Manual sobre el correo electrónico

(http://espam.esp.st)

Introducción.

Este manual pretende ser una simple introducción a uno de los sistemas más utilizados de internet, el del correo electrónico. Sobretodo, el texto intentará dar respuesta a las dudas más frecuentes sobre el funcionamiento interno del mismo, pasando por alto cosas como la utilización de los agentes de correo, su configuración o similares. La idea es explicar ¿como?, o ¿por qué? pasan determinadas cosas que muchos usuarios se preguntán pero desconocen como averiguar. Nunca se ha preguntado ¿cómo és posible enviar correo falso? o porque es tan dificil localizar a los "*spamers*", o incluso como podría saber si un correo electronico lo ha enviado quien dice que lo ha enviado. Las respuestas a todas estas preguntas y algunas otras están en este manual.

Capitulo 1. ¿Cómo funciona el correo electrónico?.

A grandes rasgos el funcionamiento del correo electrónico se basa en tres elementos: la persona que envia el correo, el medio por donde circula el correo y el destinatario. Empecemos por el primero. Lo primero que se necesita para enviar un correo electrónico (entre otras cosas) es un editor de textos mediante el cual podamos escribir la información que deseamos transmitr. Si bien como veremos mas adelante cualquier editor de textos nos es válido, lo mejor es utilizar cualquiera de los ya integrados en los ***agentes de usuario***, tanto comerciales como gratuitos. Con el termino *agente de usuario* se denominan a los programas que sirven para escribir y recibir correo. Ejemplo de estos son, en el caso de Windows el archiconocido outlook, o el evolution en Linux. Son aplicaciones que nos proporcionan una cierta comodidad a la hora de organizar y escribir nuestros mensajes, permitiéndonos abstraernos totalmente del proceso de envio del correo. No se entrará en el proceso de configuración de éstos porque no es la finalidad de este texto, para más información acerca de como configurar un agente simplemente se puede mirar la ayuda adjunta al programa. Bien ya tenemos escrito nuestro correo, ahora queremos enviarlo; normalmente pulsamos en nuestro agente en un botón que pone enviar o alguno similar y el correo es enviado al destinatario. Es en este punto en donde tenemos que bajar un poco el nivel de abstracción para así ver lo que pasa. Realmente lo que ocurre es que nuestro agente envia la información que hemos escrito a otro programa, que puede estar instalado en nuestro propio ordenador o bien en un sistema diferente (más habitual). Estas aplicaciones son conocidas con el nombre de ***agentes de envio o transporte***. Estos agentes de envio utilizan un protocolo de conunicaciones llamado SMTP, es decir, ***protocolo simple de transporte de correo*** y es el protocolo que se utiliza para enviar y recibir correo electrónico por la red internet. Así, un correo electrónico esta compuesto por dos partes, una parte visible, que es nuestro texto y una parte que no vemos y que es la parte de control. En esta última aparece la información necesaria para poder enviar el correo al destinatario. Este protocolo de comunicaciones tiene una serie de particularidades, entre las cuales una de las más interesantes es que no puede transmitir más que correos de texto, no es capaz de enviar mensajes con fotos, videos o cualquier otro elemento multimedia. Más concretamente algunas de las limitaciones del protocolo SMTP son las siguientes:

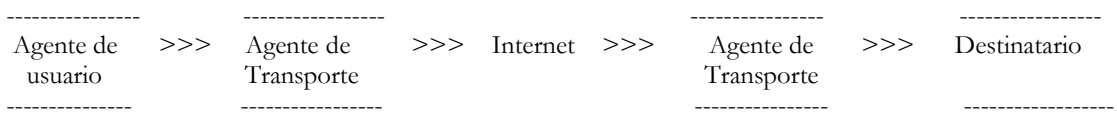
1.- SMTP no puede enviar archivos ejecutables o binarios. Existen algunos sistemas que permiten convertir estos archivos a archivos de texto y así poder utilizar el protocolo SMTP como *Uuencode/UUdecode* pero tienen el problema de que no son un estandar.

2.- No se pueden transmitir mensajes que incluyan carácteres especiales de los idioma nacionales ya que estos se representan con 8 bits y SMTP sólo soporta caracteres ASCII de 7 bits.

3.-Algunas implementaciones del protocolo no cumplen completamente el estandar, surguiendo algunos problemas como:

- Eliminación, reordenación o incorporación de caracteres de fin de linea o de retorno de carro.
- Eliminación de espacios finales.
- Truncar o dividir lineas de más de 80 caracteres,etc.

