snap/core22/1748/usr/bin/expiry
/snap/core22/1748/usr/bin/ssh-agent
/snap/core22/1748/usr/sbin/pan_extrausers_chkpwd
/snap/core22/1748/usr/sbin/unix_chkpwd
/snap/core20/2496/usr/bin/chage
/snap/core20/2496/usr/bin/expiry
/snap/core20/2496/usr/bin/ssh-agent
/snap/core20/2496/usr/sbin/pan_extrausers_chkpwd
/snap/core20/2434/usr/bin/chage
/snap/core20/2434/usr/bin/expiry
/snap/core20/2434/usr/bin/ssh-agent
/snap/core20/2434/usr/sbin/pan_extrausers_chkpwd
/snap/core20/2434/usr/sbin/unix_chkpwd

```

Creamos unos ficheros para hacer la prueba de los ficheros suid y sgid

```

albamorejon@albamorejon:~/Documentos$ pwd
/home/albamorejon/Documentos
albamorejon@albamorejon:~/Documentos$ sudo touch /home/albamorejon/Documentos/prueba_suid
albamorejon@albamorejon:~/Documentos$ sudo chown root:root /home/albamorejon/Documentos/prueba_suid
albamorejon@albamorejon:~/Documentos$ sudo chmod u+s /home/albamorejon/Documentos/prueba_suid
albamorejon@albamorejon:~/Documentos$ sudo touch /home/albamorejon/Documentos/prueba_sgid
albamorejon@albamorejon:~/Documentos$ sudo chown root:root /home/albamorejon/Documentos/prueba_sgid
albamorejon@albamorejon:~/Documentos$ sudo chmod g+s /home/albamorejon/Documentos/prueba_sgid

```

```

albamorejon@albamorejon:~/Documentos$ ls -l
total 0
-rwxr-sr-x 1 root root 0 mar 11 19:54 prueba_sgid
-rwsr-xr-x 1 root root 0 mar 11 19:52 prueba_suid

```

Resultados

```

albamorejon@albamorejon:~/Documentos$ sudo find /home/albamorejon/Documentos -type f -perm /4000 -o -perm /2000
/home/albamorejon/Documentos/prueba_suid
/home/albamorejon/Documentos/prueba_sgid

```

Creamos un fichero más, para hacer la prueba de comparar con la lista de gtfobins.github.io

```

albamorejon@albamorejon:~/Documentos$ sudo touch /home/albamorejon/Documentos/prueba_gtfobins
albamorejon@albamorejon:~/Documentos$ sudo chown root:root /home/albamorejon/Documentos/prueba_gtfobins
albamorejon@albamorejon:~/Documentos$ sudo chmod u+s /home/albamorejon/Documentos/prueba_gtfobins

```

```

albamorejon@albamorejon:~/Documentos$ ls -l /home/albamorejon/Documentos/prueba_gtfobins
-rwsr-xr-x 1 root root 0 mar 11 20:02 /home/albamorejon/Documentos/prueba_gtfobins

```

No conseguimos encontrar nada, estamos descargando el contenido de la página (curl), extrayendo los nombres de los ficheros (grep) y guardando la lista en un archivo (>), para después encontrar los ficheros con el SUID o SGID activado y compararlos con la lista creada.

```
albamorejon@albamorejon:~$ curl -s https://gtfobins.github.io/ | grep -oP '(?<=<td>)[^<]+' > /tmp/gtfobins_list.txt
albamorejon@albamorejon:~$ sudo find / -type f \( -perm -4000 -o -perm -2000 \) -user root | grep -f /tmp/gtfobins_list.txt
[sudo] contraseña para albamorejon:
```

Se probó de diferentes métodos, pero no pude conseguirlo

```
albamorejon@albamorejon:~/Documentos$ curl -s https://gtfobins.github.io/ | grep -oP '(?<=<td>)[^<]+' > /tmp/gtfobins_list.txt
albamorejon@albamorejon:~/Documentos$ cat /tmp/gtfobins_list.txt
albamorejon@albamorejon:~/Documentos$ sudo find /home/albamorejon/Documentos -type f \( -perm -4000 -o -perm -2000 \) -user root 2>/dev/null | grep -f /tmp/gtfobins_list.txt
```

4. Las carpetas compartidas mal configuradas que permiten realizar acciones no controladas.

Listamos los permisos de los directorios del PATH, pudiendo ver los de escritura

