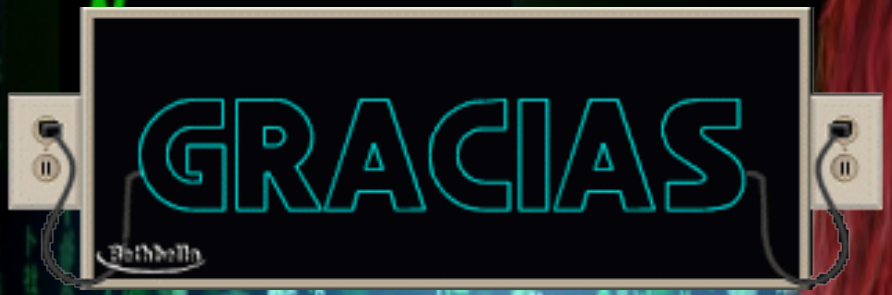
LXC
HACKING & HARDENING GAMES

Kao & Kio ArdeTroya

CAPITULO 1
THE PHILOSOPHY & CORDIALITY...

EN PRIMER LUGAR:



- A vosotros por elegirnos, estar aquí y a la organización por traernos.

Sin olvidar a:

S4uron,Mari,Ninguno,Belky, Kalambre, Borja, Vilas...(Seguro que me olvido de un montón de nombres aquí)

Por sus consejos para esta presentación y aguantar nuestro stres en los días previos.

Un especial agradecimiento a Alberto Cartier de ttqstraducciones.com por su taller de como hablar en público cosa que nos daba pánico, Gracias Alberto, Seguro que nos ayuda un montón!.

¿QUÉ VAMOS A VER?

Round 1

@The theory (1h/30):~$

1. ¿Qué es lxc?
2. Diferencias con otros tipos de de virtualización
3. Componentes
4. Configurando lxc
5. Con/Sin privilegios
6. Backup y mantenimiento

Round 2

@The practice (1h/30):~$

1. Montar nuestras infras en lxc how to
2. sanboxing con lxc
3. intentando atacar lxc
4. ~~Preguntas>Oh yeah!~~ ->Fuera con Cerveza!
4. Enjoy or just joint ;)

¿QUIENES SOMOS?

Kao

@MininaKaotika

Kio Ardetroya

@KioArdetroya

hackingcodeschool.net

WHY HARDENING?

Aprender a defenderme me permite atacar relativamente tranquila.

Todo el mundo te habla de sus exploits y bla bla bla pero nadie te cuenta como se oculta/protege.

¿DE DONDE SALE ESTE TALLER?

El problema:

Necesitabamos aislar ciertas cosas en ciertos casos

Muchos clientes pequeños compartiendo servicios en el mismo servidor.

Pocas ganas de que me tocaran la moral, erhm digo... el teléfono.

El planteamiento:

Si meto a cada uno de ellos en su cajita, con sus propios servicios, si alguno la lía le afecta a él sólo...

La idea:

Usemos virtualización

¿DE DONDE SALE ESTE TALLER?

La investigación:

Probamos diferentes sistemas de virtualización , pero eran muy rígidos o complejos o privativos o poco versátiles.

Ninguno nos acababa de convencer

La solución:

Linux Containers (LXC);

CAPITULO 2
CONOCIMIENTOS PREVIOS Y REPASO

¿QUE NO ES LXC?

LXC ! {

- Emulación
- Virtualización Completa
- Virtualización asistida por hardware
- Paravirtualización

}

“””

Para quien no entienda las diferencias entre los diferentes sistemas que se baje la siguiente presentación:

www.gonzalonazareno.org/cloud/material/IntroVirtualizacion.pdf

“””

¿QUE ES LXC?

ES UN MÉTODO DE VIRTUALIZACIÓN A NIVEL DE SISTEMA OPERATIVO PARA HACER FUNCIONAR VARIOS SISTEMAS LINUX (CONTENEDORES), BAJO EL CONTROL DE UN ÚNICO HOST.

Eso quiere decir:

- -Comparte kernel con el Host.
- -El s.o virtualiza el hardware.
- -No existe hipervisor.

¿ QUE DIFERENCIA HABÍA ENTRE LOS DIFERENTES SISTEMAS DE VIRTUALIZACIÓN?

Virtualización de plataforma
Virtualización de recursos

Virtualización de plataforma

- emulación o simulación
- virtualización nativa o completa
- virtualización asistida por hardware
- paravirtualización
- virtualización a nivel de sistema operativo
- otros

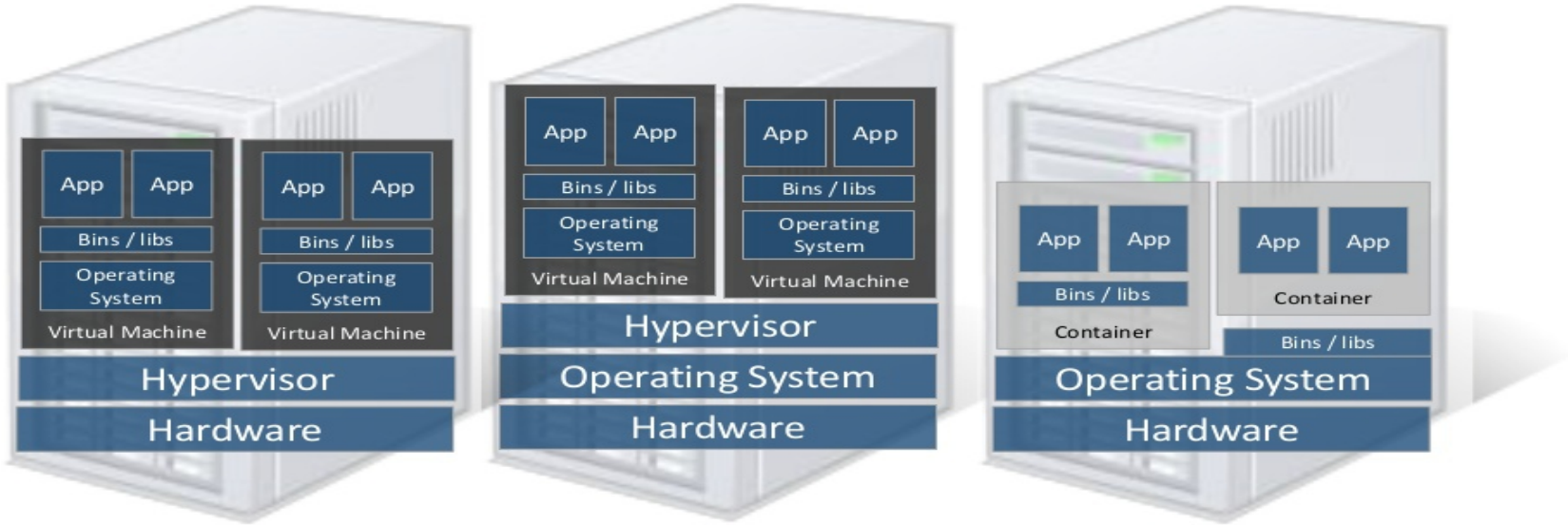
UNA IMAGEN SUELE VALER MÁS QUE MIL PALABRAS

Hypervisors vs. Linux Containers

IBM

Containers share the OS kernel of the host and thus are lightweight. However, each container must have the same OS kernel.

Containers are isolated, but share OS and, where appropriate, libs / bins.



