

# Seguridad Informática Gnu/Linux

Ing. Ricardo Naranjo Faccini M.Sc  
soporte@skinait.com



<https://www.skinait.com/seguridad-informatica-en-linux-Escritos-55/>

# Seguridad Informática Gnu/Linux

- Manizales  
IV Congreso Internacional de Software Libre  
Marzo 2005
- Bogotá  
Universidad Autonoma  
Septiembre 25 2002
- Bogotá  
Instituto Politécnico Grancolombiano  
Marzo 30 2001

**RIESGO = AMENAZA \* VULNERABILIDAD**

$$\frac{\textit{Funcionalidad}}{\textit{Seguridad}} \Leftrightarrow \frac{\textit{Costo}}{\textit{Beneficio}}$$

# Cartilla: Juanito conoce su equipo

- **Cada proceso tiene su usuario**
  - top, ps - feauxw
- **Cada dispositivo tiene un archivo asociado**
  - /proc/
- **Cada servicio es un proceso y tiene un puerto asignado**
  - 21 ftp                      22 ssh
  - 443 https                  25 smtp
- **Cada equipo tiene su dirección**
  - 127.0.0.1
  - 255.255.255.255
  - 0.0.0.0

- **Una simple bitácora descifra un ataque.**
- **El reto: Escoger cuales eventos se van a registrar.**
- **¡¡¡HAY QUE PROTEGER LA BITACORA!!!**
- **El arte del monitoreo es el análisis de estos datos para reconstruir la escena del crimen y ubicar los culpables.**
- **El primer objetivo de un Cracker es la bitácora del sistema.**

- **syslog**

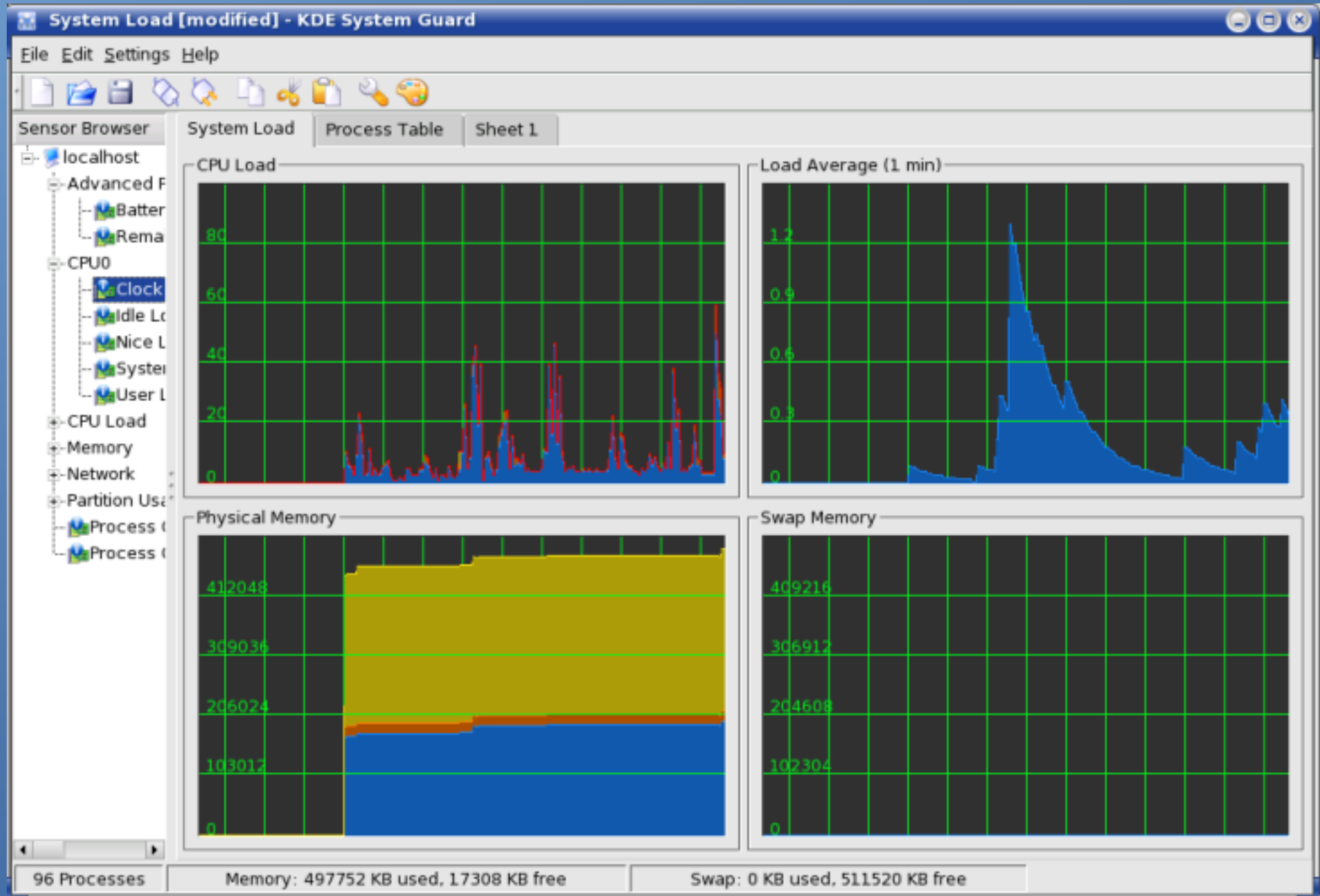
- `/etc/syslog.conf`
- Maneja eventos del kernel, de autenticación y otros.
- Puede almacenar la bitácora remotamente:
  - `.debug @loghost`

