UNDERCODE

Taller: Malwares

Tema Principal: Troyanos Parte II

Practica adicional

Tutor:

ANTRAX

Temas:

- NO-IP
- Puertos
- Infeccion remota

..Mas

DISEÑADO POR HAZTOR

Tema central: Troyanos Parte II

Temas a tratar:

NO-IP

Puertos

Infección Remota

Autor: ANTRAX

Contacto: antrax.dc0de@gmail.com

Hola a todos, en esta entrega seguiremos con troyanos, solamente que orientadas a la infección remota.

NO-IP

Lo primero que haremos, será crearnos una DNS en NO-IP. No se si recordaran que en la entrega anterior cuando hablamos de autoinfección colocamos 127.0.0.1… en este caso lo que haremos será reemplazar esa IP, por una NO-IP.

Primero explicare un poco lo que hace y que es lo que es la NO-IP…

Vamos a empezar desde el principio para que todos tengan en claro y que no hayan dudas.

IP Local: 127.0.0.1 (Es la IP que tiene la PC como local).

IP Privada: Es la IP que se le asigna a la PC dentro de una RED LOCAL o RED LAN.

IP Publica: Es la IP que se le asigna a una PC cada vez que entra a Internet.

NO-IP: Es una suplantación a la IP Publica.

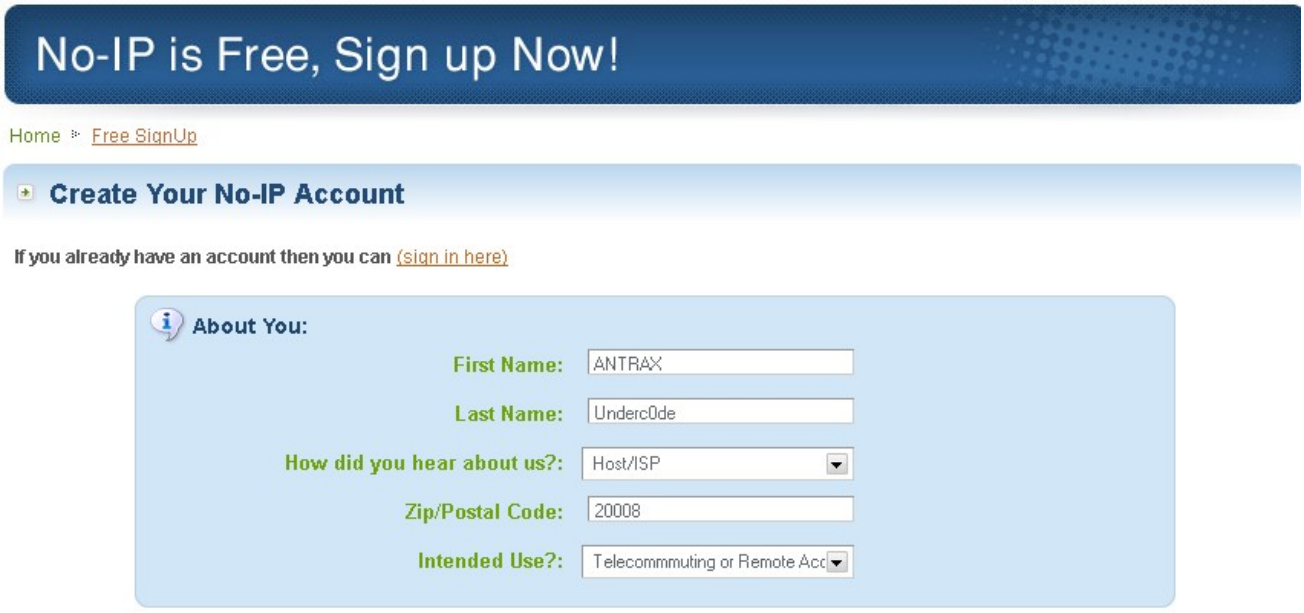
¿Por que usamos NO-IP?

Bueno, es una pregunta muy sencilla de responder. Como bien dijimos antes, la IP Publica es una IP que se le da a una PC cada vez que entra a internet. Lo malo de esto, es que cada vez que entramos a internet tenemos una distinta. Entonces si configuramos nuestro server con la IP Publica que tenemos, a la próxima vez que entremos a internet, nuestra IP cambiara y perderemos a todos nuestros remotos infectados.

Con la NO-IP, tendremos algo fijo y no perderemos los remotos.

Para entenderlo mejor, lo pondremos en práctica.

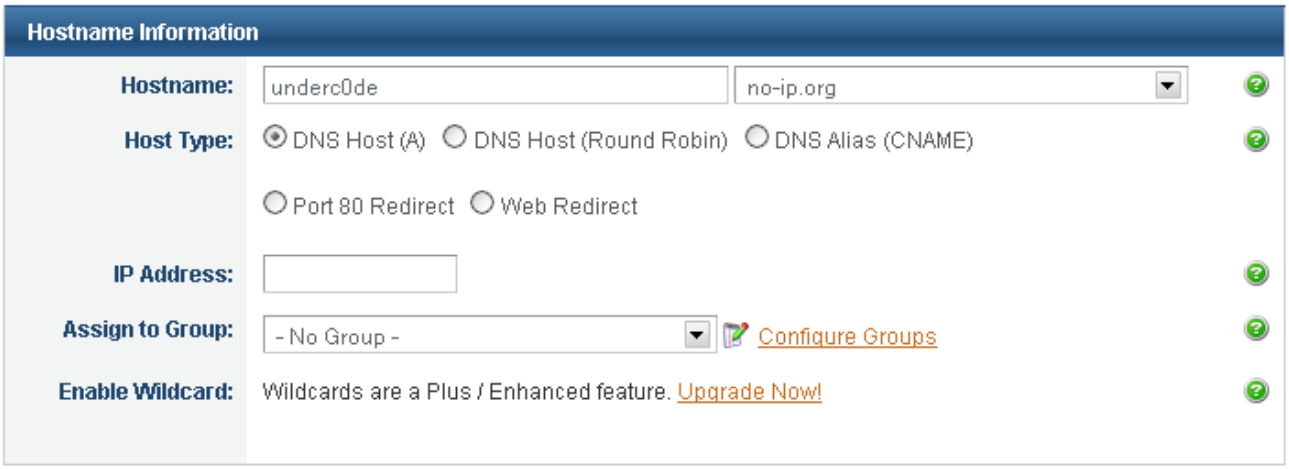
Comenzaremos creando una NO-IP. Entramos a www.no-ip.com y nos registramos.



