Manual BackTrack:

En este articulo vamos a aprender como instalar BackTrack desde cero y como utilizarlo. También aprenderemos a utilizar y enumerar algunas de las herramientas que incluye y el funcionamiento del John The Ripper en esta distribución ya que permite realizar el crackeo de una contraseña con diversos PCS a la vez cosa que da una mayor rapidez y eficiencia. Este proceso no lo incluyen las otras distribuciones ya que es una característica propia de esta distribución.
Lo que veréis entre * en los cuadros de texto son mis propios comentarios eso no debéis ponerlo en la consola ya que son pequeñas aclaraciones que os permitirán entender mejor los procesos que estamos realizando.

BackTrack:

BackTrack es una distribución Linux en formato Live-CD enfocada a la seguridad y al hacking. Esta distribución consta de numerosas herramientas enfocadas a la seguridad. BackTrack es una distribución muy aceptada y popular entre las comunidad de Seguridad Informática. BackTrack fue creada de la unión de dos distribuciones orientadas a la seguridad, el Auditor +Whax.

Inicio de BackTrack:

Lo primero que debemos hacer es descargar el Live-CD de su pagina Web donde podemos encontrar la distribución en descarga directa http://www.remote-exploit.org/backtrack_download.html ahora tenemos que grabar el archivo .iso como imagen de Cd.

Como grabar un ISO:

Si nunca ha grabado un una imagen iso una manera muy sencilla de hacerlo es instalar el Nero (uno de los programas mas conocidos para grabar cds o DVDs) después de la instalación tema que no vamos a abordar en este artículo debéis hacer lo siguiente. Clic derecho—Abrir con—Elegir programa—Examinar.
Después buscad el ejecutable Nero.exe y lo seleccionáis el mismo programa identificara el archivo y solo deberéis seguir los pasos típicos de grabación.

Sigamos...:

Una vez hemos realizado todo esto debemos iniciar el PC desde el disco previamente grabado, últimamente los nuevos PCs ya lo detectan solo metiendo el CD en el lector que tengas si es un PC mas antiguo deberemos configurar la bios para que arranque desde CD bien ahora ya estamos iniciando el BackTrack (Ver Imagen 1.0)

Imagen 1.0

Si todo ha cargado correctamente nos pedirá los siguientes datos:
Usuario: root

Pasword: toor
Luego nos quedara de la siguiente manera (Ver Imagen 1.1).

Imagen 1.1

Creando Particiones:

Cada disco duro constituye una unidad física distinta. Sin embargo, los sistemas operativos no trabajan con unidades físicas directamente sino con unidades lógicas. Dentro de una misma unidad física de disco duro puede haber varias unidades lógicas. Cada una de las unidades lógicas es lo que nosotros nombramos partición. Eso quiere decir que podemos dividir nuestro disco duro en dos unidades lógicas y hacer como si tuviéramos dos discos duros. Las particiones pueden ser de dos tipos: particiones primarias y particiones lógicas. Aunque solo las particiones primarias se pueden activar. Para que un disco duro sea utilizable tiene que tener al menos una partición.
Los SO deben instalarse en particiones primarias porque si no el SO no arrancaría. El resto de particiones que no contengan un SO pueden ser creadas como particiones lógicas. Hay algunos SO que dicen poder ser instalados en particiones primarias pero esto no es del todo cierto ya que deben tener instalados un pequeño programa en una partición primaria.
Uno de los programas más conocidos para crear particiones en el Partition Magic ahora en su versión 8.0 para mas información podéis visitar http://es.wikipedia.org/wiki/PartitionMagic pero en este caso vamos a crear las particiones desde la misma consola del BackTrack introducimos lo siguiente. Para escribir la típica / lo debemos hacer desde el teclado numérico ya que el teclado en el BackTrack no es en español y es diferente al que nosotros solemos usar. Ahora realizamos los siguientes pasos.
Código:

```
BT ~ # fdisk /dev/sda
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF
disklabel
Building a new DOS disklabel. Changes will remain in memory only, until you
decide to write them. After that, of course, the previous content won't be
recoverable.
     Command (m for help):n [enter]
Command action
       e        extended
       p        primary partition (1-4): p [enter]*Aquí seleccionamos la
partición primaria*
Partition number (1-4): 1[enter] *Esto es el numero de la partición*
       First cylinder (1-456, default 1):[enter] *Presionando enter lo que
hacemos
 es seleccionar la opción default que es 1 *
     Using default value 1
    Last cylinder or +size or +sizeM or +sizeK (1-456, default 456): +50M
[enter] *Esto
 es el tamaño en megas de la partición creada*
Command (m for help):n [enter]
```

```
Command action
       e        extended
       p        primary partition (1-4):p [enter]
Partition number (1-4): 2 [enter]
First cylinder (52-456, default 52):[enter]
    Using default value 8
     Last cylinder or +size or +sizeM or +sizeK (8-456, default 456): +512M
[enter]
    Command (m for help): n [enter]
Command action
       e        extended
             p  primary partition (1-4):p [enter]
Partition number (1-4): 3 [enter]
    First cylinder (71-456, default 71):[enter]
    Using default value 71
    Last cylinder or +size or +sizeM or +sizeK (71-456, default 456): [enter]
Using default value 456
Command (m for help): a [enter]
Partition number (1-4): 1 [enter]
Command (m for help): t [enter]
Partition number (1-4): 2 [enter]
Hex Code (Type L to list codes ): L  * Nos listara el numero de las opciones que
podemos elegir*
Hex Code (Type L to list codes): 82 *(Ver Imagen 1.2) El  82 es Linux Swap,
vosotros podéis elegir la que más os convenga*
Command (m for help): w [enter]
The partition table has been altered!
Calling ioctl() to re-read partition table.
Syncing disks.
```