- **Mínimo a registrar**

- Intentos de autenticación (entradas, salidas e interfaces externas)
- Intentos de acceso a archivos o dispositivos de seguridad o críticos
- Fallos en la comunicación
- Acciones del administrador de la máquina y de la seguridad
- Activación y desactivación de las funciones de seguridad
- Anomalías de integridad del sistema



# Monitores del sistema: ksysguard (ojo: no hay que descargarlo)





# Monitores del sistema: ksysguardd

Personalizada [modified] - KDE System Guard

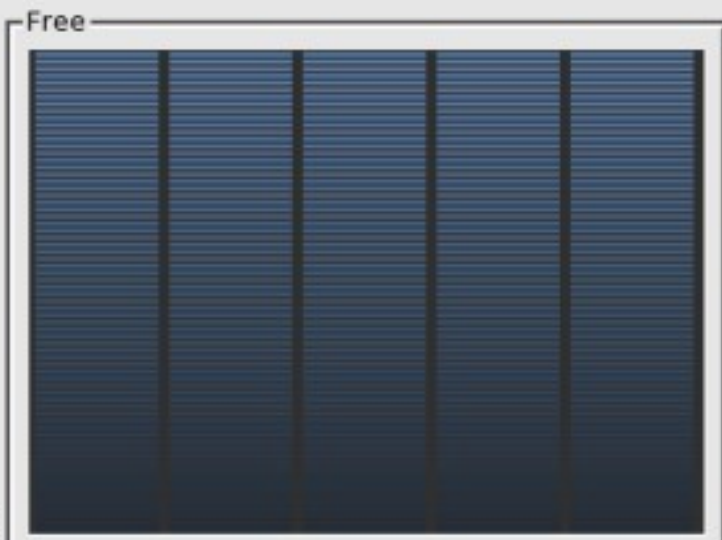
File Edit Settings Help

Sensor Browser    Sensor Type

- System Load Integer Value
- User Load Integer Value
- Memory
  - Physical Memory
    - Application Memory Integer Value
    - Buffered Memory Integer Value
    - Cached Memory Integer Value
    - Free Memory Integer Value
    - Used Memory Integer Value
  - Swap Memory
    - Free Memory Integer Value
    - Used Memory Integer Value
- Network
- Partition Usage
  - home
  - mnt
  - proc
  - root
  - System Load
    - Fill Level Integer Value
    - Free Space Integer Value
    - Used Space Integer Value
  - usr
  - Process Controller Process Count
  - Process Count Integer Value

