

# Bootloaders Tomo I – x86 BIOS Legacy

## Tabla de contenidos

El autor.....	¡Error! Marcador no definido.
Preparando el espacio de trabajo .....	¡Error! Marcador no definido.
Para quién es este libro .....	¡Error! Marcador no definido.
¿Cómo leer este libro?.....	¡Error! Marcador no definido.
Introducción.....	¡Error! Marcador no definido.
Saca el máximo partido de leer este libro .....	¡Error! Marcador no definido.
Convenciones en el libro .....	¡Error! Marcador no definido.
Detalles sobre las fuentes.....	¡Error! Marcador no definido.
Repositorio en Github.....	¡Error! Marcador no definido.
Alcance de este libro .....	¡Error! Marcador no definido.
Contactar .....	¡Error! Marcador no definido.
¡Deja una revisión!.....	¡Error! Marcador no definido.
Capítulo 0. Mi entorno de trabajo .....	¡Error! Marcador no definido.
Linux .....	¡Error! Marcador no definido.
Makefile vs build.sh vs .py .....	¡Error! Marcador no definido.
nasm — Netwide Assembler .....	¡Error! Marcador no definido.
gdb.....	¡Error! Marcador no definido.
GEF, pwndbg y PEDA.....	¡Error! Marcador no definido.
GEF .....	¡Error! Marcador no definido.
pwndbg.....	¡Error! Marcador no definido.
PEDA.....	¡Error! Marcador no definido.
radare2 .....	¡Error! Marcador no definido.
QEMU .....	¡Error! Marcador no definido.
Capítulo 1. Lo más básico.....	¡Error! Marcador no definido.
El inicio .....	¡Error! Marcador no definido.
El triple fault .....	¡Error! Marcador no definido.
Primer fallo (first fault).....	¡Error! Marcador no definido.
Segundo fallo (double fault).....	¡Error! Marcador no definido.
El proceso con BIOS Legacy.....	¡Error! Marcador no definido.

El MBR y el bootloader.....	;Error! Marcador no definido.
La memoria en arranque .....	;Error! Marcador no definido.
El Modo Real (Real Mode) .....	;Error! Marcador no definido.
Bootloader mínimo.....	;Error! Marcador no definido.
Invocación simple de QEMU .....	;Error! Marcador no definido.
Crear un disco y cargarlo con QEMU.....	;Error! Marcador no definido.
Registros de 32 bits desde Modo Real .....	;Error! Marcador no definido.
Capítulo 2. Usando interrupciones.....	;Error! Marcador no definido.
La interrupción int 10h .....	;Error! Marcador no definido.
La interrupción int 11h .....	;Error! Marcador no definido.
La interrupción int 12h .....	;Error! Marcador no definido.
La interrupción int 13h .....	;Error! Marcador no definido.
Lectura con CHS.....	;Error! Marcador no definido.
Puertos serie para hacer debug .....	;Error! Marcador no definido.
Lectura en modo Extendido.....	;Error! Marcador no definido.
La interrupción int 15h .....	;Error! Marcador no definido.
Capítulo 3. Bootloaders más complejos .....	;Error! Marcador no definido.
Bootloader con dos etapas.....	;Error! Marcador no definido.
Unos dibujos básicos con VGA .....	;Error! Marcador no definido.
Capítulo 4. El Modo Irreal (Unreal mode).....	;Error! Marcador no definido.
Línea A20.....	;Error! Marcador no definido.
Global Descriptor Table (GDT) .....	;Error! Marcador no definido.
Hidden bases.....	;Error! Marcador no definido.
Uso de interrupciones.....	;Error! Marcador no definido.
A por el Modo Irreal: versión simplificada .....	;Error! Marcador no definido.
Para qué sirve esto.....	;Error! Marcador no definido.
Previo a cargar kernel de Linux de más de 1 MB .....	;Error! Marcador no definido.
Breve introducción al diagnóstico en arranque .....	;Error! Marcador no definido.
Paso 1: QEMU con las opciones de gbd .....	;Error! Marcador no definido.
Paso 2: abrimos pwndbg, gdb o r2.....	;Error! Marcador no definido.
Paso 3: diagnosticar cosas relevantes .....	;Error! Marcador no definido.
Capítulo 5. Cargando el kernel de Linux.....	;Error! Marcador no definido.

