Seguridad y Hardening en Servidores Linux

Alex Callejas
Technical Account Manager
Noviembre 2014

redhat.

Agenda

- Qué queremos proteger?
- Instalación endurecida
- Post instalación
- Administración segura del sistema
- Control de acceso
- Servicios seguros
- Preparandónos para el desastre

Qué queremos proteger?


Instalación Endurecida
donde todo comienza!

Seguridad física y control de acceso

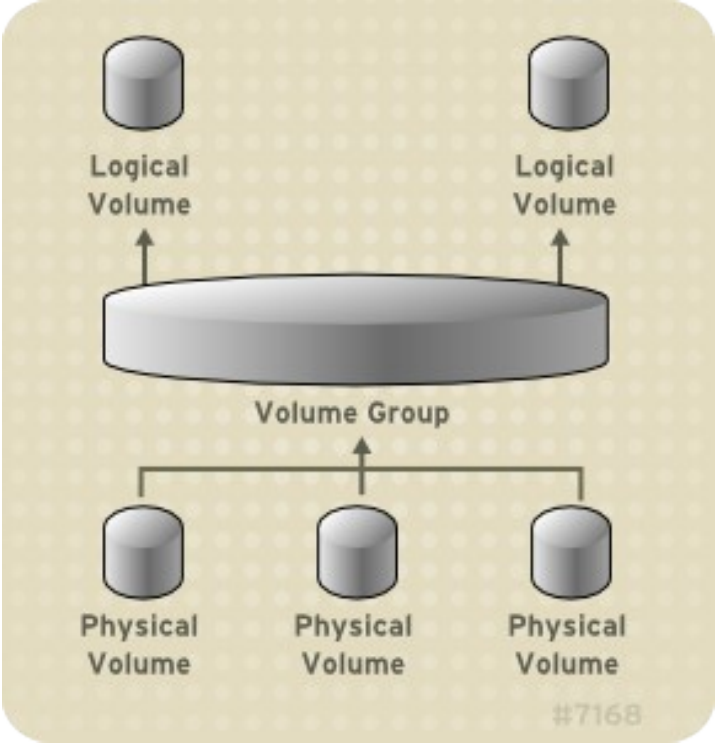
- Si existe acceso físico al equipo, tenemos un punto crítico de falla
- Acceso al servidor
  - Rack
  - Acceso físico y control de acceso
- Proteger el BIOS/UEFI
  - Prevención de modificaciones
  - Evita el boot no autorizado
- Deshabilitar periféricos no utilizados
- Fuentes redundantes
- RAID

Instalación: Mejores prácticas

- Tipo de instalación
  - Minimal/Basic
- Particionamiento
  - Planeación
    - Reduce el tiempo de acceso a datos
    - Facilita la recuperación ante desastres
    - Minimiza los problemas por disponibilidad de espacio en disco
- Swap
  - Analizar el caso de uso

Instalación: Mejores prácticas

- **Use LVM!**
  - A demanda
- `/boot`
  - kernel, GRUB
  - Sin encripción
  - Contraseña en GRUB
- `/home`
  - Sólo datos de usuario
- `/var/tmp` y `/tmp`
  - Archivos temporales
  - No se almacenan durante un largo periodo



Post Instalación

Ya puedo entrar en producción?

Actualización del Sistema

- Actualización completa del sistema
  - `yum update`
- Revisión de erratas
  - `yum check-update --security`
- Instalación de erratas
  - `yum update --security`

Prevenir combinación de reinicio

```
[root@server ~]# cp /etc/init/control-alt-delete.conf
/etc/init/control-alt-delete.override
[root@server ~]# vi /etc/init/control-alt-
delete.override
...
exec /bin/true
[root@server ~]#
```

