Trabajo Práctico Final Laboratorio de Redes y Sistemas Operativos

Profresor: José Luis Di Biase

Alumno: Sánchez, José María

Descripción del proyecto:

En el presente trabajo se pretende obtener acceso de administrador para un celular Motorola moto g3 Osprey (2015) y como prueba de que el acceso está funcionando se instalará una aplicación desde el Play Store que solamente puede correrse con permisos de este tipo. Se detallarán los distintos pasos efectuados y se explicarán las terminologías asociadas indispensables para concretar dicho acceso de manera eficiente. Asimismo, se hará un relevo de la máquina con la cual realicé el trabajo y el proceso de instalación de las distintas herramientas utilizadas.

Nota: en determinados casos, pondré entre paréntesis los términos en inglés utilizados para facilitar las búsquedas en los navegadores.

Relevamiento Pc utilizada:

- Modelo: Acer Aspire-E5-571P
- CPU: Intel Core i5 (4th Gen) 4210U 1.7ghz
- RAM: 4gb
- Sistema operativo: Linux Ubuntu 17.10

Relevamiento Celular Utilizado

- Modelo: Moroloa Moto g3 osprey XT1542
- Qualcomm Snapdragon 410 1,4Hz
- RAM: 2gb
- Sitema Operativo: Android 5.1.1

Software utilizado:

- fastboot tools
- adb (Android Device Bridge)

Instalación de fastboot y adb vía shell

1) sudo apt-get udpate // nos trae la última actulización de las bibliotecas oficiales de linux
2) sudo apt install android-tools-adb android-tools-fastboot

Conceptos fundamentales

Particiones en Android

Todo dispositivo Android viene con una lista standard de particiones de memoria como la que se detalla a continuación:

/boot
/system
/recovery
/data
/cache
/misc

Para a lo que concierne al trabajo, sólo nos interesaran las particiones boot y recovery. La primera de ellas, como su nombre lo indica, nos permite bootear nuestro dispositivo móvil. Es decir, posee todo lo necesario para darle el arranque al sistema. Uno de esos componentes es el Android ramdisk que, al igual que el que se enceuntra en Linux, es usado para montar todas las particiones del sistema (llamado en Linux como “normal linux boot procedure”).

La otra partición interesante es el recovery, la cual nos perminte un arranque independiente del sistema, con lo que si nuestro Android no arranca podemos acceder a este modo de recuperación para intentar recuperar nuestro dispositivo.

El uso de la misma para nuesro proyecto radica en que instalaremos un custom recovery, que nos permite opciones más avanzadas

Bootloader

Es un programa desarrolado por el fabricante del dispositivo, el cual permite bootear el sistema operativo. También realiza algunos tests en las particiones para ubicar el kernel y el recovery. Cuando uno apreta el botón de encendido, dicho programa elige el kernel autorizado para arrancar. De otra manera, si pulsás el encendido junto con las teclas de subir y bajar el volumen (estas combinaciones cambian entre dispositivos), el dispositivo entra en el fastboot mode, que nos brinda otras opciones.

Por defecto, el bootloader se encuentra bloqueado, lo que quiere decir que el dispositivo sólo va a bootear con la firma digital autorizada que el fabricante proporciona. El primer paso para tener acceso de administrador va a ser desbloquear el programa recién explicado.

¿Qué significa root o rutear Android?

Obtener acceso de root o rutear el dispositivo, significa, como hemos mencionado anteriormente, obtener acceso como usuario administrador. En Linux, esto se logra cuando a través de la consola encabezamos el comando con “sudo”. En Windows, a diferencia de los dos anteriores, no se hace distinción entre el usuario root y el común.

El acceso como root nos permite tener prácticamente acceso total del dispositivo. Con este tipo de privilegios podemos instalar un sistema operativo distinto al Android que viene por defecto, correr aplicaciones que necesitan este acceso, instalar una custom ROM, etc.

Apenas obtenemos el acceso a root perdemos automáticamente la garantía del celular. Otro problema es que potencialmente uno podría llegar a dañar parte del sistema y dejar inutilizado el dispositivo, por lo que entonces hay que tener sumo cuidado en cada paso.

