Seguridad Básica de Linux

Agenda

1. Sistemas de archivos
2. Auditoria del sistema (syslogd)
3. Control de acceso de red
4. Técnicas de autentificación
5. Cortafuegos de host (basico)
6. Protección de conexiones de red
7. IDS de “target”
8. Pruebas y monitoreo del sistema

1 Sistemas de archivos

- Una norma básica de seguridad radica en la asignación a cada usuario sólo de los permisos necesarios para poder cubrir las necesidades de su trabajo sin poner en riesgo el trabajo de los demás.

1 Sistemas de archivos

- **Riesgos**
  - Dentro del sistema Linux todo son archivos: desde la memoria física del equipo hasta el ratón, pasando por módems, teclado, impresoras etc.
  - Esta filosofía de diseño es uno de los factores que mas éxito y potencia proporciona a Linux , pero también uno de los que mas peligros, debido a que un simple error en un permiso puede permitir a un usuario modificar todo el disco duro, o leer los datos tecleados desde una Terminal etc.

1 Sistemas de archivos

- El sistema de archivos es la parte del núcleo (Kernel) mas visible por los usuarios; se encarga de abstraer propiedades físicas de los diferentes dispositivos para proporcionar una interfaz única de almacenamiento: el archivo.
- Cada sistema Linux tiene su sistema de archivos nativo. (ejemplo ext3)

1 Sistemas de archivos

Parque Tecnologico
Mérida - Venezuela

- Un primer criterio para mantener un sistema seguro es una correcta distribución del espacio de almacenamiento.
- Esto limita el riesgo de que el deterioro de una partición afecte a todo el sistema. La pérdida se limitaría al contenido de esa partición.

1 Sistemas de archivos

Parque Tecnologico
Mérida - Venezuela

- Tamaño de las particiones
  - No hay unas normas generales aplicables; el uso al que vaya destinado el sistema y la experiencia son las bases de la decisión adecuada, aunque por lo general se recomienda:
    - Si el sistema va a dar servicio a múltiples usuarios que requieren almacenamiento para sus datos es conveniente que el directorio /home tenga su propia partición.
    - Si el equipo va a ser un servidor el directorio /var o incluso /var/spool deberían tener su propia partición.

1 Sistemas de archivos

Parque Tecnologico
Mérida - Venezuela

- Tamaño de las particiones (continuación)
  - Debe dimensionar cuidadosamente la partición raíz.
  - El directorio /usr/local contiene los programas compilados e instalados por el administrador.
  - Resulta conveniente usar una partición propia para proteger estos programas personalizados de futuras actualizaciones del sistema.
  - Este criterio también se puede aplicar al directorio /opt.

1.1 Protección de archivos

Parque Tecnologico
Mérida - Venezuela

- Permisos de un archivo
  - Los permisos de cada archivo son la protección mas básica de estos objetos del sistema operativo; definen quien puede acceder a cada uno de ellos, y de que forma puede hacerlo. Cuando hacemos un ls -l podemos ver sus permisos junto al tipo de archivo correspondiente,
  - en la primera columna de cada línea:

```
user:~# ls -l texto.txt
-rw-r--r--    1 user  electric   512 Aug  3  2003 texto.txt
```

1.1 Protección de archivos

- Permisos de un archivo (continuación)
- **Propiedad:**
  - Qué usuario y grupo posee el control de los permisos del i-nodo. Se almacenan como dos valores numéricos, el uid (user id) y gid (group id).
- **Permisos:**
  - Bits individuales que definen el acceso a un Archivo o directorio. Los permisos para directorio tienen un sentido diferente a los permisos para Archivos. Más abajo se explican algunas diferencias.

