

## Tutorial para enmascarar y registrar nuestra IP pública (VPN/TOR) desde el inicio en Linux

Publicado por Vicente Motos on sábado, 27 de agosto de 2016 Etiquetas: [anonimato](#), [linux](#), [privacidad](#), [tor](#), [tutoriales](#), [vpn](#)



Anonimizar y cambiar la IP periódicamente suele ser un requisito indispensable a la hora de realizar cualquier pentest, bien para mantener la privacidad (sobretudo si se están realizando pruebas digamos... no consentidas) o bien para evitar y/o evadir las listas negras de los IPS (sistemas de prevención de intrusiones). Por ello es buena idea crear un **servicio que en el arranque de nuestra máquina inicie automáticamente TOR** (o el cliente de otra red anónima) **y la VPN** que normalmente utilizemos. De esta manera lo más importante es que se evitarán las situaciones en las que, normalmente por olvido, se lanzan herramientas antes de enmascarar la IP real del atacante, **exponiendo de forma inmediata su geolocalización**.

A continuación veremos cómo crear un **sencillo servicio en Linux** (Kali en el ej.) que en el inicio del sistema levante tor, sobretudo para lanzar algunos comandos con proxychains y navegar a través de privoxy, y un cliente vpn ([vpnbook](#) en nuestro ejemplo) **para no salir nunca directamente con la IP de nuestro ISP**. Además, irá guardando cada cierto tiempo **la IP en un fichero de log**, algo muy útil por si nos lo piden para el informe o timeline del test de intrusión. Y por último, se comprobará que la IP con la que navegamos está enmascarada y, **en caso de no estarlo, parará de inmediato los interfaces de red**. Vamos a ello:

Primero descargamos los ficheros de configuración .ovpn en el directorio /etc/openvpn/profiles. Aquí, dependiendo de la VPN o VPNs utilizadas dejaremos tantos ficheros como configuraciones y peers disponga el proveedor, normalmente ubicados en diferentes países. En el ejemplo sólo usaremos cuatro de Europa, pero se pueden añadir muchos más incluso de distintos proveedores de VPN:

```
root@kali:/etc/openvpn/profiles# wget -q0- -O tmp.zip
http://www.vpnbook.com/free-openvpn-account/VPNBook.com-OpenVPN-
Euro1.zip && unzip tmp.zip && rm tmp.zip
Archive:  tmp.zip
  inflating: vpnbook-euro1-tcp80.ovpn
  inflating: vpnbook-euro1-tcp443.ovpn
```

```
inflating: vpnbook-euro1-udp53.ovpn
```

```
inflating: vpnbook-euro1-udp25000.ovpn
```

Después crearemos un fichero **pass.txt** que contenga el usuario y la contraseña de la VPN, en el caso de vpnbook está disponible y ni siquiera es necesario registrarse:

```
root@kali:/etc/openvpn/profiles# echo -e "vpnbook\nnu4uTEc" >
pass.txt
```

vpnbook (usuario)  
nnu4uTEc (contraseña)

**Actualización:** este paso ya no es necesario ya que, gracias a un comentario anónimo en esta entrada, se ha añadido en el primer script los comandos para descargar las credenciales y guardarlas de forma automática en el fichero pass.txt.

El siguiente paso será reemplazar en todos los ficheros .ovpn la línea 'auth-user-pass' por 'auth-user-pass pass.txt' para que utilice el fichero recientemente creado:

```
root@kali:/etc/openvpn/profiles# sed -i -- 's/auth-user-pass/auth-
user-pass pass.txt/g' *.ovpn
```

Posteriormente creamos un directorio /anonimato (directamente en el raíz) y dentro los scripts necesarios para el servicio. Primero el script de arranque/parada **anon-init.sh** que iniciará o parará los servicios de tor y vpn (para la vpn **cargará un fichero .ovpn de forma aleatoria**) y ejecutará el fichero específico para la creación de logs.

```
root@kali:/anonimato# vi anon-init.sh
```

```
#!/bin/bash
# Authors: vmotos & cantonini
CREDFILE="/etc/openvpn/profiles/pass.txt"

start() {
ifconfig $(ls /sys/class/net/ | grep -E '^eth|^en|^wl' | head -1) up && sleep 5
#dhclient eth0

# Obtención de credenciales de vpnbook
curl -s http://www.vpnbook.com/freevpn -o results.html
username=$(cat results.html | grep "Username:" | cut -d' ' -f2 | cut -d'>' -f2 | cut -d'<' -f1)
password=$(cat results.html | grep "Password:" | cut -d' ' -f2 | cut -d'>' -f2 | cut -d'<' -f1 | uniq)
echo $username > $CREDFILE && echo $password >> $CREDFILE
rm results.html

IPREAL=$(curl icanhazip.com)
sed $A'1!b;/IPREAL/c\IPREAL\=$IPREAL' -i start-logs.sh
cd /etc/openvpn/profiles ; nohup openvpn --config $(ls *.ovpn | shuf -n 1) &
```

```

systemctl start tor
cd /anonimato ; nohup sh start-logs.sh &
}

stop() {
systemctl stop tor
ps -uax | grep log- | awk '{print $2}' | xargs kill -9
ps -aux | grep openvpn | awk '{print $2}' | xargs kill -9
ifconfig $(ifconfig | egrep -io "tun\w") down 2> /dev/null
rm -f $CREDFILE
ifconfig $(ls /sys/class/net/ | grep -E '^eth|^en|^wl' | head -1) down
}

case $1 in
start|stop) "$1" ;;
esac

