

## **PRACTICA 7. Enviar mail anónimo usando telnet (Por HxC Mods-Adm)**

Imagino que todos conocéis el programa **Telnet**, incluso alguno de vosotros lo habréis usado en alguna ocasión. Ciertamente es una de esas utilidades que *vienen* con el Sistema Operativo y que a nadie le gusta porque carece de entorno gráfico y normalmente hay que escribir todo lo que se desea hacer en lugar de *coger el ratón y empezar a hacer clic por todas las ventanas* y controles que vemos.

Quizá esta sea la razón por la que todo el mundo se olvida de que existe la aplicación **Telnet**, no tiene *dibujitos*, sonidos, ni nada de eso que a todos los usuarios de Windows nos gusta, quienes tengáis experiencia en *Unix o Linux* estaréis más acostumbrados a olvidar el entorno gráfico y no os suponga un *trauma* dejar a un lado las *ventanitas*...

Bueno a lo que vamos, **Telnet** es un programa que se usa para conectarse a otro ordenador a través de un puerto. Hasta Windows 2000 dispone de una aplicación que se puede configurar como *Servidor Telnet*, muchos *routers, Firewalls, switches*, etc. pueden utilizar la conexión **telnet** para su configuración, aunque casi todos optamos por otro tipo de accesos (SMNP, HTTP, etc.) que siempre son más vistosas.

Otra vez vuelvo a hablar de los **puertos**, ¿Qué son? En una frase: Un puerto lógico es un vínculo que une dos ordenadores o aplicaciones para comunicarse entre ellas.

Los **puertos lógicos** en cuanto a su función son muy parecidos a los puertos físicos (COM,LPT,USB,...) sirven para lo mismo, **COMUNICARSE**.

El conjunto de protocolos que soporta TCP/IP utiliza **puertos lógicos** (a partir de ahora simplemente **puertos**) para establecer las sesiones de comunicación, a su vez, diferentes aplicaciones utilizan los protocolos para mostrar esa información de forma que los *humanos la entendamos*.

Existen protocolos muy conocidos asociados a puertos determinados, no varían, son usados por la mayoría de la gente del mismo modo, así entonces tenemos algunos muy comunes:

| Protocolo | Puerto | Aplicación                             |
|-----------|--------|----------------------------------------|
| http      | 80     | Navegadores                            |
| SMTP      | 25     | Servidores de correo o correo saliente |
| POP       | 110    | Servidores de correo o correo entrante |
| FTP       | 21     | Servidores de FTP                      |
| ....      | ....   | .....                                  |
| ....      | ....   | .....                                  |

Se pueden utilizar 65536 puertos, que pueden ser asociados respectivamente a las aplicaciones correspondientes y a los protocolos usados por las mismas.

**Telnet** utiliza por defecto el puerto 23 para conectarse a **Servidores Telnet**, cuando en nuestro navegador ponemos esos de <http://www.yahoo.es> estamos indicando a *IE* que acceda a un servidor llamado yahoo.es por el **puerto 80** y que nos muestre esa información dentro de la pantalla del navegador (si no le decimos lo contrario *IE* está preparado para dirigir las conexiones http al puerto 80, por eso no es preciso indicarlo), pero también podríamos haber escrito: <http://www.yahoo.es:80>

*¿Quiere decir esto que podemos usar cualquier puerto, cualquier protocolo y cualquier aplicación?*

**SÍ.** Lo que pasa es que, si a nuestro Servidor de páginas Web le ponemos a escuchar peticiones de páginas por el puerto 4590, sólo las personas que lo sepan podrían conectarse a él usando <http://www.yahoo.es:4590>

*¿Quiere decir esto que podemos usar cualquier aplicación para conectarnos a un servidor a través de un puerto?*

**SÍ.** Es perfectamente posible lo siguiente: telnet [www.yahoo.es](http://www.yahoo.es) 80, lo que ocurre es que por la “pantallita” del **telnet** no podemos ver la página web solicitada, por lo menos los contenidos activos, multimedia, etc. de la misma, pero si lo pruebas verás que la conexión se establece sin problemas, aunque no “sale” nada. ¿Y si pulsas 2 veces enter qué pasa? ¿y si escribes GET / HTTP /1.0 qué pasa?. Prueba y piensa.

