¿De verdad es Linux más seguro ?

Francisco Jesus Monserrat Coll,

IRIS-CERT ,RedIRIS

II Jornadas CALDUM

Murcia 11 de Julio 2005

Índice

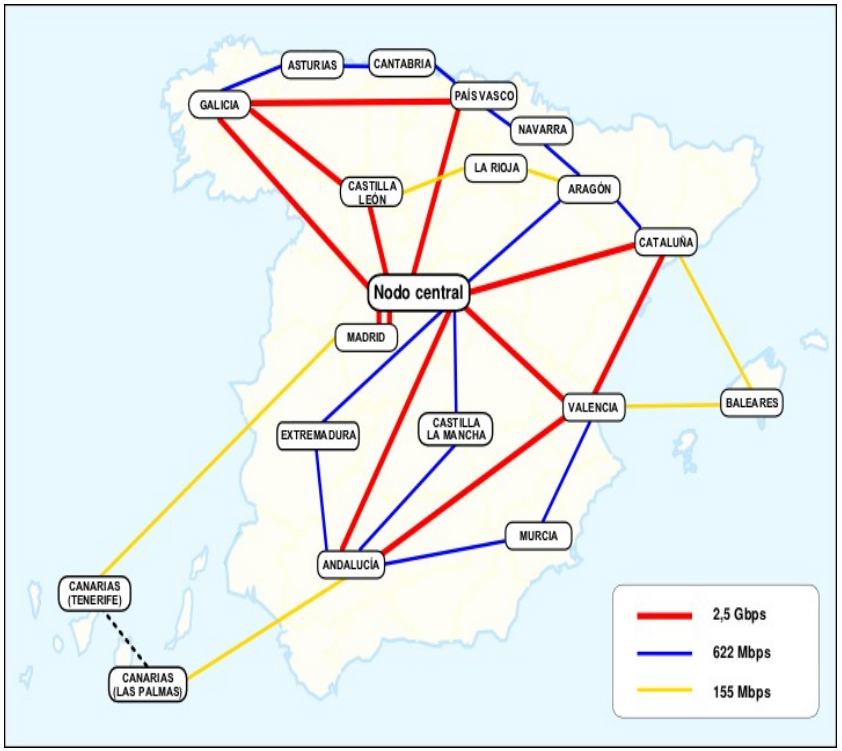
RedIRIS Inicios

Surge en 1998 para proporcionar conectividad a Universidades y centros de I+D Españoles.

Pioneros en la puesta en marcha de servicios en Internet en España: DNS, News,etc.

Conexión basada en un punto de acceso regional al que se conectan los centros.

Desde Enero de 2004 , incluida dentro del Ente Publico Empresarial Red.es



RedIRIS y el Código Libre

Desde sus inicios RedIRIS ha apoyado las iniciativas de código libre:

- Repositorio de distribuciones y programas y documentación (Sunsite)
- Desarrollos de herramientas y documentación de libre disposición.
- Puesta de diversos recursos (Listas de correo, espacio www, para algunos proyectos específicos),
- Colaboración con fabricantes que emplean código libre en sus sistemas. (cyclades, redhat, sun)

Internamente:

- La mayoría de los servicios emplean aplicaciones de código libre
- Empleo mayoritario de Linux como S.O. De escritorio

IRIS-CERT

Formado en 1995 para gestionar los incidentes de seguridad en redes conectadas a RedIRIS.

Punto central de recogida de denuncias relativas a equipos conectados a RedIRIS

Coordinación internacional con otros equipos de seguridad

Actividades de concienciación y fomento de la seguridad dentro de RedIRIS.

Proyectos de seguridad específicos:

- Cifrado de comunicaciones (PKI y PGP)
- Máquinas trampas y análisis forense
- Monitorización y control de tráfico

¿Qué hace IRIS-CERT?