Prerequisitos

- Tener instalado adb y fastboot tools
- Que el dispositivo cuente con al menos un 80% de batería, dado que si un proceso se corta por falta de energía, puede que ocurran daños en el mismo.

Preparación

Primero que nada, debemos tener el celular permitiendo la depuración por USB (USB debugging). Para esto, debemos ir a configuración - > Acerca del teléfono. Abajo de todo aparece el número de complicación, apretamos entre 8 y 9 veces ahí y debe aparecernos un mensaje “ya eres programador”. Estos pasos cambian entre modelos pero suelen ser similares entre dispositivos.

Ahora entre las configuraciones disponibles nos aparecerá la de Programador. Entramos a ese menú y activamos la opción “Depuración por USB”.

Lo segundo a tener en cuenta, es que debemos hacer un backup de nuestro dispositivo, ya que rutearlo hará un formateo completo del mismo (hard reset).

¡Comenzamos!

1) Besqloquear el bootloader (unlocked bootloader)

a) entrar al fastboot mode del dispositivo con las teclas de apagado, subir y bajar el volumen (este paso casi siempre cambia según el modelo, pero con el dispositivo siempre apagado).

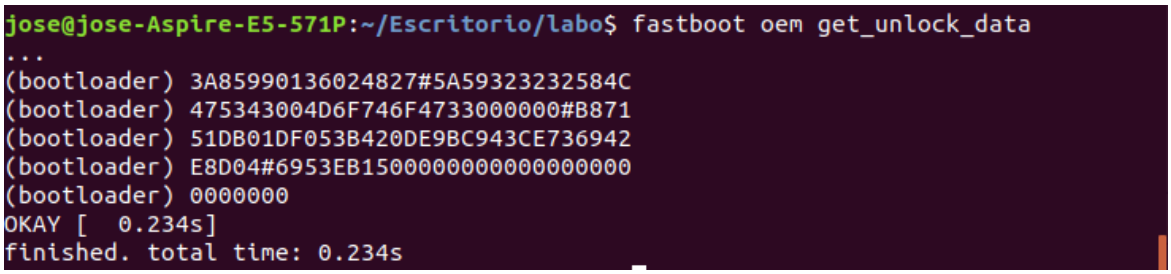
b) conectar el dispositivo con el cable usb a la pc a utilizar
c) abrir una línea de comandos y chequear si el dispositivo está conectado correctamente con el siguiente comando.
fastboot devices

Si el dispositivo está conectado correctamente, debe aparecer en consola un código alfanumérico que es el serial number del dispositivo. Dicho número se puede observar en el fastboot mode.

d) Lo siguiente que se necesita es una información (que va a ser un string) que nos ayudará en el proceso de desbloqueo. En la línea de comandos, pasar lo siguiente:

fastboot oem get_unlock_data

Nos aparecerá en la consola lo siguiente:



Guardamos cada uno de los textos que aparece después de bootloader en un archivo de texto sin espacios en blanco.

e) Accedemos al siguiente link:
https://motorola-global-portal.custhelp.com/app/standalone/bootloader/unlock-your-device-a

En este link, obtendremos el código que nos permitirá desbloquear el bootloader, pero primero debemos crear una cuenta en Motorola.

Ya habiendo generado la cuenta y en el link anterior, en el paso 6 que nos muestra la página, agregamos el código que habíamos anotado antes de la consola y lo pegamos en el espacio que muestra. Damos click “Can my device be unlocked?”. Si nuestro dispositivo es efectivamente “desbloqueable”, nos aparecerá debajo de todo “Request unlock key”. Damos click a ese botón.