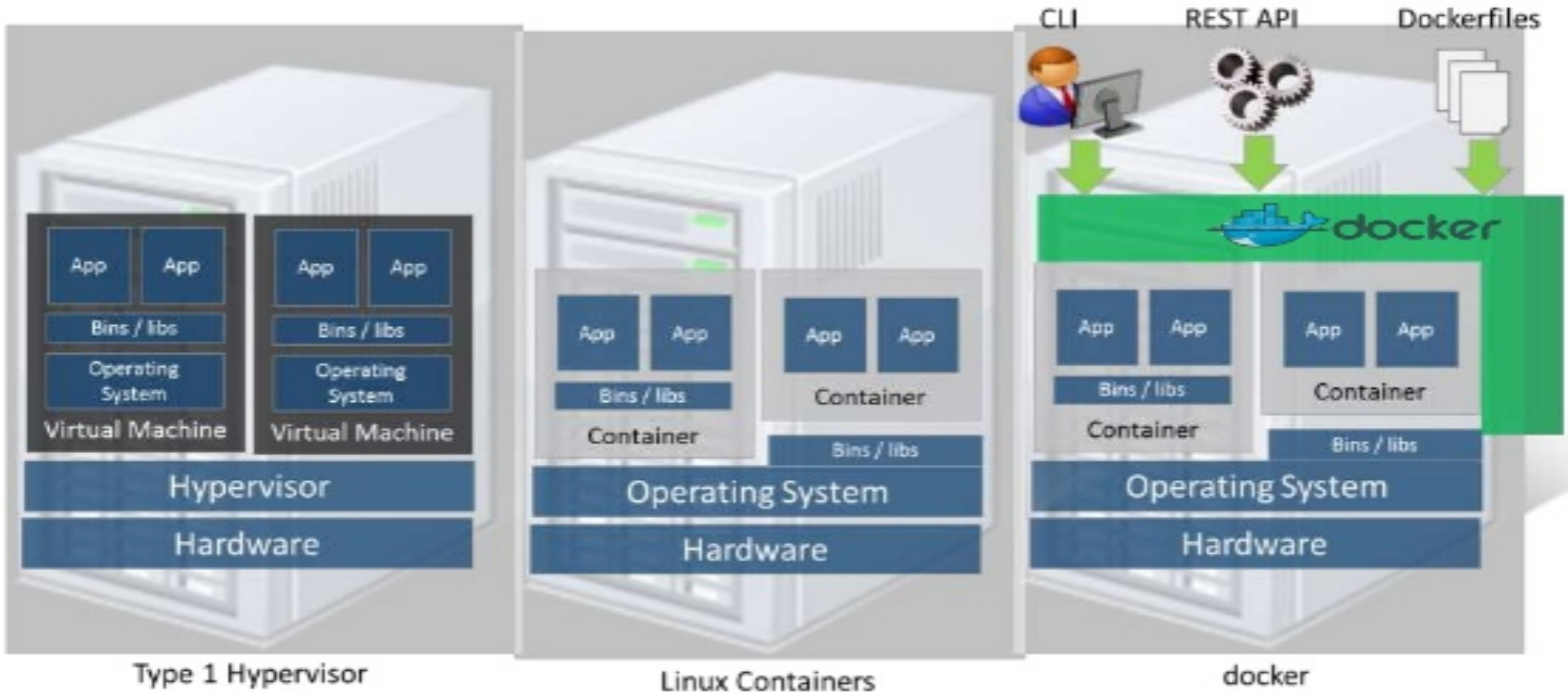
Type 1 Hypervisor | Type 2 Hypervisor | Linux Containers

Imágen sacada de www.slideshare.net/BodenRussell/kvm-and-docker-lxc-benchmarking-with-openstack

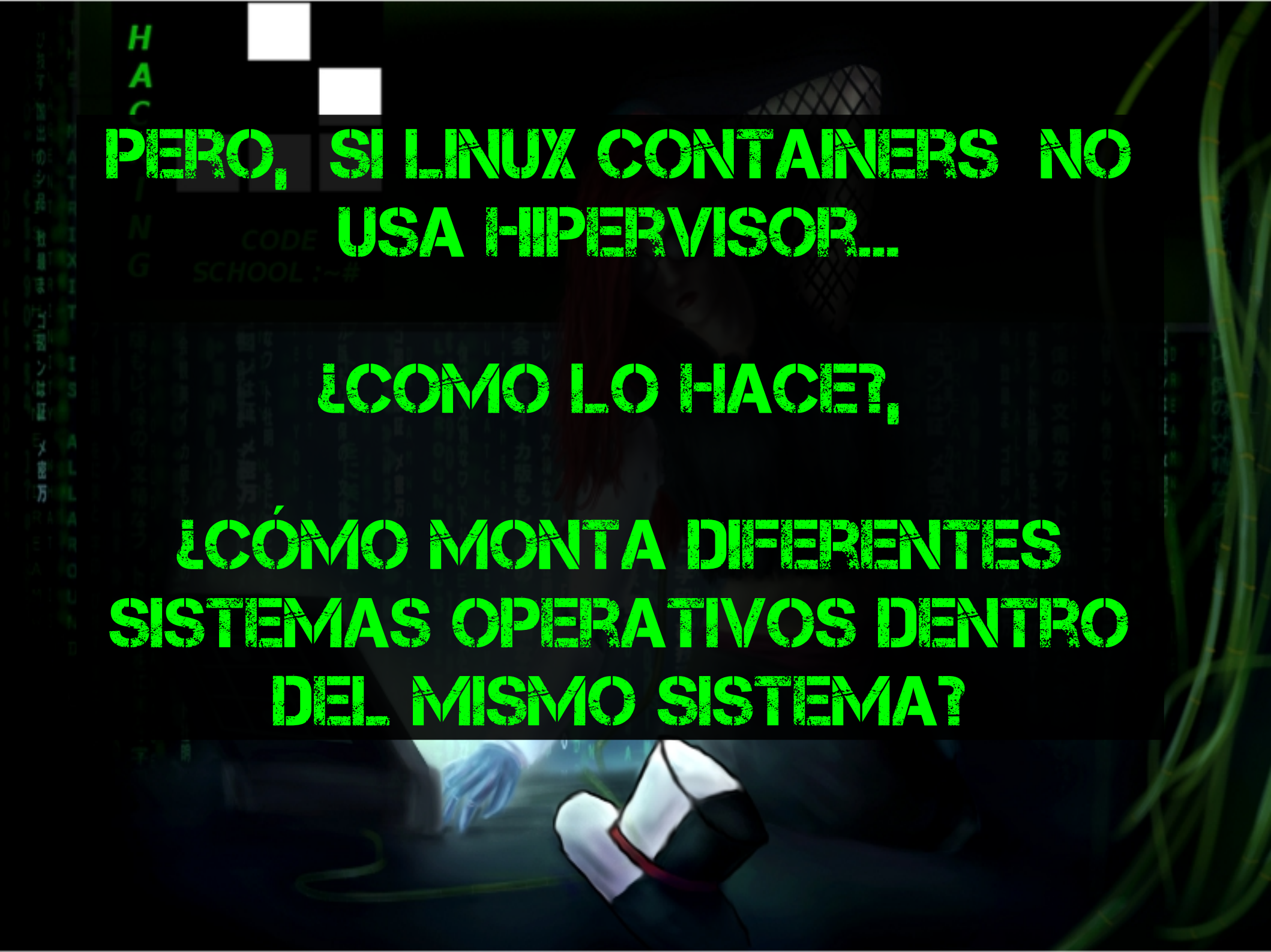
LXC I DOCKER

Hypervisor VM vs. LXC vs. Docker LXC

IBM



Imagén sacada de www.slideshare.net/BodenRussell/kvm-and-docker-lxc-benchmarking-with-openstack


PERO, SI LINUX CONTAINERS NO USA HIPERVISOR...
¿COMO LO HACE?,
¿CÓMO MONTA DIFERENTES SISTEMAS OPERATIVOS DENTRO DEL MISMO SISTEMA?

