

# Module 2

## Footprinting & Reconnaissance

Những Nội Dung Chính Trong Chương Đây

### **FOOTPRINTING**

Quy Trình Thu Thập Thông Tin

Competitive Intelligence

Nslookup và DNSstuff

Tìm Kiếm Địa Chỉ IP Của Mục Tiêu

DNS Record

Traceroute

Email Tracking

Web Spider Là Gì ?

### **RECONNAISSANCE**

# FOOTPRINTING



Bước đầu tiên trong quá trình tấn công là thu thập thông tin về mục tiêu từ các dữ liệu mà đối tượng hay tổ chức công khai trên internet. Việc này có thể thực hiện bằng những ứng dụng trực tuyến như *Whois*, *Domain Check* hay công cụ cài đặt trên máy tính như *DNS Walk*, *DNS Enum*. Quá

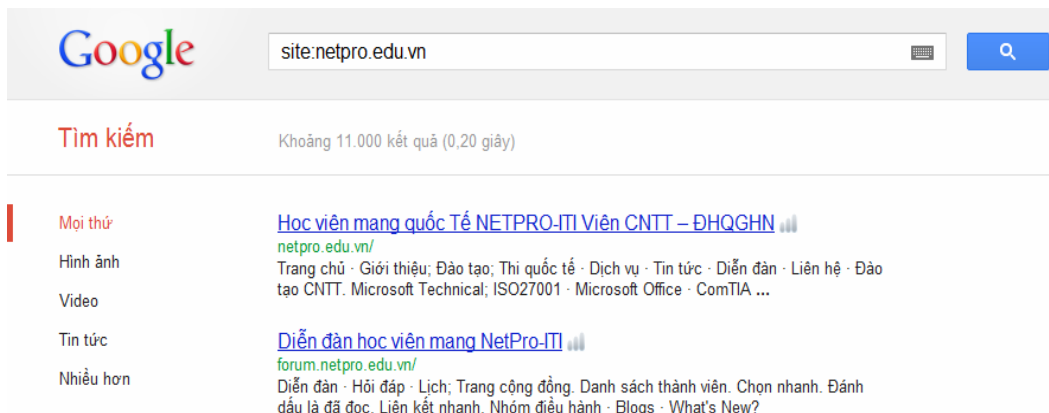
trình trên được gọi là *footprinting* hay *in dấu ấn*, với những thông tin mà *footprinting* thu thập hacker có thể đoán được chủ sở hữu của tên miền trang web bị tấn công, địa chỉ IP của mục tiêu, máy chủ phân giải tên miền DNS ...

Bên cạnh những biện pháp mang tính kỹ thuật còn có những cách thức phi kỹ thuật nhưng không kém phần hiệu quả được gọi là *Social Enginerring* mà chúng ta sẽ bàn đến ở phần tiếp theo. Với nhiều phương pháp khác nhau thì một hacker lão luyện có thể tổng hợp được khá nhiều thông tin hữu ích phục vụ cho các bước tấn công thực sự sau này của mình, và trong vài trò của một chuyên gia bảo mật hay ethical hacker thì chúng ta cần nắm rõ ý nghĩa của khái niệm footprinting cũng như cách thực hiện để tìm xem có những thông tin nào của tổ chức bị công bố quá nhiều trên môi trường internet, từ đó đưa ra những phương án xử lý kịp thời và chuẩn xác nhất.

Những công cụ hỗ trợ đắc lực cho tiến trình *footprinting* chính là công cụ tìm kiếm như *Yahoo*, *Bing* nhưng hữu ích nhất là *Google Search*, thông qua các ứng dụng này hacker có thể tìm kiếm nhiều thông tin liên quan đến một trang web mục tiêu từ những nội dung được công bố trên internet cho đến các thông tin bí mật như tập tin lưu trữ mật mã nếu như không được phân quyền chặt chẽ. Phương pháp này được gọi là *Google Hacking* (tham khảo thêm về Google hacking tại website <http://www.exploit-db.com/google-dorks/>).

Sau đây là một số tùy chọn thường được dùng cho tìm kiếm nâng cao với Google :

- **Site :** Khi tìm kiếm với tùy chọn "*site : domainname.com*" sẽ cho những kết quả liên quan trực tiếp đến trang web. Ví dụ tìm kiếm các thông tin liên quan đến trang web netpro.edu.vn theo cú pháp "*site:netpro.edu.vn*" như Hình 2.1 :



Hình 2.1 – Tìm những thông tin liên quan đến một trang web.

- **Filetype** : Chỉ tìm những kết quả liên quan đến chủ đề nào đó hay tập tin với định dạng xác định. Ví dụ tìm kiếm các tài liệu pdf liên quan đến chủ đề *ceh* chúng ta tìm kiếm theo cú pháp “*filetype: pdf ceh*” như Hình 2.2.



Hình 2.2 – Tìm theo nội dung và định dạng tập tin.

