

# Traffic Obfuscation Quick Reference

For Ethical Hackers

---

## Obfs4proxy Installation

Update system:

```
bash  
sudo apt update && sudo apt upgrade -y
```

Install obfs4proxy:

```
bash  
sudo apt install obfs4proxy
```

Verify installation:

```
bash  
obfs4proxy --version
```

---

## Tor Configuration

Install Tor Browser:

```
bash  
sudo apt install torbrowser-launcher
```

Edit Tor config:

```
bash  
sudo vim /etc/tor/torrc
```

## Add bridge configuration:

```
UseBridges 1
ClientTransportPlugin obfs4 exec /usr/bin/obfs4proxy
Bridge obfs4 <IP>:<PORT> <FINGERPRINT> cert=<CERT> iat-mode=0
Log notice file /var/log/tor/tor.log
```

Get bridges from: <https://bridges.torproject.org/>

---

## Service Management

### Create log directory:

```
bash

sudo mkdir -p /var/log/tor
sudo touch /var/log/tor/tor.log
sudo chown -R debian-tor:debian-tor /var/log/tor
```

### Restart Tor:

```
bash

sudo systemctl restart tor
```

### Check status:

```
bash

sudo systemctl status tor
```

### Monitor logs:

```
bash

sudo tail -f /var/log/tor/tor.log
sudo journalctl -u tor
```

---

## Testing Connection

### Test Tor connectivity:

```
bash  
curl --socks5-hostname 127.0.0.1:9050 https://check.torproject.org
```

### Check external IP:

```
bash  
curl --socks5 127.0.0.1:9050 -4 ifconfig.me  
curl --socks5 127.0.0.1:9050 -4 icanhazip.com  
curl --socks5 127.0.0.1:9050 -4 api64.ipify.org
```

---

## Troubleshooting

### Connection refused:

- Check Tor service: `sudo systemctl status tor`
- Verify bridge configuration in torrc
- Try different bridge from torproject.org

### Slow speeds:

- Switch to different obfs4 bridge
- Check network throttling

### Binary issues:

- Verify installation: `which obfs4proxy`
- Check permissions: `ls -l /usr/bin/obfs4proxy`

---

## Use Cases

- Bypassing government censorship
- Evading corporate firewalls

- Hiding penetration testing traffic
- Avoiding deep packet inspection (DPI)
- Accessing blocked websites in restrictive environments