**Parcial 1 - Parte 2**

**6. En el proceso de construcción (building) de un programa ejecutable, después de compilar el código fuente y tener los archivos con el código objeto que puede cargarse en cualquier ubicación de memoria física (relocatable object file) ¿Cuál es la función del encadenador (linker) y del cargador (loader)?¿De qué parte del material del curso tomó las ideas para la respuesta de esta pregunta?**

El linker se encarga de tomar el código y convertirlo en un ejecutable. Su función es cargar los recursos necesarios, como bibliotecas, eliminar aquellos que no se utilizarán y enlazar el código objeto con sus bibliotecas, lo que finalmente produce un ejecutable o una biblioteca que se entrega al loader. Por otro lado, el loader tiene la tarea de cargar programas en memoria a partir de los ejecutables generados por el linker. Generalmente, el cargador es una parte del núcleo del sistema operativo, se carga al iniciar el sistema y permanece en memoria hasta que el sistema se reinicia o se apaga.  
  
Esa información fue sacado en el Clasroom parte de Gestión de Proceso publicado el 30 de noviembre del 2024

**7. A.** En qué páginas del libro The Linux Command Line del año 2019 se presentan los comandos cat, grepy wc **[**[**https://www.arcesio.net/so/libros/The\_Linux\_Command\_Line\_2019.pdf**](https://www.arcesio.net/so/libros/The_Linux_Command_Line_2019.pdf)**]**

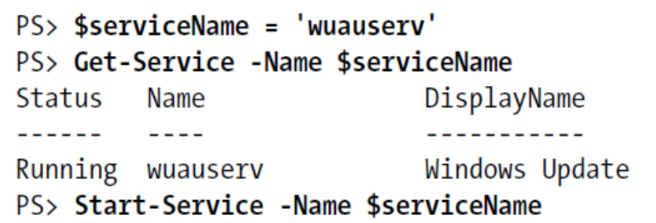
El comando Cat se encuentra en la página 102 y 103 del PDF, el libro no tiene conteo de páginas, grep en la página 107, wc en la página 106.

**B. Explique brevemente qué hace el siguiente comando**

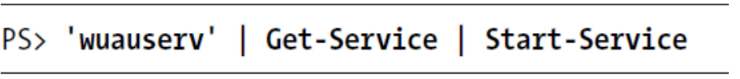
**cat lista estudiantes.txt | grep Rodriguez | wc**

CAT se utiliza frecuentemente para visualizar el contenido de un archivo de texto de manera sencilla. GREP permite buscar una palabra o patrón específico, imprimiendo las líneas que lo contengan. Este comando busca un patrón que definimos en un archivo de texto. WC es un comando de Linux que nos ayuda a contar directorios, archivos y líneas dentro de los archivos. Primero, con cat mostramos el contenido del archivo ‘lista\_estudiantes.txt’; luego, con grep buscamos "Rodriguez" para encontrar las líneas que lo incluyan. Finalmente, con wc contamos cuántas líneas hemos encontrado. Así que, en resumen, esta línea de comandos cuenta cuántas veces aparece "Garcia" en el archivo.

**8. A continuación, se muestra una secuencia de comandos en PowerShell de Windows**

****

**A. ¿Qué relación tiene la secuencia anterior con el siguiente comando?**

****

La relación entre la secuencia anterior de comandos y el comando: 'wuauserv' | Get-Service | Start-Service

Ambos tienen el objetivo de obtener información sobre el servicio llamado **wuauserv** y, si es necesario, iniciarlo.

### Explicación:

1. **Secuencia anterior**:

Get-Service -Name $serviceName: Obtiene el estado actual del servicio especificado en la variable $serviceName (en este caso, 'wuauserv').

Start-Service -Name $serviceName: Inicia el servicio si no está ya en ejecución.

1. **Comando simplificado**:

'wuauserv' | Get-Service | Start-Service: Utiliza un *pipeline* para pasar directamente el nombre del servicio (wuauserv) como entrada a Get-Service, que obtiene información del servicio, y después lo pasa a Start-Service para iniciarlo si es necesario.

### Relación:

* La secuencia de comandos **manual** en la primera parte logra lo mismo que el comando con *pipeline*, pero de forma más explícita.
* El uso del *pipeline* en el segundo comando simplifica el proceso al concatenar las operaciones en una sola línea.

B. En qué páginas del libro PowerShell for Sysadmins de 2020 se muestran los comandos utilizados como referencia aquí [<https://www.arcesio.net/so/libros/PowerShell_for_Sysadmins_2020.pdf>]  
  
Todos los comandos de comando se encuentran en la página 38 del libro o en la página 64 del PDF.