Para aclarar un poco las cosas, lo mejor es mostrar lo explicado con un esquema:



Llegados a este punto, es posible que el usuario se plantee el hecho de ¿cómo es posible esto? ya que todos hemos escrito algún correo adjuntando algun archivo multimedia, como videos o archivos comprimidos. La respuesta a esta sencilla pregunta es otro protocolo más: MIME. No entraremos en detalle en el funcionamiento de este protocolo, simplemente y a grandes rasgos, decir que lo que hace es transformar los archivos binarios en archivos de texto que son transmisibles por SMTP. Este protocolo implica que nuestros archivos crecen un tercio de su tamaño cuando los enviamos debido al sistema de codificación.

Capitulo 2. - Analisis de las cabeceras del correo.

Es inevitable, el correo basura nos llega. No importa lo que hagamos, ni filtros ni antivirus ni nada. Cada día nos despertamos con unos cientos de mensajes basura. Estamos desesperados y queremos una solución. Una forma de solucionar este problema es no teniendo cuentas de correo electronico. Otra de las posibilidades consiste en intentar detectar a los spamers y denunciarles. Nunca os tomeis la justicia por vuestra mano, ya que aunque sea muy tentador, al final los perjudicados sereis vosotros. Si detectais a un espamer lo mejor es que lo denuncieis a vuestro administrador de correo. El se encargará de tomar las medidas oportunas. En este capitulo se enseñará a analizar las cabeceras de control de los correos para así saber si son falsos o no. Aunque los que envian correos basura siempre intentan falsificar sus origenes, muchas veces es muy fácil saber si un correo es auténtico o no.

Fase 1. ¿És este correo spam?.

Es relativamente fácil saber si un correo es spam o no:

- ¿Desconozco al remitente?
- ¿Contienen mensajes sobre empresas u otras ofertas no solicitadas?
- ¿El destinatario del mensaje es otro diferente de usted?
- ¿Contiene virus?

Si la respuesta es afirmativa para alguna de las preguntas, probablemente sea spam.

Fase 2. Este correo es spam. ¿ahora qué hago?.

En esta fase aprenderemos a analizar las cabeceras del correo electrónico. Estas cabeceras permanecen ocultas para la mayoria de los usuarios de sistemas informáticos. En ellas podemos encontrar información valiosa para desenmascarar (o almenos intentarlo) a esos malosos de los *spamers.*

Lo primero será analizar la cabecera de un correo normal para poder ver los diferentes elementos que suelen aparecer.

```
X-UIDL: 71663ac1b2197051d838c6c81e4e5b8f
X-Mozilla-Status: 0011
X-Mozilla-Status2: 00000000
X-Apparently-To: correo@yahoo.es via 66.218.93.158; Wed, 04 Aug 2004
06:02:32 -0700
X-Originating-IP: [62.42.230.12]
1.- Return-Path: <correo@ono.com>

2.- Received: from 62.42.230.12  (EHLO resmta03.ono.com) (62.42.230.12)
  by mta426.mail.scd.yahoo.com with SMTP; Wed, 04 Aug 2004 06:02:32 -0700

3.- Received: from MODDING (62.43.11.2) by resmta03.ono.com (7.1.016.11)
id 40D79551000D206F for correo@yahoo.es; Wed, 4 Aug 2004 14:57:30 +0200

4.- From: "correo" <correo@ono.com>
5.- To: "'corre ...'" <correo@yahoo.es>
6.- Subject: RE: Practica de asoA
7.- Date: Wed, 4 Aug 2004 14:57:34 +0200
8.-Message-ID: <000501c47a22$a11f3430$020b2b3e@MODDING>

MIME-Version: 1.0
Content-Type: multipart/alternative;
     boundary="----=_NextPart_000_0006_01C47A33.64A80430"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook, Build 10.0.2627
Importance: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2742.200

This is a multi-part message in MIME format.
```

Comentar que para explicar de forma sencilla la cabecera de este correo electrónico se han numerado las diferentes lineas para ir comentandolas, en el correo original no están. También se han cambiado algunos datos por razones obvias para garantizar la privacidad.

Lo primero que tenemos que observar son los posibles campos que empiezan por una “X”. Estos campos son añadidos normalente por los programas de usuario o de entrega como una extensión y a la hora de analizar el correo electrónico son totalmente descartables. Las ignoramos.

La linea 1 contiene el campo *return-path* que se suele utilizar como dirección de retorno en caso que se produzca algún tipo de error enviando el correo.

