

KỸ THUẬT TÌM IP SERVER SAU CLOUDFLARE

Present: [Vietnix](#) - [ChongLuaDao.vn](#)



Nội dung

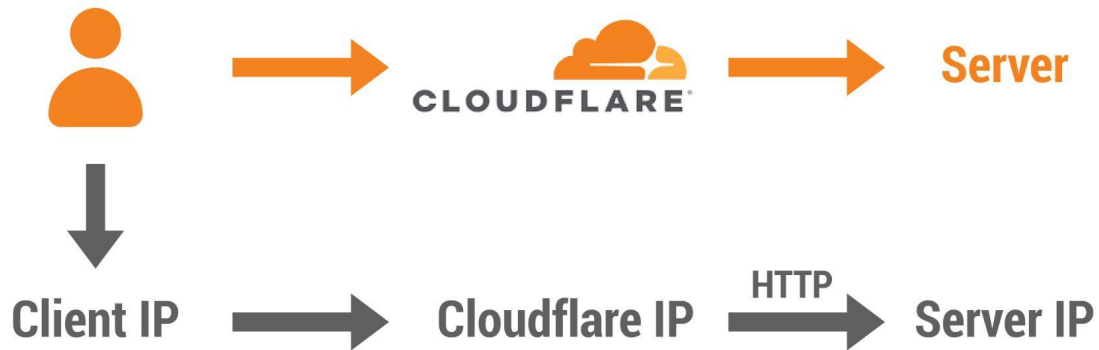
1. Disclaimer
2. Mô hình CloudFlare & Kiến thức liên quan
3. Truy vết bằng kỹ thuật
 - a. MX Record
 - b. Sub Domain
 - c. NS History
 - d. NS Default
 - e. Email Server
 - f. Ping
 - g. Remote Image
 - h. XMLRPC
 - i. NSLOOKUP + Ping
 - j. NMap
4. Truy vết bằng dữ liệu công khai
 - a. Shodan
 - b. Censys
 - c. Security Trails
 - d. ZoomEye
 - e. Dnsdumpster
 - f. Fofa.so
 - g. Tools Automation (Mitaka extension, CloudFail)



Disclaimer

- Tất cả các target (domain) sử dụng trong buổi trình bày đều được lựa chọn một cách ngẫu nhiên với mục đích demo phương pháp. Chúng tôi không chủ ý nhắm vào bất cứ cá nhân/tổ chức nào.
- Các kỹ thuật sử dụng đều khai thác các thông tin công khai và không xâm phạm, xâm nhập hoặc chiếm quyền điều khiển bất cứ mục tiêu nào.
- Các mục tiêu chỉ được sử dụng duy nhất cho mục đích học tập, nếu các cá nhân/tổ chức nào lợi dụng thông tin trong buổi thuyết trình để gây hại cho mục tiêu sẽ phải tự chịu hoàn toàn trách nhiệm trước pháp luật.
- Cuối cùng, chúng tôi xin thành thật xin lỗi vì bất cứ sự bất tiện nào đã gây ra cho các website mục tiêu.

Mô hình CloudFlare





Mô hình CloudFlare

- Reverse Proxy đứng giữa người dùng (Client) và Web Server (Backend)
- Forward các HTTP request hợp lệ từ người dùng về Backend
- WAF
- CDN, Caching Server
- Không forward các TCP/UDP/ICMP ... connection (trừ các gói cao cấp như Magic Transit, Spectrum - không nằm trong phạm vi bài hôm nay)
- Tham khảo thêm phần "Cơ chế hoạt động của CloudFlare" tại :
<https://blog.vietnix.vn/chong-ddos-bypass-cloudflare-bang-csf-p1.html>



Kiến thức liên quan

- Virtual Host: 1 IP chạy nhiều Website
- Default Virtual Host: khi truy cập vào 1 domain chưa được khai
- Truy cập vào Virtual Host thông qua IP bằng curl
 - Get content: `curl https://192.168.0.100 -H "Host: facebook.com"`
 - Get Header: `curl https://192.168.0.100 -H "Host: facebook.com" -I`
 - Không check Cert: `curl https://192.168.0.100 -H "Host: facebook.com" -k`
- hosts file: trỏ 1 domain về 1 IP cụ thể nhưng chỉ có tác dụng trên máy được cấu hình
 - `192.168.0.100 facebook.com` (+++ dành cho pentester khi kiểm được IP thật, tiện cho việc pentest)
- dig: tương tự nslookup - dùng để query DNS
 - `dig @8.8.8.8 vietnix.vn`
- NS = Nameserver: máy chủ chứa DNS record của domain
- Registrar: Nhà đăng ký tên miền
- whois: kiểm tra thông tin tên miền
 - `whois facebook.com`

