

MUNDOHACKERS

INICIO

HACKING

VÍDEOS

SHOUTBOX

DONACIONES

CONTACTO

EVITAR LA DETECCIÓN EN REDES



CON TECNOLOGÍA DE

CER CIERTAS COSAS QUE NO DEBERÍAS HACER, TE EMPIEZAS A PREGUN

¿POR TU SEGURIDAD... ¿ESTARÉ
Envíenos un mensaje

SEGURO?, ¿ESTARÉ DEJANDO RASTRO?, ¿QUÉ PASA CON MI IP?, ¿QUÉ PASA CON MI MAC?, ¿ME VA A DETENER LA POLICÍA Y VOY A TENER CADENA PERPETUA?, ¿MORIRÉ EN UNOS DÍAS?

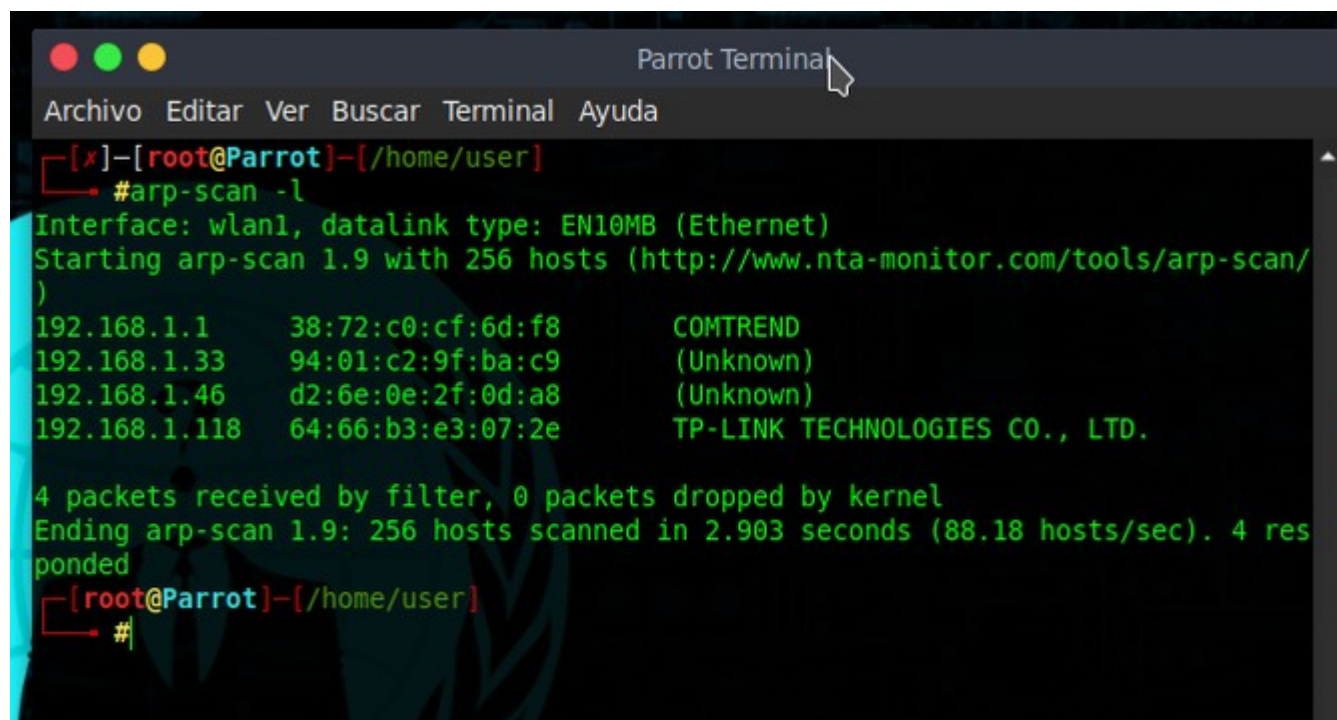
COMO YA HEMOS HABLADO DE ANONIMIZADORES EN OTRAS SECCIONES DE LA PÁGINA, ESTA VEZ TOCA LA EVASIÓN EN REDES. CUANDO NOSOTROS ESTAMOS EN UNA RED, ADEMÁS DE TENER UNA IP SABEMOS QUE TENEMOS UNA DIRECCIÓN MAC. LAS DIRECCIONES MAC TAMBIÉN SE PUEDEN GEOLOCALIZAR, POR SI NO LO SABÍAS, Y PUEDEN DAR CIERTA INFORMACIÓN DE TI.