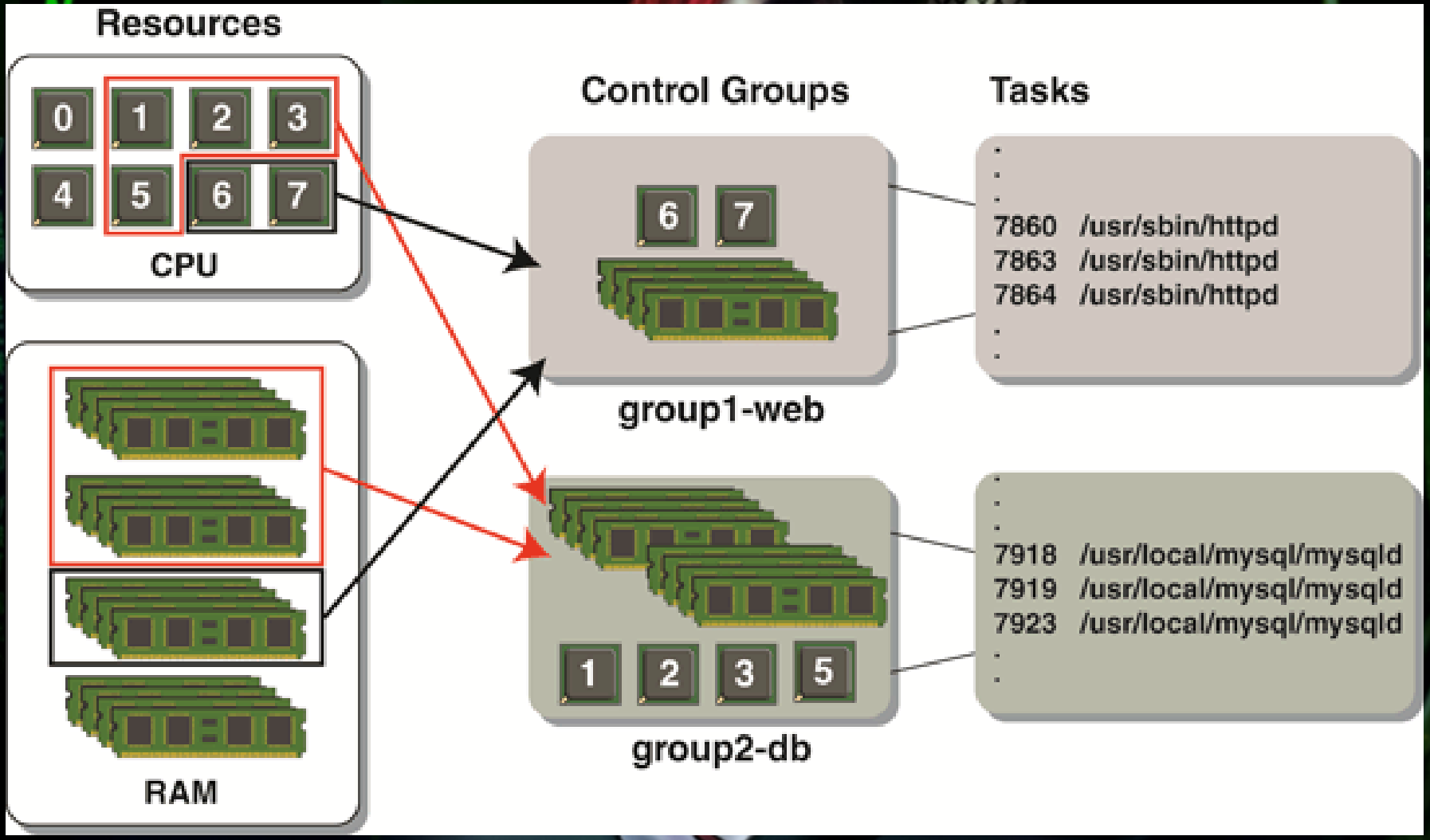
- Usa los espacios de nombres del kernel (ipc, uts, mount, pid, network, user)
- Tiene perfiles de Apparmor y Selinux
- Permite chroots
- Usa las capacidades del kernel
- Usa CGroups

Y QUÉ SIGNIFICA TODO ESO?

-Mira Jason, vayamos por partes...

Ok Freddy ¿Quien empieza?

LQUE SON LOS CGROUPS?



NAMESPACES O ESPACIOS DE NOMBRES ¿QUE SON ?

ANTES / SYSVINIT

```
init─┬─acpid
     ├─atd
     ├─avahi-daemon───avahi-daemon
     ├─clock-applet───2*[{clock-applet}]
     ├─console-kit-dae───64*[{console-kit-dae}]
     ├─cron
     ├─crtmpserver
     ├─cupsd
     ├─2*[dbus-daemon]
     ├─dbus-launch
     ├─dconf-service───2*[{dconf-service}]
     ├─dhclient
     ├─dovecot─┬─anvil
     │         └─log
     ├─flumotion-manag
     ├─flumotion-worke───{flumotion-worke}
     ├─gconfd-2
     ├─6*[getty]
     ├─gnome-keyring-d───5*[{gnome-keyring-d}]
     ├─gvfs-afc-volume───{gvfs-afc-volume}
     ├─gvfs-gdu-volume
     ├─gvfs-gphoto2-vo
     ├─gvfsd
     ├─gvfsd-computer
     ├─gvfsd-metadata
     ├─gvfsd-trash
     ├─hostd-worker───10*[{hostd-worker}]
     ├─irqbalance
     ├─lightdm─┬─Xorg
     │         ├─lightdm─┬─mate-session─┬─caja───2*[{caja}]
     │         │         │              ├─docky───4*[{docky}]
```

NAMESPACES

```
root@4nnc5edwithlov3:~# lxc-start -d -n miprima
root@4nnc5edwithlov3:~# pstree
init─┬─acpid
     ├─atd
     ├─cgmanager
     ├─cron
     ├─dbus-daemon
     ├─dnsmasq
     ├─6*[getty]
     ├─irqbalance
     ├─lxc-monitord
     ├─lxc-start───systemd
     ├─mdadm
     ├─named───10*[{named}]
     ├─rsyslogd───3*[{rsyslogd}]
     ├─sshd───sshd───bash───pstree
     ├─systemd-logind
     ├─systemd-udevd
     ├─upstart-file-br
     ├─upstart-socket-
     └─upstart-udev-br
root@4nnc5edwithlov3:~# uname -a
Linux 4nnc5edwithlov3 3.13.0-63-generic #103-Ubuntu SMP Fri Aug 14 21:42:59 UT
C 2015 x86_64 x86_64 x86_64 GNU/Linux
```

www.toptal.com/linux/separation-anxiety-isolating-your-system-with-linux-namespaces

CAPITULO 3
THE PREVIUS HARDEN

CUANDO NOS PLANTEAMOS EL HARDENING DE UNA MÁQUINA, ¿QUÉ ASEGURAMOS?

Mecanismos de:

Prevención:

- -Firewall
- -Ids/Ips
- -Logrotate(rotación de logs)

Detección:

- -Ids/Ips
- - Monitorización (nagios …)

Recuperación:

- -Backups

- Kernel
- Procesos
- Servicios
- Usuarios
- Red

EL KERNEL

El kernel de Linux como sabemos es modular, esto le aporta la flexibilidad que tiene.

Modular =->Compuesto de módulos

¿Los necesitamos todos?

+ Componentes = + posibles vectores de error/ataque/para monitorizar

Hay parches...

Parcheamos o no parcheamos?| if True: ¿Qué parcheamos?

