

PDIH-Seminario LKM

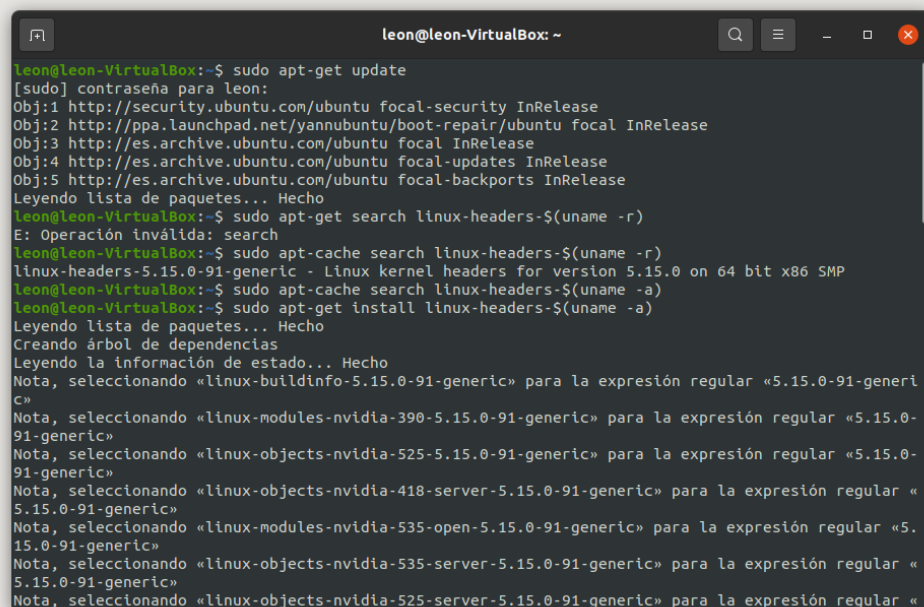
León Corbacho Rodríguez 4º 28/04/2024

- 1. Desarrollará un módulo sencillo en lenguaje C y lo cargará en el kernel usando las herramientas estudiadas. Comprobará su correcto funcionamiento inspeccionando los logs del sistema y finalmente descargará el módulo:**

Siguiendo la guía para la realización de la práctica antes de ejecutar nada, hay que preparar el sistema que en mi caso es un Ubuntu.16 en una máquina virtual. Antes de incluso inicializar el sistema he creado una instantánea del sistema operativo por si acaso algo falla como nos recomienda el profesor.

Tras todo esto vamos a preparar la máquina primero accediendo a la terminal y ejecutando los siguientes comandos:

- `-sudo apt-get update` (Para actualizar el sistema operativo)
- `-sudo apt-cache search linux-headers $(uname -r)` (Nos indica la versión de las cabeceras del Linux del sistema operativo de la máquina virtual)
- `-sudo apt-get install linux-headers$(uname -r)`



```
leon@leon-VirtualBox: ~  
leon@leon-VirtualBox:~$ sudo apt-get update  
[sudo] contraseña para leon:  
Obj:1 http://security.ubuntu.com/ubuntu focal-security InRelease  
Obj:2 http://ppa.launchpad.net/yannubuntu/boot-repair/ubuntu focal InRelease  
Obj:3 http://es.archive.ubuntu.com/ubuntu focal InRelease  
Obj:4 http://es.archive.ubuntu.com/ubuntu focal-updates InRelease  
Obj:5 http://es.archive.ubuntu.com/ubuntu focal-backports InRelease  
Leyendo lista de paquetes... Hecho  
leon@leon-VirtualBox:~$ sudo apt-cache search linux-headers-$(uname -r)  
E: Operación inválida: search  
leon@leon-VirtualBox:~$ sudo apt-cache search linux-headers-$(uname -r)  
linux-headers-5.15.0-91-generic - Linux kernel headers for version 5.15.0 on 64 bit x86 SMP  
leon@leon-VirtualBox:~$ sudo apt-cache search linux-headers-$(uname -a)  
leon@leon-VirtualBox:~$ sudo apt-get install linux-headers-$(uname -a)  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Nota, seleccionando «linux-buildinfo-5.15.0-91-generic» para la expresión regular «5.15.0-91-generi  
c»  
Nota, seleccionando «linux-modules-nvidia-390-5.15.0-91-generic» para la expresión regular «5.15.0-  
91-generic»  
Nota, seleccionando «linux-objects-nvidia-525-5.15.0-91-generic» para la expresión regular «5.15.0-  
91-generic»  
Nota, seleccionando «linux-objects-nvidia-418-server-5.15.0-91-generic» para la expresión regular «  
5.15.0-91-generic»  
Nota, seleccionando «linux-modules-nvidia-535-open-5.15.0-91-generic» para la expresión regular «5.  
15.0-91-generic»  
Nota, seleccionando «linux-objects-nvidia-535-server-5.15.0-91-generic» para la expresión regular «  
5.15.0-91-generic»  
Nota, seleccionando «linux-objects-nvidia-525-server-5.15.0-91-generic» para la expresión regular «
```

