

---

# Necromantux

---

<http://necromantux.gpul.org>

---

# índice

- 1. Pruebas de hardware del sistema
- 2. Seguridad en Necromantux
- 3. Auditoría y gestión de red

---

# 1.- Pruebas de Hardware

- 1.- Pruebas de memoria
- 2.- Procesador
- 3.- Discos duros
- 4.- Tarjetas de red
- 5.- Información del hardware

---

## 1.1.- Pruebas de memoria

- Teclar “memtest86+” en el arranque de la distribución
- Una vez arrancado el SO teclar en la línea de comandos: memtest (indicando el total de memoria que tenemos – M=MB y G= GB – y opcionalmente un fichero para enviar el resultado:
  - Memtest 128M –l fichero.log

---

## 1.2. Procesador

- Necesitamos 2 programas: uno para proporcionar carga de trabajo al procesador y otro para ver los parámetros de sistema ( temperatura,...) durante la prueba:
  - Cpuburn: genera carga
  - Mbmon: modo texto #mbmon -A 10
  - Xmbmon: modo gráfico # xmbmon -A ( -A indica autodetectar sensores)
- Existen distintos binarios por procesador, debiendo ejecutar el adecuado:

Procesador	Binario
AMDK6	burnK6
AMDK7	Burnk7
Pentium/Pentium Pro	ProburnP5
Pentium II / Pentium	IIIburnP6
- También podemos teclear simplemente burn en la línea de comandos

---

## 1.3 Discos duros

- a) Pruebas clásicas: comprobar corrección (p.e. badlocks).
  - Si no nos importa perder la información que tenga el disco duro haremos pruebas de lectura/escritura
    - Badlocks -w /dev/hda
  - O de sólo lectura
    - Badlocks -n /dev/hda
- b) Pruebas informativas
  - Extraer estadísticas que el propio disco duro genera durante su trabajo. Por ejemplo smartctl -pertenece al paquete smartmontools -.
    - Samrtcl -H /dev/hda
- c) Pruebas de stress: uso intensivo de E/S para probar funcionamiento y rendimiento:
  - Dbench: dbench -s -S10 # 10 clientes leen/escriben de manera síncrona
  - Bonnie++: bonnie -a root

---

## 1.4 Tarjetas de red

- `mii_diag`: usa los registros de la tarjeta
  - `mii_diag eth0`
  
- `nictools`: en función del chipset tendremos distintos binarios, p.e. `rtl8139_diag`

---

## 1.5 Información del Hardware

- Usando /proc y algún programa adicional
  - `cat /proc/cpuinfo`
- `lspci`: dispositivos PCI
- `cardinfo`: para PCMCIA
- `isadump`: dispositivos ISA
- `lshw`: incluso podemos solicitarle una salida de la información en formato html

```
lshw -html >in.html
```

---

## 2. Seguridad

1. Herramientas de exploración
2. Redes inalámbricas
3. Redes windows
4. Equipo local
  1. Tiger
  2. Detección de cambios en los ficheros
  3. Detección de rootkits
5. Recuperación de incidentes leves de seguridad habituales
  1. Olvido contraseña de root
  2. Pérdida de la contraseña de la BIOS
  3. Recuperación de contraseñas de administración Windows

---

## 2.1 Herramientas de exploración

- Nmap con detección del SO y versión Probe
- Consultar foros con Bugtraq los fallos más comunes
- Nessus (cliente/servidor):
  - podemos iniciar el servidor con “Nigromante” ( botón dcho – Wizards – Inicio y parada de servicios)
  - Después iniciamos el cliente: botón dcho – redes – seguridad – Nessus conectamos a localhost con login “ncxuser” y contraseña “necromantux”

---

## 2.2 Redes inalámbricas

- Aireplay: para provocar tráfico y localizar la clave WEP, capturando los datos con Airodump o Aircrack-ng.
- Posteriormente podemos romper la clave con Aircrack-ng.
- Kismet: inspeccionador de redes wireless de la zona, detector de intrusos o de posibles ataques.