TRUY VẾT BẰNG KỸ THUẬT





MX Record

- Demo: barmanandcompany.com
 - [host barmanandcompany.com](https://host.barmanandcompany.com)
- Nguyên nhân:
 - Không thay đổi/xóa bỏ MX record mặc định được import vào CloudFlare
 - Sử dụng mail server trên chính server chạy web
- Cách khắc phục:
 - Xóa bỏ MX record nếu không sử dụng.
 - Sử dụng các dịch vụ email của bên thứ 3 khác: Gmail, Outlook, Zoho



MX Record: nslookup + ping

- Demo: hickorybibletabernacle.org
 - Nslookup → set type=MX → hickorybibletabernacle.org và ping (nếu cần)
- Nguyên nhân:
 - Không thay đổi/xóa bỏ MX record mặc định được import vào CloudFlare
 - Sử dụng mail server trên chính server chạy web
- Cách khắc phục:
 - Xóa bỏ MX record nếu không sử dụng.
 - Sử dụng các dịch vụ email của bên thứ 3 khác: Gmail, Outlook, Zoho



Sub Domain

- Demo: hickorybibletabernacle.org
 - Ping hay host mail.hickorybibletabernacle.org
- Nguyên nhân:
 - Không thay đổi/xóa record của các subdomain.
 - Không cấu hình subdomain chạy qua CloudFlare
 - Subdomain không qua CloudFlare và dùng chung IP với Website
- Khắc phục
 - Xóa record của các subdomain không sử dụng
 - Cấu hình toàn bộ subdomain chạy qua CloudFlare
 - Sử dụng IP riêng cho các subdomain



Sub Domain: nmap

- Demo: [mail.hickorybibletabernacle.org](mailto:hickorybibletabernacle.org)
 - `nmap --script dns-brute -sn hickorybibletabernacle.org`
 - `nmap -sV -sS -F mail.hickorybibletabernacle.org`
- Nguyên nhân:
 - Không thay đổi/xóa record của các subdomain.
 - Không cấu hình subdomain chạy qua CloudFlare
 - Subdomain không qua CloudFlare và dùng chung IP với Website
- Khắc phục
 - Xóa record của các subdomain không sử dụng
 - Cấu hình toàn bộ subdomain chạy qua CloudFlare
 - Sử dụng IP riêng cho các subdomain



History of NS Server

- Demo: hanulstyle.com
 - `dig @ns2.slhosting.biz hanulstyle.com`
- Nguyên nhân
 - Không remove records ở Nameserver cũ sau khi chuyển qua dùng Nameserver của CloudFlare
- Cách khắc phục
 - Remove hết records liên quan domain ở Nameserver cũ



Default Nameserver of Registrar

- Demo:
 - **gmocloud.com** - Dựa vào SOA record: [ns.namedserver.net](#)
 - **uslustildus.com** - Whois registrar NS: [ns1.nicproxy.com](#)
- Nguyên nhân
 - Không xóa các DNS records khi sử dụng NS mặc định của Registrar sau khi chuyển qua CloudFlare
- Khắc phục
 - Xóa các DNS records ở Nameserver cũ khi chuyển qua dùng CloudFlare



Trigger Email

- Demo: szaixue.com
- Nguyên nhân:
 - Sử dụng email server trên cùng Web Server để gửi ra ngoài.
- Cách khắc phục:
 - Dùng dịch vụ gửi email của bên thứ 3 như: Gmail, Outlook, Email Relay
 - Tách server gửi mail và server web ra riêng.

Trigger Email

DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=pxhuxsj.site; q=dns/txt; s=mx;
t=1618286084; h=Content-Transfer-Encoding: Content-Type: MIME-Version:
Message-ID: Subject: Reply-To: From: To: Date: Sender: X-Feedback-Id;
bh=0pes4feKuBgIvpfKflz/Rj24pbKNsKxdKfcG0PmXUi0=; b=lhXdhMjGQIXnthck9JMVFXbnJ8/6KDBh9uaoAMVB0QnaVLsWwYmym
SR0kH0UqH1cnXqawvy45gVam15Zo7eRX/UCn0B8BXRmzQVYKbttGWeHDzKPuqYVPwrw+92Kl
RtfcXv//UEDn1510X3VpUZH8FX8=
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=mailgun.org; q=dns/txt; s=mg;
t=1618286084; h=Content-Transfer-Encoding: Content-Type: MIME-Version:
Message-ID: Subject: Reply-To: From: To: Date: Sender: X-Feedback-Id;
bh=0pes4feKuBgIvpfKflz/Rj24pbKNsKxdKfcG0PmXUi0=; b=Xmgky4Fa2FTyKSoVrQ3AbCV3jiDNuiqY0kwQy00GWDsl66+GLznhQ1
BEV2ZtCbzIdi2io90kk1+80EoqtZoiKSgcG5JYQk3oetGzZX8hNUICNx28V6l5ivuq/ghdAV
Q8umNXF3KiqrIf91P7iDcZ4/jl8=
X-Feedback-Id: 5f33af8e18502a9587654d95:mailgun
X-Mailgun-Sending-Ip: 69.72.42.5
X-Mailgun-Sid: wyJmNWRlZSIsICJuZ3V5ZW50dW5nMTYyMDA0QGdYwlsLmNvbSIsIClYNTJhY2QxXQ==
Received: from sxaixue.com (<unknown> [45.14.226.54]) by
smtp-out-n03.prod.us-west-2.postgun.com with SMTP id
607515f62cc44d3aea7fbb1a (version=TLS1.2,
cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256); Tue, 13 Apr 2021 03:54:30
GMT
Sender: nk=kswor.com@pxhuxsj.site