Bien, como ya viste antes, los *servidores de correo utilizan los puertos 110 y 25* para que podamos recibir y enviar nuestros correos electrónicos utilizando los protocolos POP/POP3 y SMTP respectivamente. Como el correo puede utilizar muchos objetos, archivos adjuntos, sonidos, etc., y además queremos gestionar una agenda, bandejas de correo, etc., utilizamos un programa para el envío o la recepción de los mismos, en el caso de Windows lo normal es usar **Outlook o Outlook Express**.

Cuando usamos ese tipo de aplicaciones, indicamos a las mismas nuestra dirección mail y los servidores de entrada y salida que queremos usar, de forma que cuando enviamos un correo, siempre se incluye nuestra dirección mail en la misma.

*El arte de la chapuza* puede estar en indicar una dirección de correo inexistente en el momento de crear la cuenta de correo en **Outlook**, por ejemplo [et@micasa.es](mailto:et@micasa.es) para que cuando enviemos un mail a nuestros amigos, conocidos o colaboradores reciban ésta dirección en lugar de la real. Este *mal paso* por llamarlo de alguna manera, es fácilmente detectable si el destinatario edita las cabeceras del mail y examina el campo **Received**, tal como se explicó.

Por otra parte, es muy probable que ni siquiera el mail *falsificado* de esa forma llegue a su destino, por los motivos expuestos en el apartado 6.9 *Servidores de Correo*, si el servidor de correo es, por ejemplo wanadoo.es, el mail será rechazado puesto que el dominio micasa.es no pertenece a wanadoo, ni tampoco pertenece al ISP con el que estableciste la conexión a Internet, todo depende de si el administrador del Servidor de Correo que usas permite o no este tipo de envíos.

Vamos a usar **telnet** para enviar un mail verdadero (es decir cumpliendo las reglas del proveedor) para aprender como debemos utilizar los *comandos SMTP*, para ello vamos a suponer que nuestro verdadero servidor de correo saliente es mailhost.terra.es, que nuestra dirección mail es [ntmsa@terra.es](mailto:ntmsa@terra.es) y que la dirección mail del destinatario es [miempresa@ctv.es](mailto:miempresa@ctv.es), sólo tienes que sustituir el servidor smtp y tu dirección mail por las mías.

También necesitaremos conocer el conjunto de *comandos válidos para smtp*, aunque hay más de los que pongo a continuación, con estos será suficiente:

**HELO** → Saludar al *host* remoto  
**MAIL FROM:** → Dirección mail desde la que enviamos el mensaje, la nuestra.  
**RCPT TO:** → Dirección mail del destinatario, a quien deseamos enviar el correo.  
**DATA** → Texto del mensaje a enviar

No se te olvide poner los dos puntos (:) después de **From** y **To**, o no funcionará.

En muchos terminales **telnet**, cuando borramos un carácter y ponemos otro, porque nos equivocamos al escribir, el mandato no funciona aunque en la pantalla se vea bien escrito, ya sabes **NO TE EQUIVOQUES** al escribir o tendrás que teclear de nuevo el comando.

No todas las versiones de **telnet** son iguales, yo voy a usar la que viene instalada con Windows 2000, si usas 9x u otro cliente telnet con pocos cambios harás lo mismo.

## Foro de HackXcrack

---

Antes de empezar, veamos que comandos acepta **telnet**, para ello desde **Inicio-Ejecutar** escribe **telnet** y luego la palabra **help** en la ventana que se te haya mostrado



```
C:\WINNT\System32\telnet.exe
Microsoft (R) Windows 2000 (TM) versión 5.000 (Compilación 2195)
Cliente Telnet de Microsoft
Cliente Telnet Build 5.00.99201.1

El carácter de escape es "CTRL++"

Microsoft Telnet> help

Los comandos se puede abreviar. Los comandos permitidos son:

close           cierra la conexión actual
display        muestra los parámetros de visualización
open           conectarse a un sitio
quit           salir de telnet
set            establecer opciones (escriba 'set ?' para mostrar lista)
status        escribe la información de estado
unset         desactivar opciones (escriba 'unset ?' para mostrar lista)
?/help        muestra información de ayuda
Microsoft Telnet>
```

No es necesario activar el echo local ni establecer el tipo de terminal usado, pero por si acaso lo haremos, de ese forma podremos ver lo que escribimos en pantalla y usar vt100 como tipo de terminal.

