ProxyChains Cheat Sheet — Kali Linux

Purpose

- Route network traffic through one or more proxies to hide your real IP.
- Useful for Tor integration, chaining free/paid proxies, and preventing DNS leaks.

File location

`/etc/proxychains.conf`

Open as root

```
su
leafpad /etc/proxychains.conf
```

Chain types (choose one)

- **strict_chain** — Proxies used in fixed order; *all* must be online.
- **dynamic_chain** — Skips dead proxies automatically. **Recommended.**
- **random_chain** — Uses random proxies each request.

Enable dynamic_chain: uncomment the `dynamic_chain` line and comment the other two.

Protect against DNS leaks

Uncomment this line in the config to prevent DNS leakage:

```
proxy_dns
```

This forces DNS resolution through the proxy chain (no accidental leak of your real IP).

ProxyList format (at bottom of file)

Under the `[ProxyList]` header, each line must follow this format:

```
[type]  [host]        [port]  [user] [pass]
```

- `type` : `socks4` , `socks5` , or `http`
- `host` : proxy IP or hostname
- `port` : numeric port
- `user pass` : optional credentials for paid proxies

Example entries:

```
socks5  127.0.0.1    9050
socks4  192.168.1.49 1080
http    203.0.113.5   8080  paiduser secret
```

Tor defaults — add socks5 entry

ProxyChains often ships with `socks4 127.0.0.1 9050`. Add a socks5 line for modern compatibility:

```
socks5 127.0.0.1 9050
```

Commands — check/start Tor

```
service tor status
service tor start     # start Tor if not running
```

Run a browser (through ProxyChains)

```
proxychains firefox www.duckduckgo.com
# or for the Tor Browser you usually use the tor-browser launcher directly
```

Test for leaks

- Visit a DNS leak test site (e.g., `dnsleaktest.com`) while using `proxychains` and compare with your normal browser.
- Expected: the test shows a proxy/foreign IP, not your real local IP.

Quick checklist (before testing)

-

Common troubleshooting

- **No connection / fails**: If `strict_chain` is enabled, ensure all listed proxies are alive or switch to `dynamic_chain`.
- **DNS leak showing real IP**: Confirm `proxy_dns` is uncommented and retest.
- **Tor not starting**: Check logs (`journalctl -u tor` or `/var/log/tor/`) and ensure port `9050` is open locally.
- **Slow browsing**: Chained proxies add latency. Test removing slower proxies.

Tips & Notes

- Use `dynamic_chain` for resilience — it automatically skips dead proxies.
- Keep paid-proxy credentials off public or shared systems.
- Test with a privacy-focused search engine (duckduckgo) and DNS leak tests while connected.
- Chaining many proxies increases fingerprinting risk and latency — prefer Tor + single proxy when appropriate.