HARDENIZANDO EL KERNEL

1 preparamos el sistema:

```
root@4nnc5edwithlov3:~/kernels# aptitude install libncurses5-dev make  module-assistant

root@4nnc5edwithlov3:~/kernels# m-a prepare

root@4nnc5edwithlov3:~/kernels# wget www.kernel.org/pub/linux/kernel/v3.x/

root@4nnc5edwithlov3:~/kernels# tar -Jxvf

linux-3.14.53.tar.xz
```

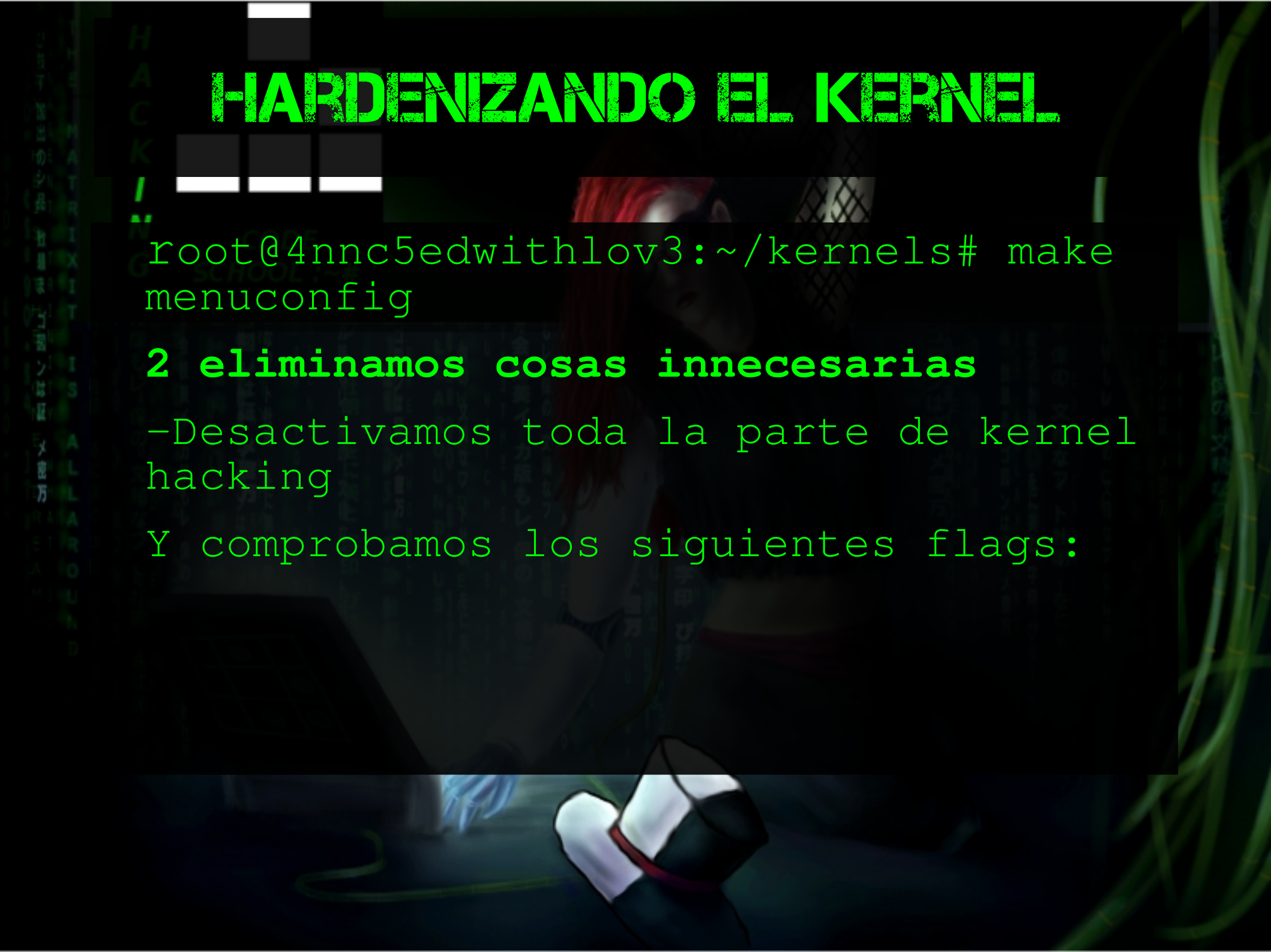
HARDENIZANDO EL KERNEL

root@4nnc5edwithlov3:~/kernels# make menuconfig

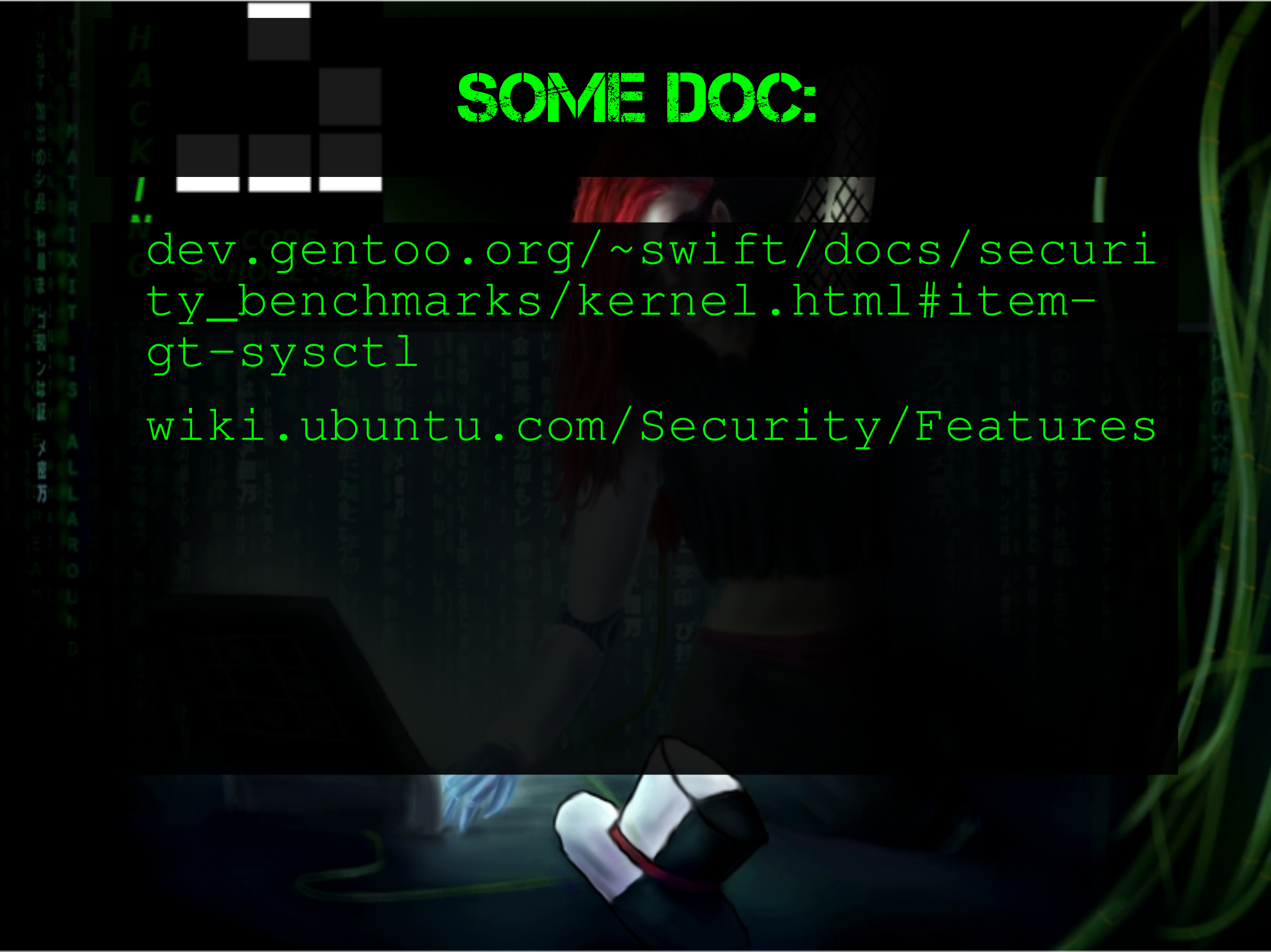
2 eliminamos cosas innecesarias

-Desactivamos toda la parte de kernel hacking

Y comprobamos los siguientes flags:




HACKING
CONFIG_ARCH_RANDOM
CONFIG_AUDIT
CONFIG_SYN_COOKIES
CONFIG_CC_STACKPROTECTOR
CONFIG_DEBUG_RODATA
CONFIG_STRICT_DEVMEM
CONFIG_SECURITY_DMESG_RESTRICT



SOME DOC:

dev.gentoo.org/~swift/docs/security_benchmarks/kernel.html#item-gt-sysctl

wiki.ubuntu.com/Security/Features

GRSEC O NO GRSEC?