Imagen 1.2

Creando Sistema de Ficheros:

Lo que tenemos que hacer ahora es crear el sistema de ficheros en las particiones para poder escribir datos en las particiones. Normalmente cada sistema de ficheros ha sido diseñado para mejorar el rendimiento de un Sistema Operativo en concreto. Hay diferentes sistemas de ficheros voy a explicar brevemente cada uno de ellos:

-FAT: Este sistema de archivos se basa en una tabla de asignación de archivos que se convierte en el índice del disco duro. Aunque este sistema tiene grandes limitaciones como por ejemplo que el nombre de archivos debe ser corto, tamaño máximo de particiones de 2GB y algunos otros inconvenientes.

-VFAT: En este sistema de archivos se consigue solucionar alguno de los problemas que tenía el FAT como por ejemplo que logra ampliar el límite de caracteres a 255 entre nombre y extensión.

-FAT32: Permite trabajar con particiones mayores de 2GB es una de las mejoras que incorpora.

-NTFS: Este es el sistema de archivos que permite utilizar todas las características de seguridad y

protección de archivos de Windows NT.
-HPFS: HPFS es el sistema de archivos propio de OS/2. Utiliza una estructura muy eficiente para organizar los datos en las particiones.
Para crear las particiones debemos hacer lo siguiente os explicare algunos de los pasos que realizaremos pero no todos porque algunos son totalmente deductivos y repetitivos.
Código:

```
BT ~ # mkfs.ext3 /dev/sda1
mke2fs 1.38 (30-Jun-2005)
Filesystem label=
    OS type: Linux
   Block size=1024 (log=0)
   Fragment size=1024 (log=0)
    14056 inodes, 56196 blocks
    2809 blocks (5.00%) reserved for the super user
    First data block=1
7 block groups
     8192 blocks per group, 8192 fragments per group
     2008 inodes per group
     Superblock backups stored on blocks:
               8193, 24577, 40961
     Writing inode tables: done
     Creating journal (4096 blocks): done
     Writing superblocks and filesystem accounting information: done
This filesystem will be automatically checked every 25 mounts or 180 days,
whichever comes first. Use tune2fs -c or -i to override
BT ~ # mkfs.ext3 /dev/sda3 *Ver Imagen 1.3*
   mke2fs 1.38 (30Jun-2005) Filesystem label=
   OS type: Linux
   Block size=4096 (log=2)
    Fragment size=4096 (log=2)
                387840 inodes, 775136 blocks
   38756 blocks (5.00%) reserved for the super user
    First data block=0
     24 block groups
     32768 blocks per group, 32768 fragments per group
     16160 inodes per group
      Superblock backups stored on blocks:
                  32768, 98304, 163840, 229376, 294912
      Writing inode tables: done
      Creating journal (16384 blocks): done
      Writing superblocks and filesystem accounting information: done
     This filesystem will be automatically checked every 27 mounts or
     180 days, whichever comes first. Use tune2fs -c or -i to overrid
```