ES POR ELLO QUE TRATAREMOS DE VER CÓMO CONFIGURAR CORRECTAMENTE NUESTRO EQUIPO PARA ESTAR EN LA RED FALSIFICANDO NUESTRA INFORMACIÓN.

CUANDO ACCEDEMOS A UN ROUTER, SIEMPRE QUEDA UN REGISTRO DE NUESTRA MAC... Y ESO PUEDE SUPONER UN RIESGO. TODOS LOS DISPOSITIVOS TIENEN DIRECCIÓN MAC, DENTRO DE LA RED LOCAL POR EJEMPLO:

CON TECNOLOGÍA DE

Envíenos un mensaje



```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
[~]-[root@Parrot]-[/home/user]
#arp-scan -l
Interface: wlan1, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.1.1      38:72:c0:cf:6d:f8      COMTREND
192.168.1.33    94:01:c2:9f:ba:c9      (Unknown)
192.168.1.46    d2:6e:0e:2f:0d:a8      (Unknown)
192.168.1.118   64:66:b3:e3:07:2e      TP-LINK TECHNOLOGIES CO., LTD.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.903 seconds (88.18 hosts/sec). 4 responded
[~]-[root@Parrot]-[/home/user]
#
```

VEMOS COMO HASTA EL PROPIO ROUTER TIENE DIRECCIÓN MAC, ES INEVITABLE. ALGUNAS DE ELLAS SON DESCONOCIDAS, OTRAS SON DETECTADAS COMO MARCAS DE REPETIDORES, DE ROUTERS, DISPOSITIVOS APPLE, ETC.

SI HACEMOS MEMORIA, EN ATAQUES A REDES INALÁMBRICAS, CUANDO EMPEZÁBAMOS A PREPARAR NUESTRO ATAQUE DE DENEGACIÓN DE SERVICIO PARA POSTERIORMENTE CAPTURAR UN HANDSHAKE Y ACTO SEGUIDO APLICAR FUERZA BRUTA USANDO UN DICCIONARIO DE POR MEDIO, ALGO QUE MENCIONÉ FUE LO DE CAMBIAR LA MAC CON MACCHAGER PARA NO DEJAR HUELLA. ESTOS ATAQUES SE HACEN SIN ESTAR