Lxc con grsec es bastante potente pero a veces grsec puede generar fallos debido justamente a sus restricciones

SOME OTHER STUFF

aptitude install rcconf

Permitir su - solo a los usuarios que pertenezcan al grupo wheel:

```
# addgroup --system wheel
# usermod -G wheel mirootuser
# vim /etc/pam.d/su
auth required pam_wheel.so
```

Esconder procesos:

Vim /etc/fstab

```
proc            /proc   proc    defaults,
hidepid=2               0       0
```

nano /etc/sysctl.conf

SOME OTHER STUFF

fail2ban

denyhost

logcheck

apparmor

lynis

mod_evasive

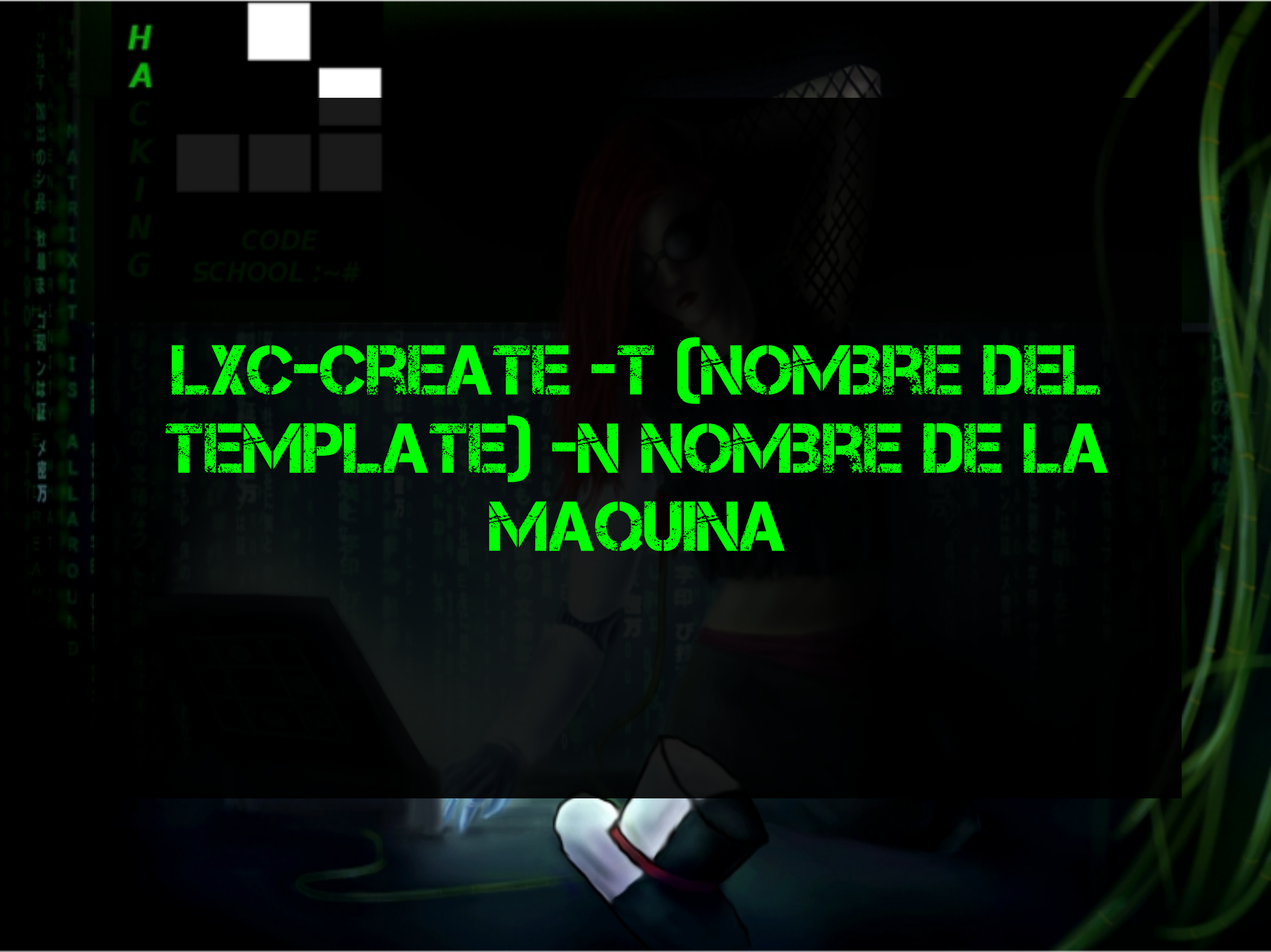
apt-watch

diffmon

CAPITULO 4
CONOCIENDO LXC...

LXC CHEATSET

```
root@4nnc5edwithlov3:~# lxc-
lxc-attach          lxc-destroy         lxc-start
lxc-autostart       lxc-device          lxc-start-ephemeral
lxc-cgroup          lxc-execute         lxc-stop
lxc-checkconfig     lxc-freeze          lxc-unfreeze
lxc-clone           lxc-info            lxc-unshare
lxc-config          lxc-ls              lxc-usernsexec
lxc-console         lxc-monitor         lxc-wait
lxc-create          lxc-snapshot
```


LXC-CREATE -T (NOMBRE DEL TEMPLATE) -N NOMBRE DE LA MAQUINA

TEMPLATES

```
/usr/share/lxc/templates
/usr/share/lxc/templates/lxc-alpine
/usr/share/lxc/templates/lxc-altlinux
/usr/share/lxc/templates/lxc-archlinux
/usr/share/lxc/templates/lxc-busybox
/usr/share/lxc/templates/lxc-centos
/usr/share/lxc/templates/lxc-cirros
/usr/share/lxc/templates/lxc-debian
/usr/share/lxc/templates/lxc-download
/usr/share/lxc/templates/lxc-fedora
/usr/share/lxc/templates/lxc-gentoo
/usr/share/lxc/templates/lxc-openmandriva
/usr/share/lxc/templates/lxc-opensuse
/usr/share/lxc/templates/lxc-oracle
/usr/share/lxc/templates/lxc-plamo
/usr/share/lxc/templates/lxc-sshd
/usr/share/lxc/templates/lxc-ubuntu
/usr/share/lxc/templates/lxc-ubuntu-cloud
```

¿DONDE SE GUARDAN LAS COSAS?

¿QUE TIPO DE CONTENEDORES PUEDO CREAR?