Escribe en la pantalla **telnet**:

```
Set local_echo
Set term vt100
```

# Foro de HackXcrack

---

Ahora ya tenemos configurado correctamente el programa *telnet* para conectarnos a cualquier *host* que lo permita, sólo nos falta crear la conexión.

## Teclea lo siguiente:

*Open smtp.mailhost.com 25*

Si todo va bien conseguiremos la conexión con el **servidor smtp** y nos enviará algo parecido a esto:

*220 transition.my.com ESMTP Sendmail 8.11.6/8.11.6; Fri, 15 Nov 2002 01:47:08 +0100*

Observa que después de la orden *open* y nombre del servidor, se indicó el **puerto de conexión. 25**

**Escribimos:** *HELO localhost*

**Recibimos:** *220 transition.my.com Hello 193-152-151-115.uc.nombres.ttd.es [193.152.151.115]*

Como verás el servidor nos saluda y nos muestra **NUESTRA DIRECCIÓN IP**

**Escribimos:** *MAIL FROM:ntmsa@terra.es*

**Recibimos:** *250 <ntmsa@terra.es> SENDER OK*

**Escribimos:** *RCPT TO:miempresa@ctv.es*

**Recibimos:** *250 RECIPIENT [miempresa@ctv.es](mailto:miempresa@ctv.es) OK*

**Escribimos:** *DATA*

**Recibimos:** *354 Send data ending with <CTRLF>.<CTRLF>*

**Escribimos:** *Hola, aquí estamos, enviando mail por Telnet. Bye.*

•

**Recibimos:** *Message Received: H5L8GEE00.D1W*

**Escribimos:** *quit*

## A saber:

Los mensajes recibidos desde el servidor pueden cambiar (depende del servidor y de su configuración), lo que debe ser idéntico son los números que los preceden (250, 354, ...)

Una vez terminado de escribir el texto del mensaje después del comando DATA debemos terminar con un punto (.) como único carácter de la línea, en el ejemplo he puesto un punto **muy gordo** para que lo veas.

Podemos escribir en minúsculas o mayúsculas, es indiferente.

Bueno no es muy elegante pero **FUNCIONA**, podemos enriquecer un poco el mensaje, por ejemplo después de escribir DATA y pulsar enter podríamos haber escrito esto en su lugar:

```
DATA
FROM:ntmsa.terra.es
TO:miempresa@ctv.es
SUBJECT:Prueba de correo por Telnet
Aquí va el texto del mensaje, bla, bla, bla, ....
```

Incluso podemos adjuntar archivos, solicitar respuestas, establecer prioridades, etc. pero para eso ya tenemos Outlook ¿no?

*¿Qué pasaría si hubiésemos enviado esto?*

**Escribimos:** *HELO QuepasasoyET*

**Recibiremos:** *220 transition.my.com Hello 193-152-151-115.uc.nombres.ttd.es [193.152.151.115]*

**Escribimos:** *MAIL FROM:et@micasa.net*

**Recibimos:** *250 <et@micasa.net> SENDER OK*

**Escribimos:** *RCPT TO:miempresa@ctv.es*

**Recibimos:** *250 RECIPIENT [miempresa@ctv.es](mailto:miempresa@ctv.es) OK*

**Escribimos:** *DATA*

**Recibimos:** *354 Send data ending with <CTRLF>.<CTRLF>*

**Escribimos:** *Hola, aquí estamos, enviando mail desde Marte, por Telnet. Bye.*

•

**Recibimos:** *Message Received: H5L8GEE00.D1W*

**Escribimos:** *quit*

Pues efectivamente, **SE ENVIA CORRECTAMENTE** y el destinatario recibirá un MAIL de [ET@micasa.net](mailto:ET@micasa.net), aunque si examina las cabeceras del correo descubrirá la IP o en su defecto el servidor real del correo, sabrá que se envió desde TERRA y si en lugar de este simpático mensaje y remitente, *te pasas*, y adviertes de una inspección de hacienda a tu jefe y lo firmas como la agencia tributaria, te puedes jugar el puesto de trabajo *si la broma* no le gusta, no te quiero decir nada si lo que envías son amenazas, chantajes u otro tipo de burradas, vamos que lo único que has falsificado es el remitente que mostrará **Outlook** al recibir el mensaje, *para lamercillos*.