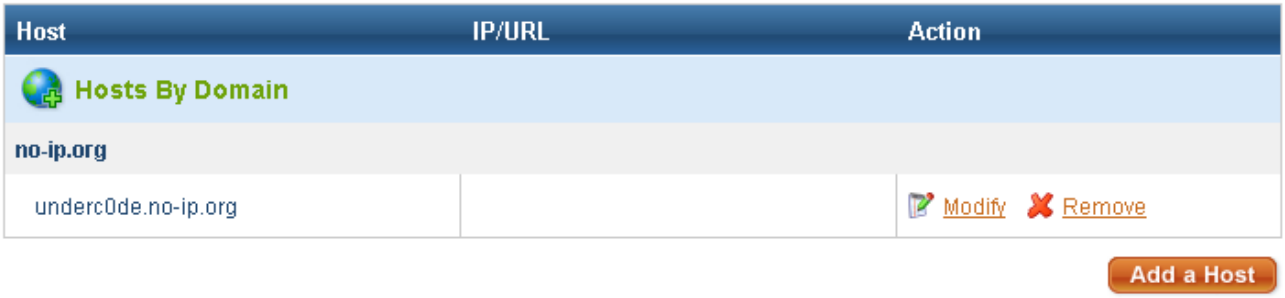
Llenamos todos los campos y nos registramos.

Luego nos llegara un mail para verificar la cuenta, la activamos y entramos con nuestra cuenta. Una vez que estemos dentro de nuestro panel damos en Add a Host

Ahora colocamos un nombre en Hostname, el resto lo dejamos igual. Pueden cambiarle el complemento al dominio, en mi caso puse no-ip.org, pero hay muchos mas.



Presionamos el botón Create Host que está debajo del cuadro y listo!

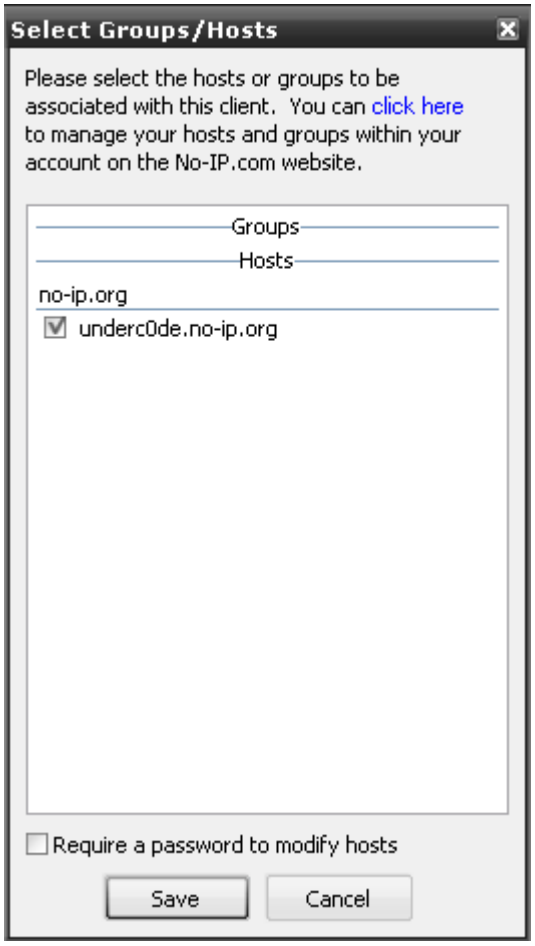


Como pueden ver ya tengo mi NO-IP. Y esta es la que usare a la hora de configurar mi troyano.

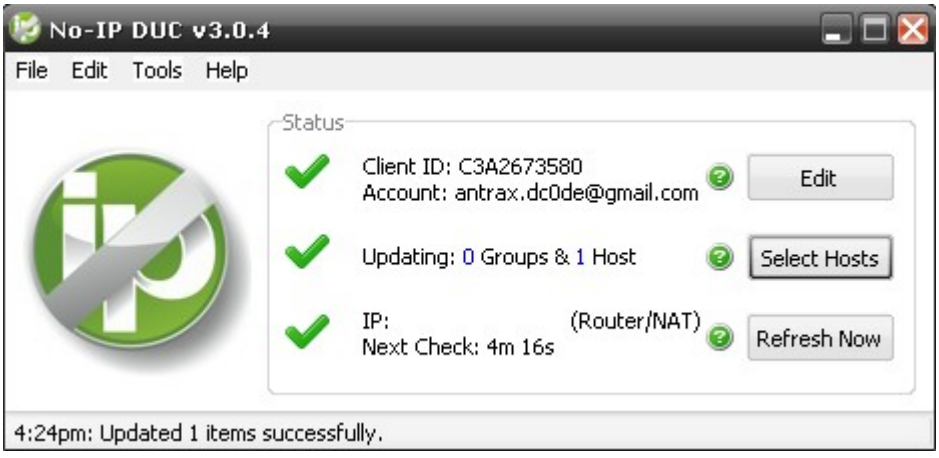
Ahora debemos descargar un programa llamado DUC. Es el que actualizara nuestra NO-IP con la IP Publica que tengamos.

