

Servidores y Seguridad

Open Source @ Inacap

2007-11-21

Arturo Hoffstadt Urrutia

Estudiante Ing. Civil Informática

ahoffsta@inf.utfsm.cl

<http://arturo.hoffstadt.cl>

- Seguridad
 - ¿Qué es seguridad?
 - Entonces... ¿que veremos?
- Mitos
- Administración de Sistemas y Servidores
 - Instalación
 - Pasos a Seguir
 - Consideraciones Físicas
 - El Proceso de Autenticación
 - Sistemas de Respaldos
- Políticas de Seguridad
- Conceptos de seguridad básicos
 - Modelos de seguridad

¿Qué es seguridad? (1/4)

● “Es la ciencia que se dedica a manejar **actos y comportamientos maliciosos** que involucran las TIC”

● Ejemplos de actos y comportamientos maliciosos:

- Robo
- Fraude
- Terrorismo
- Espionaje
- Sabotaje
- Spam
- Contenido Ilegal



¿Qué es seguridad? (2/4)

- Aspectos que cubre la Seguridad de Sistemas Computacionales:
 - Disponibilidad
 - Asegurar que los usuarios autorizados tienen acceso a la información cuando sea requerido.
 - Confidencialidad
 - Asegurar que la información es accesible solo a los que poseen autorización para verla.
 - Integridad
 - Salvaguardar la correctitud y completitud de la información y métodos de procesamiento.

¿Qué es seguridad? (3/4)

- ¿Porqué nos interesa la Seguridad de Sistemas Computacionales?
 - Hoy en día casi todos la información es administrada computacionalmente. Entonces, nos interesa para:
 - Mantener privacidad de nuestra información medica
 - Resguardar nuestras cuantas bancarias
 - Autenticar la veracidad de un mensaje
 - Salvaguardar vidas en los hospitales.
 - Etc.
 - Por eso, la aproximación de Seguridad que se requiere hoy en día, es sistémica. Debe aplicarse seguridad en todos las componentes del Sistema, y en sus canales de comunicación.