Imagen 1.3

Montar los dispositivos:

Lo siguiente que debemos hacer es montar los dispositivos. Accedemos al directorio tmp para montarlos. Creamos los directorios necesarios y montamos los dispositivos. Lo haremos todo de la siguiente manera:

Código:

```
BT ~ # cd /tmp *Accedemos al
directorio tmp*
BT tmp ~ # mkdir boot *Creamos el
directorio boot*
BT tmp ~ # mkdir bt2 *Creamos el
direcotorio bt2*
BT tmp ~ # mount /dev/sda1 boot
*Montar la primera particion de la unidad sda, en el directorio mencionado *
BT tmp ~ # mount /dev/sda3 bt2
*Montar la tercera particion de la unidad sda, en el directorio mencionado *
```

Lo que debemos introducir ahora es startx en la consola lo que hará será iniciar el entorno grafico KDE. Bueno una vez iniciado el entorno grafico nos quedara así. (Ver Imagen 1.4).

Imagen 1.4

Ahora vamos a instalar el BackTrack en nuestro HD (disco duro). Bueno lo primero que hacemos es desplegar el menú. Por si alguien no lo sabe es la K azul que hay abajo a la izquierda. Seguidamente vamos a System y después a BackTrack Installer.

Nos saldrá el cuadro de instalación lo que debemos hacer es rellenarlo con los datos adecuados con los que antes hemos utilizado para prepara la instalación.

Debemos rellenar los datos de la siguiente manera: (Ver Imagen 1.5).

Imagen 1.5

Source: /Boot

Install BackTrack to: /tmp/bt2

Write MBR to: /dev/sda
Installation Method: Real (2700 MB Requiered)
Y seguidamente le damos a install. Y nos quedara el SO instalado en nuestro disco duro ahora no nos hará falta el Live-CD para usar BackTrack.

De paseo:

Bueno ahora vamos a dar un paseo por BackTrack y nombrar algunas de los comandos de Linux y seguidamente las herramientas que lleva incluida esta distribución.

Comandos Básicos Linux:

Cd /nombre directorio/- Cambia al directorio señalado
Cp /origen/ /destino/- Copia el archivo especificado
Mkdir /dirección/- Crea un directorio donde le especifiquemos
Mv /origen/ /destino/- Mueve el archivo donde le digamos
Ls- Lista del contenido del directorio en el que nos encontremos
Cat- Se utiliza para ver el contenido de un archivo

Herramientas:

BackTrack lleva una serie de herramientas muy interesantes enfocadas al mundo de la seguridad y del hack. Voy a señalar el tipo de herramientas que lleva y voy a nombrar algunas de ellas. Os voy a explicar como utilizar una herramienta por consola así tendréis una guía a seguir para poder utilizar todas las herramientas ya que todas pueden utilizarse de manera intuitiva y con ayuda de un pequeño traductor.
Alguno de los grupos de herramientas no voy a explicarlos porque son demasiado evidentes y otros no demasiado interesantes. Para acceder a las herramientas vamos al menú de BackTrack y después BackTrack aquí como podéis ver es donde están todas las herramientas.
El primer tipo de herramientas son las de:

Enumeration: (Ver Imagen 1.6)

Imagen 1.6

Estas herramientas se utilizan para sacar información de las maquinas como por ejemplo su SO y algunas de ellas también dan información sobre los servicios que corren en el PC examinado. Una de las herramientas más conocidas en este campo es Nmap que funciona como scanner pero también puede englobarse en este campo.
Os voy a explicar como usar una de las herramientas que incluye Enumeration en la pestaña de Operating System---> XProbe2.
Esta aplicación se utiliza por consola como habréis podido comprobar después de ejecutarla.
Al abrir la aplicación nos quedara así (Ver Imagen 1.7)

Imagen 1.7

Arriba del todo nos sale el nombre de programa y el autor.
Más abajo nos sale su modo de uso que es: Xprobe2 [Options] target.
Como vemos primero va el nombre de programa para hacer referencia a el en consola después las opciones que salen enumeradas justo debajo del modo de uso y target es la ip o dns del PC a escanear. Vamos a realizar una prueba.
haremos la prueba con nuestro mismo PC. Pondremos Xprobe2 127.0.0.1 en esta ocasión no daremos ninguna opción eso ya deberéis ponerlas a vuestro gusto. Suponiendo que no entendáis nada de lo que dicen las opciones podéis usar el mismo traductor que tiene google http://www.google.es/language_tools?hl=es esto os permitirá utilizar cualquier herramienta ya que podréis traducir las palabras que no entendáis.
Bueno después de hacer realizado el escaneo nos quedara lo siguiente. (Ver Imagen 1.8)