1.1 Protección de archivos

Parque Tecnologico
Mérida - Venezuela

- Permisos de un archivo (continuación)
- **Lectura (r)**:
  - **Archivo**: Poder acceder a los contenidos de un Archivo
  - **Directorio**: Poder leer un directorio, ver qué Archivos contiene
- **Escritura (w)**:
  - **Archivo**: Poder modificar o añadir contenido a un Archivo
  - **Directorio**: Poder borrar o mover Archivos en un directorio

1.1 Protección de archivos

- Permisos de un archivo (continuación)

- **Ejecución(x)**:
  - **Archivo**: Poder ejecutar un programa binario o guión de shell
  - **Directorio**: Poder entrar en un directorio

1.1 Protección de archivos

- Permisos de un archivo (continuación)

Atributos de un archivo

- En el sistema de archivos ext2 (Second Extended File System) de Linux existen ciertos atributos para los archivos que pueden ayudar a incrementar la seguridad de un sistema.

1.1 Protección de archivos

Parque Tecnologico
Mérida - Venezuela

Atributo	Signicado
A	Dont update Atime
S	Synchronous updates
a	Append only
c	Compressed file
i	Immutable file
d	No Dump
s	Secure deletion
u	Undeletable

1.2 Listas de control de acceso

Parque Tecnologico
Mérida - Venezuela

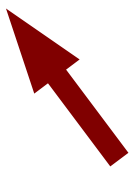
- Listas de control de acceso (ACLs Access Control Lists)
- Las ACL proveen de un nivel adicional de seguridad a los archivos extendiendo el clásico esquema de permisos en Unix: con los permisos solo podemos especiar opciones para los tres grupos de usuarios habituales (propietario, grupo y resto)
- Las ACLs permien asignar permisos a usuarios o grupos concretos; por ejemplo, se pueden otorgar ciertos permisos a dos usuarios sobre unos archivos sin necesidad de incluirlos en el mismo grupo.

ACL

Parque Tecnologico
Mérida - Venezuela

- # setfacl -R -m \
  d:u:donkey:rwx,d:u:chirico:rwx,d:u:bozo2:rwx /fs
- $ ls -l /fs/one/stuff

  -rw-rw----+ 1 chirico chirico 0 Sep 3 17:48 /fs/one/stuff



EL KERNEL TIENE QUE HABER SIDO COMPILADO PARA PERMITIR ALC!

Acl cont...

Parque Tecnologico
Mérida - Venezuela

- $ getfacl /fs/one/stuff

```
# file: fs/one/stuff
# owner: chirico
# group: chirico
user::rw-
user:chirico:rwx                #effective:rw-
user:donkey:rwx                 #effective:rw-
user:bozo2:rwx                  #effective:rw-
mask::rw-
other::---
```

1.3 Almacenamiento seguro

Parque Tecnologico
Mérida - Venezuela

- Cifrado de archivos:
  - PGP: Pretty Good Privacy
  - GnuPG: Gnu Privacy Guard
  - TCFS: Transparent Cryptographic File System (Posiblemente prontamente abandonado)
  - Cryptographic File System CFS

2 Auditoria del sistema

- Casi todas las actividades realizadas en un sistema Linux son susceptibles a ser monitorizadas: desde las horas de acceso de cada usuario al sistema hasta las paginas web mas frecuentemente visitadas, pasando por los intentos fallidos de conexión, los programas ejecutados o incluso el tiempo de CPU que cada usuario consume.

2 Auditoria del sistema

- Es evidente que esta facilidad para recolectar información tiene grandes ventajas para la seguridad.
- Existen también una gran desventajas, ya que la gran cantidad de información que potencialmente se registra puede ser aprovechada para crear ataques de negaciones de servicio.

2 Auditoria del sistema

Parque Tecnologico
Mérida - Venezuela

- El demonio syslogd
  - El demonio syslogd es el encargado de recolectar los datos de los eventos del sistema y demás actividades dependiendo de su archivo de configuración (/etc/syslogd.conf).
  - Los logs creados por el syslogd son comúnmente usados por los IDS-Host
  - Los archivos de salida del syslogd son en texto plano lo cual facilita su visualización
  - Los archivo de logs se encuentran por lo general en /var/logs/
  - Todas las entradas que presenta syslogd tienen como mínimo una fecha y una hora, el nombre de la maquina y del programa que generó el evento.

