

2. Pasos de un Ataque a la Ciberseguridad

1. Footprinting y Reconnaissance

1.1 Introducción

Aunque el número de fases en un ataque a la seguridad informática y su nombre depende de la documentación consultada y está estandarizado, podemos definir a groso modo las siguientes etapas:

1. Reconocimiento
 - a. Activo/pasivo
2. Escaneo
3. Obtener acceso
 - a. Nivel de S.O./ Nivel de aplicación
 - b. Nivel de red
 - c. DoS
4. Mantener acceso
 - a. Subir/alterar/descargar programas o datos
5. Cubrir pistas

En este punto del curso vamos a centrarnos en la fase inicial de Reconocimiento.

1.2 Reconocimiento

El reconocimiento se refiere a la fase preparatoria en la que el atacante recopila tanta información (Information Gathering) como sea posible sobre un objetivo de evaluación antes de lanzar un ataque.

Se denomina information gathering a la instancia previa al intento de ejecutar una intrusión informática a un sistema por parte de alguien no autorizado. También es empleada (generalmente en organizaciones) por los profesionales éticos en caso de llevar a cabo una comprobación de seguridad. Information gathering implica llevar a cabo la tarea previa y minuciosa de inteligencia (similar a un reconocimiento del terreno), más precisamente a la recolección de datos acerca del objetivo o de algún componente relacionado a este o a parte de él. Esta fase se compone, fundamentalmente, de investigación y análisis de datos recabados.

El sistema de información cuenta con incontables piezas y, por lo tanto, el factor permeable (brecha o agujero de seguridad) inicial de éste podría encontrarse en cualquiera de los niveles, comprendidos entre un fallo humano, uno de infraestructura (técnica), lógica y hasta externa por los agentes involucrados (por ejemplo, un proveedor de Internet o hosting inseguro o una sucursal con su red desprotegida) o distintos ambientes interconectados.

Los datos que buscan los intrusos antes de atacar pueden estar relacionados con algún empleado, ya sea ejecutivo u operario, con algún sistema o tramo de él o con algún procedimiento u operación que nos permita intervenir en él. También puede ser una dirección IP, un sitio, una red, una aplicación, un servicio (puerto abierto de autenticación o no), un protocolo, un determinado descuido de programación o de administración, un directorio, un documento, una plataforma o bien cualquier dato de ubicación física o denominación de algún sector de la misma organización.

Por supuesto, si puede directamente conseguir logins, lo intentará. No interesa si el dato es muy importante o casi insignificante. Todo es útil a la hora de la escalada en el sistema y la previa planificación de este embate (chequeo o simulación de ataque). Algunas de las preguntas útiles antes de proceder serían:

- ¿Qué sabemos de nuestro objetivo?
- ¿Dónde están sus redes, sitios o por dónde fluye su información?
- ¿Qué partes lo conforman?
- ¿Qué sistemas poseen y cómo están formados?
- ¿Cómo se llaman los integrantes de la organización?
- ¿Quiénes son sus empleados y qué hacen? ¿Cómo y dónde?
- ¿Qué información sobre ellos se puede consultar o conseguir en Internet?

Aquí tenemos una lista de alguna información crítica que debería obtenerse durante esta fase de reconocimiento:

Información de Red	<ul style="list-style-type: none">• Direcciones IP• Máscara de subred• Topología de Red• Nombres de dominio
Información de Host	<ul style="list-style-type: none">• Nombres de usuario• Nombres de grupos• Tipo de arquitectura (x86, SPARC,...)• Familia y versión de sistema operativo• Servicios TCP y UDP que se están ejecutando
Políticas de Seguridad	<ul style="list-style-type: none">• Requisitos de complejidad de contraseñas• Frecuencia de cambio de contraseñas• Retención de cuentas caducadas/deshabilitadas• Seguridad física• Cortafuegos• Sistemas de Detección de Intrusos
Información Personal	<ul style="list-style-type: none">• Dirección postal• Número de teléfono• Conocimientos en informática• Secretos “oscuros”

Comúnmente, se denomina footprinting a esta recolección de información previa. De todos modos, cada atacante o consultor tiene sus propios métodos y recursos durante esta búsqueda. Cuanto más minuciosa e ingeniosa sea, más posibilidades tendrá de dar con un descuido, un objetivo o por lo menos, una pista para comenzar con otra etapa del ataque. Por ejemplo, un atacante real que posee en su haber algunas o la mayoría de las bases de datos de ISP (proveedores de Internet) del país, o tiene acceso a ellas, cuenta con una clara ventaja sobre el resto ya que, en éstas, posiblemente habrá mucha información útil relacionada con personas de la organización que pueden tener algún dato importante, como passwords, o permiten con seguirlo.