Imagen 1.8

Como podéis ver al finalizar el escaneo abajo del todo pone:
-Host 127.0.0.1 Running OS: Linux Kernel 2.4.30" (Guess probability: 100%)
El host es nuestra propia maquina por eso mismo el Sistema Operativo o el Kernel que detectara será el del BackTrack y nos dice que el Sistema Operativo que usa es el Kernel 2.4.30 como veis la herramienta nos ha dado el Kernel que tiene la máquina que hemos escaneado. La herramienta ha cumplido totalmente su función. Este tipo de herramientas son muy útiles cuando queremos saber el Kernel que tiene alguna maquina en concreto para saber que exploits podemos utilizar.

Exploit Archives: (Ver Imagen 1.9)

Este grupo de herramientas son los exploits este apartado consta de la herramienta ya muy conocida Metasploit.
Y por otro lado de otra herramienta muy importante en esta distribución y es Milw0rm-Milw0rm Archive. Esta herramienta consta de todos los exploits de milw0rm ordenados por Plataforma seguidamente por Denial of Service, Remote o Local, cuando hemos dado todos estos datos

obtendremos una lista de todos los exploits disponibles ahora solo cabe elegir uno y utilizarlo. Se ha de reconocer que si uno sabe utilizar esta herramienta tendrá en su poder una herramienta de gran potencial.

Imagen 1.9

En este apartado del artículo os voy a enseñar a utilizarla esta herramienta. Una vez la hemos abierto desde el menú de herramientas accederemos a platfmors de la siguiente manera. Cd platfmors una vez en este directorio miraremos que elecciones tenemos por hacer. Ejecutamos el comando Ls para saber que carpetas hay en este directorio (Ver Imagen 2.0) Como podemos ver nos sale una lista con las diferentes plataformas entre ellas destacaremos Linux y Windows que son las mas destacables.

Imagen 2.0

Una vez elegida la plataforma haremos lo siguiente cd nombredelaplatarforma.
Según la plataforma que elijamos nos saldrá, Denial of Service, Remote, Local ahora accedemos al tipo de exploit que queramos por ejemplo cd Remote cuando estemos en este directorio volvemos a ejecutar el comando Ls y nos saldrá una lista con todos los posibles exploits ahora lo que debemos hacer es darles permisos de ejecución para eso haremos lo siguiente.

Permisos de ejecución:

Para cambiar los permisos de un archivo debemos usar el comando chmod.
Este comando tiene varias sintaxis permitidas la primera es:
chmod [opciones] modo-en-octal fichero
Opciones típicas son: -R para que mire también en los subdirectorios de la ruta.
- v para que muestre cada fichero procesado
El modo en octal es un número en base 8 que especifique el permiso. Por ejemplo, 777 es indica todos los permisos posibles para todos los tipos de usuario. 666 indica que se dan permisos de lectura y escritura, pero no de ejecución. 766 indica que se dan permisos de lectura y escritura, pero sólo tienen permiso de ejecución para los usuarios que son dueños del archivo. 755 indica permisos

para lectura y ejecución, pero escritura sólo para el usuario que es dueño del archivo.
Ejemplo:
chmod 777 exploit.sh
Asigna todos los permisos al archivo exploit.sh
La segunda no utiliza los números de manera octal
chmod [opciones] modo [, modo]… fichero
Para ello tenemos que tener claros los distintos grupos de usuarios:
u: usuario dueño del fichero
g: grupo de usuarios del dueño del fichero
o: todos los otros usuarios
a: todos los tipos de usuario
También hay que saber la letra que abrevia cada tipo de permiso:
R: son los permisos de lectura
W: se refiere a los permisos de escritura
X: son los permisos de ejecución
Ejemplo:
chmod a=rwx exploit.sh
Después de hace resto el archivo exploit.sh tendrá permisos de lectura, escritura, ejecución para todos los usuarios.
Cuando un archivo tenga permisos de ejecución nos saldrá de color verde en la consola.
Una vez le hemos dado permisos lo que debemos hacer es compilar el exploit para eso hacemos gcc nombre.c destino.
Si no ponemos destino simplemente hacemos gcc nombreexploit.c
Lo que hará será crear un archivo con el nombre de a.out simplemente lo que debemos hacer ahora es ejecutar el exploit de la siguiente manera
A.out (Ver Imagen 2.1)

Imagen 2.1
Una vez ejecutado el exploit nos dirá el modo de usarlo.
Usage: a.out –h <hostname> -port <Puerto> -u <usuario> -s <password>
Como veis nos da unos pasos muy sencillos para ejecutar y utilizar correctamente el exploit.

