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

Ecuaciones básicas para hablar de Seguridad

RIESGO = AMENAZA * VULNERABILIDAD

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

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`

La bitácora del sistema

- **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.**

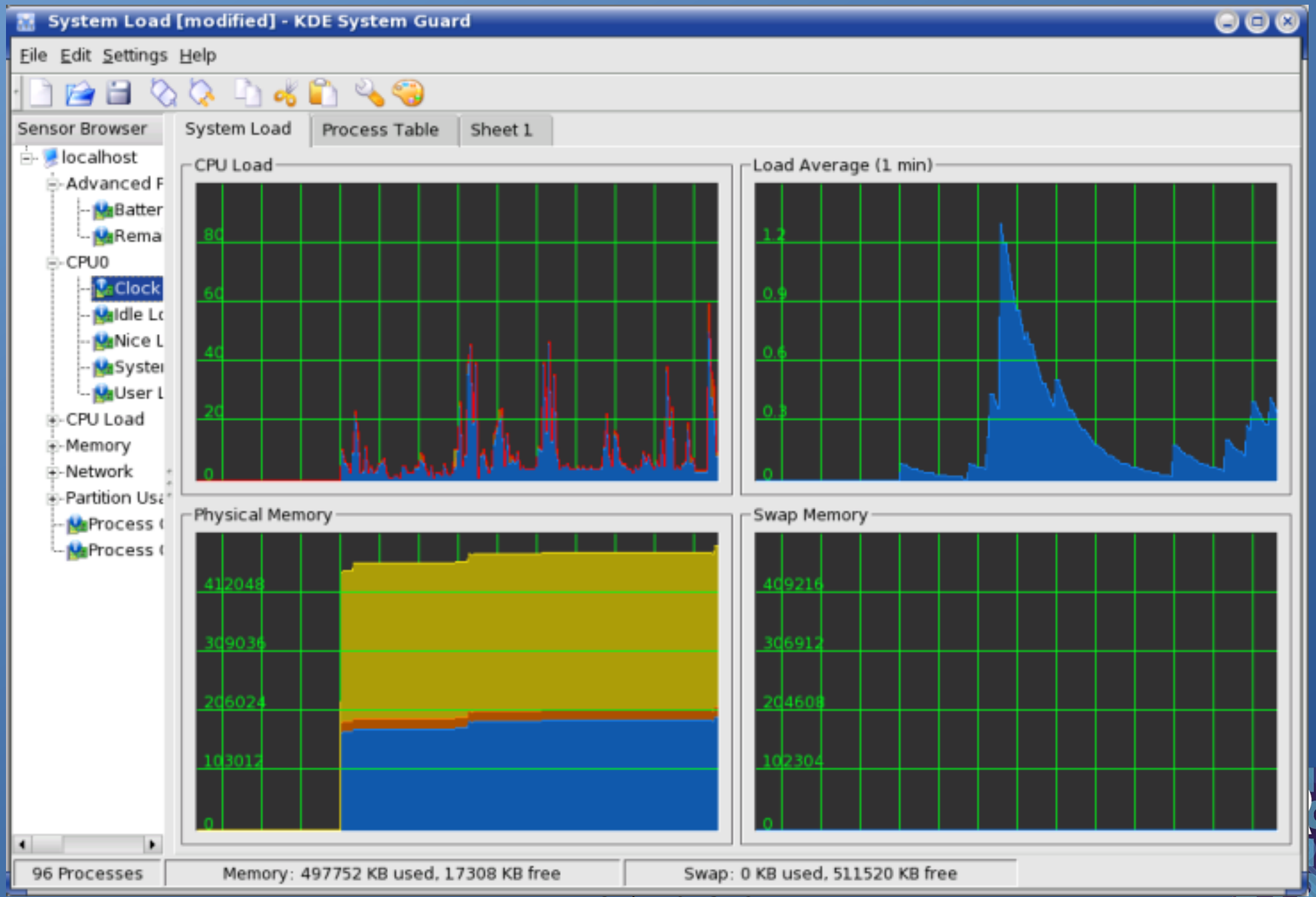
La bitácora del sistema

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

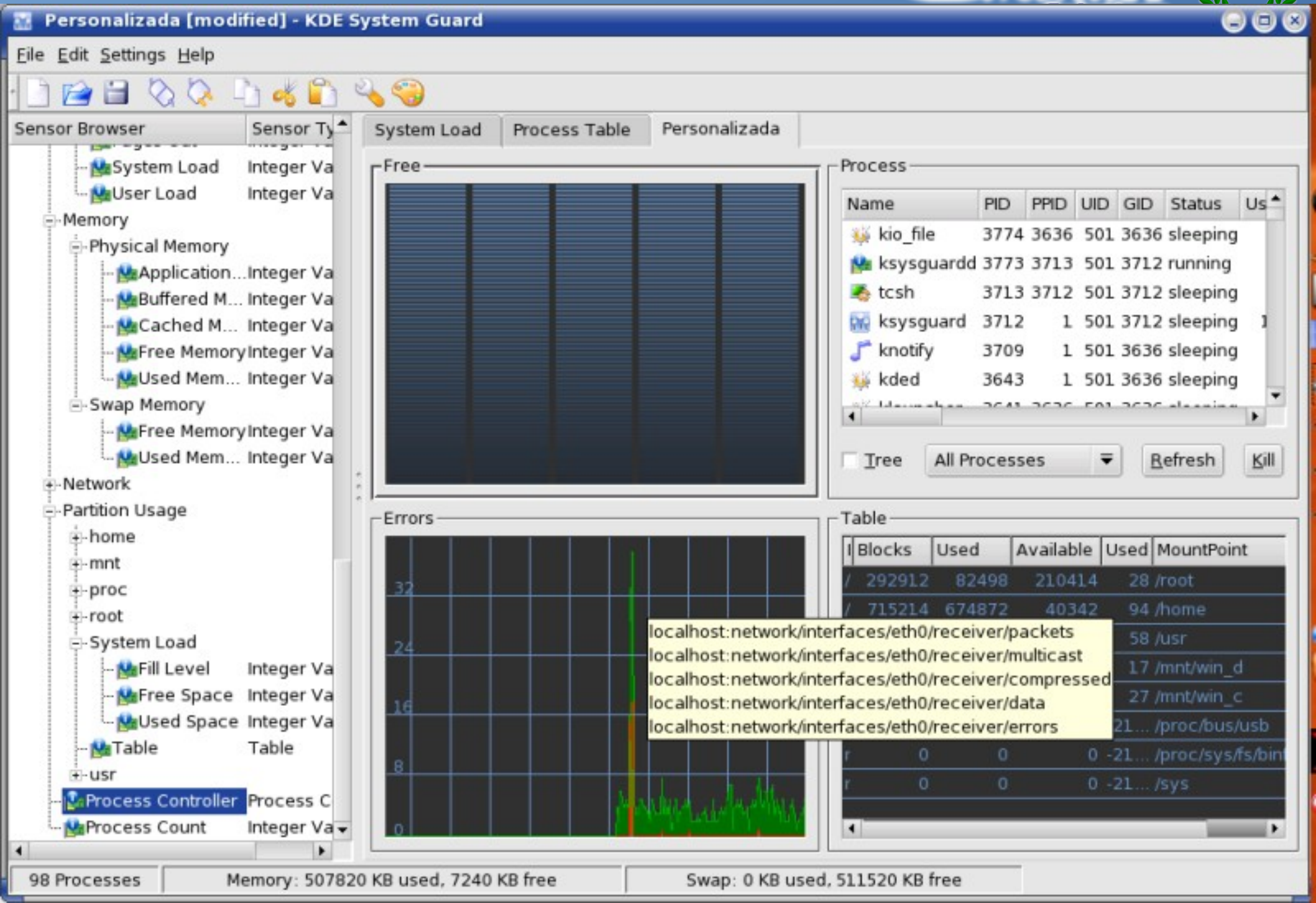
La bitácora del sistema

- **Mínimo a registrar**
  - Intentos de autenticación (entradas, salidas e interfases 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
  - Anomalias de integridad del sistema