2 Auditoria del sistema

Parque Tecnologico
Mérida - Venezuela

- Existen diferentes tipos de archivos de log dependiendo de la información.
- Los logs del sistema deben ser rotados periódicamente para poder disminuir su tamaño
- Los logs pueden ser comprimidos
- Los parametros y la cantidad de logs que se guardan en el sistema dependerán en parte de la capacidad de los discos duros.

2 Auditoria del sistema

Parque Tecnologico
Mérida - Venezuela

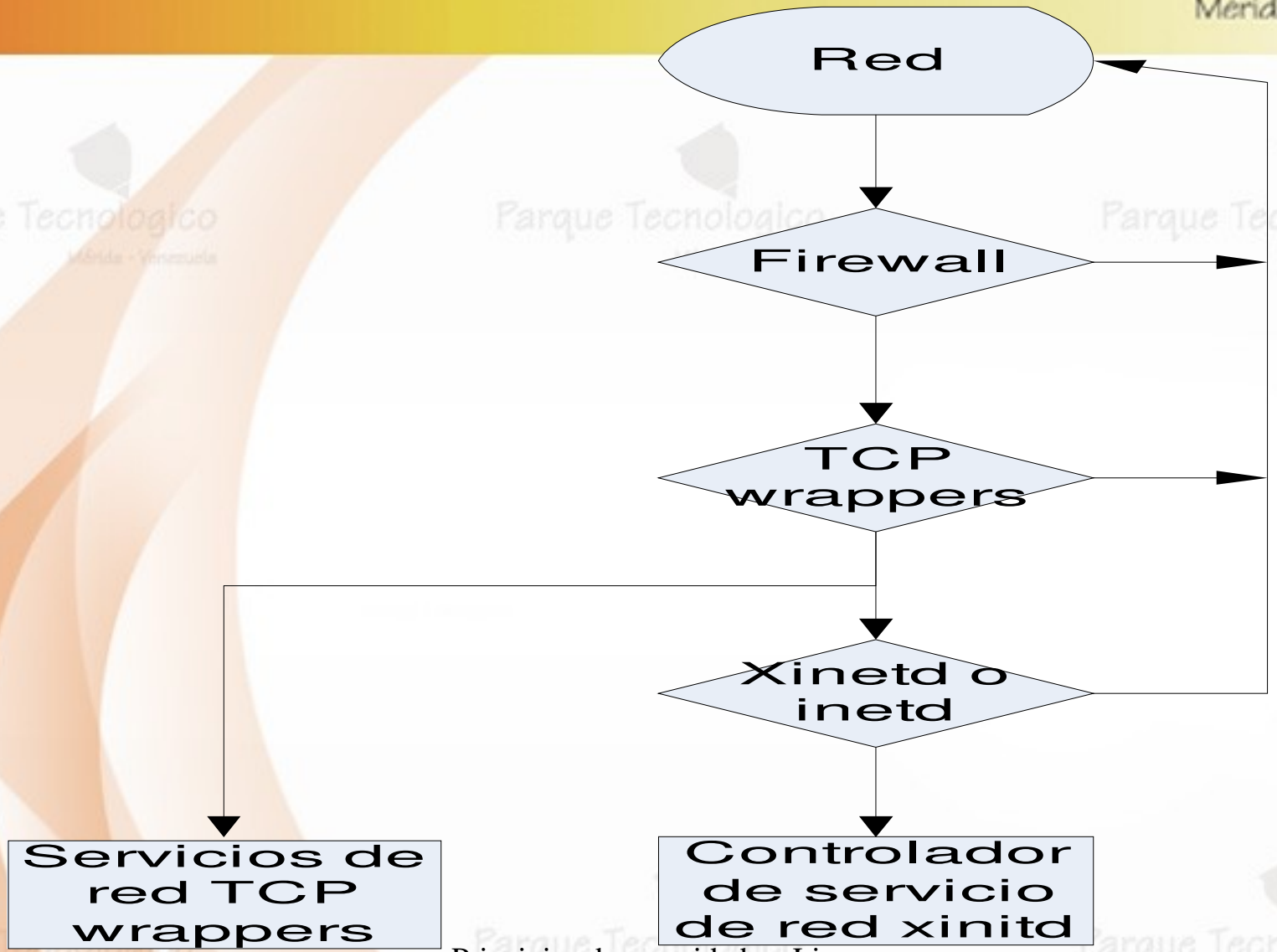
- Archivos de logs mas comunes:
  - **/var/log/syslog:** es el archivo de log mas importante del sistema; en el se guardanmensajes relativos a la seguridad de la maquina, como los accesos o los intentos de acceso a ciertos servicios. No obstante, este archivo es escrito por syslogd, por lo que dependiendo de nuestro archivo de configuración encontraremos en el archivo una u otra información.
  -

