

Como evitar a detecção usando Proxychains

A pior coisa que pode acontecer a qualquer hacker é ser investigado por um administrador da segurança (TI), as tecnologias de segurança (IDS, firewall, etc.), ou um investigador forense.

Cada vez que enviamos um pacote para o nosso alvo, o pacote contém nosso endereço IP no cabeçalho IP do pacote. Quando nós fazemos uma conexão TCP, o sistema alvo registrará nosso endereço IP, assim como registra todas as conexões. Se nós dispararmos algum alarme de segurança ou alerta, nosso endereço IP será registrado. Todos esses eventos aumentam a possibilidade de detecção.

A fim de manter o hack com a menor chance de detecção nós usamos uma máquina intermediária, a qual o endereço IP ficará registrado no sistema alvo, isso pode ser feito usando proxys.

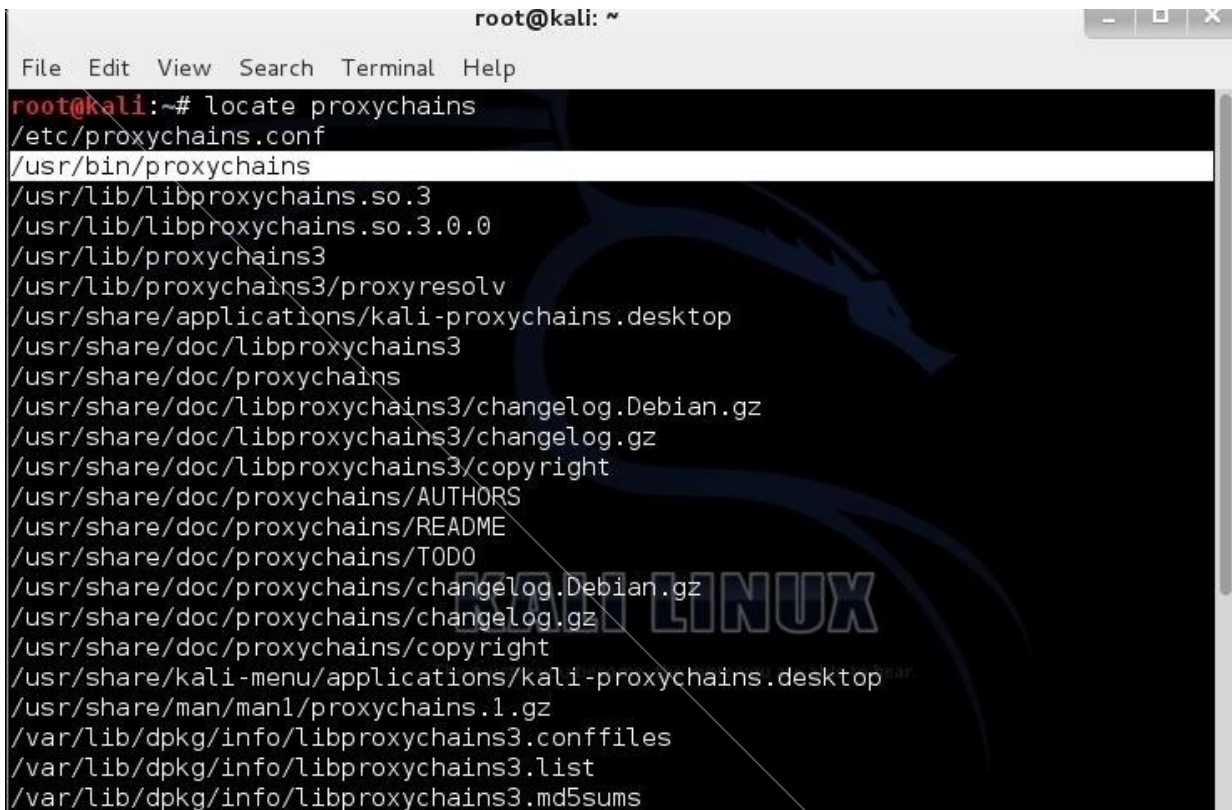
Esses sistemas são desenhados para aceitar nosso tráfego e então encaminhá-lo para o destino. É claro que o proxy registra nosso tráfego, mas um investigador teria que ter uma intimação ou um mandado de busca para obter os logs.

