

Chương

2

Thăm dò - Footprinting

Nội dung

- ❖ Khái niệm về Thăm dò (Footprinting)
- ❖ Phương pháp cạnh tranh thông minh
- ❖ Phương pháp liệt kê DNS
- ❖ Phương pháp Whois và ARIN Lookups
- ❖ Tìm kiếm vùng địa chỉ mạng

Nội dung

- ❖ Các loại mẫu tin DNS
- ❖ Sử dụng Traceroute trong Thăm dò
- ❖ Theo dõi email (E-mail Tracking)
- ❖ Thu thập thông tin qua Web Spider
- ❖ Tổng kết

Khái niệm về Thăm dò - Footprinting

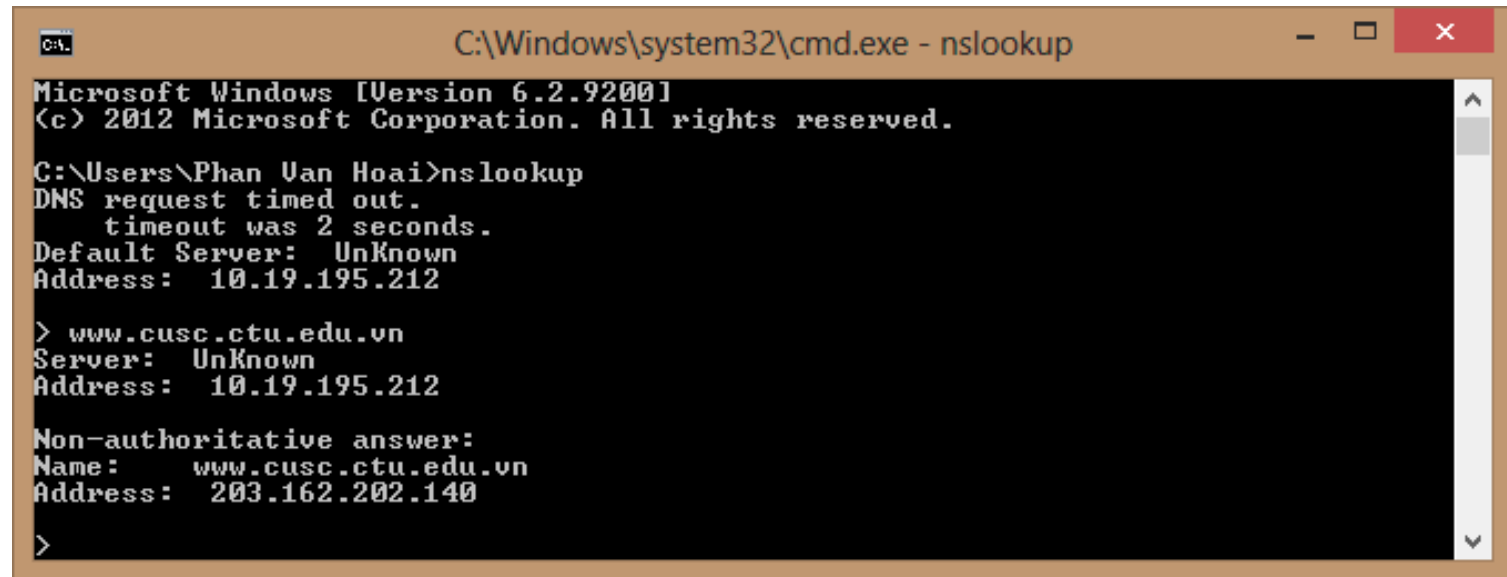
- ❖ Thăm dò là quá trình thu thập thông tin để tạo ra một kế hoạch tấn công chi tiết hoặc sơ đồ hệ thống mạng của một tổ chức mục tiêu.
- ❖ Thăm dò bắt đầu bằng cách xác định hệ thống, ứng dụng, hoặc vị trí vật lý của mục tiêu.
- ❖ Các thông tin khác thu được có thể bao gồm: công nghệ Internet, hệ điều hành, phần cứng, địa chỉ IP, địa chỉ e-mail, số điện thoại,....

Phương pháp cạnh tranh thông minh

- ❖ Thu thập thông tin về sản phẩm của đối phương, chiến lược tiếp thị và những công nghệ mà họ đang sử dụng
- ❖ Không xâm nhập đến hệ thống đang được điều tra và được bắt đầu một cách tự nhiên.
- ❖ Được dùng để so sánh sản phẩm, cách thức bán hàng và chiến thuật marketing để hiểu rõ hơn cách mà những đối thủ đang thực hiện.

