PaperLab

Hacking Ético

Seguridad Informática

“El juego de la ocultación”

Ciberseguridad

Revisión 3 -10.11

José luis Prado Seoane

En este laboratorio práctico le explicaré básicamente como podemos configurar GNU/Linux para poder navegar “anónimamente” sin necesidad de mostrar nuestra IP así como, el posterior uso de herramientas disponibles de la misma forma usando la red TOR, ProxyChains y Privoxy.

TOR
www.torproject.org
Establece una red de comunicaciones distribuida sobre Internet que permite a quién la usa intercambiar mensajes si “revelar” su identidad (IP) y mantener en “secreto” la información que se trasmite. Se le conoce también como la Deep Web (Web profunda).

PROXYCHAINS
Es una aplicación disponible para GNU/Linux que nos permitirá crear cadenas ordenadas de Proxies y de esta forma poder “ocultar” nuestra IP en todo tipo de conexiones sean estas http, SSH, FTP, etc.-, y movernos por Internet sin revelar nuestra identidad real.

PRIVOXY
www.privoxy.org
Es una aplicación que se utiliza como Proxy Web. Su capacidad de filtrado en lo que ha privacidad se refiere, control de accesos, modificación de contenidos, administración de cookies, etc.-, permite un alto grado de personalización.

Antes de nada, deberéis determinar el Release del sistema y la distribución

Release 10.04 (lucid)
Kernel Linux 2.6.38

Posteriormente deberá “logearse” como root-administrador, ¡menos dolor de cabeza!. Si utiliza Backtrack o Kali para la realización del Lab obtendrá acceso como root- administrador (#) una vez se haya inicializado el sistema, si utiliza otra distribución similar, acceda a su cuenta de root-administrador o cree una a su medida, es mejor.

Si tiene cuenta root .. (Estamos trabajando en el directorio raíz pwd “ / “)
usuario@lab:/$ su
Contraseña: ____
…
root@lab:/#

Crear una nueva cuenta. Le pedirá la clave de usuario para realizar la operación.

usuario@lab:/$ sudo passwd root

[sudo] password for usuario: ____
Introduzca la nueva contraseña de UNIX: ____
Vuelva a escribir la nueva contraseña de UNIX: ____
passwd: contraseña actualizada correctamente

usuario@lab:/$ su
Contraseña: ____
…
root@lab:/#

A continuación modificá el archivo de repositorios del sistema para agregar uno que nos permita descargar TOR y Privoxy ..

root@lab:/# nano /etc/apt/sources.list

GNU nano 2.2.2 File: /etc/apt/sources.list

deb http://all.repository.backtrack-linux.org revolution main microverse non-free testing
deb http://32.repository.backtrack-linux.org revolution main microverse non-free testing
deb http://source.repository.backtrack-linux.org revolution main microverse non-free testing

Añada al final de las existentes la siguiente línea, tener en cuenta que en la misma aparece reflejada el Release y nombre de la misma…

deb http://deb.torproject.org/torproject.org lucid main
(En mi caso)

Actualice..

root@lab:/# apt-get update
Get:1 http://32.repository.backtrack-linux.org revolution Release.gpg [198B]
Get:2 http://deb.torproject.org lucid Release.gpg [490B]
. . .
Ign http://32.repository.backtrack-linux.org/ revolution/microverse Translation-en_US
Ign http://deb.torproject.org lucid/main Packages
. . .

Proceda a instalar las aplicaciones correspondientes, TOR y Privoxy utilizando el instalador Apt. Cuando pregunte verificaciones, etc.-, responda a todo que si, (Y).

TOR

root@lab:/# apt-get install tor tor-geoipdb
Reading package lists... Done
. . .
0 upgraded, 3 newly installed, 0 to remove and 121 not upgraded.
Need to get 2,290kB of archives. After this operation, 6,214kB of additional disk space will be used.
Do you want to continue [Y/n]? Y
. . .

PRIVOXY

root@lab:/# apt-get install privoxy proxychains
Reading package lists... Done
Building dependency tree
libdebconfclient0 dmraid keyutils
. . .
Need to get 753kB of archives.
After this operation, 2,867kB of additional disk space will be used.
Do you want to continue [Y/n]? Y

PROXYCHAINS

root@lab:/# apt-get install privoxy proxychains
Reading package lists... Done
. . .
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 120 not upgraded.