Limitar información sobre el equipo

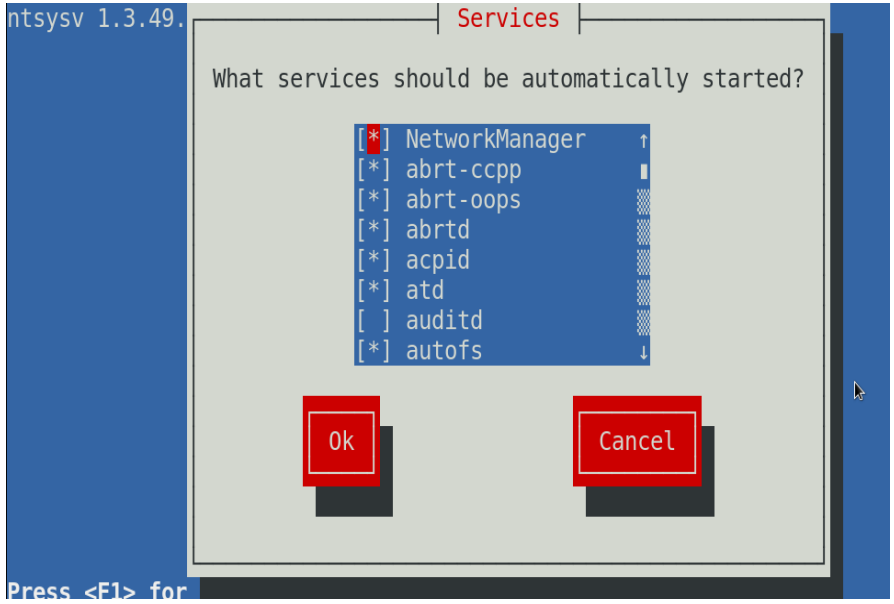
- Modificar /etc/banner y /etc/banner.issue

```
Este sistema es para el uso exclusivo de usuarios
autorizados, por lo que las personas que lo
utilicen estarán sujetos al monitoreo de todas
sus actividades en el mismo. Cualquier persona
que utilice este sistema permite expresamente tal
monitoreo y debe estar consciente de que si este
revelara una posible actividad ilicita, el