La recolección de datos previos al ataque generalmente comienza en algún tipo de base de datos y otros recursos que se dispongan. Después de cotejar las coincidencias de personas (existencia tanto en la base de datos como en la organización), tomará los datos personales y tratará de emplear como password sus fechas de nacimiento, sus números de documento de identidad, sus oficios o las mismas contraseñas allí utilizadas, pero esta vez en las cuentas de correo de la organización u otro servicio que requiera autenticación (ssh, ftp, telnet, ...)

Veamos algunos ejemplos. Si en su cuenta personal la víctima tiene una pregunta secreta relacionada con un libro (supongamos El principito) o encuentra en un foro que a esa persona le interesa ese libro, el intruso probará claves como las siguientes: elprincipito, zorro, invisiblealosojos, víbora, antoine, exupery, baobab, asteroide3251, b612, rosa, etcétera.

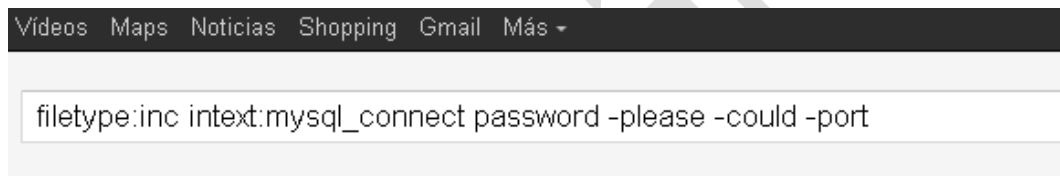
Incluso los datos personales (como nombre y apellido) servirán para deducir los usuarios de login y no solo la clave. El típico ejemplo es el UserID (el usuario que antecede al signo @) de las actuales cuentas de e-mail corporativas e institucionales, formadas por la primera letra del

primer nombre, seguido del apellido. Por ejemplo, aperez@dominiovictima.com. Información como ésta le servirá al intruso para sacar más información aún, quizá desde otros lugares. Esta persona, además, buscará en bases ilegales, como la de tarjetas de crédito, padrones de todo tipo (disponibles hasta en redes P2P), entidades privadas o bajadas de servidores de organizaciones que fueron previamente atacadas y comprometidas.

Para el intruso, una fuente de passwords o datos sensibles de ese estilo es de relevancia atemporal. Esto significa que no importa si la base de datos que tiene en su poder es antigua, ya que podrá usarse en un futuro como dato o como pista para conseguir el dato necesario actual.

Es común además que éste, más allá del análisis íntegro del sitio institucional del objetivo, busque también información de algún componente de la organización en portales o sitios relacionados con ofertas laborales (miles de currículum vitae), foros, blogs y comunidades online de todo tipo, eventos, registros de dominios, portales de educación, guías empresariales, telefónicas, profesionales e industriales, búsqueda de colegas, redes sociales tipo LinkedIn, Facebook, Twitter, Myspace, avisos clasificados de todo tipo, policía y agencias de seguridad online.

Los buscadores también son una increíble fuente de clasificación, análisis, búsqueda y caché de información, confidencial o no, sobre un objetivo. Altavista fue el buscador preferido en los años 90, Yahoo lo fue más cerca del año 2000 y hoy lo es Google. Seguramente habremos escuchado hablar de Google hacking (lo trataremos en un tema posterior), es decir, utilizar el famoso buscador para encontrar datos relevantes del objetivo.



Aproximadamente 2.210 resultados (0,44 segundos)

[<?php /* \\$server = "localhost"; \\$database = "iie"; \\$user ...](#)
[www.iithai.org/web/inc/config.inc - Traducir esta página](#)
[<?php /* \\$server = "localhost"; \\$database = "iie"; \\$user = ""; \\$password = "" ...](#)
[iithai"; \\$user = "root"; \\$password = "iie@bundith"; mysql_connect\(\\$server, \\$user, ...](#)

[<?php \\$dbname = 'grizle_pn'; \\$hostname = 'humbug'; \\$username ...](#)
[www.grizle.co.uk/veryoldsite/common.inc - Traducir esta página](#)
[<?php \\$dbname = 'grizle_pn'; \\$hostname = 'humbug'; \\$username = 'grizle'; \\$password](#)
[= '13f4cff19bcb62e7'; \\$id_link = @mysql_connect\(\\$hostname, ...](#)

[\\$servidor="localhost"; \\$usuario="root"; \\$password="contracara ...](#)
[tarwi.lamolina.edu.pe/exceltosql/conexion.inc](#)
[\\$servidor="localhost"; \\$usuario="root"; \\$password="contracara"; \\$base="foro"; \\$SQLid](#)
[= mysql_connect\(\\$servidor,\\$usuario,\\$password\); ...](#)

Las búsquedas que hacen uso de Google para encontrar información sensible se suelen llamar Google Dorks. Podemos encontrar una gran cantidad de dorks en:

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



Por su parte, el proyecto Google Hack Honeygot (<http://ghh.sourceforge.net>) merece especial atención.



