

RECOLECCIÓN DE INFORMACIÓN (Information Gathering)



Recolección de Información:

“En este módulo se introduce en el tema de las técnicas de recopilación de información a nivel general, las cuales más tarde serán la base para los procesos de Scanning, Análisis de Vulnerabilidades, Explotación y Post Explotación”

“Si yo tuviera 6 horas para cortar un árbol, me pasaría las primeras cuatro afilando mi Hacha”



-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Recolección de Información:

La recolección de información (Information Gathering), también es conocida como **«Reconocimiento»**.

La recopilación de información es una de las etapas más importantes de la auditoria de seguridad del tipo Hacking Ético. Aquí es donde el auditor o atacante reúne información básica acerca del objetivo con el propósito de poder lanzar el ataque o la auditoria más adelante. Hay una ecuación simple que hay que tener en cuenta:

MÁS INFORMACIÓN RECOLECTADA= mayor probabilidad de Éxito en el ataque.



-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Recolección de Información: Objetivos

1. Al final de este módulo, el estudiante debe ser capaz de reunir la información pública de una empresa en especial, mediante diversos recursos, tales como Google, Herramientas On-Line, LA-Foca, Whois, entre otras.
2. Identificar la importancia del proceso de recolección de información, con sus respectivas herramientas y técnicas.
3. Construir un perfil básico de una empresa/organización utilizando información que está disponible de forma pública.



-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Recolección de Información: Definición

“Es la primera y mas importante fase del Hacking Ético. El atacante o auditor de seguridad tratará de recopilar de forma metodológica toda la información que mas pueda al respecto del objetivo”. Dentro de las características del proceso de recolección de información se encuentran



- ✓ **No se realiza ningún tipo de escaneo o contacto con la maquina objetivo.**
- ✓ **Permite Construir un perfil del Objetivo, sin interactuar con él.**
- ✓ **Existen menos herramientas informáticas que en las otras fases.**
- ✓ **Recolección de Información Pública (Ingeniería Social, Hacking con buscadores, OSINT, entre otros)**

-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Recolección de Información: Como ha sido descubierta?

Un aspecto de gran relevancia en el proceso de recolección de información, es registrar en el informe técnico que se le va a entregar al cliente, cual es la forma en que la información fue descubierta. Hay diversas maneras de descubrir información en un proceso de auditoria del tipo Hacking Ético. Algunas de las maneas son:



- ✓ **Información suministrada por el personal de la empresa**
- ✓ **Identificada por búsquedas en google,bing,yahoo**
- ✓ **Por medio de una transferencia de zona DNS**
- ✓ **Por medio de un ping sweep (Seria ya invasivo)**
- ✓ **Por medio de una conexión Inalámbrica vulnerable.**

-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Recolección de Información: Técnicas de Recolección de información

Son muchas las técnicas utilizadas y recursos disponibles para el proceso de recolección de Información. Algunas de ellas son:

- **Herramientas de red: Whois, Traceroute, Ping entre otros.**
- **Información del sitio Web corporativo**
- **Hacking con Buscadores (Google Hacking)**
- **Obtención y Extracción de Metadatos**
- **Automatización con Plug-in Firefox**
- **Scripts públicos**
- **OSINT**
- **Ingeniería Social**



-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Recolección de Información: Técnicas de Recolección de información

Utilizando Herramientas de red: Son muchas las herramientas y protocolos de red disponibles para realizar recolección de información, algunas herramientas combinadas con técnicas de ataque o auditoria, funcionan muy bien. Observemos algunas.

El protocolo **WHOIS**, aunque es un antiguo protocolo, aun sigue suministrando información importante a un atacante o a un auditor Informático. Este protocolo a nivel cliente, esta por defecto y presente en muchos sistemas operativos de uso comun, como Linux por ejemplo.



-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Recolección de Información: Técnicas de Recolección de información

WHOIS (Definición): WHOIS es un protocolo TCP basado en petición/respuesta que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet. Las consultas WHOIS se han realizado tradicionalmente usando una interfaz de línea de comandos, pero actualmente existen multitud de páginas web que permiten realizar estas consultas. Estas páginas siguen dependiendo internamente del protocolo WHOIS para conectar a un servidor WHOIS y hacer las peticiones. Los clientes de línea de comandos siguen siendo muy usados por los administradores de sistemas.