Fuzzers: (Ver Imagen 2.2)

Es una metodología para buscar errores en un protocolo, mediante la cual se envían diferentes tipos de paquetes que contienen datos que empujan las especificaciones del protocolo al punto de romperlas. Estos paquetes se mandan a un sistema capaz de recibirlos para después monitorear los resultados.
Que puedes hacer con el Fuzzing:
1. Descubrir vulnerabilidades en cualquier tipo de protocolo.
2. Dar información para crear códigos con el fin de ejecutar código arbitrario o cause DoS.
3. Causar una denegación del servicio.

4. Causar logs en el sistema atacado.
5. En pocos casos romper permanentemente un servicio.
6. Probar la fiabilidad de ciertas aplicaciones.
Como veis es una técnica que si sabiendo utilizarla podemos sacarle un gran rendimiento.

Spoofing: (Ver Imagen 2.3)

Imagen 2.3

En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.
Hay diferentes tipos de Spoofing que voy a enumerar y explicar muy brevemente:
IP Spooging- Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.
Arp Spoofing- Suplantación de identidad por falsificación de tabla ARP.
DNS Spoofing- Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa.
Web Spoofing- Suplantación de una página web real aunque no debe confundirse con el pishing.
Mail Spoofing- Suplantación en correo electrónico de la dirección e-mail de otras personas o entidades. Esta técnica es usada con asiduidad para el envío de e-mails como suplemento perfecto para el uso de phising y para SPAM, es tan sencilla como el uso de un servidor SMTP configurado para tal fin.

Tunneling: (Ver Imagen 2.4)

La técnica de tunneling consiste en implementar un protocolo de Red sobre otro .El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo, la redirección de tráfico.

Imagen 2.4

Forensic Tools: (Ver Imagen 2.5)

Imagen 2.5

Se denomina análisis forense al proceso de analizar una copia completa de un sistema que ha sufrido una intrusión o ataque.
El análisis forense permite obtener la mayor cantidad posible de información sobre:
El método utilizado por el atacante para introducirse en el sistema
Las actividades ilícitas realizadas por el intruso en el sistema
El alcance y las implicaciones de dichas actividades
Las "puertas traseras" instaladas por el intruso
Realizando un análisis forense nos permitirá, entre otras cosas, recuperarnos del incidente de una manera más segura y evitaremos en la medida de lo posible que se repita la misma situación en cualquiera de nuestras máquinas.
Un buen análisis forense debe dar respuestas a varias cuestiones, entre las que se encuentran las siguientes:
¿En que fecha exacta se ha realizado la intrusión o cambio?
¿Quién realizó la intrusión?
¿Cómo entró en el sistema?
¿Qué daños ha producido en el sistema?
Si una vez realizado el análisis forense no conocemos con exactitud las respuestas a estas preguntas, no tendremos un análisis funcional. Esto puede derivar en futuros ataques, bien por la misma persona, o bien por diferentes medios de intrusión que desconozcamos.

Crackeo de Contraseñas:

Bueno lo que os voy a enseñar ahora es como aprovechar el Jonh The Ripper y el BackTrack para poder creackear contraseñas con varios pcs. Teniendo la potencia de varios pcs lo que conseguiremos es reducir el tiempo de creackeo por ejemplo si en un pc normal una contraseña tarda en ser crackeada 2 días si utilizáramos este método 2 pcs solo tardaría 1 día imagínense el potencial que podemos sacarle a esto.
Para los que no saben:
John the Ripper es un programa de criptografía que aplica fuerza bruta para descifrar contraseñas. Es uno de lo más utilizados en su campo. Esta herramienta fue diseñada en principio para sistemas operativos Unix pero luego se extendió u ahora funciona en al menos 15 Sistemas Operativos diferentes. Al ser de software libre se puede encontrar en la mayoría de distribuciones Linux.
Aunque es una herramienta catalogada para el cracking. Es una utilidad para administradores que si es usada adecuadamente no crea ningún tipo de peligro para el Sistema Operativo en el que se usa dicha Herramienta.