- **Link** : Tìm kiếm các thông tin có liên kết tới trang web cần tìm, ví dụ “*link : netpro.edu.vn*” sẽ hiển thị những trang web có nội dung liên quan đến domain *netpro.com.vn*.
- **Intitle** : Tìm các thông tin dựa theo tiêu đề của trang web, với cách tìm kiếm này sẽ cho kết quả tập trung vào chủ đề cần quan tâm, chẳng hạn các bạn muốn tìm kiếm những tài liệu liên quan đến “*ethical hacking*” hãy gõ vào Google dòng *intitle: “ethical hacking”*
- **Inurl** : Tìm kiếm tất cả các trang web chứa cụm *url* được xác định trong tùy chọn *inurl* như “*inurl:wp-content/plugins/age-verification/age-verification.php*”.

## Quy Trình Thu Thập Thông Tin

Để tiến hành thu thập thông tin một cách khoa học, các bạn cần thực hiện theo một sơ đồ như sau:

1. *Tìm kiếm từ các nguồn thông tin.*
2. *Xác định các dãy địa chỉ mạng.*
3. *Xác định các máy còn hoạt động*
4. *Tìm kiếm những cổng mở hay điểm truy cập của mục tiêu.*
5. *Dò tìm hệ điều hành của mục tiêu.*
6. *Tìm kiếm các dịch vụ đang hoạt động trên những cổng mở.*
7. *Lập mô hình mạng.*

Trong bảy bước trên thì bước 1 và 2 chính là tiên trình *footprinting*, các bước còn lại thuộc giai đoạn *scanning* và *enumeration*. Tiếp theo chúng ta sẽ đi vào phân tích chi tiết các bước trên và những thao tác kỹ thuật cần tiến hành. Trong công đoạn đầu tiên các bạn cần tận dụng các nguồn tài nguyên được công bố trên internet.

### Thông tin tìm kiếm :

- ☐ Domain name.
- ☐ Vị trí.
- ☐ Thông tin liên lạc (điện thoại / email)

### Các nguồn thông tin :

- ☐ Open source : Các nguồn tài nguyên mở là những dữ liệu công khai như trang vàng doanh nghiệp, danh bạ điện thoại.
- ☐ Whois : Cơ sở dữ liệu về chủ sở hữu tên miền.
- ☐ Nslookup : Thông tin về máy chủ phân giải tên miền.

### Công Cụ :

- ☐ Sam Spade ([www.samspade.org](http://www.samspade.org)) : Đây là công cụ trực tuyến bao gồm những tiện ích như Whois, nslookup và traceroute. Vì là ứng dụng trực tuyến nên trong một số trường hợp có thể không kết nối được do trang web đang bảo trì hoặc do kết nối mạng, do đó chúng ta nên sử dụng tiện ích *samspade* cài đặt trực tiếp trên máy

tình để cho kết quả tốt hơn hoặc sử dụng những trang web có chức năng tương tự khác như [www.network-tool.com](http://www.network-tool.com).

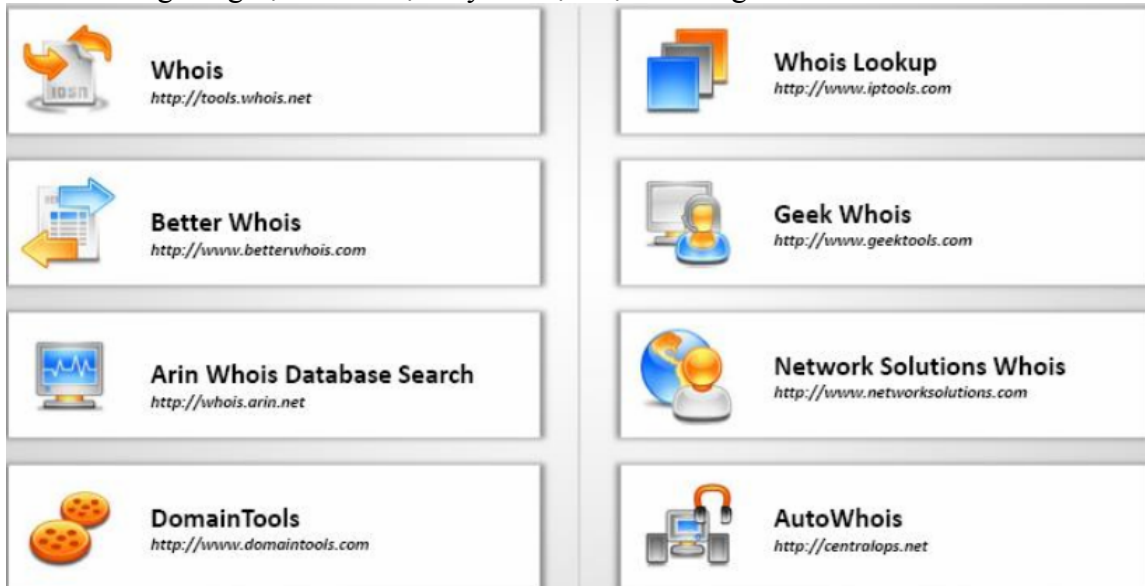
## Competitive Intelligence

*Competitive intelligence* là phương pháp thu thập thông tin từ các nguồn trên internet về một công ty hay tổ chức nào đó. *Competitive intelligence* có thể là sản phẩm hay một tiến trình ví dụ như các hành động thu thập và phân tích dữ liệu, xác nhận thông tin.