Privilegiados

No privilegiados

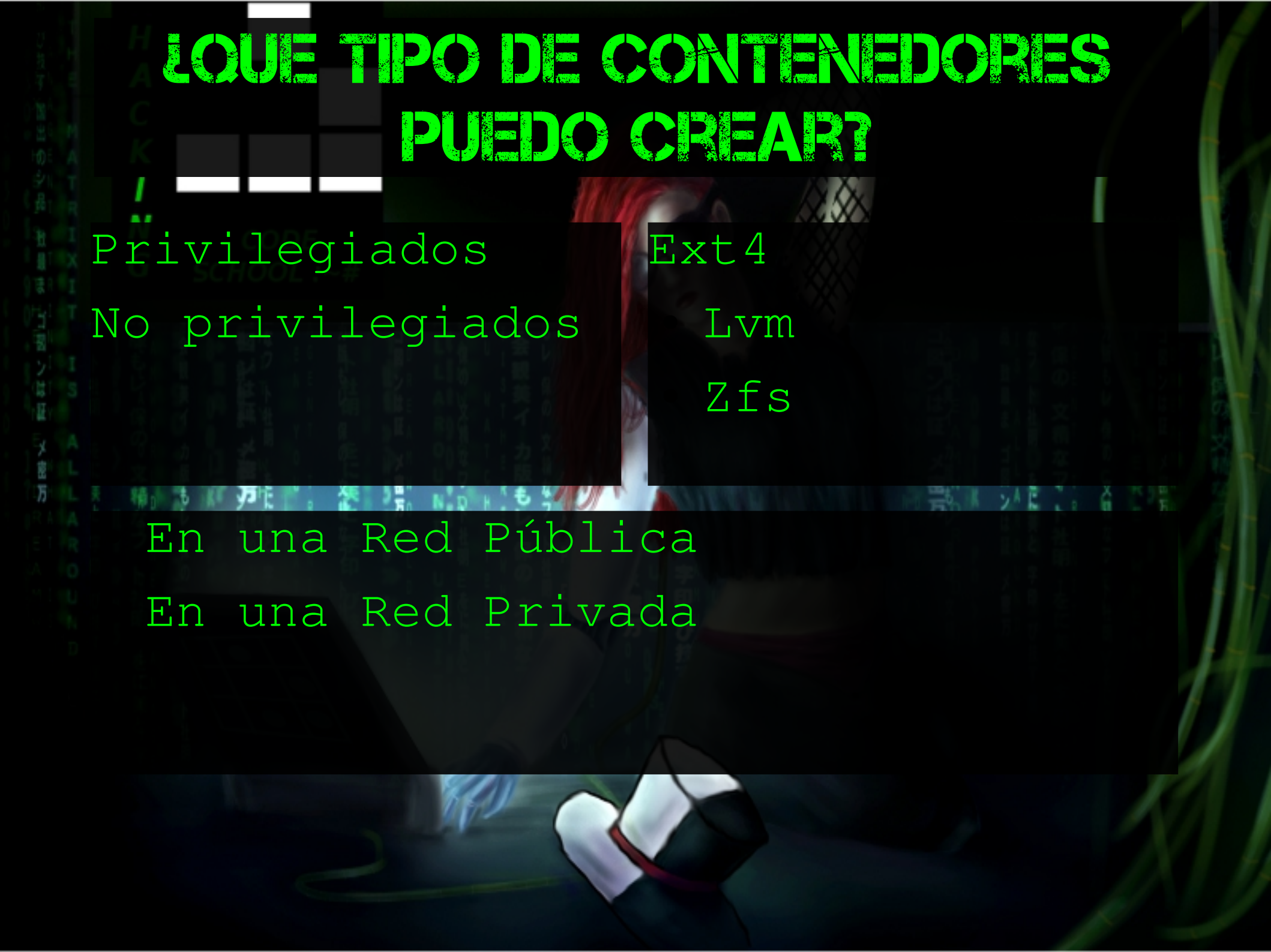
Ext4

Lvm

Zfs

En una Red Pública

En una Red Privada




HACKING
CODE
SCHOOL :~#
CAP5
THE NET

1 BRIDGE / IPS PÚBLICAS

```
auto eth0
iface eth0 inet manual

auto br0
    iface br0 inet static
    bridge_ports eth0
    bridge_fd 0
    address 37.59.43.62
    broadcast 37.59.43.255
    netmask 255.255.255.0
    network 37.59.43.0
    gateway 37.59.43.254

#LXC CONTAINERS
    up route add -host 5.135.67.44 dev br0
    up route add -host 5.135.67.45 dev br0 #Ips Compradas

# default route to access subnet
up route add -net 5.135.67.44 netmask 255.255.255.252 gw 37.59.43.62 br0
up route add -net 5.135.67.45 netmask 255.255.255.252 gw 37.59.43.62 br0
```


THE BRIDGE
/etc/lxc/default.conf
lxc.network.type = veth
lxc.network.link = br0
lxc.network.flags = up
lxc.network.hwaddr =
02:00:00:xx:xx:xx

THE CONTAINER CONF

/etc/default/lxc-net

```
USE_LXC_BRIDGE="false"
```

THE CONTAINER CONF

```
# Container specific configuration
lxc.rootfs = /var/lib/lxc/p1/rootfs
lxc.utsname = p1
lxc.autodev=1
lxc.kmsg=0

# Network configuration
lxc.network.type = veth
lxc.network.flags = up
lxc.network.link = br0
lxc.network.veth.pair = crackme
lxc.network.ipv4 = 5.135.67.46/30
lxc.network.ipv4.gateway = 37.59.43.62

#Autostart
lxc.start.auto=1
```

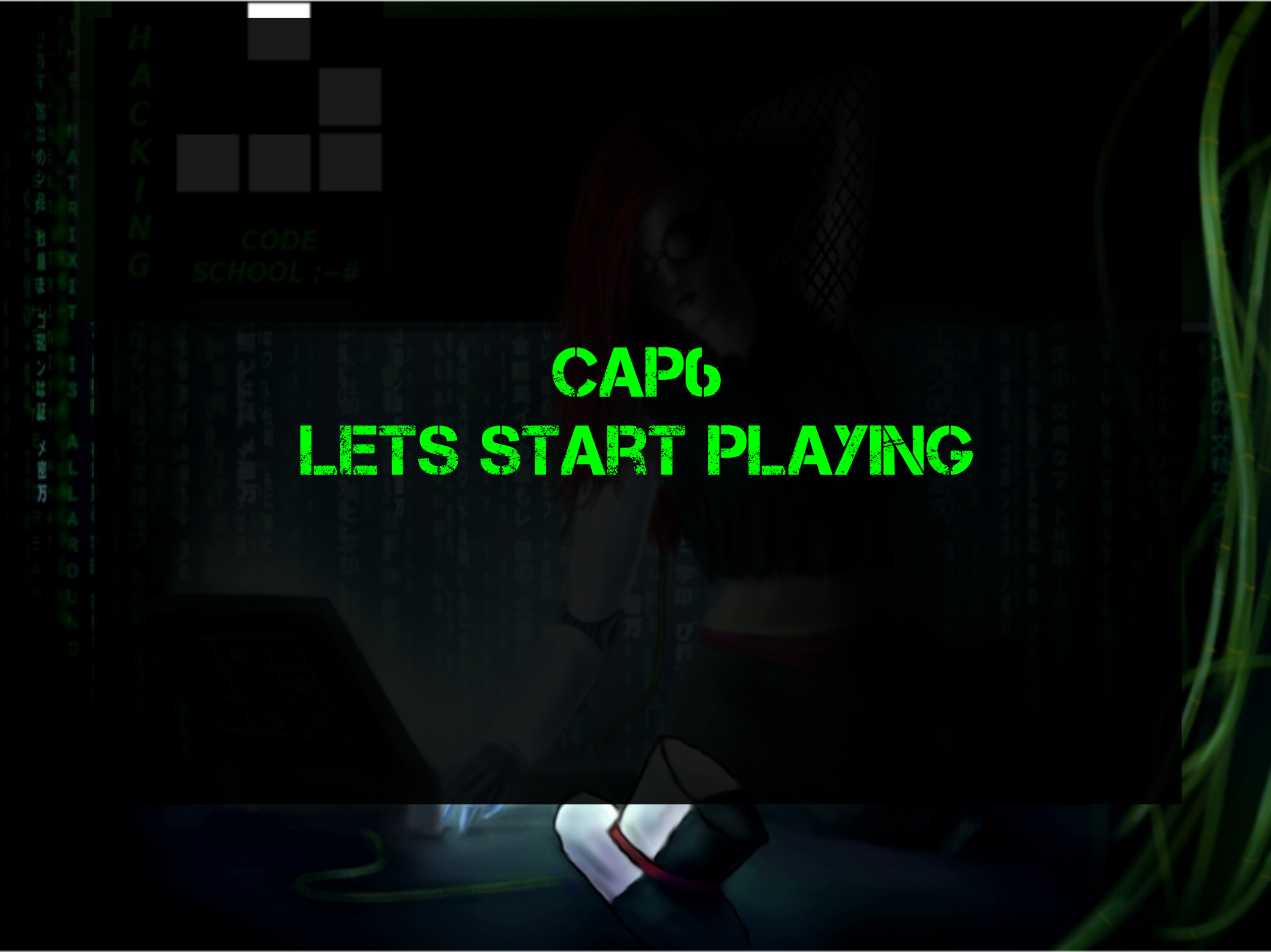
/ETC/NETWORK/INTERFACES

```
# The loopback network interface
auto lo
iface lo inet loopback

iface eth0 inet static
        address 5.135.67.45
        netmask 255.255.255.252
        #pointopoint 37.59.43.62
        broadcast 5.135.67.47
        gateway 37.59.43.62
        dns-nameservers 213.186.33.99

up route add default gw 37.59.43.62
```


HACKING
CODE
SCHOOL :~#
Interneeeeeeeeeeeet!!!!!!!