System Load    Process Table    Personalizada

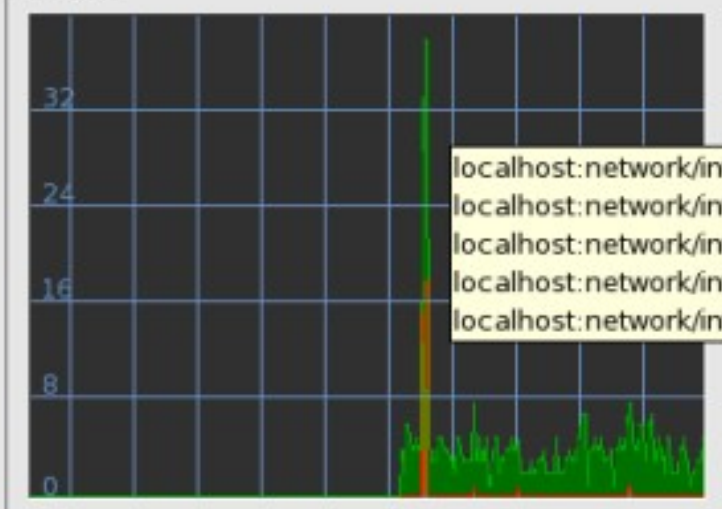
Free



Process

Name	PID	PPID	UID	GID	Status	Us
kio_file	3774	3636	501	3636	sleeping	
kysysguardd	3773	3713	501	3712	running	
tcssh	3713	3712	501	3712	sleeping	
kysysguard	3712	1	501	3712	sleeping	
knotify	3709	1	501	3636	sleeping	
kded	3643	1	501	3636	sleeping	

Errors



Table

Blocks	Used	Available	Used	MountPoint
/	292912	82498	210414	28 /root
/	715214	674872	40342	94 /home
			58	/usr
			17	/mnt/win_d
			27	/mnt/win_c
			21	/proc/bus/usb
	0	0	0	-21 /proc/sys/fs/bin
	0	0	0	-21 /sys

98 Processes    Memory: 507820 KB used, 7240 KB free    Swap: 0 KB used, 511520 KB free

# Monitores del sistema: gnome-system-log

**/var/log/messages - Sistema de visualización de bitácora**

Archivo	Ver	Ayuda	
a	Nombre del host	Proceso	Mensaje
10:39:29	elmbtapmnov	ntpd[2052	synchronized to LOCAL(0), stratum=10
10:39:29	elmbtapmnov	ntpd[2052	kernel time sync disabled 0041
10:39:30	elmbtapmnov	su(pam_ur	session closed for user root
10:40:33	elmbtapmnov	ntpd[2052	kernel time sync enabled 0001
10:41:49	elmbtapmnov	nmbd[270	[2005/03/15 10:41:49, 0] nmbd/nmbd_become_lmb.c:become_local_master_
10:41:49	elmbtapmnov	nmbd[270	*****
10:41:49	elmbtapmnov	nmbd[270	
10:41:49	elmbtapmnov	nmbd[270	Samba name server ELMBTAPMNOV is now a local master browser for workg
10:41:49	elmbtapmnov	nmbd[270	
10:41:49	elmbtapmnov	nmbd[270	*****
10:57:48	elmbtapmnov	kernel	ethereal uses obsolete (PF_INET,SOCK_PACKET)
11:01:00	elmbtapmnov	CROND[35	(root) CMD (nice -n 19 run-parts /etc/cron.hourly)
11:01:01	elmbtapmnov	msec	set variable ShowUsers to All in /usr/share/config/kdm/kdmrc
11:01:01	elmbtapmnov	msec	changed mode of /var/log/cups/error_log from 644 to 640
11:01:01	elmbtapmnov	msec	changed mode of /var/log/wtmp from 664 to 640
11:01:01	elmbtapmnov	msec	changed group of /var/log/wtmp from utmp to adm
11:01:01	elmbtapmnov	msec	changed mode of /var/log/XFree86.0.log from 644 to 640
11:01:01	elmbtapmnov	msec	changed group of /var/log/XFree86.0.log from root to adm
11:01:01	elmbtapmnov	msec	changed mode of /var/log/ksyms.0 from 644 to 640
11:01:01	elmbtapmnov	msec	changed group of /var/log/ksyms.0 from root to adm

Última modificación: 15/03/05

# y... ¿si necesito automatizar el monitoreo de mi equipo?



- **SWATCH**

- The Simple WATCHer and filter
- Escrito en Perl
- Análisis EN VIVO
- Envía mensajes al administrador

## Bitácora de procesos

- Registrar la ejecución de cada proceso
  - /var/log/wtmp
  - /var/log/lastlog
- Registra el día, hora, duración y lugar desde donde se invocó el proceso (terminal o IP)
- Segundo punto de ataque de un Cracker (tanto para borrar como para modificar)



## Bitácora de procesos

- ¿CÓMO HABILITARLA?
- Compilar el kernel con `CONFIG_BSD_PROCESS_ACCT` habilitada
- Instalar psacct
  - `accton /var/log/psacct`
- Dar los permisos de lectura únicamente a root