What is GHH?

Google Hack Honeygot is the reaction to a new type of malicious web traffic: search engine hackers. GHH is a "Google Hack" honeypot. It attracts attackers that use search engines as a hacking tool against your resources. GHH implements honeypot theory to provide additional security.

Google has developed a powerful tool. The search engine that Google has implemented allows for searching on an immense amount of billions of pages [February 2005] and continues to grow daily. Mirroring the growth of the Google index, the spread of web-based administrative tools has resulted in an increase in the number of misconfigured and vulnerable web apps available on the Internet.

These insecure tools, when combined with the power of a search engine and index which Google provides, results in a convenient attack vector to combat this threat.

GHH is powered by the [Google](#) search engine index and the Google Hacking Database (GHDB) maintained by the johnny.ihackstuff.com

Honeynet Research with GHH

You can view research done with GHH in the HoneyNet Project's "Know Your Enemy" [paper on web application honeypots](#).

GHDB Honeypots Available:

GHDB Signature #365 **Emulated** (intitle:"PHP Shell *" "Enable stderr" filetype:php)
GHDB Signature #833 (filetype:php HAXPLORER "Server Files Browser")
GHDB Signature #733 ("Enter ip" inurl:"php-ping.php")
GHDB Signature #365 (intitle:"PHP Shell *" "Enable stderr" filetype:php)

Se denomina Honeygot al sistema (a modo de cebo) cuya intención es atraer a intrusos simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática usada para recoger información sobre los atacantes y sus técnicas. Los Honeygot pueden distraer a los atacantes y advertir al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque.

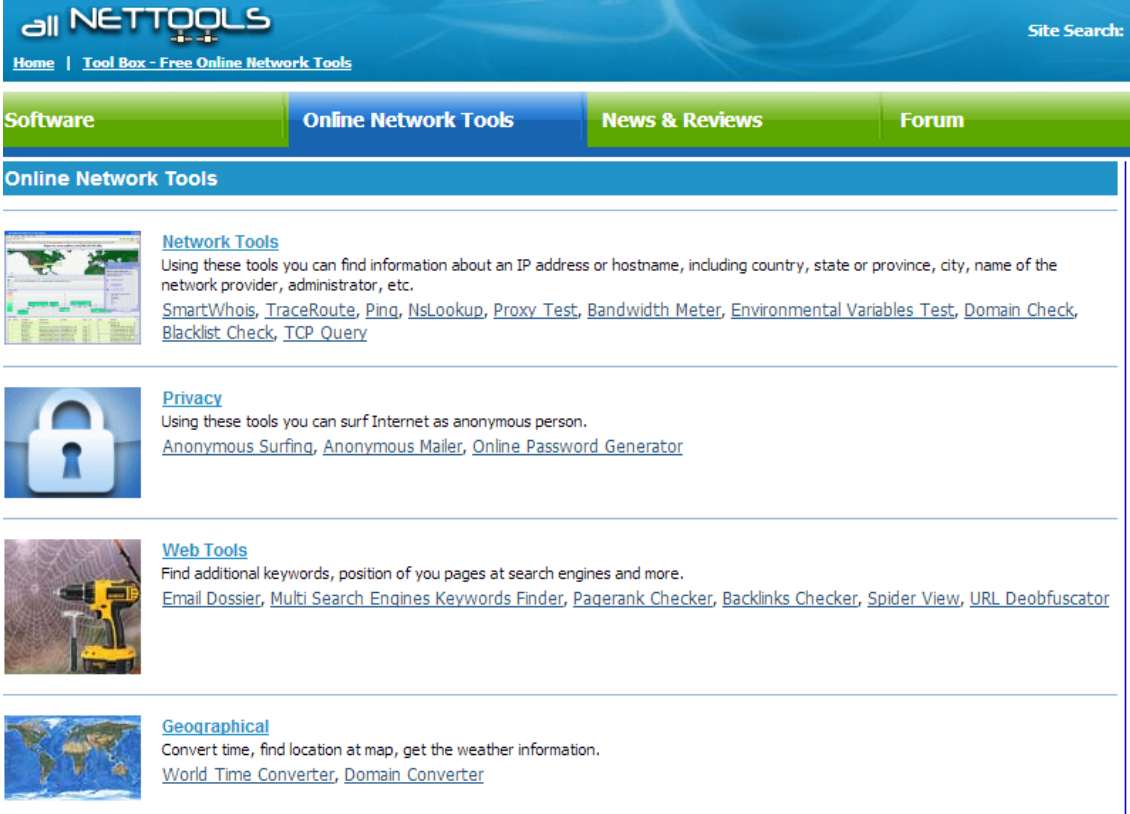
La gente de Google no es tonta y lo más probable es que cuando un atacante, buscando objetivos al azar, coloque algunos de los métodos descritos en la GHDB (Google Hack Database) sea redireccionado hacia alguna honeygot o a una mayoría de links con resultados 404 y a más honeygot. Esto permite controlar los ataques indiscriminados de script-kiddies, pero no así el ataque a organizaciones de modo focalizado.