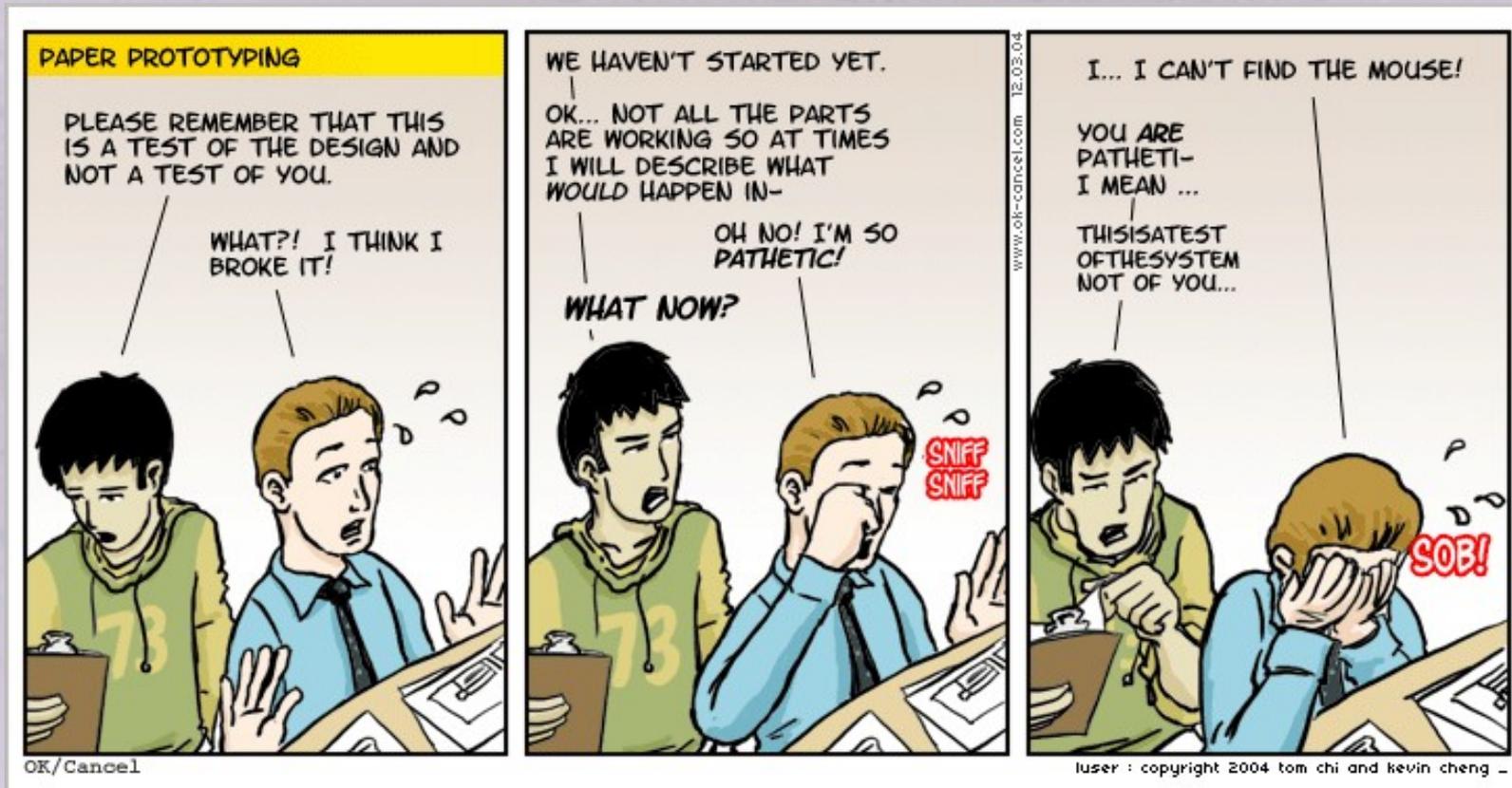
Finalmente...

Recordar que la seguridad (de sistemas) envuelve acciones humanas. No solo nos debemos preocupar de los computadores y programas, sino también de las USUARIOS.

Entonces... ¿Qué veremos? (1/2)

Veremos

- Servidores y proceso de instalación
- Administración de Sistemas
- Políticas de Seguridad
- **Usuario**, Capa 8, e interfaz teclado-silla.



Entonces... ¿Qué veremos? (2/2)

❖ No veremos

❖ Seguridad y programación.

- ❖ Memoria de Rodrigo Riveros, DI, UTFSM.
- ❖ Secure Programming for Linux and Unix HOWTO (<http://www.dwheeler.com/secure-programs>)
- ❖ La charla “Web: Ataque y Defensa”, por Claudio Salazar.

❖ Criptografía.

- ❖ Si necesitan implementar criptografía, no inventen un algoritmo. Existen muchos algoritmos de especificación abierta (e incluso implementación), que son extremadamente seguros y efectivos.
- ❖ Aprender a utilizarlo es mucho mas importante que programar un buen algoritmo. Si la llave de encriptación es administrada debilmente, **el algoritmo no sirve de nada.**

- **Un firewall, es lo único que necesito.**
 - El firewall solo restringe puertos, orígenes, destinos, y protocolos (depende, normalmente capa 3 y 4).
 - Varios de los problemas de seguridad, no suelen ser solucionados por un firewall (usuario anoto su contraseña).
- **Si un software que uso esta mal programado, no es mi problema.**
 - El software es un medio de acceso a los datos que resguardo.