Những công cụ thường được sử dụng cho quá trình *Footprinting - Competitive Intelligence* là :

- ☐ Whois (<http://www.whois.net>)
- ☐ ARIN (<https://www.arin.net>)
- ☐ Nslookup (<http://network-tools.com/nslookup>)
- ☐ Neo Trace
- ☐ VisualRoute Trace
- ☐ Smart Whois
- ☐ Visual Lookout
- ☐ eMailTrackerPro

*Whois* là công cụ offline (như *SmartWhois*) hay tiện ích online như [www.whois.net](http://www.whois.net) dùng để thu thập thông tin liên quan đến một tên miền nào đó bao gồm nơi lưu trữ trang web, tên và địa chỉ liên lạc của người quản trị, địa chỉ IP và các máy chủ phân giải tên miền DNS. Những công cụ Whois trực tuyến được liệt kê trong Hình 2.3 :



Hình 2.3 – Các công cụ Whois trực tuyến

Sau đây là một kết quả tìm kiếm thông tin về tên miền eccouncil.org với Whois và Smart Whois trong Hình 2.4 :

*WHOIS OUTPUT FOR WWW.ECCOUNCIL.ORG*

*Domain ID:D81180127-LROR*

*Domain Name:ECCOUNCIL.ORG*

*Created On:14-Dec-2001 10:13:06 UTC*

*Sponsoring Registrar:Tucows Inc. (R11-LROR)*

*Status:OK*

*Registrant ID:tuTv2ItRZBMNd4lA*

*Registrant Name: John Smith*

*Registrant Organization:International Council of E-Commerce Consultants*

*Registrant Street1:67 Wall Street, 22nd Floor*

*Registrant City:New York*

*Registrant State/Province:NY*

*Registrant Postal Code:10005-3198*

*Registrant Country:US*

*Registrant Phone:+1.2127098253*

*Registrant Phone Ext.:*

*Registrant FAX:+1.2129432300*

*Information-Gathering Methodology 45*

*Registrant FAX Ext.:*

*Registrant Email:forum@eccouncil.org*

*Admin ID:tus9DYvpp5mrbLNd*

*Admin Name: Susan Johnson*

*Admin Organization:International Council of E-Commerce Consultants*

*Admin Street1:67 Wall Street, 22nd Floor*

*Admin City:New York*

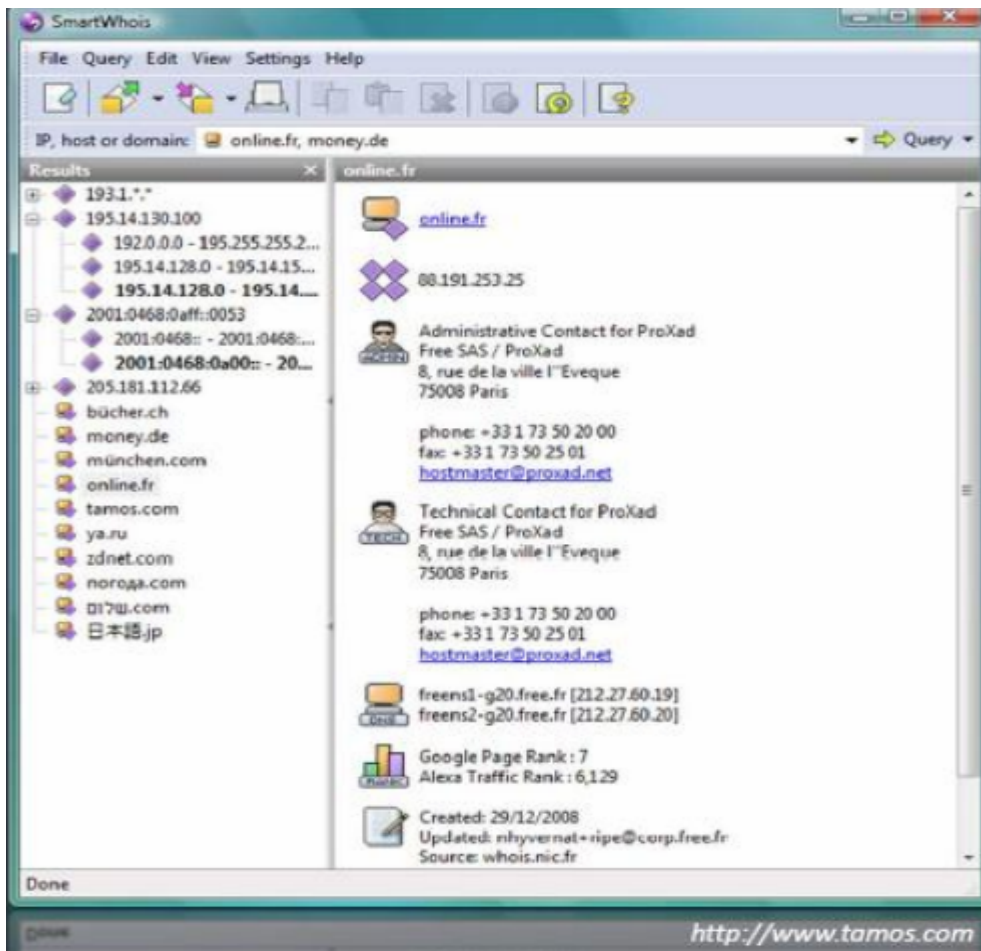
*Admin State/Province:NY*

*...*

*Tech Email:forum@eccouncil.org*

