



Black System

Seguridad Informática

Seguridad Informática

FPTD/2021/019/2080

<http://www.free-powerpoint-templates-design.com>

Comandos

01

➤ GREP

02

➤ FIND

03

➤ FILE, SORT, STRINGS Y BASE64



Grep: El comando grep perteneciente a la familia Unix es una de las herramientas más versátiles y útiles disponibles. Este busca un patrón que definamos en un archivo de texto. En otras palabras, con grep en Linux puedes buscar una palabra o patrón y se imprimirá la línea o líneas que la contengan.

La sintaxis del comando grep al buscar un solo archivo es así:

```
grep [opciones] pattern [ARCHIVO] - grep naranjas prueba.txt
```

[opciones]: modificadores del comando

pattern: el patrón que queremos encontrar con la búsqueda

[ARCHIVO]: el archivo en el que estás realizando la búsqueda



Las opciones más importantes y comunes son:

- i: la búsqueda no distinguirá entre mayúsculas y minúsculas. Es decir, si quieres buscar la palabra «auto» será lo mismo que «AUTO»
- c: muestra el número de líneas que coinciden con el patrón buscado
- r: habilita la búsqueda recursiva en el directorio actual
- n: busca líneas y precede cada línea coincidente con un número de línea.
- v: con esta opción, se nos muestran las líneas que no coinciden con el patrón que hemos buscado
- l: muestra el nombre de los archivos que contienen la palabra definida
- e: sirve para encadenar búsquedas, tiene que ir entre comillas simples las palabra
grep -e 'hola' -e 'adiós' prueba.txt

Si necesitamos buscar una cadena de texto, tendrá que ir entre comillas simples:
grep 'mi nombre' prueba.txt

Para buscar un conjunto de caracteres: grep 'hola[1234]' prueba.txt

Grep "^hola" prueba.txp – solo saca los resultados que estén al principio de la línea

Grep "hola\$" – solo saca los resultados que estén al final de la línea

find: Cuando se trata de localizar archivos o directorios en su sistema, el comando de búsqueda en Linux no tiene paralelo. Es simple de usar, pero tiene muchas opciones diferentes que te permiten afinar la búsqueda de archivos

find ruta -opciones

Las opciones más importantes y comunes son:

- Para buscar archivos ocultos `-name “.”`
- Para buscar recursivamente ponemos un `.` – `find .`
- Para buscar archivos con tamaños específicos `-size +10M` (mas de 10 megas)
- `c` par bytes
- Para encontrar archivos vacios – `find ruta -type f -empty`
- Para encontrar directorios vacios – `find ruta -type d -empty`
- Si queremos borrar o archivos o directorios vacios – `find ruta -type f -empty -delete` (cambiar la `f` por la `d` si son directorios)
- Para encontrar comandos que tengan ciertos tipos de permiso (importante) – `find ruta -perm /4000` (4000 son permisos `suid`, permiten a usuarios normales ejecutar un programa con privilegios)
- Al usar `find` sobre todo desde la raíz habrá muchos directorios que no tengamos permisos para leer y nos arrojará un permiso denegado, para evitar que salgan estos errores por pantalla redireccionamos la salida a la carpeta `/dev/null` – `find / -perm 4000 2>/dev/null`
- Para buscar archivos modificados en los últimos X días – `find ruta -type f -mtime -30`
- `Find` tiene la opción de especificar que busque los archivos que son `readable`, `writable` o `executable` (para poner el contrario pondremos una exclamación cerrada antes)



file: nos dice el tipo de archivo que es (datos, texto, gif, etc)

file ruta - file prueba/* - así nos diría que tipo de archivos son todos los que hay dentro de la carpeta prueba

sort: es un comando para ordenar líneas de archivos de texto, alfabéticamente, por número, mes y también puede eliminar duplicados
Por defecto ordena alfabéticamente – sort archivo.txt

Las opciones más importantes y comunes son:

- Para orden inverso –r
- Para orden numérico –n
- Para eliminar los duplicados –u
- Para ordenar por meses –M

strings: nos sirve para extraer texto legible de un archivo de datos

strings data

base64: podemos codificar un archivo en base64 o decodificarlo

Codificarlo = base64 prueba.txt

Decodificarlo = base64 -d prueba.txt