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



Monitores del sistema: ksysguardd



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

La mejor defensa: el conocimiento

- **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

Auditoría del sistema

- **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

Auditoría del sistema

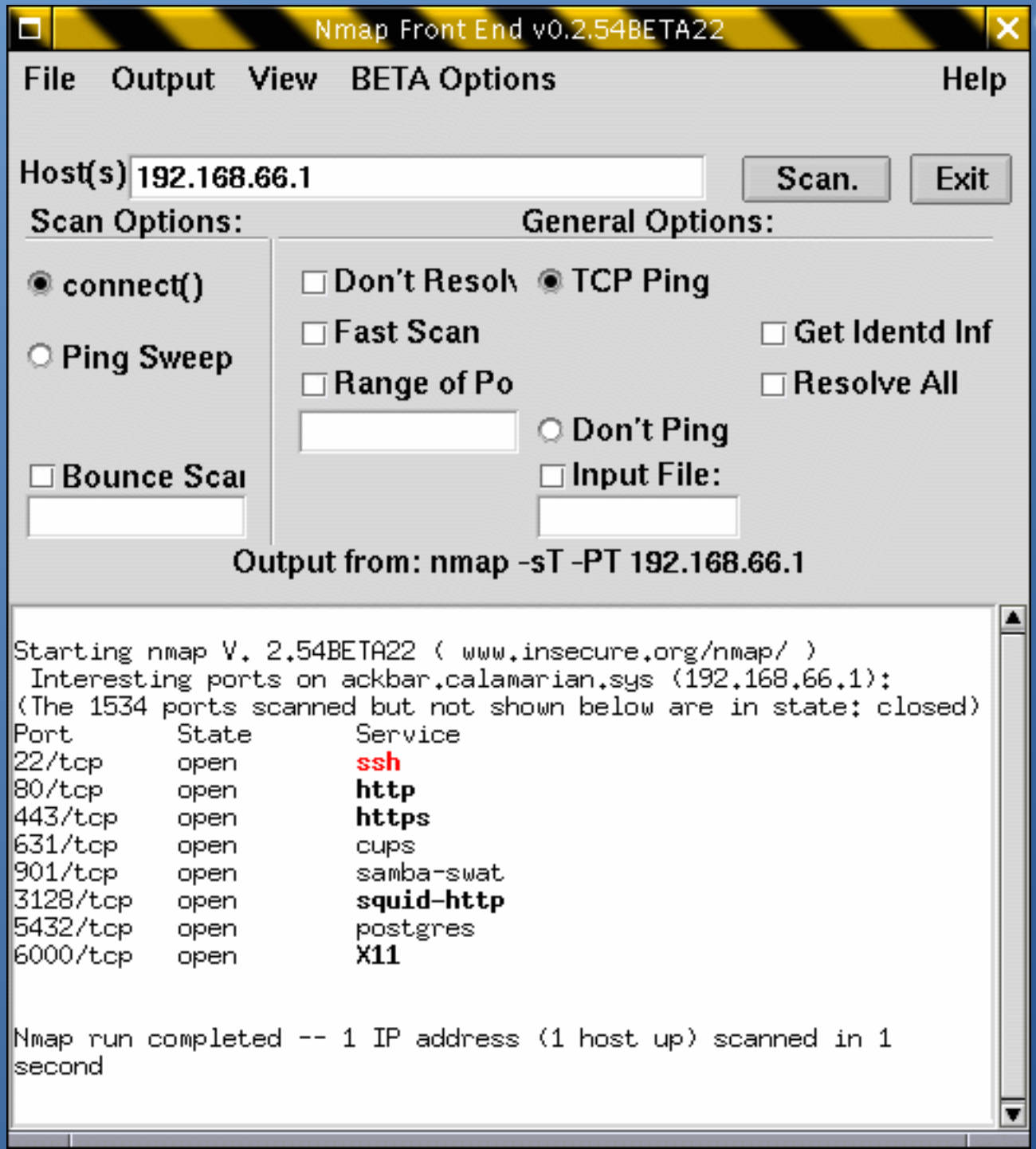
- **Virtudes del auditor**
  - Regularidad
  - Consistencia
  - Minuciosidad
  - Respeto ante la contraparte

La complacencia es la aliada del intruso.

