



UNIVERSIDADE DE VIGO

“Seguridad

en

Sistemas Linux”



Ponente: Javier Terceiro López

Correo: jtlopez@gulo.org

Lugar: Monforte de Lemos

Hora: 12:30

Título da charla: Seguridad Avanzada en Sistemas Linux



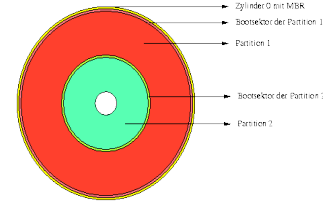
- Seguridad básica
 - Grub
 - LiLo
- Sistema de ficheros cifrado
 - cryptoloop
 - Particiones cifradas
- Seguridad en el sistema
 - Aide
 - Log's
 - iptables
- Bibliografía



- Seguridad física en grandes servidores
 - Control de puertas
 - Control de acceso
 - Control de personal
- Seguridad en contraseñas
 - Mínimo de 8 caracteres
 - Alternar letras – números – símbolos
- Concepto básico de seguridad:
 - **Nunca gastar más dinero en el sistema de seguridad que precio de los datos a guardar**



- ¿Qué es?
- ¿Por qué es necesario seguridad?
 - Evitar entrada al S.O.
 - Diferenciar Sistemas Operativos
- Configuración
 - `/etc/lilo.conf`



```
boot=/dev/hda
```

```
password=L1n3&ux9
```

```
timeout=100
```

```
image=/boot/vmlinuz
```

```
label="Linux"
```

```
root=/dev/hdb1
```

```
initrd=/boot/initrd.img
```

```
vga=791
```

```
read-only
```

```
other=/dev/hda1
```

```
label="windows"
```

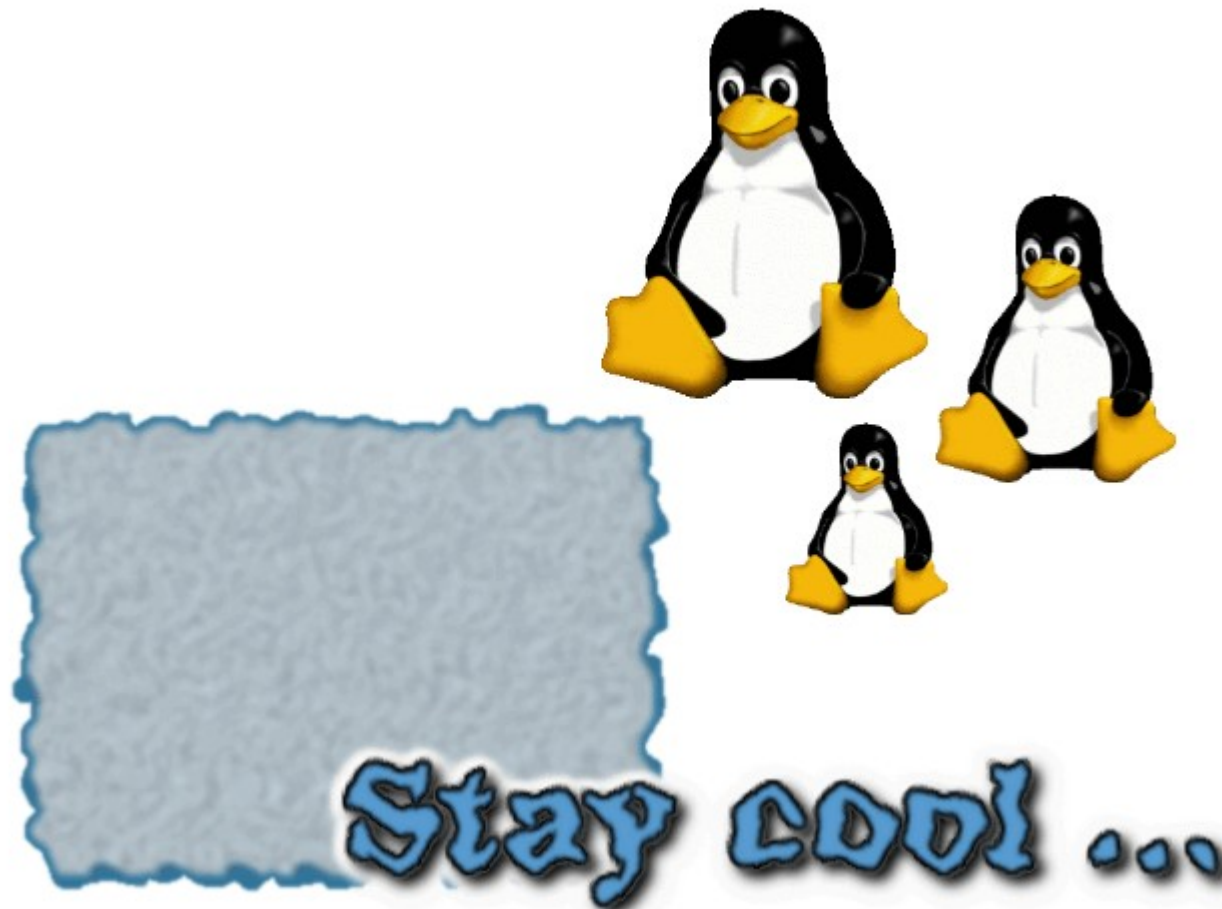
```
table=/dev/hda
```



```
boot=/dev/hda
timeout=100
image=/boot/vmlinuz
    label="Linux"
    root=/dev/hdb1
    initrd=/boot/initrd.img
    vga=791
    read-only
    password=L1n3&ux9
other=/dev/hda1
    label="windows"
    table=/dev/hda
```



