Anonima Tor

OWASP

Bio

#whoami

Administración General del Estado

Master Social Media Universidad de Sevilla

CoLeader OWASP Sevilla

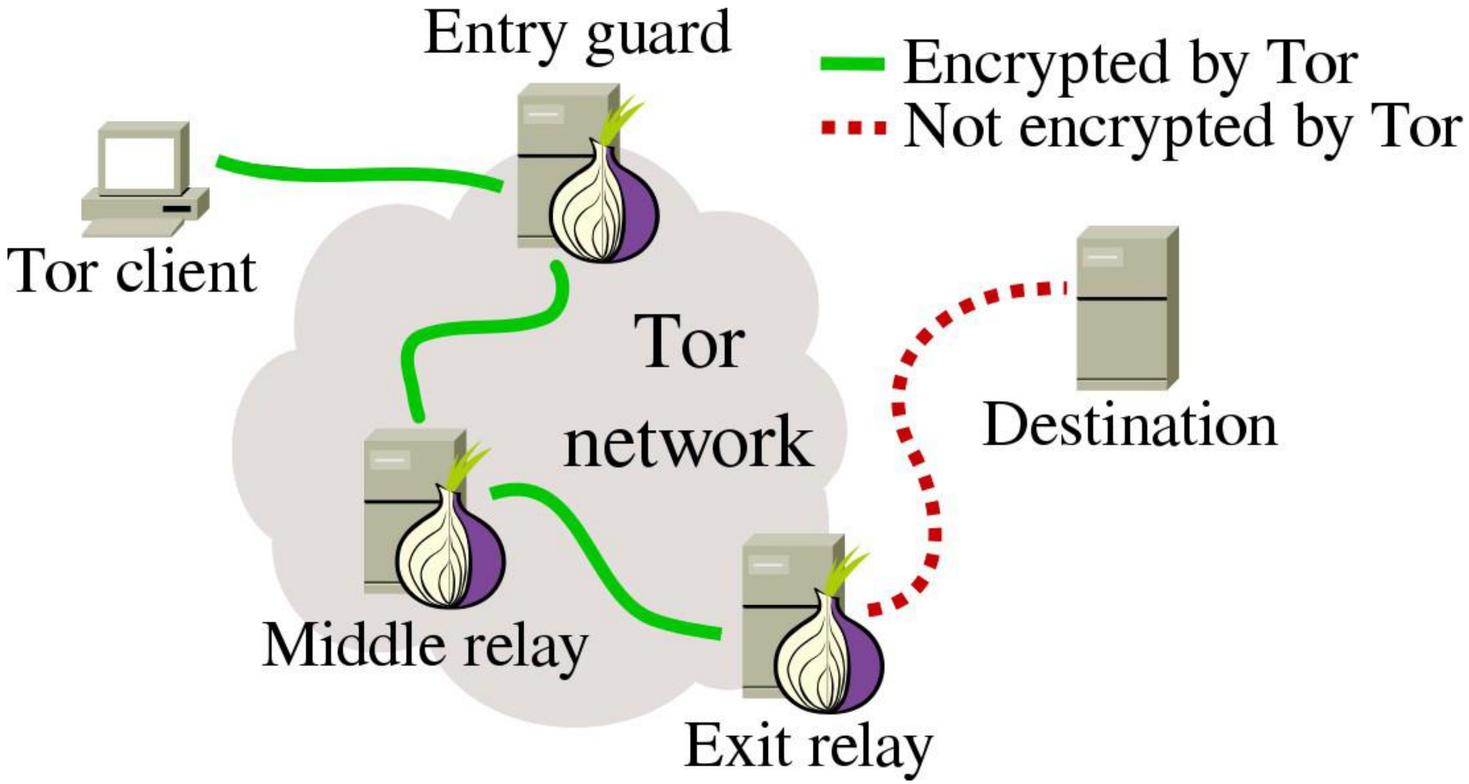