---

## 2.2 kismet

- Algunos ataques que permite detectar:
  - NESTUMBLER: Uso del programa netstumbler para análisis de redes
  - Deauthflood: Ataque de desautenticación por flood – para obtener datos relativos a credenciales, essids, ...
  - LUCENTEST: uso de programas de pruebas como lucent
  - WELLENREITER: uso del analizador wireless del mismo nombre
  - CHANCHANGE: cambios de canal que pueden indicar un AP falso
  - BCASTDISCON:ataques que intentan desasociar a los clientes de los ap – buscando tráfico interesante o capturar essids ocultos
  - AIRJACKSSID: AP con essid propio de la herramienta Airjack
  - PROBENOJOIN: dispositivos que prueban redes abiertas sin asociarse a ellas
  - DISASSOCTRAFFIC: ataque de desasociación
  - NOPROBERESP: posible ataque DoS
  - BSSTIMESTAMP: posible ataque spoof del BSSID ( mac del AP)
- Mediante el uso de kismet\_drone y kismet\_server podemos situar sondas en ordenadores y enviar con kismet\_drone las señales a un único servidor:
  - La configuración se realiza:
    - /etc/kismet.conf
    - Sondas: /etc/kismet\_drone.conf
  - En el primero configuramos las fuentes de datos (drones)  
source=madwifi\_g,ath0,madg  
source=kismet\_drone,192.168.1.100:3501,drone  
enablesources=drone,madg
    - Hemos habilitado dos fuentes de datos la primera la propia tarjeta y la segunda una sonda, finalmente las habilitamos
  - En el segundo lo configuramos para realizar una captura normal de datos

## 2.3 Redes Windows

Además de nessus podemos emplear, p.e. smb-nat apra comprobar carpetas compartidas y/o claves.

## 2.4 Equipo local

- Tiger: conjunto de scripts que tratan de ahcerse root en un sistema:  
tiger -e -E -H -l /root
- Herramientas para detectar cambios en los ficheros:
  - cuando sospechamos que hemos sido atacados podemos comparar lo ficheros con las firmas de los mismos que previamente habremos almacenado p.e. en un disquete
  - Fam
  - AIDE: clon del producto no libre Tripwire. La configuración se lleva a cabo en /etc/aide/aide.conf
    - Indicamos dónde se escribirán las bases de datos y los directorios que se chequearán:  
database=file:/root/aide.db  
database\_out=file:/root/aide.db.new
    - Creamos alias que representan qué se comprobará en cada fichero:  
Binlib=p +i+n+u+g+s+b+m+c+md5+shal ( permisos -p-, inodos -i -,links-n-, usuario - u-, grupo -g-,...
    - Posteriormente definiremos directorios y los alias de los objetos a aplicar a los ficheros:  
/lib Binlib
    - Crearemos la primera vez la base de datos:  
aideinit
    - Guardaremos la BD en un lugar distinto de la máquina del sistema para compararla con el sistema actual:  
aide -C
- Herramientas para detección de rootkits:
  - Rootkits son conjuntos de programas introducidos en una intrusión que sustituyen a programas habituales (ls, netstat,...) con la intención de camuflar la intrusión ocultando procesos, conexiones de red,....Son síntoma inequívoco de que el sistema ha sido vulnerado.
  - **chkrootkit** : detecta los rootkits más conocidos. Simplemente le indicamos el directorio dónde hemos montado el sistema a auditar:  
chkrootkit -r /mnt/system
  - **Clamav**: un antivirus muy usado bajo linux

## 2.5 Recuperación de incidentes leves de seguridad

### a) Olvido de la contraseña de root

- a) Primero debemos montar el sistema de ficheros del sistema "huésped".
- b) Pasamos a trabajar en el sistema huésped como administrador:  
`chroot /mnt/system bash`
- c) Cambiamos la contraseña. Como somos administradores no nos pide la anterior  
`passwd`

### ■ Pérdida de la contraseña de una BIOS

- a) `cmospwd` :
  - Para guardar el contenido en un fichero: `cmospwd /d /w fichero`
  - Para averiguarla: `cmospwd`: nos dará contraseñas para las BIOS que que conoce o alternativas para seguir.
  - Podemos intentar borrar la CMOS para anular la contraseña:  
`cmospwd /k`
  - Como aviso de los autores "NUNCA" borrar la CMOS del IBM ThinkPad 765 y usar el comando como último recurso.

### a) Recuperación de contraseñas de administración de Windows:

- `chntpwd`: sólo sobre FAT no sobre NTFS, de momento
  - Primero debemos localizar el fichero SAM, en XP: `c:\windows\system32\config\SAM`
  - Para ver la lista de usuarios: `chntpw -l /mnt/system/windows/system32/config/SAM`
  - Para cambiar la contraseña de un usuario: `chntpw -u usuario /mnt/system/windows/system32/config/SAM`
  - Otra opción muy útil que permite modificar registro, usuarios,.. `chntpw -i`

---

## 3. Auditoría y Gestión de red

1. Introducción
2. Monitorizando dispositivos SNMP
3. ¿Qué hay en la red?
4. Aspirando el éter
5. Midiendo y probando la red
6. Redes windows
7. Redes wireless

---

## 3.1 Introducción

- Podemos usarla para montar rápidamente un servicio de red que ha sido dañado y se ha caído, p.e. cortafuegos, router,...
- Para comenzar debemos configurar la red:
  - Manualmente:
    - Nigromante – configuración manual de red
    - Ifconfig eth0 ip\_deseada
  - Mediante DHCP: dhclient -i eth0
- Deberíamos asegurar el SO, ya que sino puede convertirse en un punto vulnerable a ataques: Nigromante – Asegurador de Necromantux.