```

Y segundo creamos el fichero start-logs.sh que comprobará que no usamos la IP real e irá insertando en el fichero de logs las IPs correspondientes durante el intervalo en segundos que especifiquemos.

root@kali:/anonimato# vi start-logs.sh

```

IPREAL=179.85.12.55
SECS=300
IPVPN=$(curl icanhazip.com)
IPTOR=$(proxychains curl icanhazip.com)

if [ $IPREAL == $IPVPN ] || [ $IPREAL == $IPTOR ];
then
    ifconfig $(ifconfig | grep Ethernet -n3 | egrep -io "1-\w+" | awk -F'- '
'{print $2}') down 2> /dev/null
    ifconfig $(ifconfig | egrep -io "tun\w") down 2> /dev/null
    echo "PRIVACY ALARM!" >> logs/log-vpn-`date +%d-%m-%Y`.log
    echo "PRIVACY ALARM!" >> logs/log-tor-`date +%d-%m-%Y`.log
    exit 1
fi

while true;do echo $IPVPN = `date` >> logs/log-vpn-`date +%d-%m-%Y`.log && sleep $SECS ;
done &
while true;do echo $IPTOR = `date` >> logs/log-tor-`date +%d-%m-%Y`.log && sleep $SECS ;
done &

```

\* No hay que olvidarse de dar permisos de ejecución a los dos scripts creados:

root@kali:/anonimato# chmod +x \*.sh

A continuación creamos el fichero de configuración unit para systemd:

root@kali:/anonimato# vi /etc/systemd/system/anon.service

```

[Unit]
Description=Inicia VPN/TOR y log

```

```
[Service]
Type=oneshot
ExecStart=/anonymato/anon-init.sh start
ExecStop=/anonymato/anon-init.sh stop
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

Para finalmente activar e iniciar el servicio:

```
root@kali:/anonymato# chmod 664 /etc/systemd/system/anon.service
```

```
root@kali:/etc/systemd/system# systemctl enable anon.service
```

Created symlink from /etc/systemd/system/multi-user.target.wants/anon.service to /etc/systemd/system/anon.service

```
root@kali:/anonymato# systemctl start anon.service
```

Ahora bien, podríamos ir revisando regularmente los logs (tail -f) o comprobando manualmente cada cierto tiempo que efectivamente la IP con la que navegamos no es la "nuestra", pero sin duda es mucho mejor utilizar un **monitor de sistema para nuestras X, que se integre en el escritorio** y que podamos ir consultándolo de forma visual casi sin querer. Hablamos de [Conky](#) para el cual os dejo el fichero de configuración que sólo tenéis que ubicar en el home de vuestro usuario, en el ejemplo en `/root/.conkyrc` para la versión 1.10.3 que es la que trae Kali (la versión posterior 1.10.4 cambia ligeramente la sintaxis):

```
conky.config = {
background = true ,
use_xft = true ,
xftalpha = 0.8 ,
update_interval = 5.0 ,
total_run_times = 0 ,
own_window = true ,
own_window_type = "normal" ,
own_window_transparent = "50" ,
background = true,
own_window_argb_visual = true ,
own_window_argb_value = "100",
own_window_argb_value = 0,
own_window_hints = "undecorated,below,skip_taskbar,sticky,skip_pager" ,
double_buffer = true ,
draw_shades = true ,
draw_outline = false ,
draw_graph_borders = true ,
stippled_borders = 8 ,
border_width = 1 ,
maximum_width = 350 ,
minimum_width = 300,
default_color = "darkgrey" ,
```

```

default_shade_color = "black" ,
default_outline_color = "black" ,
alignment = "top_right" ,
gap_x = 4 ,
gap_y = 4 ,
no_buffers = true ,
uppercase = false ,
cpu_avg_samples = 2 ,
net_avg_samples = 2 ,
override_utf8_locale = false ,
use_spacer = "left"
}

conky.text = [[

$color
${color #ffffff}[SYSTEM] ${hr 2}$color
${color #ffffff}UPTIME: $color ${uptime}

${color #ffffff}[CPU] ${hr 2}$color
$cpu% ${color ffcf00} ${cpubar 6}$color

${color #ffffff}[MEMORY] ${hr 2}$color
${color #ffffff}RAM Used: $color${mem}
${color #ffffff}RAM Free: $color${memfree}/ ${memmax}
${color #ffffff}RAM:$color $memperc% ${color ffcf00} ${membar 6}$color