CiberCooperante de INCIBE

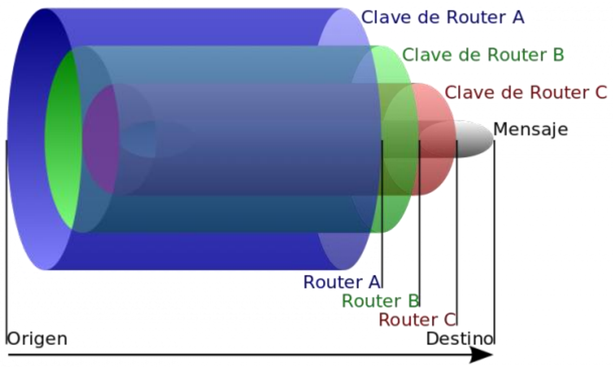
10 años de experiencia en Sistemas y Seguridad

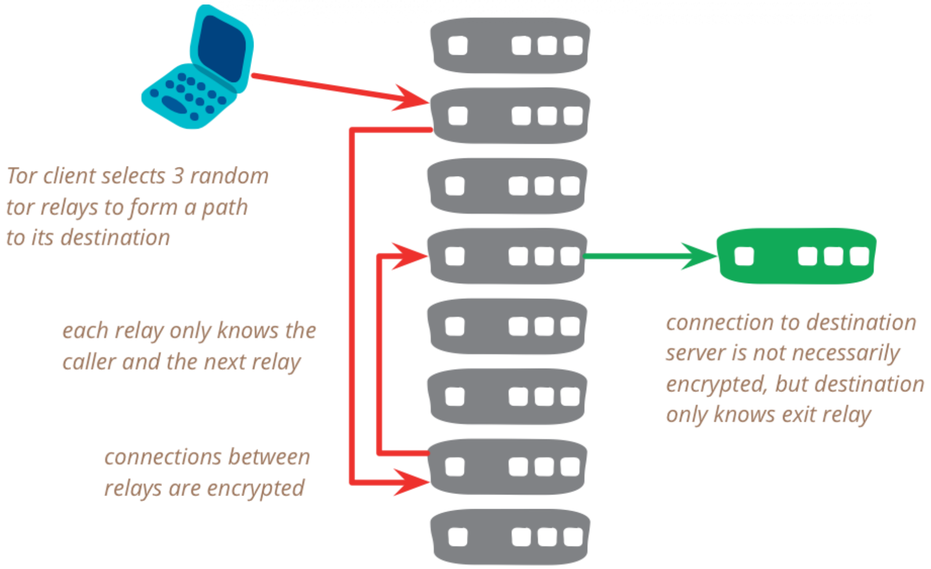
5 años en Desarrollo y Seguridad en WordPress