(Observe la última línea con atención. Como verá no se ha actualizado, ni instalado, ni borrado nada del sistema de pruebas porque la distribución empleada (Backtrack o Kali) para los Labs ya tiene instalado por defecto la misma, por lo que podrá evitar de realizar este paso o instalación si coincide con la suya)

A continuación retoque un poco la configuración de Privoxy y habilite TOR como Proxy en su máquina de trabajo. Para ello modifique su archivo de configuración en el directorio correspondiente. Elimine a mano o mediante un Script personalizado los comentarios no relevantes del archivo siempre antes realizando una copia de seguridad del mismo.

root@lab:/# nano /etc/privoxy/config
confdir /etc/privoxy
. . .
enforce-blocks 0
. . .
keep-alive-timeout 300
socket-timeout 300

Añada al final la siguiente línea si no existe como en nuestro caso…

socks4 127.0.0.1 9050

(Tiene otras líneas de configuración y tipos diferentes de Proxies (SocksX´s) por lo que no le vendría mal jugar un poco con la configuración en la búsqueda de lo que mejor se adapte a sus expectativas. Si lo desea podrá también configurar el Connetion Settings de su Browser (navegador) habitual para que apunte a dicha IP: puerto y a su correspondiente tipo (Socks v4/Socks v5) , aunque lo aconsejable será en todo momento el modo consola porque verá lo que está sucediendo en realidad)

Una vez configurado los archivos de configuración y repositorio, y haber instalado las herramientas de anonimación, procederá a iniciar los procesos y comprobar que todo ha sido realizado perfectamente.

root@lab:/# /etc/init.d/tor start
** Starting tor daemon...*

root@lab:/# /etc/init.d/privoxy start

Utilice la Web (www.myip.es), - aunque podrá utilizar cualquier otra -, para determinar su nueva IP dentro de TOR. Deberá haber comprobado y anotado la original con anterioridad para poder contrastarlas posteriormente .

Una vez ejecutado el comando siguiente verá la nueva IP asignada en el terminal de trabajo, así como a través del navegador en la Web especificada para su determinación. Copie dicha IP en una nueva ruta de navegación y compruebe que realmente la IP de salida y obtenida pertenece a TOR para que le devuelva el banner asociado.

No olvide anteponer el termino “proxychains….” a su llamada, o de lo contrario no estará utilizando esta tecnología de “anonimato”.
Observe el camino de acceso por los diferentes Proxies, algunos serán autorizados y otros rechazados, y finalmente obtendrá la IP de salida que será la que será ofuscada para que sea localizada por la Web (www.myip.es) enmascarando la auténtica.

Habrá observado la potencia del “anonimato”, pero al mismo tiempo la cantidad de información que se podría obtener si establece uno o varios Proxies en el Deep Web tal y como hacen todo tipo de empresas de seguridad u organismos, - no es de extrañar que en el recorrido o encaminamiento TOR encuentre todo tipo de “enmascaramientos IP” observables o no -, agencias u organismos de Ciberseguridad, agencias de

Inteligencia, organismos militares, etc.-, en la búsqueda de información relacionada con el Cibercrimen, Hacktivismo, Ciberterrorismo en lo que a protección de Infraestructuras Críticas o de Alta Disponibilidad u organismos de Defensa se refiere, Ciberespionaje tanto militar como industrial, etc.- y como no, también los Hackers en busca de todo tipo de información o nexo de datos, Cibercrimen, Ciberhactivistas o simplemente personas (periodistas, activistas, etc.-) que por su seguridad utilizan estos canales para sentirse más anónimos y seguros en la canalización de datos o documentos, etc.- , pero en definitiva, la inmensa mayoría se dedican a la búsqueda, robo o transferencia de información principalmente. Desde mi punto de vista, no aconsejo su uso, con excepción de algunos ámbitos o actuaciones específicas.

root@lab:/# proxychains firefox www.myip.es
ProxyChains-3.1 …
. . .
*|S-chain|-<>-127.0.0.1:9050-<><>-**178.XX.XX.XX:80**-*
(Nuestra nueva IP al cargar el navegador FireFox a la Web referenciada)

Banner

This is a Tor Exit Router

Most likely you are accessing this website because you had some issue with the traffic coming from this IP. This router is part of the Tor Anonymity Network, which is dedicated to providing privacy to people who need it most: average computer users. This router IP should be generating no other traffic, unless it has been compromised.

Tor sees use by many important segments of the population, including whistle blowers, journalists, Chinese dissidents skirting the Great Firewall and oppressive censorship, abuse victims, stalker targets, the US military, and law enforcement, just to name a few. While Tor is not designed for malicious computer users, it is true that they can use the network for malicious ends. In reality however, the actual amount of abuse is quite low. This is largely because criminals and hackers have significantly better access to privacy and anonymity than do the regular users whom they. . . (mensaje original)

Le dejo este pequeño ejercicio para que juegue un poco..

Acceder a (www.google.es) a través de TOR en modo consola. Registre y verifique los Proxies intercalados que le permita determinar, - si es posible -, empresas u organismos de control y seguridad en la misma.

TRUCO: Realice varios intentos para que sea incluido en las lista de no exclusión o aceptación, - con responsabilidad siempre, no olviode esta premisa -, una vez le hayan hecho un tracking efectivo.

Proxies a medida

En este laboratorio práctico le explicaré como podemos configurar ProxyChains para poder navegar a través de una lista de Proxies escalonados públicos pre-configurados.

Esta solución en más “controlable” y “segura” si cabe, y más aún, si lo hacemos a través de “círculos privados de amistad/seguridad cerrados” dónde podemos controlar o monitorizar (Bypass) nosotros mismos nuestra red, por lo que las posibilidades de control y gestión de tráfico son muy amplias, claro está, con el presupuesto adecuado.