Para evitar problemas, en nuestros sitios web conviene utilizar un filtrador de robots de indexación, si no deseamos que Google u otro buscador cacheen el sitio o parte de ellos.

Algunas herramientas automatizan la búsqueda a través de Google, como QGoogle, GoogleScan, Google Enum o Site Digger. Incontables scripts en Perl y otras herramientas podrán ser encontradas en Securityfocus o Packetstorm para buscar en Google usuarios de sistema e información relacionada al footprinting (Kali Linux tiene en su colección varias de éstas). Pero la búsqueda y el análisis manual es lo más recomendable para hacerlo de modo profesional dirigido a un objetivo en concreto.

1.3 Otros Recursos Online

Hay otras bases de datos públicas y herramientas que brindarán datos en tiempo real en Internet. Entre estos últimos, los sitios más conocidos en el pasado fueron www.samspade.org y www.netcraft.com, que permitían saber el sistema operativo de los servidores, sus rangos de direcciones, qué sistema tenía históricamente, su uptime, IP, los nombres de administradores, teléfonos y direcciones físicas, entre otras cosas. Como ejemplo, veamos qué datos podemos obtener en el sitio www.all-nettools.com/toolbox, que tiene muchas herramientas.



The screenshot shows the 'all NETTOOLS' website interface. At the top, there is a navigation bar with 'Home' and 'Tool Box - Free Online Network Tools'. Below this is a menu with 'Software', 'Online Network Tools', 'News & Reviews', and 'Forum'. The main content area is titled 'Online Network Tools' and lists four categories:

- Network Tools**: Using these tools you can find information about an IP address or hostname, including country, state or province, city, name of the network provider, administrator, etc. Tools listed include SmartWhois, TraceRoute, Ping, Nslookup, Proxy Test, Bandwidth Meter, Environmental Variables Test, Domain Check, Blacklist Check, and TCP Query.
- Privacy**: Using these tools you can surf Internet as anonymous person. Tools listed include Anonymous Surfing, Anonymous Mailer, and Online Password Generator.
- Web Tools**: Find additional keywords, position of your pages at search engines and more. Tools listed include Email Dossier, Multi Search Engines Keywords Finder, Pagerank Checker, Backlinks Checker, Spider View, and URL Deobfuscator.
- Geographical**: Convert time, find location at map, get the weather information. Tools listed include World Time Converter and Domain Converter.

- **SmartWhois**: encuentra información acerca de una dirección IP, hostname, incluyendo país, provincia, ciudad, nombre del proveedor de Internet, su administrador.

Registrant:
targetcompany (targetcompany-DOM)
XXX Everest Bk A.Enclave
Amerpet
Hyderabad
Andrapradesh,500038
IN
Domain Name: targetcompany.COM

Administrative Contact:
***** (R1XXZ-0G) targetcompany@D1.VSH-REG.IN
targetcompany
XXX, Everest Block, A.Enclave,
Amerpet
Hyderabad, Andrapradesh 500038
IN 91 40 XXXX 329X Fax- 91 40 XXXX 329X
Technical Contact:
***** (VSXX) techcontact@WEBINDIA.COM
XXXX Inc
XXXX-Reliance
Hoffman Estates, IL 60194
US 409/XXX-XXXX 409/XXX-XXXX
Record expires on 14-Oct-200X.
Record created on 13-Oct-1997.]
Database last updated on 12-Mar-2003 07:49:04 EST.