AnonimaTOR

The Onion Router







CIFRA LA INFORMACIÓN A SU ENTRADA
Y LA DESCIFRA A LA SALIDA

AnonimaTOR

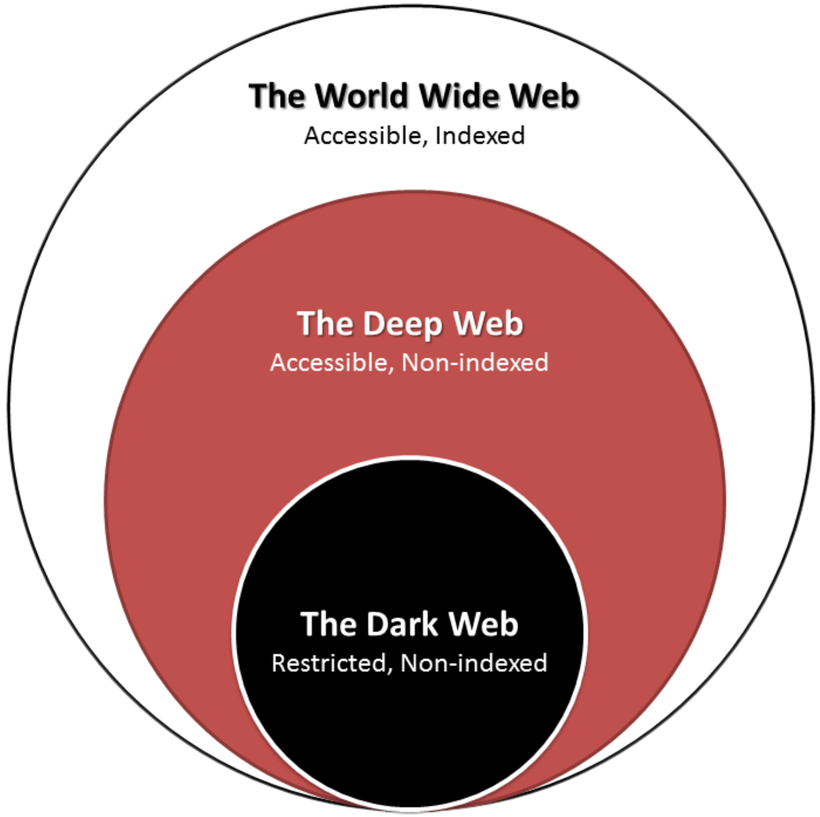
Visión General

Visión negativa de la red, cuando su fin es la privacidad y el anonimato.

En su origen, nace como una herramienta contra la censura .

