Hola, soy **Gusanoloko.** Alguien pidió un tutorial de Termineter …..... intentare explicar humilde y buenamente hasta donde llego. Perdonen las faltas de ortografía y demás obscenidades que puedan ustedes encontrar.
Puede usted criticar, copiar, pegar , modificar, maltratar, redistribuir e incluso comerse la info las afotos o lo que desee.

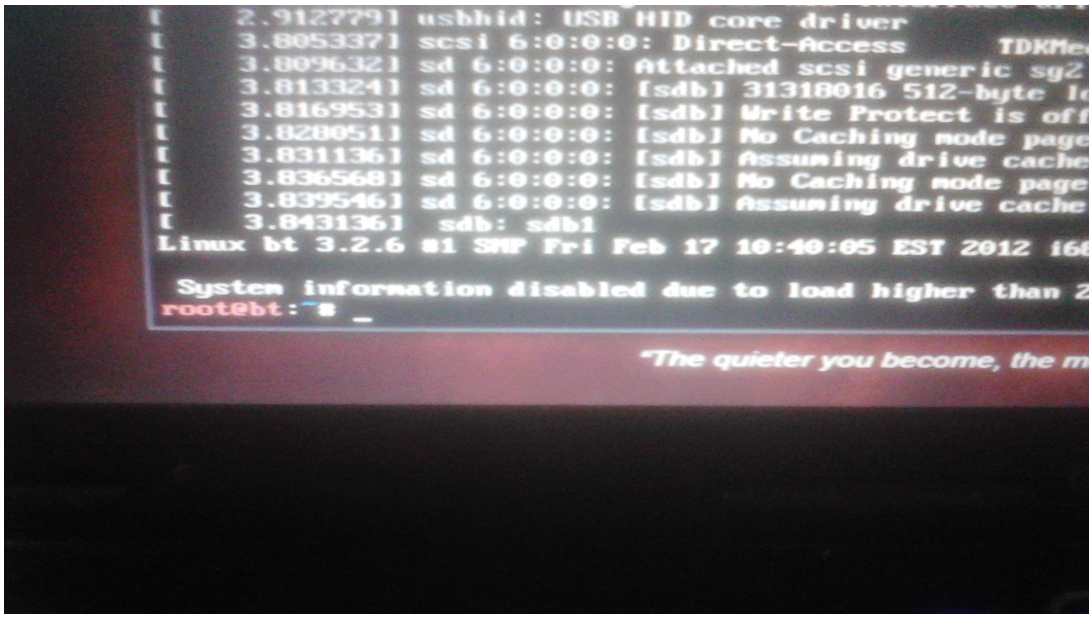
Lo primero donde encontramos Termineter. http://code.google.com/p/termineter/ es su descarga oficial.
También lo encontramos instalado en los sistemas de penetración y test Linux como Backtrak5 R3 http://www.backtrack-linux.org/ o en Kali Linux http://www.kali.org/. Estos sistemas operativos vienen con todas las librerías y lenguajes necesarios para trabajar.
Yo basare este escrito (o bodriotuto) en Backtrack5, pero lo pueden instalar en cualquier distro Linux, lo probé en Ubuntu y en Mint . (perdonen pero el ventanas es mu carismo ,coge muchismos virus y demasiado lento)
Backtrack solo tienen que descargarlo, montarlo en un pendrive y arrancar su ordenador con el pendrive. (puede ser que tengas que configurar en las BIOS el firts boot...primer arranque).

El amigo Termineter en cuestión es un programa escrito en Python (uno de los muchos lenguajes de programación http://www.python.org/) que realiza la función de poder conectarnos o entendernos con el contador inteligente mediante un puerto serie y su protocolo de comunicación. Utiliza las librerías python-serial http://pyserial.sourceforge.net/ para crear la conexión mediante su Framework http://es.wikipedia.org/wiki/Framework .
Mas link de la familia esta que lo crío:
http://blog.securestate.com/author/spencer_mcintyre/
https://github.com/GrayHatLabs/john_commor_c1218/tree/master/termineter2
https://github.com/zeroSteiner/termineter
Que es un protocolo:(esto no recuerdo de donde lo saque pero queda mu bien)
En informática y *telecomunicación*, un protocolo de comunicaciones es un conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellos para transmitir información por medio de cualquier tipo de variación de una *magnitud física*. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos.
Si usted miro los links anteriores ya en sus primeras lineas descubrimos que termineter es para protocolo ANSI C12.18 es un ANSI estándar que describe un protocolo utilizado para la comunicación de dos vías con un metro, utilizado principalmente en los mercados de América del Norte. El estándar C12.18 está escrito específicamente para las comunicaciones de metro a través de un tipo ANSI 2 puerto óptico, y especifica de nivel inferior los detalles de protocolo. ANSI C12.19 especifica las tablas de datos que se utilizarán. ANSI C12.21 es una extensión del C12. 18 escritas para módem en lugar de las comunicaciones ópticas, por lo que es más adecuado para la lectura automática de contadores. También descubrimos que el sistema es de 7 bites.
Aquí funcionan con Protocolo IEC 60870- 5- 102: De comunicación serial que fue definido para lectura de totales integrados o contadores y sistema de 8 bit.
Info sobre protocolo utilizado en el estado español.
http://eprints.ucm.es/9151/1/TC2006-73.pdf
http://www.ree.es/sites/default/files/01.../**protoc_RMCM10042002.pdf**

Ya sabemos algo..... NO NOS SIRVE AKI.
Verán ustedes al final porque sigo con esto.
Una vez que ya sabemos algo empecemos con el lio este.