The five-layer TCP/IP model

5. Application layer

DHCP · DNS · FTP · Gopher · HTTP · IMAP4 · IRC · NNTP · XMPP · POP3 · SIP · SMTP · SNMP · SSH · TELNET · RPC · RTCP · RTSP · TLS · SDP · SOAP · GTP · STUN · NTP · (more)

4. Transport layer

TCP · UDP · DCCP · SCTP · RTP · RSVP · IGMP · PPTP · (more)

3. Network/Internet layer

IP (IPv4 · IPv6) · OSPF · IS-IS · BGP · IPsec · ARP · RARP · RIP · ICMP · ICMPv6 · (more)

2. Data link layer

802.11 · 802.16 · Wi-Fi · WiMAX · ATM · DTM · Token ring · Ethernet · FDDI · Frame Relay · GPRS · EVDO · HSPA · HDLC · PPP · L2TP · ISDN · (more)

1. Physical layer

Ethernet physical layer · Modems · PLC · SONET/SDH · G.709 · OFDM · Optical fiber · Coaxial cable · Twisted pair · (more)

- ❖ **Si el software que tengo en mis sistema, usa encriptación, no tengo que preocuparme.**
 - La administración de las contraseña/llave es más delicada que el método de encriptación usado.
- ❖ **Las jaulas chroot, son impenetrables.**
 - Las jaulas chroot tienen que ser creadas por el usuario root, y por ende, el mismo puede salir de ellas.
 - Chroot no fue creado con el fin de contener programas con posibles fallos o exploits de seguridad.

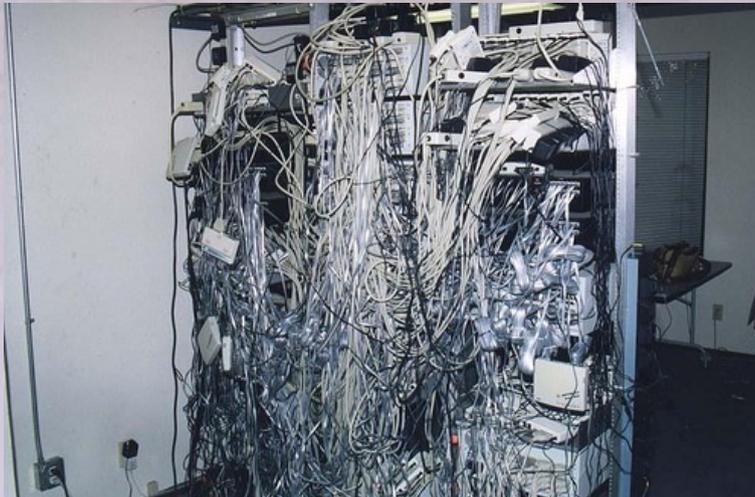


- ❖ **La seguridad de sistema es un problema/tarea solo de Administración de Sistemas**
 - QUÉEEEEEEEEEEEE!!!!!!!!!!!!!!!!!!!!!!



Administración de Sistemas y Seguridad

- La Administración de Sistemas, es uno de los trabajos que más se encuentra con Seguridad (después, obviamente, de la Ingeniería de Seguridad).
- Veremos varios puntos de las tareas de un Administrador de Sistemas, partiendo por la instalación de un servidor.





CentOS

O cualquier otro
“Enterprise” o
“Server” Edition

Que ofrece CentOS



Welcome to CentOS-4 i386

During this installation, you can use your mouse or keyboard to navigate through the various screens.

The **Tab** key allows you to move around the screen, the Up and Down arrow keys to scroll through lists, + and - keys expand and collapse lists, while **Space** and **Enter** selects or removes from selection a highlighted item. You can also use the **Alt-X** key command combination as a way of clicking on buttons or making other screen selections, where **X** is replaced with any underlined letter appearing



CentOS

 Hide Help

 Release Notes

 Back

 Next

Ingles... ¿porqué?



Language Selection

Choose the language you would like to use during this installation.



What language would you like to use during the installation process?