Se colocarmos múltiplos proxys em cadeia ficará muito mais difícil detectar nosso IP original. Se algum desses proxies estiver fora da jurisdição da vítima, isso tornará inútil atribuir qualquer tráfego ao nosso endereço IP.

Kali e o BackTrack possuem uma excelente ferramenta para enviar para proxys todo o nosso tráfego, chamada proxychains. Neste tutorial eu mostrarei como é simples o uso, porém é uma ferramenta poderosa.

Passo 1

Usando o comando [kali > locate proxychains] no terminal você verá a localização do mesmo no sistema.

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The command 'root@kali:~# locate proxychains' has been executed, resulting in a list of files and directories found. The output is as follows:

```
root@kali:~# locate proxychains
/etc/proxychains.conf
/usr/bin/proxychains
/usr/lib/libproxychains.so.3
/usr/lib/libproxychains.so.3.0.0
/usr/lib/proxychains3
/usr/lib/proxychains3/proxyresolver
/usr/share/applications/kali-proxychains.desktop
/usr/share/doc/libproxychains3
/usr/share/doc/proxychains
/usr/share/doc/libproxychains3/changelog.Debian.gz
/usr/share/doc/libproxychains3/changelog.gz
/usr/share/doc/libproxychains3/copyright
/usr/share/doc/proxychains/AUTHORS
/usr/share/doc/proxychains/README
/usr/share/doc/proxychains/TOD0
/usr/share/doc/proxychains/changelog.Debian.gz
/usr/share/doc/proxychains/changelog.gz
/usr/share/doc/proxychains/copyright
/usr/share/kali-menu/applications/kali-proxychains.desktop
/usr/share/man/man1/proxychains.1.gz
/var/lib/dpkg/info/libproxychains3.conffiles
/var/lib/dpkg/info/libproxychains3.list
/var/lib/dpkg/info/libproxychains3.md5sums
```

Você pode instalar o proxychains em seu sistema e usá-lo.

Nas distros baseadas no debian basta digitar no terminal:

```
sudo apt-get install proxychains
```

Passo 2

A sintaxe para o proxychains é simples e direta.

Kali> proxychains <o comando que você deseja passar pelo proxy> <qualquer argumento>

Então, se eu quero usar o proxychains para escanear um site com nmap anonimamente eu poderia digitar:

```
kali> proxychains nmap -sS <endereço IP>
```

Passo 3

Setando o arquivo Config.

Como quase todas as aplicações Linux/Unix, configurações são gerenciadas por um simples arquivo de texto chamado *config file*. No caso do proxychains, este arquivo é */etc/proxychains.conf*. Nós podemos abri-lo com qualquer editor de texto (leafpad, vi, emacs, gedit, kwrite, nano, etc.) digitando:

```
kali> leafpad /etc/proxychains.conf
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# leafpad /etc/proxychains.conf
```

Quando fizermos isso veremos um arquivo como o disposto abaixo, se você rolar para baixo o arquivo, você verá uma sessão que eu destaquei chamada “*add proxy list here ...*”.

```
*proxychains.conf
File Edit Search Options Help

# ProxyList format
#   type host port [user pass]
#   (values separated by 'tab' or 'blank')
#
#   Examples:
#
#       socks5 192.168.67.78 1080 lamer secret
#       http   192.168.89.3  8080 justu hidden
#       socks4 192.168.1.49 1080
#       http   192.168.39.93 8080
#
#   proxy types: http, socks4, socks5
#   ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...

# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 9050
```

Para que o proxychains use proxys intermediários, nós simplesmente precisamos adicionar o endereço IP do proxy que nós queremos usar aqui. É importante notar que por padrão o proxychains usa o TOR.

Observe a última linha no screenshot acima, ela direciona o proxychains para mandar o trafego primeiro através da nossa máquina no 127.0.0.1 na porta 9050 (configuração padrão TOR). Se você está usando Tor deixe essa linha assim, mas se não estiver usando Tor, você precisa comentar essa linha.