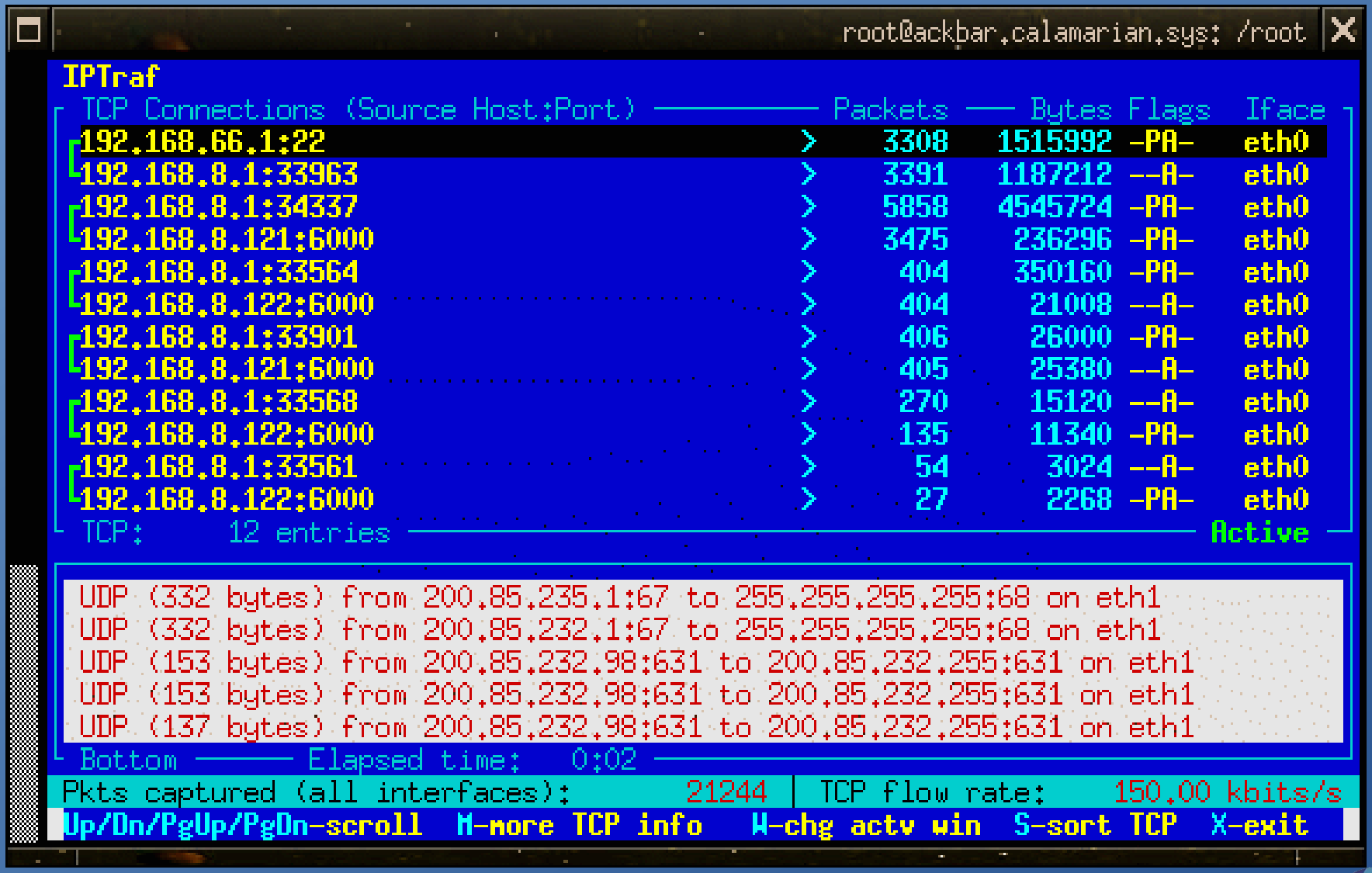
Auditoría del sistema

- **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

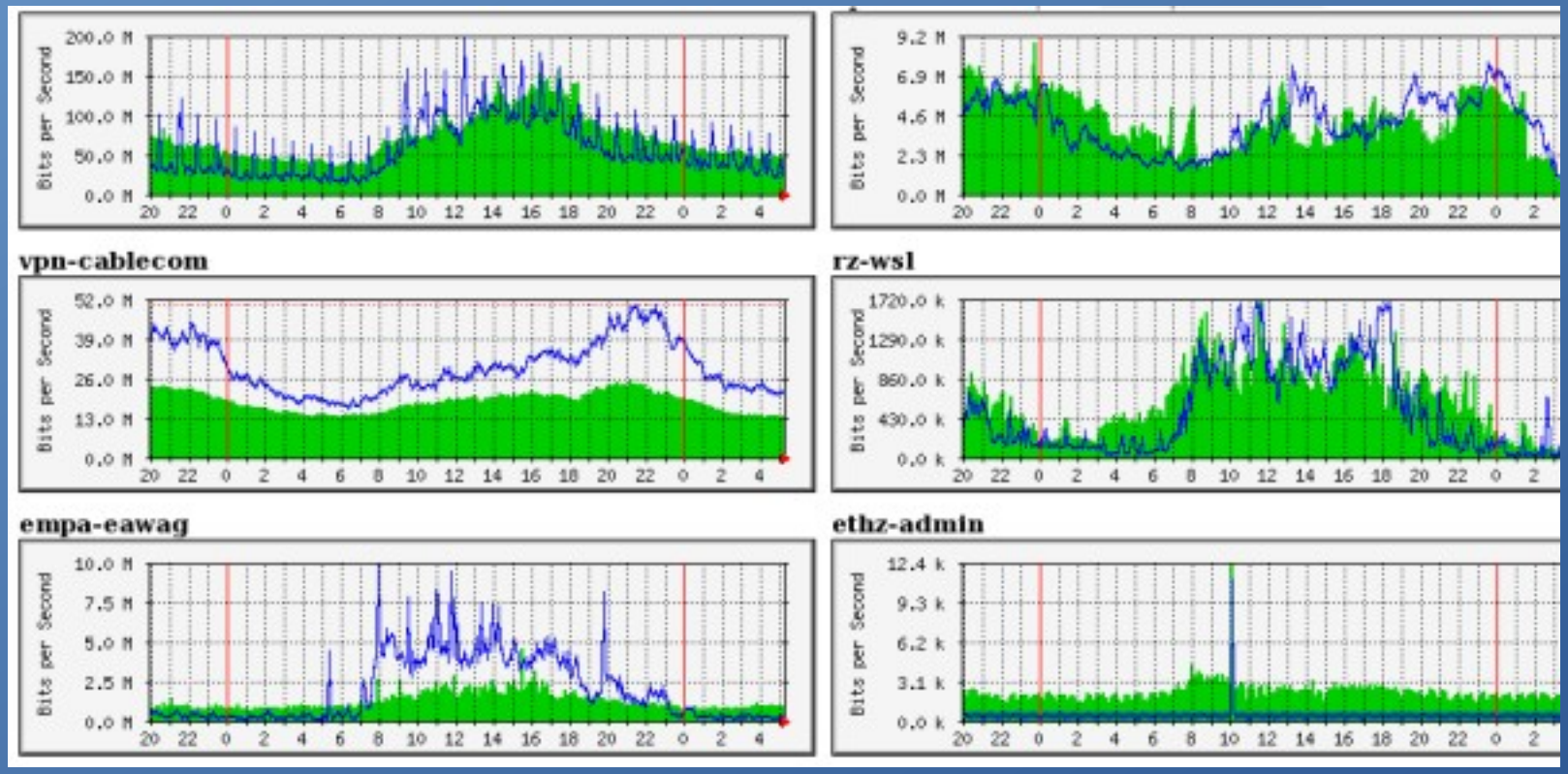