Trigger Ping

- Demo: gsuite.tools
 - `trigger ping` & `tcpdump` to capture ICMP packet
- Nguyên nhân:
 - Thực thi lệnh trên server chạy web
- Cách khắc phục
 - ...

Trigger Pingback (XMLRPC) - WordPress

- Demo: quantrilinux.vn
 - Sử dụng Remote URL (có thể dùng iplogger.org hoặc canarytokens.org)
 - Sử dụng Curl , Burp Suite hoặc bất kỳ Web proxy software nào có khả năng intercept request
 - Payload với Burp Suite: <https://pastebin.com/ZeuNMWTF>
 - Payload với Curl: <https://pastebin.com/14svwfCt>
- Nguyên nhân:
 - Tính năng pingback của WordPress
- Khắc phục:
 - Giới hạn truy cập đến xmlrpc.php

Thêm mã sau vào tệp .htaccess để fix vấn đề này (Còn nhiều cách nữa)

```
<Files xmlrpc.php>
```

```
Order Allow,Deny
```

```
Deny from all
```

```
</Files>
```




Trigger Pingback (XMLRPC) - WordPress

```
[zero2hero@vietnix.vn ~]$ cat test.xml
<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
<methodName>pingback.ping</methodName>
<params>
  <param>
    <value>
      <string>http://blog.vietnix.vn/</string>
    </value>
  </param>
  <param>
    <value>
      <string>https://quantrilinux.vn/hello-world/</string>
    </value>
  </param>
</params>
</methodCall>
```



Trigger Remote Image

- Demo: quantrilinux.vn
 - Update Avatar sử dụng Remote URL (có thể dùng iplogger.org hoặc canarytokens.org)
- Nguyên nhân:
 - Server GET image from remote resources
- Cách khắc phục
 -



Shodan + Censys + Dnsdumpster + Securitytrails +Fofa.so + ZoomEye

- Shodan demo: 51sec.org
- Shodan favicon hash: `http.favicon.hash:1179099333` (Youtube.com/favicon.ico)
- Shodan Google Analytics Tracking Code: `http.html:UA-187441274-1` (GA của Hackthebox.eu)
- Censys http header Cloudflare: `80.http.get.headers.server: cloudflare`
- Demo Censys IPv4: `parsed.names: rocket-internet.com` and `tags.raw: trusted` (parsed.names: domain name to be resolved tags.raw: trusted: Display valid content)
- Demo Censys SSL certificate: 51sec.org
- Demo Dnsdumpster: hanulstyle.com
- Demo Securitytrails: hanulstyle.com
- Demo Fofa: 51sec.org
- Demo ZoomEye: 51sec.org



Vài tips khi cấu hình

- Luôn luôn xóa các DNS records cũ/ không sử dụng.
- Cẩn thận với các subdomain, MX record.
- Khi chuyển domain qua CF, nếu trước đó đã chạy IP trực tiếp thì nên đổi IP mới.
- Cấu hình Network Firewall (Layer 3/4) chỉ accept HTTP connection từ các range IP của CloudFlare.
- Luôn luôn cấu hình Default Virtual Hosts
- Sử dụng Fake (Self-signed với domain random) cho Default Virtual Hosts + Website ở Backend.
- Tắt hoặc thay thế các tính năng được xử lý trên server có thể bị trigger bởi người (pingback - xmlrpc.php, Email, Ping, Remote Image ...)
- Ẩn version của Nginx, Apache. Thay thế nội dung của default webpage của Apache hoặc Nginx.
- Dùng một cloud load balancer như: Amazon ELB
- Dùng Argo Tunnel của CloudFlare

THANK YOU!

Documented by Nguyễn Hưng - Quản trị Linux
& Hieupc - ChongLuaDao.Vn