AnonimaTOR

Visión más Real



ES PRACTICAMENTE IMPOSIBLE SABER SU PESO

AnonimaTOR

Alternativas a TOR

freenet 2000

Tor 2002

I2P 2003

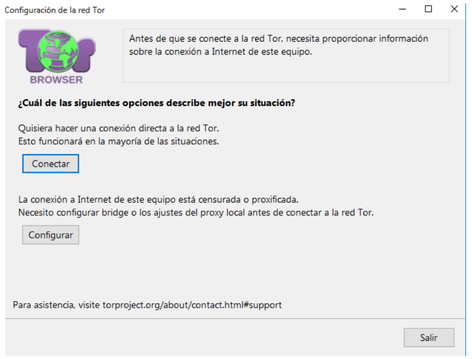
JoNDo

ZeroNet

GNUnet

AnonimaTOR

Métodos de Acceso

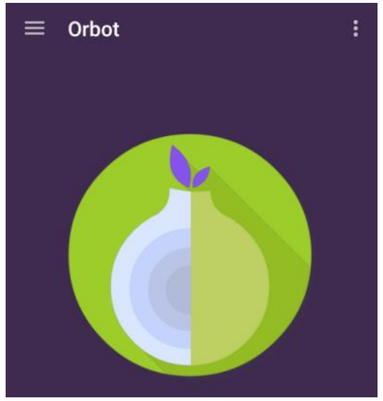


TOR Browser

Tails

OnionPi

TOR Phone



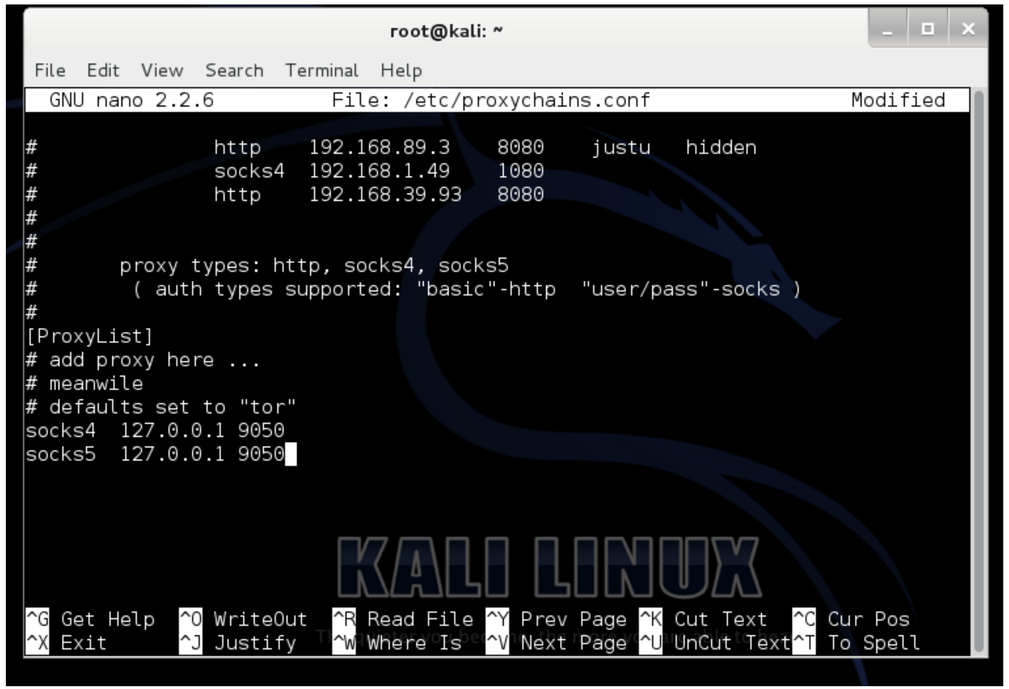
Orbot y Orfox

...

AnonimaTOR

Mejorando TOR

Firefox permite convertir tanto el tráfico DNS como el HTTP a SOCKS5 y enviárselo al cliente Tor



TORSOCK

PROXYXHAINS

PRIVOXY

POLIPO

…

VPN?

AnonimaTOR

TOR y VPN

¿VPN+TOR?

¿TOR+VPN?

AnonimaTOR

The Onion Router

LAS DIRECCIONES ONION SON 16 CARACRERES (A-Z Y 1-16), SE BASAN EN UNA CLAVE PRIVADA QUE ES LA QUE LO GENERA, NO PODEMOS ELEGIRLO PERO SI FORZARLO (SHALLOT GITHUB)

zqktlwi4fecvo6ri.onion.to
kbhpodhnfxl3clb4.onion

AnonimaTOR

LOS NODOS

https://uncharted.software/blog/2016/01/torflow/

AnonimaTOR

LOS NODOS

Más links

https://hackertarget.com/tor-exit-node-visualization/
https://torstatus.blutmagie.de/
https://check.torproject.org/exit-addresses
https://www.dan.me.uk/tornodes
https://uncharted.software/blog/2016/01/torflow/
https://exonerator.torproject.org/
https://atlas.torproject.org/
https://explorer.ooni.torproject.org/world/

