

Forum:[Hack Forums](#)

Thread: [Educational Only: Proxychains for On-path Attacks](#)

Tyr - November 24, 2024, 11:38 am

Ultimate Guide: Using Proxychains on Kali Linux for IP Masking and On-Path Attacks

1. What is Proxychains?

Proxychains is a tool used to route network traffic through multiple proxy servers (SOCKS, HTTP, HTTPS) to obscure the source IP address. It allows penetration testers to anonymize their activity while interacting with services such as SSH, HTTP, FTP, or other network protocols.

Why Use Proxychains?

- To hide your real IP address during penetration tests.
- To chain multiple proxies for added anonymity.
- To bypass network restrictions or firewalls.

2. Installing and Configuring Proxychains

a. Install Proxychains

Proxychains is pre-installed on Kali Linux. If it is missing, install it by running:

Code `sudo apt install proxychains`

b. Edit the Configuration File

The main configuration file for Proxychains is:

Code `/etc/proxychains.conf`

Open the file using a text editor like `nano`:

Code `sudo nano /etc/proxychains.conf`

Key Sections to Edit:

1. Proxy Mode:

- Uncomment the desired mode:
Code `# dynamic_chain`
`strict_chain`
`# random_chain`
 - `dynamic_chain`: Routes traffic through a sequence of proxies; skips unavailable proxies.
 - `strict_chain`: Uses proxies in order; fails if one proxy is down.
 - `random_chain`: Selects proxies randomly from the list.

2. DNS Settings:

Uncomment the line to route DNS requests through the proxy:

Code `proxy_dns`

3. Add Proxies:

Add your proxy servers to the bottom of the file. Each line should be in this format:

Code `type IP_address port`

Example:

Code `socks4 127.0.0.1 9050`

`http 192.168.1.100 8080`

`socks5 10.0.0.1 1080`

Save the file with `Ctrl + O` and exit with `Ctrl + X`.

3. Testing Proxychains

a. Check Proxies

To verify that Proxychains is working, use the `curl` command:

Code `proxychains curl https://ifconfig.me`

This should display the IP address of the proxy server rather than your real IP.

b. Debug Mode

Run Proxychains in debug mode to see how traffic flows through each proxy:

Code `proxychains -d curl https://ifconfig.me`

4. Using Proxychains with Common Tools

a. Using Nmap

Perform a masked Nmap scan through a proxy chain:

Code `proxychains nmap -sT -Pn 192.168.1.1`

b. SSH Through Proxychains

Connect to an SSH server while masking your IP:

Code `proxychains ssh user@192.168.1.100`

c. Web Browsing

Launch a browser (like Firefox) with Proxychains:

Code `proxychains firefox`

d. Exploitation Frameworks

Use Proxychains with Metasploit:

Code `proxychains msfconsole`

5. Advanced Proxychains Scenarios

a. Chaining Multiple Proxies

You can add multiple proxies to create a chain, increasing anonymity:

Code `socks5 127.0.0.1 9050`

`http 192.168.1.2 8080`

`socks4 192.168.1.3 1080`

With this setup, traffic will pass through all these proxies in the specified mode.

b. Using Tor with Proxychains

Tor is a popular option for routing traffic anonymously. To use Tor with Proxychains:

1. Start the Tor service:

Code `sudo service tor start`

2. Add the Tor proxy to the configuration file:

Code `socks5 127.0.0.1 9050`

3. Run any tool through Proxychains with Tor:

Code `proxychains curl https://ifconfig.me`

c. On-Path Attacks with Proxychains

For educational purposes, use Proxychains with on-path attack tools like Bettercap or Ettercap.

Example with Bettercap:

Code `proxychains bettercap -iface eth0 -eval "set arp.spoof.targets 192.168.1.105; arp.spoof on"`

d. Avoiding Proxy Detection

Some services may block proxies. To avoid detection, use a mix of residential proxies and rotate IP addresses frequently.

6. Troubleshooting Tips

- Proxy Timeout: If connections fail, ensure the proxies are online and reachable.
- DNS Leaks: Ensure `proxy\_dns` is enabled in the configuration to avoid exposing your real IP via DNS queries.
- Proxy Order Issues: Use dynamic chaining to skip over unreliable proxies.

7. Ethical Considerations

Proxychains is a powerful tool. Use it responsibly:

- Only test systems where you have explicit authorization.
- Do not use Proxychains for illegal activities.

Proxychains is a valuable tool for ethical hackers. Use it wisely and ethically to enhance your cybersecurity skills.

RedditAccountSeller - November 25, 2024, 6:44 pm

Really interesting, thanks for sharing.

Tyr - November 25, 2024, 6:44 pm

(Nov 25, 2024 07:44 PM)RedditAccountSeller Wrote: [\[CITE\]](#) Really interesting, thanks for sharing. Hope you gained something beneficial from this. You're welcome.