Cuando esta cargando backtrack5 llega un momento que se para y sale en la pantalla abajo unas

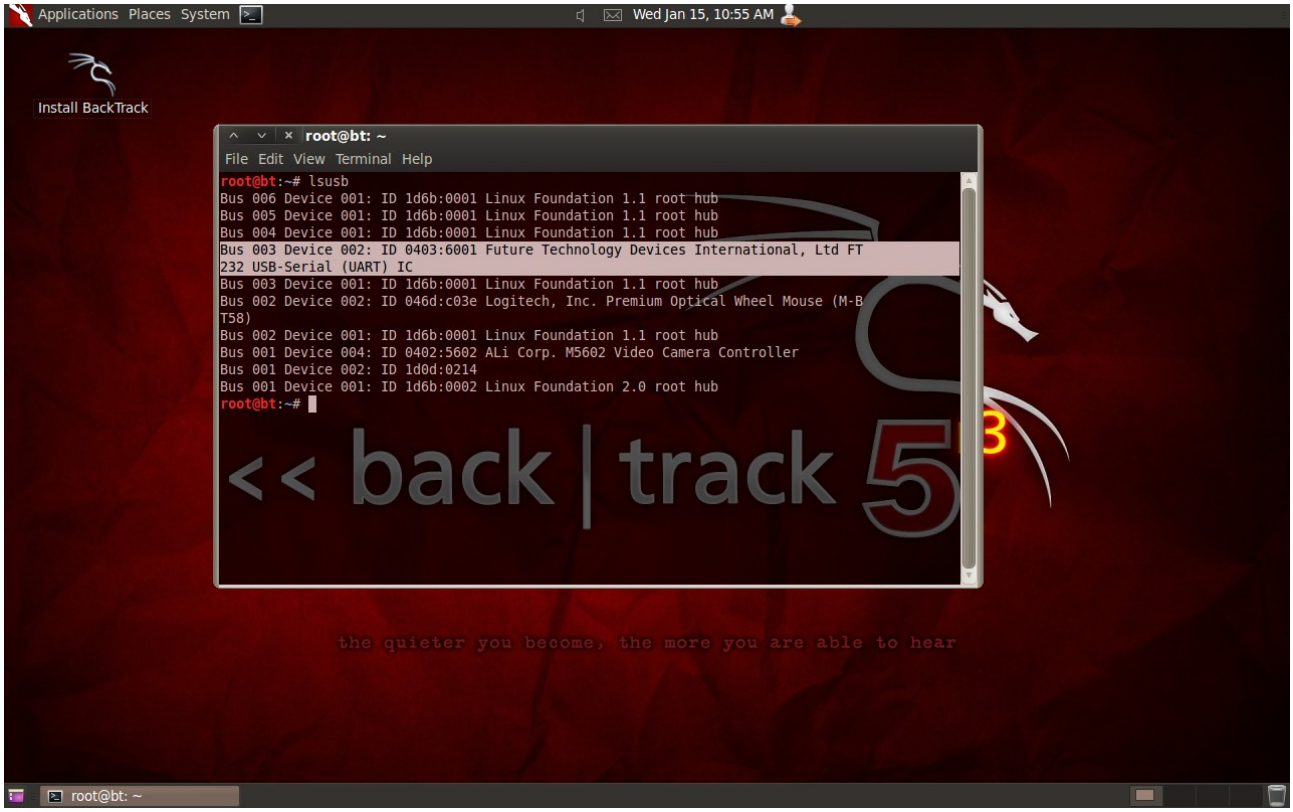
lineas que pone esto;
root@bt: #
Con afoto mejol.