Lo podemos descargar desde la misma página del no-ip.

Seleccionamos nuestro sistema operativo y descargamos. Seguido a esto lo instalamos y nos logueamos.



Seleccionamos nuestra NO-IP



Y deberíamos tener algo como en la imagen. (Los tres tildes en verde)

Si han llegado hasta acá, y tienen los tres tildes en verde, es porque han hecho todo a la perfección, de lo contrario, deben haber hecho algún paso mal.

Para verificar si funciona correctamente, le pedimos a algún amigo que le haga ping a nuestra NO-IP y ver si responde tirando nuestra IP.

Recuerden que el amigo, debe estar fuera de nuestra red.

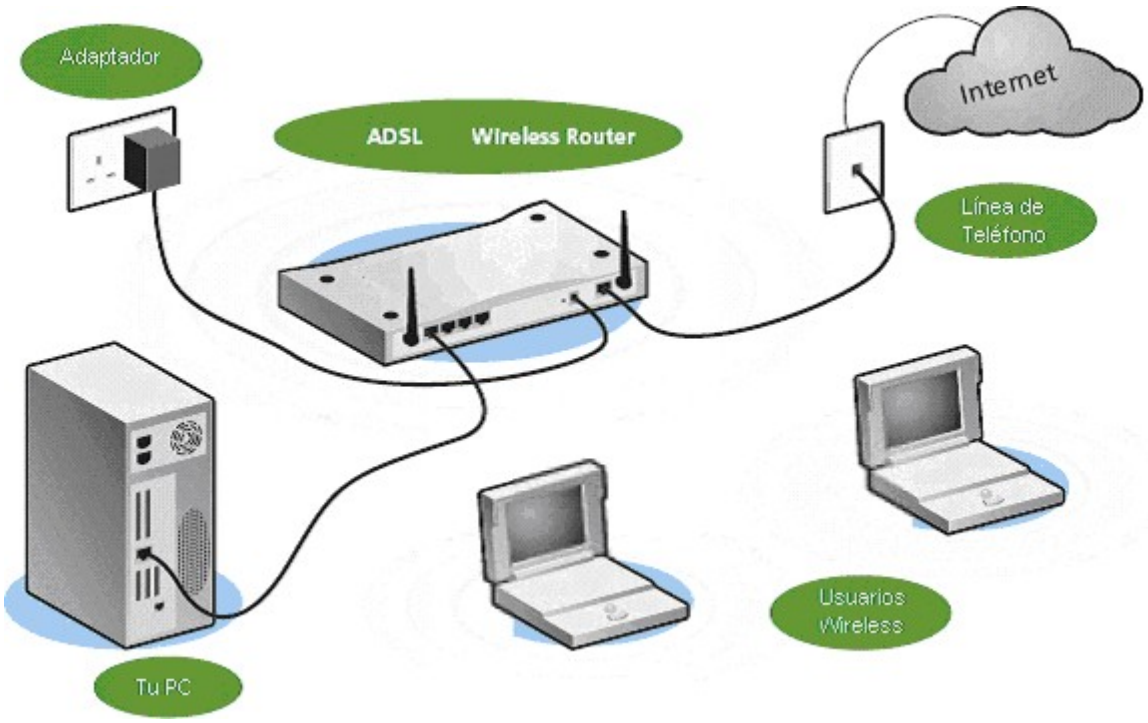
Debe entrar a la consola y teclear: “ping undercode.no-ip.org” (Recuerden pasarle su NO-IP, este es un ejemplo de cómo sería con la mía)

PUERTOS

Lo otro que nos queda para que nuestro troyano conecte de forma remota, es abrir un puerto en nuestro router (si es que tenemos router) para lo que tienen modem, no hace falta que hagan este paso.

Voy a explicar porque motivo debe abrirse un puerto.

La mayoría de nosotros tenemos algo como la siguiente imagen:



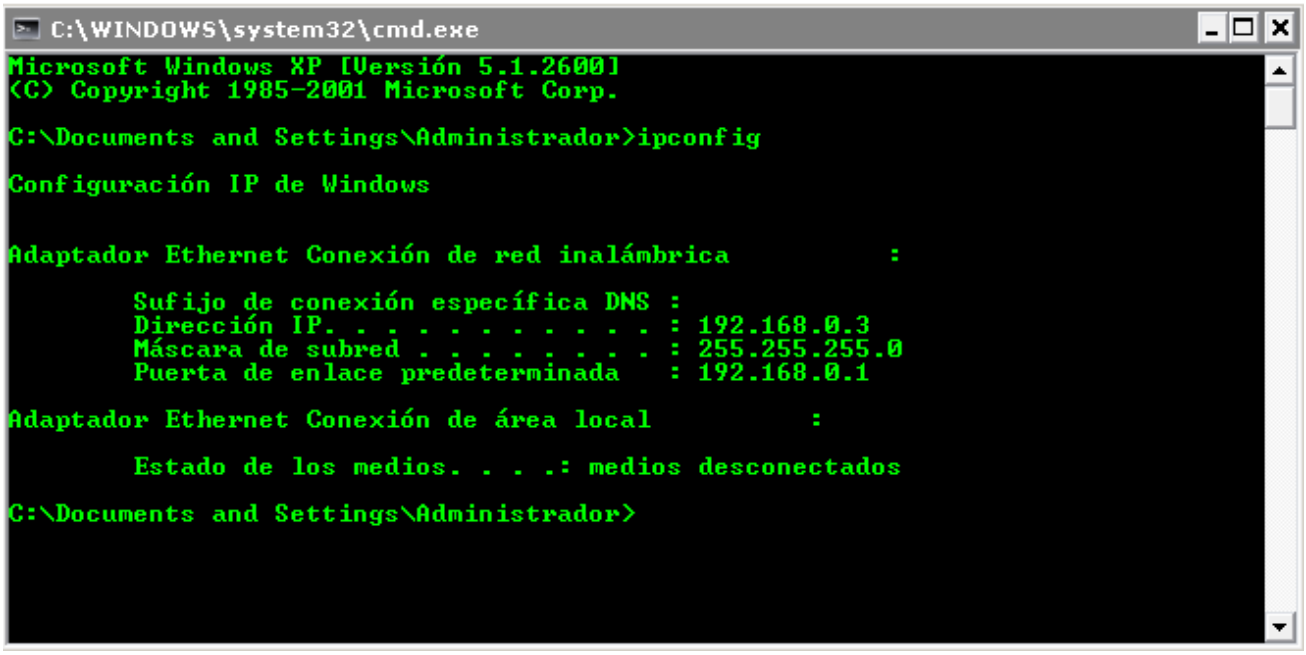
De la línea telefónica o desde el modem, va al router, el cual se encarga de distribuirlo a la PC, ya sea por Wireless o cableado.