```
albamorejon@albamorejon:~/brs08$ echo $PATH | tr ':' '\n' | while read dir; do ls -ld "$dir"; done
drwxr-xr-x 2 root root 4096 mar 16 2023 /usr/local/sbin
drwxr-xr-x 2 root root 4096 mar 16 2023 /usr/local/bin
drwxr-xr-x 2 root root 20480 mar 11 19:36 /usr/sbin
drwxr-xr-x 2 root root 40960 mar 11 16:17 /usr/bin
lrwxrwxrwx 1 root root 8 dic 25 12:56 /sbin -> usr/sbin
lrwxrwxrwx 1 root root 7 dic 25 12:56 /bin -> usr/bin
drwxr-xr-x 2 root root 4096 mar 16 2023 /usr/games
drwxr-xr-x 2 root root 4096 mar 16 2023 /usr/local/games
drwxr-xr-x 2 root root 4096 mar 11 20:09 /snap/bin
```

En caso de que se quiera hacer un script para ello:

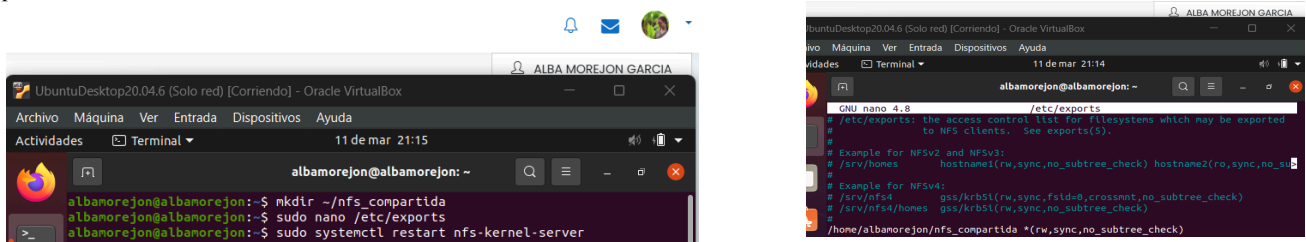
```
albamorejon@albamorejon:~/brs08$ sudo nano comando4.sh
albamorejon@albamorejon:~/brs08$ cat comando4.sh
#!/bin/bash
IFS=':' read -r -a paths <<< "$PATH"
for path in "${paths[@]}; do
  find "$path" -maxdepth 1 -type d -writable -exec ls -ld {} \; 2>/dev/null
done
albamorejon@albamorejon:~/brs08$ sudo chmod +x comando4.sh
albamorejon@albamorejon:~/brs08$ ./comando4.sh
```