Auditoría del sistema: NMAP



Auditoría del sistema: IPTRAF



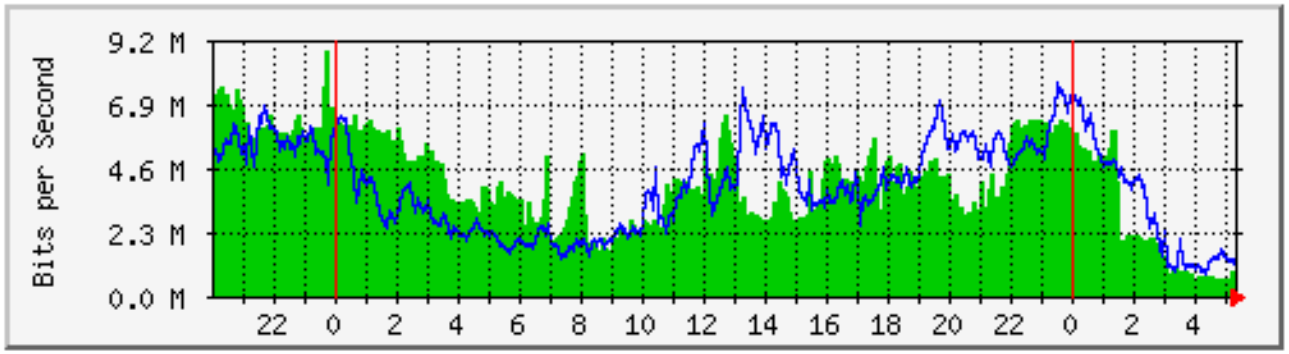
Auditoría del sistema: MRTG



Auditoría del sistema: MRTG