*Name Server: ns1.xyz.net*

*Name Server: ns2.xyz.net*

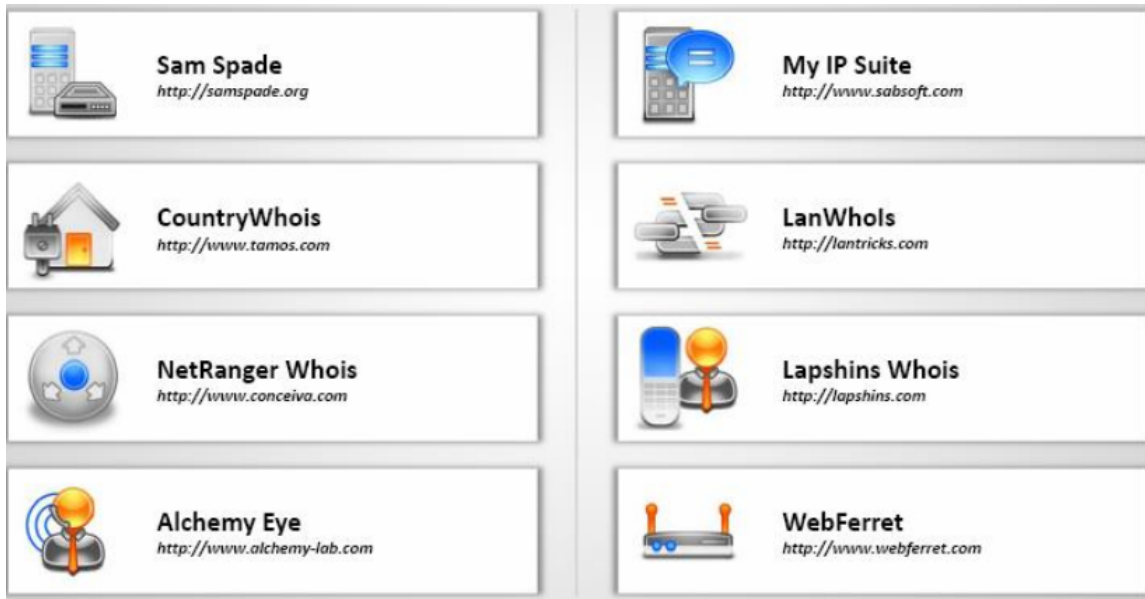


Hình 2.4 – Kết quả tìm kiếm với SmartWhois

Cơ sở dữ liệu của *Whois* được chia làm 4 vùng chính là

- ARIN (North America và sub-Saharan Africa)
- APNIC (Asia Pacific)
- LACNIC (Southern và Central America và Caribbean)
- RIPE NCC (Europe và northern Africa)

Thông tường cơ sở dữ liệu của ARIN Whois sẽ được tìm kiếm trước tiên, nếu không tìm thấy thông tin của một trang web trong ARIN thì có thể thông tin này sẽ được lưu giữ ở cơ sở dữ liệu của APNIC, LACNIC hay RIPE NCC. Các bạn có thể sử dụng [www.allwhois.com](http://www.allwhois.com) để tiến hành tìm kiếm thông tin trên tất cả các cơ sở dữ liệu thuộc các vùng khác nhau. Ngoài những trang web chuyên cung cấp những dịch vụ *Whois* thì có nhiều công cụ trong Hình 2.5 có thể đáp ứng được yêu cầu này



Hình 2.5 - Các công cụ Whois được đề cập trong CEH

## Nslookup và DNSstuff

```

C:\WINDOWS\system32\cmd.exe

C:\>nslookup www.eccouncil.org
Server: 192.168.1.1
Address: 64.190.176.10

Non-authoritative answer:
Name:    www.eccouncil.org
Address: 64.190.176.10

```

Nslookup là chương trình truy vấn tên miền trên Internet của các máy chủ, các kết quả thu được từ Nslookup có thể được hacker sử dụng để mô phỏng cấu trúc DNS của tổ chức, tìm kiếm thêm các thông tin bổ sung về những máy tính nội bộ hay thông tin MX record của mail server. Trên các hệ thống Windows hay Linux/Unix đều có công cụ *nslookup* kèm theo như hình minh họa.

Ngoài việc tìm kiếm các thông tin về tên miền internet của các máy chủ thì nslookup còn là một công cụ hữu ích cho quá trình chẩn đoán, khắc phục và xử lý các sự cố mạng liên quan đến vấn đề phân giải tên miền, truy cập internet của người dùng hay kiểm tra hệ thống Active directory sau khi cài đặt.