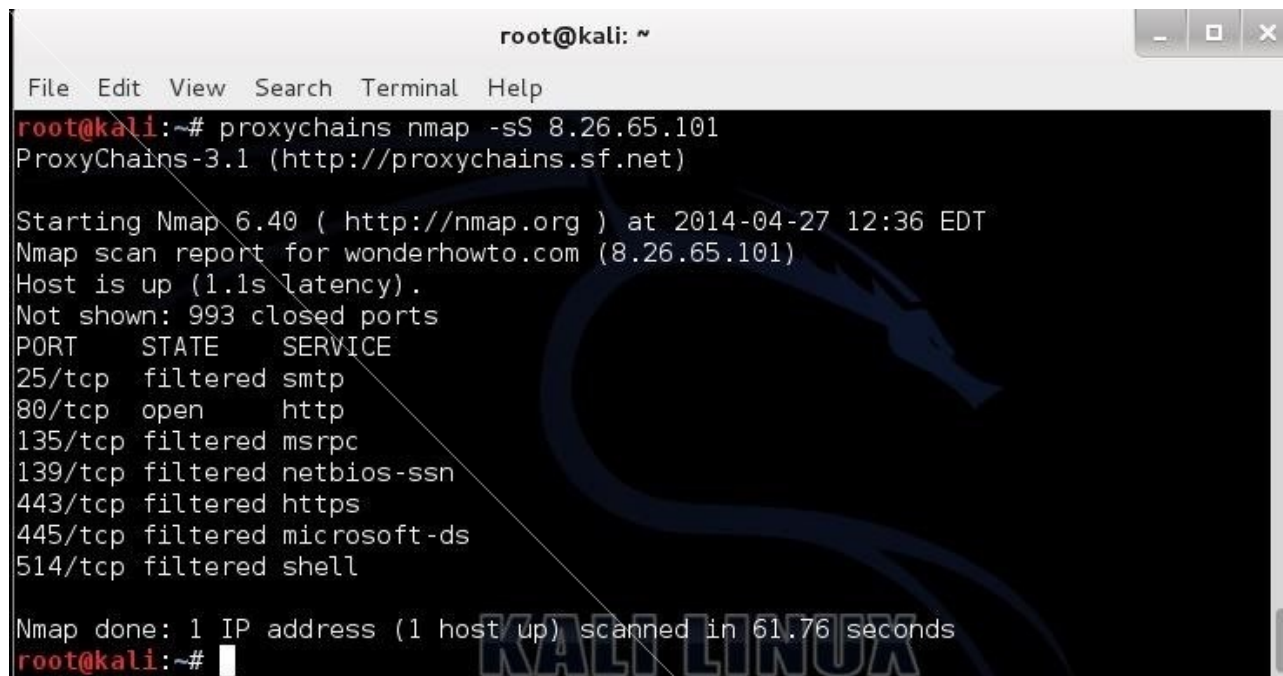
Por mais que eu goste do Tor, ele é muito lento, e nós sabemos que a NSA quebrou o anonimato (lembra do caso da Silk Road na deepweb?), assim sou muito menos propenso a depender dele para anonimato.

Passo 4

Hora de testar.

Agora nós colocamos um proxy entre nós e qualquer tráfego que enviamos, vamos testar. Neste caso, eu irei simplesmente fazer um scan com nmap to wonderhowto.com anonimamente enviando o scan por um proxy. O comando será:

```
kali> proxychains nmap -sS 8.26.65.101
```

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the command 'proxychains nmap -sS 8.26.65.101' being executed. The output indicates that the scan was successful, showing the state of various ports on the target host. The terminal has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The background of the terminal window features a faint, stylized dragon logo and the text 'KALI LINUX'.

```
root@kali:~# proxychains nmap -sS 8.26.65.101
ProxyChains-3.1 (http://proxychains.sf.net)

Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-27 12:36 EDT
Nmap scan report for wonderhowto.com (8.26.65.101)
Host is up (1.1s latency).
Not shown: 993 closed ports
PORT      STATE      SERVICE
25/tcp    filtered  smtp
80/tcp    open      http
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
443/tcp   filtered  https
445/tcp   filtered  microsoft-ds
514/tcp   filtered  shell

Nmap done: 1 IP address (1 host up) scanned in 61.76 seconds
root@kali:~#
```

Como você pode ver no screenshot acima eu tive sucesso no meu scanearno através do proxy que escolhi e retornou para mim os resultados. Deste jeito, o que consta é que o meu proxy escaneou wonderhowto.com e não o meu endereço IP.