Fuente: <http://es.wikipedia.org/wiki/WHOIS>



-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Recolección de Información: Técnicas de Recolección de información

Ejemplo cliente WHOIS Grafico : En el siguiente ejemplo se utiliza el protocolo whois para hacer una consulta y determinar información de un sitio web. Para el ejemplo se usa el cliente whois del sitio web <http://www.geektools.com/whois.php>



Key: clai

Whois: cinde.org.co

Whois >>

Lo único que nos pide el sitio es digitar el valor de un captcha.

Recolección de Información: Técnicas de Recolección de información

Ejemplo cliente WHOIS no Gráfico: Como se mencionaba anteriormente, muchos sistemas operativos, como Linux por ejemplo, tienen un cliente whois por defecto. Para este segundo ejemplo usaremos la misma consulta realizada en el ejemplo anterior, pero esta vez usamos el cliente whois de Kali Linux, obteniendo resultados similares a los anteriores.

```
root@kali:~# whois -h whois.nic.co cinde.org.co
Domain Name:                CINDE.ORG.CO
Domain ID:                  D597001-CO
Sponsoring Registrar:      .CO INTERNET S.A.S.
Sponsoring Registrar IANA ID: 111111
Registrar URL (registration services): www.cointernet.com.co
Domain Status:              ok
Registrant ID:              21983-REG
Registrant Name:            Centro Internacional de Educacion
                             y Desarrollo Humano
Registrant Organization:    Centro Internacional de Educacion
                             y Desarrollo Humano
Registrant Address1:        CL 77S N 43A 27
Registrant City:            SABANETA
Registrant Postal Code:     00000
Registrant Country:         Colombia
Registrant Country Code:    CO
Registrant Phone Number:    +57.00288127
Registrant Email:           soporte@cinde.org.co
Administrative Contact ID:  21983-REG
Administrative Contact Name: Centro Internacional de Educacion
                             y Desarrollo Humano
Administrative Contact Organization: Centro Internacional de Educacion
                             y Desarrollo Humano
Administrative Contact Address1: CL 77S N 43A 27
```

Recolección de Información: Técnicas de Recolección de información

WHOIS – Otras herramientas en línea: De forma complementaria a los dos ejemplos, hay otros sitios web en los cuales se puede hacer uso del cliente whois. Algunos de los sitios web son:

<http://whois.domaintools.com/>

<http://www.networksolutions.com/whois/index.jsp>

<http://whois.co/>



-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Recolección de Información: Técnicas de Recolección de información

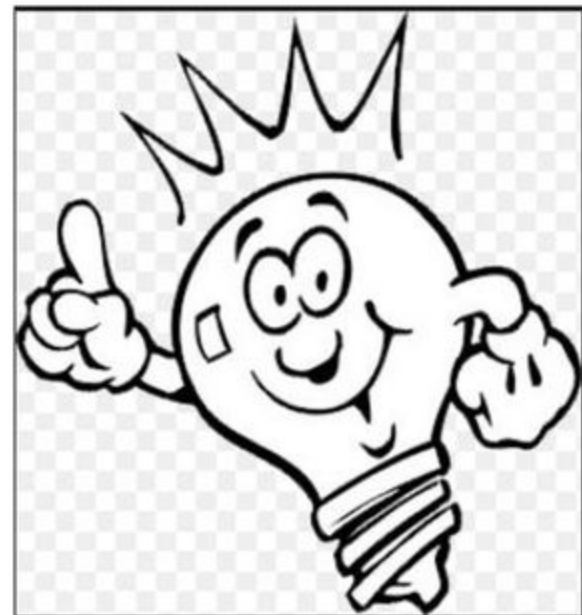
Tips: También se puede realizar una consulta whois utilizando una dirección IP. Para el caso vamos a usar el sitio web <http://lacnic.net/cgi-bin/lacnic/whois?lg=EN> perteneciente a **lacnic**, y buscar información al respecto de una dirección IP administrada por esta entidad.

```
201.232.58.47 SEARCH

* Joint Whois - whois.lacnic.net
* This server accepts single ASN, IPv4 or IPv6 queries
* LACNIC resource: whois.lacnic.net

* Copyright LACNIC lacnic.net
* The data below is provided for information purposes
* and to assist persons in obtaining information about or
* related to AS and IP numbers registrations
* By submitting a whois query, you agree to use this data
* only for lawful purposes.
* 2013-10-12 04:55:15 (BRT -03:00)

inetnum: 201.232.0/17
status: allocated
aut-num: H/A
owner: EPM Telecomunicaciones S.A. E.S.P.
ownerid: CO-EPN01-LACNIC
responsible: Administrador EPN01
address: Carrera 77 39B-16, -, -
```



