# VPN Setup & Security Quick Reference

**For Ethical Hackers**

---

## OpenVPN Installation

**Install OpenVPN:**

```bash
sudo apt update
sudo apt install openvpn
```

**Connect to VPN:**

```bash
sudo openvpn --config /etc/openvpn/config.ovpn
```

---

## Configuration File Types

**TCP vs UDP:**

- TCP Port 443: Reliable, rarely blocked
- UDP Port 53: Faster, good for streaming
- TCP Port 80: Works behind firewalls

**Move config file:**

```bash
sudo cp /path/to/vpnbook-*.ovpn /etc/openvpn/
```

---

## Testing Your Connection

**Check IP Address:**

```bash
curl ifconfig.me
```

**DNS Leak Test:** Visit dnsleaktest.com

**IPv6 Leak Prevention:**

```bash
sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1
```

**Make permanent in /etc/sysctl.conf:**

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

---

## Log Management

**View logs:**

```bash
sudo cat /var/log/openvpn.log
```

**Disable logging (add to config):**

```
log /dev/null
verb 0
```

**Clear logs:**

```bash
sudo rm /var/log/openvpn.log
```

---

## Quick IP Reset

**Reset router for new IP:**

- Unplug router for 30 seconds
- Or manually release/renew DHCP lease

---

## VPN Provider Selection

**Look for:**

- No-log policy
- OpenVPN support
- Privacy-friendly jurisdiction

**Avoid:**

- Five Eyes countries (US, UK, Canada, Australia, New Zealand)
- Providers that log data