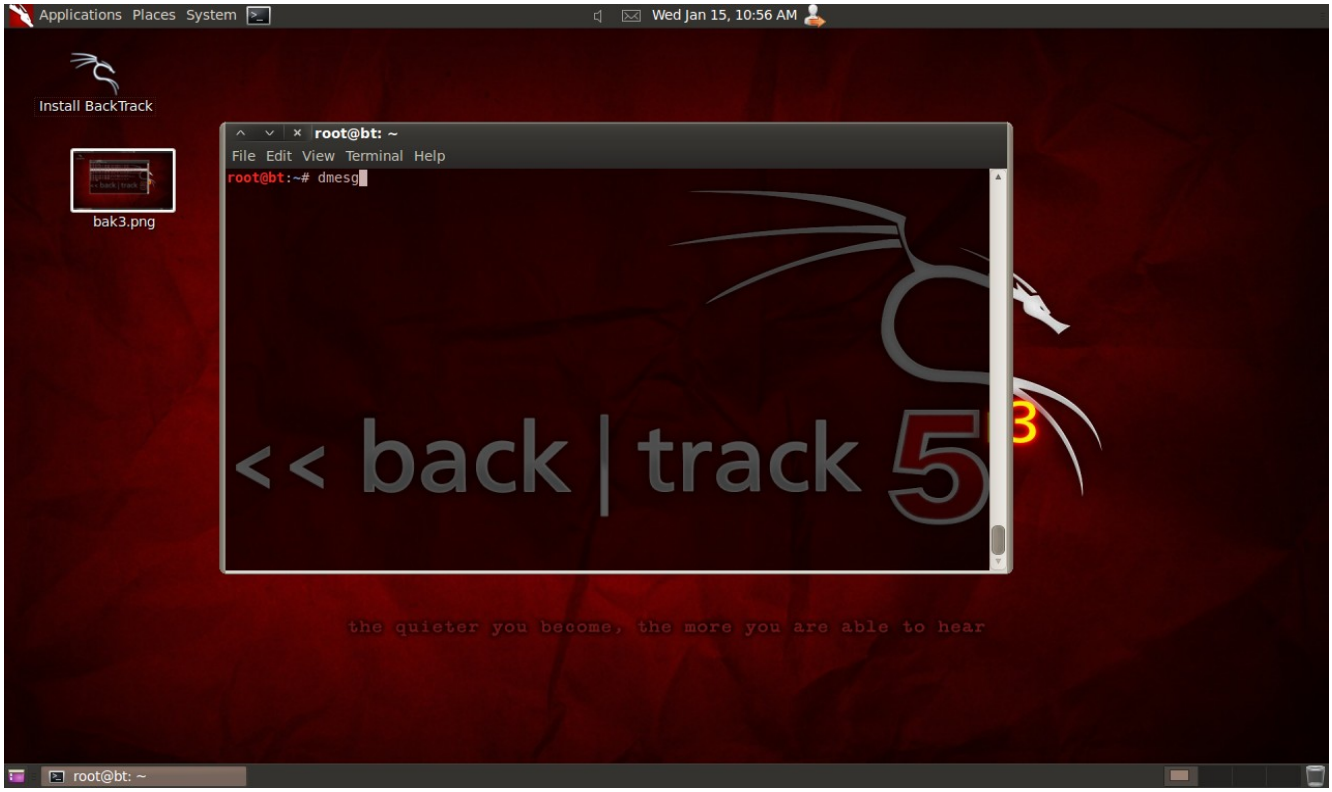
Escribiremos al lado " **startx** " (sin comillas, que sirva para todo el tuto). Le daremos a enter y ahora ya nos sale el sistema operativo Linux Backtrack5.

Adespues tendremos que conectar nuestra sonda a ver si la reconoce el sistema, como le llama y en que directorio la pone. Linux trata los dispositivos como directorios, siempre en la carpeta **"dev".**
Entonces pinchamos en la terminal (como la cmd del ventanas, esta arriba en la izquierda …. el icono cuadrado negro al lado de System).
En nuestra primera terminal pondremos este comando "**lsusb**" y apretamos enter (como en cada comando) .
Estamos pidiendo que nos liste los dispositivos usb conectados

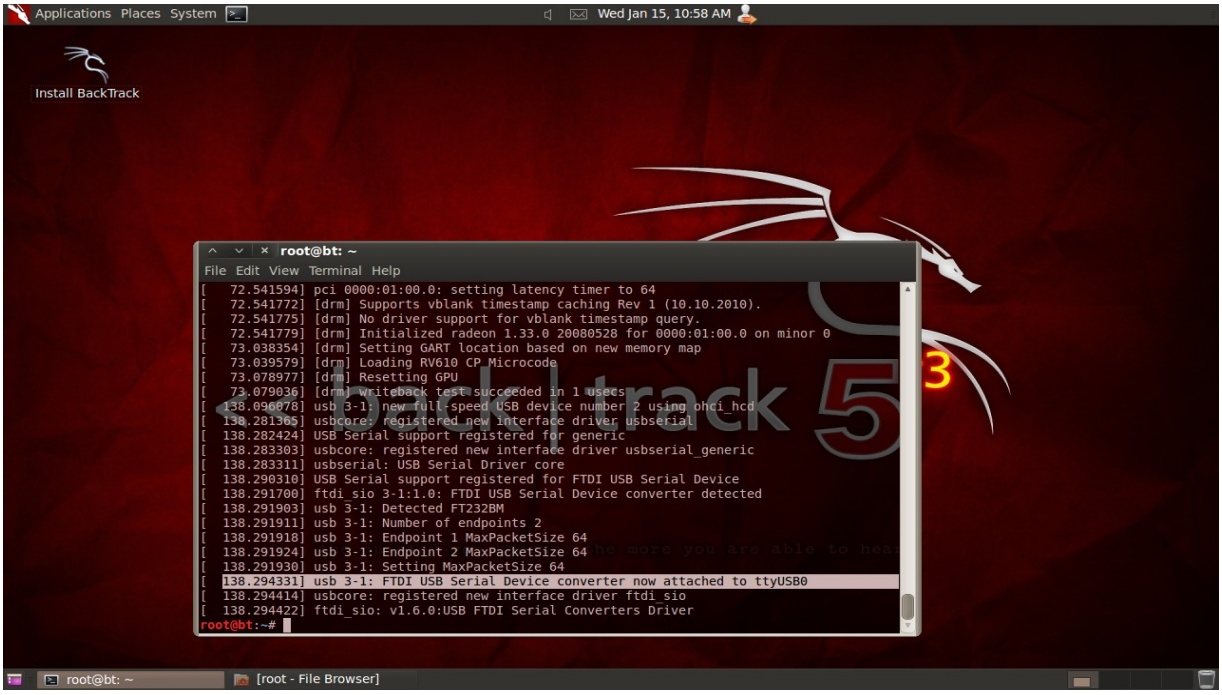
Nos encuentra todos estos ,donde destaco la sonda recién conectada. !!No vamos mal¡¡ la reconoce como Ft 232 usb-serial.