Chinese(Simplified) (简体中文)
Chinese(Traditional) (繁體中文)
Croatian (Hrvatski)
Czech (Čeština)
Danish (Dansk)
Dutch (Nederlands)
English (English)
Estonian (eesti keel)
Finnish (suomi)
French (Français)
German (Deutsch)
Gujarati (ગુજરાતી)
Hindi (हिन्दी)
Hungarian (magyar)
Icelandic (Íslenska)
Italian (Italiano)
Japanese (日本語)

Hide Help

Release Notes

Back

Next



Installation Type

Choose the type of installation that best meets your needs.

An installation destroys any previously saved information on the selected partitions.

For more information concerning the differences among these installation classes, refer to the product documentation.



Personal Desktop

Perfect for personal computers or laptops, select this installation type to install a graphical desktop environment and create a system ideal for home or desktop use.



Workstation

This option installs a graphical desktop environment with tools for software development and system administration.



Server

Select this installation type if you would like to set up file sharing, print sharing, and Web services. Additional services can also be enabled, and you can choose whether or not to install a graphical environment.



Custom

Select this installation type to gain complete control over the installation process, including software package selection and partitioning.

Hide Help

Release Notes

Back

Next

Particiones manuales



Disk Partitioning Setup

One of the largest obstacles for a new user during a Linux installation is partitioning. This process is made easier by providing automatic partitioning.

By selecting automatic partitioning, you do not have to use partitioning tools to assign mount points, create partitions, or allocate space for your installation.

To partition manually, choose the **Disk Druid** partitioning tool.

Use the **Back** button to choose

Automatic Partitioning sets partitions based on the selected installation type. You also can customize the partitions once they have been created.

The manual disk partitioning tool, Disk Druid, allows you to create partitions in an interactive environment. You can set the file system types, mount points, partition sizes, and more.

- Automatically partition
- Manually partition with **Disk Druid**

Hide Help

Release Notes

Back

Next

Esquema de partición



CentOS

Disk Setup

Choose where you would like CentOS-4 i386 to be installed.

If you do not know how to partition your system or if you need help with using the manual partitioning tools, refer to the product documentation.

If you used automatic partitioning, you can either accept the current partition settings (click **Next**), or modify the setup using the manual partitioning tool.

If you are manually partitioning your system, you can see your current hard drive(s) and partitions displayed below. Use the partitioning tool to add, edit,

Drive `/dev/sda` (6142 MB) (Model: VMware, VMware Virtual S)

sda2
16040 MB

[New](#) [Edit](#) [Delete](#) [Reset](#) [RAID](#) [LVM](#)

Device	Mount Point/ RAID/Volume	Type	Format	Size (MB)	Start	End
▼ LVM Volume Groups						
▼ seg						
var_log	/var/log	ext3	✓	1024		
slash	/	ext3	✓	1024		
swap		swap	✓	256		
var	/var	ext3	✓	1152		
usr	/usr	ext3	✓	1504		
home	/home	ext3	✓	1024		

Hide RAID device/LVM Volume Group members

Hide Help

Release Notes

Back

Next

Password en grub... ¿porqué?



Boot Loader Configuration

By default, the GRUB boot loader is installed on the system. If you do not want to install GRUB as your boot loader, select **Change boot loader**.

You can also choose which OS (if you have more than one) should boot by default. Select **Default** beside the preferred boot partition to choose your default bootable OS. You cannot move forward in the installation unless you choose a default boot image.

You may add, edit, and delete the boot loader entries by

The GRUB boot loader will be installed on /dev/sda.

[Change boot loader](#)

You can configure the boot loader to boot other operating systems. It will allow you to select an operating system to boot from the list. To add additional operating systems, which are not automatically detected, click 'Add.' To change the operating system booted by default, select 'Default' by the desired operating system.

Default	Label	Device	
<input checked="" type="checkbox"/>	CentOS-4 i386	/dev/seg/slash	Add
			Edit
			Delete

A boot loader password prevents users from changing options passed to the kernel. For greater system security, it is recommended that you set a password.

[Use a boot loader password](#) [Change password](#)

[Configure advanced boot loader options](#)

[Hide Help](#)

[Release Notes](#)

[Back](#)

[Next](#)



Network Configuration

Any network devices you have on the system are automatically detected by the installation program and shown in the **Network Devices** list.