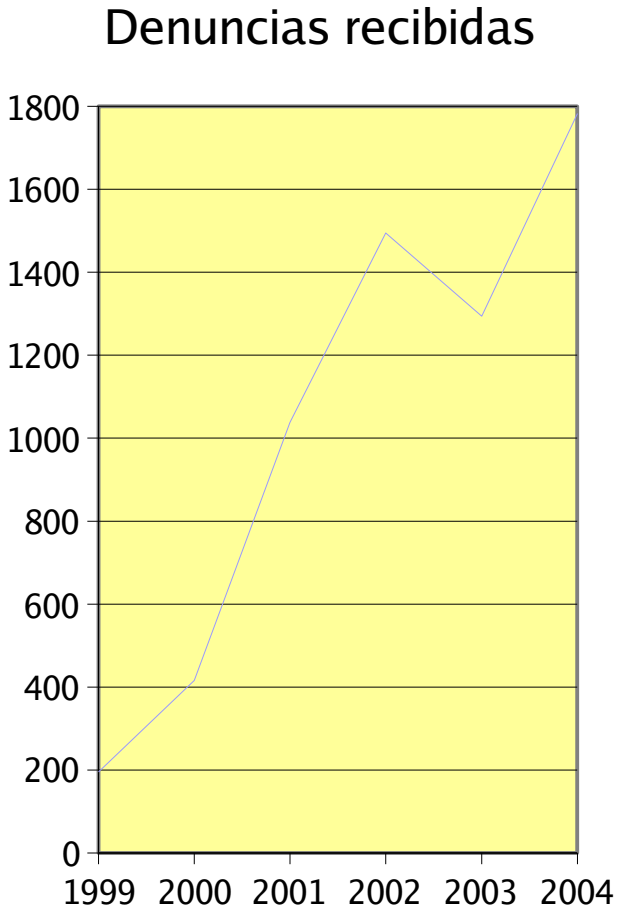
Punto centralizado de recepción de quejas

Sobre todo quejas externas (una máq
otra red).

**Coordinación con los técnicos de cada c
problema.**

Visión "global" de los problemas.

Difusión y fomento de la seguridad con lo



¿Para qué se van a conectar a mi equipo ?

Hace unos años era una pregunta normal.

En 1998, se podían detectar 1 o dos intentos de ataques contra una red del tamaño de la Universidad.

Pocos usuarios empleaban Linux

Hasta el año 2001~2002, gran parte de los ataques iban destinados a Servidores de organizaciones conectadas a internet:

- Equipos conectados 24h/día a internet.
- Mejor conectividad que equipos de usuario.

Actualmente se producen más de 1000 intentos de ataque diariamente (ruido de fondo).

Aunque gran parte de los ataques estén destinados a otras plataformas (¿Windows?) se producen diariamente ataques destinados a equipos Linux

El gran bazar actual

Según indican diversas fuentes existe un floreciente mercado de compra de estos equipos.

Intercambio de herramientas y ataques

Compra/venta de equipos comprometidos (¿50$ la docena ?) .

- Para la difusión de SPAM
- Ataque a otros sistemas
- Falsificación de mensajes de banca electrónica.

Extorsión a sitios de comercio electrónico:

- Denegación de servicio contra sistemas de comercio y/o juegos on-line
- Robo de información bancaria

Los sistemas Linux son usados especialmente:

Para alojar las páginas WWW de los fraudes bancarios.

Como repositorios donde almacenar las herramientas y programas para su posterior uso.

Como plataformas de ataques contra otros sistemas.

Los sistemas Linux son valiosos ya que:

Permiten un control remoto más sencillo que los sistemas Windows.

Mayor variedad de herramientas a instalar.

Amplia difusión y escaso control, sobre todo en entornos Universitarios con gran ancho de banda.

Linux es más seguro, ya que los gusanos/ virus no se pueden propagar en el.

Algunas definiciones

Virus(Informático): Código que es capaz de modificar un fichero (programa), para insertarse en el y así propagarse.

Famosos hace unos años, existen también para Linux, pero al igual que en Windows las medidas de seguridad del S.O. Impiden su proliferación.

Gusano: Programa que es capaz de transmitirse de forma autónoma y propagarse entre los ordenadores.

Los famosos “CodeRed, Nimda, Sasser” son ejemplos de gusanos.

Bots: Variante de los gusanos que además es capaz de ser controlado de forma remota por un atacante y tiene mayor “funcionalidad” que un gusano

Gran parte de los usuarios y antivirus no distinguen entre un tipo u otro.

Gusanos

El primer gusano (Morris 1989), empleaba una puerta falsa en el programa de distribución de correo electrónico para propagarse.

En el año 2001 (Feb) vuelven a surgir “gusanos” que se propagaban por equipos Linux debido a problemas de seguridad en algunas aplicaciones (DNS, LPR, rcp).