Recolección de Información: Técnicas de Recolección de información

Ping: Otra comando de red importante y que esta presente en casi todos los sistemas operativos es el Ping (Utilidad de diagnostico de red) . Por ejemplo si queremos saber la dirección IP de un sitio web o host en especial, el comando ping seria de mucha utilidad.

```
PING cinde.org.co (162.212.130.182) 56(84) bytes of data:
64 bytes from 162.212.130.182.static.a2webhosting.com (162.212.130.182): icmp_req=1 ttl=128 time=130 ms
64 bytes from 162.212.130.182.static.a2webhosting.com (162.212.130.182): icmp_req=2 ttl=128 time=133 ms
64 bytes from 162.212.130.182.static.a2webhosting.com (162.212.130.182): icmp_req=3 ttl=128 time=253 ms
64 bytes from 162.212.130.182.static.a2webhosting.com (162.212.130.182): icmp_req=4 ttl=128 time=131 ms
64 bytes from 162.212.130.182.static.a2webhosting.com (162.212.130.182): icmp_req=5 ttl=128 time=128 ms
64 bytes from 162.212.130.182.static.a2webhosting.com (162.212.130.182): icmp_req=6 ttl=128 time=157 ms
^C
--- cinde.org.co ping statistics ---
7 packets transmitted, 6 received, 14% packet loss, time 6012ms
rtt min/avg/max/mdev = 128.476/155.854/253.605/44.825 ms
root@kali:~#
```

```
C:\Users\teletran1>ping www.cinde.org.co

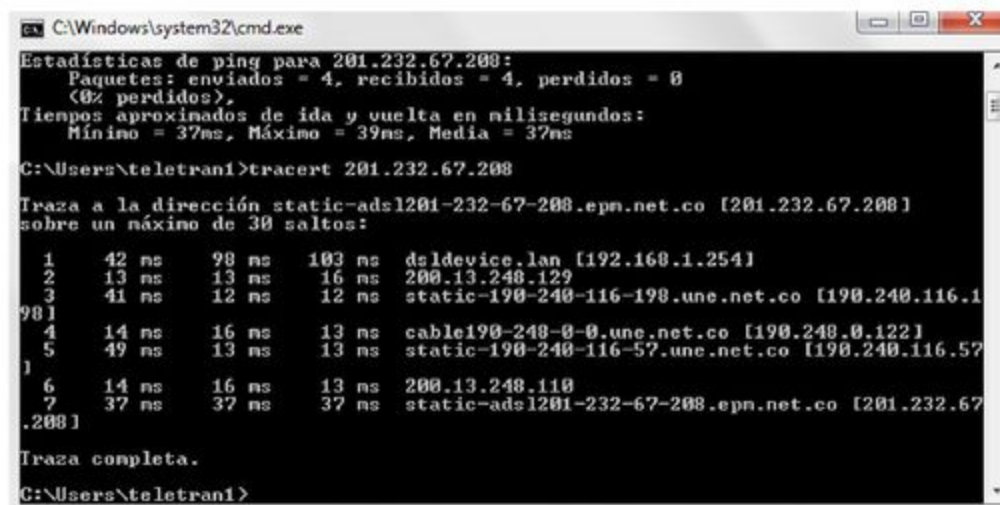
Haciendo ping a www.cinde.org.co [162.212.130.182] con 32 bytes de datos:
Respuesta desde 162.212.130.182: bytes=32 tiempo=110ms TTL=47
Respuesta desde 162.212.130.182: bytes=32 tiempo=109ms TTL=48
Respuesta desde 162.212.130.182: bytes=32 tiempo=108ms TTL=48
Respuesta desde 162.212.130.182: bytes=32 tiempo=109ms TTL=47

Estadísticas de ping para 162.212.130.182:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 108ms, Máximo = 110ms, Media = 109ms

C:\Users\teletran1>
```