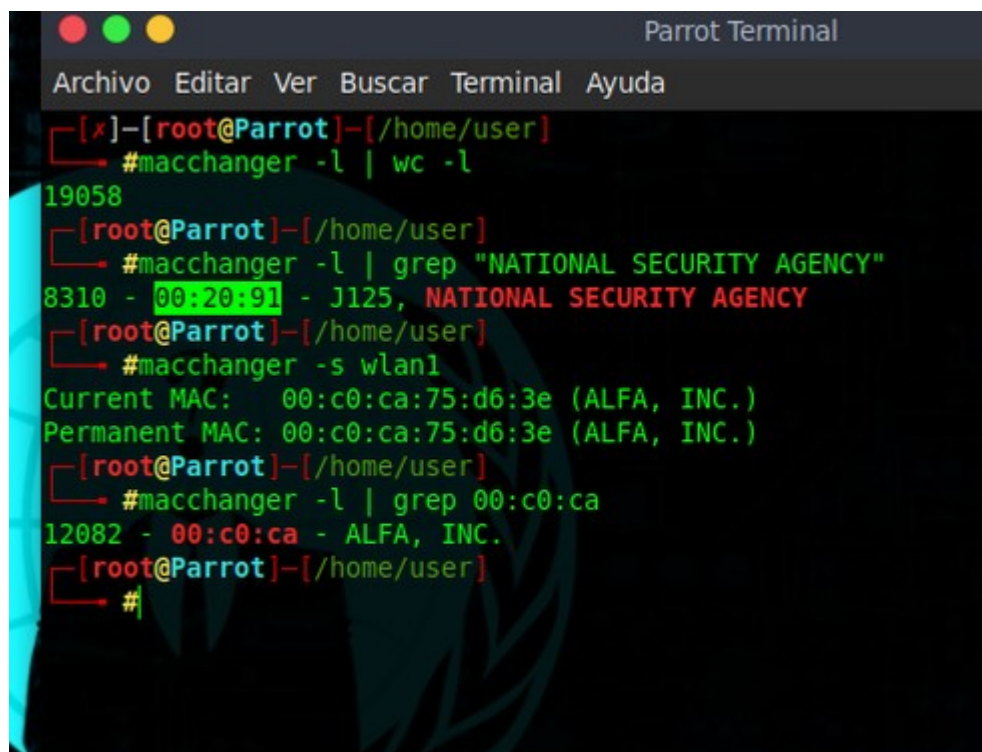
CON TECNOLOGÍA DE

CIÓN, PERO DICHAS PETICIONES QUEDAN REGISTRADAS TAMBIÉN EN EL

TER... SIENDO CAPACES DE V...
Envíenos un mensaje

EL NÚMERO DE PAQUETES ENVIADO Y NUESTRAS INTENCIONES.

COMO LO QUE AHORA VAMOS A HACER ES ESTAR DENTRO DE LA RED EN CUESTIÓN, OBVIAMENTE ANTES DE CONECTARNOS TENDREMOS QUE TENER YA EL EQUIPO CORRECTAMENTE CONFIGURADO. USAREMOS MACCHANGER NUEVAMENTE, DE HECHO... VAMOS A VER EL LISTADO DE MACS QUE NOS OFRECE EL PROGRAMA:



```
Parrot Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[~]-[root@Parrot]-[/home/user]
#macchanger -l | wc -l
19058
[~]-[root@Parrot]-[/home/user]
#macchanger -l | grep "NATIONAL SECURITY AGENCY"
8310 - 00:20:91 - J125, NATIONAL SECURITY AGENCY
[~]-[root@Parrot]-[/home/user]
#macchanger -s wlan1
Current MAC: 00:c0:ca:75:d6:3e (ALFA, INC.)
Permanent MAC: 00:c0:ca:75:d6:3e (ALFA, INC.)
[~]-[root@Parrot]-[/home/user]
#macchanger -l | grep 00:c0:ca
12082 - 00:c0:ca - ALFA, INC.
[~]-[root@Parrot]-[/home/user]
#
```