${color #ffffff}NAME PID CPU% MEM%$color
${font GE Inspira:size=10}${color #ffffff}${top name 1} ${top pid 1} ${top cpu 1} ${top
mem 1}
${top name 2} ${top pid 2} ${top cpu 2} ${top mem 2}
${top name 3} ${top pid 3} ${top cpu 3} ${top mem 3}
${top name 4} ${top pid 4} ${top cpu 4} ${top mem 4}
${top name 5} ${top pid 5} ${top cpu 5} ${top mem 5}$color$font

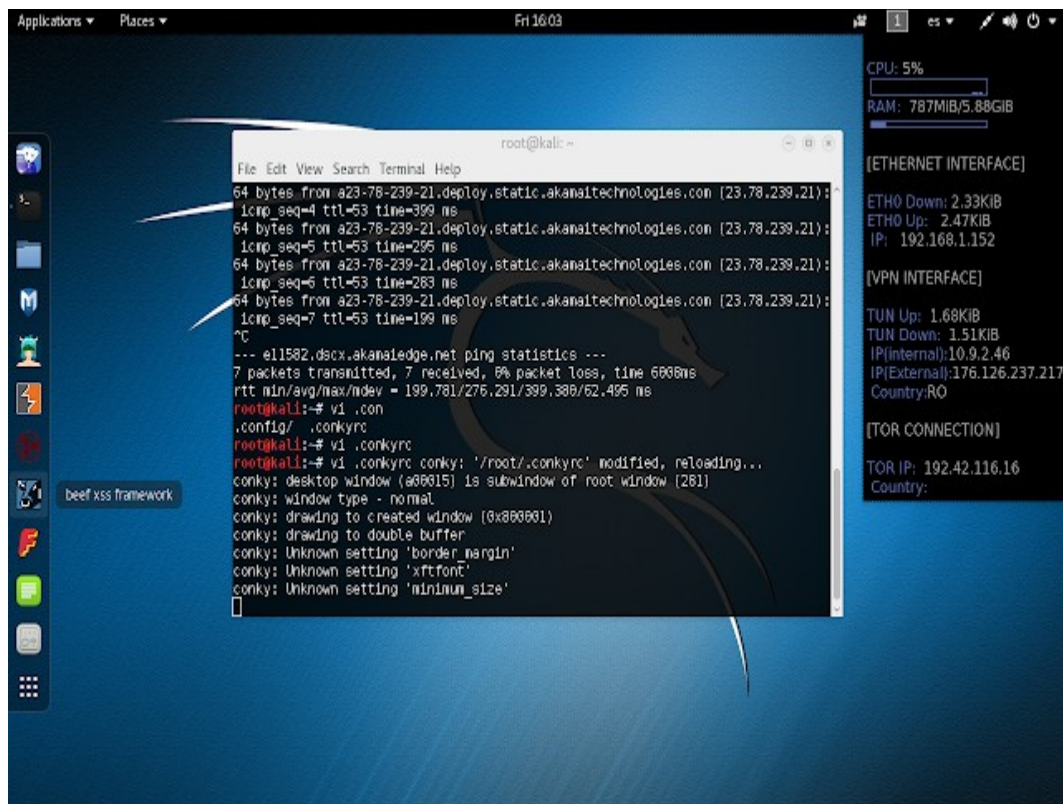
${color #ffffff}[ETHERNET INTERFACE] ${hr 2}$color
${color #ffffff}ETH0 Down: $color${downspeed eth0}${alignr}${downspeedgraph eth0 15,110
ffffff CAF200 -t}
${color #ffffff}ETH0 Up: $color${upspeed eth0}${alignr}${upspeedgraph eth0 15,110 ffffff
CAF200 -t}
${color #ffffff}IP: $color${addr eth0}${alignr}

${color #ffffff}[VPN INTERFACE] ${hr 2}$color
${color #ffffff}TUN Down: $color${downspeed tun1}${alignr}${downspeedgraph tun1 15,110
ffffff CAF200 -t}
${color #ffffff}TUN Up: $color${upspeed tun1}${alignr}${upspeedgraph tun1 15,110 ffffff
CAF200 -t}
${color #ffffff}IP(internal): $color${addr tun1}${alignr}
${color #ffffff}IP(External): $color${execi 1 curl icanhazip.com 2> /dev/null '{print
$1}'}${alignr}
${color #ffffff}Country: $color${execi 1 curl ipinfo.io 2> /dev/null | grep "country" |
awk -F'"' '{print $4}'}${alignr}

