El proyecto Necromantux

David Fernández Vaamonde <davidfv@alfa21.com>
Carlos Temes Casas <carlos@alfa21.com>

IV Jornadas sobre el sistema operativo Linux
Universidade da Coruña

Guión

- ¿Qué es el Proyecto Necromantux?
- Necromantux Live CD
  - Proposito
  - Diseño
  - Características
  - Funcionalidades
  - Herramientas propias: Nigromante
  - Documentación en Necromantux
- El futuro de Necromantux Live CD
- Demostración práctica

¿Qué es Necromantux?

Diccionario de la RAE:

Nigromante

(De nigromancia).

1. com. Persona que ejerce la nigromancia.

¡Nigromancia!

1. f. Práctica supersticiosa que pretende adivinar el futuro invocando a los muertos.

(que tiene tratos con los muertos)

¿Qué es Necromantux?

- Anécdota: GPUL live CD para recuperación
- Surge entorno a una live CD
  - Recuperación de equipos principalmente
  - Seguridad
  - Reemplazo rapido de servicios
- Se amplia proyecto general:
  - Live CD
  - Metodologías de recuperación
  - Intercambio de conocimiento sobre el tema
  - Transmitir lo que sabemos (¡y aprender!).

¿Qué es Necromantux

Dos partes bien diferenciadas:

- **Foros, weblog y listas de correo**
  - **Soporte a la distribución**
  - **Discusión de metodologías de recuperación y seguridad**
- **Necromantux Live CD**
  - **Herramientas y entorno para aplicar todo eso**

Necromantux Live CD

Propósito:

Crear una herramienta para la recuperación, prueba y seguridad en equipos informáticos.

Una herramienta de "intervención rápida" ante cualquier tipo de desperfectos:

- **Fallos hardware y recuperación de infraestructura (discos, particiones...)**
- **Seguridad informática en el equipo (intrusiones, detección de problemas, forense)**
- **Reemplazo rápido de servicios (routing, firewalling, etc...)**

Necromantux Live CD

Diseño

- Basada totalmente en software libre
- Se usan proyectos de software libre como base de trabajo
  - Debian:
    - Sistema de paquetes (Base de distribución)
    - Repositorios APT (Nigromante, Documentación)
    - Herramientas de Debian (Añadir paquetes)
  - Proyecto Metadistros
    - "Calzador"
    - Sistema de distribución (retocado en NCX)
  - Trasno
    - Linux en gallego

Necromantux Live CD

Diseño (II)

- La distribución ha de ser ligera y correr en todos los equipos
  - Gestor de Ventanas: Fluxbox
  - Arranque en texto por defecto
  - Posibilidad de eliminar todas las "filigranas"
  - ...
- La distribución tiene que ser cómoda
  - Configuración de idioma simple
  - Listas de programas y su explicación
  - Un entorno gráfico cómodo y ligero
  - Herramientas que hagan todo más sencillo (Nigromante)
  - Arranque como root (¿O no?)

Necromantux Live CD

Diseño (III)

- **Programas:**
  - Meter siempre los más ligeros
  - Cubrir ciertas funcionalidades
  - *SIEMPRE* han de funcionar
    - (por esto, todavía no hay version definitiva ;))
- **Feedback:**
  - Necesitamos gente que la use para saber si es o no comoda :)

Necromantux Live CD

Características

- **Arranque:**
  - Permite ejecutar programas en arranque:
    - Grub
    - Memtest
  - Permite arrancar en distintos lenguajes
  - Configurar red por DHCP
  - "Pretty-boot" o arranque normal
  - Saltos de algunas partes "conflictivas" (NOSCSI)

- **Configuración:**
  - Autodetección de hardware:
    - Red, Sonido, etc...
  - Soporte de tarjetas wireless
  - Autoconfiguración de X-Window

Necromantux Live CD

Características (II)