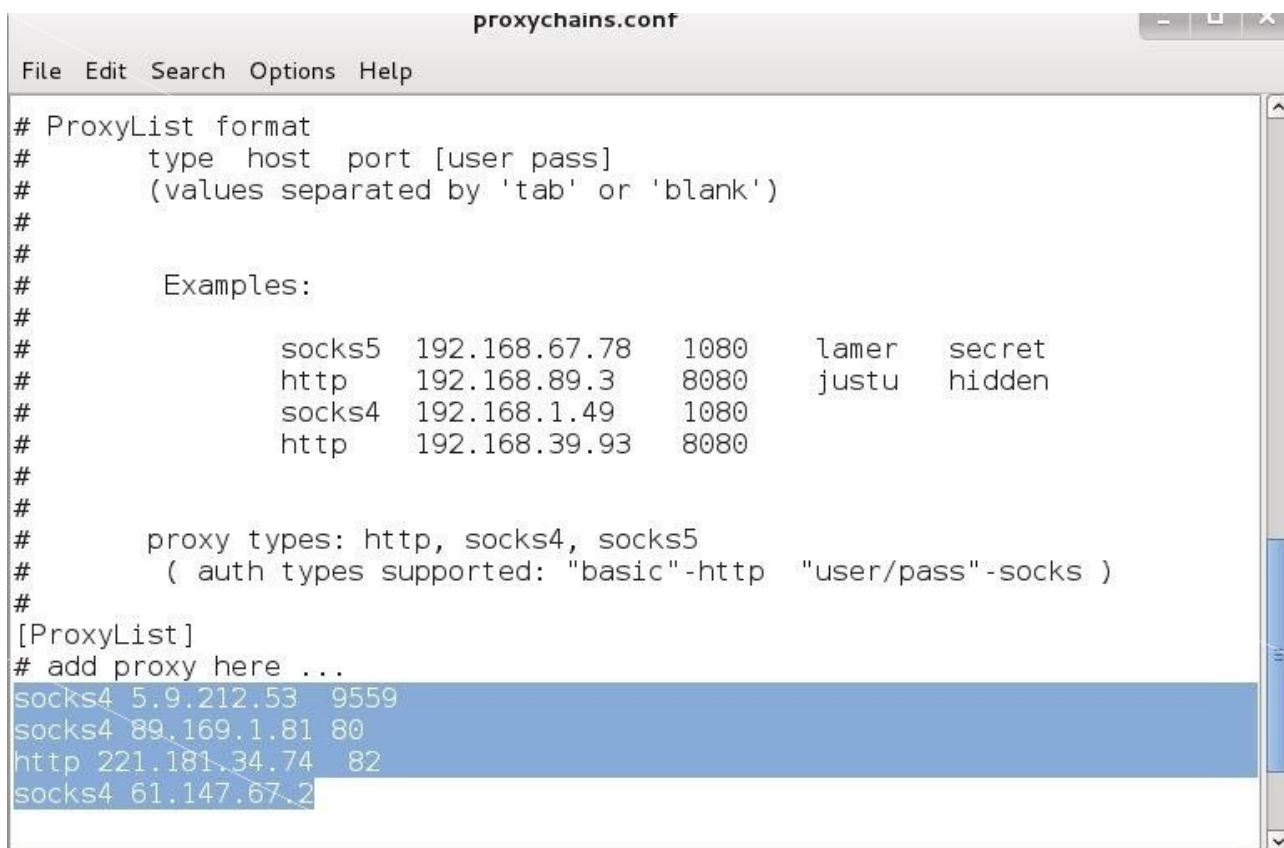
Algumas opções interessantes.