Recolección de Información: Técnicas de Recolección de información

Tracert: Otra utilidad importante en el proceso de recolección de información es el comando o herramienta de diagnostico **tracert**, el cual permite realizar un proceso de trazado de paquetes y ruta entre un host origen y un host destino, con lo cual el atacante o auditor informático puede obtener información relevante al respecto de la víctima o empresa que se esta auditando. La herramienta es llamada **tracert** en sistemas operativos Windows, y **traceroute** en sistemas operativos GNU/Linux



```
C:\Windows\system32\cmd.exe
Estadísticas de ping para 201.232.67.208:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    <0% perdidos>,
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 37ms, Máximo = 39ms, Media = 37ms

C:\Users\teletran1>tracert 201.232.67.208

Trazo a la dirección static-ads1201-232-67-208.epn.net.co [201.232.67.208]
sobre un máximo de 30 saltos:

  1  42 ns   98 ns  103 ns  dsldevice.lan [192.168.1.254]
  2  13 ns   13 ns   16 ns  200.13.248.129
  3  41 ns   12 ns   12 ns  static-190-240-116-190.une.net.co [190.240.116.190]
  4  14 ns   16 ns   13 ns  cable190-240-0-0.une.net.co [190.240.0.122]
  5  49 ns   13 ns   13 ns  static-190-240-116-57.une.net.co [190.240.116.57]
  6  14 ns   16 ns   13 ns  200.13.248.110
  7  37 ns   37 ns   37 ns  static-ads1201-232-67-208.epn.net.co [201.232.67.208]

Trazo completa.

C:\Users\teletran1>
```

Recolección de Información: Técnicas de Recolección de información

Ejemplo uso del comando tracert : En el siguiente ejemplo se utiliza el comando tracer, no desde el punto de vista de un administrador de red, sino del punto de vista de un auditor o atacante informático, con el propósito de identificar mas host y/o equipos informáticos que vulnerar.

```
C:\Users\teletran1>tracert 201.232.67.208

Traza a la dirección static-adsl201-232-67-208.epm.net.co [201.232.67.208]
sobre un máximo de 30 saltos:

  1    42 ms    98 ms    103 ms    dsldevice.lan [192.168.1.254]
  2    13 ms    13 ms    16 ms    200.13.248.129
  3    41 ms    12 ms    12 ms    static-190-240-116-198.une.net.co [190.240.116.1
98]
  4    14 ms    16 ms    13 ms    cable190-248-0-0.une.net.co [190.248.0.122]
  5    49 ms    13 ms    13 ms    static-190-240-116-57.une.net.co [190.240.116.57
]
  6    14 ms    16 ms    13 ms    200.13.248.110
  7    37 ms    37 ms    37 ms    static-adsl201-232-67-208.epm.net.co [201.232.67
.208]

Traza completa.
C:\Users\teletran1>
```

En el resultado del ejemplo se puede identificar los host por los cuales pasa un paquete de red entre el origen (auditor-atacante) y el destino (victima).