To configure the network device, first select the device and then click **Edit**. In the **Edit Interface** screen, you can choose to have the IP and Netmask information configured by DHCP or you can enter it manually. You can also choose to make the device active at boot time.

If you do not have DHCP client access or are unsure as to

Network Devices

Active on Boot	Device	IP/Netmask
<input checked="" type="checkbox"/>	eth0	DHCP

Hostname

Set the hostname:

automatically via DHCP

manually (ex. "host.domain.com")

Miscellaneous Settings

Gateway:

 . . .

Primary DNS:

 . . .

Secondary DNS:

 . . .

Tertiary DNS:

 . . .



Firewall Configuration

A firewall sits between your computer and the network, and determines which resources on your computer remote users on the network are able to access. A properly configured firewall can greatly increase the out-of-the-box security of your system.

Choose the appropriate security level for your system.

No Firewall — No firewall provides complete access to your system and does no security checking. Security checking is the disabling of access to certain services. This should only be selected if you

A firewall can help prevent unauthorized access to your computer from the outside world. Would you like to enable a firewall?

- No firewall
 Enable firewall

You can use a firewall to allow access to specific services on your computer from other computers. Which services, if any, do you wish to allow access to ?

- Remote Login (SSH)
 Web Server (HTTP, HTTPS)
 File Transfer (FTP)
 Mail Server (SMTP)

Security Enhanced Linux (SELinux) provides finer-grained security controls than those available in a traditional Linux system. It can be set up in a disabled state, a state which only warns about things which would be denied, or a fully active state.

Enable SELinux?:

Hide Help

Release Notes

Back

Next

Inglés, ¿nuevamente?



Additional Language Support

Select a language to use as the default language. The default language is the language used on the system once installation is complete. If you choose to install other languages, it is possible to change the default language after the installation.

The installation program can install and support several languages. To use more than one language on your system, choose specific languages to be installed, or select all languages to have all available languages installed on the system.

Select the default language for the system: English (USA) ▾

Select additional languages to install on the system:

- English (Great Britain)
- English (Hong Kong)
- English (India)
- English (Ireland)
- English (New Zealand)
- English (Philippines)
- English (Singapore)
- English (South Africa)
- English (USA)
- English (Zimbabwe)
- Estonian
- Faroese (Faroe Islands)
- Finnish
- French (Belgium)
- French (Canada)
- French (France)
- French (Luxemburg)

Select All

Select Default Only

Reset

Hide Help

Release Notes

Back

Next



Set Root Password

Use the root account *only* for administration. Once the installation has been completed, create a non-root account for your general use and `su -` to gain root access when you need to fix something quickly. These basic rules minimize the chances of a typo or incorrect command doing damage to your system.



The root account is used for administering the system.
Enter a password for the root user.

Root Password:

Confirm:

Hide Help

Release Notes

Back

Next

Paquetes a instalar... Mínimo



Package Group Selection

Select the package (application) groups that you want to install. To select a package group, click on the check box beside it.

Once a package group has been selected, click on **Details** to view which packages are installed by default and to add or remove optional packages from that group.

System

Administration Tools [0/12]



This group is a collection of graphical administration tools for the system, such as for managing user accounts and configuring system hardware.

System Tools [0/44]



This group is a collection of various tools for the system, such as the client for connecting to SMB shares and tools to monitor network traffic.

Printing Support [0/12]



Install these tools to enable the system to print or act as a print server.

Miscellaneous

Everything



This group includes all the packages available. Note that there are substantially more packages than just the ones in all the other package groups on this page.

Minimal



Choose this group to get the minimal possible set of packages. Useful for creating small router/firewall boxes, for example.

Total install size: 722M

Hide Help

Release Notes

Back

Next



About to Install

Caution: Once you click **Next**, the installation program begins writing the operating system to the hard drive(s). This process cannot be undone. If you have decided not to continue with this installation, this is the last point at which you can safely abort the installation process.