**9. Liste las ventajas de UEFI (Unified Extensible Firmware Interface) con base en el libro Hands-on Booting de 2020. [**[**https://www.arcesio.net/so/libros/Hands-on\_Booting\_Learn\_the\_Boot\_Process\_of\_Linux\_Windows\_and\_Unix\_2020.pdf**](https://www.arcesio.net/so/libros/Hands-on_Booting_Learn_the_Boot_Process_of_Linux_Windows_and_Unix_2020.pdf)**]**

Las ventajas de UEFI son las siguientes:

1. **Compatibilidad con procesadores de 64 bits**: UEFI puede aprovechar todo el potencial del procesador (hasta 64 bits), mientras que el BIOS se limita a 16 bits.
2. **Acceso completo a la RAM**: UEFI puede utilizar módulos de RAM completos, a diferencia del BIOS, que tiene una limitación de 1 MB en el espacio de direcciones.
3. **Tabla de particiones GPT**: UEFI utiliza la tabla de particiones GUID (GPT), que permite un número ilimitado de particiones primarias, eliminando la necesidad de particiones primarias y lógicas.
4. **Tamaño máximo de partición**: El tamaño máximo de una partición en UEFI es de 8 zettabytes, lo que es significativamente mayor que los 2,2 TB que permite el BIOS.
5. **Herramientas de gestión empresarial**:

* Reparación remota de la computadora.
* Acceso a Internet desde el firmware UEFI.
* Posibilidad de modificar el comportamiento o la configuración del firmware UEFI desde el sistema operativo, sin necesidad de reiniciar.

1. **Sistema operativo en miniatura**:

* Acceso completo a dispositivos de audio y video.
* Capacidad de conectarse a WiFi.
* Uso de mouse para la navegación.
* Interfaz gráfica de usuario (GUI) rica, con botones, menús desplegables y animaciones.
* Tienda de aplicaciones integrada, similar a Google Play o App Store, donde se pueden descargar aplicaciones como calendarios, clientes de correo electrónico, navegadores, juegos, entre otros.
* Capacidad de ejecutar cualquier binario en formato ejecutable EFI.

1. **Arranque seguro (Secure Boot)**: UEFI permite verificar la autenticidad de los archivos del cargador de arranque antes de su ejecución, lo que previene la ejecución de archivos maliciosos o no autorizados.
2. **Compatibilidad retroactiva (backward compatibility)**: UEFI es compatible con el "modo BIOS heredado", lo que permite que los sistemas operativos que no admiten UEFI se inicien a través de UEFI.

**10. En Windows**

**A. ¿para qué sirve el comando bcdedit?**

BCDEDIT es un comando que se encuentra en la consola de CMD y permite, a través de la herramienta Bcdedit.exe, cambiar, modificar y personalizar la configuración de arranque de Windows. Podemos utilizarlo de manera sencilla para establecer el orden de los sistemas operativos, su nombre en el menú de arranque, utilizar sistemas en discos virtuales, habilitar o deshabilitar efectos, entre otras cosas. Es fundamental en situaciones donde tenemos instaladas dos o más versiones diferentes de Windows en un mismo equipo.

**B. En el libro Windows Internals Part 2 del año 2021, en la página 398 ¿sobre qué se habla de bcdedit?**

Se habla de bcdedit en el contexto de modificar el almacén de configuración de arranque (BCD) en sistemas Windows. Aquí están los puntos clave sobre bcdedit:

1. **Uso de bcdedit /store**:

Este comando permite modificar el BCD fuera de línea, facilitando el acceso a un almacén de BCD específico, ya sea un archivo local o remoto.

1. **Habilitar depuración del kernel**:

bcdedit se utiliza para identificar la configuración correcta en el BCD, como la sección del Cargador de Arranque de Windows. Se menciona el comando bcdedit /v para verificar identificadores y valores clave.

1. **Modificación de valores BCD:**

Se añade un nuevo subárbol (0x2600000a) en el subárbol Elements del BCD, configurado para habilitar la depuración del kernel al establecer el valor del elemento en 1.

* El valor agregado corresponde a BcdOSLoaderBoolean\_KernelDebuggerEnabled.

Las respuestas a las preguntas 6 a 10 deben ser entregadas en el Classroom del curso junto con la evidencia de la realización del módulo Introduction to Academy de The Hack the Box Academy (<https://academy.hackthebox.com/>)

Aquí la evidencia