El router bloquea varios puertos, y es por eso que necesitan ser abiertos para poder salir a internet.

Lo que haremos será entrar a la configuración del router y abrir el puerto.

Para saber la IP del router, debemos ir a INICIO > EJECUTAR > CMD

Se nos abrirá la consola de comandos y escribimos: **ipconfig**



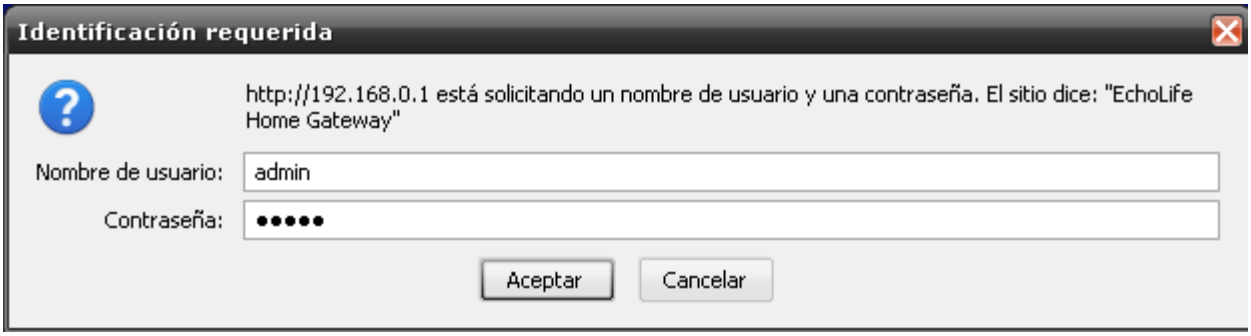
Bueno, acá debemos tener en cuenta dos cosas importantes, La Dirección IP y la Puerta de enlace predeterminada.

La Dirección IP es nuestra IP Privada que como vimos más arriba, es la IP que tenemos en la RED LAN.

Y la puerta de enlace predeterminada es la IP del Router. Teniendo estos datos, ya podemos seguir abriendo los puertos.

Abrimos el navegador de internet y escribimos la IP del **router**.

Una vez dentro, lo más probable es que nos pida user y pass…



Todos los routers tienen distintos datos. Pero los default son:

admin – admin

admin – 1234

1234 – 1234

1234 – admin

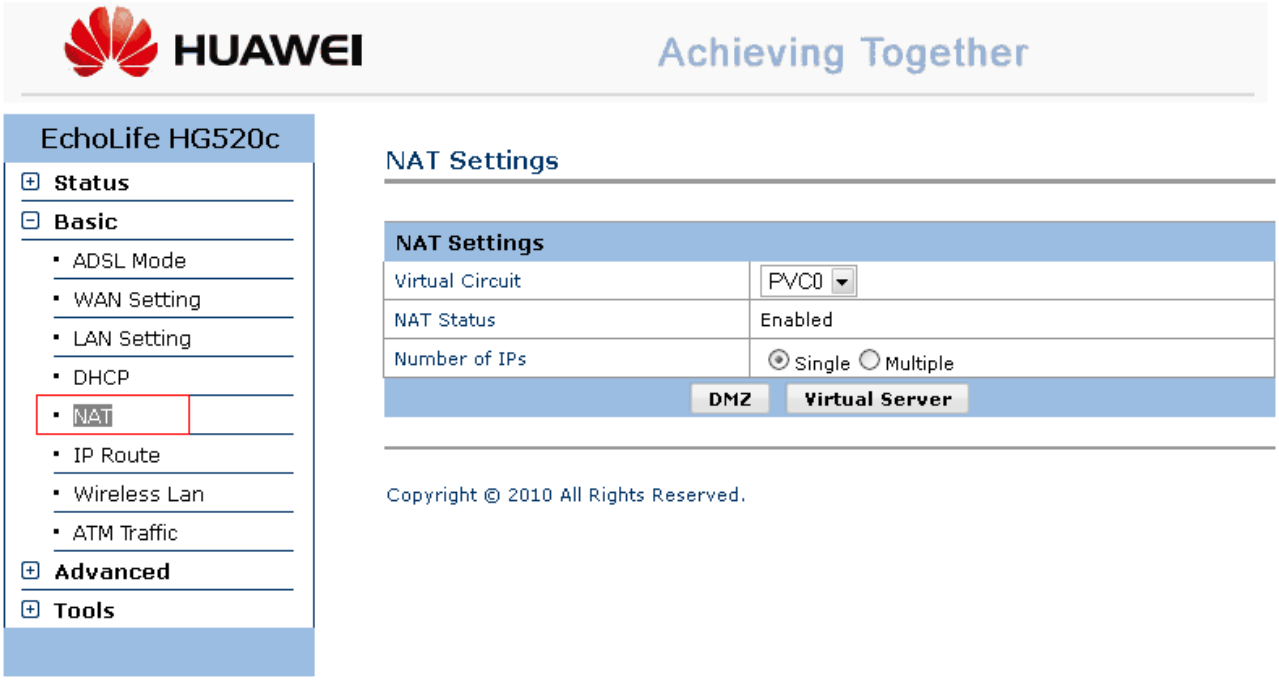
Cuando ingresemos los datos, podremos entrar al panel de configuración del router.