${color #ffffff}[TOR CONNECTION] ${hr 2}$color
${color #ffffff}TOR IP: $color${color #CAF200}${execi 1 proxychains curl ipinfo.io 2>
/dev/null | grep "ip" | awk -F'"' '{print $4}'}${alignr}$color
${color #ffffff}Country: $color${color #CAF200}${execi 1 proxychains curl ipinfo.io 2>
/dev/null | grep "country" | awk -F'"' '{print $4}'}${alignr}$color
]]

```

El dock (a falta de embellecerlo) es bastante útil, ya que podremos ver las IPs asignadas y el tráfico de bajada/subida consumido en tiempo real:



```
root@kali: ~  
File Edit View Search Terminal Help  
64 bytes from a23-78-239-21.deploy.static.akamaitechnologies.com (23.78.239.21):  
icmp_seq=4 ttl=53 time=399 ms  
64 bytes from a23-78-239-21.deploy.static.akamaitechnologies.com (23.78.239.21):  
icmp_seq=5 ttl=53 time=295 ms  
64 bytes from a23-78-239-21.deploy.static.akamaitechnologies.com (23.78.239.21):  
icmp_seq=6 ttl=53 time=283 ms  
64 bytes from a23-78-239-21.deploy.static.akamaitechnologies.com (23.78.239.21):  
icmp_seq=7 ttl=53 time=199 ms  
^C  
--- ell582.dscc.akamaiedge.net ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6008ms  
rtt min/avg/max/ndev = 199.781/276.291/399.388/62.495 ms  
root@kali:~# v1 .con  
.config/.conkyrc  
root@kali:~# v1 .conkyrc  
root@kali:~# v1 .conkyrc conky: '/root/.conkyrc' modified, reloading...  
conky: desktop window (a66015) is subwindow of root window (281)  
conky: window type - normal  
conky: drawing to created window (0x800001)  
conky: drawing to double buffer  
conky: Unknown setting 'border margin'  
conky: Unknown setting 'xftfont'  
conky: Unknown setting 'minimum_size'  
█
```

CPU: 5%  
RAM: 787MiB/5.88GiB  
[ETHERNET INTERFACE]  
eth0 Down: 2.33KiB  
eth0 Up: 2.47KiB  
IP: 192.168.1.152  
[VPN INTERFACE]  
TUN Up: 1.68KiB  
TUN Down: 1.51KiB  
IP(internal):10.9.2.46  
IP(External):176.126.237.217  
Country:RO  
[TOR CONNECTION]  
TOR IP: 192.42.116.16  
Country:



### 39 comentarios :

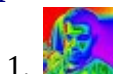
1.

[Anónimo28 de agosto de 2016, 23:41](#)

buenas tardes, muy bueno el artículo, realice lo comentado en la entrada, sin embargo todavía salgo con la ip de mi isp. para entender un poco mi eth0 debe tener la ip pública que me entrega mi ISP? el único cambio que realice fue la ipreal en el start-logs.sh y coloque la que me entrega mi isp. saludos y gracias!

[Responder](#)

[Respuestas](#)



1.

[Vicente Motos29 de agosto de 2016, 9:35](#)

Ostia! es que no estaba el "if" en el script 'start-log.sh', se me coló al pegarlo, lo acabo de añadir:

```
if [ $IPREAL==$IPVPN ] || [ $IPREAL==$IPTOR ];
```

Luego no es necesario que añadas manualmente la IPREAL en el script, ya se añade automáticamente con el anterior (anon-init.sh):

```
IPREAL=$(curl icanhazip.com)
sed $A/IPREAL/c\IPREAL\'$IPREAL" -i start-logs.sh
```

Saludos y disculpa por el fallo.



2.

[Vicente Motos](#)[29 de agosto de 2016, 9:44](#)

es decir, como ves con el if, si la IPREAL que es la que se obtuvo justo antes de lanzar el cliente VPN y el de TOR, sigue siendo la misma.. el script detendrá el interfaz de red para mantener la privacidad...

[Responder](#)

2.

[2Polar](#)[29 de agosto de 2016, 2:09](#)

Buenísimo artículo por las dos partes... tanto por el servicio que va a darme como por lo bien explicado que está ... Pero... me salta ese error al iniciar el proceso