```
albamorejon@albamorejon:~/brs08$ ./comando4.sh
albamorejon@albamorejon:~/brs08$
```

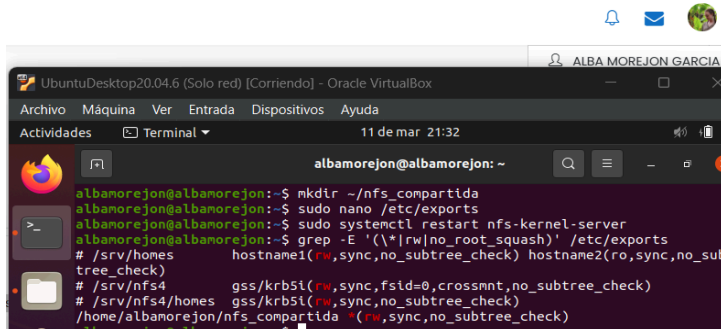
```
albamorejon@albamorejon:~/brs08$ echo $PATH | tr ':' '\n' | while read dir; do ls -ld "$dir"; done
drwxr-xr-x 2 root root 4096 mar 16 2023 /usr/local/sbin
drwxr-xr-x 2 root root 4096 mar 16 2023 /usr/local/bin
drwxr-xr-x 2 root root 20480 mar 11 19:36 /usr/sbin
drwxr-xr-x 2 root root 40960 mar 11 16:17 /usr/bin
lrwxrwxrwx 1 root root 8 dic 25 12:56 /sbin -> usr/sbin
lrwxrwxrwx 1 root root 7 dic 25 12:56 /bin -> usr/bin
drwxr-xr-x 2 root root 4096 mar 16 2023 /usr/games
drwxr-xr-x 2 root root 4096 mar 16 2023 /usr/local/games
drwxr-xr-x 2 root root 4096 mar 11 20:09 /snap/bin
drwxrwxrwx 2 albamorejon albamorejon 4096 mar 11 20:27 /home/albamorejon/Documentos/test
```

5. Las carpetas compartidas mal configuradas que permiten realizar acciones no controladas.

Probamos a hacer una carpeta compartida y conocer cómo se comparte y da los permisos



Buscamos las carpetas compartidas que pueden tener configuraciones más débiles



Algunas configuraciones de NFS pueden ser inseguras y permitir acciones no controladas. Aquí hay algunas opciones que pueden representar un problema de seguridad:

1. Permisos demasiado amplios (rw para todos), la opción read/write permite lectura y escritura a todos los clientes. Esto puede ser peligroso si no se controla adecuadamente, ya que cualquier cliente en la red puede modificar los archivos compartidos.

Ej: /home/usuario/nfs_compartida *(rw,sync,no_subtree_check)

Solución: Limita el acceso a un rango específico de IP y usa root_squash para mapear las solicitudes del usuario root en los clientes a un usuario no privilegiado en el servidor.

Ej: /home/usuario/nfs_compartida 192.168.1.0/24 (rw,sync,no_subtree_check,root_squash)

2. Acceso sin restricciones (*), usar * para permitir acceso a todos los clientes en la red puede ser inseguro. Es mejor especificar direcciones IP o rangos de IP específicos. El problema de seguridad es que permite que cualquier dispositivo en la red acceda a la carpeta compartida, lo que puede incluir dispositivos no autorizados.

Ej: /home/usuario/nfs_compartida *(rw,sync,no_subtree_check)

Solución: Limita el acceso a un rango específico de IP.

Ej: /home/tu_usuario/nfs_compartida 192.168.1.0/24(rw,sync,no_subtree_check)

3. Sin autenticación (no_root_squash):

La opción no_root_squash permite que los usuarios root en los clientes tengan privilegios root en el servidor NFS. Esto puede ser un gran riesgo de seguridad, ya que permite a los usuarios root en los clientes realizar cualquier acción en el servidor.

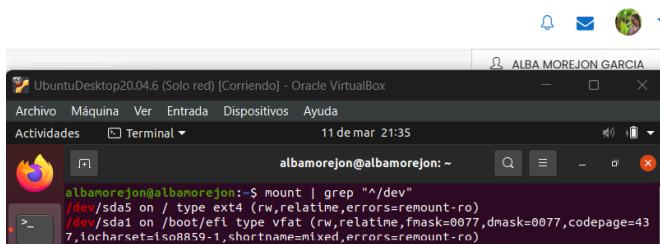
Ej: /home/usuario/nfs_compartida 192.168.1.0/24(rw,sync,no_subtree_check,no_root_squash)

Solución: Usa root_squash para mapear las solicitudes del usuario root en los clientes a un usuario no privilegiado en el servidor.

Ej: /home/usuario/nfs_compartida 192.168.1.0/24(rw,sync,no_subtree_check,root_squash)

6. Las particiones que tienen permisos para ejecutar ficheros y otras características que tienen impacto sobre la seguridad.

Como en directorio /dev, donde se guarda la configuración e información de las particiones del disco duro. Por tanto la forma más rápida sería esta primera opción:



Con este comando podremos listar todas las particiones y sus puntos de montaje

```
albamorejon@albamorejon:~$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0       7:0    0    4K  1 loop /snap/bare/5
loop1       7:1    0   63,7M 1 loop /snap/core20/2434
loop2       7:2    0   63,8M 1 loop /snap/core20/2496
loop3       7:3    0   73,9M 1 loop /snap/core22/1722
loop4       7:4    0   73,9M 1 loop /snap/core22/1748
loop5       7:5    0   346,3M 1 loop /snap/gnome-3-38-2004/119
loop6       7:6    0   349,7M 1 loop /snap/gnome-3-38-2004/143
loop7       7:7    0   505,1M 1 loop /snap/gnome-42-2204/176
loop8       7:8    0   91,7M 1 loop /snap/gtk-common-themes/1535
loop9       7:9    0   12,2M 1 loop /snap/snap-store/1216
loop10      7:10   0    46M 1 loop /snap/snap-store/638
loop11      7:11   0   104,2M 1 loop /snap/core/17200
loop12      7:12   0    44,3M 1 loop /snap/snapd/23258
loop13      7:13   0    44,5M 1 loop /snap/snapd/23771
loop14      7:14   0    240K 1 loop /snap/jq/6
sda         8:0    0   30G  0 disk 
├─sda1      8:1    0   512M  0 part /boot/efi
├─sda2      8:2    0     1K  0 part 
└─sda5      8:5    0   29,5G  0 part /
sr0        11:0    1  1024M  0 ram
```

También podremos usar este comando para ello

