Ocultación de IPs

Este texto es una explicación para novatos(abstenerse gurus)de diversos términos y técnicas que nos sirven para ocultar nuestra dirección ip

1. Introducción
2. Proxys
3. Wingates
4. Bouncer
5. IP-Spoofing

1- Introducción

Seguro que habéis iodo hablar o elido en algún texto cosas como un Bouncer un Wingate o un Proxy pero es fácil que no lo tengáis muy claro o que tengáis alguna duda, porque estos términos se confunden bastante amenudo
Antes de empezar quiero que entendáis lo que realmente significa ocultar vuestra IP. Pues bien en Internet vuestra IP es lo mismo que en la vida real pueden ser tus huellas dactilares, tu DNI o código genético, sin estos datos podrías hacer "todo" lo que quisieras. Si lo piensas podrías decir que eres "invisible", pues en Internet lo mismo, si "no tienes IP" eres un ordenador fantasma

2- Proxys

Bien voy explicar lo que es un Proxy solo para los más novatos porque cualquiera que lea esto creo que ya lo tendría que saber:-P Cuando hablamos de una red siempre pensamos en un grupo mas o menos grande de ordenadores conectados entre sí, pero esto no funciona solamente así tiene que tener una determinada estructura, necesita lo que se llama un servidor, que no es otra cosa que una maquina con unas mejores prestaciones (aunque no siempre sea así) y que usa un sistema operativo con distintos usuarios

```
(server)        |------ equipo B
equipo A        |------ equipo C
                |------ equipo D
                |------ equipo E
```

Bien pues cuando nuestra red necesita tener salida al exterior, ya sea a otra red local o a Internet, decimos que es un servidor Proxy, todos los datos que lleguen de fuera de nuestra red tienen que pasar por esta maquina su función entonces seria la de un router(esto no es así exactamente, que no me mate nadie xD), es entonces cuando tienen utilidad palabras como ***wingate o bouncer***

Existen muchos tipos de servidores proxy, sin ir mas lejos vuestro proveedor de Internet funciona como un server proxy y vosotros formáis parte de su red, solo que a diferencia de una pequeña red local, el server de vuestro ISP tiene que asignar una ip distinta cada vez que accedéis a el(entre otras diferencias). En una red local (LAN) las ips suelen estar predefinidas.

3- Wingates

Wingate es un programa que funciona en Win 95/98 y NT. Este programa lo usan los servers proxys para dirigir el trafico circula por una red local es lo que hace que realice funciones similares a un router
Realmente todo el software que hace estas funciones es conocido con el nombre de wingate pero existen muchos programas que realizan esta función cada uno con su propio nombre pero el más común es el que realmente se llama wingate (mas adelante explicare como diferenciar los distintos wingates)Bien pues estos programas no es que sean muy difíciles de configurar pero amenudo los admis se dejan muchas puertas abiertas que el programa trae por defecto, sobre todo las versiones mas antiguas y sin parchear, las cuales permiten acceso telnet al puerto 23 sin pedir pass (jejeje :))
Con estos datos podemos usar el wingate para muchas cosas... cada uno... Podemos acceder al IRC para lo que solo necesitamos algunos comandos del mIRC

1) /server wiley231h038.roadrunner.nf.net 23
WinGate>NICK Aule
Connecting to host NICK...Host name lookup for 'NICK' failed
USER aule "pss" "wiley231h038.roadrunner.nf.net" The truth is out there...
Connecting to host USER aule "pss" "wiley231h038.roadrunner.nf.net"
...Host name lookup for 'USER aule "pss"
"wiley231h038.roadrunner.nf.net" ' failed

2) /raw dubhe.irc-hispano.org 6667
-> Server: dubhe.irc-hispano.org 6667
Connecting to host dubhe.irc-hispano.org...Connected

3) /raw nick Aule

-> Server: nick Aule

PING? PONG!

4) /raw user taigual kemasda el@mio.com ikepasa

-> Server: user taigual kemasda el@mio.com ikepasa

Welcome to the Internet Relay Network Aule
Your host is dubhe.irc-hispano.org[dubhe.acn.es], running version
This server was created Mon Aug 16 1999 at 00:57:47 EDT

dubhe.irc-hispano.org u2.10.06.24.(nullchan) dioswkg biklmnopstv

Bueno y ya tamos dentro del irc usando un wingate :-) también se puede usar el comando QUOTE en lugar de RAW y los puntos 3 y 4 pueden ir en orden contrario. Si te sientes intrigado por que es lo que has hecho hazte ***un whois*** y seguro que lo comprenderás.