Para saber como la nombra escribiremos en la terminal (o consola) “**dmesg**”. Esto es una orden de que nos de los mensajes del Kernel de Linux. http://es.wikipedia.org/wiki/Dmesg



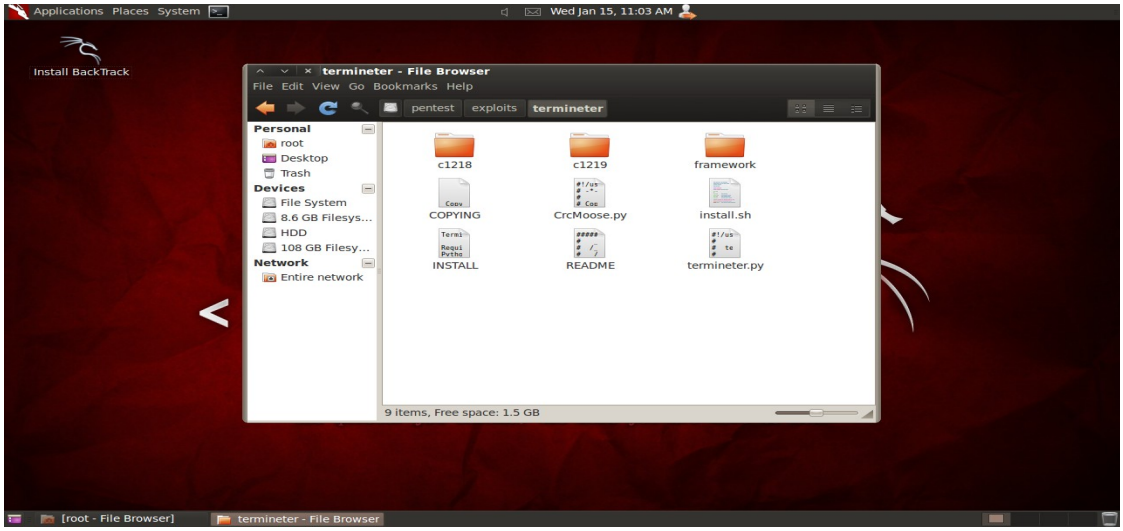
Saldrán un montón de cosas (no asustarse aun)…... fijarse en las ultimas lineas... allí se encuentra nuestra sonda.



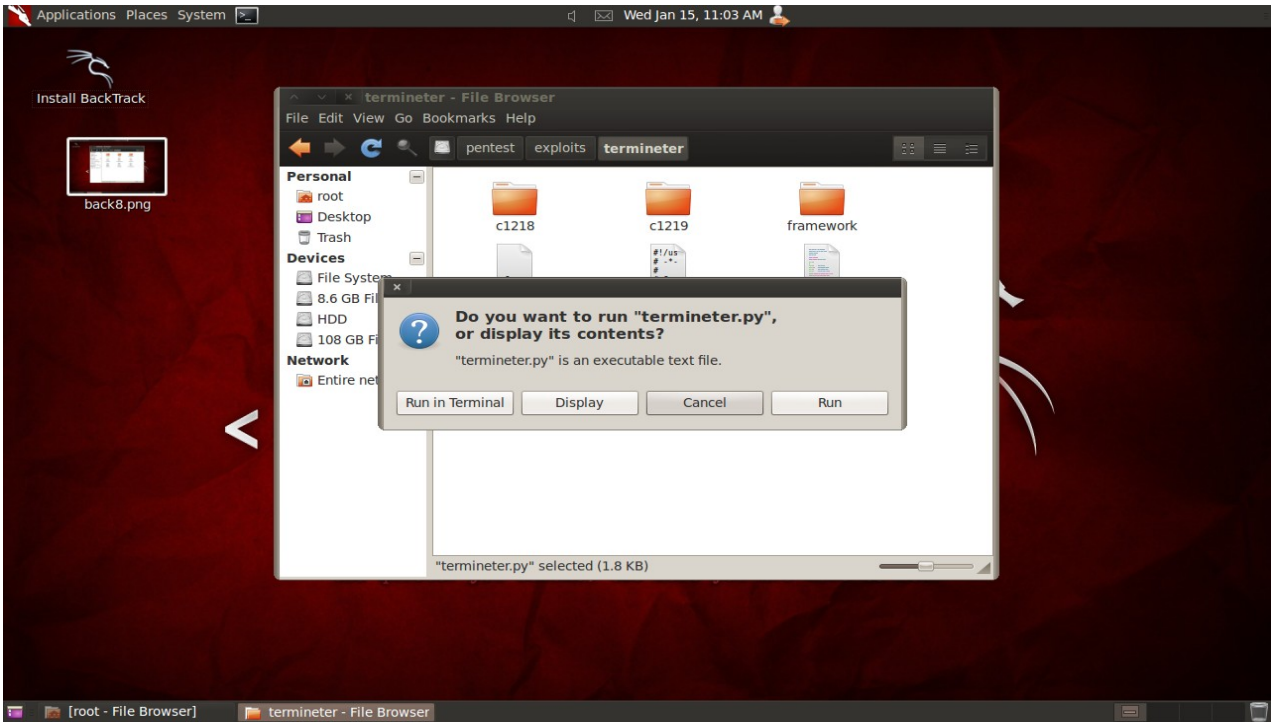
La llama “ **ttyUSB0** ” y por lógica estará en la carpeta **dev** de Filesystem que antes hemos nombrado.