Ví dụ sau là kết quả của tiến trình sử dụng dụng công cụ nslookup trên Linux/Unix về máy chủ cracker.com:

```

$ nslookup
Default Server: cracker.com
Address: 10.11.122.133
Server 10.12.133.144
Default Server: ns.targetcompany.com
Address 10.12.133.144
set type=any
ls -d target.com
systemA 1DINA 10.12.133.147

```



```
1DININFO "Exchange MailServer"  
1DINMX 10 mail1  
geekL 1DINA 10.12.133.151  
1DINTXT "RH6.0"
```

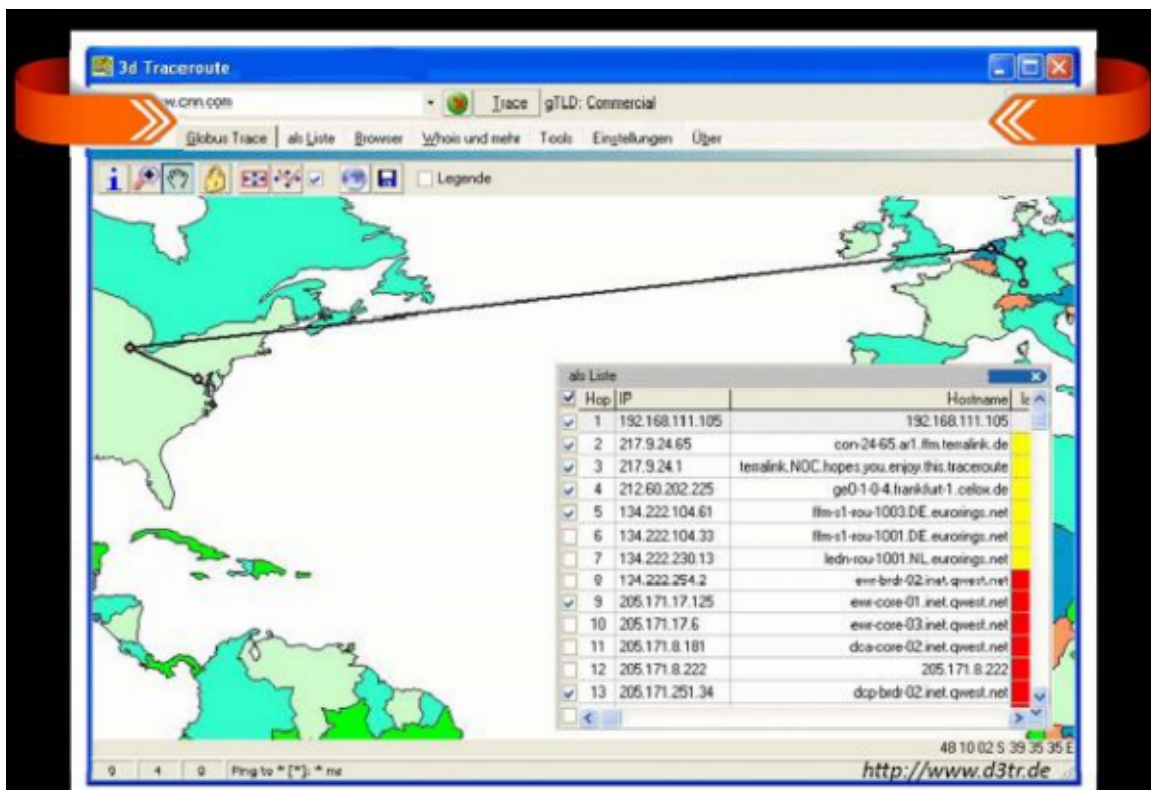
Bên cạnh *nslookup* các bạn có thể sử dụng ứng dụng trực tuyến *dnsstuff* tại [www.dnsstuff.com](http://www.dnsstuff.com) để tìm kiếm các thông tin liên quan đến các dns record của một trang web nào đó, như Hình 2.6 minh họa kết quả tìm kiếm liên quan đến <http://www.eccouncil.org>

DNS Lookup: eccouncil.org A record				
Generated by <a href="http://www.DNSStuff.com">www.DNSStuff.com</a> at 13:01:51 GMT on 12 Apr 2006.				
How I am searching:				
Searching for eccouncil.org A record at i.root-servers.net [198.32.64.12]: Got referral to TLD4.ULTRAINS.org. [took 94 ms]				
Searching for eccouncil.org A record at TLD4.ULTRAINS.org. [199.7.67.1]: Got referral to AUTH2.NS.NYI.NET. [took 9 ms]				
Searching for eccouncil.org A record at AUTH2.NS.NYI.NET. [66.111.15.154]: Reports eccouncil.org. [took 9 ms]				
Answer:				
Domain	Type	Class	TTL	Answer
eccouncil.org	A	IN	3600	64.90.176.10
eccouncil.org	NS	IN	3600	auth2.ns.nyi.net
eccouncil.org	NS	IN	3600	auth1.ns.nyi.net
auth2.ns.nyi.net	A	IN	7765	66.111.15.154
There is no need to refresh the page -- to see the DNS traversal, to make sure that all DNS servers are reporting the same results, you can <a href="#">Click Here</a> .				
Note that these results are obtained in real-time, meaning that these are <b>not</b> cached results. These results are what DNS resolvers all over the world will see right now (unless they have cached information).				

Hình 2.6 – DNS Lookup

## Tìm Kiếm Địa Chỉ IP Của Mục Tiêu

Bất kì *ethical hacker* nào cũng cần nắm vững cách thức xác định địa chỉ IP hay dãy địa chỉ của trang web mục tiêu thông qua các cơ sở dữ liệu của ARIN hay Internet Assigned Numbers Authority (IANA). Bên cạnh đó chúng ta có thể xác định được vị trí địa lý của địa chỉ IP trên hay để truy cập đến mục tiêu này cần phải qua bao nhiêu bước nhảy (hop). Để thực hiện điều này các bạn hãy sử dụng traceroute, visularoute với kết quả rất rõ ràng như Hình 2.7.



