## 🛠 Tool Name:

Proxychains

## 🕘 History

Originally developed as a Unix-based utility, Proxychains was designed to force any TCP connection made by any given application through a proxy—most commonly SOCKS or HTTP proxies. It’s widely used in the ethical hacking, red teaming, and penetration testing community.

## 📄 Description:

A command-line tool used to route network connections through a series of proxy servers to anonymize traffic and bypass restrictions.

## 📌 What Is This Tool About?

Proxychains is used to anonymize network activity by chaining multiple proxies. It wraps a program's network calls and forces them through user-defined proxy servers, making it a powerful utility for penetration testers and those seeking to maintain privacy.

## ⭐ Key Characteristics / Features:

* • Supports SOCKS4, SOCKS5, and HTTP proxies
* • Dynamic, strict, and random chaining modes
* • Easy configuration via proxychains.conf
* • Compatible with most Linux tools (nmap, curl, firefox, etc.)
* • Helps bypass IP-based restrictions
* • Useful for geographical spoofing
* • Works without modifying source code of target applications
* • Allows chaining through Tor
* • Supports DNS through proxy
* • Lightweight and terminal-based
* • Supports proxy authentication
* • Can be used in scripting/automation
* • Integrates well with Kali Linux and other pen-test distros
* • Can anonymize brute force and scanning tools
* • Maintained by the open-source community

## 🔧 Types / Modules Available:

* • Proxychains (original version)
* • Proxychains-NG (Next Generation – better maintained and enhanced)
* • Dynamic chaining
* • Strict chaining
* • Random chaining
* • Configuration File Parser Module

## 🎯 How Will This Tool Help?

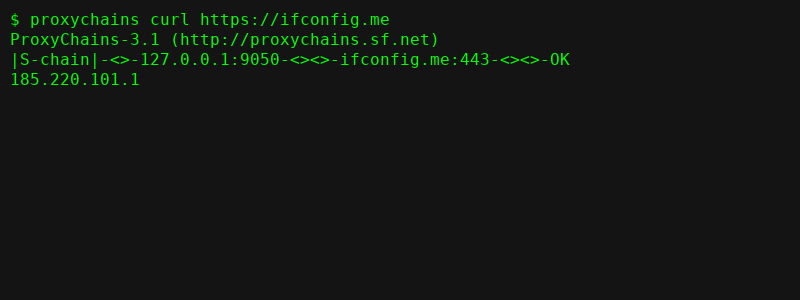
* • Hides the source IP address during security testing
* • Bypasses geographical and IP-based restrictions
* • Enables private access to blocked services
* • Used for anonymous scanning and reconnaissance
* • Helps simulate attacker behavior in red team assessments
* • Protects against retaliation during ethical hacking exercises

## 🖼 Proof of Concept (PoC) Images:

Screenshot: proxychains\_nmap.png



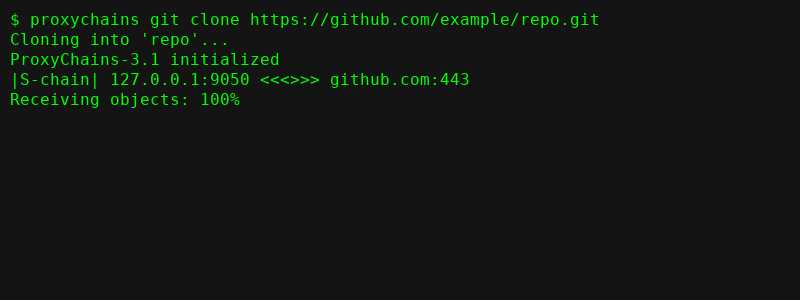
Screenshot: proxychains\_curl.png



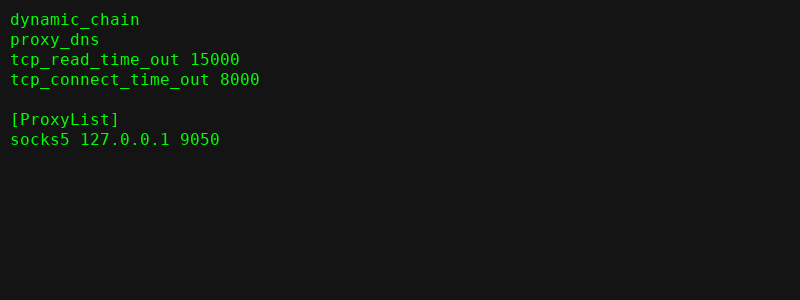
Screenshot: proxychains\_firefox.png



Screenshot: proxychains\_git.png



Screenshot: proxychains\_conf.png



## 🧾 15-Liner Summary:

* • Forces TCP traffic through proxies
* • Supports SOCKS4, SOCKS5, and HTTP
* • Lightweight and command-line driven
* • Compatible with most pen-test tools
* • Helps anonymize offensive security operations
* • Allows strict/dynamic/random proxy chaining
* • Enables use of multiple proxy servers
* • Useful in censorship bypass
* • Ideal for red team and privacy advocates
* • Works with Tor for high anonymity
* • Supports proxy authentication
* • Customizable via simple config file
* • Minimal system resource usage
* • DNS through proxy supported
* • Well-documented and open-source