Ya preparado el Sistema, vamos a realizar la verdadera actividad de este seminario. La realización de este se basa, siguiendo la guía del seminario, en cargar un módulo del Kernel nuevo en el sistema. Gracias a un código proporcionado por el profesor usaremos este módulo, que

básicamente crea un mensaje en los registros logs del Kernel. Tras descargarlo en nuestra máquina vemos que está constituido por un makefile que al ejecutarlo realiza las instrucciones dentro de este y nos compila el código del módulo.

```
leon@leon-VirtualBox: ~/modulo
leon@leon-VirtualBox:~$ cd modulo/
leon@leon-VirtualBox:~/modulo$ ls
hello.c  Makefile
leon@leon-VirtualBox:~/modulo$ make Makefile
make: No se hace nada para 'Makefile'.
leon@leon-VirtualBox:~/modulo$ make
make -C /lib/modules/5.15.0-91-generic/build/ M=/home/leon/modulo modules
make[1]: se entra en el directorio '/usr/src/linux-headers-5.15.0-91-generic'
  CC [M] /home/leon/modulo/hello.o
  MODPOST /home/leon/modulo/Module.symvers
  CC [M] /home/leon/modulo/hello.mod.o
  LD [M] /home/leon/modulo/hello.ko
  BTF [M] /home/leon/modulo/hello.ko
Skipping BTF generation for /home/leon/modulo/hello.ko due to unavailability of vmlinux
make[1]: se sale del directorio '/usr/src/linux-headers-5.15.0-91-generic'
leon@leon-VirtualBox:~/modulo$ ls -l
total 452
-rw-r--r-- 1 leon leon 2424 may 11 2020 hello.c
-rw-rw-r-- 1 leon leon 217696 abr 29 10:21 hello.ko
-rw-rw-r-- 1 leon leon 27 abr 29 10:21 hello.mod
-rw-rw-r-- 1 leon leon 892 abr 29 10:21 hello.mod.c
-rw-rw-r-- 1 leon leon 108968 abr 29 10:21 hello.mod.o
-rw-rw-r-- 1 leon leon 110264 abr 29 10:21 hello.o
-rw-r--r-- 1 leon leon 154 may 11 2020 Makefile
-rw-rw-r-- 1 leon leon 27 abr 29 10:21 modules.order
-rw-rw-r-- 1 leon leon 0 abr 29 10:21 Module.symvers
leon@leon-VirtualBox:~/modulo$
```

Para comprobar que está instalado el módulo, podemos ver la lista de los módulos del kernel en el sistema, algunos cargados per no ejecutados y otros que si lo están. En el caso de nuestro modulo esta cargado pero no iniciado. Para iniciarlo usamos el código:

- `-sudo ismod hello.ko`

Y el comando para mirar los modulos es:

