Cloudflare & CDN Bypass Quick Reference

Host Header Poisoning

```bash
# Test for host header injection
curl -H "Host: target.com" https://target.com/

# Try different host values
curl -H "Host: admin.target.com" https://target.com/
curl -H "Host: internal.target.com" https://target.com/
```

SSL Certificate Analysis

```bash
# Extract SSL certificate details
openssl s_client -connect target.com:443 2>/dev/null | \
openssl x509 -noout -text | grep "DNS:"

# Get full certificate info
openssl s_client -connect target.com:443 -showcerts
```

DNS Historical Records

- **SecurityTrails:** https://securitytrails.com
- **DNSdumpster:** https://dnsdumpster.com
- Look for old A records before Cloudflare

LeakIX Search

- Visit: https://leakix.net
- Search by domain name
- Look for exposed services on backend IPs

Non-Standard Port Scanning

```bash
# Cloudflare proxied ports:
# HTTP: 80, 8080, 8880, 2052, 2082, 2086, 2095
# HTTPS: 443, 2053, 2083, 2087, 2096, 8443

# Scan non-proxied ports
nmap -p 8080,8443,8888 target.com --script http-server-header

# Check for internal IP disclosure
nmap --script http-internal-ip-disclosure target.com
```

Common CDN Bypass Techniques

- **Historical DNS records** (old IPs before CDN)
- **SSL certificate SANs** (subdomains)
- **Non-proxied ports** (direct server access)
- **Exposed services** (SSH, FTP, mail not behind CDN)
- **Misconfigured headers** (host header injection)

Defensive Tips

- Block direct IP access to origin server
- Configure web server to ignore arbitrary Host headers
- Ensure all services route through CDN
- Regular audit of DNS records and certificates