En este Lab nos centraremos en los Proxies públicos y le dejamos para su reflexión como podría implementar o desarrollar un sistema privado aunque sea simplemente basado en un modelo teórico. (**Practica 1**)

proxy.org/
tools.rosinstrument.com/proxy/?rule1
incloak.es/proxy-list/
www.publicproxyservers.com/proxy/list1.html
www.proxys.com.ar/
…

A continuación retocaremos el archivo de configuración de ProxyChains - eliminando los comentarios no importantes o descriptivos antes de nada -, habilitando Dynamic_chain (quitando el símbolo anterior #) y configurando nuestra lista de Proxies a medida buscados a través de páginas especializadas dónde

estableceremos como hemos comentado anteriormente la IP:puerto y el tipo (SocksX) en la configuración.

Deberá ser cuidadoso con la elección, busque siempre sitios "confiables" dentro de lo posible, pregunte a su comunidad en foros, redes, eventos, etc.-, pero tenga algo siempre claro, no se fíe de quién está detrás de los mismos, ¡se podría llevar una sorpresa!.

Otra característica importante que deberá tener en cuenta es la elección y los saltos de los mismos. No es lo mismo establecer un punto escalonamiento de tres Proxies, que de cinco, que de diez, que de veinte. Su exposición será mayor cuantos más nodos existan, por no decir la rapidez de su micro-red que se verá afectada a la baja, por no decir los cortes o falta de accesos temporales, etc.-.

Otra característica que deberá tener en cuenta en la elección de los mismos es su localización geográfica, no es lo mismo un proxy en Barcelona que en China, Rusia, Rumanía, Croacia, Brasil, EE.UU, etc.-, dónde será candidato a llevarse un buen susto además, evite en la mayor medida escalonamientos geográficos muy grandes y geo-políticos específicos con marcos jurídicos no deterministas o poco claros, los cuales si serán utilizados por los Hackers, Cibercrimen, etc.-, para todo tipo de actos delictivos en la red que dificulten su rastreo y les permitan temporalmente aumentar el tiempo de actuación en dichos canales de datos.

Imagínese por un momento la utilización de ProxyChains u otras tecnologías similares incluso aquellas desarrolladas a medida específicamente utilizadas para cometer todo tipo de actos delictivos en la red. Imagínese por un solo momento la utilización de estas técnicas y tecnologías aplicadas al desarrollo de todo tipo Malware específico dirigido al eslabón más débil de la cadena, - cada uno de nosotros -, que permita a todos aquellos que la desarrollen o la utilicen obtener un "anonimato" e "impunidad" sin precedentes, controlando todo tipo de máquinas o dispositivos (móviles) en la red de diversa localización para acometer robos de información, anonimación, denegaciones de servicios, etc.-.

Le acabo de mostrar una de las "puertas de entrada" a lo que se conoce en el mundo del Hacking como el UnderGround, - confundido a mi modo de ver algunas veces con el Deep Web que más bien es un subconjunto del mismo -.

root@lab:/# nano /etc/proxychains.conf

 # proxychains.conf VER 3.1
dynamic_chain
strict_chain
proxy_dns
tcp_read_time_out 15000
tcp_connect_time_out 8000
[ProxyList]

socks5 xxx.xxx.xxx.xxx 3128
socks5 xxx.xxx.xxx.xxx 8080
socks5 xxx.xxx.xxx.xxx 3128

#Tor
#socks4 127.0.0.1 9050

¡ Listo !. A partir de ahora lo mismo que antes, recuerde siempre que se debe de manejar este tipo de tecnología con responsabilidad y de una forma segura.

Es posible que existan diferencias en las salidas de los ficheros de configuración, nombres de máquinas, usuarios, directorios, etc.-, en su máquina cuando realice los Labs, por lo que no deberá preocuparse, siendo esto una situación normal, todo ello en función de su configuración, versión y otros factores, lo importante es adquirir los conocimientos de los labs que se le proponen . Existen otras formas de implementación y configuración a parte de la mostrada aquí , tanto en modo consola como gráficas, por lo que le animo a experimentar, ahí radica la clave del éxito!!.

(*)Referencias

Autor: José Luis Prado Seoane
Freelance especializado en Seguridad Informática y Electrónica de sistemas y/o dispositivos en los entornos empresariales.
Blog: joseluispradoseoane.wordpress.com

(*)Comunidad

Compartir parte de tu trabajo y tiempo con la comunidad técnica (Researchers), sectores académicos, sectores profesionales de la seguridad, empresas del sector o con todos aquellos interesados en este mundo, etc.-, hace que el Hacking Ético bien enfocado adquiera su verdadero significado o sentido aportando un nuevo valor añadido a la seguridad en los entornos empresariales.

ADVERTENCIA

“ Actúe siempre con responsabilidad y recuerde, la finalidad es siempre el aprendizaje y la adquisición de conocimientos para la protección de los entornos informáticos en el ámbito de la empresa o la Ciberseguridad“

Joseluispradoseoane.wordpress.com