- Seguridad de fichero de configuración
chmod 600 /etc/lilo.conf
- No solo un gestor de arranque en modo texto...



- ¿Qué es?
- Contraseñas en grub
 - Mucho más potente y seguro que LiLo
 - Contraseña cifrada en **md5**
- Configuración
 - `/boot/grub/menu.lst`



```
dark:~# grub-md5-crypt
```

```
Password:
```

```
Retype password:
```

```
$1$.RdVp1$mauD9CLqT4mNVcK6Jlq6u1
```

```
/boot/grub/menu.lst
```

```
default      1
```

```
timeout      5
```

```
color cyan/blue white/blue
```

```
password -md5 $1$.RdVp1$mauD9CLqT4mNVcK6Jlq6u1
```

```
title        Windows 95/98/NT/2000
```

```
root         (hd0,0)
```

```
title        Linux
```

```
root         (hd0,1)
```

```
kernel       /vmlinuz root=/dev/hda2 ro
```



- ¿Por qué cifrar un sistema de ficheros?
 - Datos muy importantes
 - Confidencialidad
 - SEGURIDAD
- ¿Cómo crearlo?
 - Dispositivos externos
 - Particiones de disco
- Algoritmos
 - Blowfish | blowfish-256
 - des-256 | des-64
- Rendimiento
 - ¿Compensa la pérdida de rendimiento a la seguridad de los datos?





- Sistema muy potente para dispositivos móviles
- Seguridad y fiabilidad de datos
- ¿Cómo lograrlo?
 - Compilar el kernel para dar soporte
 - Soporte para la criptografía
 - Creando sistema de ficheros cifrado
 - Montar el dispositivo
 - Usarlo
 - Desmontar y transportar
- Veremos a continuación en más detalle



- Incluir soporte en el kernel para:
 - loop devices
 - crypto loop devecos
 - Sistemas de cifrado

Device Drivers ->

Block Devices ->

Loopback device support

Cryptographic API

<*> MD4 digest algorithm

<*> MD5 digest algorithm

<*> DES and Triple DES EDE cipher algorithms

<*> Blowfish cipher algorithm

- Compilación



- Cargar los módulos necesarios
 - modprobe cryptoloop
 - modprobe blowfish
- loopback device
- blowfish



- dd

```
dd if=/dev/urandom of=/dev/sda1 bs=1024
```
- losetup

```
losetup -e blowfish /dev/loop0 /dev/sda1
```

```
losetup -e blowfish /dev/loop0 /dev/sda1
```
- mkfs.ext3

```
mkfs.ext3 /dev/loop0
```
- mkfs.reiserfs

```
mkfs.reiserfs /dev/loop0
```



- **mkdir**
`mkdir /mnt/pen`
- **mount**
`mount -t ext3 /dev/loop0 /mnt/pen`
`mount -t reiserfs /dev/loop0 /mnt/pen`
`mount -t ext3 /dev/sda1 /mnt/pen -oencryption=blowfish`
- **/etc/fstab**
`/dev/sda1 /mnt/pen ext3 noauto,encryption=blowfish 0 0`