Recolección de Información: *Técnicas de Recolección de información*

Geo-Localización de la IP: Con el propósito de tener en cuenta las normas y criterios legales de cada país , en lo que respecta a seguridad y delitos informáticos, es de gran importancia para el auditor o atacante Informático poder determinar la Geo-localización de la dirección IP de la víctima o target de evaluación. Para el caso del ejemplo anterior, se logro identificar que la dirección IP del sitio web www.cinde.org.co es **162.212.130.182**. Para identificar la Geo-localización de la dirección IP en mención, podemos ayudarnos con el siguiente sitio web:

<http://cqcouter.com/whois/>

162.212.130.182 - Geo Information	
IP Address	162.212.130.182 ←
Host	162.212.130.182.static.a2webhosting.com
Location	🇺🇸 US, United States ←
City	-, - -

Recolección de Información: Técnicas de Recolección de información

Haciendo consultas DNS: Las consultas a los servidores DNS, son también una técnica que le permite a un atacante o auditor Informático realizar procesos de recolección de información. **nslookup** es un comando y/o una herramienta DNS que permite realizar diversas operaciones, entre las cuales esta hacer consultas DNS. **nslookup** viene por defecto en muchos sistemas operativos tales como Linux y Windows.

nslookup

```
root@kali:~# nslookup cinde.org.co
Server:      192.168.153.2
Address:     192.168.153.2#53

Non-authoritative answer:
Name:   cinde.org.co
Address: 162.212.130.182

root@kali:~#
```

Certified Offensive and Defensive Security Professional

- Entrenamiento E-learning -

Ejemplo usando nslookup: En el siguiente ejemplo realizaremos una consulta usando la herramienta nslookup, con el objetivo de poder identificar el registro MX correspondiente al sitio web <http://www.cccauca.org.co/> con el propósito de identificar servidores de correo asociados a este dominio.

```
root@bt:~# nslookup
> set type=mx
> cccauca.org.co
Server:          192.168.153.2
Address:         192.168.153.2#53

Non-authoritative answer:
cccauca.org.co  mail exchanger = 1 intraccc.cccauca.org.co.

Authoritative answers can be found from:
cccauca.org.co  nameserver = intraccc.cccauca.org.co.
intraccc.cccauca.org.co internet address = 190.25.237.18
>
```

Recolección de Información: Técnicas de Recolección de información

Ejemplo usando nslookup: Luego hacemos un telnet a los puertos 25 y 110 respectivos a los protocolos de correo SMTP y POP3, y obtenemos los siguientes resultados.

```
root@bt:~# telnet 190.25.237.18 25
Trying 190.25.237.18...
Connected to 190.25.237.18.
Escape character is '^]'.
220 intraccc.cccauca.org.co ESMTP Sendmail 8.13.8/8.13.8; Sat, 12 Oct 2013 03:27:09 -0500
```

```
root@bt:~# telnet 190.25.237.18 110
Trying 190.25.237.18...
Connected to 190.25.237.18.
Escape character is '^]'.
+OK Dovecot ready.
```

Recolección de Información:

Recolección de información disponible en la Web: Otras de las practicas que se debe de hacer antes de un ataque o auditoria informática, es pasar un tiempo navegando en la web y buscar información de fondo sobre la organización que se quiere evaluar o atacar. Por lo general se visita el sitio web de la organización que se esta analizando, y se busca información como: **Contactos, números de teléfono y fax, correos electrónicos gratuitos, corporativos, entre otros.**



-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Hacking Ético –Fases de Análisis de Seguridad.

1. RECONOCIMIENTO PASIVO: Técnicas de Recolección de Información

“Google Hacking” Google ha demostrado ser uno de los motores de búsqueda mas poderosos y efectivos. Pero por su gran poder, puede, causar la exposición de información sensible en un sitio web específico.

**Google
Hacking**

Google Hacking se introdujo por primera vez por **"Johnny Long"**, que desde entonces ha publicado un par de libros sobre el tema



-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Hacking Ético –Fases de Análisis de Seguridad.

1. RECONOCIMIENTO PASIVO: Técnicas de Recolección de Información

“Google Hacking” se hace mas efectivo, usando los operadores de búsquedas avanzadas de Google. Algunos operadores de búsqueda avanzada son: **site**, **inurl**, **filetype**



<http://www.exploit-db.com/google-dorks/>



-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Hacking Ético –Fases de Análisis de Seguridad.