También existen lo que son los socks que permiten el acceso al IRC a través de la maquina Wingate pero por el puerto 1080. Con del mIRC su uso es de lo más sencillo no tienes mas que indicarle al mIRC que usas a la maquina con el Wingate como un firewall y el puerto que usas para acceder a el, el 1080.
Esto se hace en la ventana del setup del mIRC en la pestaña que pone firewall, hay distintas casillas, en la del host ponemos la dirección del Wingate, puerto 1080 que ya viene por defecto, y pulsamos los socks,bueno... y conectar con el server de IRC como haces siempre.
La diferencia de hacerlo así es que si realizamos un DCC con otro usuario este va conocer nuestra autentica IP
Si eres un poco inteligente entenderás que con esto te puedes saltar cosas como un G-LINE y un KILL o bans en canales donde no te has portado bien :P
Además si alguien te esta intentando nukear lo tiene mucho más difícil porque intentara nukear al server del wingate no tu ordenador.
Decir por ultimo del wingate en el IRC, que en la red hispano.org el uso de wingates esta en vais de extinción :((pero esto no es el tema de este txt Bueno sigamos con nuestro amigo Wingate como dije antes el programa abre el puerto 23 y permite acceder a el sin pedirnos pass, con lo cual lo podemos usar para saltar a otras maquinas. Esto es lo que seria hacer Bouncing pero lo explico en este apartado por que es atraves de un wingate.
Como dije antes no todos los Proxys usan el mismo software, existen distintos programas que usan estos servers cada uno tiene sus propios fallos de seguridad, pero vamos a diferenciar que tipo de soft se trata:

- Winproxy

realizamos un telnet al server

Trying 195.76.206.157...
Connected to 195.76.206.157.
Escape character is '^]'.
Enter : <host> [port] :
---

para estar seguros conectamos al ftp (puerto 21)

Connected to 195.76.206.157.
220 WinProxy FTP Gateway ready, enter username@host[:port]
---

esta claro que es un winproxy

- Wingate

Esta claro, el conocido Wingate.

Las ultimas versiones vienen parcheadas para que no se pueda acceder desde el exterior

Realizamos un telnet y vemos clarito el prompt

```
--------------------------------------------------
Trying 195.76.206.62...
Connected to 195.76.206.62.
Escape character is '^]'.
WinGate>
--------------------------------------------------
```

FTP

```
--------------------------------------------------
Connected to 195.76.206.62.
220 WinGate V1.3 FTP Gateway ready, enter user@host[:port]
--------------------------------------------------
```

sed buenos.... si podeis :-P

- S-Proxy

Este es soft espa¤ol!

Telnet

```
--------------------------------------------------
Trying 194.75.196.77...
Connected to 194.75.196.77.
Escape character is '^]'.
Host:
--------------------------------------------------
```

Para reconocerlo correctamente **FTP**

```
--------------------------------------------------
Connected to 194.75.196.77.
220 S-Proxy preparado para recibir.
--------------------------------------------------
```

Cuando realizamos telnet solo nos deja hacerlo al puerto 23 lo que aumenta su seguridad pero nos permite Bouncear igualmente.

Creo que ya sabeis que es lo que se puede hacer con esto.. al hacer un telnet al wingate podemos saltar a cualquier otra maquina

Wingate>mi.vecino.es 23

La ventaja es clara... no nos conectamos a la maquina de mi.vecino.es desde nuestro ordenador si no desde el del wingate quedando en la maquina de mi.vecino.es la IP del wingate y no la nuestra. Pero no todo es tan fácil en la maquina del wingate pueden quedar los logs así que andar con cuidado.

4- Bouncer

Como la técnica explicada en el apartado anterior existe alguna otra manera de hacer bouncing. Creo que ya entendéis lo que es bouncing pero bueno....

mi maquina Bouncer objetivo
A ----------> B ----------> C

El bouncer puede ser como el caso anterior un wingate mal configurado o un programa colocado en la maquina B por una mano un tanto "inocente" Bouncing se puede hacer en maquinas Unix haciendo correr un daemond que nosotros hallamos colocado (ojo con el root!) solo le indicaremos el puerto por el que nosotros entraremos y la maquina y puerto al que "saltamos" Esto se puede usar para conectarse al IRC de forma mas segura o para otros menesteres.

Para los usuarios Win deciros que existen distintos programas Win para hacer Bouncer, muchos de ellos los traen los scripts de IRC como el WANIRC del 7th sphere explicado por Qva$aR en su txt "como saltarse una k-line" en http://www.undersec.com o el famoso y conocido IRCap de GSi que incorpora un bouncer hecho por el (los que sepais algo de scripting podeis mirar y haceros uno a vuestro gusto). Existen mas programas de este tipo como el WinBouncer muy faciles de configurar y que podeis usar para cualquier cosa solo teneis que indicar los puertos y el host Muchos direis que como utilizo yo un Bouncer si no tengo ninguna shell y solo el PC de mi habitacion... pues para saltarse bans o jugar en el IRC podeis hacerlo con algun inconsciente amiguete que os deje usar su ip :)
Si sois algo mas avispados o quereis hacer cosas mas interesantes en el hacking podeis colocarlo en ordenatas de vuestro instituto, en la academia donde estudiais, a ese pardillo que el otro dia a la noche estaba infectado con el netbus etc etc ...