- `/mnt/pen ==> escribimos en pen`
- `umount`
`umount /mnt/crypto`
- `losetup`
`losetup -d /dev/loop0`



- Igual que para dispositivos externos
- Interés de cifrado en /home
- Rendimiento no puede decaer mucho
 - Algoritmo no muy potente
- /etc/fstab

```
/dev/hda4 /home ext3 noauto,encryption=blowfish 0 0
```



- Depende del algoritmo utilizado
 - Algoritmo más seguro, mayor penalización

Cifrado / No cifrado

```
pangea:~# hdparm -t /dev/sda1  
/dev/sda1:
```

Timing buffered disk reads: 50 MB in 3.08 seconds = 16.22 MB/sec

Timing buffered disk reads: 66 MB in 3.08 seconds = 21.57 MB/sec

Cifrado / No cifrado

```
pangea:~# hdparm -T /dev/sda1  
/dev/sda1:
```

Timing buffer-cache reads: 756 MB in 2.00 seconds = 377.11 MB/sec

Timing buffer-cache reads: 812 MB in 2.00 seconds = 406.09 MB/sec



- Un sistema funciona puede sufrir ataques y entradas no deseadas
- Si no es posible evitarlas
 - Fallos de seguridad nuevos
- Intentar detectarlas lo antes posible
 - Sistemas de chequeo de integridad
 - Aide
 - Log`s del sistema
 - logcheck
- Seguridad básica en redes
 - IPTables



- Definición
 - Entorno de detección de intrusos
- Sustituto de Tripwire.
- Funcionamiento
 - Crea un base de datos desde reglas de expresiones regulares de todos los ficheros del sistema.
 - Una vez creada, puede chequear la integridad de los mismos para garantizar su fiabilidad.
 - Algoritmos: md5, sha1
 - `/etc/aide/aide.conf`
 - Controlar especialmente ficheros de configuración: `/etc/`
 - Incluir chequeo en cron
 - En caso de fallo, envía mail a root



- Parte muy importante del sistema!!
 - Registra TODO lo que sucede
 - Demonio syslog
/var/log/
- Control de integridad de log's del sistema
 - logcheck (/usr/sbin/logcheck)
 - Envío de log's diarios
 - Permite expresiones regulares de filtrado de log's
 - /etc/logcheck/logcheck.conf
 - SENDMAILTO="logcheck@localhost"
 - REPORTLEVEL="paranoid"
 - /etc/cron.d/logcheck
 - MAILTO="logcheck@localhost"
 - 2 09,16 * * * logcheck test -x /usr/sbin/logcheck &&
nice -n10



- ¿Qué es?
 - Firewall de Linux
 - Funcionamiento a nivel del kernel
 - IPTables = Tablas de IP
- Introducción
 - Comando (como root) iptables
 - Opciones:
 - P: Establece política por defecto
 - p: Protocolo (tcp, udp, icmp, etc)
 - A: Crea una nueva regla
 - F: Limpia las reglas existentes
 - Z: Contados de paquetes a cero
 - t nat -F: Limpia las tablas de *nateo*
 - y muchas más



- Denegamos TODO, permitir necesario

```
#!/bin/bash
```

```
# Limpiamos reglas
```

```
iptables -F
```

```
iptables -X
```

```
iptables -Z
```

```
iptables -t nat -F
```

```
# creamos política por defecto
```

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT ACCEPT
```

```
iptables -P FORWARD ACCEPT
```



dejamos entrar a mysql y ftp a una IP

```
iptables -A INPUT -s 10.0.0.26 -p tcp --dport 3306 -j ACCEPT
```

```
iptables -A INPUT -s 10.0.0.29 -p tcp --dport 20:21 -j ACCEPT
```

Apache a todo el mundo

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

A mi IP todo

```
iptables -A INPUT -s 10.0.0.2 -j ACCEPT
```





- Grub: <http://www.gnu.org/software/grub/>
- LiLo: http://www.acm.uiuc.edu/workshops/linux_install/lilo.html
- Cryptoloop: <http://tldp.org/HOWTO/Cryptoloop-HOWTO/>
- logcheck: <http://logcheck.org/>
- Aide: <http://www.cs.tut.fi/~rammer/aide.html>
- IPTables: <http://www.netfilter.org/>
- Kernel: <http://www.kernel.org>
- Debian: <http://www.debian.org>



¿Cuestiones?