personal de sistemas proporcionara la evidencia
del monitoreo al personal de seguridad, con el
fin de emprender las acciones civiles y/o legales
que correspondan.
```

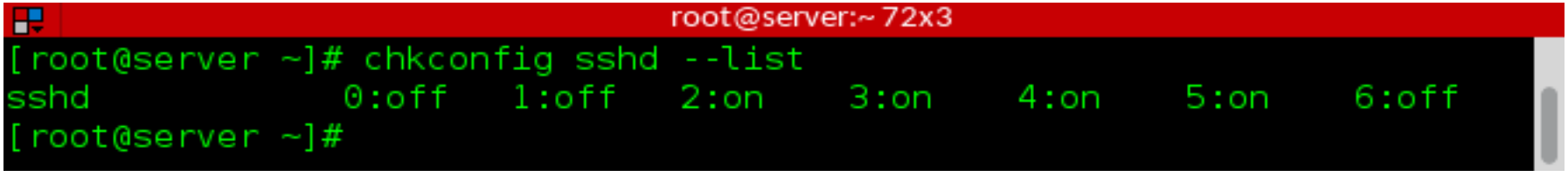
- /etc/motd
  - Política de uso de información y del sistema

Servicios: Cuáles deben estar activos?

- Sólo los necesarios!
  - ntsysv
  - chkconfig
  - systemctl

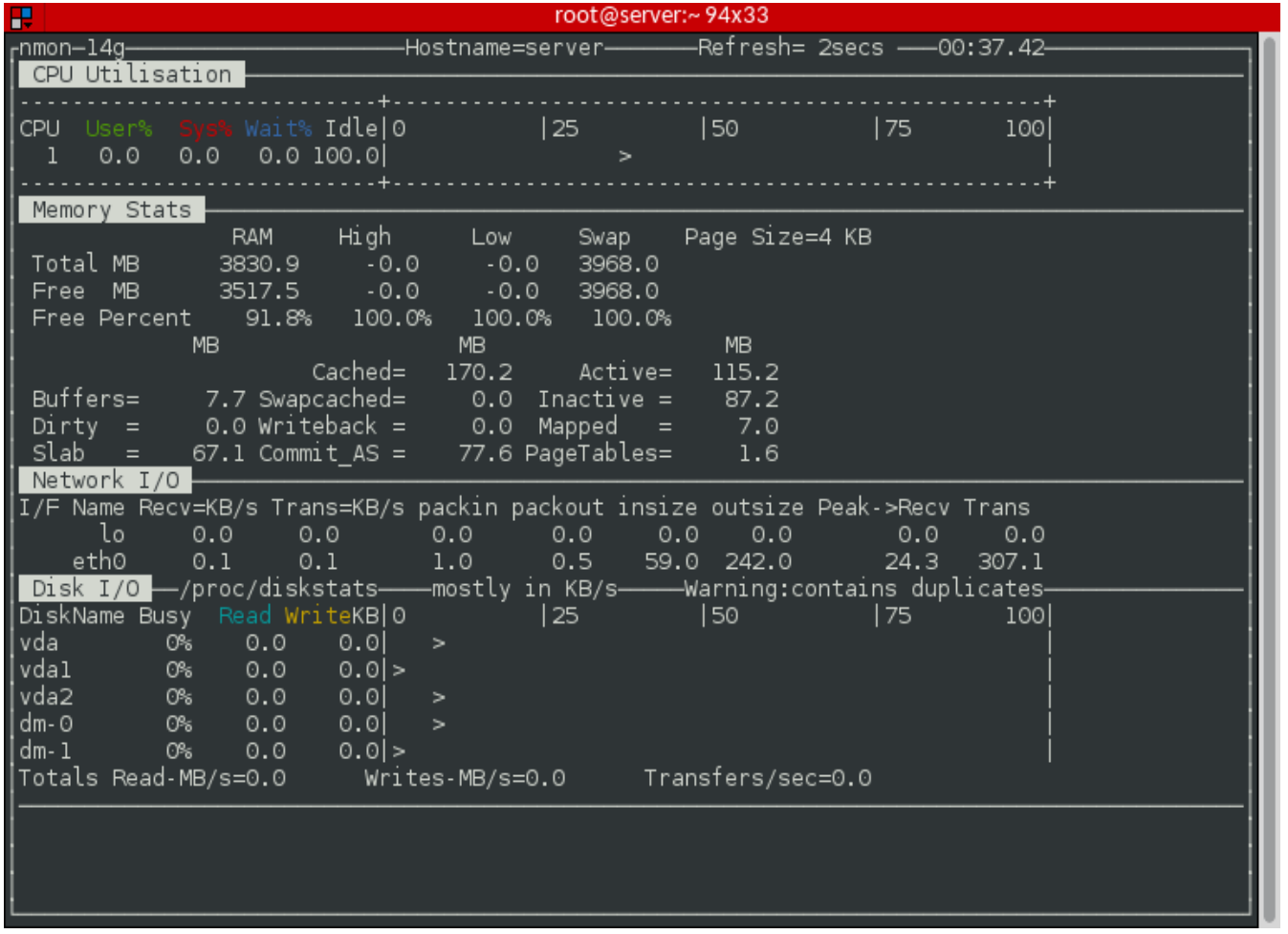



```
# systemctl list-unit-files
# systemctl disable httpd
```