Lo siguiente es abrir nuestro email y copiar el código que nos llego como respuesta

f) Volvemos a la consola y tipeamos lo siguiente:

fastboot OEM unlocks <códigoObtenidoEnElMailDeMotorola>

Listo, nuestro bootloader ya sido desbloqueado

2) Instalar un custom recovery

Como dijimos anteriormente, un custom recovery nos permitirá realizar más tareas que una normal. En nuestro caso, será flashear un .zip no firmado.

a) Descargar del siguiente link twrp: forum.xda-developers.com/attachment.php?attachmentid=3655400&d=1456122222
Twrp es una custom recovery que además es software libre

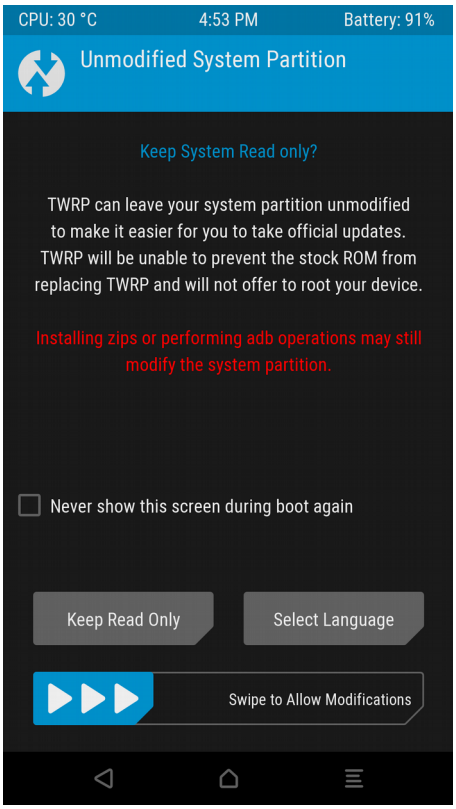
b) Con el celular en fastboot mode y conectado vía usb, correr el siguiente comando en consola:

fastboot flash recovery pathDelArchivo/twrp.img

Debe aparecernos en consola algo similar a lo siguiente:

```
jose@jose-Aspire-E5-571P:~/Escritorio/labo$ fastboot flash recovery /home/jose/D
ocumentos/twrp287r7.img
(bootloader) has-slot:recovery: not found
target reported max download size of 268435456 bytes
sending 'recovery' (8122 KB)...
OKAY [  0.259s]
writing 'recovery'...
OKAY [  0.383s]
finished. total time: 0.642s
```

Reinciamos nuestro teléfono. Volvemos a entrar a fastboot mode del dispositivo, seleccionamos el recovery mode, entramos con enter y si todo salió bien debe aparecernos la siguiente pantalla:



Listo, ya tenemos instalado nuestro custom recovery

3) Get root access

a) Ahora desde el celular, entrar al navegador y poner el siguiente link: forum.xda-developers.com/attachment.php?attachmentid=3655401&d=1456122222 Con esto nos descargamos el programa superSu, que nos permitirá obtener el acceso a root. El archivo que nos descargamos es un .zip con firma no autorizada, por eso es necesario tener el custom recovery.

b) Aún desde el celular, entramos a nuestra custom recovery y seleccionamos “Install”. Buscamos el archivo .zip del superSu y al econtrarlo swipeamos la pantalla en donde corresponda para instalar.

Si todo sale bien, twrp nos da la opción para reiniciar el celular.

c) Desde el Play Store del celular, descargamos la aplicación SuperSu (no es la misma que la anterior). Si el rooteo se completo correctamente, SuperSu nos mostrará la pantlla que se muestra a continuación, sino nos mostrará un mensaje similar “a necesita ser root para acceder”

Listo, ya tenemos rooteado nuestro moto g3.

Probar alguna aplicación de root

La aplicación que vamos a probar nos da la posibilidad de eliminar el bloatware de nuestro celular. ¿Qué es el bloatwatr? Son aplicaciones presintaladas por el fabricante del dispositivo que rara vez usamos y ocupan espacio sin necesidad (o casi sin necesidad).

Instalar y correr la app

1) Entrar al playstore y buscar “System app remover” o similar.
2) Descargar la app que muestra un tachito rojo con una flecha.
3) Cuando entremos a la app ya instalada nos mostrará un cartel que dice que necesita permisos de root, le damos permitir.
4) En la app, vamos a aplicaciones del sistema - > seleccionamos las apps a desinstralr - > Apretamos desinstalar

Links utilizados:

- Tutorial paso a paso:
https://motog5.net/unlock-bootloader-install-twrp-root-moto-g3/
- Particiones de Android:
https://www.addictivetips.com/mobile/android-partitions-explained-boot-system-recovery-data-cache-misc/