Registrant:
targetcompany (targetcompany-DOM)
Street Address
City, Province
State, Pin, Country
Domain Name: targetcompany.COM

Administrative Contact:
Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

Technical Contact:
Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX

Domain servers in listed order:
NS1.WEBHOST.COM XXX.XXX.XXX.XXX
NS2.WEBHOST.COM XXX.XXX.XXX.XXX

- **TraceRoute:** devuelve la máquina y la IP de cada salto que da un paquete desde la máquina original hasta la de destino por Internet. Además, también informa el tiempo en milisegundos que tarda éste.
- **Ping:** envía un echo request a una máquina específica en la red. Esto puede ser utilizado para comprobar la comunicación entre dos máquinas o para ver si el host específico está corriendo o existe.
- **Nslookup:** resuelve un hostname a dirección IP o viceversa.
- **ProxyTest:** comprueba si un Proxy es realmente anónimo. Este trata de reconocer la verdadera dirección IP incluso si ésta se encuentra detrás de un Proxy httpd.
- **Environmental Variables Test:** muestra varias configuraciones remotas del navegador y de nuestra máquina.

Muchos de los datos obtenidos a través de estas páginas, también pueden conseguirse directamente mediante la utilización de comandos de consola en un sistema operativo como Windows, Linux o Unix.

```
cmd
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS>tracert

Uso: tracert [-d] [-h saltos_máximos] [-j lista_de_hosts] [-w tiempo_de_espera]
nombre_destino

Opciones:
-d          No convierte direcciones en nombres de hosts.
-h saltos_máximos  Máxima cantidad de saltos en la búsqueda del
                  objetivo.
-j lista-de-host  Enrutamiento relajado de origen a lo largo de la
                  lista de hosts.
-w tiempo_espera  Cantidad de milisegundos entre intentos.

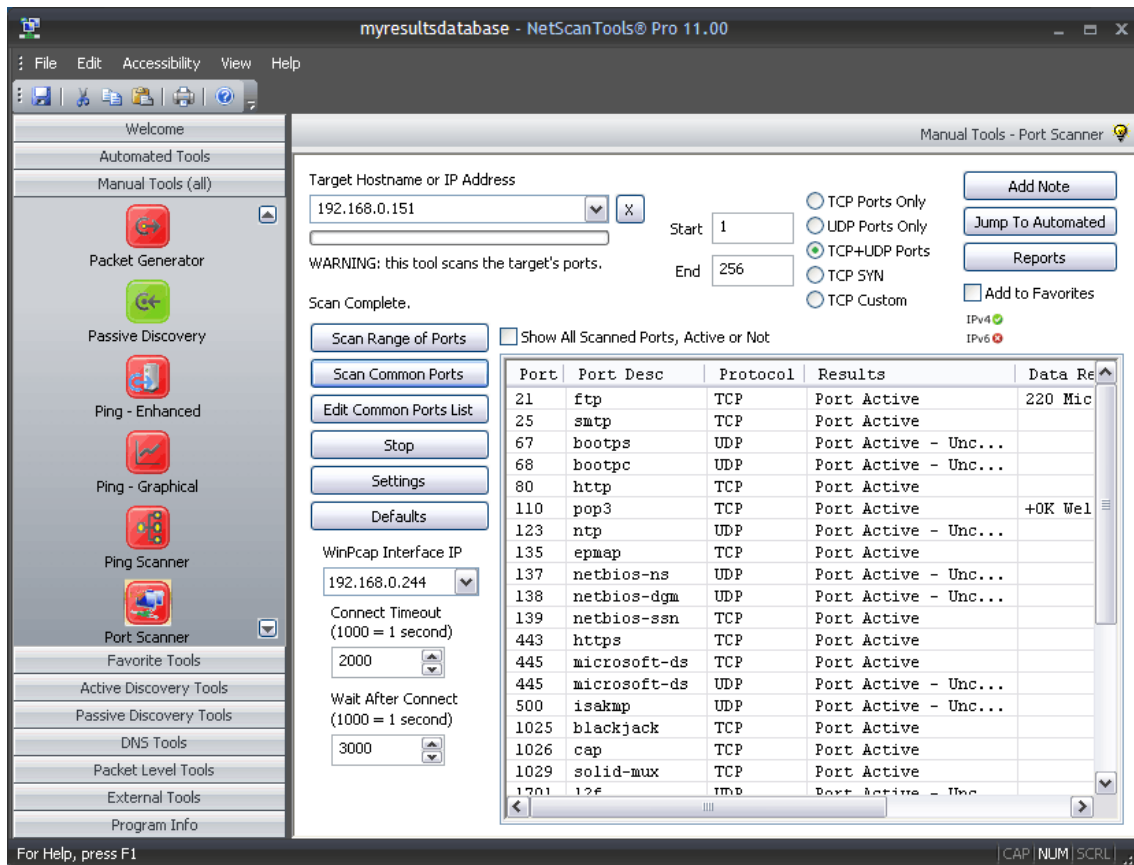
C:\WINDOWS>ping

Uso: ping [-t] [-a] [-n cuenta] [-l tamaño] [-f] [-i TTL] [-v TOS]
         [-r cuenta] [-s cuenta] [-j lista-host] [-k lista-host]
         [-w tiempo de espera] nombre-destino

Opciones:
-t          Ping el host especificado hasta que se pare.
           Para ver estadísticas y continuar - presionar Control-Inter;
           Parar - presionar Control-C.
-a          Resolver direcciones en nombres de host.
-n cuenta  Número de peticiones eco para enviar.
-l tamaño  Enviar tamaño del búfer.
-f          Establecer No fragmentar el indicador en paquetes.
-i TTL     Tiempo de vida.
-v TOS     Tipo de servicio.
-r cuenta  Ruta del registro para la cuenta de saltos.
-s count   Sello de hora para la cuenta de saltos.
-j lista-host Afloja la ruta de origen a lo largo de la lista- host.
-k lista-host Restringir la ruta de origen a lo largo de la lista- host.
-w tiempo de espera  Tiempo de espera en milisegundos para esperar cada
                    respuesta.

C:\WINDOWS>
```