1. RECONOCIMIENTO PASIVO: Técnicas de Recolección de Información

Algunos ejemplos de búsqueda básica, usando la técnica de “**Google Hacking**”:

SITE, FILETYPE, INURL

intitle:"Remote Desktop Web Connection" inurl:tsweb

<http://www.sahw.com/wp/archivos/2006/03/08/google-hacking-ejemplos-y-medidas-para-evitar-sus-efectos/>

http://www.googleguide.com/advanced_operators.html



-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Recolección de Información: Técnicas de Recolección de información

Ejemplo usando Google hacking: la técnica de recolección de información de Google hacking es muy extensa, ya que tiene cientos de ejemplos. Para la demostración de esta técnica, vamos a tomar como ejemplo la búsqueda planteada en la siguiente URL:

<http://www.exploit-db.com/ghdb/3886/>



La anterior búsqueda encontrara directorios compartidos en servidores, con documentos (Archivos) que en ocasiones suelen ser privados (Confidenciales) y de carácter empresarial, los cuales en muchas ocasiones son compartidos y publicados, pero el usuario no se percata, o no es consciente de ello.

Recolección de Información: Técnicas de Recolección de información

Ejemplo usando Google hacking: Y si cambiamos el criterio de búsqueda aplicando la palabra myshare por la palabra en español compartir. Entonces la búsqueda en google quedaría así:

intitle:"index of" compartida

Observando los siguientes resultados:



Recolección de Información: Técnicas de Recolección de información

Ejemplo usando Google hacking: mas resultados.....

Index of /Compartida

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
	Parent Directory		-	
	â€œCUENTO PARA CONEJ..>	08-Oct-2013 14:13	4.1M	
	A40BA533.tmp	10-Oct-2013 09:46	0	
	ARMO LA CARTA.pptx	25-Sep-2013 14:50	68K	
	America-latina-satel..>	07-Aug-2013 08:45	204K	
	DIEGO.docx	10-Oct-2013 09:40	11K	
	DIEGO F..docx	10-Oct-2013 09:39	11K	
	DIEGO ORTIZZZZZZZZZ..>	10-Oct-2013 09:41	12K	
	Emanuel.G.docx	10-Oct-2013 09:42	12K	
	GeoGebra-Windows-Ins..>	24-Apr-2012 14:40	11M	
	Hace unos dÃas.docx	10-Oct-2013 10:45	710K	
	-	-	-	-

Recolección de Información: Técnicas de Recolección de información

Ejemplo usando Google hacking: Y cambiando el criterio de búsqueda por el siguiente: **intitle:"index of" privado**

Los resultados serian mas interesantes??????????

Index of /privado/Docuementos/SESIONES CLÍNICAS

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 Avances CMF Oviedo.Dr. Colado.pdf	06-Mar-2013 10:27	35M	
 Ciclo celular.Dr. Jonte.ppt	06-Mar-2013 10:26	444K	
 Enfermedad e Von Willebrand.Dr.Vanegas.ppt	06-Mar-2013 10:27	72M	
 Fiebre persistente en receptor TMO.ppt	06-Mar-2013 10:27	1.9M	
 GammopatiasMonoclonales.Dr.Taboada.ppt	06-Mar-2013 10:27	2.7M	
 Plasma fresco congelado.Dra.Fernández.ppt	06-Mar-2013 10:27	1.0M	
 Policitemia vera.Dra. Vázquez.ppt	06-Mar-2013 10:27	12M	
 Punción medular.Dr.Palicio.ppt	06-Mar-2013 10:28	32M	
 Thumbs.db	06-Mar-2013 10:27	35K	
 Trombocitopenia.Dr.Vanegas.ppt	06-Mar-2013 10:27	757K	

Hacking Ético –Fases de Análisis de Seguridad.

RECONOCIMIENTO PASIVO: Metadatos

Otra de las técnicas útiles para el proceso de recolección de información, son los METADATOS que están contenidos en archivos de Office, PDF, entre otros.

Los Metadatos pueden definirse como unos datos que describen a otros datos. Por ejemplo en las propiedades de un documento de Office, se puede encuentra información clasificada como Metadatos.