## Bitácora de procesos

- HERRAMIENTAS:
- lastlog: accesos de usuarios.
- last: última vez que un usuario ingresó al sistema.
- lastcomm: comando, terminal, nombre de usuario y duracion

- **Auditoría del sistema**

- Notar cambios en la integridad del sistema
- Primer paso: ESTABLECER LINEA BASE
- Definir la periodicidad de la auditoría
- Definir la lista ordenada de comparaciones con la línea base



- **Consideraciones para la Auditoría**

- Conocer las horas normales de trabajo de cada usuario
- Ubicar las horas "pico" y laxas de carga del sistema
- Revisar el estado, permisos y propietario de archivos claves del sistema
- Verificar los archivos de configuración y ejecutables importantes para el sistema

- **Virtudes del auditor**

- Regularidad
- Consistencia
- Minuciosidad
- Respeto ante la contraparte

☐ **La complacencia es la aliada del intruso.**

- **NMAP**

- Para revisar puertos.
- Previene los Troyanos.
- Genera huellas digitales

- **Wireshark**

- Scanner de tráfico  
**USAR UNICAMENTE  
CON AUTORIZACIÓN**

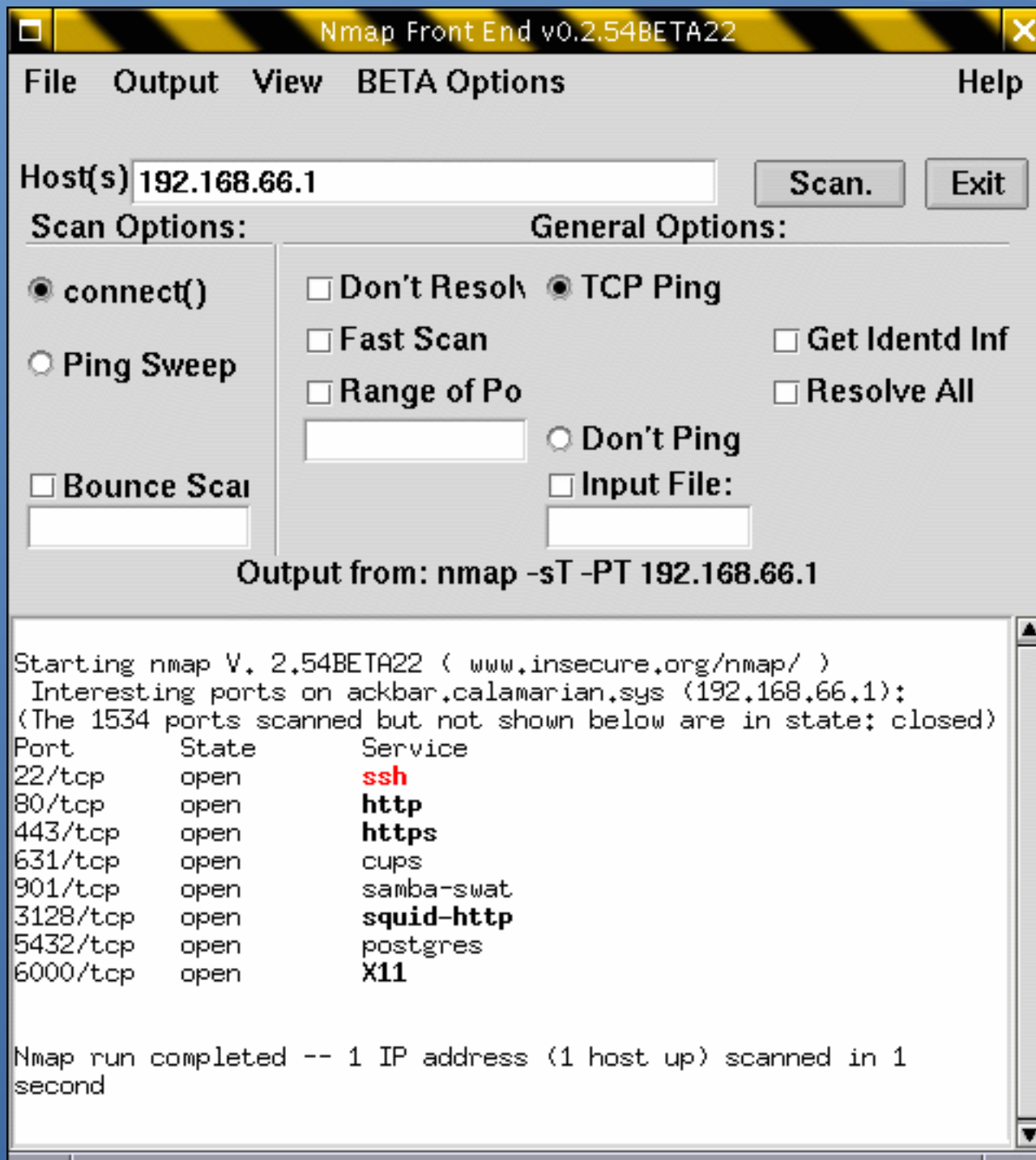
- **IPTRAF**

- Genera estadísticas del uso de la red.
- Registra:  
Protocolos,  
interface y conteo de bytes.

- **MRTG**

- Registro de tráfico

# Auditoría del sistema: NMAP



Nmap Front End v0.2.54BETA22

File Output View BETA Options Help

Host(s) 192.168.66.1 Scan. Exit

Scan Options: General Options:

connect()  Don't Resolve  TCP Ping

Ping Sweep  Fast Scan  Get Identd Inf

Bounce Scan  Range of Po  Resolve All

Don't Ping  Input File:

Output from: nmap -sT -PT 192.168.66.1

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on ackbar.calamarian.sys (192.168.66.1):
(The 1534 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open       ssh
80/tcp    open       http
443/tcp   open       https
631/tcp   open       cups
901/tcp   open       samba-swat
3128/tcp  open       squid-http
5432/tcp  open       postgres
6000/tcp  open       X11

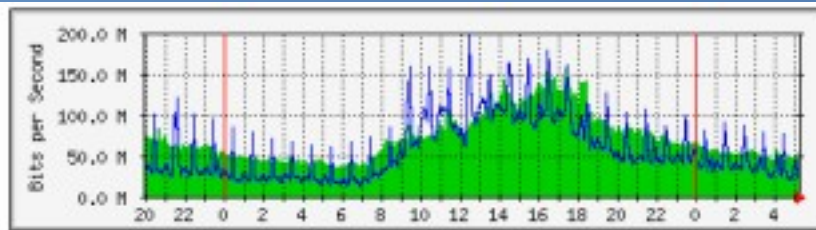
Nmap run completed -- 1 IP address (1 host up) scanned in 1
second
```

# Auditoría del sistema: IPTRAF