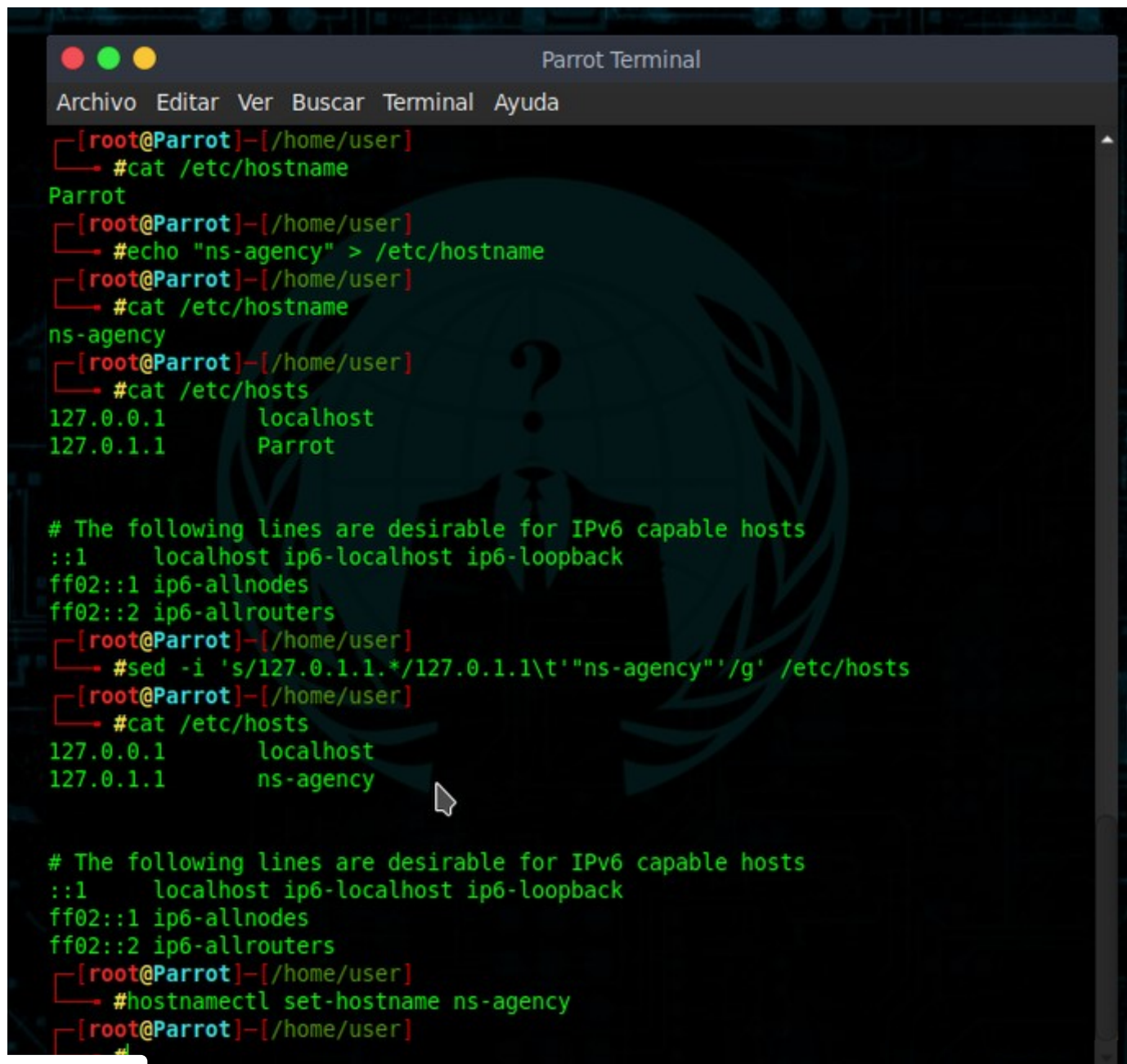
CON TECNOLOGÍA DE

Envíenos un mensaje

VEMOS QUE EN TOTAL HAY 19.058 MACS DIFERENTES, POR ELLO NO VOY A PERDER EL TIEMPO EN MOSTRARLAS. EN CONCRETO DE DICHO LISTADO VOY A SACAR UNA MAC... LA CORRESPONDIENTE A LA NSA. COMO VEIS LAS MACS DE LA NSA EMPIEZAN POR 00:20:91, ESTO ES INTERESANTE... TRABAJAREMOS CON ESTO MÁS ADELANTE. SI TRATAMOS DE VER CON MACCHANGER LA MAC DE MI TARJETA DE RED (EN MI CASO USO UNA TARJETA DE RED EXTERNA - ALFA), VEMOS QUE ES LA 00:C0:CA:75:D6:3E, Y SON JUSTAMENTE LOS 3 PRIMEROS BYTES (00:C0:CA) QUE SE CONOCEN COMO *VENDOR ID*, LOS QUE IDENTIFICAN QUE MI DISPOSITIVO ES UN ALFA.

