Al habla de Ingeniería Inversa de Malware (Reverse-Engineering Malware – REM) es obligatorio hablar del experto investigador Lenny Zelter y aun más cuando recién está realizando los cursos por parte de SANS sobre esta materia.
Entre uno de sus proyectos de investigación se encuentra el desarrollo de una distribución de GNU/Linux basada en Ubuntu y enfocada al Análisis e Ingeniería Inversa de Malware. REMnux se presenta entonces como un completo entorno de análisis de malware que puede ser incluido en nuestros laboratorios de investigación. Entre sus funcionalidades se encuentra la posibilidad de implementación de servicios en determinados puertos para simular el sistema que recibe algún tipo de instrucción o petición desde un equipo del laboratorio infectado.
Permite además realizar análisis de malware basado en aplicaciones web, como javascripts maliciosos, apps de java y películas en flash (animaciones maliciosas). También dispone de diferentes herramientas para el análisis en busca de documentos maliciosos como pueden ser los de Microsoft Office, OpenOffice y PDF's. Algo que llama aun más la atención en la funcionalidad e realizar ejecuciones del malware en el propio REMnux y realizar volcados de memoria para su posterior análisis en el mismo sistema.
REMnux se distribuye como un archivo imagen de VMWare, por lo tanto solo basta descomprimir el archivo descargado y luego abrir con cualquiera de los productos de VMWare (WorkStation, Server, Player).

Entre las herramientas incluidas se encuentran las siguientes:
Análisis de Malware en Archivos Flash: swftools, flasm, flare.
Análisis de Boots IRC: Inspire, Irssi.
Monitoreo de red: Wireshark, Honeyd, INetSim, fakedns, fakesmtp, NetCat.
Análisis de JavaScripts: Firebug, NoScript, JavaScript Deobfuscator, Rhino debugger, SpiderMonkey, Windows Sript Decoder, Jsunpack-n.
Interacción con malware basado en web: TinyHTTPd, Paros Proxy.
Análisis de Shellcode: gdb, objdump, Radare, shellcode2.exe
Detección de protecciones y cifrados: upx, packerid, bytehist, xorsearch, TRiD.
Análisis de PDF maliciosos: Didier's PDF tools, Origami framework, Jsunpack-n, pdftk.
Análisis de memoria: Volatility Framework

Dejo algunos screen shots del entorno REMnux.
Boot y pantalla de login:

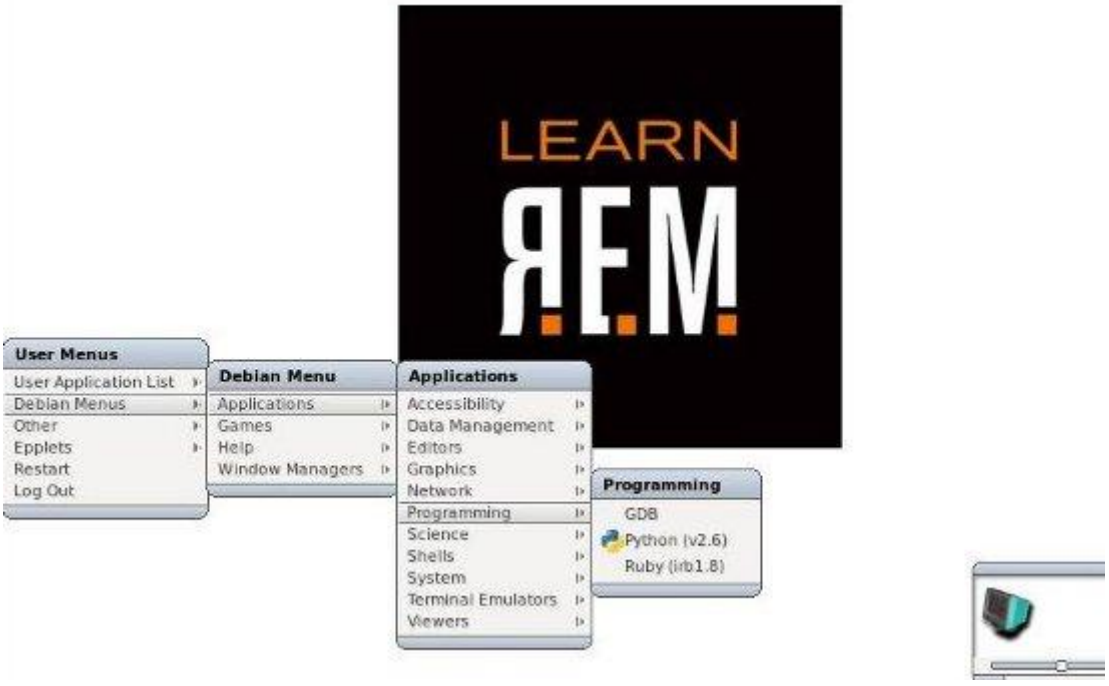
```
fsck from util-linux-ng 2.16
/dev/sda1: clean, 68574/373152 files, 391692/1490020 blocks
[    5.716793] ACPI: I/O resource piix4_smbus [0x1040-0x104
I region SMB_ [0x1040-0x104b]
 * Setting preliminary keymap...
 * Starting AppArmor profiles
 * Setting up console font and keymap...
Ubuntu 9.10 remnux tty1

remnux login: _
```

User: remnux

Password: malware

X:



Tools:

[Página oficial del proyecto REMnux]

[Descargar REMnux] - **MD5:** dc28330411acafc6b7f595a11e8b7ea4

Lo que REMnux NO es

REMnux no es una distribución de lujo que fue construida desde cero (o from scratch)... En términos simples, es una máquina virtual que corre Ubuntu y tiene varias herramientas útiles para deteccion y analisis de malware creadas en él.
REMnux no pretende incluir todas las herramientas de análisis de malware existentes. Muchas de estas herramientas están diseñadas para funcionar en Microsoft Windows, y los investigadores prefieren utilizar los sistemas Microsoft Windows para hacerlas funcionar. Si usted está interesado en ejecutar el análisis de herramientas de Windows en una plataforma Linux, echa un vistazo al «Zero Wine project».
Si usted está buscando una distribución Linux, mas completamente equipada, más centrada en el análisis forense, eche un vistazo a «SANS Investigative Forensic Toolkit (SIFT) Workstation».