---

## 3.2 Monitorizando dispositivos SNMP

- SNMP (Single Network Management Protocol): no sólo lo soporta este Live CD, sino que, además, se puede monitorizar a través de SNMP usando la comunidad `necromantux` por defecto y cualquier cliente capaz de acceder a un dispositivo SNMP estándar.
- Previamente deberemos haber iniciado el servicio, p.e. `NetworkManager` y parada de servicios
- Herramientas de línea de comandos: `snmpget` y `snmpwalk`; `snmpwalk -v 1 -c necromantux crypt`
- `tkined`

---

## 3.3 ¿Qué hay en la red?

- Ping a la dirección de broadcast:  
ping -b 192.168.0.0
- nmap y su versión gráfica nmapfe
  - Nmap -sv -o 192.168.0.0/24
    - v: versiones de servicios
    - o: versiones del SO
    - oN : para sacarlo a fichero
    - oX: fichero XML

---

## 3.4 Aspirando el éter: sniffers o analizadores de red

- Tcpcmdump: uno de los mejores sniffers, trabaja en modo consola
- Ethereal: interfaz gráfica muy intuitiva, con versiones para windows y linux, capaz de cargar los ficheros generados con tcpcmdump.
- Ettercap: engaña a la red y reenvía los paquetes a su destinatario (man in the middle)
  - Tiene dos interfaces en modo texto, una con ventanas (ettercap -C) y otro sin ellas.
  - Podemos elegir dos tipos de sniffing:
    - Unified Sniffing: con sólo una tarjeta de red, pero el tráfico se queda en nuestro equipo.
    - Bridged Sniffing: con dos interfaces de modo que podamos reenviar los paquetes al destinatario.
  - Con la opción Host- Scan for hosts, obtenemos los hosts existentes en la red
  - Con view- profiles: vemos con que tipo de máquinas estamos actuando, los perfiles de los puntos de conexión que intervienen en la comunicación: MAC, fabricante,...
  - Start – Start sniffing
  - Para que pasen por nuestra máquina usaremos las técnicas “man in the middle” que encontraremos en el menú Mitm.
    - La más básica y conocida es ARP Poisoning: respuestas ARP que hacen que el switch asocie la dirección de nuestro ordenador con la del equipo al que debería ir.
    - Si no se usan parámetros captura el tráfico de todos los hosts.
  - View- connections: vemos las conexiones y pulsando en cualquiera vemos el contenido

---

## 3.5 Midiendo y probando la red

- Son programas para obtener estadísticas, rendimientos,...
- ethstatus : interfaz, tráfico,...
- Ettercap: view – statistics
- iptraf
- mtr : nos permite, dada una IP, obtener las máquinas por dónde circula hacia su destino: `mtr 192.168.1.100`
- bing: para medir el ancho de banda entre dos puntos  
`bing 192.168.1.100 192.168.1.200`
- iperf: más fiable que el anterior, pero requiere que esté funcionando en modo servidor en uno de los equipos y cliente en el otro.  
`iperf -s #arrancar en modo servidor`  
`iperf -c 192.168.1.1. #arranca el cliente y se conecta con el equipo 192.168.1.1`
- hping2, isic, fragroute,...

---

## 3.6 Redes Windows

- smb4k: ver las máquinas windows de la red y los recursos que comparten
- nbtscan: redes con NetBios  
nbtscan -r 192.168.1.0/24 #mostrar servidores NetBios  
nbtscan -s ":" -r 192.168.1.0/24 #separados con ":"
- smb-nat: máquinas con NetBios intentando acceder a los shares con passwords por defecto, intentando recuperar información de seguridad sobre la misma:
  - smb-nat 192.168.1.1-10
  - También se puede pasar una lista de usuarios y passwords:  
:  
smb-nat -u lista\_usuarios -p lista\_passwords 192.168.1.1

---

## 3.7 Redes Wireless

- wavemon: permite ver señales de ruido, relación señal a ruido y calidad del enlace, velocidad de conexión, modo de la tarjeta,...
- Para capturar tráfico nuestra tarjeta tiene que tener la posibilidad de trabajar en modo monitor – equivalente al modo promiscuo en redes de cable.
- Airtsnort y airtraf: permiten ver tipos de conexiones, número de paquetes
- Kismet: completo analizador de tráfico que permite comprobar conexiones, pruebas de rotura de claves,...(fichero /etc/kismet/kismet.conf)

---

# Bibliografía

- Proyecto necromantux:  
<http://necromantux.gpul.org>
- Mundo Linux: números 78, 80, 85