Recuerden una cosa…

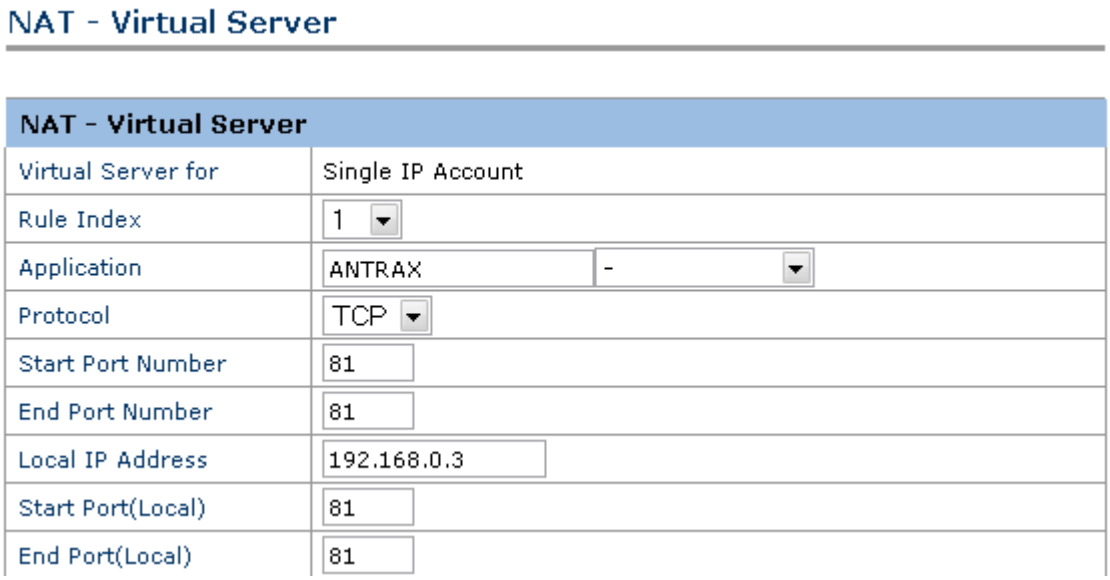
TODOS LOS ROUTERS SON DISTINTOS

Por lo tanto no piensen que será igual que el mío.

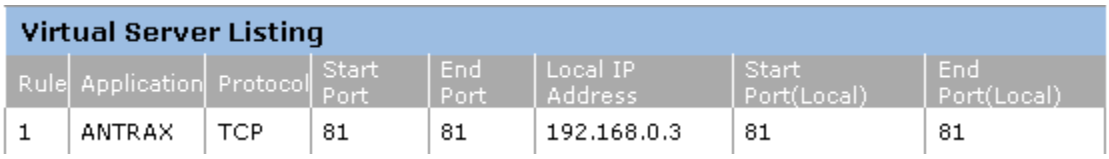
En mi caso debo ir a Basic > NAT > Virtual Server



Una vez dentro de Virtual Server, llenamos los campos con nuestra IP Privada y el puerto que deseamos abrir:

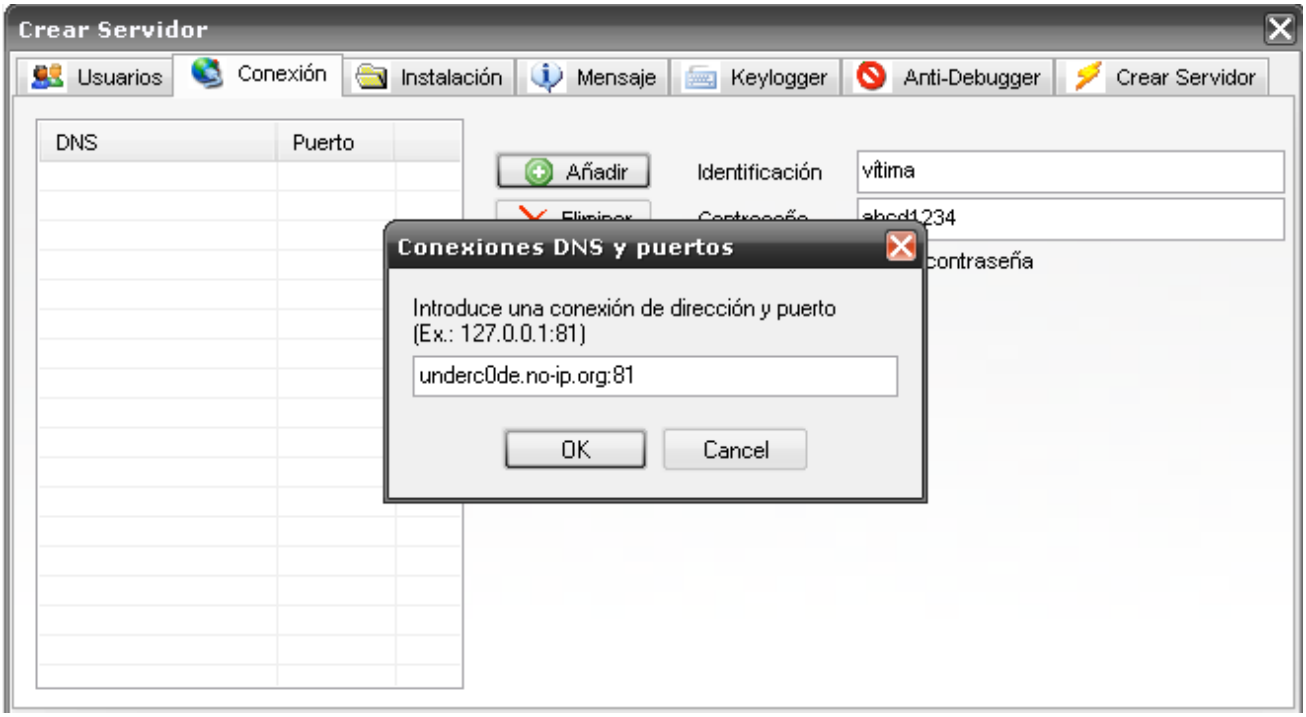


Damos en Submit y el puerto se agregara a la lista

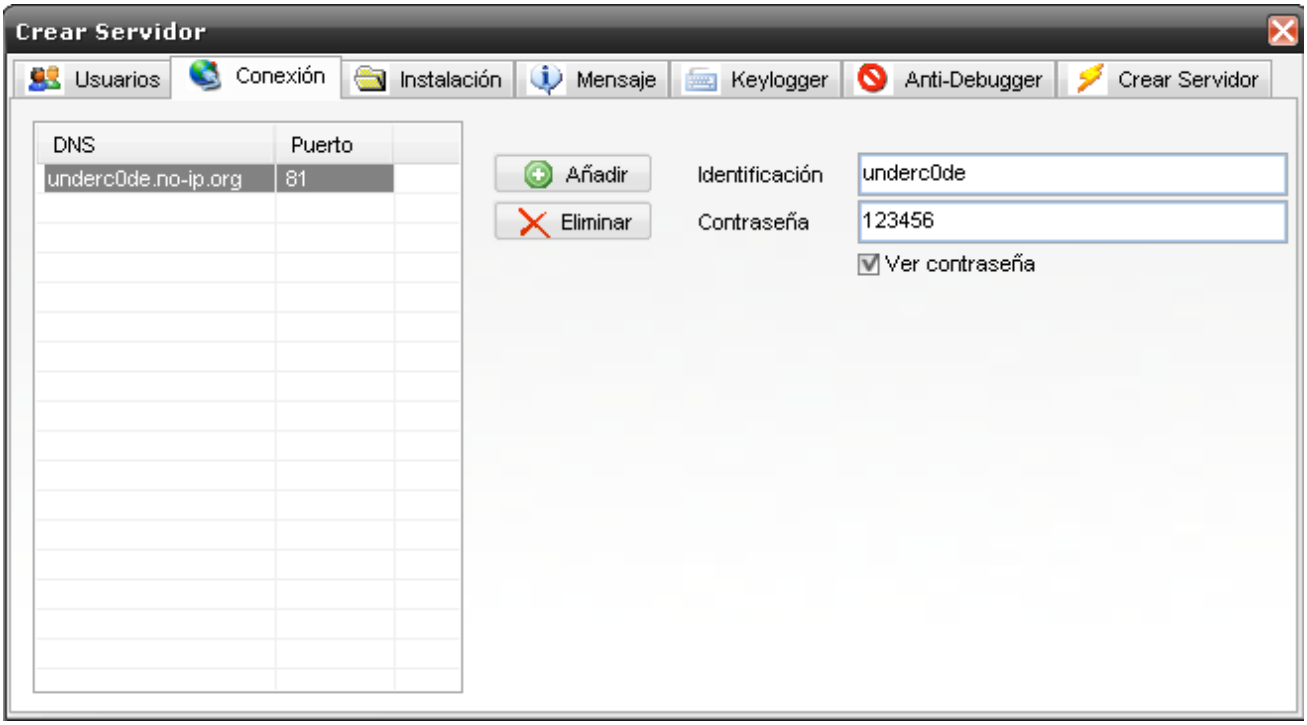


INFECCION REMOTA

Bueno, aquí solo aplicaremos un pequeño cambio en la configuración de nuestro troyano.



A diferencia de la entrega anterior, lo único que modifique fue la DNS en este caso la NO-IP en lugar de la IP Local.

