Seguridad de la Información

Una introducción con enfoque práctico

Ing. Mariano Aliaga

Universidad Católica de Córdoba - Facultad de Ingeniería

2021

Panorama General

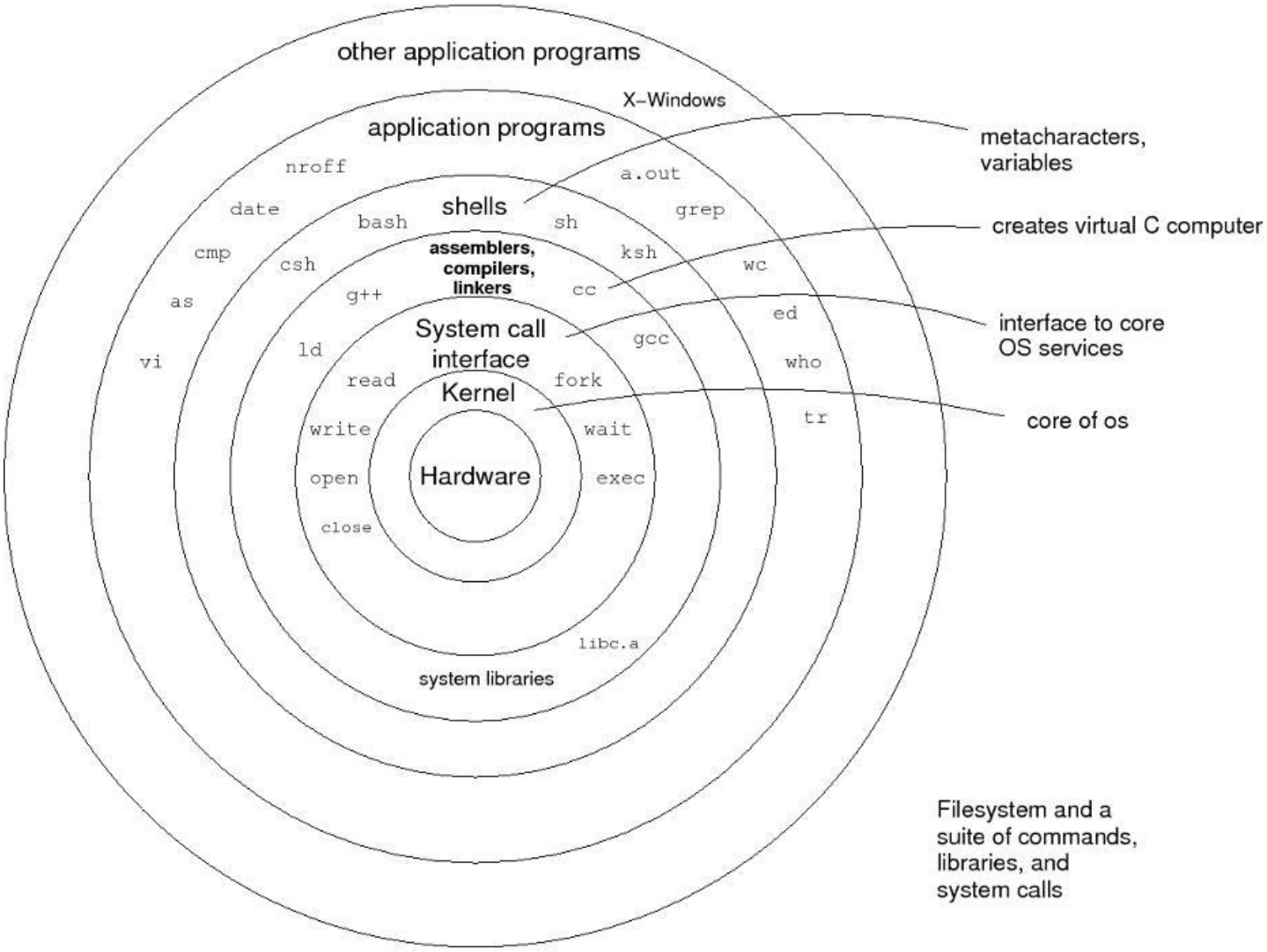
La línea de comandos

Los hackers no usan el mouse!

Interfaz de Comandos en Línea: Una interfaz de comandos en línea (CLI) es un mecanismo para interactuar con un Sistema Operativo de computadora o software escribiendo comandos para realizar tareas específicas.

Shell (o Command-line Interpreter): programa encargado de recibir, analizar y ejecutar el comando solicitado. Luego de completar el comando, muestra al usuario la salida correspondiente en forma de texto.

