Proxychains Traffic Analysis Quick Reference

For Ethical Hackers

Traffic Monitoring Setup

Start Tshark capture:

```bash
sudo tshark -i eth0 -f "host [target_ip]" -w proxychains_capture.pcap
```

Example with Metasploitable2:

```bash
sudo tshark -i eth0 -f "host 192.168.1.10" -w proxychains_capture.pcap
```

Nmap with Proxychains

Service discovery:

```bash
proxychains4 nmap -sV -Pn [target_ip]
```

Vulnerability scan:

```bash
proxychains4 nmap --script vuln [target_ip]
```

Verify proxy routing:

```bash
proxychains4 curl ifconfig.me
```

Wireshark Analysis

Open capture file:

```bash
wireshark proxychains_capture.pcap
```

Key filters:

```
dns                    # DNS traffic
ip.addr == [your_local_ip]    # Direct traffic from your IP
tcp.port == 443            # TLS/SSL encrypted traffic
```

What to Look For

Proxy routing verification:

- Traffic originates from proxy IPs, not your real IP
- Follow TCP streams to check source IPs
- No direct connections from your machine

Encrypted traffic:

- Most traffic on port 443 (TLS/SSL)
- No plaintext HTTP requests
- No exposed credentials

DNS leak detection:

- DNS queries routed through proxies
- No queries to your ISP's DNS servers
- proxy_dns option enabled in config

Suspicious traffic:

- Direct HTTP requests bypassing proxy

- ICMP packets from your real IP
- Unexpected delays or dropped packets

Troubleshooting

No output/slow scans:

- Check proxy list in /etc/proxychains4.conf
- Reduce number of proxies
- Use dynamic_chain mode

Connection refused:

- Update proxy list
- Try different proxy types
- Use paid proxies for reliability

DNS leaks:

- Enable proxy_dns in config
- Test with dnsleaktest.com