2 Auditoria del sistema

Parque Tecnologico
Mérida - Venezuela

- Archivos de logs mas comunes: (continuacion)
-
  - /var/log/messages : En este archivo se almacenan datos `informativos' de ciertos programas, mensajes de baja o media prioridad destinados mas a informar que a avisar de sucesos importantes, como información relativa al arranque de la maquina.

3 Control de acceso de red



3 Control de acceso de red

- Inetd
- Al crecer el número de servicios que se necesitaban, se optó por una mejor idea, se empezó a utilizar un sólo demonio llamado /etc/inetd (El daemon de Internet).
- Este programa escuchaba en varios puertos a la vez y ejecutaba los servidores que se necesitaran en el momento en que se recibía la petición de conexión.
- Cuando empieza su ejecución revisa el archivo de configuracion /etc/inetd.conf para determinar qué servicios de red debe controlar.

3 Control de acceso de red

Parque Tecnologico
Mérida - Venezuela

- **Inetd como funciona**
- Cuando un host cliente intenta conectarse a un servicio de red controlado por inetd, el súper servicio recibe la petición y verifica por cualquier regla de control de acceso wrappers TCP.
- Si se permite el acceso, inetd verifica que la conexión sea permitida bajo sus propias reglas para ese servicio y que el servicio no esté consumiendo más de la cantidad de recursos o si está rompiendo alguna regla. Luego comienza una instancia del servicio solicitado y pasa el control de la conexión al mismo.

3 Control de acceso de red

Parque Tecnologico
Mérida - Venezuela

- **TCP wrappers**

- El wrappers TCP proporciona control de acceso basado en host a los servicios de red.
- El componente más importante dentro del paquete es la librería /usr/lib/libwrap.a.
- Cuando un intento de conexión es hecho a un servicio wrapped TCP, el servicio primero referencia los archivos de *acceso de host* (/etc/hosts.allow y /etc/hosts.deny) para determinar si el cliente tiene permitido conectarse.
- Luego utiliza el demonio syslog (syslogd) para escribir el nombre del host solicitante y el servicio solicitado a /var/log/secure o /var/log/messages.

3 Control de acceso de red

- **TCP wrappers**

- Si a un cliente se le permite conectarse, los TCP wrappers liberan el control de la conexión al servicio solicitado y no interfieren más con la comunicación entre el cliente y el servidor.
- Algunas de los demonio que utilizan TCP wrappers son /usr/sbin/sshd, /usr/sbin/sendmail, y /usr/sbin/xinetd.

4 Técnicas de autentificación

- Método clásico
  - Uso del archivo /etc/passwd
    - Un podría tratar de romper la contraseña, aunque esto es poco probable, el atacante cifrara una palabra junto a un determinado *salt*, y comparar el resultado con la cadena almacenada en el archivo de claves.

4 Técnicas de autentificación

- Método clásico
  - De esta forma, un atacante leerá el archivo /etc/passwd y mediante un programa adivinador (o *crackeador*) como Crack o John the Ripper cifrará todas las palabras de un archivo denominado *diccionario*, comparando el resultado obtenido en este proceso con la clave cifrada del archivo de contraseñas; si ambos coinciden, ya ha obtenido una clave para acceder al sistema de forma no autorizada

4 Técnicas de autentificación

Parque Tecnologico
Mérida - Venezuela

- Shadow Password
- La idea básica de este mecanismo es impedir que los usuarios sin privilegios puedan leer el archivo donde se almacenan las claves cifradas. En equipos con /etc/shadow el archivo /etc/passwd sigue siendo legible para todos los usuarios, pero a diferencia del mecanismo tradicional, las claves cifradas no se guardan en él, sino en el archivo /etc/shadow, que sólo el *root* puede leer.