```
/etc/openvpn/profiles/anonimato# systemctl start anon.service
```

```
Job for anon.service failed because the control process exited with error code. See "systemctl status anon.service" and "journalctl -xe" for details.
```

Alguna sugerencia ?.

Saludos

[Responder](#)

[Respuestas](#)

1.

[Anónimo](#)[29 de agosto de 2016, 8:03](#)

Me ocurre lo mismo. Mismo error.

A ver si nos da Vicente una solución.



2.

[Vicente Motos](#) 29 de agosto de 2016, 8:51

Necesitaría la salida del comando `systemctl status anon.service` y `journalctl -xe` para ver el error concreto.

No obstante revisar las rutas... en mi caso los scripts están en el directorio `/anonimato`, es decir, directamente en el raíz. A ver si es eso.

Saludos,

3.

[Anónimo](#) 29 de agosto de 2016, 9:57

Hola Vicente.

En mi caso está copiado tal cual de tu entrada (mismas rutas). Te dejo las salidas.  
`systemctl status anon.service`

- `anon.service` - Inicia VPN/TOR y log

Loaded: loaded (/etc/systemd/system/anon.service; enabled)

Active: failed (Result: exit-code) since lun 2016-08-29 09:53:59 CEST; 22s ago

Process: 10875 ExecStart=/anonimato/anon-init.sh start (code=exited, status=203/EXEC)

Main PID: 10875 (code=exited, status=203/EXEC)

ago 29 09:53:59 kali systemd[10875]: Failed at step EXEC spawning /anonimato/anon-init.sh: No such file or directory

ago 29 09:53:59 kali systemd[1]: anon.service: main process exited, code=exited, status=203/EXEC

ago 29 09:53:59 kali systemd[1]: Failed to start Inicia VPN/TOR y log.

ago 29 09:53:59 kali systemd[1]: Unit anon.service entered failed state.

-----  
`journalctl -xn`

- `anon.service` - Inicia VPN/TOR y log

Loaded: loaded (/etc/systemd/system/anon.service; enabled)

Active: failed (Result: exit-code) since lun 2016-08-29 09:53:59 CEST; 22s ago

Process: 10875 ExecStart=/anonimato/anon-init.sh start (code=exited, status=203/EXEC)

Main PID: 10875 (code=exited, status=203/EXEC)

ago 29 09:53:59 kali systemd[10875]: Failed at step EXEC spawning /anonimato/anon-init.sh: No such file or directory



ago 29 09:53:59 kali systemd[1]: anon.service: main process exited, code=exited, status=203/EXEC  
ago 29 09:53:59 kali systemd[1]: Failed to start Inicia VPN/TOR y log.  
ago 29 09:53:59 kali systemd[1]: Unit anon.service entered failed state.  
root@kali:~/anonimato# journalctl -xn  
-- Logs begin at vie 2016-08-26 14:30:59 CEST, end at lun 2016-08-29 09:53:59 CEST.  
--  
ago 29 09:45:25 kali gnome-session[1279]: (gnome-settings-daemon:1362): color-plugin-WARNING \*\*: unable to get EDID for x  
ago 29 09:46:22 kali pulseaudio[1376]: ALSA nos despertó para escribir nuevos datos al dispositivo, ¡pero en realidad no  
ago 29 09:46:22 kali pulseaudio[1376]: Probablemente sea un error en el controlador ALSA 'snd\_ens1371'. Por favor, inform  
ago 29 09:46:22 kali pulseaudio[1376]: Nos despertaron con POLLOUT puesto -- sin embargo, una llamada a snd\_pcm\_avail() d  
ago 29 09:52:14 kali org.gnome.Terminal[1341]: (gnome-terminal-server:1637): GLib-GIO-WARNING \*\*: Failed to parse transla  
ago 29 09:52:14 kali org.gnome.Terminal[1341]: (gnome-terminal-server:1637): GLib-GIO-WARNING \*\*: Using untranslated defa  
ago 29 09:53:59 kali systemd[10875]: Failed at step EXEC spawning /anonimato/anon-init.sh: No such file or directory  
-- Subject: Process /anonimato/anon-init.sh could not be executed  
-- Defined-By: systemd  
-- Support: <http://lists.freedesktop.org/mailman/listinfo/systemd-devel>  
--  
-- The process /anonimato/anon-init.sh could not be executed and failed.  
--  
-- The error number returned while executing this process is 2.  
ago 29 09:53:59 kali systemd[1]: anon.service: main process exited, code=exited, status=203/EXEC  
ago 29 09:53:59 kali systemd[1]: Failed to start Inicia VPN/TOR y log.  
-- Subject: Unit anon.service has failed  
-- Defined-By: systemd  
-- Support: <http://lists.freedesktop.org/mailman/listinfo/systemd-devel>  
--  
-- Unit anon.service has failed.  
--  
-- The result is failed.  
ago 29 09:53:59 kali systemd[1]: Unit anon.service entered failed state.

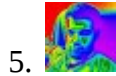
Gracias por tu tiempo.

4.

[2Polar29 de agosto de 2016, 13:29](#)

Perfecto!!!..

Pasé /anonimato al raiz y funciona bien.



5.

[Vicente Motos29 de agosto de 2016, 14:29](#)

Ok, ojo que el sed del primer script sustituía también la línea que contenía el IF (porque también encontraba ahí "IPREAL".. xD

He puesto que haga la sustitución sólo en la primera línea del script start-logs.sh, subiendo la asignación de la variable igualmente:

```
sed $A'1!b;/IPREAL/c\IPREAL\= "$IPREAL" -i start-logs.sh
```

Os recomiendo volver a copiar el contenido de ambos scripts.

6.

[Anónimo29 de agosto de 2016, 14:39](#)

Ok, probaré a ver si es eso. Gracias.

[Responder](#)



3.

[Giomel Jose29 de agosto de 2016, 19:05](#)

Hola Vicente, una pregunta, porque cuando detengo el servicio anon.service se me apaga la conexión eth0, me gustaría que esto no pasara, quisiera tener la posibilidad de usar la VPN cuando me plazca, lo que hago es que detengo el servicio cuando inicio la maquina, pero esto me apaga la tarjeta eth0

[Responder](#)



4.

[Vicente Motos](#)[29 de agosto de 2016, 20:39](#)

Hola Giomel, simplemente comenta o borra la siguiente linea del script anon-init.sh y listo:

```
ifconfig eth0 down
```

Saludos,

[Responder](#)

[Respuestas](#)



[Giomel Jose](#)[29 de agosto de 2016, 21:59](#)

Listo, Muchas Gracias



[Daniel Buttt Haleem](#)[18 de enero de 2018, 18:50](#)

vicente este script o programa permite cambiar tu ip cada X tiempo? Gracias

[Responder](#)



[xBalBan](#)[30 de agosto de 2016, 0:58](#)

Excelente muy bueno, me funciona.

[Responder](#)

6.

[Anónimo](#)[30 de agosto de 2016, 20:24](#)

Muy buen artículo. Una duda, en la línea donde indicas la IP real, no hay forma de scriptearla para coger el valor? Sobre todo para quienes tengan ip dinámica.

[Responder](#)

[Respuestas](#)



[Vicente Motos](#)[31 de agosto de 2016, 1:01](#)

Pensando en alto se me ocurre que se podría añadir una ruta local a un webserver que te devuelva la IP (ej. ipinfo.io). Es decir, que se salga por el eth0 a ipinfo.io en lugar de por el interfaz tun, de tal forma que devuelva la IP real incluso si está levantada la VPN. Luego añadir esta comprobación en cualquiera de los 'while true' y ya lo tendrías para IPs dinámicas...



2. [Ismael Berón](#)30 de octubre de 2017, 6:57

podrías poner un ejemplo gráfico?



3. [Ismael Berón](#)30 de octubre de 2017, 7:26

He intentado configurar el primer script (tengo IP dinámica) y me pasa lo mismo que antes.

Durante el proceso no creó el symlink, y cuando activo el servicio me sale un telefonillo al lado del icono de conexión que dice algo así como quitando privilegios elevados. Compruebo con ifconfig y sigo teniendo la misma IP.

[Responder](#)

7.

[2Polar](#)31 de agosto de 2016, 20:17

Buenas... me funciona todo correctamente, pero (siempre hay algún pero.. :( ....) el navegador de kali linux Iceweasel me queda sin conexión. ¿¿Alguna sugerencia al respecto???

[Responder](#)

8.

[Anónimo](#)1 de septiembre de 2016, 13:44

Hola a todos, a mí me ha ocurrido que las credenciales del tutorial para acceder a vpnbook ya no son correctas, así que he pensado en modificar ligeramente el script de anon-init.sh para que coja las nuevas credenciales automáticamente (es un poco chapuza, pero a mi me funciona por el momento):

```
curl -s http://www.vpnbook.com/freevpn -o results.html
```

```
username=$(cat results.html | grep "Username:" | cut -d' ' -f2 | cut -d'>' -f2 | cut -d'<' -f1)
```

