**Antecedentes**

Kali es una distribución que reúne herramientas utilizadas para un PenTest. La distribución es gratuita y se puede bajar del sitio oficial ( www.kali.org ). La distribución solo cuenta con un usuario, root, con contraseña toor. Lo primero que tiene que hacer es cambiar la configuración del teclado a español/latinoamericano o localizar las teclas de los caracteres &, -, ‘

En algunos puntos se enlistan los comandos a utilizar de forma explícita. Los carácteres # y $ representan el prompt del sistema y no es necesario escribirlos, hay que escribir los comandos que se encuentran a la derecha de estos caracteres.

**I. Preparando el teclado**

Por default Kali presenta su teclado en inglés, para cambiarlo a español es necesario utilizar el comando setxkbmap, especificando el lenguaje a usar. Ingrese al sistema y abra una terminal virtual. En la parte superior de la pantalla presione el icono que se encuentra al lado de Places y del icono de navegador Iceweasel. Una vez que la terminal se abra, teclee lo siguiente:

```
# setxkbmap es
```

**III. John The Ripper**

1. Baje el archivo juanito.zip de la siguiente dirección **http://cryptomex.org/Crack/juanito.zip**, cópielo dentro del directorio Desktop y extraiga su contenido dentro del directorio tecleando:

```
# unzip  juanito.zip
```

2. El comando anterior creará un directorio de nombre Juanito, posesiónese dentro de este y después vea su contenido

```
# cd Juanito
# ls
alta            dico50          passwd.no.shadow.file   shadow01
alta.md5        dictionary      passwd.vocales          shadow02
diccionario     passwd1         passwdVOCALES           windows.passwords.list
dico1           passwd2         pwd01
dico2           passwd.md5      pwd02
#
```

3. Dentro de los archivos extraídos, se encuentra uno de nombre limpia. Este archivo contiene un script encargado de borrar el archivo john.pot y volverlo a crear vacío. Lo primero a hacer es que el contenido cumpla con el formato de Linux:

```
# dos2unix limpia
```

Con el comando chmod proporcione permisos de ejecución al archivo creado;

```
# chmod 755 limpia
```

Es muy importante que use este script DESPUES de probar el comando john, de otra forma no obtendrá resultado alguno.

4. Probando el modo single (*recuerde ejecutar limpia después de john* )

```
# john -single passwd1
# john -single passwd2
# john -single passwd.no.shadow.file
```

Compruebe el contenido de los archivos de contraseñas con el comando more y saque sus conclusiones.

5. Probando el modo wordlist ( *recuerde ejecutar limpia después de john*)

Para atacar el archivo de contraseñas passwd1 con el diccionario dico1 teclee lo siguiente:

```
# john –w:dico1 passwd1
```

Ataque los tres archivos de contraseñas con los cuatro diccionarios: dico1, dico2, diccionario y dictionary.

6. Combinando diccionario y reglas.

   a. Cambie el formato del archivo palabras:

```
# dos2unix palabras
```

Comprueba las palabras que se van a probar con john tecleando

```
# john  -w:palabras  -stdout
```

Ahora comprueba las palabras que se prueban cuando se combina el diccionario con reglas y obtenga sus conclusiones.

```
# john  -w:palabras –rule  -stdout
```

Vuelva a hacer lo mismo que en el punto anterior, pero con la opción rules. Por ejemplo para hacer esto con el diccionario dico1 y el archivo de contraseñas passwd1, teclee:

```
# john –w:dico1 passwd1
# john –w:dico1 passwd2
# john –w:dico2 passwd1
# john –w:dico2 passwd2
```

Ejecute el script *limpia* y corra ahora con reglas:

```
#john –w:dico1 –rules passwd1
#john –w:dico1 –rules passwd2
#john –w:dico2 –rules passwd1
#john –w:dico2 –rules passwd2
```

7. Probando el modo incremental

Use el script alta para crear cinco cuentas, pero primero otorgue permisos de ejecución al archivo que contiene el script

```
# chmod 755 alta
#./alta pdigitos
Para terminar capture *** como cuenta
Cuenta:emata
Passwd:345789
        :
        :
Cuenta:rtorres
Passwd:721946
Cuenta:***
./alta: line 45: unexpected EOF while looking for matching `""
./alta: line 46: syntax error: unexpected end of file
#
```

Pruebe la opción digits, del modo incremental con las cuentas que acaba de crear:

```
# john --incremental:digits  pdigitos
```

Valide todas las opciones que se probaron:

```
# john --incremental:digits  –stdout
```

Teclee lo siguiente:

Si no hay respuesta de un minuto aborte la ejecución presionando las teclas CTRL y C al mismo tiempo.
Recuerde que debe correr el script de limpia antes.

```
# john --incremental:lower passwd1
# john --incremental:alpha passwd1
# john --incremental:asciipasswd1
```

Haga lo mismos con los archivos de contraseñas passwd2 y passwd.no.shadow.file

8. Pruebe john con el archivo de contraseñas de Windows ( windows.passwords.list )

**IV Creando su propio modo incremental**

1. Ejecute la utilería limpia

```
# limpia
```

2. Abra el archivo john.pot e introduzca los siguientes caracteres

```
:AEIOUaeiou
```

*Asegúrese que sean los únicos caracteres en el archivo.*

3. Ejecute john con la opción makechars y proporcionando como archivo de salida ***vocales.chr***

```
# john --make-charset=vocales.chr
```

4. Una vez terminado tome nota del número de caracteres generados ( lo que se despliega después del mensaje *Successfully written charset file: vocales.chr* )

5. Haga una copia de seguridad del archivo de configuración john.conf

```
# cp   john.conf   john.conf.original
```

6. Añada las siguientes líneas en el archivo john.conf ( antes de la línea con el comentario: *# Some pre-defined word filters* )

```
[Incremental:vocales]
File = /root/.john/vocales.chr
MinLen = 1
MaxLen = 8
CharCount = 10
```

7. Ejecute john con la nueva opción incremental y sobre el archivo ***passwd.vocales***

```
# ./john --incremental:vocales passwd.vocales
```

8. Modifique los parámetros anteriores, cambiando la longitud mínima del password a 8, quedando:

```
[Incremental:vocales]
File = /root/.john/vocales.chr
MinLen = 8
MaxLen = 8
CharCount = 10
```

9. Vuelva a ejecutar john sobre el archivo de passwd.vocales

```
#  ./john --incremental:vocales passwd.vocales
```

¿Percibió alguna diferencia?

**VI Crackeo en línea**

Para probar los diferentes programas de crackeo en línea, posesiónese en el directorio Juanito

1. Inicie el servicio ssh en su equipo
2. Extraiga su dirección IP y compártala con su compañero:

```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:74:a1:d9
inet addr:192.168.235.135  Bcast:192.168.235.255  Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe74:a1d9/64 Scope:Link
```

3. Probando el programa Hydra. Teclee lo siguiente:

```
# hydra  -l root  -P dico50  <IP de su vecino>  ssh
```

4. Para probar ncrack teclee lo siguiente:

```
# ncrack -p 22 –user root -P dico50  <IP de su vecino>
```

5. Para probar medusa, teclee lo siguiente:

```
# medusa -u root -P dico50  -h   <IP de su vecino>   -M ssh
```