Algunos ejemplos de Metadatos son:

- Creador del Documento
- Nombre del equipo donde se creo
- Sistema Operativo
- Una nombre de una impresora.
- Una Ruta (Path)



Hacking Ético –Fases de Análisis de Seguridad.

RECONOCIMIENTO PASIVO: Metadatos

Existen muchas herramientas para la extracción de los METADATOS, la FOCA es una de ellas. Es una herramienta para el S.O Windows, y es un software iniciado por el consultor de seguridad Español **“Chema Alonso”**.

La herramienta se puede descargar desde la siguiente dirección:

<https://www.elevenpaths.com/es/labs-herramientas-foca.html>

Además tiene una versión online.

<http://www.informatica64.com/foca/>



Recolección de Información: Herramientas para la Extracción de Metadatos

ExifTool Otra interesante herramienta para la extracción de metadatos es ExifTool. Esta poderosa herramienta permite escribir, leer y cambiar metadatos. Entre algunas de las características de esta herramienta se encuentran:

- ✓ Puede ejecutarse en Windows, Linux y Mac OS
- ✓ Soporta más de 100 formatos de archivos para extraer los metadatos
- ✓ Inicialmente esta herramienta solo analizaba archivos de imagen y audio
- ✓ Soporta el análisis de archivos del tipo, pdf, doc, docx, xls, xlsx, entre otros
- ✓ Procesa archivos de varias cámaras digitales
- ✓ Procesa Geotags y Georeferencias

ExifTool by Phil Harvey

<http://www.sno.phy.queensu.ca/~phil/exiftool>

Recolección de Información: Técnicas de Recolección de información

Ejemplo usando la herramienta ExifTool : Para este ejemplo vamos a usar la herramienta ExifTool, la cual viene por defecto instalada en kali Linux:

```
root@kali:~# exiftool metadataimagen.JPG
ExifTool Version Number      : 8.60
File Name                    : metadataimagen.JPG
Directory                    : .
File Size                    : 1954 kB
File Modification Date/Time   : 2014:05:17 00:47:15-04:00
File Permissions              : rwxr--r--
File Type                    : JPEG
MIME Type                    : image/jpeg
Exif Byte Order               : Little-endian (Intel, II)
Make                         : SAMSUNG
Camera Model Name             : SAMSUNG PL120,PL121 / VLUU PL120,PL121
Orientation                   : Horizontal (normal)
X Resolution                  : 96
Y Resolution                  : 96
Resolution Unit               : inches
Software                      : 1108304
Modify Date                   : 2013:03:21 17:03:35
Y Cb Cr Positioning           : Co-sited
Copyright                     : COPYRIGHT, 2011
```

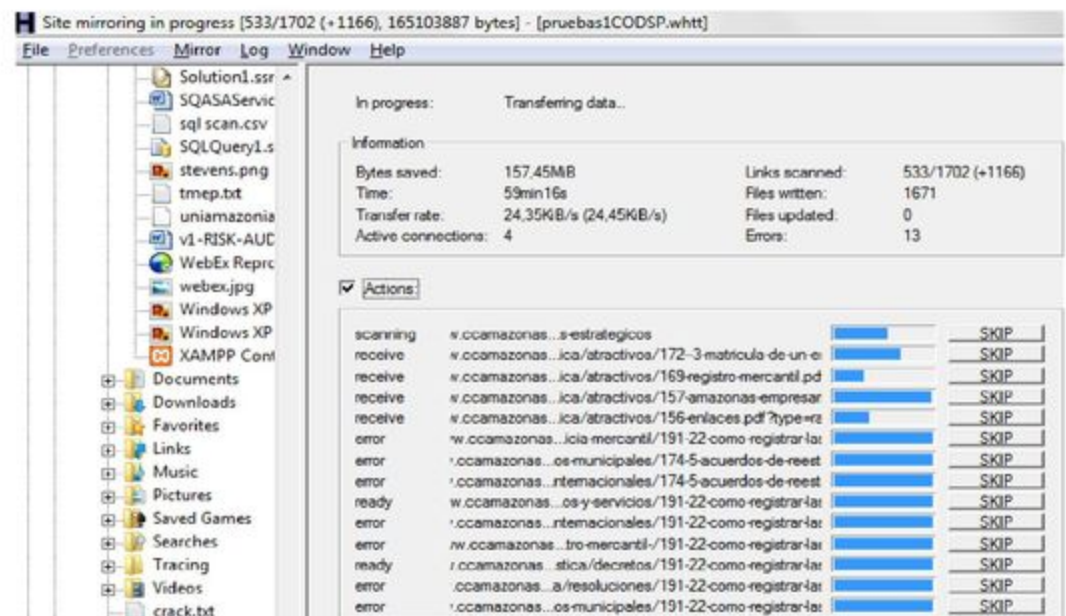
Recolección de Información: Técnicas de Recolección de información