4 Técnicas de autentificación

- Shadow Password
- El aspecto de /etc/shadow es en cierta forma similar al de /etc/passwd que ya hemos comentado: existe una línea por cada usuario del sistema, en la que se almacena su *login* y su clave cifrada.
- Sin embargo, el resto de campos de este archivo son diferentes; corresponden a información que permite implementar otro mecanismo para proteger las claves de los usuarios.

4 Técnicas de autentificación

- Claves de un solo uso (one time password)
  - Existen dos métodos para implementar esta técnica:
    - Tokens de hardware
    - Code books

4 Técnicas de autentificación

- Sistemas de autentificación de red
  - Nis y Nis+
  - Kerberos
  - Radius
  - LDAP

4 Técnicas de autentificación

- Otras métodos de autentificación
- **PAM** (*Pluggable Authentication Module*)
  - PAM no es un modelo de autenticación en sí, sino un mecanismo que proporciona una interfaz entre las aplicaciones de usuario y diferentes métodos de autenticación, trantado de esta forma de solucionar uno de los problemas clásicos de la autenticación de usuarios: el hecho de que una vez que se ha definido e implantado cierto mecanismo en un entorno, es difícil cambiarlo.

4 Técnicas de autentificación

- Otras métodos de autentificación
- **PAM** (*Pluggable Authentication Module*)
  - Mediante PAM podemos comunicar a nuestra aplicaciones con los métodos de autenticación que deseemos de una forma transparente, lo que permite integrar las utilidades de un sistema Unix clásico (login, ftp, telnet...) con esquemas diferentes del habitual *password*: claves de un solo uso, biométricos, tarjetas inteligentes...

5 Protección de conexiones de red

- Para proteger las conexiones de red Linux puede usar herramientas y protocolos tales como tales como:
- Ssh
- Ipsec
- CIPE
- Vtun
- PKI

6 Cortafuegos de host (basico)

- Utilice políticas por omisión tales como:
  - Para iptables:
    - iptables -P INPUT DROP
    - iptables -P OUTPUT ACCEPT
    - iptables -P FORWARD DROP
  - Para ipchains:
    - ipchains -P input DENY
    - ipchains -P output ACCEPT
    - ipchains -P forward DENY

6 Cortafuegos de host (basico)

- También puede utilizar paquetes tales como:
- Firestarter
- Shorewall
- TuxFrw
- Turtle Firewall

7 IDS de target

Parque Tecnologico
Mérida - Venezuela

- Tripwire:
- El software de aseguramiento de integridad de los datos Tripwire, monitorea la consistencia de archivos y directorios de sistema críticos identificando todos los cambios hechos a ellos.
- Esto lo hace mediante un método automatizado de verificación que se ejecuta a intervalos regulares.
- Si Tripwire detecta que uno de los archivos monitoreados ha sido cambiado, lo notifica al administrador del sistema vía email. Debido a que Tripwire puede fácilmente identificar los archivos que son modificados, agregados o eliminados, se agiliza el proceso de recuperación luego de una entrada forzada pues mantiene el número de archivos que deben ser restaurados a un mínimo.

7 IDS de target

- Tripwire:
- Estas habilidades hacen de Tripwire una herramienta excelente para los administradores de sistemas que requieren tanto de facilidades para detección de intrusos como de control de daños para sus servidores.
- Tripwire compara los archivos y directorios con una base de datos de la ubicación de archivos, las fechas en que han sido modificados y otros datos. Tripwire genera la base tomando una instantánea. Esta base de datos contiene *hash*
- . Los contenidos de la base de datos de hash deberían ser generados antes de que el sistema esté en riesgo, esto es antes de que se conecte a la red.