Como Funciona:

Jonh the Ripper lo que hace es usar un ataque de fuerza bruta usando un diccionario con palabras que puede ser contraseñas típicas y las van probando de una en una. Esto funciona bien porque la

mayor parte de las contraseñas que usa la gente son palabras de diccionario. Pero John the Ripper también prueba con variaciones de estas palabras: les añade números, signos, mayúsculas y minúsculas, cambia letras, combina palabras, etc.
Además ofrece el típico sistema de fuerza bruta en el que se prueban todas las combinaciones posibles, sean palabras o no. Éste es el sistema más lento, y usado sólo en casos concretos, ya que los sistemas anteriores.
Bueno lo que debemos hacer ahora es bajarnos los archivos apropiados para realizar esta actividad.

Bajando las herramientas necesarias:

Para bajar las herramientas que necesitamos debes entrar en la página http://offensive-security.com/downloads.html.

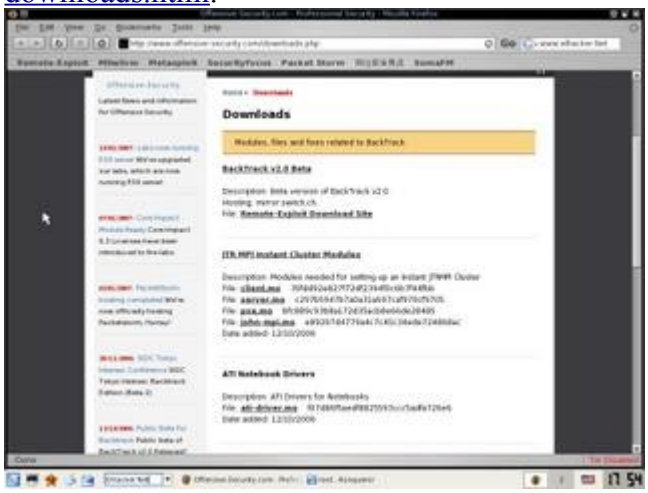

Imagen 2.6

Hemos de bajar estos archivos: (Ver Imagen 2.6)

Pxe.mo
Client.mo
Server.mo
John-mpi.mo

Las guardaremos en el directorio Root ya que así a la hora de ejecutarlas nos será más cómodo.
Ahora lo que vamos a hacer es darles permisos de ejecución como ya hicimos anteriormente con otros archivos. (Ver Imagen 2.7)

Imagen 2.7

Una vez que ya les hemos dado permisos de ejecución lo que debemos hacer ahora es lo siguiente.
Lo siguiente lo haremos utilizando el entorno grafico primero de todo abrimos el menú después abrimos la sección Internet y seguidamente abrimos Konqueror (Konqueror es un navegador libre. Funciona como gestor de archivos y también como navegador Web) y accedemos al directorio /root que es donde están los archivos que bajamos hace un momento.

Preparando el Servidor:

Una vez que accedemos al directorio. Ejecutamos el archivo Server.mo y nos creara un archivo llamado Server.py esto es un modulo cosa que ara que ahora el Sistema Operativo cargue este modulo al iniciarse. Ahora debemos reiniciar el PC abrimos la consola y escribimos reboot comando que utilizaremos siempre que queramos que el Pc se reinicie. Una vez reiniciado el Pc nos saldrá lo siguiente: (Ver Imagen 2.8)