HACKING
CODE
SCHOOL :~#
THE MATRIX IS ALL AROUND
CAP6
LETS START PLAYING

1 NO PRIVILEGIADO

1 Creamos el usuario

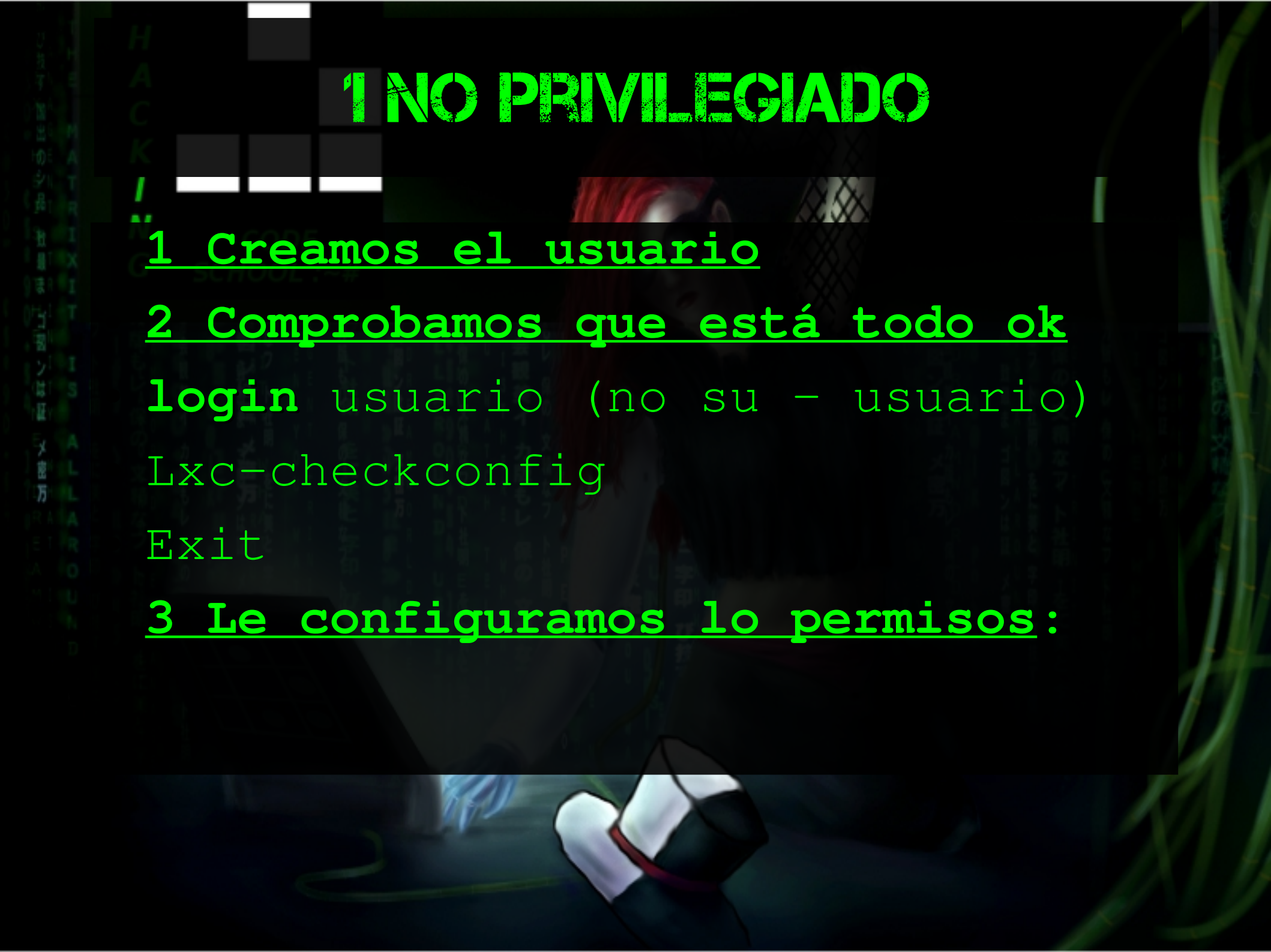
2 Comprobamos que está todo ok

login usuario (no su - usuario)

Lxc-checkconfig

Exit

3 Le configuramos lo permisos:



LXC NO PRIVILEGIADOS/VISUDO

```
# User alias specification
User_Alias MYADMINS =  baulete
# Cmnd alias specification
Cmnd_Alias INSTALL = /usr/bin/aptitude, /usr/bin/dpkg
Cmnd_Alias USERMOD = /usr/sbin/usermod
Cmnd_Alias CHMOD = /bin/chmod
Cmnd_Alias EDITORS = /usr/bin/nano, /usr/bin/vi, /usr/bin/touch
Cmnd_Alias LXC = /usr/local/bin/lxc-info, /usr/local/bin/lxc-ls,
Cmnd_Alias ARCHIVOS = /bin/cp , /bin/mv, /bin/mkdir, /bin/ls
Cmnd_Alias USERS = /usr/sbin/adduser,  /usr/sbin/deluser
# User privilege specification
root    ALL=(ALL:ALL) ALL
MYADMINS   ALL= INSTALL , USERMOD, CHMOD, EDITORS, LXC, ARCHIVOS, USERS
```