Otro modo de obtenerlos es con herramientas de interfaz gráfica en dichos sistemas. La diferencia entre utilizar estas últimas y hacerlo de forma online (a través de sitios) es que el intruso hábil difícilmente lo haga desde su máquina (a menos que sea a través de un servidor proxy o intermediario) para no dejar rastros en el objetivo de los comandos ejecutados y su búsqueda. El intruso inteligente jamás dejará su dirección IP real en algún log del objetivo, a diferencia del profesional ético que no ve ningún problema en hacerlo.



Para obtener información del tipo contenido histórico de sitios, podemos visitar, por ejemplo, www.archive.org. Éste nos muestra, en una línea temporal, las diferentes páginas web que tuvo una actual. Lo importante de esto es que muestra variaciones de contenido en el tiempo (imaginemos nombres de contactos de empleados, cuentas de e-mail, archivos o directorios sensibles, etcétera).

Internet Archive Wayback Machine

http://web.archive.org/web/*/http://homestudio.thing.net/

WayBackMachine

Enter Web Address: All Take Me Back Adv. Search Compare Archive Pages

Searched for <http://homestudio.thing.net/> 102 Results

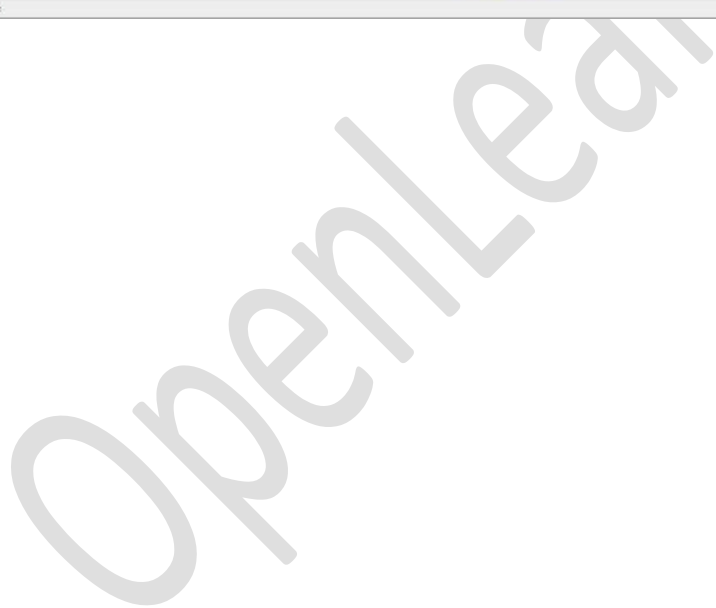
Note some duplicates are not shown. [See all.](#)
* denotes when site was updated.
Material typically becomes available here 6 months after collection. [See FAQ.](#)