Agora que nós temos proxychains funcionando vamos dar uma olhada em algumas opções que podemos configurar através do *proxychains.conf*. Com nós configuramos, nós estamos simplesmente usando um único proxy. Nós podemos colocar inúmeros proxys e usar todos eles, nós podemos usar um número limitado de uma lista, ou podemos ter o proxychains mudando a ordem randomicamente. Vamos tentar todas essas opções.

Passo 5

Adicionando mais proxys

Primeiro vamos adicionar mais proxys para a nossa lista. Abra */etc/proxychains.config* e adicione mais proxys Ips como eu fiz abaixo.

A screenshot of a text editor window titled 'proxychains.conf'. The window has a menu bar with 'File', 'Edit', 'Search', 'Options', and 'Help'. The content of the file is as follows:

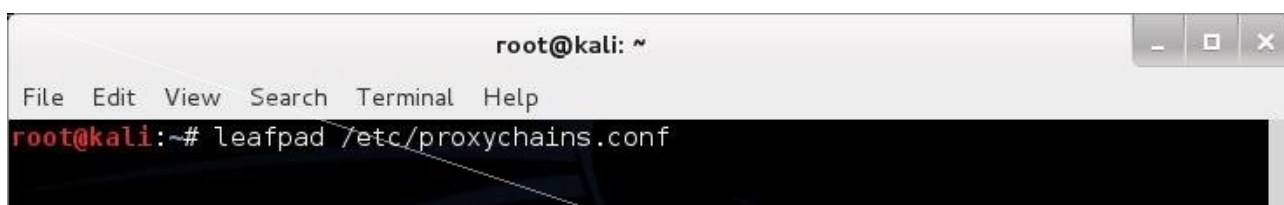
```
# ProxyList format
#      type host port [user pass]
#      (values separated by 'tab' or 'blank')
#
#      Examples:
#
#          socks5 192.168.67.78 1080 lamer secret
#          http 192.168.89.3 8080 justu hidden
#          socks4 192.168.1.49 1080
#          http 192.168.39.93 8080
#
#      proxy types: http, socks4, socks5
#      ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
socks4 5.9.212.53 9559
socks4 89.169.1.81 80
http 221.181.34.74 82
socks4 61.147.67.2
```