Las lineas 2 y 3 son tal vez las más importantes a la hora de analizar un correo electrónico. Estos campos son añadidos conforme el correo va circulando por internet y va pasando por los diferentes ordenadores. Cada ordenador por el que el correo pasa añade su campo received. Se han de leer de abajo arriba, es

decir el primero es la linea 3 y el segundo la 2. La estructura básica de los campos *received* es muy simple y consta de dos partes. La primera parte indica la máquina que envio el correo y siempre viene encabezada por la palabra *from.* La segunda parte indica la máquina que recibe el correo y siempre viene precedidad por la palabra *by.* En el ejemplo en la linea 3 tenemos:

```
Received: from MODDING (62.43.11.2) by resmta03.ono.com (7.1.016.11)
id 40D79551000D206F for correo@yahoo.es; Wed, 4 Aug 2004 14:57:30 +0200
```

from MODDING (62.43.11.2): es la máquina que originó el mensaje cuya ip podemos ver entre paréntesis.

resmta03.ono.com (7.1.016.11)id 40D79551000D206F for correo@yahoo.es; Wed, 4 Aug 2004 14:57:30 +0200: esta parte es la máquina que recibió el mensaje procedente de la máquina llamada MODDING. La máquina que recibió el mensaje se llama *resmta03.ono.com y* su ip aparece entre parentesis. La información que aparece a continuación puede variar según sea el agente de transporte que se utilice. Como regla general en el caso de la primera linea de received aparecerá el correo del destinatario y además en el resto de *received* la fecha además del offset en formato UTC de la fecha local. En nuestro caso particular tenemos en primer lugar el identificador del correo en la máquina: *id 40D79551000D206F,* el destinatario: *for correo@yahoo.es,* la fecha en que se envió el correo: *Wed, 4 Aug 2004 14:57:30* y finalmente el offset respecto la fecha local: *+0200.* Las fechas así como las máquinas por donde va pasando el correo son lo que entre otras cosas nos permitirán descubrir correos falsos. Para ello veamos el siguiente *received:*

```
Received: from 62.42.230.12  (EHLO resmta03.ono.com) (62.42.230.12)
  by mta426.mail.scd.yahoo.com with SMTP; Wed, 04 Aug 2004 06:02:32 -0700
```

como podemos ver la máquina que envia el correo es la misma que lo recibió en el anterior *received: from 62.42.230.12 (EHLO resmta03.ono.com).* Si no fuera así, significaria que el correo habría sido manipulado y por tanto que es un correo basura. Es como una cadena de ordenadores en la que uno envia y el otro recibe. Si la cadena se rompe significa que algo no está bién. En este caso la máquina que recibe el correo de *resmta03.ono.com* es la máquina *mta426.mail.scd.yahoo.com.* Podemos observar que la fecha de recepción son las 6 de la madrugada hora local. Se podría llegar a pensar que el correo ha sido manipulado por la enorme diferencia de tiempo entre el envio y la recepción (15 horas hacia atrás ya que es el mismo día) pero no es así si tenemos en cuenta el offset. La diferencia horaria es de -7 horas respecto el 0. En el origen tenemos que son las 3 de la tarde, le quitamos las dos horas respecto el 0 y después le quitamos las siete hasta el destino, el resultado es de las 5:57, es decir, entre el envio y la recepcion han pasado unos 5 o 6 minutos dependiendo de que los relojes estubieran bien sincronizados etc. Así tenemos que entre las horas de envió y recepción apenas hay diferencia temporal. Si hubiera un excesivo tiempo o fechas absurdas sería una señal de que estamos ante un

correo basura.

Saltemos un momento a la linea 9. En ella encontramos el identificador del mensaje de correo a lo largo de todo el sistema de correo allá por donde pase. Es su identificador digital y siempre es el mismo. Su formato es también siempre el mismo. Siemrpe entre corchetes y después del identificador ha de aparecer separado por una "@" el nombre de la máquina que envió el correo inicialmente. Si esto no es así es problemente un correo falso.

