Trabajo Practico Nº 1.2

Herramientas :

Para la realización de esta práctica se provee una máquina virtual con las herramientas necesarias instaladas. Sin embargo, puede resultar de interés para el alumno el uso de otras distribuciones. Unadistribución Linux que puede resultar útil para investigar y encontrar nuevas herramientas de seguridad es KALI Linux - http://www.kali.org/

En una primer parte realizaremos un acceso a sistema operativo Linux sin la necesidad de contar con credenciales válidas y en la segunda mitad crackearemos passwords y usuarios de un sistema Windows utilizando Rainbow Tables.

Seguridad Física - Acceso a un Linux sin contraseña

1. Entrar a la maquina Virtual LINUX KALI manipulando el bootloader

(a) Cuando aparece grub ingresar en el modo edición presionando la tecla **e**

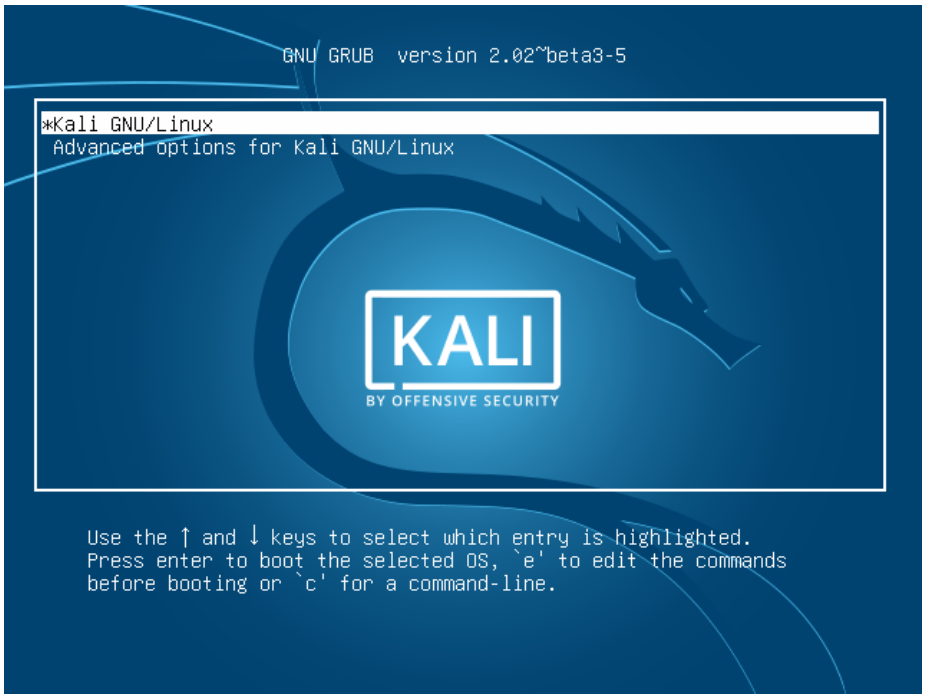

Figure 1: img/img1.jpg

(b) Luego, edite la entrada que especifica como Linux debe arrancar y agregue al final de la misma una indicación que diga que queremos hacer un By-Pass del sistema operativo. Para ello debe agregar **init=/bin/bash** y reemplazar **ro**(read only) por **rw**(read write)

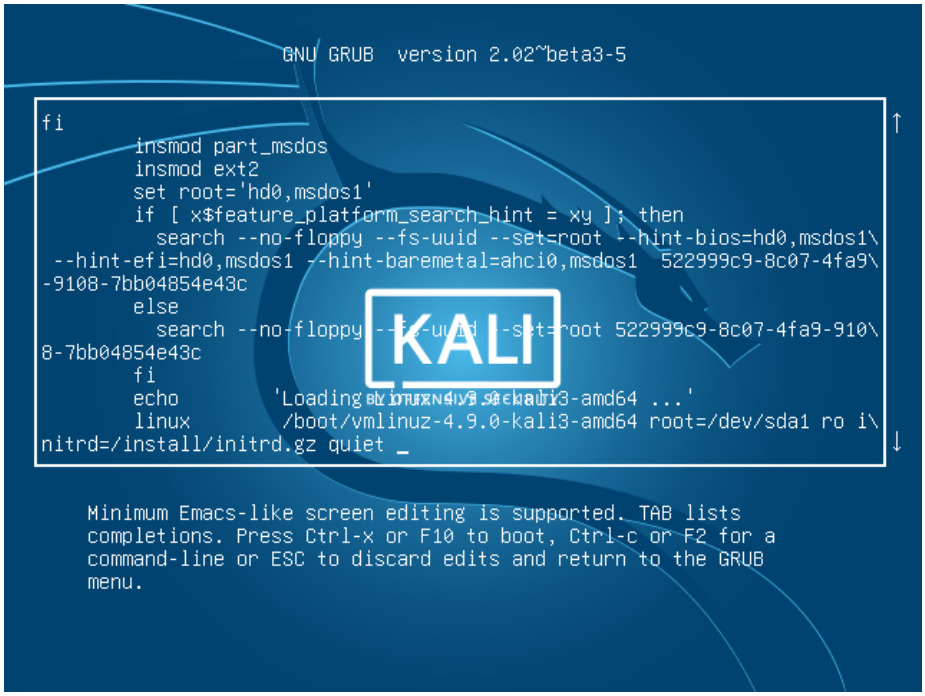

Figure 2: img/img2.jpg

(c) Luego presione **F10** para bootear con la entrada editada **Nota: Una vez que bootea, tenemos acceso a todos los archivos del sistema. Tal vez podemos poner un pendrive y copiar todo lo que nos interese.**

2. Manipular las claves del sistema (crack o modificación de contraseñas)

(a) En ambos casos necesitaremos permisos de escritura en el filesystem, si en el punto anterior no se reemplazo en la linea del kernel **ro** por **rw** vamos a necesitar ejecutar:

```
mount -o remount,rw /
```

para remontar la particion con permisos de escritura.

(b) Cracking de las contraseñas 1. Dado que en el sistema esta instalada la herramienta para crackear passwords, llamada “john”, podemos ejecutarla para crackear el archivo de passwords del sistema que es el archivo /etc/shadow, con el siguiente comando:

```
john /etc/shadow
```

2. Luego de haber realizado el cracking se puede verificar los resultados obtenidos con el siguiente comando:

```
john --show /etc/shadow
```

(c) En caso de querer cambiar la contraseña ejecutamos el comando: “‘ passwd

“‘ (d) Reinicie la PC utilizando la secuencia que provee VirtualBox para la combinación de teclas CONTROL – ALT - SUPRIMIR

Seguridad Física – Crack de claves de un sistema Windows

Con un método como el anterior, es posible entrar al filesystem de un sistema sin tener una contraseña de acceso. Luego podremos sacar la carpeta donde se almacenan las contraseñas de los usuarios

```
%systemroot%\system32\config\*
```

1. Arrancar la maquina virtual KALI
2. Iniciar la herramienta ophcrack para el ckack de password windows (KALI Linux → Password Attacks → ophcrack)
3. Instalar las rainbow tables que se encuentran en /root/rainbow_tables_xp_free_fast (Tables → Install)

```
Abrir el directorio /root/tables_xp_free_fast/
```

4. Abrir la carpeta donde están los archivos de contraseña windows provistos por el instructor (Load → Encrypted SAM)

```
Abrir el directorio /root/Windows_SAM/_config
```

5. Presione el botón Crack para empezar el CRACK!!! de las contraseñas
6. En base a la información reportada, que usuarios y que contraseñas había en el sistema Windows al que se le extrajo el archivo de contraseñas (SAM)