Ejemplo formas de Obtener archivos para analizar los Metadatos:

- ✓ Ejemplo desde Linux usando la herramienta wget

```
wget -nd -r -A pdf,doc,xls -P /root/metadatosweb/pdf cepre.uni.edu.pe/pdf
```

- ✓ Ejemplo usando HTTrack



Hacking Ético –Fases de Análisis de Seguridad.

RECONOCIMIENTO PASIVO: Addon Firefox PassiveRecon

Otra importante herramienta en el proceso de recolección de información, es un Plug-in de Firefox llamado **PassiveRecon**: Este Plug-in permite a los analista de seguridad realizar procesos de recolección de información que esta disponible al publico, en lo que respecta aun host (Sitio Web) especifico.

Con tan solo visitar el sitio del cual se desea recolectar información, y darle clic derecho, el Plug-in comienza el proceso de recolección de información total, o parcial, según las indicaciones que se le al Plug-in



<https://addons.mozilla.org/en-us/firefox/addon/passiverecon/>

Hacking Ético –Fases de Análisis de Seguridad.

RECONOCIMIENTO PASIVO: Otros recursos “OSINT”

Los datos de fuentes abiertas y publicas o lo que comúnmente se conoce como “Open sources for intelligence”, también es un buen recurso para la recolección de información.



http://en.wikipedia.org/wiki/Open_source_intelligence#OSINT_communities

Hacking Ético –Fases de Análisis de Seguridad.

RECONOCIMIENTO PASIVO: Netcraft

Netcraft es una compañía de monitoreo de Internet con sede en Bradford-on-Avon, Inglaterra. Sus servicios más destacados son el seguimiento tiempos de funcionamiento y modo operativo de servidor del sistema de detección. Netcraft se puede utilizar para encontrar indirectamente información sobre los servidores web en Internet, incluyendo el sistema operativo subyacente, la versión del servidor web, gráficos de tiempo de actividad, entre otros.

OS, Web Server and Hosting History for www.unisabaneta.edu.co

<http://www.unisabaneta.edu.co> was running Apache on Linux when last queried at 12-Aug-2011 17:16:44 GMT - [refresh now](#) [Site Report](#)

[FAQ](#)

[Try out the Netcraft Toolbar!](#)

OS	Server	Last changed	IP address	Netblock Owner
Linux	Apache	12-Aug-2011	66.235.180.14	HopOne Internet Corporation

Hacking Ético –Fases de Análisis de Seguridad.

RECONOCIMIENTO PASIVO: Otros recursos “SHODAN”

Esta herramienta nos sirve para identificar dispositivos que están expuestos en Internet. Para usar esta herramienta se requiere de un registro.



<http://www.shodanhq.com/>

Create an Account

Username

Email

Password

Confirm password

By clicking on the button below, you agree to the [Terms of Use](#) and the [Privacy Policy](#).

I accept. Create my Account.

Hacking Ético –Fases de Análisis de Seguridad.

RECONOCIMIENTO PASIVO: “Ingeniería Social”



La Ingeniería Social se define como el proceso mediante el cual tratamos de engañar a una persona o grupo de personas, para que nos suministren información que necesitamos saber.

http://www.social-engineer.org/framework/Social_Engineering_Framework