Hình 2.7 – Kết quả tìm kiếm với ứng dụng 3d Traceroute

## Các Kiểu DNS Record

Để có thể truy cập vào một trang web hay máy tính thông qua tên miền như [security365.vn](http://security365.vn) hay tên máy là [filesrv.netpro.edu.vn](http://filesrv.netpro.edu.vn) máy tính của chúng ta cần phải chuyển đổi các tên dễ nhớ trên ra địa chỉ IP, công việc này được thực hiện bởi các máy chủ phân giải tên miền DNS và dòng thông tin ánh xạ giữa một tên dễ nhớ sang địa chỉ IP được gọi là DNS record. Sau đây là các record trên máy chủ DNS :

- ⌞ A (address)— Record này liên kết một hostname với địa chỉ IP.
- ⌞ SOA (Start of Authority)— Xác định máy chủ DNS chịu trách nhiệm phân giải
- ⌞ CNAME (canonical name)— Cung cấp tên bí danh.
- ⌞ MX (mail exchange)— xác định máy chủ email của domain.
- ⌞ SRV (service)—Xác định các máy chủ cung cấp dịch vụ như Active Directory
- ⌞ PTR (pointer)— Liên kết một địa chỉ IP với một host name

<sup>L</sup> NS (name server)— Xác định các máy chủ phân giải tên khác của domain

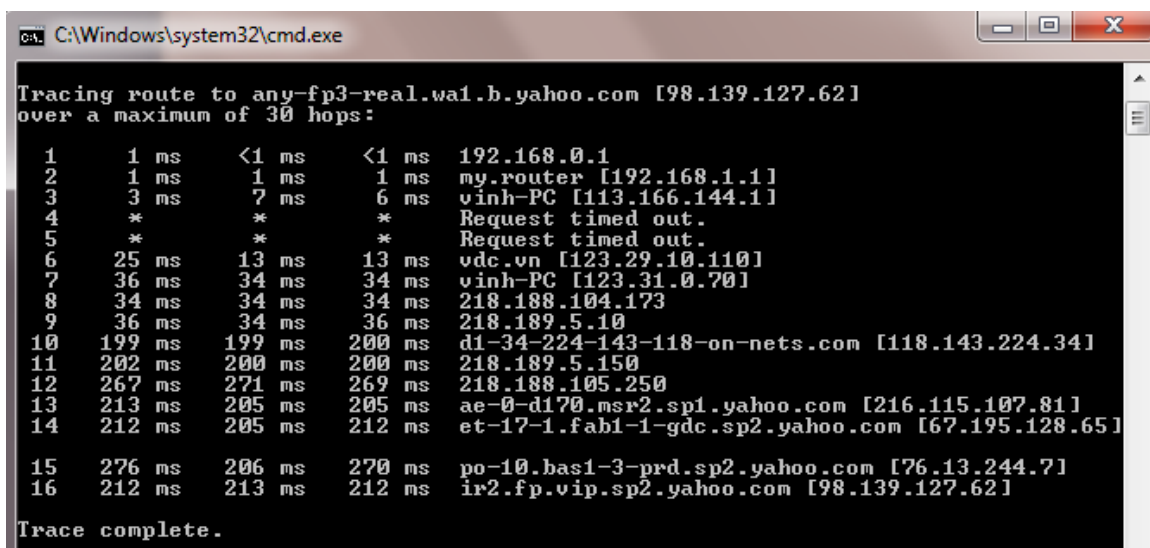
## Sử Dụng Traceroute Trong Tiến Trình Footprinting

Traceroute là công cụ lưu dấu các gói tin trong quá trình truyền đến một mục tiêu, có thể sử dụng trên các hệ điều hành *Windows* hay *Linux*. *Traceroute* vận hành bằng cách gửi các tín hiệu *Internet Control Message Protocol* (ICMP) đến các trạm (*hop*) có thể là *router* hay *gateway* trên tuyến đường mà gói tin đi qua cho đến khi đến được trạm đích, và khi một router phản hồi với tín hiệu *ICMP ECHO Reply* thì giá trị *Time To Live* (TTL) sẽ giảm xuống một giá trị cho biết cần phải nhảy qua bao nhiêu *hop* mới đến được đích.

Một trong những trở ngại của quá trình *traceroute* là thời gian tồn tại của gói tin bị hết (hiển thị bằng các dấu sao), điều này xảy ra khi các *router* hay *firewall* chặn các tín hiệu trả về (ICMP) nhưng qua đó các hacker cũng biết được sẽ có những hệ thống bảo vệ nào trong toàn bộ tuyến đường đi đến mục tiêu.