```
albamorejon@albamorejon:~$ sudo blkid -o list
device fs_type label mount point UUID
-----
/dev/sda5 ext4 / df328f9a-a606-4edb-8c
/dev/loop0 squashfs /snap/bare/5
/dev/loop1 squashfs /snap/core20/2434
/dev/loop2 squashfs /snap/core20/2496
/dev/loop3 squashfs /snap/core22/1722
/dev/loop4 squashfs /snap/core22/1748
/dev/loop5 squashfs /snap/gnome-3-38-2004/119
/dev/loop6 squashfs /snap/gnome-3-38-2004/143
/dev/loop7 squashfs /snap/gnome-42-2204/176
/dev/sda1 vfat /boot/efi 2EED-6CB4
/dev/loop8 squashfs /snap/gtk-common-themes/1535
/dev/loop9 squashfs /snap/snap-store/1216
/dev/loop10 squashfs /snap/snap-store/638
/dev/loop11 squashfs /snap/core/17200
/dev/loop12 squashfs /snap/snapd/23258
/dev/loop13 squashfs /snap/snapd/23771
/dev/loop14 squashfs /snap/jq/6
```

Con este comando podremos ver los permisos de las particiones

```
albamorejon@albamorejon:~$ findmnt -o TARGET,OPTIONS
TARGET OPTIONS
----
/sys kernel/security rw,relatime,errors=remount-ro
/sys/fs/cgroup squashfs rw,nosuid,nodev,noexec,relatime
/sys/fs/cgroup/systemd rw,nosuid,nodev,noexec,relatime,xattr,nan
/sys/fs/cgroup/devices rw,nosuid,nodev,noexec,relatime,devices
/sys/fs/cgroup/net_cls,net_prrio rw,nosuid,nodev,noexec,relatime,net_cls,n
/sys/fs/cgroup/hugetlb rw,nosuid,nodev,noexec,relatime,hugetlb
/sys/fs/cgroup/rdma rw,nosuid,nodev,noexec,relatime,rdma
/sys/fs/cgroup/freezer rw,nosuid,nodev,noexec,relatime,freezer
/sys/fs/cgroup/cpu,cpuacct rw,nosuid,nodev,noexec,relatime,cpu,cpuac
/sys/fs/cgroup/memory rw,nosuid,nodev,noexec,relatime,memory
/sys/fs/cgroup/misc rw,nosuid,nodev,noexec,relatime,misc
/sys/fs/cgroup/perf_event rw,nosuid,nodev,noexec,relatime,perf_event
/sys/fs/cgroup/pids rw,nosuid,nodev,noexec,relatime,pids
/sys/fs/cgroup/cpuset rw,nosuid,nodev,noexec,relatime,cpuset
/sys/fs/pstore rw,nosuid,nodev,noexec,relatime
/sys/fs/bpf rw,nosuid,nodev,noexec,relatime,node=700
/sys/kernel/tracing rw,nosuid,nodev,noexec,relatime
/sys/kernel/debug rw,nosuid,nodev,noexec,relatime
/sys/fs/fuse/connections rw,nosuid,nodev,noexec,relatime
/sys/kernel/config rw,nosuid,nodev,noexec,relatime
/proc rw,relatime,fd=28,pgrp=1,timeout=0,minpro
/proc/sys/fs/binfmt_misc rw,relatime,fd=28,pgrp=1,timeout=0,minpro
/proc/sys/fs/binfmt_misc rw,relatime,fd=28,pgrp=1,timeout=0,minpro
/proc/fs/nfsd rw,relatime,fd=28,pgrp=1,timeout=0,minpro
/dev rw,nosuid,nodev,noexec,relatime,size=1687196k,n
/dev/pts rw,nosuid,nodev,noexec,relatime,gid=5,node=620,
/dev/shm rw,nosuid,nodev,noexec,relatime,inode64
/dev/hugepages rw,relatime,pagesize=2M
/dev/mqueue rw,nosuid,nodev,noexec,relatime,size=3470
/run rw,nosuid,nodev,noexec,relatime,size=5120
/run/lock rw,nosuid,nodev,relatime,size=347016k,mod
/run/user/1000 rw,nosuid,nodev,relatime,user_id=1000,gro
/run/snapd/ns rw,nosuid,nodev,noexec,relatime,size=3470
/run/snapd/ns/jq.mnt rw,relatime
/run/rpc_pipefs rw,relatime
/snap/bare/5 ro,nodev,relatime,errors=continue
/snap/core20/2434 ro,nodev,relatime,errors=continue
/snap/core20/2496 ro,nodev,relatime,errors=continue
/snap/core22/1722 ro,nodev,relatime,errors=continue
```


7. Borrado seguro de archivos.

Hay diferentes tipos de borrado seguro, en este caso hemos elegido wipe

Con el comando wipe borrará un archivo pero antes lo sobrescribirá varias veces para que sea imposible recuperar los datos.