To abort this installation, press your computer's **Reset** button or reset using **Control-Alt-Delete**, and then remove the installation media between the unmounting and reboot screen messages.



Click next to begin installation of CentOS-4 i386.

A complete log of the installation can be found in the file `'/root/install.log'` after rebooting your system.

A kickstart file containing the installation options selected can be found in the file `'/root/anaconda-ks.cfg'` after rebooting the system.

Hide Help

Release Notes

Back

Next



Installing Packages

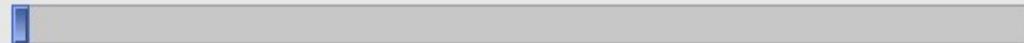
We have gathered all the information needed to install CentOS-4 i386 on the system. It may take a while to install everything, depending on how many packages need to be installed.

Welcome to CentOS 4 !

Thank you for installing CentOS 4.

CentOS is an Enterprise-class Linux Distribution derived from sources freely provided to the public by a prominent North American Enterprise Linux vendor. CentOS conforms fully with the upstream vendors redistribution policy and aims to be 100% binary compatible. (CentOS mainly changes packages to remove upstream vendor branding and artwork.)

More Info: <http://www.centos.org/>



Installing rootfiles-8-1.noarch (20 KB)
The basic required files for the root user's directory.

Hide Help

Release Notes

Back

Next

Y como recién salido del horno...

```
CentOS release 4.5 (Final)  
Kernel 2.6.9-55.EL on an i686  
  
lc-dyn-120 login: _
```

- Deshabilitar servicios sin usar
 - Seguir el principio de mínima superficie de exposición
 - Saber que tienes instalado en tu sistema
- Habilitar NTP, y mantenerlo sincronizado.
 - Instalar y levantar el servicio ntpd
- ```
echo "export HISTFILESIZE=10000"
>> /root/.bashrc
```

- Control remoto del servidor:
  - Ssh y sus llaves
- Yum
  - Aplicar yum update
  - Actualizar a lo menos diariamente
  - Seleccionar cuidadosamente los repositorios a utilizar
- Opciones (nosuid, noexec) a las particiones /tmp /var, /home

# Consideraciones Físicas

- Aire acondicionado
- Acceso Físico
  - Limitado
  - Solo en casos que se necesite contacto directo
- Electricidad
  - UPS
    - Energía **continua** en cortes no prolongados
  - Equipos Electrógenos (generadores)
    - Energía en cortes prolongados
- Detectores de Humo
- Sensor de Temperatura
- Instalación eléctrica
- Discos con soporte SMART (y activarlo)

# El Proceso de Autenticación

- Entendiendo el sistema de autenticación:
  - Linux guarda la información de los usuarios (por defecto), en /etc/passwd
  - Inclusive la contraseña
    - Lo cual es muy inseguro, dado que a este archivo deben tener acceso muchas aplicaciones.

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
```

8,1

Comienzo

user:password:uid:gid:comentario:home:shell

# El Proceso de Autenticación

- Se introduce el sistema Shadow.
  - Las password, pasan de /etc/passwd a /etc/shadow, y el root es el único que puede leerlas.