Primer paso: stage1 .....	;	Error!	Marcador no definido.
Segundo paso: stage2 leyendo kernel de Linux.....	;	Error!	Marcador no definido.
Segundo paso bis: debug de la escritura en memoria alta;	Error!	Marcador	no definido.
Tercer paso: cómo el kernel de Linux toma el control;	Error!	Marcador no definido.	
1. Nuestro propio initrd .....	;	Error!	Marcador no definido.
2. Pasamos un initrd real .....	;	Error!	Marcador no definido.
Tercer paso bis: saltar a algo ejecutable en el kernel .;	Error!	Marcador no definido.	
Cuarto paso: Linux Boot Protocol .....	;	Error!	Marcador no definido.
La cabecera del kernel de Modo Real .....	;	Error!	Marcador no definido.
Estructura de memoria en Modo Real.....	;	Error!	Marcador no definido.
Capítulo 6: Kernel de Linux funcionando .....	;	Error!	Marcador no definido.
A) Continuamos con las decisiones tomadas: parchear;	Error!	Marcador no definido.	
Paso 1. Buscar firma “HdrS” y leer valor de setup_sects;	Error!	Marcador	no definido.
Paso 2. Leer el valor de setup_sects.....	;	Error!	Marcador no definido.
Paso 3. Calcular el valor de setup_size .....	;	Error!	Marcador no definido.
Paso 4. Copiar el setup a la dirección correcta .....	;	Error!	Marcador no definido.
Paso 5. Copiar el payload a la dirección correcta ;	Error!	Marcador no definido.	
Paso 6. Ubicar la línea de comando (kernel_cmdline);	Error!	Marcador	no definido.
Paso 7. Ubicar initrd .....	;	Error!	Marcador no definido.
Paso 8. Tipo de bootloader .....	;	Error!	Marcador no definido.
Paso 9. Verificar los campos del header.....	;	Error!	Marcador no definido.
Paso 10. Saltar al punto de entrada del kernel .....	;	Error!	Marcador no definido.
Crear el disco de arranque de nuevo.....	;	Error!	Marcador no definido.
Problemas con el diagnóstico .....	;	Error!	Marcador no definido.
Problemas con qemu+gdb y radare2 .....	;	Error!	Marcador no definido.
Monitor con QEMU.....	;	Error!	Marcador no definido.
¿Qué estamos haciendo mal?.....	;	Error!	Marcador no definido.
B) Corregimos y seguimos el estándar .....	;	Error!	Marcador no definido.
Estructura de memoria predecible.....	;	Error!	Marcador no definido.

Cambios en el código .....	¡Error! Marcador no definido.
Paso 1: verificación de salud .....	¡Error! Marcador no definido.
Paso 2: cargar initrd en memoria .....	¡Error! Marcador no definido.
Paso 3: iniciamos boot protocol con setup_sects	¡Error! Marcador no definido.
Paso 4: copiamos el kernel setup .....	¡Error! Marcador no definido.
Paso 5: copiamos el payload del kernel .....	¡Error! Marcador no definido.
Paso 6: kernel cmdline .....	¡Error! Marcador no definido.
Paso 7: informamos a setup sobre el initrd .....	¡Error! Marcador no definido.
Paso 8: tipo de bootloader .....	¡Error! Marcador no definido.
Paso 9: kernel loadflags y final del heap .....	¡Error! Marcador no definido.
Paso 10: transferimos el control al kernel .....	¡Error! Marcador no definido.
Capítulo 7. Modo Protegido (Protected Mode) .....	¡Error! Marcador no definido.
Cambios en la estructura de las etapas .....	¡Error! Marcador no definido.
El nuevo stage1 .....	¡Error! Marcador no definido.
El nuevo stage2 .....	¡Error! Marcador no definido.
Pruebas de verificación de Modo Protegido .....	¡Error! Marcador no definido.
Lectura de disco en 32 bits .....	¡Error! Marcador no definido.
Cargando el kernel en Modo Protegido .....	¡Error! Marcador no definido.
Capítulo 8: stage2 mejorado .....	¡Error! Marcador no definido.
Nuevo build.py .....	¡Error! Marcador no definido.
Mejoras en el initrd .....	¡Error! Marcador no definido.
Mejoras en el init.sh .....	¡Error! Marcador no definido.
Cambios en stage2.asm .....	¡Error! Marcador no definido.
Capítulo 9: el Modo Largo .....	¡Error! Marcador no definido.
Qué es el Modo Largo .....	¡Error! Marcador no definido.
Entrando en Modo Largo .....	¡Error! Marcador no definido.
Código en C .....	¡Error! Marcador no definido.
Mini-kernel en C .....	¡Error! Marcador no definido.
Mini-kernel en Rust .....	¡Error! Marcador no definido.
Capítulo 10. Un kernel con userspace .....	¡Error! Marcador no definido.
Niveles de privilegio .....	¡Error! Marcador no definido.
Syscalls .....	¡Error! Marcador no definido.

Mejorando nuestro kernel .....	¡Error! Marcador no definido.
Tabla IDT: idt64.asm.....	¡Error! Marcador no definido.
GDT64 mejorada .....	¡Error! Marcador no definido.
Kernel con soporte para syscall.....	¡Error! Marcador no definido.
Capítulo <EOT>: nuevos libros y trabajo futuro .....	¡Error! Marcador no definido.
Anexo I. Códigos de resultado de la int 13h.....	¡Error! Marcador no definido.
Anexo II. Identificadores de bootloaders.....	¡Error! Marcador no definido.
Anexo III. herramientas estáticas .....	¡Error! Marcador no definido.
Python 3.....	¡Error! Marcador no definido.
Frida server .....	¡Error! Marcador no definido.
Referencias .....	¡Error! Marcador no definido.