- A finales de Julio surge CodeRed el primer gusano para servidores WWW Windows, no afectaba a estaciones de trabajo.

- En 2002 surgen los gusanos para Windows que empleaban el protocolo NetBIOS de estos sistemas para propagarse.

- Este año también aparece el gusano Slapper que afectaba a servidores Apache incluidos en diversas distribuciones Linux

Bots & Zombies

Bot::

Inicialmente del termino “robot”, se aplicaba a trozos de código que simulaban una identidad

- Control de canales en IRC
- Simulación de jugadores en juegos multijugador.

Su definiciön se generaliza a programas “sirvientes” , que realizan determinadas acciones en base comandos emitidos desde el controlador.

Zombies:

Maquinas comprometidas usadas en DDOS (año 2000)

A partir de 2003 se generaliza el termino botnet (red de bots) para describir las redes de equipos comprometidos controlados por un canal de IRC

Bot e IRC

Empleado inicialmente solamente para compartir información entre los grupos de atacantes

Hasta el 2002 era frecuente el compromiso de equipos Unix/Linux para la instalación de servidores de IRC privados y proxies

Debido a que todas las conexiones provienen del servidor no es posible observando el tráfico de un equipo comprometido descubrir desde donde se conecta el atacante.

Su uso muy extendido en algunas comunidades impide el filtrado del trafico hacia estos servidores.

- Si se filtra el 6667, ¿por qué no emplear el 80 ?

Protocolo fácil de depurar

Modificaciones en los servidores para ocultar información (número de equipos, direcciones de conexión, etc).

Linux es más seguro ya que cualquiera puede revisarlo, comprobarlo y hacer las correcciones oportunas

Con los programas de Código Libre cualquiera puede:

revisar el código de los programas.

Modificar el programa y distribuir las modificaciones.

¿ Como 100 ojos ven mejor que 2 los problemas se detectan más rápidamente ?

Sin embargo gran parte de los programas de código libre han presentado problemas de seguridad:

Servidor WWW Apache,

Servidor de conexiones , OpenSSH,

Etc, etc.

Problemas en el núcleo de Linux:

En los últimos meses han aparecido diversos problemas de seguridad en el núcleo Linux.

Algunos de los problemas afectan a varias versiones (más de 4 meses).

Los problemas no han sido detectados por los desarrolladores.

Han aparecido diversas herramientas que hacían uso de estos problemas para conseguir acceso desde una cuenta normal a la de administrador.

Cuanta gente revisa el código de una aplicación ?

¿ El programador ?,

¿Quien hace la distribución ?

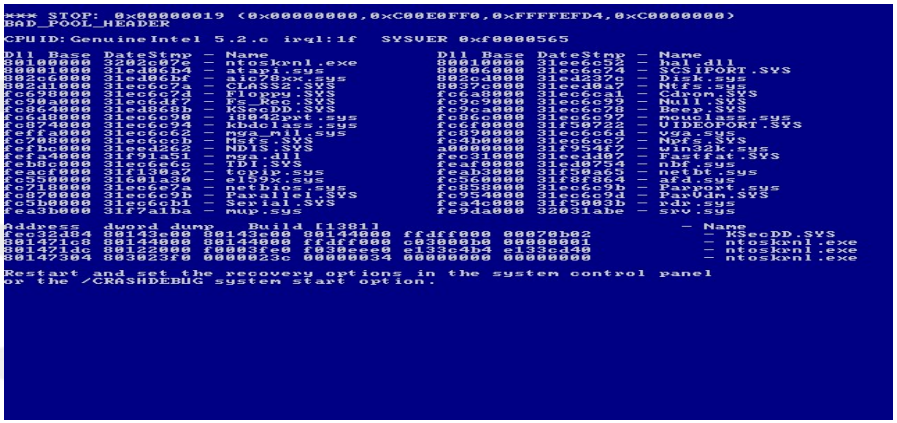
¿Qué sucede con las distribuciones “gratuitas” ?

¿Por qué ocurren los problemas ?

Los programas escritos en “C”, permiten en determinadas ocasiones que una entrada de datos pueda hacer que se modifique lel programa de una forma no deseada.

Los famosos “core” o segmentation faul en Unix/Linux

La famosa “BSOD” en otros sistemas operativos:



Estos fallos de programación es lo que permite a un atacante tomar control del programa

Problemas en la programación

Algunos estudios indican que un programador "experimentado" puede producir un fallo por cada 100 lineas de código.