Además, tiene *algo de truco*. Por que si en lugar de utilizar el servidor de Terra (que en el ejemplo es el mismo que se usó en la conexión) utilizamos otro cualquiera (por ejemplo smtp3.looptele.com), cuando se escribe la línea:

*RCPT TO:miempresa@ctv.es*

**Recibiremos:** *550 Relaying to <[miempresa@ctv.es](mailto:miempresa@ctv.es)> prohibited by administrator*

**¿Por qué?**

Por lo explicado en varias ocasiones anteriormente, la IP o el dominio de conexión no pertenece al servidor de correo usado, ni por supuesto la dirección [et@micasa.net](mailto:et@micasa.net) es válida para el mismo.

Por tanto, no podemos enviar correos “falsificados” o sin falsificar mediante servidores que autentifican la cuenta POP del usuario que accede al servidor SMTP, de lo contrario cualquiera podría usarlo para “abusar” del envío de correos, además por supuesto, **el servidor registra TODAS las conexiones**, con lo que si envías 5.000 correos a *alguien* te descubrirán al instante.

Hasta hace poco tiempo casi todos los servidores de correo permitían el envío de correos sin verificar todo lo dicho anteriormente, pero debido al “*gran éxito*” de los **SPAM** y **mail bombing** se tomaron las medidas pertinentes.

Entonces, ¿No es posible?. Claro que sí. Lo único que necesitamos es encontrar un servidor que lo permita, o montarnos uno propio, añadiendo el programa *telnet.exe* a la ventana **de SocksCap** para que cuando se establezca la conexión vía **telnet** se haga a través de la **cadena de Proxys anónimos** que tengamos configurados **en SocksChain**.

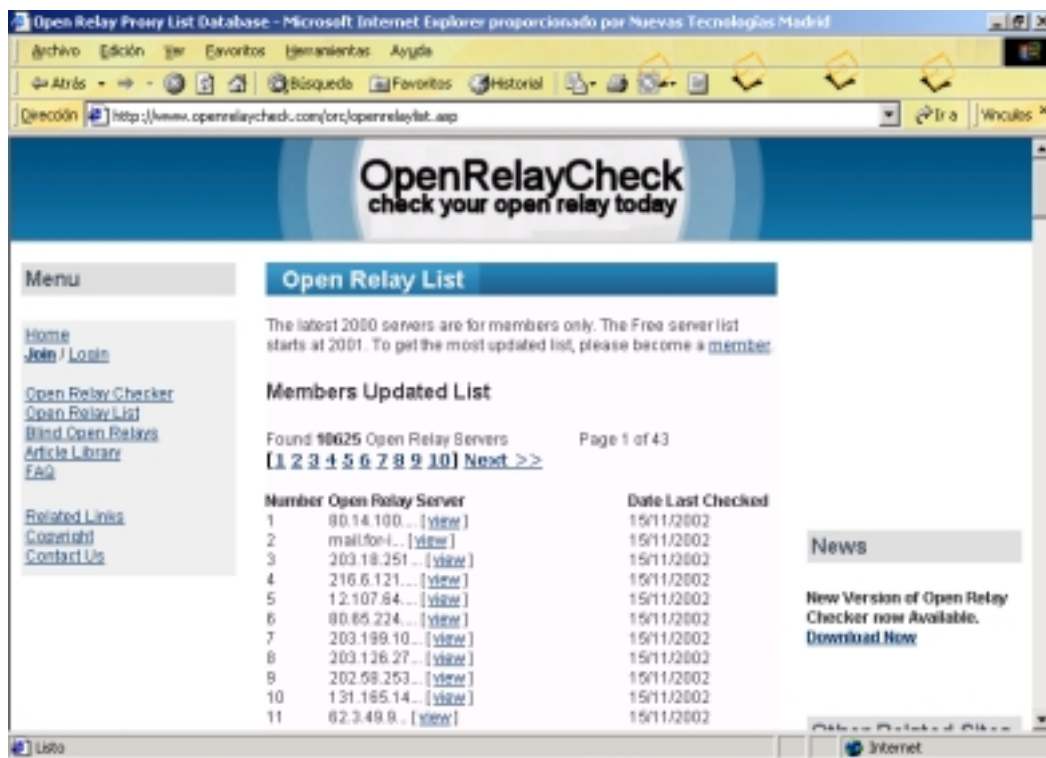
Para encontrar un servidor que permita **OPEN RELAY** (este es el nombre técnico de lo que buscamos) podemos usar un **Remailer** desde la Web o mediante alguna aplicación como **Private Idaho**.