```
root:1rs9pdsmt$yd/0.RBJDrPBXtWPh8W/b/:13795:0:99999:7:::
bin:*:13731:0:99999:7:::
daemon:*:13731:0:99999:7:::
adm:*:13731:0:99999:7:::
lp:*:13731:0:99999:7:::
sync:*:13731:0:99999:7:::
shutdown:*:13731:0:99999:7:::
!alt:*:13731:0:99999:7:::
"/etc/shadow" [Sólo lectura] 87L, 2303C 8,1 Comienzo
```

user:password:1stchg:min:max:warn:inact:expire

Contraseña en Shadow:

User:: Indica que no tiene password.

User:\*: Indica cuenta lockeada.

# El Proceso de Autenticación

- PAM (Pluggable Authentication Modules)
  - Elimina el problema de autenticación y obtención de datos de usuario, de los programas.
  - Proporcionan una interfaz de acceso, y una arquitectura de modulos, lo que permite cambiar la fuente de datos de usuarios.
    - Shadow
    - LDAP
    - Samba
    - NIS
  - Permite restringir acceso a cuentas en base a muchos criterios
  - Permite restringir las password que se asignan.

- **Siempre ponte en el peor caso, porque va a suceder**  
**(y si... los edificio arden, muahahaha).**
- Si realmente quieres Disponibilidad, vas a necesitar tener Respaldos
  - Incluso a pesar de los múltiples servidores failover, con RAID 1 o 5.
  - Los errores no necesariamente son maliciosos, accidentes o desastres. El mismo software puede corromper datos.
- Una vez definido, probarlo. Siempre puede faltar algo por respaldar.

## Tipos de Respaldos

- Full: Respaldan todo
  - Incremental: Necesita un fullbackup, y solo respalda los cambios entre si, y el último fullbackup, o incremental.
  - Diferencial: Necesita un fullbackup, y solo respalda los cambios entre si, y el último fullbackup.
- ## Restaurar:
- Simplemente restaurar sobre los corruptos
  - Reinstalación y restaurar sobre el sistema nuevo.
  - BareMetal Restore: El respaldo debe ser del sistema completo. Ni siquiera se reinstalar, sino que se “quema” la imagen al disco duro.

# Sistemas de Información de Usuarios

## ● Opciones (algunas)

- Local
- LDAP
- NIS
- Samba

## ● Consideraciones

- Tráfico encriptado (SSL/TLS)
- La administración debe ser consistente con las políticas de administración de usuarios.
- Control de la información pública, privada
- Permitir Replicación -> aumenta disponibilidad

# Políticas de Seguridad

- Hasta el momento, nos hemos restringido al ámbito de servidores y estaciones de trabajo.
- Pero no hemos visto el factor mas importante, la interfaz silla-computador.
  - La mayor parte de los problemas de seguridad se generan ahí.
    - Compartir la cuenta
    - Anotar la password
    - Dar la password a cualquier persona
    - Publicar su email en forma plana
- ¿Como solucionar el problema?
  - No hay solución completa. Solo recomendaciones, reglas, y pautas a seguir:
    - Políticas
    - Buenas practicas, etc

- Administración de Usuarios
  - Mantener a todos los usuarios registrados
    - Saber quien puede entrar a que sistema, y quien no.
  - No mantener usuarios “fantasmas”
    - Usuarios usados por una aplicación, o como ejemplo o pruebas.
  - Solo tener a los usuarios necesarios en el sistemas
    - Considerar un ciclo de vida establecido que ate un usuario con un(as) cuenta(s).
    - Si un usuarios abandona la organización, borrar su cuenta inmediatamente (tras respaldarla).
  - Por sanidad mental, tener un sistemas de autenticación e información de usuarios centralizado.
    - Evitar tener sistemas que no se integren con la autenticación centralizada, porque requieren MUCHO más trabajo ser mantenidos.

## ● Administración de Usuarios

- 1 usuario <-> 1 cuenta
  - Permite auditar las acciones de los usuarios.
  - Asigna un responsable identificable.
- Tener sanciones para las violaciones a las reglas
- Desconfiar del usuario:
  - El usuario promedio es ignorante en computación e informática, por lo tanto, todo debe hacerse para que el usuario y los sistemas DEBAN estar lo más seguros.

## ● Administración de Contraseñas

- Explicar al usuario porque una contraseñas debe ser segura.