## Công Cụ

Có khá nhiều công cụ có thể thực hiện công việc *tracerouter* và hiển thị cả những thông tin địa lý liên quan đến địa chỉ IP, hay chủ sở hữu của tên miền trang web như các ứng dụng Visual Router, 3D Trace đã giới thiệu trong phần trên. Ngoài ra, trên hệ thống *Windows* các bạn sử dụng lệnh *tracert* để dò tìm tuyến đường đi đến mục tiêu như Hình 2.8 minh họa dùng *tracert* với tên miền là [www.yahoo.com](http://www.yahoo.com)



```
C:\Windows\system32\cmd.exe

Tracing route to any-fp3-real.wa1.b.yahoo.com [98.139.127.62]
over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  192.168.0.1
  1  1 ms  1 ms  1 ms  my.router [192.168.1.1]
  2  3 ms  7 ms  6 ms  vinh-PC [113.166.144.1]
  3  *      *      *      Request timed out.
  4  *      *      *      Request timed out.
  5  25 ms  13 ms  13 ms  vdc.vn [123.29.10.110]
  6  36 ms  34 ms  34 ms  vinh-PC [123.31.0.70]
  7  34 ms  34 ms  34 ms  218.188.104.173
  8  36 ms  34 ms  36 ms  218.189.5.10
  9  199 ms  199 ms  200 ms  d1-34-224-143-118-on-nets.com [118.143.224.34]
 10  202 ms  200 ms  200 ms  218.189.5.150
 11  267 ms  271 ms  269 ms  218.188.105.250
 12  213 ms  205 ms  205 ms  ae-0-d170.msr2.sp1.yahoo.com [216.115.107.81]
 13  212 ms  205 ms  212 ms  et-17-1.fab1-1-gdc.sp2.yahoo.com [67.195.128.65]
 14  276 ms  206 ms  270 ms  po-10.bas1-3-prd.sp2.yahoo.com [76.13.244.7]
 15  212 ms  213 ms  212 ms  ir2.fp.vip.sp2.yahoo.com [98.139.127.62]

Trace complete.
```

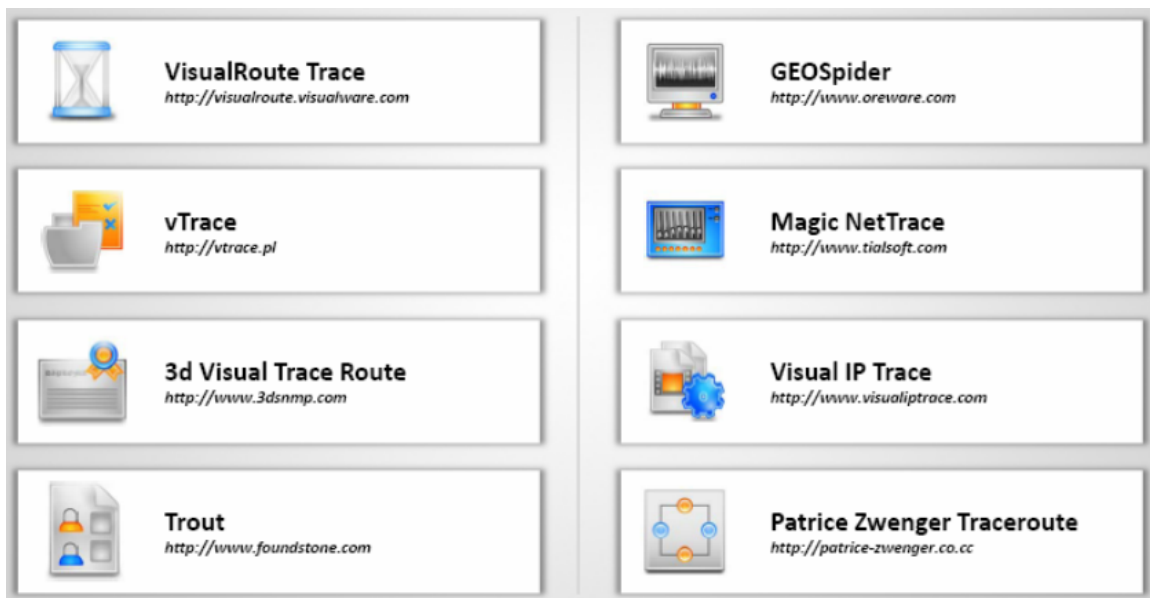
Hình 2.8 – Tiện ích *tracert* trên *Windows*

## Email Tracking Là Gì ?

Đúng như tên gọi *Email tracking* là những chương trình cho phép người gửi kiểm tra xem email của mình gửi đi đã được đọc hay chưa hay thậm chí có bị xóa, chuyển tiếp, thay đổi gì không. Phần lớn các ứng dụng *email tracking* sẽ gắn thêm một tên miền vào địa chỉ email như *readnotify.com*. Hay một tập tin hình ảnh nhỏ được gắn vào bức thư mà không cho người nhận biết và khi người nhận có những hành động như đề cập ở trên thì hình ảnh này sẽ kết nối về máy chủ để thông báo cho người gửi biết về các hành động xảy ra.

## Công Cụ

Những ứng dụng thường được dùng để theo dõi hành động của người nhận trong giao dịch thư tín như là *Email Tracking Pro*, *MailTracking.Com*... Hình 2.9 liệt kê một số công cụ thông dụng được giới thiệu trong CEH :



Hình 2.9 - Một số công cụ Email Tracking

## Web Spider

Các spammer hay những kẻ phát tán thư rác rất quan tâm đến địa chỉ email của người dùng, vì vậy họ thường sử dụng các công cụ thu thập địa chỉ email liên quan đến một tên miền nào đó trên internet, những ứng dụng như vậy gọi là *Web Spider* như *MetaGoofil* hay một số ứng dụng thu thập địa chỉ email được cài đặt sẵn trên bộ công cụ bảo mật nổi tiếng Back Track 5 (phiên bản mới nhất hiện nay là BackTrack 5 R.1).