Fíjate que es **importante esconder la IP** antes de utilizar el “*servidor de correo anónimo*” porque estos servidores lo único que hacen es cambiar las cabeceras del correo por “*otras suyas*” pero no te quepa la menor duda que **guardarán el registro de tu IP durante años**, si alguna autoridad lo solicita y te buscan, te encontrarán tarde o temprano. Si fuiste precavido y te escondiste *desde unos cuantos Proxys*, será más tarde que temprano (puede que nunca), a menos que *te pases tres pueblos con el destinatario*.

Bueno, sólo me hace falta encontrar “*ese servidor*” y si no guarda los registros de acceso es LA LECHE, por eso lo de “*montarnos uno propio*”.

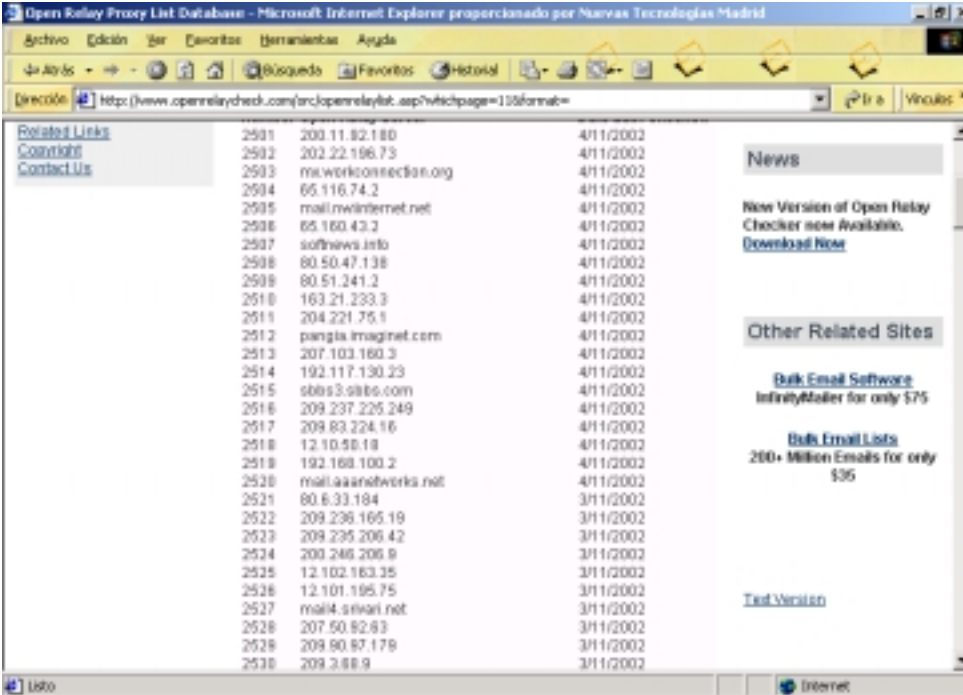
Si te cuento esto no es para que empieces a buscar por Internet como un loco y enviar cientos de e-mail a *todos los que te caen mal*, te lo digo, por que es perfectamente posible que te “*cuelen*” un servidor smtp en tu red, en tu PC, en tu mismo servidor y que lo usen para abusar del envío de correo, mail bombing, actividades delictivas (pornografía infantil, terrorismo, etc) **sin que te des cuenta**, de forma que cuando la policía busque y encuentre a alguien, ése **SERAS TU**. ¿A que ahora ya no te parece tan “*divertido*” y estas pensando lo que se te puede venir encima?

La mejor lista de servidores que admiten **OPEN RELAY** y que cambiarán las cabeceras de los correos enviados la encontrarás en: <http://www.openrelaycheck.com/orc/openrelaylist.asp> esta lista se actualiza **DIARIAMENTE**, si quieres disponer de la lista completa hay que hacerse miembro, esto supone unos **30\$ CADA MES**.