Servicios: performance y seguridad

- ps, netstat
- top, htop, nmon
- lsof, pgrep
- systemtap



Limitar recursos

- Limitar el acceso como root a las terminales
  - `/etc/securetty`
- Forzar el logout de los usuarios
  - `.bashrc` ó `/etc/profile`
    - `TMOUT=360`
- Limitar el acceso a los recursos
  - `/etc/security/limits.conf`

Administración Segura del Sistema

Cómo aplica los parches de seguridad?

Equipo de Respuesta a Incidentes de Seguridad Infomática

- **CERT**

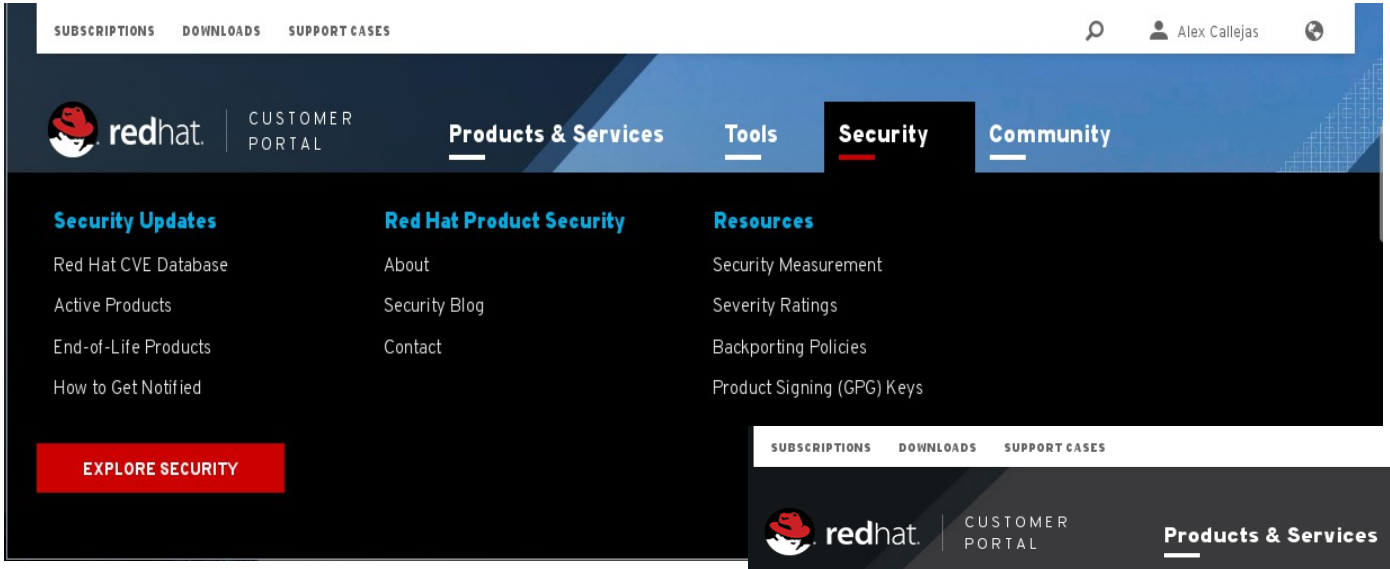
  http://www.cert.org.mx/index.html

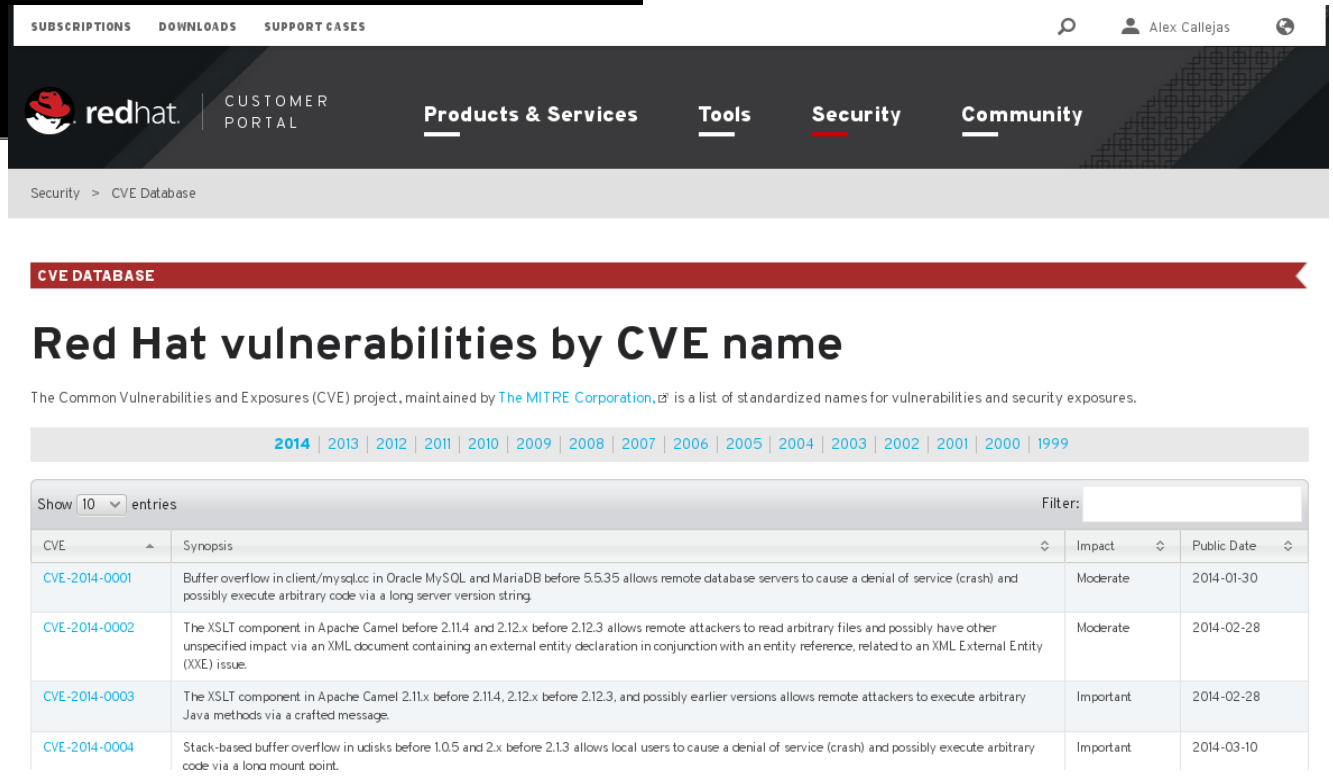
  - Publica información respecto a vulnerabilidades de seguridad y alertas de la misma índole
  - Realiza investigaciones sobre productos afectados y sus contramedidas

- **Publicación de erratas**

  - Severidades
  - Impactos
  - CVE (Common Vulnerabilities and Exposures)