5- IP-Spoofing

Bueno llegamos a la parte mas difícil del texto seguro que la mayoría de vosotros habéis oído hablar de esta técnica o tenéis idea de en que consiste pero no lo tenéis muy claro. Veamos el IP-Spoofing es una técnica bastante difícil y compleja que requiere bastantes conocimientos sobre todo del protocolo TCP-IP
Explicándolo a la ligera podría decir que el IP-Spoofing consiste en engañar a una maquina (host A) haciéndole creer que somos otra maquina (host B) que en realidad no somos

acceso
host B -------> host A
sin pass

Esta técnica se basa en el procedimiento usado (mal usado) en algunos sistemas de permitir el acceso sin una comprobación a través de contraseña y utilizando la confianza en las direcciones IP
El server A tiene depositada confianza en el server B (trust host), conoce la IP de este y no pide contraseña de entrada a su sistema desde esa maquina
Supongo que ya iréis cogiendo la idea no??? Para realizar esta técnica es necesario tener privilegios de Root desde la maquina que se realiza el ataque. Además hay que tener en cuenta una cosa que os puede pasar y que es muy importante, cuando vosotros realizáis el ataque modificáis los paquetes de datos cambiando en estos vuestra dirección IP y usando la del Trust host (esto no se hace "a mano" lo realiza un software especifico para esta tarea, seguid leyendo) debido a esto las respuestas que la maquina objetivo mande a esa transmisión TCP-IP no las recibiréis vosotros sino el trust host pero no os preocupéis por esto porque serán ignoradas al no haber el realizado la conexión. El problema viene de que teneis que intuir las respuestas que manda y tb el tiempo para realizar el siguiente envío de datos esto dependerá de la pericia de cada uno de vosotros.
Había pensado incluir el código de un programa de IP-spoofing pero os lo dejo para vosotros porque la mayoría son mas grandes que todo este documento, de todas maneras en **http://www.rootshell.org/** podéis encontrar cientos y para multitud de sistemas operativos, solo buscad por la palabra "spoof"
Otro de los problemas con lo que os encontrareis es localizar el Trust host de la maquina que queréis atacar (si es que lo tiene!) y el momento de realizar el ataque porque si entre las dos maquinas están realizando una comunicación es imposible que vosotros os coléis en medio. Lo que debéis de hacer es cortar el trafico del trust host y así poder realizar vosotros la conexión, esto se puede hacer de distintas maneras, procurad que no cante mucho, mirar cosas del protocolo TCP-IP,(TCP SYN flooding puede ser buena manera)
Una vez que tengáis controlado todo el proceso es decir tengais la maquina objetivo el trust host y os halláis asegurado que esta no reciba trafico TCP-IP
Procedéis al ataque IP-Spoofing pero recordar que no recibiréis respuestas por parte de la maquina objetivo.
Bueno comentaros también la existencia de algún programa para Win 95/98 que utilizan su propio conjunto de instrucciones TCP (no el paquete de Win) realizan Ip-Spoofing uno de estos programas es el **Aggressor Exploid**, lo podeis encontrar en

http://www.aggressor.net con este programa además de spoofear vuestra Ip también podreis realizar otros ataques pero sin tener relación con lo que explique del Trust host que es la principal aplicación del IP-Spoofing

Existen otros programas que también spoofea la IP pero de dudosa efectividad y casi todos orientados al IRC "cambian" vuestra IP y hasta el nombre de vuestro host (similar al DNS-inject) estos programas son como un Bouncer pero sin la necesidad de usar una maquina puente con el server de IRC (difícil de realizar no?? al menos el cambio de IP desde Win)

Con el DNS-inject conseguis que en vez de conectaros asi:

*** LuKaS (~lukas@ctv21225137015.ctv.es) has joined #sexo

saldria esto otro

*** LuKaS (~lukas@mi.polla.es.la.mas.grande) has joined #sexo

mola??? :) algunos programas consiguen esto ultimo solo sin spoofear vuestra IP, otros hacen las dos cosas, hay muchas posibilidades, estos programas
orientados al spoof en el IRC suelen venir en scripts asi que ya sabeis, si quereis provar si de verdad funcionan.....downdload RLz!

Todo lo explicado en este texto es con fines educativos, el autor no es responsable del mal uso de lo que aqui se cuenta.

Este txt es de libre distribución siempre que no se altere el nombre de su autor

Agradecimientos a M|Gel,Craig,aptc,y los que me dejo, por aguantarme :)

Para cualquier duda, sugerencia, critica.....
Búscame en el IRC-Hispano.org (www.irc-hispano.org) mi nick es Aule tb por mail a aule@mixmail.com

Open your eyes! Open your mind!!
By Aule (c) 1999