```
root@ackbar.calamarian.sys: /root X
IPTraf
TCP Connections (Source Host:Port) ----- Packets ----- Bytes Flags Iface
192.168.66.1:22 > 3308 1515992 -PA- eth0
192.168.8.1:33963 > 3391 1187212 --A- eth0
192.168.8.1:34337 > 5858 4545724 -PA- eth0
192.168.8.121:6000 > 3475 236296 -PA- eth0
192.168.8.1:33564 > 404 350160 -PA- eth0
192.168.8.122:6000 > 404 21008 --A- eth0
192.168.8.1:33901 > 406 26000 -PA- eth0
192.168.8.121:6000 > 405 25380 --A- eth0
192.168.8.1:33568 > 270 15120 --A- eth0
192.168.8.122:6000 > 135 11340 -PA- eth0
192.168.8.1:33561 > 54 3024 --A- eth0
192.168.8.122:6000 > 27 2268 -PA- eth0
TCP: 12 entries Active
UDP (332 bytes) from 200.85.235.1:67 to 255.255.255.255:68 on eth1
UDP (332 bytes) from 200.85.232.1:67 to 255.255.255.255:68 on eth1
UDP (153 bytes) from 200.85.232.98:631 to 200.85.232.255:631 on eth1
UDP (153 bytes) from 200.85.232.98:631 to 200.85.232.255:631 on eth1
UDP (137 bytes) from 200.85.232.98:631 to 200.85.232.255:631 on eth1
Bottom ----- Elapsed time: 0:02
Pkts captured (all interfaces): 21244 TCP flow rate: 150.00 kbits/s