Passo 6

Mudança de proxy

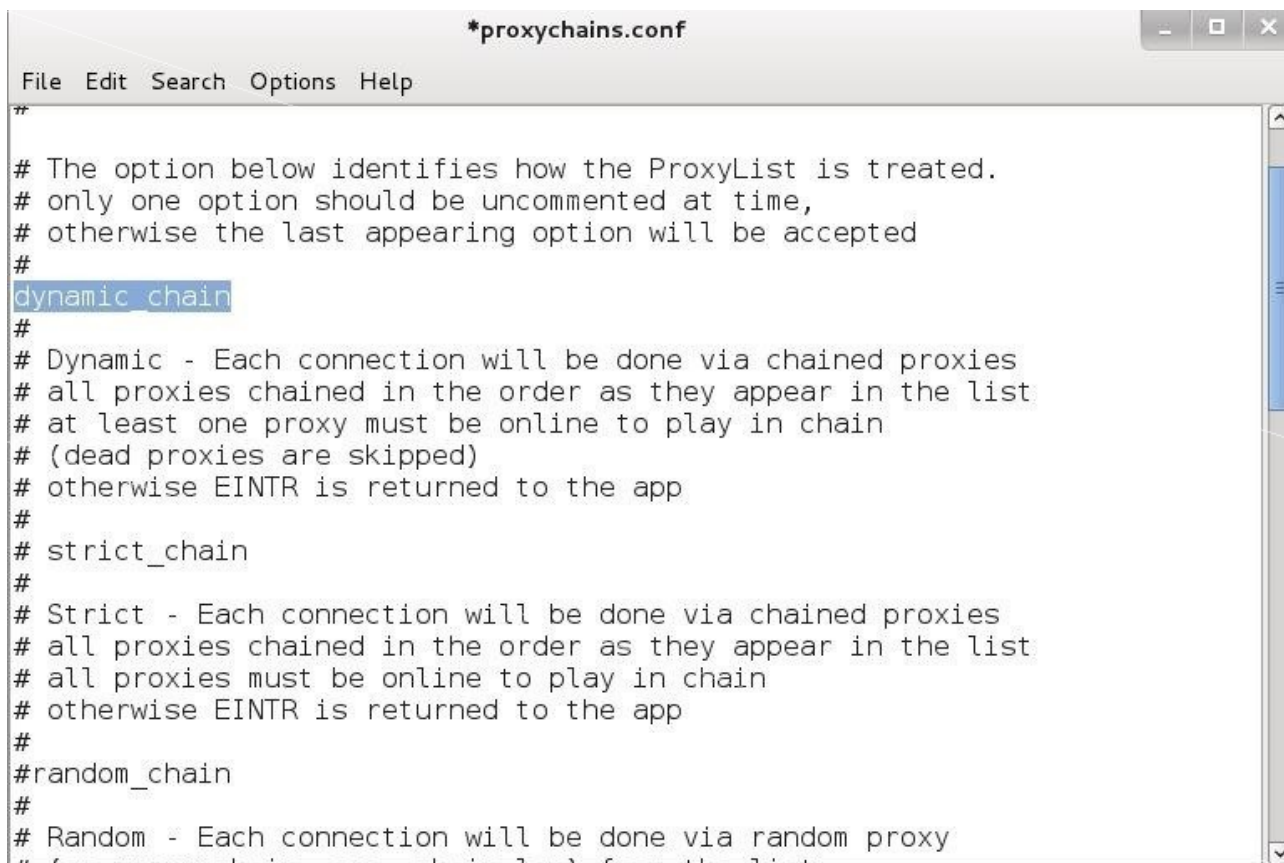
Agora nós temos múltiplos Ips em nosso *proxychains.conf* nós podemos setar uma mudança dinâmica. Mudança dinâmica irá nos habilitar para enviar nosso trafego através de cada proxy em nossa lista, e se um dos proxys estiver desativado ou não responder, ele automaticamente irá para o próximo proxy na lista sem lançar um erro.

Primeiro vamos abrir novamente o arquivo de configuração.

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'leafpad /etc/proxychains.conf' being entered at the prompt 'root@kali:~#'.

```
root@kali:~# leafpad /etc/proxychains.conf
```

Com o arquivo aberto, descomente a linha "*dynamic_chains*". Isso irá habilitar a mudança dinâmica dos nossos proxy permitindo uma melhor anonimidade e um hacking livre de problemas.



```
**
# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
# strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#random_chain
#
# Random - Each connection will be done via random proxy
# (chain_len is chain_len) from the list
```