7 IDS de target

- Tripwire:
- Después de crear la base de datos de fundamentos, Tripwire compara la base de datos actual con la base de datos de fundamentos e informa de cualquier modificación, adición o eliminación.

- Otra alternativa
  - aide

7 IDS de target

- AIDE
  - AIDE (Entorno Avanzado de Detección de Intrusiones).
  - Genera una base de datos que puede ser usada para verificar la integridad de los archivos en el servidor. Usa expresiones regulares para determinar que archivos son tomados para añadirlos a la base de datos. Puede usar una gran cantidad de algoritmos de verificación para asegurar que los archivos no han sido alterados

7 IDS de target

- AIDE
  - Se crea una base de datos a partir de una serie de reglas y expresiones regulares desde un archivo de configuración. Una vez que esta base de datos ha sido inicializada esta puede ser usada para verificar la integridad de los archivos. Usa un gran numero de algoritmos de verificación (md5,sha1,rmd160,tiger,haval,etc.) que son usados para verificar al integridad de los archivos. Todos los atributos usuales también pueden ser verificados contra inconsistencias. También puede leer archivos de bases de datos de versiones mas antiguas y nuevas

8 Pruebas y monitoreo del sistema

- Las pruebas y monitoreo del sistema debe centrarse el:
  - Logins y passwords
  - Sistemas de archivos
  - Red
  - Logs del sistema

8 Pruebas y monitoreo del sistema

- Pruebas de fortaleza de passwords
  - John the Ripper
  - Cracklib

8 Pruebas y monitoreo del sistema

- Cuentas sin password
  - Para ello revisar el archivo /etc/shadow
  - Ejemplo
  - # awk -F: '$2 =="" {print $1 “ sin password"}' /etc/shadow
  - # pedro sin password

- Cuentas de superusuario
  - Para ello revisar el archivo /etc/pasword
  - Ejemplo
  - # awk -F: '$3 ==0 {print $1 " es superuser"}' /etc/passwd
  - # root es superuser

8 Pruebas y monitoreo del sistema

- Usuarios que se han entrado al sistema
  - Para esto usar el comando:
    - # Lastlog
  - También se puede revisar los últimos acceso de red mediante el comando:
    - # tail /var/log/secure

8 Pruebas y monitoreo del sistema

- Sistemas de archivos
  - Estandarizar el uso de los IDS de target tales como los ya mencionados
  - Para encontrar archivos con permisos de escritura para todos:
    - # find / -xdev -perm +o=w ! \(-type d -perm +o=t \) ! -type l -print

8 Pruebas y monitoreo del sistema

- Sistemas de archivos
  - **Búsqueda de rootkits**
  - Para esto se puede utilizar herramientas tales como
  - Chkrootkit

    - Chkrootkit : es un shell script que busca en nuestro sistema binarios modificados por esos root kits usados por los hakers para comprometer sistemas.

8 Pruebas y monitoreo del sistema

- Red
  - Búsqueda de puertos en escucha:
    - Usar el netstat
    - Usar herramientas tales como nmap
      - Ejemplo
      - nmap -v -sV localhost

8 Pruebas y monitoreo del sistema

- Red
  - Utilizar herramientas observar las conexiones de red tales como:
    - Tcpdump
    - Ethereal
  - Revisar periódicamente si alguno de los servicios de red acepta contraseñas planas:
    - Para capturar las mismas podemos usar dsniff

8 Pruebas y monitoreo del sistema

- Red
  - Utilice un detector de intruso de red tal como
  - SNORT

  - Utilice herramientas tales como Nessus para revisar sus servicios de red en búsqueda de vulnerabilidades.

8 Pruebas y monitoreo del sistema

- Logs del sistema
  - Revise periódicamente el funcionamiento de los logs del sistema, y el sistema de rotado de los mismos.
  - Para faciltar la vizalisuacion de los mismo puede usar herramientas tales como logwatch.
    - Ejemplo:
    - # logwatch --range all --print | less

FIN

Parque Tecnologico
Mérida - Venezuela

Esto es solo una visíon básica!!