Up/Dn/PgUp/PgDn-scroll M-more TCP info M-chg actv win S-sort TCP X-exit
```



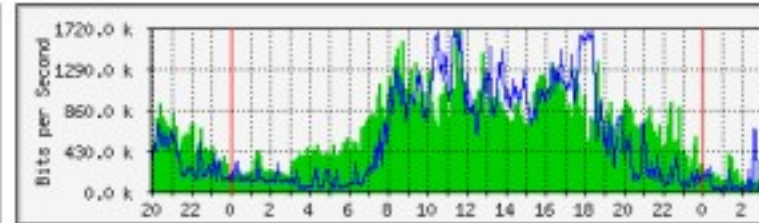
# Auditoría del sistema: MRTG



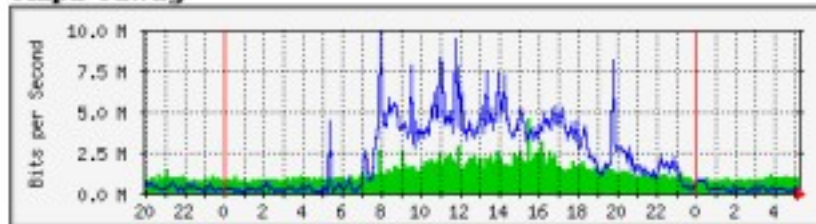
**vpn-cablecom**



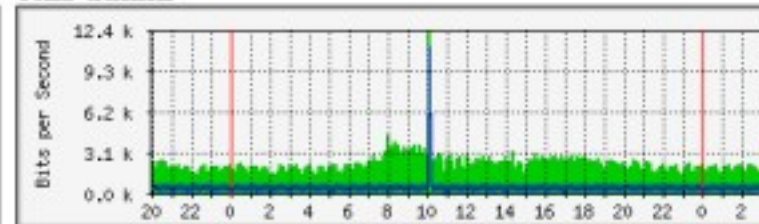
**rz-wsl**



**empa-eawag**



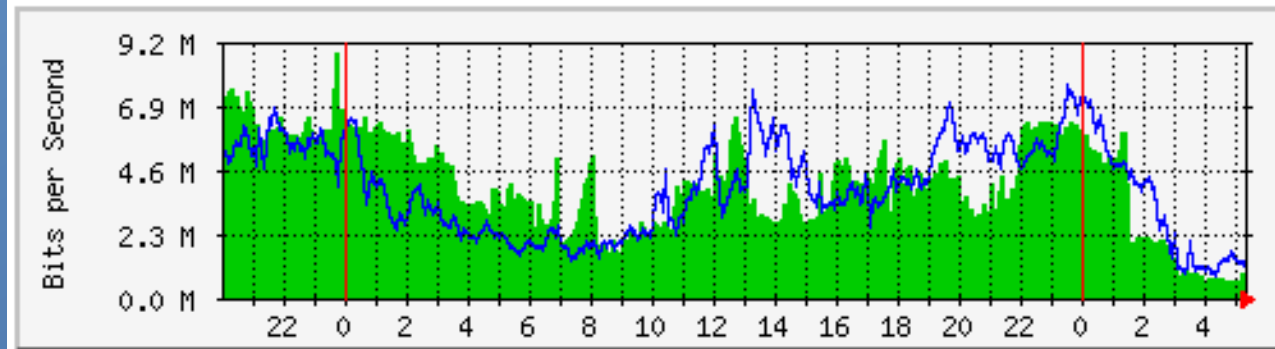
**ethz-admin**



# Auditoría del sistema: MRTG

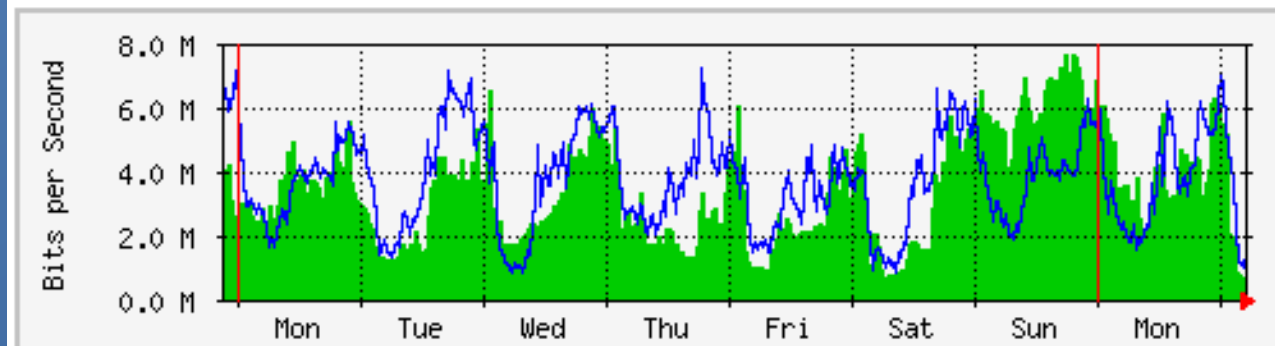
The statistics were last updated **Tuesday, 15 March 2005 at 5:20**, at which time '**rou-rz-gw.ethz.ch**' had been up for **70 days, 15:30:20**.

## `Daily' Graph (5 Minute Average)



Max **In**:8826.2 kb/s (8.8%) Average **In**:4012.4 kb/s (4.0%) Current **In**:573.5 kb/s (0.6%)  
Max **Out**:7562.3 kb/s (7.6%) Average **Out**:3893.3 kb/s (3.9%) Current **Out**:835.6 kb/s (0.8%)

## `Weekly' Graph (30 Minute Average)



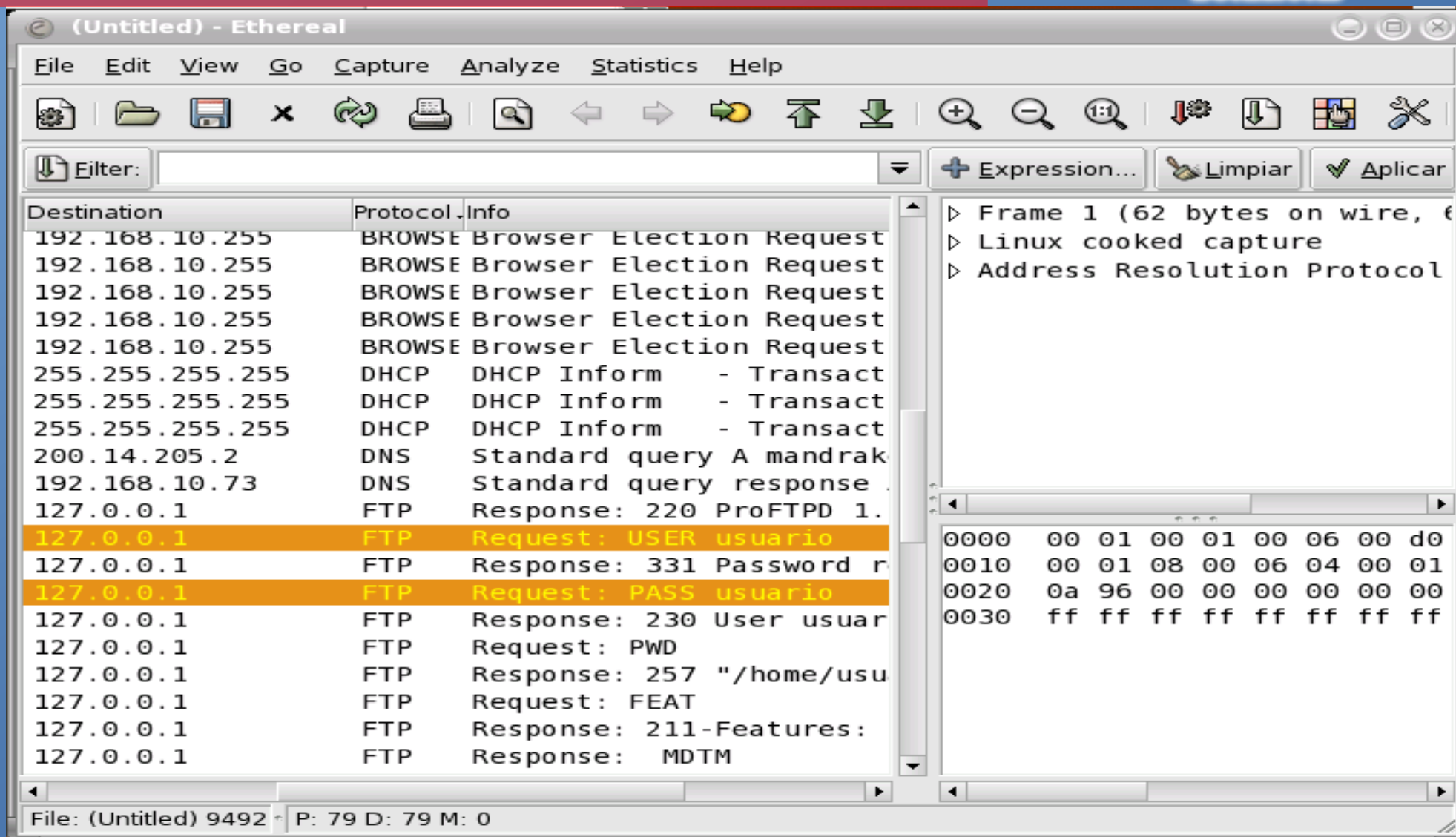
Max **In**:7628.7 kb/s (7.6%) Average **In**:3376.7 kb/s (3.4%) Current **In**:629.0 kb/s (0.6%)  
Max **Out**:7134.1 kb/s (7.1%) Average **Out**:3704.0 kb/s (3.7%) Current **Out**:1388.9 kb/s (1.4%)

