INTRODUCCIÓN AL ANONIMATO

El *anonimato* es **imprescindible para un atacante que no quiere ser cazado por sus actos ilegales.**

1.

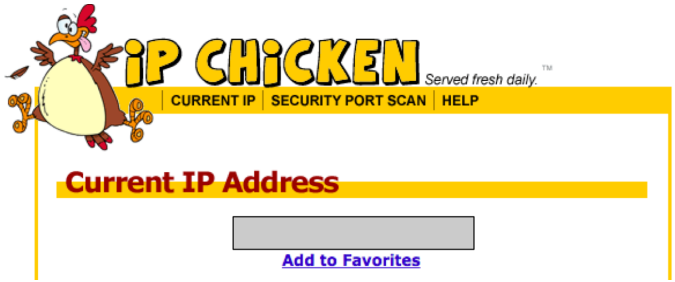
INTRODUCCIÓN

INTRODUCCIÓN

El anonimato no es tenido en cuenta siempre:

- *novatos* o *script-kiddies*
- Poderosos scripts contra objetivos
- No esconden su identidad
- Identificados por su dirección IP pública

WEBS IP PÚBLICA



¿RECURSOS?

Redes de anonimato (*The Onion Router*)

- *TOR*: Red compuesta por *routers* que ocultan la dirección IP origen del usuario.
- Usada por atacantes y usuarios que desean ocultar su identidad.

www.torproject.org

2.

TOR

THE ONION ROUTER

Multiplataforma: *Windows*, *Mac* o *Linux*

THE ONION ROUTER

Comprobación de IP pública

WhatIsMyIP.com®
THE IP ADDRESS EXPERTS

Your IP Address Is:

171.25.193.78

City:	Stockholm
State:	Stockholms Lan
Country:	SE
ISP:	Foreningen for Digitala Fri- och Rattigheter

Cual es mi IP

Tu IP real es 85.93.218.204
(tor.localhost.lu)
No navegas a través de proxy

THE ONION ROUTER (Comprobación)

Lista de nodos Tor: https://www.dan.me.uk/tornodes

85.90.245.11|Unnamed|9001|0|EFRV|313068|Tor 0.2.5.12|
85.90.246.30|purringcat1|9001|0|FRSV|5642500|Tor 0.2.7.6|larsgroeber7 <AT> gmail <DOT> com - 112RbQSfrccaPGc1ufYo4BK3H45xNcD1cM
85.93.16.47|alterspalter|9001|9030|FGHRSDV|1466829|Tor 0.2.8.12|Tor <tor AT alterspalter dot de>
85.93.17.143|ripde|9001|0|FHRSDV|629525|Tor 0.2.9.9|
85.93.209.44|0x3d003|19001|19030|FGHRSDV|2556670|Tor 0.3.0.2-alpha-dev|tor at 0x3d dot lu - 1x3dG3utS7FDrTtJutnR3zuCo4Z8fUUAL
85.93.217.20|Lucloud|9001|0|FHRSDV|3256169|Tor 0.2.8.10|
85.93.218.204 HelpCensoredOnes|9001|9030|EFGHRSDV|5339477|Tor 0.2.5.12|tor at localhost dot lu
86.101.127.122|Unnamed|9001|9030|FHRSDV|9419400|Tor 0.2.6.10|
86.103.176.214|AbseitsTOR|9001|0|RV|83|Tor 0.2.5.12|
86.104.15.15|cheik|443|80|FGHRSDVX|6579913|Tor 0.2.6.10|
86.105.212.130|firstor2|443|9030|FGHRSDV|9828668|Tor 0.2.5.12|tor terjan net
86.105.212.204|torpidsFRtechcrea|443|80|FGHRSDV|5227319|Tor 0.3.0.1-alpha|torpids AT yahoo dot com - 1JYHfzVFVD7n2Sezz3DEHDFgGYjQWpDjqF
86.106.137.6|papadouka|443|80|FGHRSDV|7505509|Tor 0.2.6.10|

THE ONION ROUTER (Comprobación)

Herramienta comprobación: https://www.dan.me.uk/torcheck

IP to Query: 85.93.218.204 Check!

Output from TOR Node Checker tool:

```
% TOR Node Checker Tool
% Copyright(c) 2017, Daniel Austin MBCS.
%
% Hello, 109.163.234.5, pleased to meet you.
%
% Checking IP: 85.93.218.204
%
Status: ACK
Exit-Node: ACK
% TOR-Name: HelpCensoredOnes
% TOR-Onion-Port: 9001
% TOR-Directory-Port: 9030
% TOR-Flags: Exit Fast Guard HSDir Running Stable V2Dir Valid
% TOR-Exit-Node: ACK
```

THE ONION ROUTER

Para la instalación en Linux:

apt-get install tor

Solo permitirá usar el proxy de *TOR*, que trabaja como proxy para sockets, no para tráfico HTTP.

/etc/init.d/tor start

Se podría usar para canales IRC, mensajería instantánea y pasarla a través del puerto donde está escuchando TOR (http://proxychains.sourceforge.net/)