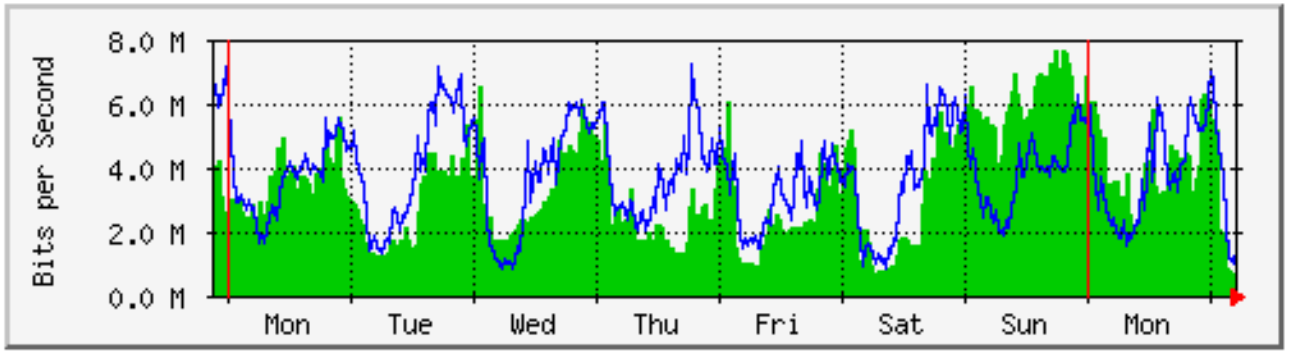
The statistics were last updated **Tuesday, 15 March 2005 at 5:20**, at which time **'rou-rz-gw.ethz.ch'** had been up for **70 days, 15:30:20**.