Muchos de estos fallos son fácilmente evitables:

- No emplear cuando se programa algunas funciones estandard (scanf, get, etc).
- Emplear herramientas de revisión automática del código.

Sin embargo estos fallos se siguen produciendo.

- En aplicaciones "grandes", revisadas por mucha gente.
- ¿Qué pasa con los proyectos pequeños ?, versiones "beta", 0.x, etc.
- ¿Se emplean estas herramientas automáticas en las distribuciones Linux ?

Problemas en Aplicaciones WWW

Cada vez es más frecuente el uso de aplicaciones para la publicación de contenidos en Internet.

El concepto "L.A.M.P" permite el desarrollo de portales de contenidos con facilidad:

- Linux
- Apache
- MySql
- PHP

Sin embargo muchas veces los programas instalados no son actualizados, en **http://www.zone-h.org/en/defacements** hay una buena indicación sobre servidores WWW atacados.

Gran parte de estos ataques son debidos a fallos de programación en los sistemas de publicación de contenidos

Linux se administra mucho más fácilmente, es más fácil de configurar de una forma segura

Esta afirmación presenta un problema:

Los sistemas Linux/Unix son más fáciles de administrar que otros.

Existe la posibilidad de encontrar documentación sobre cualquier aspecto de administración de estos equipos.

Pero:

"Más fácil" no significa que no se tenga que emplear tiempo en la administración del equipo.

La información muchas veces se encuentra dispersa en varios lugares.

Desactivación de las medidas de seguridad incluidas por defecto:

- Mensajes de "avisos" de ataques
- Avisos de actualización

No actualización de algunos componentes

Actualizaciones automáticas:

Disponibles para la mayoría de las distribuciones de código Libre existentes.

Permiten tener el sistema actualizado.

Exigen que los “empaquetadores” de los programas mantengan las versiones actualizadas de los sistemas.

La actualización automática puede entrar en conflicto con las aplicaciones instaladas por el usuario.

Esto es cada vez más frecuente en las aplicaciones WWW .

Fraudes y Problemas de Seguridad independientes del S.O.

Phising

Phising: Deformación de “fishing”: ¿ ir de pesca ?

“Lanzar un “cebo” e intentar “pescar” información de usuarios incautos.

Empleada sobre con usuarios de comercio y banca electrónica para intentar obtener su información de acceso

Combinación de dos técnicas antiguas:

Difusión masiva de mensajes no deseados (SPAM)

“Ingeniería Social”, simular ser otra persona o entidad para obtener información del destinatario

Muchas veces no es un problema “técnico” sino de formación

Phising (II)

No solamente se trata de “mensajes bancarios”

Suplantación (Falsificación) de la dirección de correo de un usuario en un foro o lista de correo.

Intentos de acceso a cuentas de usuarios

Evolución de la Ingeniería Social:

1996: Llamadas a personal de una Universidad para “verificar” las cuentas de correo.

2003: “phising”, correos a usuarios de una una Universidad, solicitándoles la comprobación de sus datos.

Palabras de Acceso fáciles

Palabras de acceso vulnerables

Muchos sistemas de autenticación requieren el uso de identificadores (login) y claves (password)

Acceso a los equipos y servidores de la Universidad

Lectura de correo electrónico

Acceso Servicios externos (mensajería instantánea , banca electrónica)

Gran parte de los equipos Linux se configuran para que el usuario pueda trabajar desde fuera.

.....

Gran parte de estos sistemas emplean cifrado:

Evitan que alguien pueda “leer los datos”

Mayor “carga de trabajo del ordenador para realizar la conexión considerados “seguros”...

Problemas con las contraseñas

Problemas:

Existencia de herramientas por “fuerza bruta” para intentar obtener contraseñas.

Mismo usuario y clave en diversos servicios:

- Listas de correo, acceso al correo.
- Bases de datos , servicios de subscripción

¿Quién garantiza la confidencialidad de las contraseñas?

- ¿Están las bases de datos protegidas ?
- ¿Se almacenan las claves en “claro”?

Muchas veces se emplea la misma clave en diversos servicios , sin tener en cuenta los problemas.

¿Qué amenazas existen ?

Nivel General:

Infección y ataque por parte de Gusanos y Virus.