AnonimaTOR

torrc

```
  GNU nano 2.3.4            File: /etc/tor/torrc                    Modified


## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

HiddenServiceDir /var/lib/tor/
HiddenServicePort 80 127.0.0.1:8080

#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22

################ This section is just for relays #####################
#
## See https://www.torproject.org/docs/tor-doc-relay for details.


^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

torrc MaxCircuitDirtness

ExitNodes {es}

ExcludeExitNodes {fr}

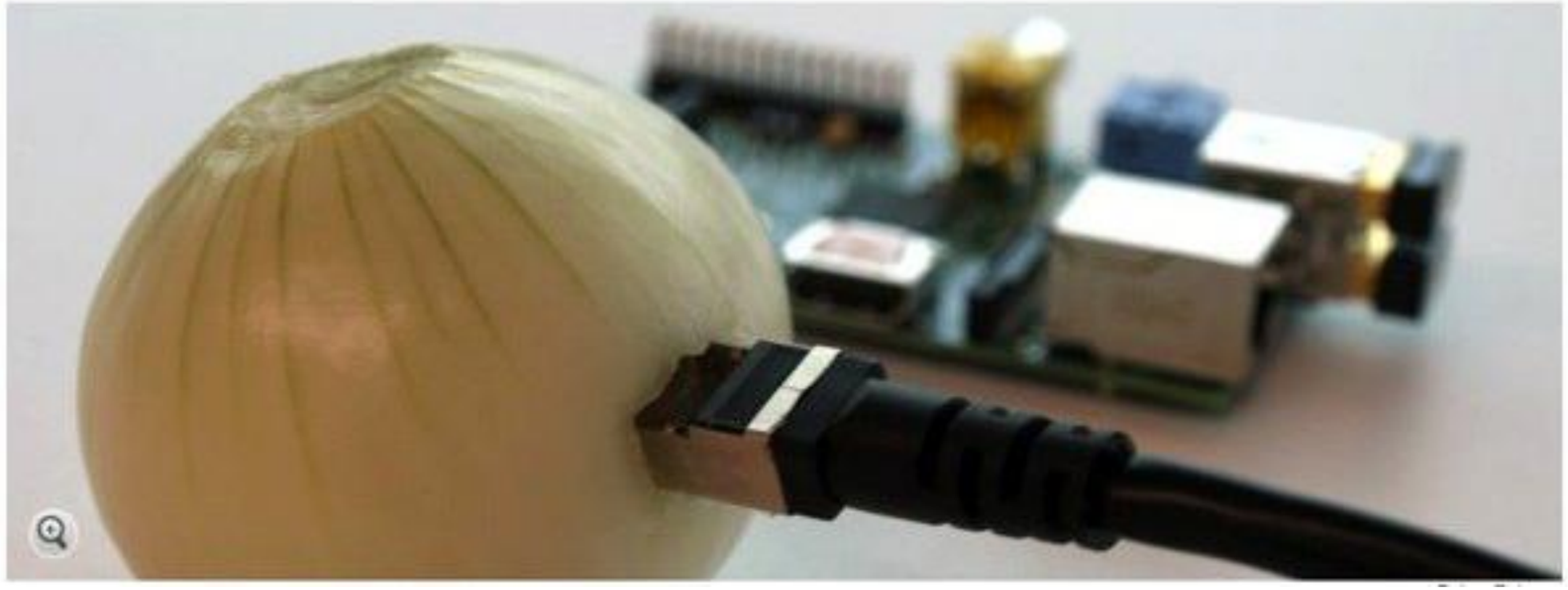
…

AnonimaTOR

CONSEJOS

- DESHABILITAR COOKIES
- NO PLUGINS JAVA, FLASH O ACTIVEX
- NOSCRIPT
- CUIDADO CON JAVASCRIPT
- DESHABILITANDO EL HISTORIAL
- REDIRIGIR EL TRÁFICO HACIA UN PROXY WEB INTERMEDIO (PRIVOXY O POLIPO)
- UTILIZAR SSL (HTTPS)
- EVITAR ‘CONEXIONES RUTINARIAS’
- PARA EVITAR BLOQUEOS UTILIZAR PROXY WEB

TorPi



TorPi. Fase I: Punto de Acceso

```
sudo apt-get install hostapd isc-dhcp-server

sudo nano /etc/dhcp/dhcpd.conf

    #option domain-name "example.org";
    #option domain-name-servers ns1.example.org,

    ns2.example.org;
    subnet 192.168.12.0 netmask 255.255.255.0 {
    range 192.168.12.5 192.168.12.50;
    option broadcast-address 192.168.12.255;
    option routers 192.168.12.1;
    default-lease-time 600;
    max-lease-time 7200;
    option domain-name "local";
    option domain-name-servers 8.8.8.8, 8.8.4.4;
    }
```

TorPi. Fase I: Punto de Acceso

```
sudo nano /etc/default/isc-dhcp-server
        INTERFACES="wlan0"

sudo ifdown wlan0

sudo nano  /etc/network/interfaces
        iface wlan0 inet static
        address 192.168.12.1
        netmask 255.255.255.0

sudo ifconfig wlan0 192.168.12.1
```

TorPi. Fase I: Punto de Acceso

```
sudo nano /etc/hostapd/hostapd.conf
        interface=wlan0
        ssid=TorPi
        hw_mode=g
        channel=6
        macaddr_acl=0
        auth_algs=1
        ignore_broadcast_ssid=0
        wpa=2
        wpa_passphrase=OwaspSevillaDemo
        wpa_key_mgmt=WPA-PSK
        wpa_pairwise=TKIP
        rsn_pairwise=CCMP

sudo nano /etc/default/hostapd
                DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