PROBABLEMENTE SI NO USAS UN ALFA COMO YO... LA MAC QUE TE SALTARÁ SERÁ LA CORRESPONDIENTE AL VENDOR ID DE TU ORDENADOR, POR LO QUE ES UNA BUENA IDEA TAMBIÉN ESTAR USANDO UN DISPOSITIVO EXTERNO QUE TE SUSTENTE CONEXIÓN CON PROPIA MAC, DANDO DE BAJA OBVIAMENTE LA TARJETA DE RED DE TU ORDENADOR PARA MANEJAR LA DEL DISPOSITIVO ALFA.

ENTONCES BIEN... ANTES DE JUGAR CON LAS MACS, LO QUE HARÉ SERÁ CAMBIAR TANTO EL HOST COMO EL HOSTNAME DE MI EQUIPO. POR EJEMPLO:



```
Parrot Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

[root@Parrot]~/home/user
#cat /etc/hostname
Parrot
[root@Parrot]~/home/user
#echo "ns-agency" > /etc/hostname
[root@Parrot]~/home/user
#cat /etc/hostname
ns-agency
[root@Parrot]~/home/user
#cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    Parrot

# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

[root@Parrot]~/home/user
#sed -i 's/127.0.1.1.*/127.0.1.1\t"ns-agency"/g' /etc/hosts
[root@Parrot]~/home/user
#cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    ns-agency

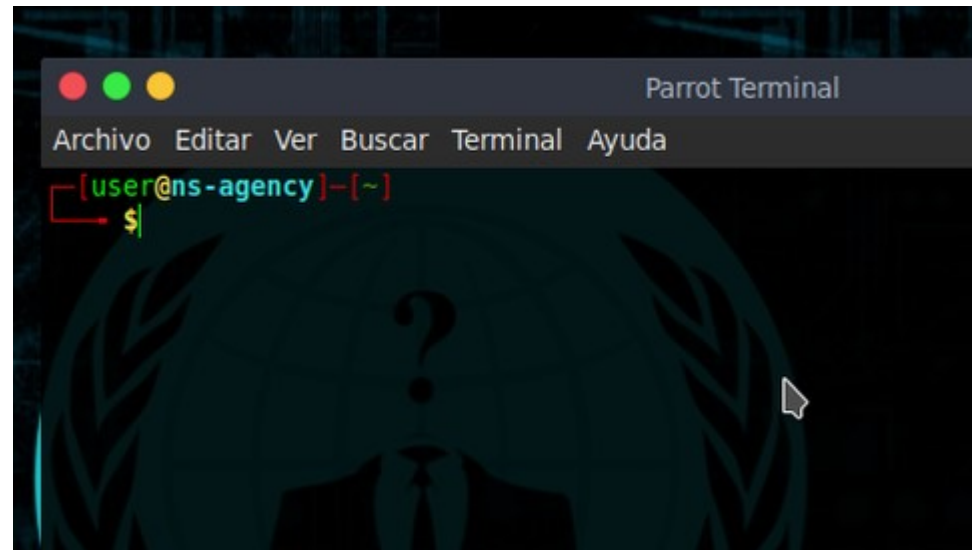
# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

[root@Parrot]~/home/user
#hostnamectl set-hostname ns-agency
[root@Parrot]~/home/user
```

CON TECNOLOGÍA DE

Envíenos un mensaje

¿QUÉ CONSEGUIMOS CON ESTO?, QUE NO SE SEPA QUE NUESTRO HOST ES UN PARROT... DE MANERA QUE AHORA ABRIENDO UNA NUEVA TERMINAL:



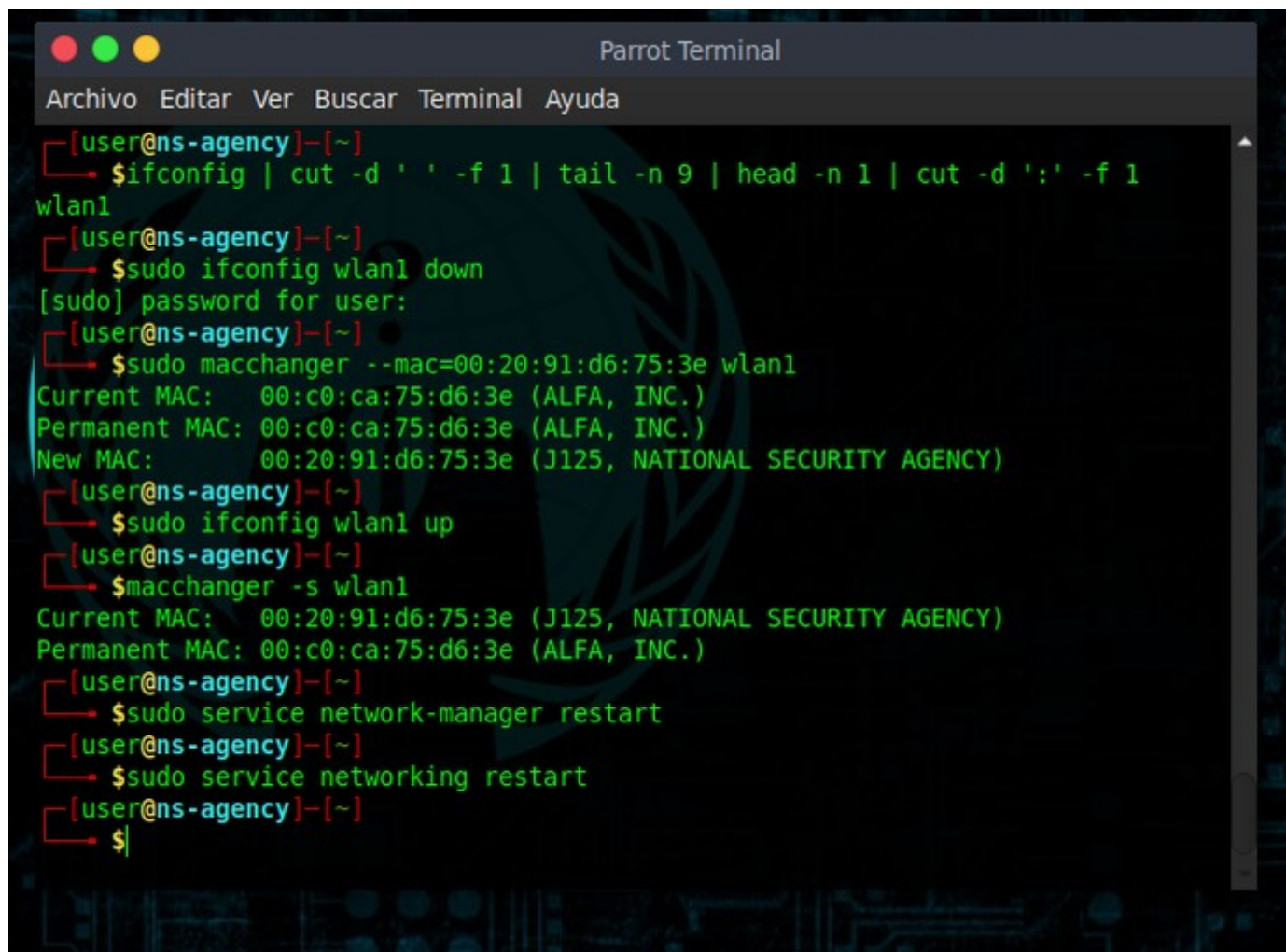
ENTONCES PERFECTO, HOST CAMBIADO... ¿PERO Y LA MAC?, VAMOS A ELLO.