Entonces sabemos que la sonda la llama **ttyUSB0** y su directorio es “ **/dev/ttyUSB0** “
Ahora con esta información ya podemos buscar a nuestro colega TERMINETER

En los sistemas Linux hay varias maneras de entrar a los directorios, intentare hacerlo lo mas ventanas posible.
Arriba a la izquierda nos encontramos en la barra “ **Places** “ pincharemos, saldrá un desplegable y pinchamos en Filesystem, buscaremos entre las carpetas una que ponga **pentest** dentro de esta encontrar otra que ponga **exploit** y como ultima carpeta para ingresar sera er coleguita **Termineter.**



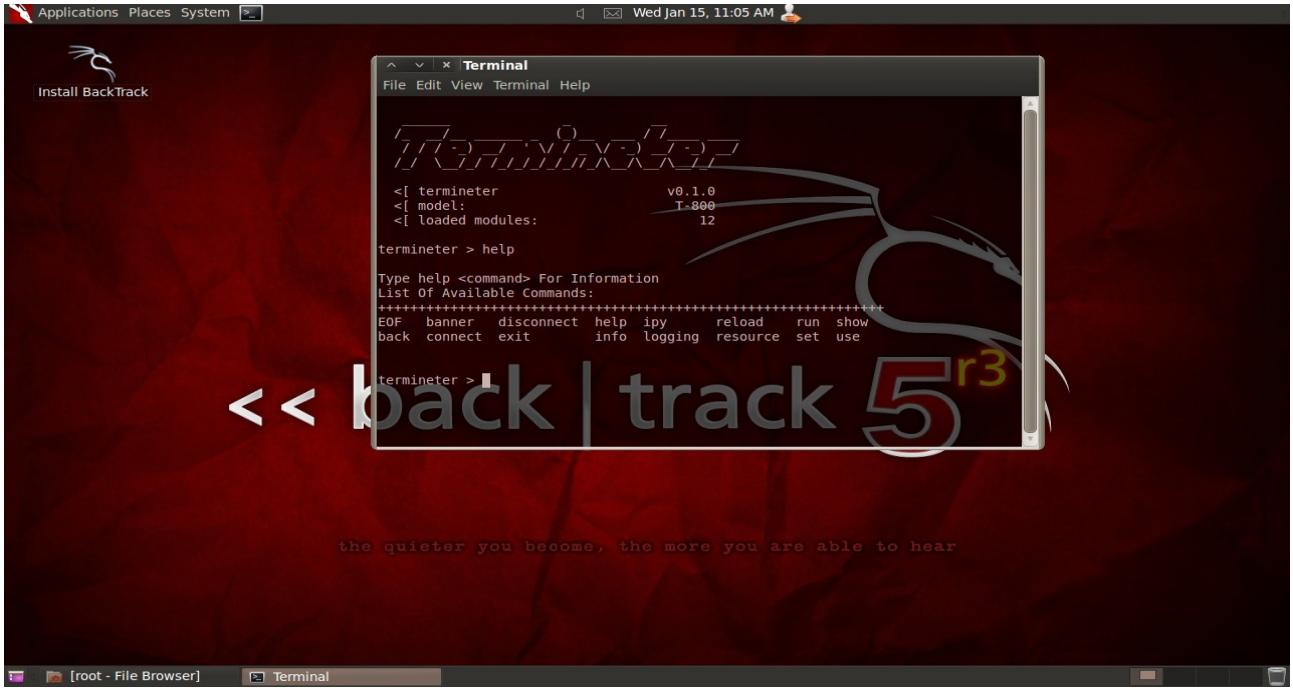
!!Buenooooo¡¡ ya hemos llegado. Aquí vemos un archivo que pone **termineter.py** , este es el que hay que ejecutar, le pinchen ustedes y saldrá esto



Run in terminal es donde tienen que pinchar.....
por fin TERMINETER y su Framework

una vez que tenemos al programa trabajando, veremos primero sus comandos útiles con el comando " **help** " ….. ayuda creo que quiere decir.

Salen todos estos



COMANDOS:
Un comando importante es " **show** " que nos hace un diagnostico de configuración de conexión o de lo que estamos cargando al framework..

" **set** " sera con el que cargaremos parámetros, tipo password, userid,etc.

Con “ **use** “ cargaremos los módulos que incluye termineter.
“ **reload** “ recarga el modulo

“**run**” y “**exploit**” son el mismo y cuando tenemos todo cargado y configurado sera el comando para que empiece la fiesta.