Red Hat CVE Database



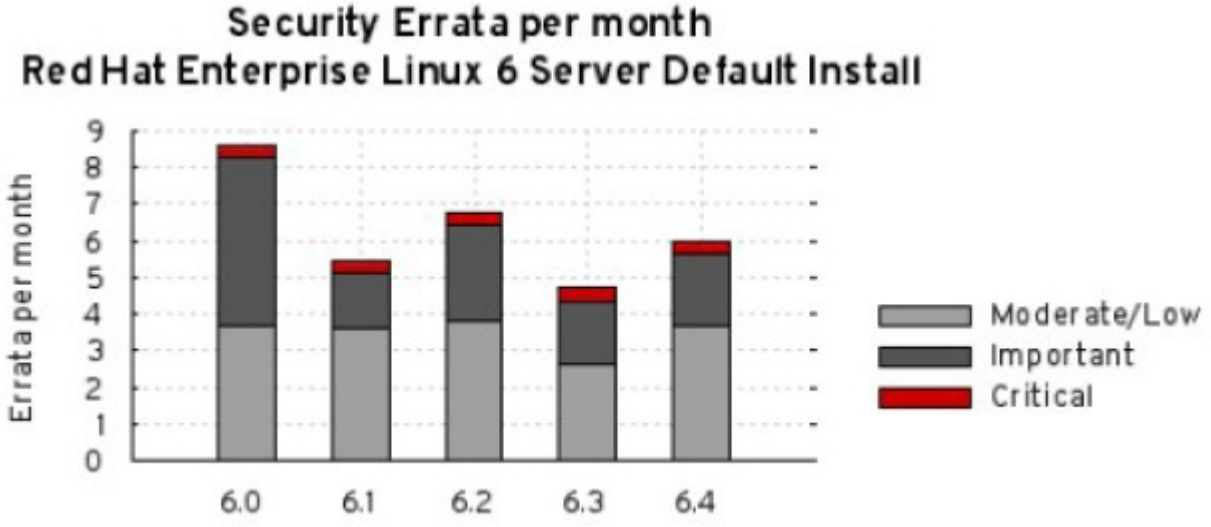


Impacto:

- ✔ Crítico
- ✔ Importante
- ✔ Moderado
- ✔ Bajo

Erratas

- Red Hat Security Advisory (RHSA)
- Red Hat Bug Fix Advisory (RHBA)
- Red Hat Enhancement Advisory (RHEA)



YUM Security plugin - instalación

```
[root@server ~]# yum -y install yum-plugin-security


[root@server ~]# cat /etc/yum/pluginconf.d/security.conf
[main]
enabled=1
[root@server ~]#
```

YUM Security plugin – verificación de erratas

```
[root@server ~]# yum updateinfo
Updates Information Summary: available
    4 Security notice(s)
        2 Important Security notice(s)
        2 Moderate Security notice(s)
    7 Bugfix notice(s)
    4 Enhancement notice(s)
updateinfo summary done
[root@server ~]#
```

YUM Security plugin – verificación de erratas

- Lista de paquetes

```
[root@server ~]# yum updateinfo list
```

- Lista de paquetes que solucionan errata

```
[root@server ~]# yum updateinfo list --advisory=RHSA-2014:1843
```

- Detalle de errata

```
[root@server ~]# yum updateinfo RHSA-2014:1843
```

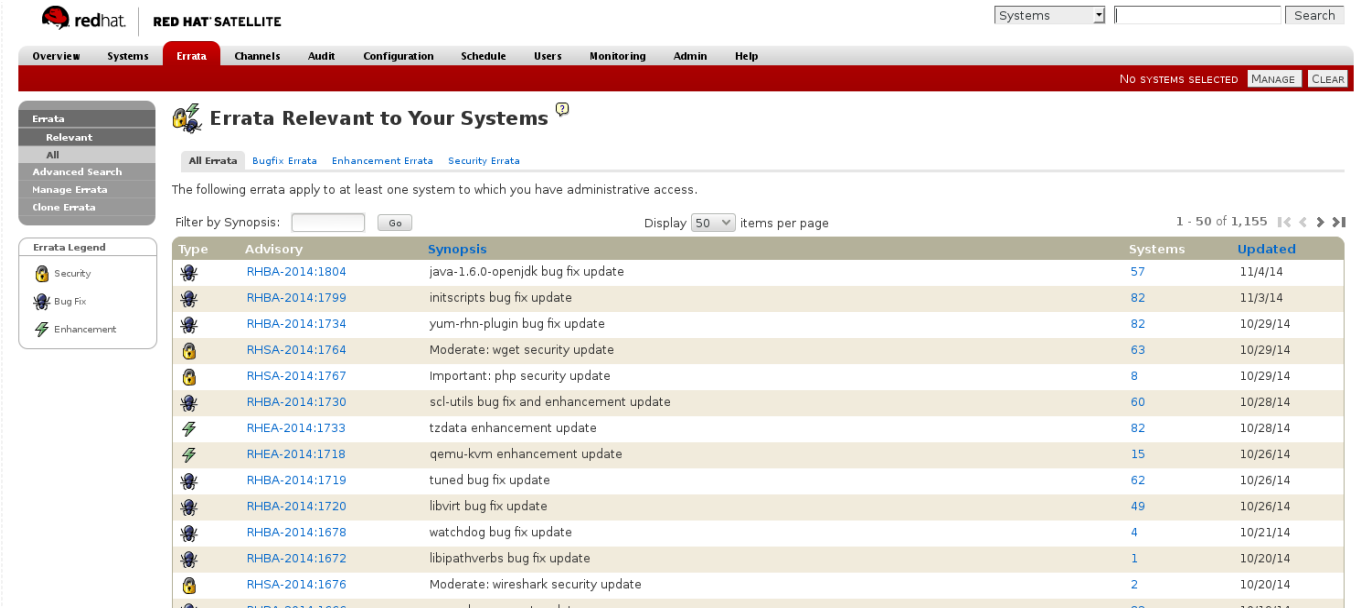
- Verificación de CVE

```
[root@server ~]# yum updateinfo list --cve=CVE-2014-3185
```