Perdida de información confidencial:

- códigos y licencias de programas instalados
- Información bancaria

Empleo del equipo como “puente” para atacar otros sistemas

A Nivel específico:

Muchos de estos programas están disponibles en la red, por lo que pueden ser utilizados para ataques “específicos” contra nuestro equipo.

Palabras de acceso

No emplear la misma palabra de acceso siempre:

Ejemplo

Diferenciar entre:

- Servicios internos (acceso al ordenador, correo corporativo)
- Servicios externos (Mensajería instantánea, correo en ISP)
- Servicios de alerta gratuitos, listas de correo.

Elegir una clave “sin sentido”

- Primera letra de cada palabra de una frase
- Añadir dígitos o códigos que indiquen el servicio

¿ (hnmplcor), para el correo ?

(Hoy No Me Puedo Levantar)

Palabras de acceso vulnerables

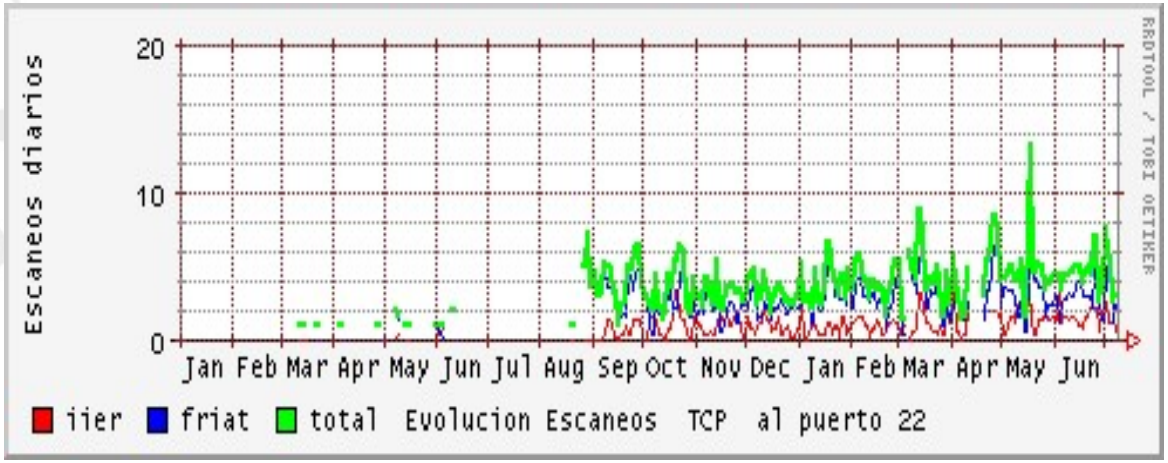
En Agosto de 2004 aparecio un programa para probar contraseñas en equipos Linux.

Claves sencillas:

usuario john , clave john.

Usuario root, clave 123456

etc



Una vez que los atacantes consiguen una clave vulnerable:

- Empleando una vulnerabilidad “local” consiguen acceder con permisos de administrador al equipo.
- Instalan diversas herramientas de ocultación (rootkits)
- Obtienen información sobre los usuarios del equipo y atacan otros sistemas.

Tras un año de ataques:

- Emplean diccionarios de usuarios específicos (nombres españoles para equipos españoles.
- Ajustan los ataques para buscar equipos dentro del mismo pais.
- Todavía se producen bastantes ataques por este motivo.
- Gran parte de los ataques se centran en equipos de usuarios finales, no servidores.

Soluciones

Soluciones

Hace falta una una concienciación del usuario final

Los mismos problemas en todas las plataformas.

Las mismas soluciones (formación y concienciación)

A nivel técnico:

Las Universidades y Centros de formación deben ser conscientes de las necesidades de seguridad

- No se puede seguir empleando las mismas técnicas de programación.

Las instalaciones y distribuciones Linux no deben olvidar la seguridad a la hora de configurar los equipos

Conclusiones

El acceso a una red implica que desde esta red se puede "acceder" a nosotros.

Los sistemas de Libre distribución tienen los mismos problemas de seguridad que otros sistemas propietarios.

Las causas más frecuentes por las que los ataques tienen éxito:

- Equipos no actualizados.
- Configuraciones inseguras de acceso.

Cada vez será más frecuente los ataques contra usuarios finales:

- Genéricos, obtención de información económica , principalmente.
- Específicos: Intento de obtención de información.

¿Preguntas ?