## `Monthly' Graph (2 Hour Average)





# Auditoría del sistema: Wireshark (solo con autorización)



(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter:  + Expression... Limpiar Aplicar

Destination	Protocol	Info
192.168.10.255	BROWSE	Browser Election Request
192.168.10.255	BROWSE	Browser Election Request
192.168.10.255	BROWSE	Browser Election Request
192.168.10.255	BROWSE	Browser Election Request
192.168.10.255	BROWSE	Browser Election Request
255.255.255.255	DHCP	DHCP Inform - Transact
255.255.255.255	DHCP	DHCP Inform - Transact
255.255.255.255	DHCP	DHCP Inform - Transact
200.14.205.2	DNS	Standard query A mandrak
192.168.10.73	DNS	Standard query response
127.0.0.1	FTP	Response: 220 ProFTPD 1.
127.0.0.1	FTP	Request: USER usuario
127.0.0.1	FTP	Response: 331 Password r
127.0.0.1	FTP	Request: PASS usuario
127.0.0.1	FTP	Response: 230 User usuar
127.0.0.1	FTP	Request: PWD
127.0.0.1	FTP	Response: 257 "/home/usu
127.0.0.1	FTP	Request: FEAT
127.0.0.1	FTP	Response: 211-Features:
127.0.0.1	FTP	Response: MDTM

▶ Frame 1 (62 bytes on wire, 62 bytes captured) on interface eth0  
▶ Linux cooked capture  
▶ Address Resolution Protocol