```
password=$(cat results.html | grep "Password:" | cut -d' ' -f2 | cut -d'>' -f2 | cut -d'<' -f1 | uniq)
```

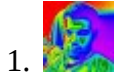
```
echo $username > /etc/openvpn/profiles/pass.txt && echo $password >>  
/etc/openvpn/profiles/pass.txt  
rm results.html
```

Lo de arriba iría justo antes de la línea: IPREAL=\$(curl icanhazip.com)

Espero que le sirva alguien, un saludo! Y enhorabuena por el tutorial.

[Responder](#)

[Respuestas](#)



[Vicente Motos3 de septiembre de 2016, 1:32](#)

chapuza o no a mi me resulta bastante útil, así que lo añado a los scripts del post :)

Muchas gracias!

2.

[Anónimo5 de septiembre de 2016, 8:39](#)

¡De nada! Gracias a tí por el tutorial, un saludo!

[Responder](#)



[Hashirama Senju2 de septiembre de 2016, 14:04](#)

Este comentario ha sido eliminado por el autor.

[Responder](#)

10.

[Anónimo2 de septiembre de 2016, 14:18](#)

¿alguien me podría decir si es seguro usar proxychains+tor en kali linux ?

Este tutorial podría servir para ser anónimo a pesar de que tor ya no es tan seguro como antes y las VPN tienen y guardan los logs ?

¿cual es el mejor método para poder ser anónimo y que las conexiones de los programas tmb lo sean ?

I2P serviría (?)

[Responder](#)

[Respuestas](#)



1.

[Vicente Motos](#) 3 de septiembre de 2016, 1:43

Partimos de que totalmente seguro no hay nada... anonimizar la IP mediante una red anónima como Tor o I2P más una VPN no sirve de nada si luego pueden identificarnos mediante otras técnicas como por ejemplo el fingerprinting de nuestro navegador.

Mi consejo es usar todo lo que esté a vuestro alcance: VPN+red anónima y adicionalmente un pool de máquinas (mejor físicas que virtuales y también en la nube) que uséis exclusivamente para la "navegación" anónima con distintos SO y navegadores... pero claro, tener los suficientes medios, tiempo y sobretodo disciplina para no cometer ningún fallo es relativamente difícil...

2.

[Anónimo](#) 10 de septiembre de 2016, 22:16

Me gustó mucho tu tutorial!, pero como dice Hashirama Senju, no me fío del todo de las VPN gratuitas, como todo lo gratuito, nosotros seremos el producto. ¿Algunas recomendación de vpn que se pueda pagar mediante bitcoins? y que pienses que sea segura.

Gracias!!

[Responder](#)



11.

[Unknown](#) 5 de septiembre de 2016, 1:55

buenas, que tal vicente, cuando ejecuto el scripts obtengo esto: Job for anon.service failed because the control process exited with error code. See "systemctl status anon.service" and "journalctl -xe" for details.

la carpeta anonimato esta en el raiz ¿alguna sugerencia?

[Responder](#)

12.



[Diego arriagada zamora6 de septiembre de 2016, 22:51](#)

hola buen tuto, segui todos los paso tal cual, pero cuando le doy a systemctl start anon.service, el conky al lado no me muestra que tenga una conexion tor, ni la ip externa nada de nada...

[Responder](#)

[Respuestas](#)



1.

[Vicente Motos7 de septiembre de 2016, 2:02](#)

¿copiaste en tu home el fichero .conkyrc? en tal caso mira que coincida el nombre de los interfaces (en el ej. eth0, tun1)

[Responder](#)

13.

[Anónimo8 de septiembre de 2016, 15:01](#)

Gracias por el tutorial. Gran blog.

A mi también me ha pasado que no me aparezca en el conky los datos de la ip externa y los datos de tor, pero creo que es por las Ip's que algunas están banedadas. En IP(External), lo he modificado y he puesto "curl icanhazip.com" en vez de "curl ipinfo.io", de esta manera, siempre tengo la IP (External), con Tor no funcionó igual ^^.

Luego los scripts de los logs, no me funciona muy bien, he tenido que comentar el exit 1, para que me funcionen los

```
while true;do echo $IPVPN = `date` >> logs/log-vpn-`date +%d-%m-%Y`.log && sleep $SECS ; done &
while true;do echo $IPTOR = `date` >> logs/log-tor-`date +%d-%m-%Y`.log && sleep $SECS ; done &
```

Por último, al arrancar no me crea la interfaz tun1.

Ejecuto service anon status y me dice que el fichero de password está en blanco, para solucionarlo, simplemente service anon stop y service anon start, y ahora si funciona todo correctamente. (trabajo sobre máquina virtual, no se si será por eso).

Os dejo el fichero .conkyrc con algunos cambios de diseño del dock, por si os interesa, es una

tontería, pero que sería el mundo sin color...

Saludos y gracias por el tutorial!.

[Responder](#)

14.

[Anónimo8 de septiembre de 2016, 15:24](#)

```
conky.config = {  
background = true ,  
use_xft = true ,  
xftalpha = 0.8 ,  
update_interval = 5.0 ,  
total_run_times = 0 ,  
own_window = true ,  
own_window_type = "normal" ,  
own_window_transparent = "50" ,  
background = true,  
own_window_argb_visual = true ,  
own_window_argb_value = "100",  
own_window_argb_value = 0,  
own_window_hints = "undecorated,below,skip_taskbar,sticky,skip_pager" ,  
double_buffer = true ,  
draw_shades = true ,  
draw_outline = false ,  
draw_graph_borders = true ,  
stippled_borders = 8 ,  
border_width = 1 ,  
maximum_width = 350 ,  
minimum_width = 300,  
default_color = "darkgrey" ,  
default_shade_color = "black" ,  
default_outline_color = "black" ,  
alignment = "top_right" ,  
gap_x = 4 ,  
gap_y = 4 ,  
no_buffers = true ,  
uppercase = false ,  
cpu_avg_samples = 2 ,  
net_avg_samples = 2 ,  
override_utf8_locale = false ,  
use_spacer = "left"
```