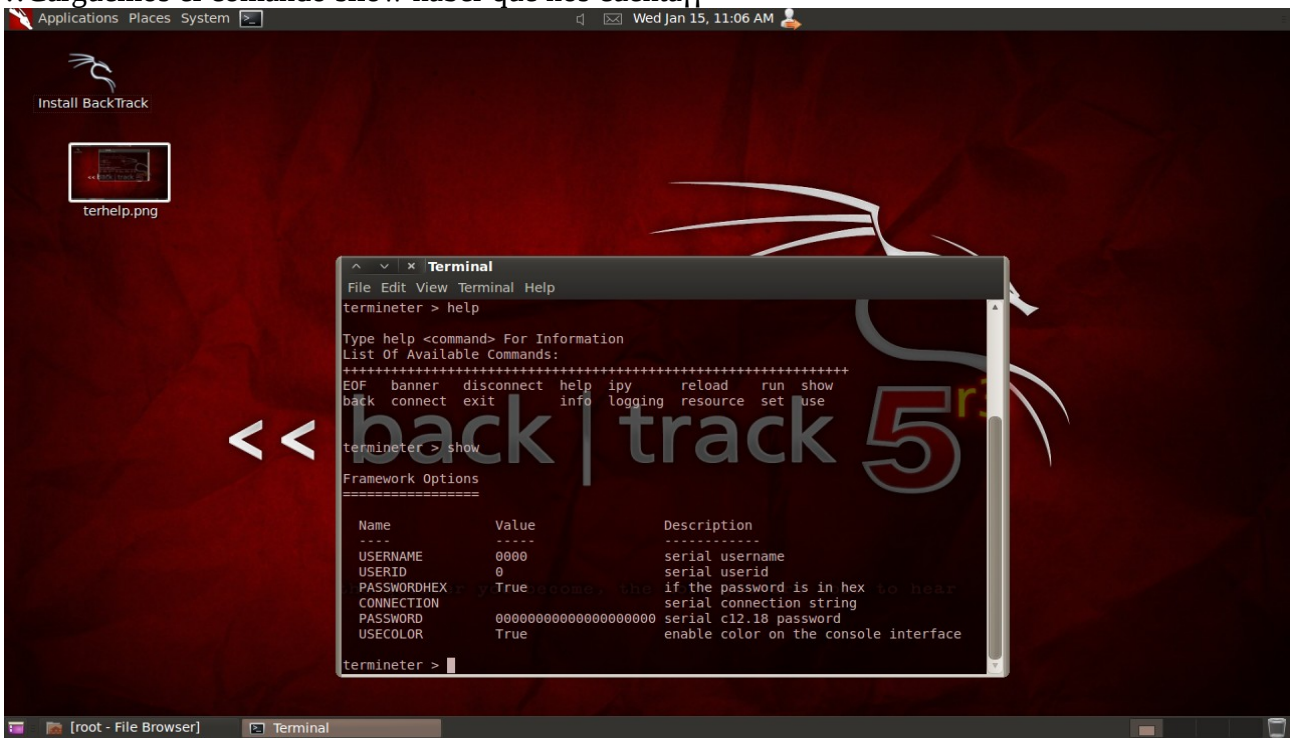
“ **connect** “ …..... este para cuando queramos hacer u obligar una conexión con parámetros fijos ya descubiertos.

“ **disconnect** ”..... pues eso..... disconesta.

“ **exit** “ sales der termineter

Algunos comandos no son importantes y otros no se que son, no los probé.... igual otro año.

!!Carguemos el comando **show** haber que nos cuenta¡¡



Nos da la variable, su valor y la descripcion.

Vemos que tenemos un USERNAME …..... 0000 ….....cambiaremos nombre de contador con
“ **set username paco** ”

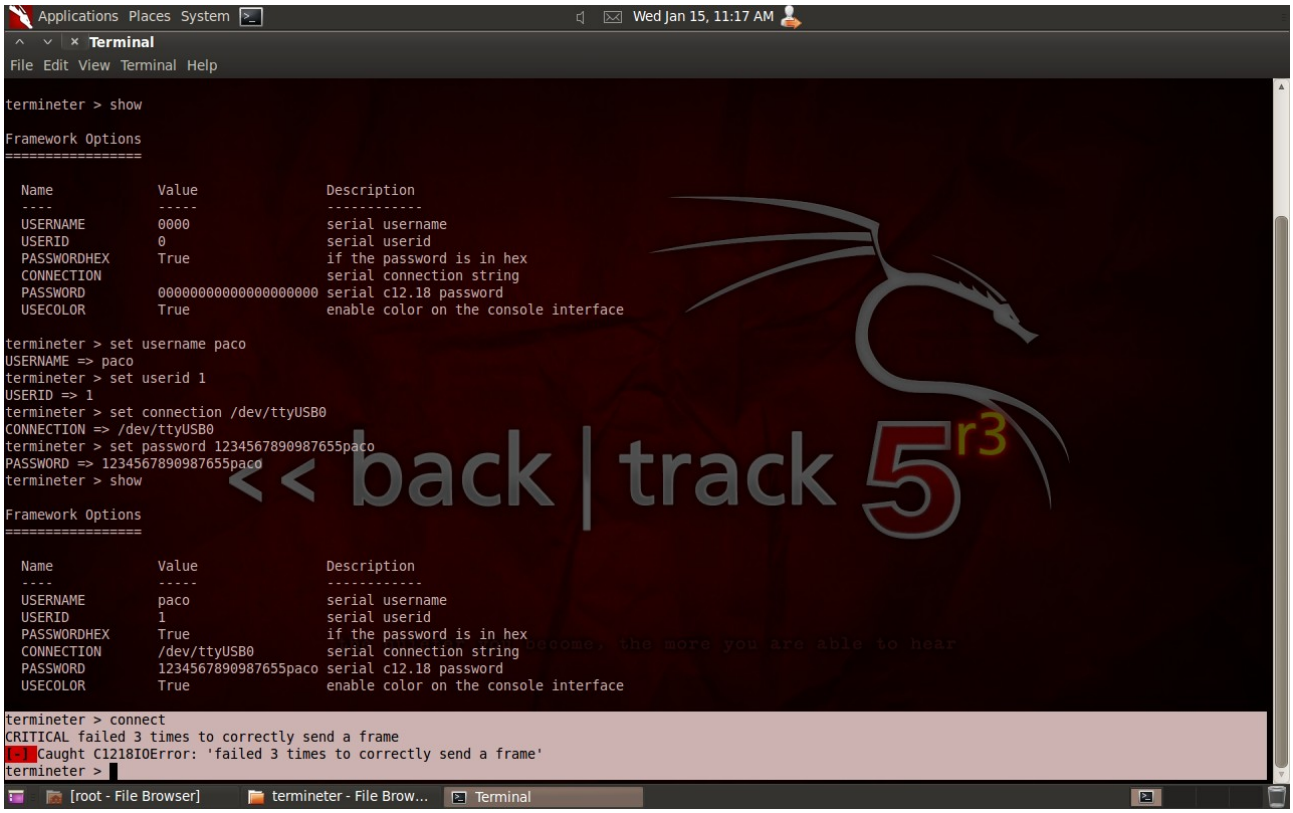
En USERID ….....0 …..... PONDREMOS dirección de ID con
“ **set userid 1** ”