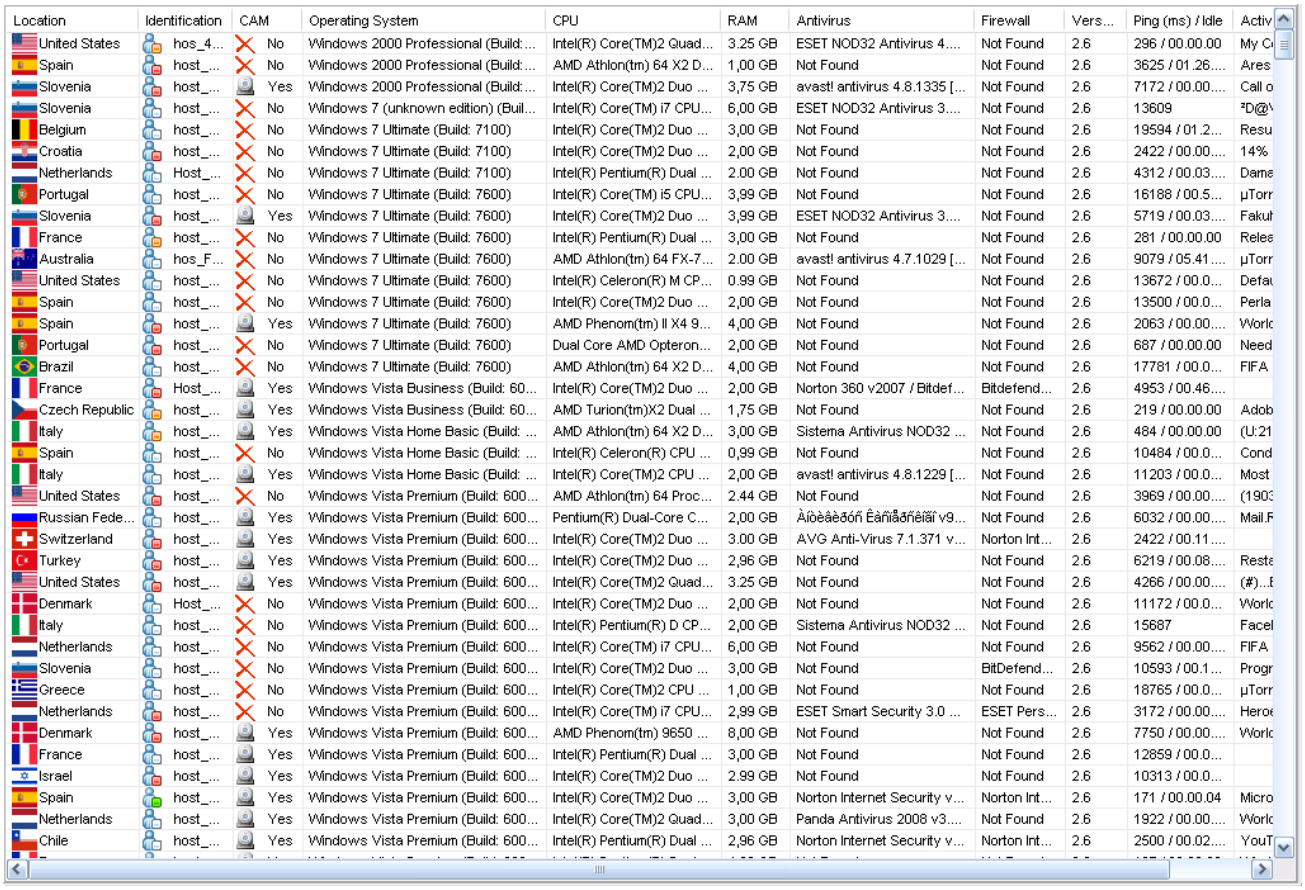


El resto de la configuración, pueden guiarse por la primer entrega porque no cambia en nada.

Una vez creado el server, ya podremos infectar de forma remota a alguna persona.

Recuerden que para que sea más creíble, el server debe ir indetectado para que no lo detecten los antivirus y camuflajeado. Pero eso lo veremos más adelante. De todas formas en el foro encontraran material sobre el tema.

Acá les muestro una captura de cómo se irá viendo nuestro troyano a medida de que infectemos.