```
}
```

```
conky.text = [[
```

```
$color
```

```
${color #ffffff}[SYSTEM] ${hr 2}$color
```

```
${color #ffffff}UPTIME: $color ${uptime}
```

```
${color #ffffff}[CPU] ${hr 2}$color
```

```
$cpu% ${color ffcf00} ${cpubar 6}$color
```

```
${color #ffffff}[MEMORY] ${hr 2}$color
```

```
${color #ffffff}RAM Used: $color${mem}
```

```
${color #ffffff}RAM Free: $color${memfree}/ ${memmax}
```

```
${color #ffffff}RAM:$color $memperc% ${color ffcf00} ${membar 6}$color
```

```
${color #ffffff}NAME PID CPU% MEM%$color
```

```
${font GE Inspira:size=10}${color #ffffff}${top name 1} ${top pid 1} ${top cpu 1} ${top  
mem 1}
```

```
${top name 2} ${top pid 2} ${top cpu 2} ${top mem 2}
```

```
${top name 3} ${top pid 3} ${top cpu 3} ${top mem 3}
```

```
${top name 4} ${top pid 4} ${top cpu 4} ${top mem 4}
```

```
${top name 5} ${top pid 5} ${top cpu 5} ${top mem 5}$color$font
```

```
${color #ffffff}[ETHERNET INTERFACE] ${hr 2}$color
```

```
${color #ffffff}ETH0 Down: $color${downspeed eth0}${alignr}${downspeedgraph eth0  
15,110 fffff CAF200 -t}
```

```
${color #ffffff}ETH0 Up: $color${upspeed eth0}${alignr}${upspeedgraph eth0 15,110 fffff  
CAF200 -t}
```

```
${color #ffffff}IP: $color${addr eth0}${alignr}
```

```
${color #ffffff}[VPN INTERFACE] ${hr 2}$color
```

```
${color #ffffff}TUN Down: $color${downspeed tun1}${alignr}${downspeedgraph tun1 15,110  
ffffff CAF200 -t}
```

```
${color #ffffff}TUN Up: $color${upspeed tun1}${alignr}${upspeedgraph tun1 15,110 fffff  
CAF200 -t}
```

```
${color #ffffff}IP(internal): $color${addr tun1}${alignr}
```

```
${color #ffffff}IP(External): $color${execi 1 curl icanhazip.com 2> /dev/null '{print $1}'}$  
{alignr}
```

```
${color #ffffff}Country: $color${execi 1 curl ipinfo.io 2> /dev/null | grep "country" | awk -F""  
'{print $4}'}${alignr}
```

```

${color #ffffff}[TOR CONNECTION] ${hr 2}$color
${color #ffffff}TOR IP: $color${color #CAF200}${execi 1 proxychains curl ipinfo.io 2>
/dev/null | grep "ip" | awk -F "" '{print $4}'}${alignr}$color
${color #ffffff}Country: $color${color #CAF200}${execi 1 proxychains curl ipinfo.io 2>
/dev/null | grep "country" | awk -F "" '{print $4}'}${alignr}$color
]]

```

[Responder](#)



15.

[Wuilmer Bolívar12 de septiembre de 2016, 22:09](#)

Excelente! Muchas gracias. Me funciona muy bien la guía sin ningún problema.

Datos geográficos de la \$IP  
Continente Europa  
País Rumanía - RO  
Posición GPS 46,25  
Zona horaria Europe/Bucharest

[Responder](#)



16.

[Wuilmer Bolívar12 de septiembre de 2016, 22:12](#)

La captura de pantalla habla por sí sola, si funciona de maravilla el tutorial! Un millón de gracia.

<https://ibin.co/2ur8fXeMi1wp.png>

[Responder](#)



17.

[Wuilmer Bolívar13 de septiembre de 2016, 4:05](#)

Al colocar lo siguiente: sh anon-init.sh stop

Me daba este error si se puede decir:

[ ok ] Stopping tor daemon...done.

warning: bad ps syntax, perhaps a bogus '-'?

See <http://gitorious.org/procps/procps/blobs/master/Documentation/FAQ>

warning: bad ps syntax, perhaps a bogus '-'?

See <http://gitorious.org/procps/procps/blobs/master/Documentation/FAQ>

En el archivo anon-init.sh

En la línea: ps -uax borre el guio "-" quedando en "ps aux" y se a solucionado.

[Responder](#)

18.

*Anónimo* [23 de septiembre de 2016, 21:13](#)

Excelente, me funciona a la perfección ,lo usare con fines educativos 3:)

[Responder](#)

19.

*Anónimo* [9 de octubre de 2016, 4:00](#)

¿Esta forma funcionará con otras distribuciones de linux?

[Responder](#)

20.

*Anónimo* [13 de mayo de 2017, 10:59](#)

Buenos días, he estado probando todo lo que se dicho pero esto no me funciona, siempre me saca mi ip pública.

No me ha dado ningún error y me dice que el servicio anon está activado.

Además, no me corta la conexión.

Alguna idea?

Ayuda por favor.

[Responder](#)

21.

*Anónimo* [27 de septiembre de 2018, 23:03](#)

Sin duda este es el puto mejor blog de (in)Seguridad Informática de la Historia. Encima no fallas un día. Sigue así compañero. Muchas gracias. Salud.