VAMOS A APROVECHARNOS DE QUE CONOCEMOS CÓMO ES EL *VENDOR ID* DE UNA MAC DE LA *NATIONAL SECURITY AGENCY (NSA)* PARA CREAR LA NUESTRA PROPIA. COMO SIEMPRE, PARA PODER CAMBIAR LA MAC DE UNA INTERFAZ DE RED, PRIMERO TENEMOS QUE DARLA DE BAJA PARA POSTERIORMENTE APLICAR LOS CAMBIOS QUE CONSIDEREMOS OPORTUNOS. DESDE QUE HAYAMOS HECHO TODO LO

CON TECNOLOGÍA DE

Envíenos un mensaje

NECESARIO, LA VOLVEMOS A DAR DE ALTA:



```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda

[user@ns-agency]~
$ifconfig | cut -d ' ' -f 1 | tail -n 9 | head -n 1 | cut -d ':' -f 1
wlan1
[user@ns-agency]~
$sudo ifconfig wlan1 down
[sudo] password for user:
[user@ns-agency]~
$sudo macchanger --mac=00:20:91:d6:75:3e wlan1
Current MAC: 00:c0:ca:75:d6:3e (ALFA, INC.)
Permanent MAC: 00:c0:ca:75:d6:3e (ALFA, INC.)
New MAC: 00:20:91:d6:75:3e (J125, NATIONAL SECURITY AGENCY)
[user@ns-agency]~
$sudo ifconfig wlan1 up
[user@ns-agency]~
$macchanger -s wlan1
Current MAC: 00:20:91:d6:75:3e (J125, NATIONAL SECURITY AGENCY)
Permanent MAC: 00:c0:ca:75:d6:3e (ALFA, INC.)
[user@ns-agency]~
$sudo service network-manager restart
[user@ns-agency]~
$sudo service networking restart
[user@ns-agency]~
$
```