Nos pregunta si la contraseña sera hexadecimal, PASSWORDHEX ….. true o false
“ **set passwordhex false** “

PASSWORD …..... 00000000000000..... igual cambiaremos el pas por 12345676543210tia
“ **set password 12345676543210tia** “

Aki espera una direccion para CONNECTION..... le diremos donde esta la sonda
“ **set connection /dev/ttyUSB0** “

Para crear una conexión entre nuestro sistema y el contador, necesitamos tener las variables anteriores fijadas.
Pongo una afoto de una configuracion completa y el comando **connect** intentando conexión (ya se ...ya se ,..... me da fallo ….puta sonda china la mia, en el siguiente tuto analizaremos el fallo)

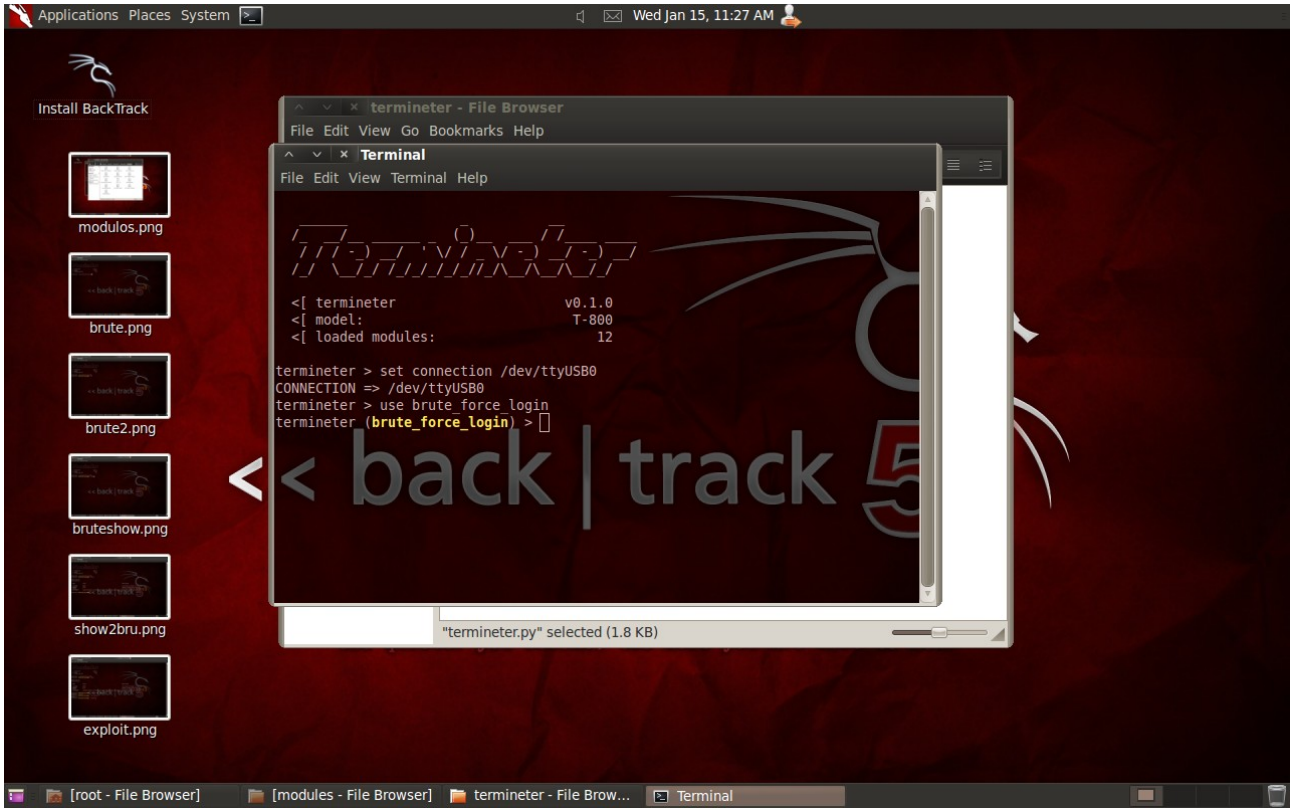


Esto ha sido como crear una conexión sabiendo los parámetros comentados.

Ahora veremos como cargar los módulos y donde se encuentran.
Este framework tiene unos modulos en python que se usan para entrar por fuerza bruta (prueba una a una la lista de password de un fichero), para login, descarga de tablas, subida de tablas y mas que no tuve tiempo de asimilar.
Los encontramos en el directorio filesystem/pentst/exploit/termineter/framework/modules ….. aki los veremos y podremos dejar nuevos modulos diseñados por nosotros para que los encuentre.