```
sudo apt install wipe
```

```
wipe archivo.txt
```

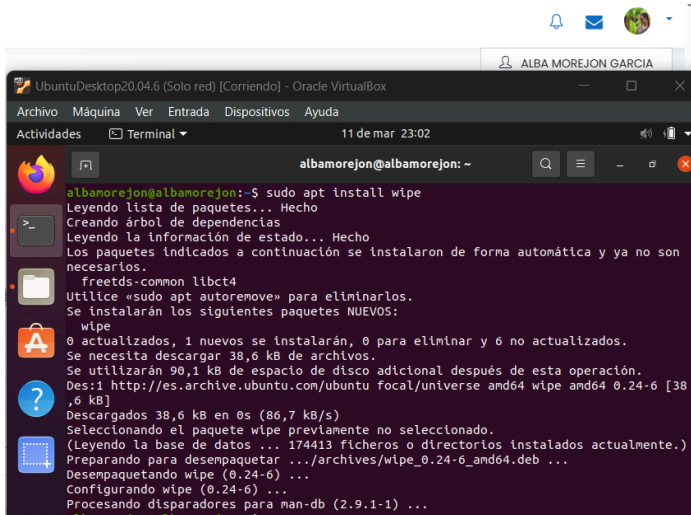
Podemos borrar una carpeta de manera segura y de forma recursiva en todas sus subcarpetas utilizando -r

```
wipe -r carpeta/
```

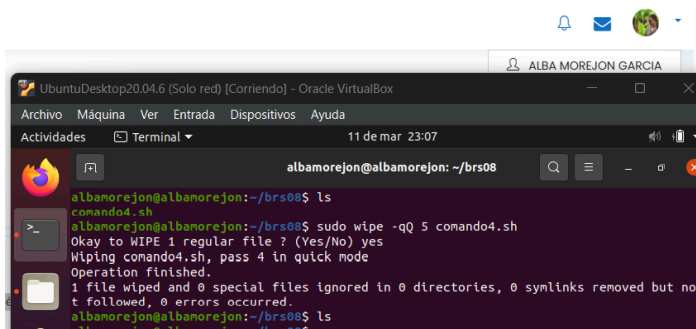
Si queremos decidir la cantidad de veces que se va a sobrescribir el archivo antes de borrarse podemos añadir -qQ

Con -q indicamos que haga un borrado rápido haciendo solo 4 sobrescripciones por defecto sobre el archivo. Al añadir -Q le indicamos cuantas sobrescripciones queremos hacer.

```
wipe -qQ 5 archivo.txt
```



```
albamorejon@albamorejon:~$ sudo apt install wipe
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  freetds-common libct4
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
  wipe
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 6 no actualizados.
Se necesita descargar 38,6 kB de archivos.
Se utilizarán 90,1 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 wipe amd64 0.24-6 [38,6 kB]
Descargados 38,6 kB en 0s (86,7 kB/s)
Seleccionando el paquete wipe previamente no seleccionado.
(Leyendo la base de datos ... 174413 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../archives/wipe_0.24-6_and64.deb ...
Desempaquetando wipe (0.24-6) ...
Configurando wipe (0.24-6) ...
Procesando disparadores para man-db (2.9.1-1) ...
```



```
albamorejon@albamorejon:~/brs08$ ls
comando4.sh
albamorejon@albamorejon:~/brs08$ sudo wipe -qQ 5 comando4.sh
Okay to WIPE 1 regular file ? (Yes/No) yes
Wiping comando4.sh, pass 4 in quick mode
Operation finished.
1 file wiped and 0 special files ignored in 0 directories, 0 symlinks removed but no
t followed, 0 errors occurred.
albamorejon@albamorejon:~/brs08$ ls
```