Administración de actualizaciones

- Aplicación actualizaciones
  - La mayor parte de los ataques ocurren con software no actualizado
- Monitoreo post actualización
- Administración de cambios
- Factibilidad

RED HAT NETWORK SATELLITE



Control de acceso

Tenga el control de la administración del sistema

Firewall

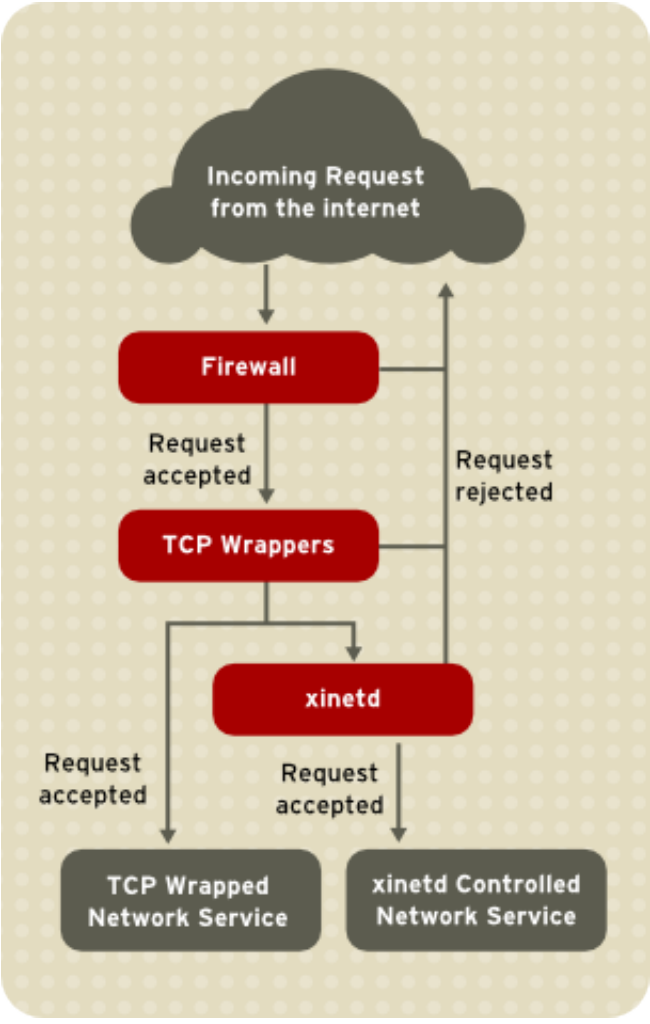
- Sirve como separación entre su red e internet
- Permite el uso legítimo de la red
- Previene el tráfico no autorizado al servidor (malicioso)

- `iptables`
  - Evaluación
  - Búsqueda de normas existentes
- Identificar las necesidades de protección
- Definición de estrategia

TCP Wrappers

- Herramienta que permite o niega el acceso a servicios
  - Utiliza la librería Libwrap
  - Archivos de control:
    - `/etc/hosts.allow`
    - `/etc/hosts.deny`
  - Usar en conjunto con firewall

```
sshd: client1.example-rh.com : allow
sshd: client1.example-rh.com : deny
```



Control de acceso

- MAC (Mandatory Access Control)
  - **SELinux** (Security-Enhanced Linux)
  - Por defecto en RHEL

    http://stopdisablingselinux.com/

- DAC (Discretionary Access Control)
  - `chmod`
  - `chattr`

- ACL
  - filesystem

Control de acceso

- Permisos especiales
  - SUID, SGID, sticky bit
- Atributos
  - `chattr`, `lsattr`
- Revisar directorios con permisos especiales

```
[root@server ~]# find / -type f -perm 1000 -ls
```