CON TECNOLOGÍA DE

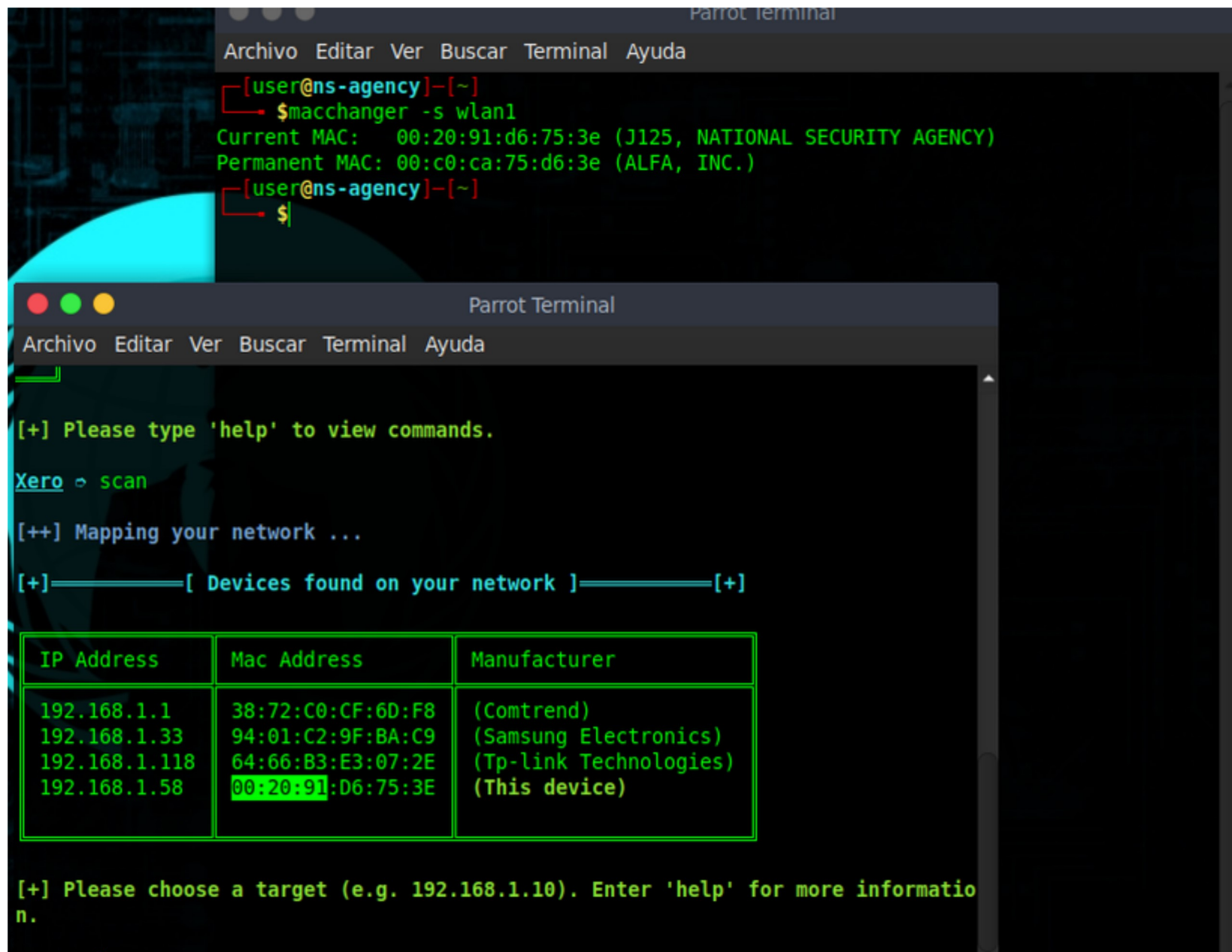
Envíenos un mensaje

LO QUE HICIMOS FUE CAMBIAR LA *VENDOR ID* DE LA MAC POR LA DE LA NSA, LOS OTROS 3 BYTES CORRESPONDIENTES AL *SERIAL* NOS LO HEMOS INVENTADO. AHORA MISMO ESTARÍAMOS CON UNA MAC QUE DE SER ESCANEADA CORRESPONDERÍA A LA DE LA AGENCIA NACIONAL DE SEGURIDAD.

CON EL *XEROSPLOIT* MISMO PODEMOS COMPROBARLO A LA HORA DE HACER UN ESCANEO EN LA RED:

CON TECNOLOGÍA DE

Envíenos un mensaje



```
[user@ns-agency]~$ macchanger -s wlan1
Current MAC: 00:20:91:d6:75:3e (J125, NATIONAL SECURITY AGENCY)
Permanent MAC: 00:c0:ca:75:d6:3e (ALFA, INC.)
[user@ns-agency]~$
```

```
[+] Please type 'help' to view commands.
Xero ▾ scan
[++] Mapping your network ...
[+]—————[ Devices found on your network ]—————[+]



| IP Address    | Mac Address       | Manufacturer           |
|---------------|-------------------|------------------------|
| 192.168.1.1   | 38:72:C0:CF:6D:F8 | (Comtrend)             |
| 192.168.1.33  | 94:01:C2:9F:BA:C9 | (Samsung Electronics)  |
| 192.168.1.118 | 64:66:B3:E3:07:2E | (Tp-link Technologies) |
| 192.168.1.58  | 00:20:91:D6:75:3E | (This device)          |



[+] Please choose a target (e.g. 192.168.1.10). Enter 'help' for more information.
```

CON TECNOLOGÍA DE

Envíenos un mensaje

VEMOS QUE LA MAC CORRESPONDE A LA MANIPULADA MANUALMENTE.

PERFECTO, PUES YA ESTARÍAMOS EN LA RED HACIÉNDONOS PASAR POR QUIEN NO SOMOS. ESTO JUNTO CON UNA VPN A LA HORA DE REALIZAR CIERTAS ACCIONES PUEDEN OCULTAR BASTANTE INFORMACIÓN RESPECTO DE QUIEN REALMENTE SOMOS. OS DIRÍA DE CONFIGURAR UN POCO EL IPTABLES DE LA MÁQUINA... PERO PARA AHORRARNOS PROBLEMAS LO EVITAREMOS.

¿CÓMO VOLVEMOS A DEJAR TODO COMO ESTABA?, DANDO DE BAJA LA TARJETA DE RED Y HACIENDO USO DE LA OPCIÓN '-P', LA CUAL RESTABLECE LA MAC DE FÁBRICA DEL DISPOSITIVO.

CON TECNOLOGÍA DE

Envíenos un mensaje