MAPEANDO EL USUARIO

4. Buscamos cuales son su subgid

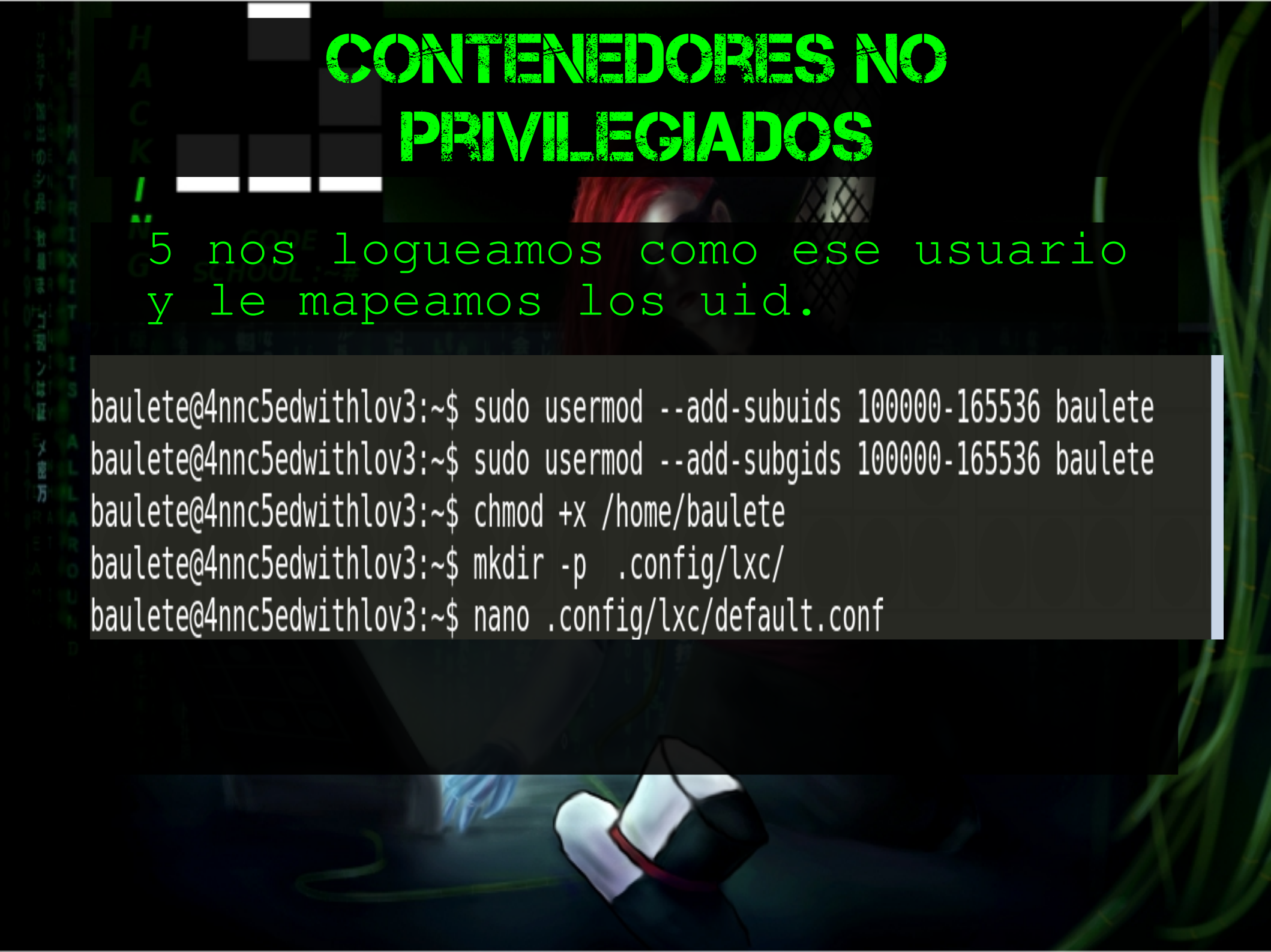
Y su subuid para mapearlos.

```
root@4nnc5edwithlov3:~# grep baulete /etc/sub* 2>/dev/null
/etc/subgid:baulete:100000:65536
/etc/subuid:baulete:100000:65536
```

CONTENEDORES NO PRIVILEGIADOS

5 nos logueamos como ese usuario y le mapeamos los uid.

```
baulete@4nnc5edwithlov3:~$ sudo usermod --add-subuids 100000-165536 baulete
baulete@4nnc5edwithlov3:~$ sudo usermod --add-subgids 100000-165536 baulete
baulete@4nnc5edwithlov3:~$ chmod +x /home/baulete
baulete@4nnc5edwithlov3:~$ mkdir -p  .config/lxc/
baulete@4nnc5edwithlov3:~$ nano .config/lxc/default.conf
```



MAPEANDO LA RED

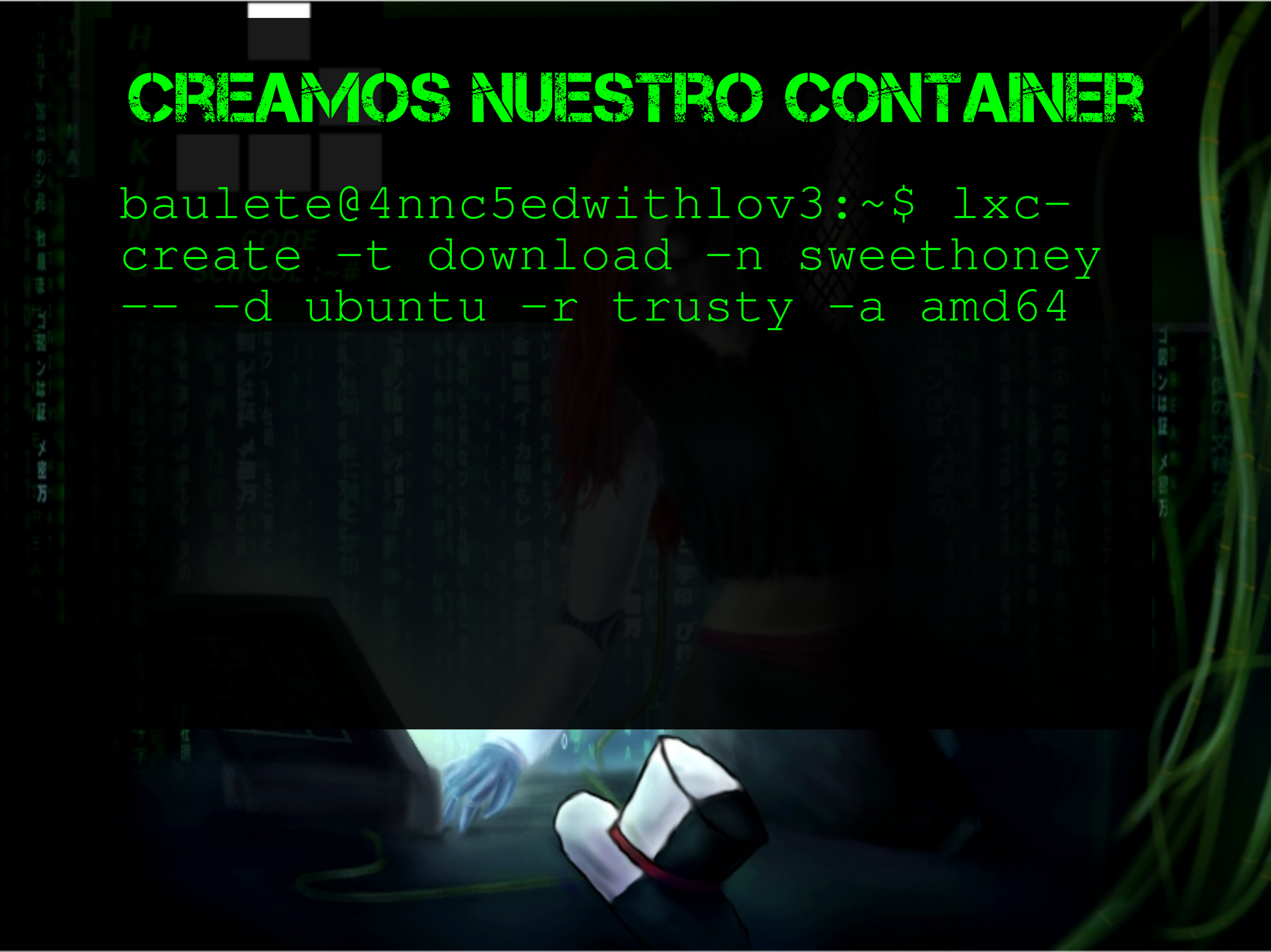
```
lxc.network.type = veth
lxc.network.link = lxcbr0
lxc.network.flags = up
lxc.network.hwaddr = 02:00:00:xx:xx:xx
lxc.id_map = u 0 100000 65536
lxc.id_map = g 0 100000 65536
```

PERMITIMOS CREAR N BRIDGES

```
sudo nano /etc/lxc/lxc-usernet
baulete veth br0 10
```

CREAMOS NUESTRO CONTAINER

```
baulete@4nnc5edwithlov3:~$ lxc-
create -t download -n sweethoney
-- -d ubuntu -r trusty -a amd64
```



CREÁNDOLO CON LVM

```
lxc-create -t download -n
primerlvm -B lvm --lvname
primercontainer --vgname vg-lxc
--fssize 30G --fstype ext4
--dir /home/contenedores
```

PARA QUE INVESTIGES

Backup de contenedores

seccop + lxc

selinux profiles

apparmor profiles

your imagination..... + lxc


HACKING
CODE
SCHOOL :~#
FIN