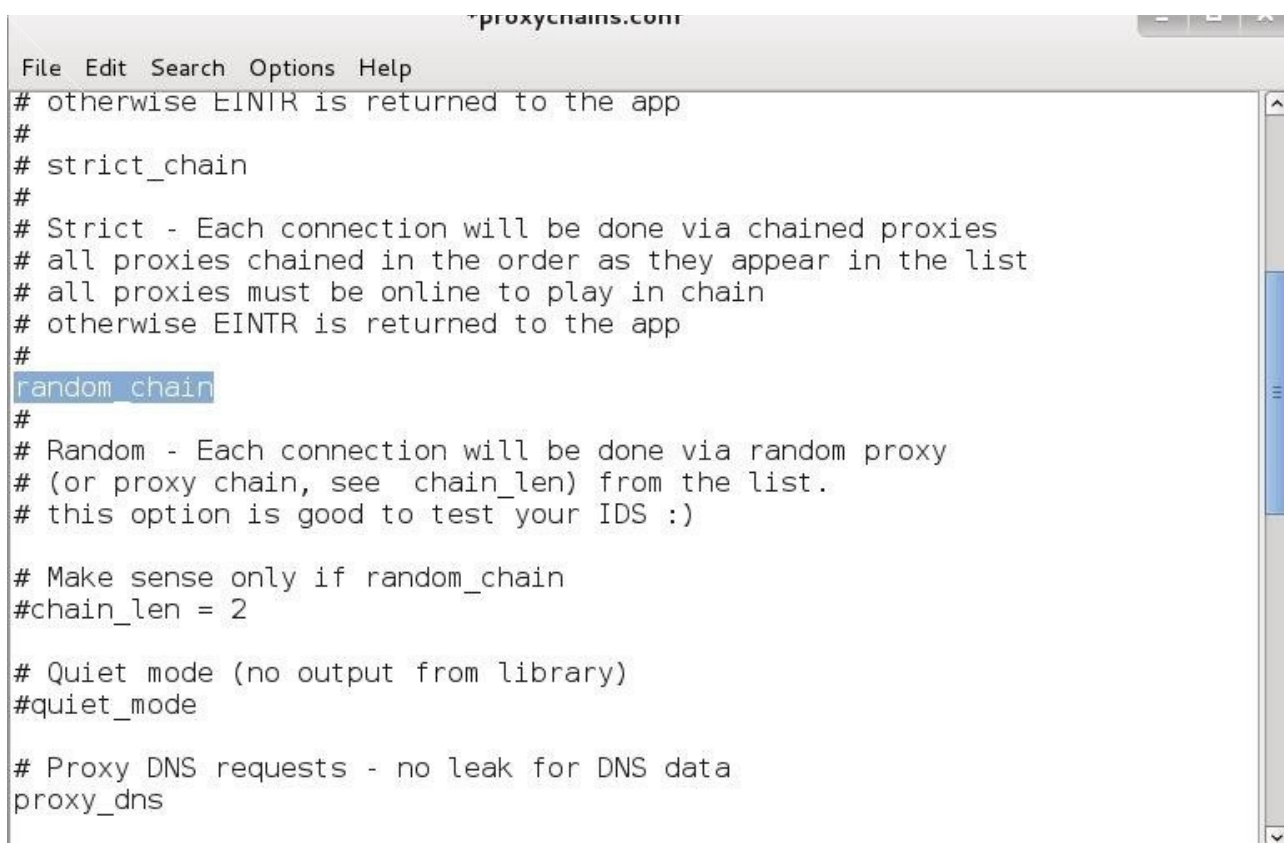
Passo 7

Mudança randomica

Finalmente só podemos usar “*random chaining*”. Com esta opção proxychains irá randomicamente escolher o endereço IP da nossa lista e usá-lo então para criar nossa cadeia de proxys. Isso significa que cada vez que usarmos proxychains, a cadeia de proxy parecerá diferente para o alvo, tornando mais difícil rastrear nosso tráfego até a fonte.

Para fazer isso abra o arquivo de configuração e comente “*dynamic chains*” e descomente “*random chain*”. Desde que só podemos usar uma opção por vez, tenha certeza que você comentou as outras opções nesta sessão antes de usar proxychains.

Como adição, você pode querer descomentar a linha com “*chain_len*”. Isso determinará quantos endereços IP na sua lista a cadeia irá usar para criar a cadeia randomica de proxys.



```
proxychains.conf
File Edit Search Options Help
# otherwise EINTR is returned to the app
#
# strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
random_chain
#
# Random - Each connection will be done via random proxy
# (or proxy chain, see chain_len) from the list.
# this option is good to test your IDS :)

# Make sense only if random_chain
#chain_len = 2

# Quiet mode (no output from library)
#quiet_mode

# Proxy DNS requests - no leak for DNS data
proxy_dns
```

Agora você sabe como usar proxychains, você pode fazer o seu hacking com relativa anonimidade, Eu disse relativa, porque não há nenhuma maneira infalível para manter o anonimato com a NSA espiar toda a nossa atividade. Tudo o que podemos fazer é fazer a detecção muito mais difícil, e proxychains pode ajudar a fazer isso por nós.

Fonte: <http://null-byte.wonderhowto.com/how-to/hack-like-pro-evade-detection-using-proxychains-0154619/>

Traduzido por SeRT4o - PR1V8