- `-lsmod`

```
leon@leon-VirtualBox: ~/modulo
leon@leon-VirtualBox:~/modulo$ sudo ismod hello.ko
sudo: ismod: orden no encontrada
leon@leon-VirtualBox:~/modulo$ sudo insmod hello.ko
leon@leon-VirtualBox:~/modulo$ lsmod
Module                  Size  Used by
hello                   16384  0
udf                     135168  1
crc_itu_t               16384  1 udf
bnep                    28672  2
nls_iso8859_1           16384  1
snd_intel8x0             49152  2
snd_ac97_codec          155648  1 snd_intel8x0
intel_rapl_msr           20480  0
ac97_bus                16384  1 snd_ac97_codec
binfmt_misc             24576  1
snd_pcm                 135168  2 snd_intel8x0,snd_ac97_codec
snd_seq_midi            20480  0
snd_seq_midi_event      16384  1 snd_seq_midi
btusb                   61440  0
btrtl                   24576  1 btusb
joydev                  32768  0
snd_rawmidi             49152  1 snd_seq_midi
vmwgfx                  364544  2
intel_rapl_common       40960  1 intel_rapl_msr
btbcm                   24576  1 btusb
crt10dif_pclmul         16384  1
btintel                 40960  1 btusb
ghash_clmulni_intel     16384  0
snd_seq                 77824  2 snd_seq_midi,snd_seq_midi_event
bluetooth               688128  12 btrtl,btintel,btbcn,bnep,btusb
```

Como dice el guión no queremos dejar un modulo no nativo del sistema, en el sistema. El siguiente paso es eliminarlo. Esto se hace con el la instrucción:

- -Sudo rmmmod hello.ko

[illegible]

Por ultimo para saber que el modulo ha funcionado mientras estaba iniciado, podemos ver si ha escrito “Hello world” en los mensajes de los logs del kernel. Estos mensajes están en la carpeta var/logs, Pero para acceder a esta carpeta debemos ser superusuario. Así que siguiendo la sucesión de estas instrucciones podemos observar que si ha funcionado y ahí está el mensaje.

- Sudo su
- Cd /var/logs
- Tail -f kern.log (comando para mirar los últimas filas escritas en el documento.)

```

root@leon-VirtualBox: /var/log

leon@leon-VirtualBox:~$ sudo su -
root@leon-VirtualBox:~# cd /var/log
-bash: cd: /var/log: No existe el archivo o el directorio
root@leon-VirtualBox:~# cd /var/log
root@leon-VirtualBox:~# var/log tail -f kern.log
Apr 29 09:58:06 leon-VirtualBox kernel: [ 413.934448] loop39: detected capacity change from 0 to 1721616
Apr 29 09:58:13 leon-VirtualBox kernel: [ 421.648745] audit: type=1400 audit(1714377493.999:96): apparmor="STATUS" operation="profile_replace" info=same as current profile,
skipping profile="unconfined" name="snap.rubymine.rubymine" pid=3868 comm="apparmor_parser"
Apr 29 09:58:13 leon-VirtualBox kernel: [ 421.659457] audit: type=1400 audit(1714377493.921:97): apparmor="STATUS" operation="profile_replace" info=same as current profile,
skipping profile="unconfined" name="snap.rubymine.rubymine" pid=3862 comm="apparmor_parser"
Apr 29 09:58:25 leon-VirtualBox kernel: [ 432.997823] loop31: detected capacity change from 0 to 2589312
Apr 29 09:58:26 leon-VirtualBox kernel: [ 433.880428] audit: type=1400 audit(1714377586.064:98): apparmor="STATUS" operation="profile_replace" info=same as current profile,
skipping profile="unconfined" name="snap.clion.clion" pid=4024 comm="apparmor_parser"
Apr 29 09:58:26 leon-VirtualBox kernel: [ 433.889588] audit: type=1400 audit(1714377586.808:99): apparmor="STATUS" operation="profile_replace" info=same as current profile,
skipping profile="unconfined" name="snap.update-ms.clion" pid=4026 comm="apparmor_parser"
Apr 29 10:26:41 leon-VirtualBox kernel: [ 2129.419397] hello: Loading out-of-tree module taints kernel.
Apr 29 10:26:41 leon-VirtualBox kernel: [ 2129.419258] hello: module verification failed: signature and/or required key missing - tainting kernel
Apr 29 10:26:41 leon-VirtualBox kernel: [ 2129.419836] EBB: Hello world from the 888 LKM!
Apr 29 10:28:39 leon-VirtualBox kernel: [ 2247.639637] EBB: Goodbye world from the 888 LKM!

```