Search Results for Jan 01, 1996 - Aug 08, 2007

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
0 pages	0 pages	0 pages	0 pages	4 pages	7 pages	11 pages	14 pages	17 pages	15 pages	21 pages	9 pages
				Mar 01, 2000	Feb 01, 2001	Jan 18, 2002	Feb 07, 2003	Feb 09, 2004	Jan 18, 2005	Jan 05, 2006	Feb 05, 2007
				Jun 21, 2000	Mar 02, 2001	Mar 30, 2002	Apr 02, 2003	Mar 20, 2004	Feb 02, 2005	Feb 09, 2006	Feb 08, 2007
				Oct 10, 2000	Mar 30, 2001	Jun 02, 2002	Apr 21, 2003	Apr 10, 2004	Feb 07, 2005	Feb 19, 2006	Feb 16, 2007
				Dec 07, 2000	Apr 05, 2001	Jun 05, 2002	Apr 24, 2003	May 19, 2004	Feb 08, 2005	Mar 06, 2006	Feb 26, 2007
					Apr 18, 2001	Aug 02, 2002	May 22, 2003	Jun 04, 2004	Feb 11, 2005	Apr 07, 2006	Apr 03, 2007
					Sep 25, 2001	Aug 11, 2002	May 25, 2003	Jun 07, 2004	Mar 08, 2005	May 01, 2006	Apr 04, 2007
					Dec 01, 2001	Sep 22, 2002	Jun 11, 2003	Jul 28, 2004	Mar 25, 2005	May 16, 2006	Apr 28, 2007
						Sep 24, 2002	Jul 30, 2003	Aug 06, 2004	Apr 01, 2005	May 17, 2006	May 19, 2007
						Oct 02, 2002	Aug 05, 2003	Aug 29, 2004	Jul 24, 2005	Jun 10, 2006	Jul 14, 2007
						Nov 22, 2002	Oct 07, 2003	Sep 23, 2004	Jul 26, 2005	Jun 15, 2006	
						Nov 26, 2002	Oct 16, 2003	Sep 28, 2004	Oct 29, 2005	Jul 08, 2006	
							Nov 22, 2003	Sep 29, 2004	Dec 02, 2005	Jul 20, 2006	
							Nov 29, 2003	Oct 01, 2004	Dec 14, 2005	Aug 13, 2006	
							Dec 14, 2003	Oct 13, 2004	Dec 26, 2005	Aug 30, 2006	
								Nov 03, 2004	Dec 30, 2005	Oct 13, 2006	
								Nov 30, 2004		Nov 05, 2006	
								Dec 04, 2004		Nov 11, 2006	
										Nov 17, 2006	
										Nov 26, 2006	
										Dec 05, 2006	
										Dec 09, 2006	

Home | Help

Terminé



1.4 Encabezados de Correo Electrónico

Con el correo electrónico nos encontramos con varias situaciones que debemos de tener muy en cuenta. Empezando por la privacidad del mensaje. Habrá situaciones en las que no queramos que el contenido de un mensaje sea leído por nadie más que por la persona a la que va dirigida. Antes escribíamos cartas que no se podían leer sin romper el sobre o postales que podía leer cualquiera que cayese en sus manos. Normalmente también firmábamos las cartas ordinarias para que se supiera que éramos realmente nosotros quien las escribía y no otro. En el correo electrónico pasa con mayor razón ya que no es difícil aparentar otra identidad o que intenten falsificar la nuestra. Ya no vale que pongamos nuestro nombre al pie del mensaje o el remite con nuestros datos correctos. Tenemos que utilizar para ello otra forma que dé veracidad a la personalidad del que remite el mensaje. Necesitamos pues una "firma digital", Por ultimo también hay situaciones en las que no queremos que se conozca quién ha enviado un mensaje, o más comúnmente, que no se puedan obtener nuestros datos de forma automática cuando enviamos los mensajes a listas, foros o grupos de noticias.

Cuando enviamos un correo electrónico, lo que estamos haciendo, siguiendo con el símil del correo ordinario, es enviar una postal, no una carta. Esa carta puede pasar por múltiples servidores y redes que la pueden leer y por supuesto, está suficientemente identificada para saber quién la ha enviado (en esto, como en todo, también existen las falsificaciones de identidad).

Un mensaje de correo electrónico se compone de una cabecera con los datos identificativos del mensaje y el texto del mensaje. Así que vamos a centrarnos en cada una de las partes para hacer de nuestro correo un medio más seguro.

Cabecera del mensaje

Es evidente que se necesitan varios datos identificativos para que un mensaje llegue a su destinatario. Además, aquí no existe un solo servicio de correo, sino miles de ellos por los que puede pasar nuestro mensaje. Cada servidor por el que vaya pasando el mensaje irá incluyendo sus propios datos en la cabecera.