  - Numero mezclados con letras, (¿y caracteres no alfanuméricos?).
  - Fácil de recordar
  - No formada por palabras
  - **Letras tomadas de una frase, es muy buen generador de contraseñas fáciles de recordar, y complicadas.**
- Indicarle que no debe entregar la contraseña. Ningún sistema bien hecho, pedirá al administrador de sistemas obtener la contraseña de un usuario.
- Toda cuenta debe tener una contraseña, y nunca crear las cuentas con contraseñas predeterminadas:
  - Existen programas que generan contraseña. (pwgen)

## ● Administración de Contraseñas

- Explicar al usuario porque una contraseñas debe ser segura.
  - Numero mezclados con letras, (¿y caracteres no alfanuméricos?).
  - Fácil de recordar
  - No formada por palabras
  - **Letras tomadas de una frase, es muy buen generador de contraseñas fáciles de recordar, y complicadas.**
- Indicarle que no debe entregar la contraseña. Ningún sistema bien hecho, pedirá al administrador de sistemas obtener la contraseña de un usuario.
- Toda cuenta debe tener una contraseña, y nunca crear las cuentas con contraseñas predeterminadas:
  - Existen programas que generan contraseña. (pwgen)

- Al cotizar equipos:
  - Evaluar soporte y actualizaciones
  - Evaluar historial de seguridad, y de reparación de bugs.
  - Es MUY raro que un equipo no tenga fallos de seguridad.
  - No comprar de empresas que dejar pasar los bugs. (A menos que hayan indicado el fin del soporte del producto (EOL)).
- Al elegir software:
  - Reporte de bugs arreglados.
  - Suscribirse a la lista de anuncios
  - El problema de “Dancing Pigs”
  - Imponer seguridad sobre comodidad

- Regla de Oro:
  - “Denegar todo, permitir según sea absolutamente necesario y **firma de venta del alma del solicitante**”
- Establecer un esquema de red
  - Internet
    - Proveedor de acceso a internet
  - DMZ
    - Segmento de red a la cual se puede tener acceso desde internet
    - Hay salida y entrada de conexiones.
    - DMZ no puede acceder a Intranet.
  - Intranet
    - Segmento de red a la cual ningún computador de internet puede tener acceso.
    - Solo hay salida de conexiones.
    - Intranet puede acceder a Internet e Intranet.

- ❖ IP Spoofing
  - Se cambia la IP de origen en los mensajes
    - DNS Amplification
- ❖ DoS (Denial of Service)
  - A través de algún método (variante), lograr que un servicio no tenga disponibilidad
    - Spam
    - DNS Amplification
    - ICMP Flooding
- ❖ Malware
  - Software malicioso, a veces crackeado para portar código malicioso.
  - Virus
  - Adware: No es solicitado

- Fuerza Bruta
  - Averiguar la password mediante ataque combinatorial
- Basado en Diccionario
  - Utiliza palabras de un diccionario, modificándolas según reglas usuales.
- Falsificación de Identidad
  - Ataque muy usual, dado que el sistema de email posee la misma seguridad que el correo tradicional.
- Buffer Overflow
  - Se aprovecha fallos en los códigos de programas, para reescribir el mismo programa.
- Cross-site Scripting
- SQL-Injection

## Modelos de Seguridad (1/2)

- Existen muchos modelos de seguridad, pero Linux solo implementa 2:
- Recursos: cada recurso, poseen atributos que indican quien puede o no realizar cierta acción sobre el recurso.
  - Normalmente es muy costoso, el indicar todos contra todos, así que se reduce a:
    - A: all
    - U: user
    - G: group
    - O: other

- ❖ ACL (Access Control List)
  - ❖ Cada agente del sistema (usuario, programa, kernel), se le indica que es lo que puede realizar.
    - ❖ Mucho mas costoso, no fue posible de implementar hasta hace poco en sistemas operativos.
    - ❖ SELinux y NSA

## ¿Te interesa al tema?, donde continuar...

- IDS e IDP
  - Detección y prevención de intrusos
- Temas de Actualidad
  - Worm Storm
  - Explosión de Spam
- Linux
  - SELinux
  - HoneyNET
- Departamento
  - Ramo de “Seguridad de Sistemas Computacionales”
  - News (resucitarlo)