## Foro de HackXcrack

Como verás, no se muestran las direcciones completas, eso es sólo para “*abonados*”, si te conformas con algunos menos, pulsa sobre en *enlace Next >>* de esta misma página, entonces se mostrarán los servidores *OPEN RELAY* más anticuados



| IP Address                 | Date      |
|----------------------------|-----------|
| 2501 200.11.82.180         | 4/11/2002 |
| 2502 202.22.186.73         | 4/11/2002 |
| 2503 mx.workconnection.org | 4/11/2002 |
| 2504 65.116.74.2           | 4/11/2002 |
| 2505 mail.mvinternet.net   | 4/11/2002 |
| 2506 65.160.43.2           | 4/11/2002 |
| 2507 softnews.info         | 4/11/2002 |
| 2508 80.50.47.138          | 4/11/2002 |
| 2509 80.51.241.2           | 4/11/2002 |
| 2510 163.21.233.3          | 4/11/2002 |
| 2511 204.221.75.1          | 4/11/2002 |
| 2512 pangla.imaginet.com   | 4/11/2002 |
| 2513 207.103.160.3         | 4/11/2002 |
| 2514 192.117.130.23        | 4/11/2002 |
| 2515 sbbs3.snlbs.com       | 4/11/2002 |
| 2516 209.237.225.249       | 4/11/2002 |
| 2517 209.83.224.16         | 4/11/2002 |
| 2518 12.10.58.18           | 4/11/2002 |
| 2519 192.168.100.2         | 4/11/2002 |
| 2520 mail.aanetworks.net   | 4/11/2002 |
| 2521 80.6.33.184           | 3/11/2002 |
| 2522 209.236.165.19        | 3/11/2002 |
| 2523 209.235.206.42        | 3/11/2002 |
| 2524 200.246.206.9         | 3/11/2002 |
| 2525 12.102.163.35         | 3/11/2002 |
| 2526 12.101.195.75         | 3/11/2002 |
| 2527 mail4.sivari.net      | 3/11/2002 |
| 2528 207.50.82.63          | 3/11/2002 |
| 2529 209.80.87.179         | 3/11/2002 |
| 2530 209.3.88.9            | 3/11/2002 |

### NOTAS INTERESANTES

Muchos *ISP* consultan las listas *OPEN RELAY* y actualizan sus *Firewalls* con estas direcciones para impedir la entrada o salida de correos que usen las mismas.

Muchos de estos servidores *OPEN RELAY* no funcionan todo el día, hay algunos que dejan de funcionar a las pocas horas de ponerse en funcionamiento.

**No todos estos servidores son anónimos**, si usas alguno, antes de nada envíate correo a ti mismo para verificarlo.

Yo **no me fiaría NADA** de la *inocencia* de estos servidores, no los uses para la recepción-envío de tus correos “*sanos*”, guarden o no guarden los “*logs*”, utilices o no utilices IP anónima, no te quepa la más mínima duda que si al operador del servidor se le antoja leer tu correo lo hará, incluso lo puede manipularlo, enviarlo a otra dirección además de la que tu pusiste, **bufff**.

Bueno también pueden hacer esto nuestros *ISP*, ¿verdad?, Pues claro, pero se les supone “*comprometidos*” con quien les paga, tienen un compromiso económico y moral con el cliente ¿no?

Aun así si te empeñas en usar **remailers**, **Open Relay**, etc., utiliza programas de encriptación de correo como *PGP*).

Para terminar, una vez descubiertos los *OPEN RELAY*, también podemos usar ese servidor dentro de nuestro *Outlook* y olvidarnos de *Telnet*, no se te olvide que los destinatarios no podrán contestar a tu dirección si la falseas, bueno la verdad es que sí se puede, incluso sin que el usuario se entere, pero esa es otra guerra que sí que se escapa al contenido de este texto, investiga, piensa, estudia (mucho) y suerte.

*Private Idaho* es más que un **remailer**, utiliza *PGP*, puede usar más de un servidor anónimo de correo a la vez, encadenándolos como hacia *SocksChain* con los *Proxys*, puede comprobar el estado de esos servidores, su velocidad, la fiabilidad de los envíos, examina cabeceras, las exporta, importa, permite navegar por la web anónimamente, etc., etc., etc.