`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%)

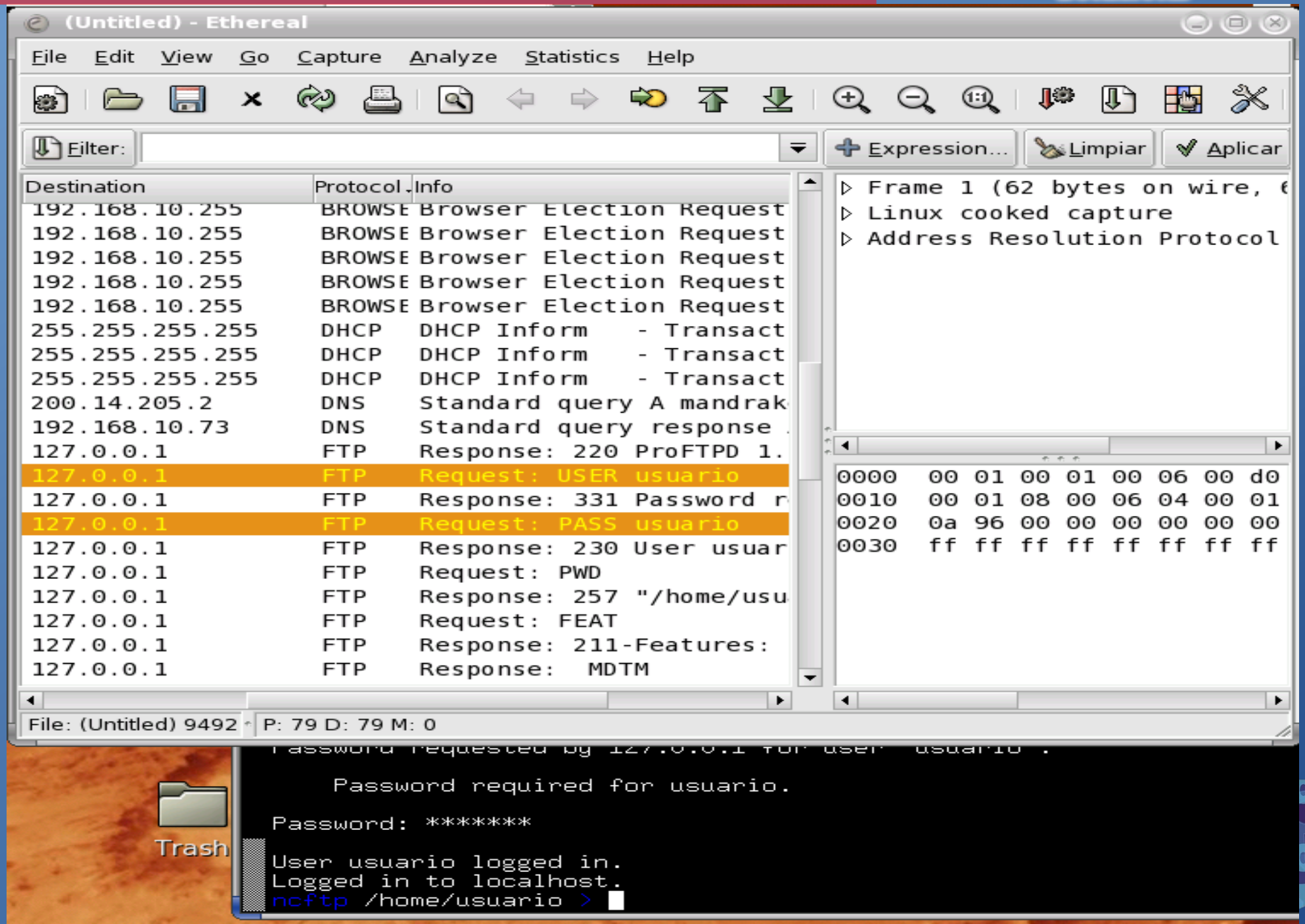
`Weekly' Graph (30 Minute Average)



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)



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.

Detección de intrusos

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

Detección de intrusos

- **¿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

Detección de intrusos

- **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