Las lineas de la 4 a la 7 son las típicas lineas de subject, from, to y la fecha. Son facilmente falsificables y por eso no son muy fiables. El resto no sirve en principio para identificar el origen del correo elecrtónico pero forma parte de la cabecera y se ha creido conveniente incluirlo. En estas lineas podemos obtener información sobre el agente de correo que se utilizó para escribir el correo, en este caso: *X-Mailer: Microsoft Outlook, Build 10.0.2627.*

Bién, ahora sabemos cuales son los elementos más importantes a la hora de analizar un correo. A continuación os indicaremos cuales son las características más rápidas para identificar a un correo basura:

1. Cualquier *received* despues del campo *date* es falso.
2. Los campos *received* tienen que encadenarse, si alguno de estos campos no coincide con el siguiente el correo ha sido falsificado.
3. Cuando encontremos dos campos *received* con nombres de host diferentes el correo electrónico habrá sido probablemente enviado mediante la tecnica del relay a través del primer host.
4. Un campo *received* con una fecha antigua y no concordante con las demás ha sido seguramente falsificada.
5. El dominio que aparece en el identificador de mensaje tiene que coincidir con el dominio del campo *from*.
6. Comprueva si todos los host que aparecen realmente existen via DNS.
7. La parte del host del campo *from* tiene que estar en concordancia con el último *received.*

Ahora veremos un correo basura y sus diferentes partes para identificar a los malosos que nos lo han enviado.

```
1.- Return-Path: <semassaq@xzapmail.com>

2.- Received: from lavin02 ([192.168.197.19]) by jones.melange.net
          (Netscape Messaging Server 4.15 jones Mar 14 2002 21:29:48) with
          ESMTP id HIHM8V00.A43 for <correo@arrakis.es>; Wed, 23 Jul
          2005 19:07:43 +0200

3.- Received: from [195.188.22.73] (helo=wtwmmail01.xzapmail.com)
      by lavin02 with esmtp id 19fNE6-0005z1-01
      for correo@arrakis.es; Wed, 23 Jul 2005 19:16:30 +0200

4.- Received: from xzapmail.com (unverified [10.49.101.5]) by xzapmail.com
 (Rockliffe SMTPRA 5.2.5) with ESMTP id
<B0002168377@wtwmmail01.xzapmail.com>;Wed, 23 Jul 2005 17:39:59 +0100

5.- Message-ID: <229811-220037323163714156@xzapmail.com>

X-Priority: 3
Return-Receipt-To:
Reply-To:
6.- From: semassaq@xzapmail.com
7.- To: semassaq@xzapmail.com
Subject:
Date: Wed, 23 Jul 2005 17:37:14 +0100
MIME-Version: 1.0
Content-type: text/plain; charset=US-ASCII
```

Lo primero que podemos observar es que los campos from y to (lineas 6 y 7) son iguales. Por si sólo este hecho no es indicativo de nada, a no ser que la persona que recibe el correo no sea la destinataria del mensaje (como ocurre en nuestro caso). Nuestro correo es *correo@arrakis.es* pero el destinatario es *semassaq@xzapmail.com.* Muchos se preguntarán el como ha podido llegar un correo a un destinatario diferente del indicado, ¿Tal vez un error del sistema de correo?. Como veremos más adelante no se trata de ningún error sino de una acción totalmente deliverada por parte de los espamers, el autentico destinatario aparece en la linea 3: *correo@arrakis.es.* Pasemos al primer *received,* es decir, la linea 4. El emisor original se supone que es: *xzapmail.com (unverified [10.49.101.5]).* El receptor es tambíen el mismo *xzapmail.com.* En prinpio es posible que el emisor y el receptor sean el mismo, por ejemplo es el caso de que nos enviemos un correo a nosotros mismos. Pero existiendo más campos *received* es poco probable que esto sea así. Comprobamos la existencia de este domino mediante la utilidad *whois* y obtenemos la siguiente información:

Consulta la base de datos de Whois

Dominio	Estado	Acción
xzapmail.com	Disponible	☐
xzapmail.net	Ocupado	Detalles / Visitar
xzapmail.org	Disponible	☐
xzapmail.info	Disponible	☐
xzapmail.biz	Disponible	
xzapmail.co.uk	Ocupado	Detalles / Visitar
xzapmail.org.uk	Disponible	☐
xzapmail.ca	Disponible	☐
xzapmail.cc	Disponible	☐
xzapmail.de	Disponible	☐
xzapmail.it	Disponible	☐
xzapmail.dk	Disponible	☐
xzapmail.us	Disponible	☐
xzapmail.be	Disponible	☐
xzapmail.se	Disponible	☐
xzapmail.eu.com	Disponible	☐
xzapmail.us.com	Disponible	☐
xzapmail.ru	Disponible	☐
xzapmail.uk.com	Disponible	☐
xzapmail.tv	Disponible	☐

Como podemos ver, esto nos indica que el dominio no esta siendo utilizado por nadie y que por tanto no puede haber sido utilizado en el correo. En principio lo que podemos deducir es que este campo received ha sido probablemente falsificado. Si seguimos analizando el siguiente campo *received (linea 3)* podremos ver que el emisor es: *wtwmmail01.xzapmail.com* en principio nuestra máquina falsa. En este caso se nos indica la ip de la máquina; lo comprobamos y tampoco existe. El correo es recibido por una máquina llamada *lavin02.* Esta máquina de la cual no se indica la ip no indica el tipo de dominio que representa (com, es, net, org ...) y es por tanto de dudosa credibilidad. La linea 2 es la única que hasta cierto punto es muy dificil de falsificar ya que es la generada por nuestro propio servidor de correo. En ella podemos observar la ip de *lavin02: 192.168.197.19*

Capitulo 3. - Envio de correo falso.