Veamos como cargar un modulo..... por ejemplo er Brute_force_login.
Primero la conexión.....
“ **set connection /dev/ttyUSB0** “

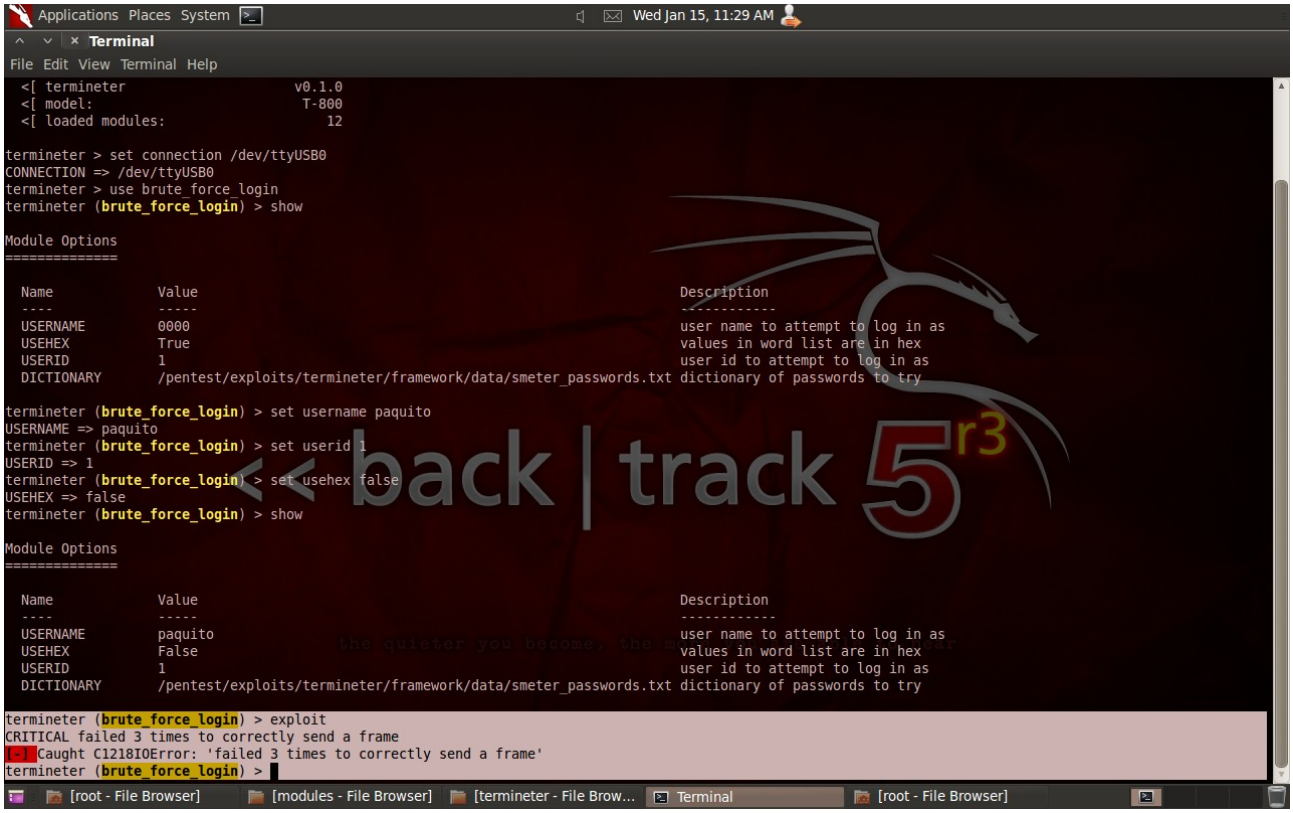
Ahora digámosle que modulo queremos cargar
“ **use brute_force_login** “
Nos cargara el modulo..... lo sabremos por el cambio de color en la terminal



Confifuremos el modulo, primero veamos exploremos **show** haber que variables tenemos

Aki podemos configurar el username,userid, si es hexadecimal y el archivo donde encontarra el diccionario a utilizar por fuerza bruta. (probara una a una todas las contraseñas)
Configurar las variables?.... ya sabemos “**set username**” “**set userid**” “**set usehex**” y el directorio de claves no tocar

Al estar todo configurado simplemente le diremos el comando “ **run** ” o “ **exploit** ”



Nos da un error de tiempo en conexión de protocolo. Normal, es para C12.18 y eso aquí no vale.
!Si no nos sirve¡ ¿Porque seguir con Termineter?
Los protocolos una vez analizados, distan unos de otros claramente, pero tampoco tanto. El Framework al estar en python sus librerías de serial son libres y utilizables, luego nos da un trabajazo precioso por el módico precio de agradecer.
Los módulos solo habría que retocar la parte de la conexión donde cambia el protocolo y el de fuerza bruta nos valdria para probar .
De las tablas hablaremos,,,,,,,, habra que desmontar un cacharro y leer la eeprom, pero primero se tarta de entrar

Ahora links para ojear, estudiar, comprender o limpiarse el orto.
http://www.metersandmore.com/
http://www.meteringsolutions.ziv.es/ziv/aplicaciones-de-software.html
http://www.meteringsolutions.ziv.es/ziv/accesorios.html#4SPLAUSB
http://setserial.sourceforge.net/setserial-man.html#lbAK
http://playground.arduino.cc//Interfacing/LinuxTTY
http://www.lawebdelprogramador.com/foros/Comunicaciones/1048228-Norma_IEC_870-5-102_para_equipos_de_medida_.html

Otro rato sigo. Espero no haberles quitado las ganas de hackear er cacharro del demoño.
Para saber como llevo los cambios o ayudar en este proyecto
gusanoloko@mail.com un saludo y recuerden mineralizarse y supervitaminarse