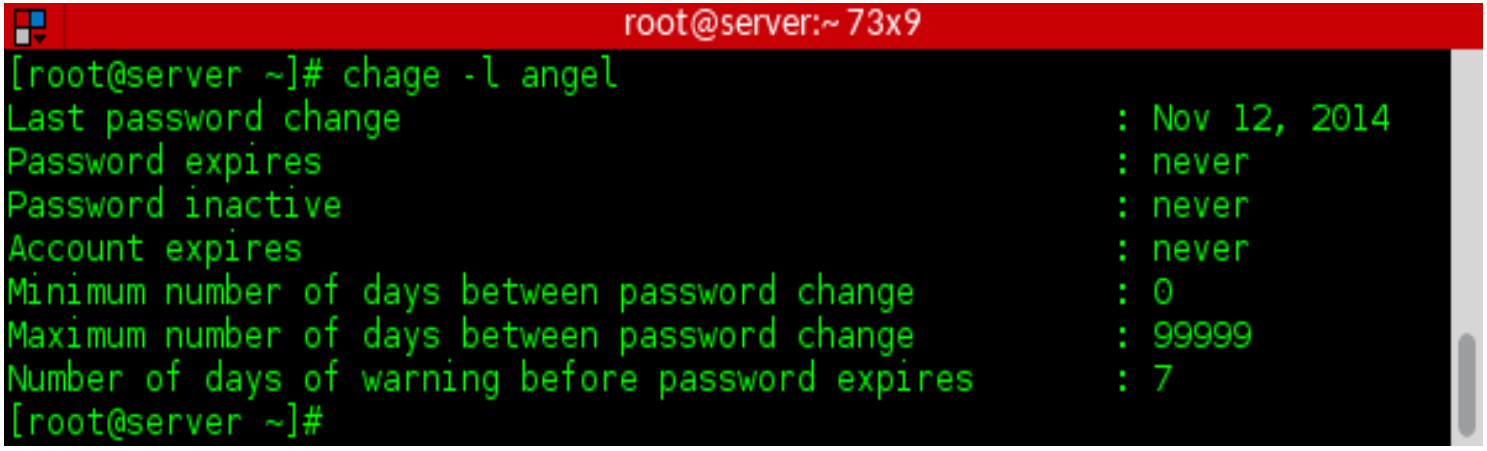
- sudo
  - `sudosh`

Auditoria: Use audit!

- Mecanismo de monitoreo de información relevante para la seguridad, basado en reglas predefinidas
- audit no proporciona ningún nivel de seguridad adicional
- Los eventos se almacenan en logs
- Es útil para la evaluación de violaciones a las políticas de seguridad y las actividades realizadas en el sistema
- Los posibles violaciones se pueden evitar con medidas preventivas conforme al análisis de logs

Auditoria: Política de login/contraseñas

chage



/etc/login.defs

```
PASS_MAX_DAYS   99999

PASS_MIN_DAYS   0

PASS_MIN_LEN    5

PASS_WARN_AGE   7

LOGIN_RETRIES   5

LOGIN_TIMEOUT   60
```

Seguridad en el almacenamiento de datos

- **Backup!**
  - Estrategia
    - Storage, cinta...
    - Calendarización
    - Software
      - Bacula
      - Amanda

Servicios Seguros

Puntos de atención, riesgos y amenazas

Servicios – algunos riesgos

- Servicios inseguros
  - Denial of Service (DoS)
  - Distributed Denial of Service (DDoS)
  - Buffer overflow
  - Remote script execution

Servicios: SSH

- **Mantenerlo actualizado!**
- Restringir el uso
- **Indispensable** para SysAdmins

`/etc/ssh/sshd_config`

```
Port 22
Protocol 2
PermitRootLogin no
LoginGraceTime 60
PermitEmptyPasswords no
Allow users tux linus
Banner /etc/issue
```

- Use Llaves!
  - ✔ `ssh-keygen`
  - ✔ `ssh-copy-id`

Servicios: FTP

- VSFTP (Very Secure FTP)
- Alternativas:
  - ProFTP, Pure-ftp, etc...
- **Mantener actualizado!**
- Enjaular (**chroot**)
- Analizar caso de uso
  - Usuarios
  - Cuota
  - Upload/Download

Servicios: vsftpd

- Configurar banner
  - `ftpd_banner=FTP Server`
- Deshabilitar login anónimo
  - `anonymous_enable=NO`
- Permitir que los usuarios suban archivos
  - `write_enable=YES`
- Delimitar usuarios
  - `userlist_enable=YES`
  - `userlist_file=/etc/vsftpd.allowed_users`
- Enjaular usuarios
  - `chroot_local_user=YES`