```
0000  00 01 00 01 00 06 00 d0
0010  00 01 08 00 06 04 00 01
0020  0a 96 00 00 00 00 00 00
0030  ff ff ff ff ff ff ff ff
```

File: (Untitled) 9492 P: 79 D: 79 M: 0



Trash

Password required for usuario.

Password: \*\*\*\*\*)

User usuario logged in.

Logged in to localhost.

ncftp /home/usuario >

# Chequeo de Integridad del Sistema

- Hay que asegurar que los programas que ejecuto no tengan puertas traseras.
- RPM
  - un ejemplo de chequeo de integridad (checksum)
- Md5sum
  - Generador de huellas digitales.  
md5sum paquete-version.release.i386.rpm  
realiza chequeo de integridad.
- Tripwire
  - chequea la integridad de archivos importantes basandose en checksums.

- **NIDS: Network Intrusion Detection System.**
  - Detecta flujos anómalos, inapropiados o no autorizados en la red.
  - A diferencia del firewall captura y analiza TODO tráfico en la red.
- **SNORT: un ejemplo liviano de NIDS.**
  - Detecta mas de 1000 vulnerabilidades del sistema.
  - Excelente solución para pequeñas redes TCP/IP.

- **¿Que hacer al detectar?**

- La pronta solución a esta pregunta es clave para la solución e investigación del problema.
- La respuesta depende del riesgo que esté dispuesto a tomar

- **Modificar estado a modo monousuario (Desconectándose de la red)**
- **Generar una copia de todo archivo que no haga parte de la instalación básica del OS.**
- **Si es posible generar una copia de TODO el sistema o, por lo menos, de los archivos de bitácora.**
- **Realizar una reinstalación completa del sistema desde los medios originales.**

**¿Preguntas?**  
**soporte@skinait.com**  
**<http://www.skinait.com>**

Seguridad informática Gnu/Linux por Ricardo Naranjo Faccini se distribuye bajo una Licencia Creative Commons Atribución 4.0 Internacional.

<https://www.skinait.com/seguridad-informatica-en-linux-Escritos-55/>