|  |
| --- |
| Anonimizarea |
|  |
| Laboratorul Nr.11 |
|  |
|  |

### [Laborator](https://sectrain.usv.ro/mod/page/view.php?id=12): Anonimizarea

# Obiective:

* Introducere
* Iluzia anonimatului
* Instalarea și configurarea aplicației TOR
* Crearea unui nou circuit în TOR
* Instalarea, configurarea și utilizarea aplicației ProxyChains

# Introducere

Internet-ul este o invenție extraordinară, care ne-a permis să accesăm aproape orice informație de pe planetă, dar în același timp a "dăruit" tutoror accesul la datele noastre private. Aproape pe orice site am merge suntem urmăriți și profilați, totate interesele, toate hobby-urile, toate datele personale: numele, numărul de telefon, adresa de email, adresa fizică, țara în care ne aflăm, totul este colectat (adesea fără permisiunea noastră) și scos la licitație!

Din acest motiv trebuie să ne putem anonimiza conexiunea.

# Iluzia anonimatului

Următoarele metode **NU** anonimizează conexiunea:

**VPN (Virtual Private Network)**

VPN-ul **NU** reprezintă o metodă de anonimizare.

În schimb VPN-ul previne interceptarea traficului de către o persoană neautorizată



Server-ul de VPN poate intercepta traficul către site-uri care nu folosesc HTTPS. Din acest motiv este foarte important ca serverul de VPN să fie unul de încredere! (NU VPN gratis)
De asemenea, server-ul VPN cunoaște IP-ul public al clientului și îl poate trece în log-uri!

# Tipuri de VPN:

* ~~PPTP~~ (DEPRECIAT, NESIGUR, NU UTILIZAȚI!)
* L2TP, IKEv2 - VPN pe bază de IPSec (A se utiliza cu criptare AES-256, NU 3DES)
* OpenVPN (A se utiliza cu criptare AES-256-GCM)

**Proxy (HTTP, HTTPS, SOCKS)**

Proxy-urile HTTP și SOCKS NU dispun de criptare! Doar cele HTTPS dispun de criptare.

Proxy-urile sunt destul de inacdevacte pentru anonimizare.

Se pot utiliza mai multe proxy-uri deodată, cu ajutorul applicației ProxyChains

# **TOR (The Onion Router)**

TOR este o rețea **decentralizată**.

Programul pentru a accesa TOR construiește un circuit prin 3 noduri, ca în figura de mai jos:



Request-ul web este criptat inițial cu cheia publică a fiecărui nod! (se formează 3 straturi de criptare)



Când mesajul criptat trece prin primul nod, se înlatura stratul A de criptare, în al doilea nod se înlătură stratul B, iar în exit node se înlătură ultimul strat C și requestul (decriptat) este redirecționat către destinație



Nodurile 1 și 2 NU au acces la mesaj, dar ultimul nod poate intercepta mesajul dacă acesta nu este criptat TLS (adică HTTPS), exact ca la VPN!

Deci nici TOR **NU** anonimizează conexiunea.

**În concluzie: NU EXISTĂ ANONIMIZARE COMPLETĂ.**

# Instalarea și configurarea aplicației TOR

TOR se poate instala pe orice distributie de Linux bazată pe Debian sau Ubuntu prin următoarea comandă:

sudo apt-get install tor



Pentru a porni TOR se execută următoarea comandă:

sudo systemctl start tor

Pentru a verifica dacă TOR rulează:

sudo systemctl status tor



Următorul pas este configurarea browserului să utilizeze TOR

TOR emulează un SOCKS5 Proxy pe portul 9050, LOCAL! dar transmite totul criptat în exterior.

Deci, se setează browser-ul să utilizeze proxy-ul 127.0.0.1:9050



Se verifică dacă conexiunea a fost realizată intrând pe site-ul www.iplocation.net

####

#### Crearea unui nou circuit

Pentru a genera un nou circuit se utilizează comanda:

sudo systemctl reload tor

Și apoi verificând se vede un nou IP!

####

#### Instalarea, configurarea și utilizarea aplicației ProxyChains

ProxyChains se poate instala pe orice distributie de Linux bazată pe Debian sau Ubuntu prin următoarea comandă:

sudo apt-get install proxychains



În configurația implicită, ProxyChains nu utilizează decât proxy-ul TOR. Dar se pot adăuga și alte proxy-uri.



ProxyChains poate fi utilizat pentru a forța aplicații care nu suportă proxy să comunice prin TOR.

De exemplu, pentru utilitarul *curl* și icanhazip.com (site de tip what's my ip compatibil curl)