La línea de comandos



Conceptual Architecture of UNIX SYSTEMS

La línea de comandos

Símbolo	Función	Ejemplo
>	Envía la salida de un comando a un archivo.	comando > archivo
>>	Agrega la salida de un comando al final (append) del archivo indicado.	comando >> archivo
<	Usa los contenidos del archivo indicado como entrada para el comando.	comando < archivo
|	Envía la "salida" de un comando a la "entrada" del siguiente.	comando1 | comando2
&&	Combinación condicional: ejecuta el comando2 SI el comando1 se completó exitosamente.	comando1 && comando2
||	El comando2 se ejecuta SÓLO SI el comando1 falla	comando1 || comando2

Shells MS Windows

- **COMMAND.COM:** utilizado en MS-DOS y hasta Windows 9.x
- **cmd.exe:** Windows NT en adelante
- **PowerShell:** intérprete de comandos y lenguaje de scripting basado en .NET. Fue liberado en 2006 y hecho open source y multiplataforma en 2016.

Manejo de archivos y directorios

- **assoc:** muestra o modifica las asociaciones de extensiones de archivos.

```
assoc [.ext[=[fileType]]]
```

- **attrib:** muestra, establece o elimina atributos de archivos y directorios.

```
attrib [{+r|-r}] [{+a|-a}] [{+s|-s}] [{+h|-h}]
[[Drive:][Path] FileName] [/s[/d]]
```

- **ftype:** muestra o define con qué programa se abre cada tipo de archivo.

```
ftype [fileType[=[openCommandString]]]
```

Manejo de archivos y directorios

- **more:** muestra la salida dividiéndola en pantallas.

```
more [[/c] [/p] [/s] [/tn] [+n]] < [Drive:]
[Path] FileName
```

- **type:** muestra el contenido de uno o más archivos de texto.

```
type [Drive:][Path] FileName
```

- **xcopy:** copia archivos o directorios.

```
xcopy source [destination] [/A | /M] [/D[:date]] [/P]
[/S [/E]] [/V] [/W] [/C] [/I] [/Q] [/F] [/L] [/G]
[/H] [/R] [/T] [/U] [/K] [/N] [/O] [/X] [/Y] [/-Y]
[/Z] [/EXCLUDE:file1[+file2][+file3]...]
```

Estado y configuración de red

- **arp:** muestra y modifica las entradas del cache ARP (Address Resolution Protocol)

```
arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr]
[-d InetAddr [IfaceAddr]]
[-s InetAddr EtherAddr [IfaceAddr]]
```

- **ipconfig:** muestra la configuración actual de TCP/IP y renueva el estado de DHCP y DNS.

```
ipconfig [/all] [/renew [Adapter]] [/release [Adapter]] [/flushdns]
[/displaydns] [/registerdns] [/showclassid Adapter]
[/setclassid Adapter [ClassID]]
```

- **netstat:** muestra información detallada del estado de las conexiones TCP/UDP, puertos que están escuchando, estadísticas Ethernet, ruteo IP, etc.

```
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
```

Estado y configuración de red

- **net:** es una suite de comandos para ver y manejar servicios de red.

  `net help` *`command`*

- **ping:** verifica la conectividad a nivel IP enviando paquetes de "Echo Request" de ICMP (Internet Control Message Protocol).

  ```
  ping [-t] [-a] [-n Count] [-l Size] [-f] [-i TTL]
  [-v TOS] [-r Count] [-s Count] [{-j HostList |
  -k HostList}] [-w Timeout] [TargetName]
  ```

- **route:** muestra y modifica las entradas de la tabla de ruteo IP local.

  ```
  route [-f] [-p] [Command [Destination] [mask Netmask]
  [Gateway] [metric Metric]] [if Interface]]
  ```

Estado y configuración de red

- **telnet:** permiten la comunicación con un host remoto utilizando el protocolo Telnet. También puede utilizarse para establecer conexiones TCP en distintos puertos.

  ```
  telnet RemoteServer [port]
  ```

- **tracert:** determina el camino tomado a un destino enviando mensajes "Echo Request" de ICMP

  ```
  tracert [-d] [-h MaximumHops] [-j HostList]
  [-w Timeout] [TargetName]
  ```

Estado e información del sistema

- **date:** muestra la fecha actual del sistema. Si se ejecuta sin parámetros, permite además cambiarla.

  ```
  date [mm-dd-yy] [/t]
  ```

- **time:** muestra la hora actual del sistema. Si se ejecuta sin parámetros, permite además cambiarla.

  ```
  time [/t] [/time] [hours:[minutes[:seconds[.hundredths]]]
  [{A|P}]]
  ```

- **ver:** muestra la versión de Windows.

Shells Linux/Unix

- **sh:** Bourne shell. Introducido en 1979 implementa las funciones minimas comunes a cualquier shell Unix.
- **bash:** Bourne-Again Shell. Implementación GNU más completa que sh y la más utilizada en distribuciones Linux.
- **dash:** subconjunto de bash utilizado por Debian.
- **ksh:** Korn shell
- **csh:** C shell
- **zsh:** Z shell

Manejo de archivos y directorios

- **cat:** muestra los contenidos de un archivo a `stdout`. Recibe como argumento el archivo que se quiere ver.