Để phòng chống các quản trị trang web thường đặt tập tin *robots.txt* ở thư mục root của trang web chứa danh sách những thư mục được bảo vệ không cho phép lấy về bởi các chương trình tự động như google bot, yahoo bot và cả các web spider.

# RECONNAISSANCE



**Reconnaissance** là một thuật ngữ xuất phát từ môi trường quân sự như trên logo của IRS, và các bạn sẽ thấy có khá nhiều thuật ngữ của môi trường này được áp dụng trong vấn đề bảo mật thông tin đó là *DMZ*, *Spy*. Quá trình *reconnaissance* là hoạt động thăm dò đối phương hay kẻ địch bằng những phương pháp do thám cao cấp với máy bay tàng hình, vệ tinh cho đến những biện pháp thông dụng như sử dụng gián điệp cài cắm vào hàng ngũ địch, dùng trinh sát viên để thu thập thông tin của đối phương. Trong môi trường tấn công và thử nghiệm tấn công mạng máy tính quá trình *reconnaissance* được áp dụng để thu thập thông tin của mục tiêu cần

tấn công nhằm xác định các cơ chế hoạt động, vào thời gian nào và ở đâu thông qua việc quan sát các thói quen, hành vi của mục tiêu để từ đó các hacker sẽ đưa ra giải pháp tấn công hữu hiệu.

Các bạn sẽ dễ dàng hình dung về *reconnaissance* với một tình huống trong đời thực, đó là kẻ gian muốn đột nhập vào một ngôi nhà hay công ty để trộm cắp tài sản thì bọn chúng thường bỏ một thời gian để theo dõi và điều nghiên kỹ lưỡng thói quen của chủ nhà như giờ giấc đi lại, cũng như các hoạt động thường ngày trong sinh hoạt và kinh doanh để có thể đưa nguyên xe tải đến để lấy cắp đồ đạc mà chủ nhân không hề hay biết do đang bận đi nghỉ mát hay công tác trong khi người dân xung quanh lại tưởng rằng chủ nhân đang giao nhận hàng hóa như thường ngày.

Hoặc một cuộc tấn công tương tự như vậy vào khoảng năm 2005/2006 đã xảy ra tại một sân bay của Hà Lan làm cho quá trình *check-in* bị trì hoãn gần 5 tiếng đồng hồ. Trong tình huống này, các hacker đã theo dõi kỹ lưỡng hoạt động bảo trì máy chủ của sân bay trên và xác định được công ty đối tác thực hiện công việc cùng với thời gian tiến hành bảo dưỡng. Sau đó các hacker đã giả dạng làm những nhân viên bảo trì với logo, đồng phục cũng như các hình thức hoạt động tinh vi đến mức qua mặt được các nhân viên an ninh và lọt vào phòng máy chủ một cách dễ dàng. Khi đã thâm nhập các hacker đã tháo gỡ toàn bộ các ổ cứng của những máy chủ quan trọng và đem ra ngoài. Đây là một ví dụ của việc vận dụng *reconnaissance* rất hiệu quả cho quá trình tấn công, nhưng qua đó cũng cho thấy sân bay trên thiếu sự kiểm soát chặt chẽ trong khâu quản lý thiết bị. Vì một trong những nguyên tắc của an toàn thông tin là khi những đối tượng thuộc vùng thiếu tin cậy (*un-trust*) ra vào và ra khu vực được bảo vệ chặt chẽ như vùng MDZ (dùng để đặt các máy chủ) thì nhân viên an ninh cần kiểm tra túi xách của họ để phát hiện có hành động gian lận nào hay không.

## Kết Luận

Qua chương này chúng ta đã tìm hiểu các bước tiền tấn công quan trọng là **Footprinting** và **Reconnaissance** cùng những công cụ mạnh mẽ hay được sử dụng cho quá trình thu thập thông tin. Trong vai trò của chuyên gia an ninh mạng các bạn cần tiến hành các thao tác sau để phòng chống bị tấn công *footprinting* :

*Cấu hình router hay firewall không phản hồi các chương trình dò tìm như Ping bằng cách chặn tín hiệu ICMP ECHO Request/Reply*

*Tắt những giao thức không dùng trên máy chủ web.*

*Kiểm soát cổng dịch vụ với những quy tắc chặt chẽ trên firewall.*

*Triển khai hệ thống IDS (dò tìm xâm nhập trái phép) để cảnh báo cho quản trị viên khi có hành động khả nghi xảy ra.*

*Kiểm soát thông tin cẩn thận trước khi công bố trên internet.*

*Tự thực hiện footprinting trên hệ thống của mình để phát hiện các thông tin nhạy cảm.*

*Ngăn ngừa những ứng dụng tìm kiếm lưu cache trang web.*

*Tắt chức năng duyệt thư mục, tách domain nội bộ với domain dùng cho mục đích công cộng.*