TorPi. Fase II: NAT

```
sudo nano /etc/sysctl.conf
        net.ipv4.ip_forward=1
sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo iptables -A FORWARD -i eth0 -o wlan0 -m state –state RELATED, ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"
sudo nano /etc/network/interfaces
    up iptables-restore
sudo service hostapd start
sudo service isc-dhcp-server start
sudo update-rc.d hostapd enable
sudo update-rc.d isc-dhcp-server enable
```

TorPi. Fase III: Tráfico a TOR

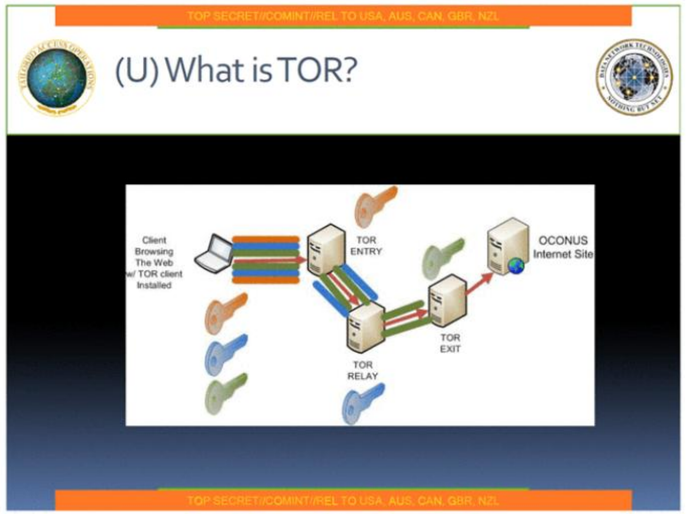
```
sudo apt-get install tor

sudo nano /etc/tor/torrc
    Log notice file /var/log/tor/notices.log
    VirtualAddrNetwork 10.192.0.0/10
    AutomapHostsSuffixes .onion,.exit
    AutomapHostsOnResolve 1
    TransPort 9040
    TransListenAddress 192.168.12.1
    DNSPort 53
    DNSListenAddress 192.168.12.1

sudo iptables -F

sudo iptables -t nat -F
```

TorPi. Fase III: Tráfico a TOR

```
sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 22 -j REDIRECT --to-ports 22
sudo iptables -t nat -A PREROUTING -i wlan0 -p udp --dport 53 -j REDIRECT --to-ports 53
sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --syn -j REDIRECT --to-ports 9040
sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"
sudo service tor start
sudo update-rc.d tor enable
sudo reboot
```

https://check.torproject.org

TorPi. Fase III: Tráfico a TOR



LINK

¿ANÓNIMO?


```
Client rects:
{"bottom":473.5999755859375,"height":18.399993896484375,"left":342.01998
90136719,"right":1013.21997703125,"top":455.1999816894531,"width":671.1
99951171875}

scrolling milis:
[5,5,2,5,3,5,72,5,3,5,5,82,4,5,2,5,130,5,3,5,5,10,468,5,3,5,5,5,10,60,5,
2,3,5,2,5,5,67,5,2,5,5,5,7]

scrolling deltas:
[109.6500015258789,109.6500015258789,109.6500015258789,109.6500015258789
,109.6500015258789,109.6500015258789,109.6500015258789,109.6500015258789
,109.6500015258789,109.6500015258789,109.6500015258789,109.6500015258789
,109.6500015258789,109.6500015258789,109.6500015258789,109.6500015258789
,109.6500015258789,109.6500015258789,109.6500015258789,109.6500015258789
,109.6500015258789,109.6500015258789,109.6500015258789,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0]

Biggest mouse step: 87.6199951171875
```


This is a test that tries to identify who are you based on how you interact with your computer, the input hardware you have, the computing power of your computer, the memory speed of your computer and similar things.

Each one of this little things reveal bits of entropy about who you are.

IMPORTANT: try to behave normal, like you would do while surfing the web, simply use this web

LINK

LINK

PRIVACIDAD Y ANONIMATO

Ramón Salado

@ramon_salado