- **Software ajeno:**
  - Completamente libre
  - Ligero y bien cohesionado
  - X-Window: Escogemos cosas de ambos mundos (Gnome-KDE)
    - Ej: gaim o smb4k y konqueror
  - X-Window: Window Manager ligero (fluxbox)

- **Software propio:**
  - Scripts que afinan la distro (fondos a medida, etc...)
  - Nigromante: Un "wizard" que simplifica tareas

Necromantux Live CD

Características (II)

- **Documentación:**
  - **Colaborativa.**
  - **Consta de:**
    - **Manual**
    - **Metodologías**
    - **Enlaces**
- **Proyecto patrocinado por una empresa del ramo: Alfa21**
  - **Diseño e imagen**
  - **Site**

Necromantux Live CD

Funcionalidades

- **Recuperación de equipos:**
  - **Discos: (MBR, Tablas de particiones, datos)**
- **Pruebas**
  - **Memoria**
  - **Discos**
  - **Tarjetas de red**
  - **CPU**
  - **Servicios de red (Correo, web, DNS...)**
- **Reemplazo de servicios**
  - **Firewalling**
  - **Routing**
- **Auditoria, Monitorización y seguridad**
  - **SNMP**
  - **Detección de intrusos**
  - **Herramientas de gestión de red**

Necromantux Live CD

Herramientas Propias: Nigromante

- **Herramienta que agrupa tareas habituales de la distribución**
  - **Configuración de red**
  - **Copia de tabla de particiones**
  - **Copia del mbr**
  - **Guardado de configuraciones**
  - **Creación de disquetes**
- **Diseño:**
  - **Bash+Zenity**
  - **Modular (Se incorporan módulos de todo tipo)**
  - **Internacionalizable**
- **Guarda la "inteligencia contextual" y la ofrece a los demás.**
- **Versión actual: 0.1**
- **Disponible en el repositorio APT**

Necromantux Live CD

El futuro de Necromantux Live CD

- **Intento de una versión estable (programa de Snapshots)**
- **Nuevas versiones:**
  - **Incorporación de nuevo software:**
    - **Antivirus libre**
    - **HoneyPot**
    - **Proxies ligeros**
    - **Librerias ligeras de programación de red**
  - **Reescritura de partes**
    - **¿Arranque como usuario normal?**
    - **Home en Pendrives USB**
    - **Modularización de la detección de hardware**
    - **...**

El futuro de Necromantux Live CD (II)

- **Ampliación de Nigromante**
  - **Scripts de securización**
  - **Scripts de Honeypotting**
  - **Mas clases de disquetes en el módulo**
- **Necromantux LITE (1 disquete, 1 cd 8mm o 1 Pen USB)**
- **Ampliación de las metodologías, manual y enlaces en la web**

La distribución y el software generado esta disponible bajo licencia GPL, todo, absolutamente todo es software libre.

Demostración práctica:

- **Roadtrip por la distribución y su software:**
  - **Modo texto**
  - **Modo gráfico**
- **Presentación de algunos de sus programas:**
  - **Programas en el arranque (memtest)**
  - **Programas en la distribución**
    - **Browser SMB (smb4k+Konqueror)**
    - **En web (ntop, autopsy)**
    - **Otros (nmap, QTparted, etc...)**
- **Presentación de nigromante:**
  - **Ejecución y pruebas**
  - **"Tripas" de Nigromante**

Enlaces

- **Web de Necromantux**
  - **http://necromantux.gpul.org**
  - **http://necromantux.alfa21.com**
- **Downloads de Necromantux**
  - **http://necromantux.alfa21.com/?q=downloads**
- **Libros de Necromantux**
  - **http://necromantux.alfa21.com/?q=book**
  - **(Manual, Metodologías, Enlaces)**
- **Lista de correo (gpul-necromantux)**
  - **http://ceu.fi.udc.es/mailman/listinfo/gpul-necromantux**
- **Patrocinadores y participantes:**
  - **http://www.alfa21.com**
  - **http://www.gpul.org**

¡Gracias por venir!