Location	Identification	CAM	Operating System	CPU	RAM	Antivirus	Firewall	Vers...	Ping (ms) / Idle	Activ
United States	hos_4...	No	Windows 2000 Professional (Build: ...	Intel(R) Core(TM)2 Quad...	3.25 GB	ESET NOD32 Antivirus 4....	Not Found	2.6	296 / 00.00.00	My C
Spain	host_...	No	Windows 2000 Professional (Build: ...	AMD Athlon(tm) 64 X2 D...	1,00 GB	Not Found	Not Found	2.6	3625 / 01.26....	Ares
Slovenia	host_...	Yes	Windows 2000 Professional (Build: ...	Intel(R) Core(TM)2 Duo ...	3,75 GB	avast! antivirus 4.8.1335 [...	Not Found	2.6	7172 / 00.00....	Call o
Slovenia	host_...	No	Windows 7 (unknown edition) (Buil...	Intel(R) Core(TM) i7 CPU...	6,00 GB	ESET NOD32 Antivirus 3....	Not Found	2.6	13609	²D@\
Belgium	host_...	No	Windows 7 Ultimate (Build: 7100)	Intel(R) Core(TM)2 Duo ...	3,00 GB	Not Found	Not Found	2.6	19594 / 01.2...	Resu
Croatia	host_...	No	Windows 7 Ultimate (Build: 7100)	Intel(R) Core(TM)2 Duo ...	2,00 GB	Not Found	Not Found	2.6	2422 / 00.00....	14%
Netherlands	Host_...	No	Windows 7 Ultimate (Build: 7100)	Intel(R) Pentium(R) Dual ...	2.00 GB	Not Found	Not Found	2.6	4312 / 00.03....	Dame
Portugal	host_...	No	Windows 7 Ultimate (Build: 7600)	Intel(R) Core(TM) i5 CPU...	3,99 GB	Not Found	Not Found	2.6	16188 / 00.5...	µTorr
Slovenia	host_...	Yes	Windows 7 Ultimate (Build: 7600)	Intel(R) Core(TM)2 Duo ...	3,99 GB	ESET NOD32 Antivirus 3....	Not Found	2.6	5719 / 00.03....	Fakul
France	host_...	No	Windows 7 Ultimate (Build: 7600)	Intel(R) Pentium(R) Dual ...	3,00 GB	Not Found	Not Found	2.6	281 / 00.00.00	Relee
Australia	hos_F...	No	Windows 7 Ultimate (Build: 7600)	AMD Athlon(tm) 64 FX-7...	2.00 GB	avast! antivirus 4.7.1029 [...	Not Found	2.6	9079 / 05.41....	µTorr
United States	host_...	No	Windows 7 Ultimate (Build: 7600)	Intel(R) Celeron(R) M CP...	0.99 GB	Not Found	Not Found	2.6	13672 / 00.0...	Defau
Spain	host_...	No	Windows 7 Ultimate (Build: 7600)	Intel(R) Core(TM)2 Duo ...	2,00 GB	Not Found	Not Found	2.6	13500 / 00.0...	Perla
Spain	host_...	Yes	Windows 7 Ultimate (Build: 7600)	AMD Phenom(tm) II X4 9...	4,00 GB	Not Found	Not Found	2.6	2063 / 00.00....	Worlc
Portugal	host_...	No	Windows 7 Ultimate (Build: 7600)	Dual Core AMD Opteron...	2,00 GB	Not Found	Not Found	2.6	687 / 00.00.00	Need
Brazil	host_...	No	Windows 7 Ultimate (Build: 7600)	AMD Athlon(tm) 64 X2 D...	4,00 GB	Not Found	Not Found	2.6	17781 / 00.0...	FIFA
France	Host_...	Yes	Windows Vista Business (Build: 60...	Intel(R) Core(TM)2 Duo ...	2,00 GB	Norton 360 v2007 / Bitdef...	Bitdefend...	2.6	4953 / 00.46....	
Czech Republic	host_...	Yes	Windows Vista Business (Build: 60...	AMD Turion(tm)X2 Dual ...	1,75 GB	Not Found	Not Found	2.6	219 / 00.00.00	Adob
Italy	host_...	Yes	Windows Vista Home Basic (Build: ...	AMD Athlon(tm) 64 X2 D...	3,00 GB	Sistema Antivirus NOD32 ...	Not Found	2.6	484 / 00.00.00	(U:21
Spain	host_...	No	Windows Vista Home Basic (Build: ...	Intel(R) Celeron(R) CPU ...	0,99 GB	Not Found	Not Found	2.6	10484 / 00.0...	Cond
Italy	host_...	Yes	Windows Vista Home Basic (Build: ...	Intel(R) Core(TM)2 CPU ...	2,00 GB	avast! antivirus 4.8.1229 [...	Not Found	2.6	11203 / 00.0...	Most
United States	host_...	No	Windows Vista Premium (Build: 600...	AMD Athlon(tm) 64 Proc...	2.44 GB	Not Found	Not Found	2.6	3969 / 00.00....	(1903
Russian Fede...	host_...	Yes	Windows Vista Premium (Build: 600...	Pentium(R) Dual-Core C...	2,00 GB	Àíòèâèðóñ Êàñïåðñêîãî v9...	Not Found	2.6	6032 / 00.00....	Mail.F
Switzerland	host_...	Yes	Windows Vista Premium (Build: 600...	Intel(R) Core(TM)2 Duo ...	3.00 GB	AVG Anti-Virus 7.1.371 v...	Norton Int...	2.6	2422 / 00.11....	
Turkey	host_...	Yes	Windows Vista Premium (Build: 600...	Intel(R) Core(TM)2 Duo ...	2,96 GB	Not Found	Not Found	2.6	6219 / 00.08....	Reste
United States	host_...	Yes	Windows Vista Premium (Build: 600...	Intel(R) Core(TM)2 Quad...	3.25 GB	Not Found	Not Found	2.6	4266 / 00.00....	(#)...E
Denmark	Host_...	No	Windows Vista Premium (Build: 600...	Intel(R) Core(TM)2 Duo ...	2,00 GB	Not Found	Not Found	2.6	11172 / 00.0...	Worlc
Italy	host_...	No	Windows Vista Premium (Build: 600...	Intel(R) Pentium(R) D CP...	2,00 GB	Sistema Antivirus NOD32 ...	Not Found	2.6	15687	Facel
Netherlands	host_...	No	Windows Vista Premium (Build: 600...	Intel(R) Core(TM) i7 CPU...	6,00 GB	Not Found	Not Found	2.6	9562 / 00.00....	FIFA
Slovenia	host_...	No	Windows Vista Premium (Build: 600...	Intel(R) Core(TM)2 Duo ...	3,00 GB	Not Found	BitDefend...	2.6	10593 / 00.1...	Progr
Greece	host_...	No	Windows Vista Premium (Build: 600...	Intel(R) Core(TM)2 CPU ...	1,00 GB	Not Found	Not Found	2.6	18765 / 00.0...	µTorr
Netherlands	host_...	No	Windows Vista Premium (Build: 600...	Intel(R) Core(TM) i7 CPU...	2,99 GB	ESET Smart Security 3.0 ...	ESET Pers...	2.6	3172 / 00.00....	Heroe
Denmark	host_...	Yes	Windows Vista Premium (Build: 600...	AMD Phenom(tm) 9650 ...	8,00 GB	Not Found	Not Found	2.6	7750 / 00.00....	Worlc
France	host_...	Yes	Windows Vista Premium (Build: 600...	Intel(R) Pentium(R) Dual ...	3,00 GB	Not Found	Not Found	2.6	12859 / 00.0...	
Israel	host_...	Yes	Windows Vista Premium (Build: 600...	Intel(R) Core(TM)2 Duo ...	2.99 GB	Not Found	Not Found	2.6	10313 / 00.0...	
Spain	host_...	Yes	Windows Vista Premium (Build: 600...	Intel(R) Core(TM)2 Duo ...	3,00 GB	Norton Internet Security v...	Norton Int...	2.6	171 / 00.00.04	Micro
Netherlands	host_...	Yes	Windows Vista Premium (Build: 600...	Intel(R) Core(TM)2 Quad...	3,00 GB	Panda Antivirus 2008 v3....	Not Found	2.6	1922 / 00.00....	Worlc
Chile	host_...	Yes	Windows Vista Premium (Build: 600...	Intel(R) Pentium(R) Dual ...	2,96 GB	Norton Internet Security v...	Norton Int...	2.6	2500 / 00.02....	YouT

Bueno, esto es todo por ahora.

Practiquen y las dudas que tengan pueden postearlas en el foro.

Saludos y hasta la próxima!

ANTRAX

antrax.dcode@gmail.com