Llegados a este punto tal vez queramos saber como enviar correo falso. Ha de quedar claro que la capacidad de enviar correo falso puede ser útil en determinados casos, las motivaciones personales dependen de cada uno, pero nunca ha de convertirse en un medio para realizar acciones ilegales ni perniciosas contra otros.

Lo primero es disponer de un programa de *telnet*. Este tipo de programas permiten la conexión remota a sistemas informaticos mediante la consola de comandos. Windows trae uno de estos programas de serie. Para ejecutarlo simplemente teneis que escribir en la consola el comando telnet.
Lo que haremos será conectarnos con una maquina de la red que disponga de un servidor de correo (un agente de transporte. Ver tema 1). Una vez conectados enviaremos el correo desde el servidor hacia el destino seleccionado. Con esto conseguimos que la persona que reciba el correo piense que éste ha sido enviado desde la máquina con la que estamos conectados. Llegados a este punto quiero recalcar el hecho de que no se deven realizar acciones dañinas con el envio de correo falso. Estas máquinas suelen llevar un registro de las personas que se les conectan registrando la ip, dominio y otros datos, así que no intenteis realizar cosas *malas* con el envio de correo falso. Bién, para empezar nos conectaremos con un servidor de correo. Existen muchos servidores a los que podeis conectaros y con una pequeña busqueda en google os será muy fácil encontralos. No indicaremos pués ninguna dirección explicita de servidores de correo.

1.-Nos conectamos.

Para conectarnos por ejemplo al servidor llamado *stmp.servidorCorreo.com* ejecutamos el siguiente comado:

telnet stmp.servidorCorreo.com 25

Telnet es el nombre del programa que nos va a permitir conectarnos al servidor, ***stmp.servidorCorreo.com*** es el nomnbre de la máquina y 25 es el puerto estandar que utilizan los servidores de correo para enviar y recibir correos.

2.-Estamos conectados. ¿y ahora qué?

Lo mas probable es que lo primero que ocurra es que el servidor nos salude (son todos muy amables :D). Ignoramos por ahora este saludo y empezamos a enviar nuestro correo. Para ello escribiremos tal cual:

HELO midominioinventado.com
Es la respuesta al saludo inicial que nos daba el servidor.

MAIL FROM: <micorreoinventado@midominioinventado.com>

Aquí escribimos el origen del correo, es decir la persona que envia el correo. Podemos poner lo que queramos.

RCPT TO: <correodemiamigo@sudominio.com>

El destinatario del correo, por ejemplo la dirección de algún amigo/a.

DATA
texto del mesaje.

Finalmente escribimos el mensaje y normalente acabamos con una linea en la que sólo escribimos un punto más enter.

QUIT
Una vez escrito el correo nos desconectamos del servidor con este comando.

Así, todo el proceso sería algo como:

```
telnet smtp.dominio.com 25

220 smtp.dominio.com Sendmail 4.1/Mork-1.0 ready at Sat, 26 Jul 00 04:26:46 EST

HELO midominioinventado.com

250 smtp.dominio.com  Hello  midominioinventado.com ( midominioinventado.com), pleased to meet you

MAIL FROM:<origen@dominio.com>

250 <origen@dominio.com>... Sender ok

RCPT TO: <midestion@dominio.com>

250 <midestino@dominio.com>... Recipient ok

DATA

354 Enter mail, end with "." on a line by itself

subject: correofalso

to: otrapersona@correo.com

Este correo es un ejemplo de correo falso, que claramente es falso porque de lo contrario seria muy autentico.

.
```

250 Mail accepted

QUIT

Así, los campos *subject*, *from* y *to* se escriben después del comado DATA en lineas separadas por un retorno de carro (un enter), pudiendo poner lo que queramos. Es así como podemos recibir un correo que aparentemente va dirigido a otras personas, basta con poner un campo diferente al real (campo RCPT) en el campo *To:.* Este campo lo leen los agentes de usuario y es como vemos, facilmente falsificable