  `cat archivo [>|>] [`*`archivo de destino`*`]`

- **cd:** permite cambiar de directorio para ir a la nueva ubicación.

  `cd` *`ruta`*

- **cmp:** compara los contenidos de dos archivos. Si no hay diferencias entre los archivos, `cmp` no devuelve nada. De otro modo, se muestra en qué difieren uno de otro.

  `cmp [-ls]` *`arch1 arch2`*

Manejo de archivos y directorios

- **cp:** permite copiar dos archivos.

  `cp [-R]` *`origen destino`*

- **cut:** extrae columnas de datos, que pueden ser bytes, caracteres o campos de una línea en un archivo.

  `cut [-cdf` *`lista`*`]` *`archivo`*

- **diff:** se utiliza para determinar las diferencias entre archivos o directorios.

  `diff [-iqb]` *`arch1 arch2`*

Manejo de archivos y directorios

- **du:** muestra el uso de disco de archivos y directorios.

  `du [-askh] archivos`

- **file:** determina el tipo de archivo en cuestión y lo muestra en la pantalla.

  `file` *`archivo`*

- **find:** sirve para buscar archivos o directorios.

  `find [`*`ubicación_de_origen`*`] [-type fdl] [-name `*`patrón`*`] [-exec `*`comando`*` {} \;]`

- **grep:** permite buscar un patrón de caracteres en uno o más archivos.

  `grep [-viw]` *`patrón archivo`*

Manejo de archivos y directorios

- **head:** muestra las primeras líneas de un archivo.

  `head [-líneas | -n número]` *`archivo`*

- **ln:** crea enlaces simbólicos a archivos o directorios.

  `ln [-s]` *`origen destino`*

- **ls:** lista los archivos (y subdirectorios) de un directorio.

  `ls [-la1]` *`archivo_o_directorio`*

- **mkdir:** crea un directorio.

  `mkdir` *`directorio`*

Manejo de archivos y directorios

- **mv:** se utiliza para mover o renombrar archivos y directorios.

  `mv [-if] origen destino`

- **pwd:** muestra por pantalla la ruta completa del directorio actual de trabajo.
- **rm:** elimina archivos o directorios.

  `rm [-rif] archivo_o_directorio`

- **tail:** muestra las últimas líneas de un archivo.

  `tail [-líneas | -fr] archivo`

- **wc:** cuenta las líneas, caracteres y/o palabras que tiene un determinado archivo.

  `wc [-lwc] archivo`

Archivado y compresión de datos

- **gzip:** permite comprimir archivos o directorios.

  `gzip [-rv9]` *`archivo`*

- **gunzip:** descomprime un archivo a su forma original.

  `gunzip [-v]` *`archivo`*

- **tar:** permite archivar múltiples archivos y directorios en un único archivo.

  `tar [t] [c] [x] [v] [z] [f` *`destino`*`] `*`origen`*

- **zip/unzip:** otra utilidad para compresión/descompresión de datos que es compatible con sistemas como MS-DOS y Windows NT.

  `zip/unzip` *`archivo`*

Estado y configuración de red

- **arp:** permite manipular el cache ARP del sistema.
- **ifconfig:** configura una interfaz de red.

```
ifconfig [-v] [-a] [-s] [interface]
ifconfig [-v] interface options | address
```

- **netstat:** muestra conexiones de red, tablas de ruteo, estadísticas de interfaces, etc.

```
netstat [-t] [-u] [-l] [-a] [-n] [-p] [-v]
```

- **ping:** envía paquetes de Echo Request ICMP a hosts de la red.

Estado y configuración de red

- **route:** muestra y configura la tabla de ruteo IP del sistema.

```
route {add|del} [-net|-host] target [netmask Nm]
[gw Gw]
```

- **traceroute:** muestra la ruta hacia un host determinado.

```
traceroute host
```

Estado e información del sistema

- **dmesg:** muestra los mensajes de estado que genera el kernel durante el proceso de arranque.
- **free:** muestra estadísticas sobre la utilización de la memoria.
- **kill:** se utiliza para enviar una señal a un proceso.

  `kill [-señal]` *`pid`*

- **ps:** produce un reporte de todos los procesos que se corren en un sistema.

  `ps [-e] [-f] [-l] [-w] [-o]`

- **shutdown:** permite cerrar el sistema para apagarlo o reiniciarlo.

  `shutdown [-r] [-h] [-c] [-k] [-t segundos] time`

Estado e información del sistema

- **top:** muestra una lista en tiempo real de los procesos corriendo en el sistema.
- **uname:** muestra información del sistema actual.

```
uname [-m] [-n] [-r] [-s] [-v] [-a]
```

- **uptime:** muestra información generada desde el arranque del sistema.

Más información

- **Wikipedia**. *Command-line interface*. `http://en.wikipedia.org/wiki/Command-line_interface`
- **Microsoft**. *Command-line reference A-Z*. `https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands`
- **LinuxManPages.com**. *Man Pages Online*. `https://linux.die.net/man/`