Esa cabecera es perfectamente legible por todos los ordenadores por los que vaya pasando (y por supuesto por nosotros mismos). Vamos a analizar qué es lo que hay en una cabecera con un ejemplo. Nota: La cabecera hay que leerla de abajo a arriba.

Dirección de respuesta	Return-Path: <mipc@dominio.org>
Servidores por los que ha pasado	Received: from mipc ([213.96.68.187]) by aseara.com (8.9.3/8.9.3) with ESMTP id NAA20948 for <usuario@destino.com>; Sun, 7 Oct 2001 13:46:50 +0200 Received: from [127.0.0.1] by mipc (ArGoSoft Mail Server, Version 1.3 (1.3.0.1)); Sun, 7 Oct 2001 14:53:06 +0200
Identificación	Message-ID: <000901c14f2f502494ce050700a8c0@dominio.ws> From: "Origen" <origen@dominio.org> To: <usuario@destino.com> Subject: prueba Date: Sun, 7 Oct 2001 14:52:47 +0200

Características del mensaje

MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4133.2400
X-MimeOLE: Produced By Microsoft MimeOLE
V5.50.4133.2400
Status: R
X-Status: N

En el ejemplo podemos ver entre otros datos cómo se ha enviado el correo y qué características tiene, con qué programa se ha hecho (X-Mailer: Microsoft Outlook Express 5.50.4133.2400), en qué fecha se ha enviado (Date: Sun, 7 Oct 2001 14:52:47 +0200), el asunto del mensaje (Subject: prueba), a quién va dirigido (To: usuario@destino.com), quien lo manda (From: "Origen" origen@destino.org) y qué identificador tiene ese correo (Message-ID: <000901c14f2f\$02494ce0\$0700a8c0@dominio.ws>)

Los siguientes campos, que empiezan por Received, nos indican todos los servidores por los que ha pasado el mensaje. El primer received y el último (siempre empezando por abajo) apuntan al servidor del emisor y del destinatario del mensaje. En este caso, y como ejemplo, hemos puesto uno con solo dos servidores de correo por los que ha pasado el mensaje (en este caso el emisor lo ha enviado desde un servidor que se ha montado en su propio PC sin utilizar ningún proveedor.

El primer received nos dice que lo ha enviado el PC llamado MiPC utilizando un programa servidor de correo de Argosoft corriendo sobre la dirección de localhost (127.0.0.1) y fue enviado por éste servidor unos cuantos segundos después de recibirlo por parte del cliente de correo.

El segundo Received nos dice que el mensaje ha sido recogido por el servidor de aseara.com, que se lo ha enviado a él un ordenador que se llama mipc que tenía en esos momentos una dirección IP determinada, para entregarlo al buzón del destinatario del mensaje.

Cuerpo del mensaje

Ahora entramos ya en el mensaje en sí. Como hemos indicado antes, todo correo enviado de la forma "normal" se envía en claro. Es decir, estamos enviando una postal, no una carta que tiene el texto protegido por un sobre para que no se lea, por lo que no tenemos ninguna garantía de que nuestra privacidad esté a salvo ya que, con medios y técnicas adecuadas, lo pueden leer mientras esta "por el camino". La única solución posible es enviar los mensajes cifrados. ¿Cómo?, pues para eso están los programas de criptografía como PGP o GNUPG. Hablaremos de criptografía en otro tema del curso.

Es posible que queramos enviar el mensaje en claro. Pues también tenemos que pensar en los problemas que eso pueda acarrear. Tenemos dos formas de enviar (o recibir) el mensaje. En texto plano o en formato html. Leer el correo en formato html funciona prácticamente igual que cuando visitamos una web. Por poner un ejemplo, históricamente algunos anunciantes, de los

<http://www.openlearning.es>

que nos llenan el buzón, han utilizado sistemas como el web bugs o gráficos descargados directamente desde su servidor para saber si hemos abierto el mensaje, que eficacia tiene, etc.. Como html que es, prácticamente se puede hacer las mismas cosas que con una página web. Pueden abrir en frames ocultas páginas web en las que va a quedar registrada nuestra IP, incluyen javascripts... en fin, es largo la cantidad de cosas que se puede hacer con el correo en formato html.

Si, por el contrario, configuramos nuestro cliente de correo para recibir el correo en formato texto, nada de eso puede suceder. El texto es eso, solo texto. El único inconveniente será que aquel que envíe el correo en html, veremos también los tag del mismo y a veces se hace muy difícil la lectura. Por lo tanto un consejo, es enviar el correo en formato texto.

OpenLearning