Servicios: vsftpd

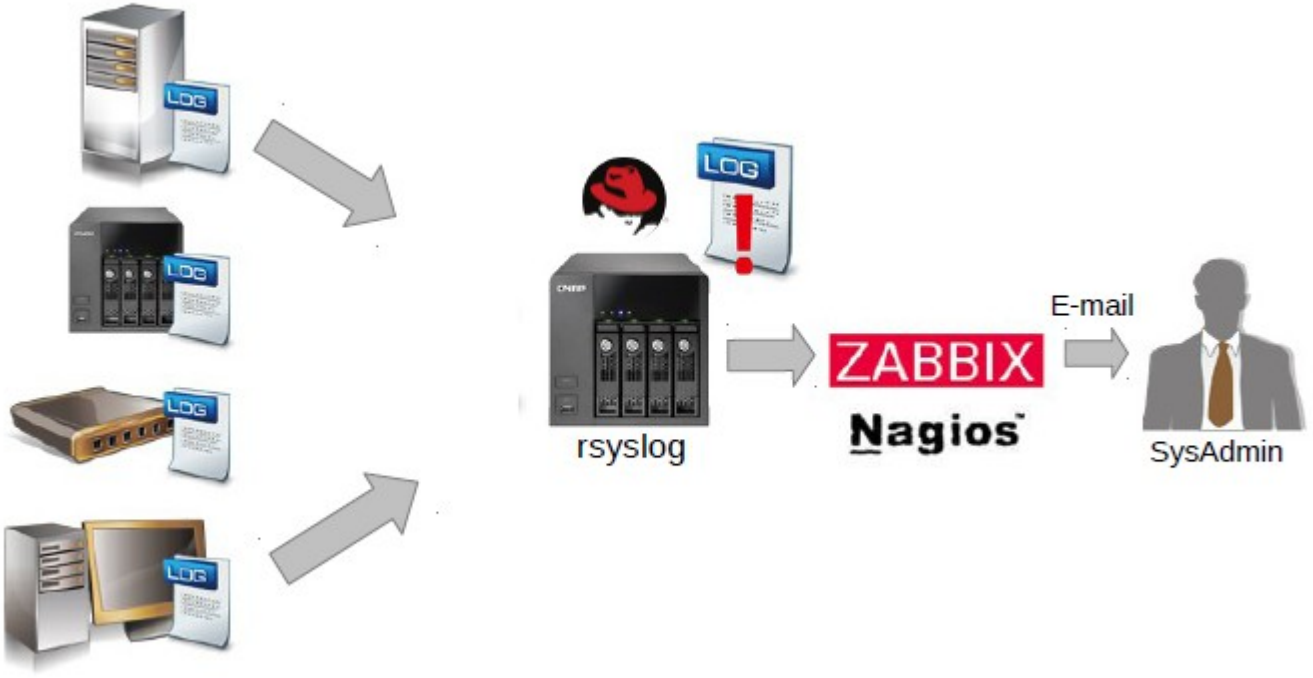
- **Control del acceso**
  - `/etc/ftpusers`
- **Prevenir DoS**
  - `ls_recurse_enable=NO`
  - `max_clients=200`
  - `max_per_ip=4`
- **FTP con SSL**
  - `ssl_enable=YES`
  - `allow_anon_ssl=NO`
  - `force_local_data_ssl=NO`
  - `force_local_logins_ssl=NO`
  - `ssl_tlsv1=YES`
  - `ssl_sslv2=NO`
  - `ssl_sslv3=NO`
  - `rsa_cert_file=/etc/vsftpd/vsftpd.pem`

Servicios: web server

- **Mantenerlo actualizado!**
- Agregar soporte a conexiones encriptadas
- Analizar el uso de modulos de seguridad
  - `mod_security, mod_evasive, mod_access, mod_authz`
- Analizar el caso de uso
- Probar las configuraciones antes de aplicar en producción
  - `apachectl configtest`
  - `apachectl gracefull`
- Restringir acceso
  - `.htaccess` y `htpasswd`

Syslog centralizado

- rsyslog
- rsyslog-gnutls
- logrotate



Tuneame el kernel

- Evitar SYN ATACK que causa negación de servicio (DoS)
  - `/proc/sys/net/ipv4/tcp_syncookies`
- Engañar el “OS guessing” en scans
  - `/proc/sys/net/ipv4/ip_default_ttl`
- Bloquear ICMP (ping)
  - `/proc/sys/net/ipv4/icmp_echo_ignore_all`
- Ignorar broadcast
  - `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`
- Deshabilitar IPV6
  - `/proc/sys/net/ipv6/conf/all/disable_ipv6`

Preparándonos para el desastre

Planificando contingencias y continuidad

BIA - Business Impact Analysis

- ¿Cuánto tiempo puede detenerse producción en caso de un incidente?
- ¿Cuál es el impacto del tiempo de inactividad en el negocio?
- ¿Cuáles son los requisitos mínimos para volver a la normalidad?
- ¿Hay contingencia?
- En caso de desastre, ¿cuanto es el tiempo minimo necesario para regresar a la normalidad?

Plan de Contingencia

- Ciclo de vida PDCA (plan-do-check-act)
- Análisis de riesgo
  - Identificar amenazas
- Plan Contingencia
  - Plan de respaldo
  - Plan de emergencia
  - Plan de recuperación

DRP – Plan de Recuperación de Desastres

DRP – BCP

- **Backup!**
- Capacitación
- Monitoreo
- Medios alternos
  - kickstart, snapshot, clonezilla

Gracias.


redhat