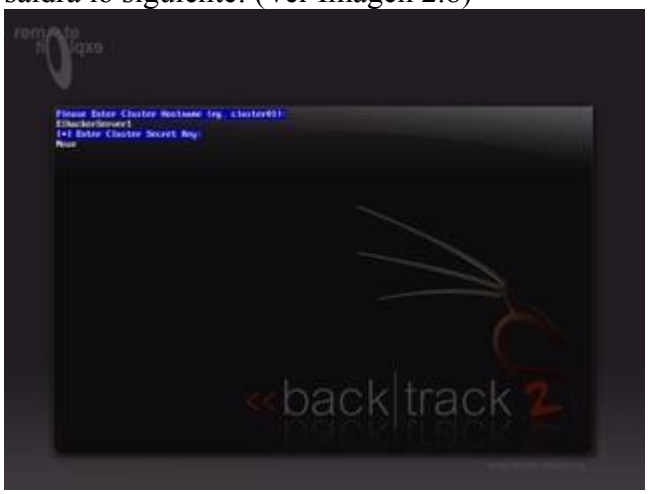

Imagen 2.8

Primero nos pide el nombre que tendrá el Hostserver aconsejo que los nombres no lleven ni – ni puntos ni otros caracteres que no sean letras ya que solo contara hasta que aya una separación o un guión o un punto. Y después la clave secreta que debemos recordarla para después poder configurar el cliente. Una vez en la consola hacemos lo siguiente mpdtrace –l y nos dará la ip que después deberemos introducir en el cliente.

Una vez configurado la maquina Server.

Configurando Cliente:

Cogeremos la máquina que actuara de cliente. Lo que haremos será lo mismo que hemos hecho con la maquina Server pero en esta ocasión el archivo que ejecutaremos será el de Client.mo que a su vez nos creara el archivo Cliente.py, una vez ejecutado este archivo reiniciamos el PC. Cuando vuelva a iniciarse nos saldrá unas cuestiones que debemos completarlo de la siguiente manera (Ver Imagen 2.9)

Imagen 2.9

1-Aquí debemos introducir el nombre que queremos darle al Hostcliente.

2-Debemos introducir la ip que obtuvimos en el Pc maquina.

3-Debemos introducir la misma contraseña que escribimos en la configuración del cliente.

Ahora para ver que los dos PCs están conectados ejecutamos el comando mpdtrace como veis en la lista nos salen 2 PCs que son los dos nombres que hemos configurado ahora si crackeamos una contraseña lo harán los dos Pcs como si fueran uno ósea un Pc con el doble de potencia bien

seguidamente lo que haremos será utilizar el crackeador.

Crackeando:

Ahora vamos a realizar las pruebas de Crackeo con los dos Pcs sobre la contraseña de administrador. El archivo que contiene la contraseña es el archivo /etc/shadow. Vamos a realizar este ejercicio paso por paso.

Lo primero que vamos a hacer es cambiar la contraseña que viene por defecto en BackTrack que es (toor), para eso abriremos la consola y ejecutaremos el comandos Passwd yo en este caso he cambiado la contraseña toor por la contraseña hacker he usado esta contraseña para que el crackeador se de prisa en creackearla ya que hacer es un termino muy corriente mediante el método diccionario le será muy fácil creckearla. (Ver Imagen 3.0)

Imagen 3.0

Bien una vez cambiada la contraseña lo que vamos a hacer es copiar el archivo shadow que se encuentro en el directorio /etc lo copiaremos en el directorio /pentest/password/john-1.7.2/run (Ver Imagen 3.1)

Imagen 3.1

El comando que se usa para realizar una acción utilizando los Dos Pcs es mdp ejecutemos el comandos en la consola mpdhelp y ahora podemos ver los comandos mas importantes de este comando. (Ver Imagen 3.2)

Imagen 3.2

Ahora ejecutaremos el comando mpdrun como veis nos informa de lo que debemos hacer para poder ejecutar acciones con diversos PCs. (Ver Imagen 3.3)

Imagen 3.3

Bien por ultimo vamos a realizar el crackeo del archivo /etc/shadow como os dije antes este es el archivo que contiene la contraseña del administrador de el Sistema.

Bien ahora vamos al menú--- BackTrack--- Password Attaks--- Offline Attaks y abrimos el crackeador john una vez abierto ejecutaremos el comando ls para ver que verdaderamente copiamos el archivo shadow en el directorio. Ahora lo que debemos hacer es darle permisos de ejecución para poder crackearlo ejecutamos chmod 777 shadow. Bien seguidamente debemos ejecutar el comando ls y como veremos estará en verde cosa que quiere decir que le dimos permisos de ejecución.

Bueno ahora lo que vamos a hacer es mirar si los dos ordenador están conectados correctamente ejecutamos el comando mpdtrace si nos sale una lista con los dos Pcs es que todo esta correcto y podemos proceder a crackear el archivo. Bien cuando de verdad hemos comprobado que están conectados ejecutaremos lo siguiente.

ElhackerCliente run ~ # mpiexec john shadow (Ver Imagen 3.4)

Como podéis ver después de ejecutar este comando john nos da la contraseña de administrador que antes habíamos puesto.

Imagen 3.4