Phương pháp liệt kê DNS

- ❖ Liệt kê DNS là thu thập thông tin từ dịch vụ DNS bằng các công cụ NSlookup, DNSstuff, ARIN và Whois.
- ❖ Sử dụng NSlookup



```
C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Phan Van Hoai>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  10.19.195.212

> www.cusc.ctu.edu.vn
Server:  UnKnown
Address:  10.19.195.212

Non-authoritative answer:
Name:    www.cusc.ctu.edu.vn
Address:  203.162.202.140

>
```

Phương pháp liệt kê DNS

❖ Sử dụng DNSstuff với <http://www.dnswatch.info>



The screenshot shows the DNSWatch website interface. At the top, there's a search bar with "Hostname or IP" and "Type" fields. The "Hostname or IP" field contains "www.cusc.ctu.edu.vn" and the "Type" field is set to "A". A "Resolve" button is next to it. Below the search bar, the breadcrumb "DNSWatch > DNS Lookup for www.cusc.ctu.edu.vn" is visible. A large banner for Lazada.vn is displayed, with the text "ĐƠN GIẢN HƠN. MỌI MIỀN ĐẤT NƯỚC." and a "Tìm hiểu thêm" button. Below the banner, the search results are shown:

Searching for www.cusc.ctu.edu.vn. A record at K.ROOT-SERVERS.NET. [193.0.14.129] ...took **16 ms**
Searching for www.cusc.ctu.edu.vn. A record at d.dns-servers.vn. [203.119.44.105] ...took **315 ms**
Searching for www.cusc.ctu.edu.vn. A record at ns.ctu.edu.vn. [203.162.41.166] ...took **335 ms**

A record found: 203.162.202.140

Domain	Type	TTL	Answer
www.cusc.ctu.edu.vn.	A	86400	203.162.202.140

At the bottom, there's a link: [Monitor performance and availability of your DNS Server \(e.g. ns.ctu.edu.vn\) - starting at \\$1/month](#). On the right side, there's an advertisement for RAM and bandwidth, featuring a stack of server hardware.

Phương pháp Whois và ARIN Lookups

- ❖ Công cụ Whois truy vấn **cơ sở dữ liệu** đăng ký để lấy thông tin liên hệ của cá nhân hoặc tổ chức đăng ký tên miền đó.
- ❖ **SmartWhois** thu thập thông tin: IP, tên máy hoặc miền, địa chỉ của nhà cung cấp mạng, người quản trị và địa chỉ hỗ trợ kỹ thuật
- ❖ **ARIN** là một cơ sở dữ liệu bao gồm thông tin chủ sở hữu của địa chỉ IP tĩnh.

Phương pháp Whois và ARIN Lookups

ARIN tìm
kiếm địa chỉ
***www.cusc.
ctu.edu.vn***

The screenshot shows the CentralOps.net website interface. The browser address bar displays <http://centralops.net/co/>. The website header includes the logo "CentralOps.net" and the tagline "Advanced online Internet utilities". A sidebar on the left lists various utilities: Domain Dossier, Domain Check, Email Dossier, Browser Mirror, Ping, Traceroute, NsLookup, AutoWhois, TcpQuery, and AnalyzePath. The main content area is titled "Address lookup" and shows the canonical name www.cusc.ctu.edu.vn and its IP address 203.162.202.140. Below this, the "Domain Whois record" section shows a query error: "NoWhoisServerForDomain". The "Network Whois record" section shows a query from whois.apnic.net for the IP 203.162.202.140, returning details about the VDC-NET network in Vietnam.

Address lookup

canonical name www.cusc.ctu.edu.vn

aliases

addresses **203.162.202.140**

Domain Whois record

Queried with "ctu.edu.vn"...

Query error: **NoWhoisServerForDomain**

Network Whois record

Queried whois.apnic.net with "203.162.202.140"...

inetnum:	203.162.192.0 - 203.162.255.255
netname:	VDC-NET
country:	vn
descr:	VietNam Data Communication Company
admin-c:	VIG1-AP
tech-c:	VIG1-AP
status:	ALLOCATED NON-PORTABLE
changed:	hm-changed@vnnic.net.vn 20090325
mnt-by:	MAINT-VN-VNPT
source:	APNIC

Tìm kiếm vùng địa chỉ mạng

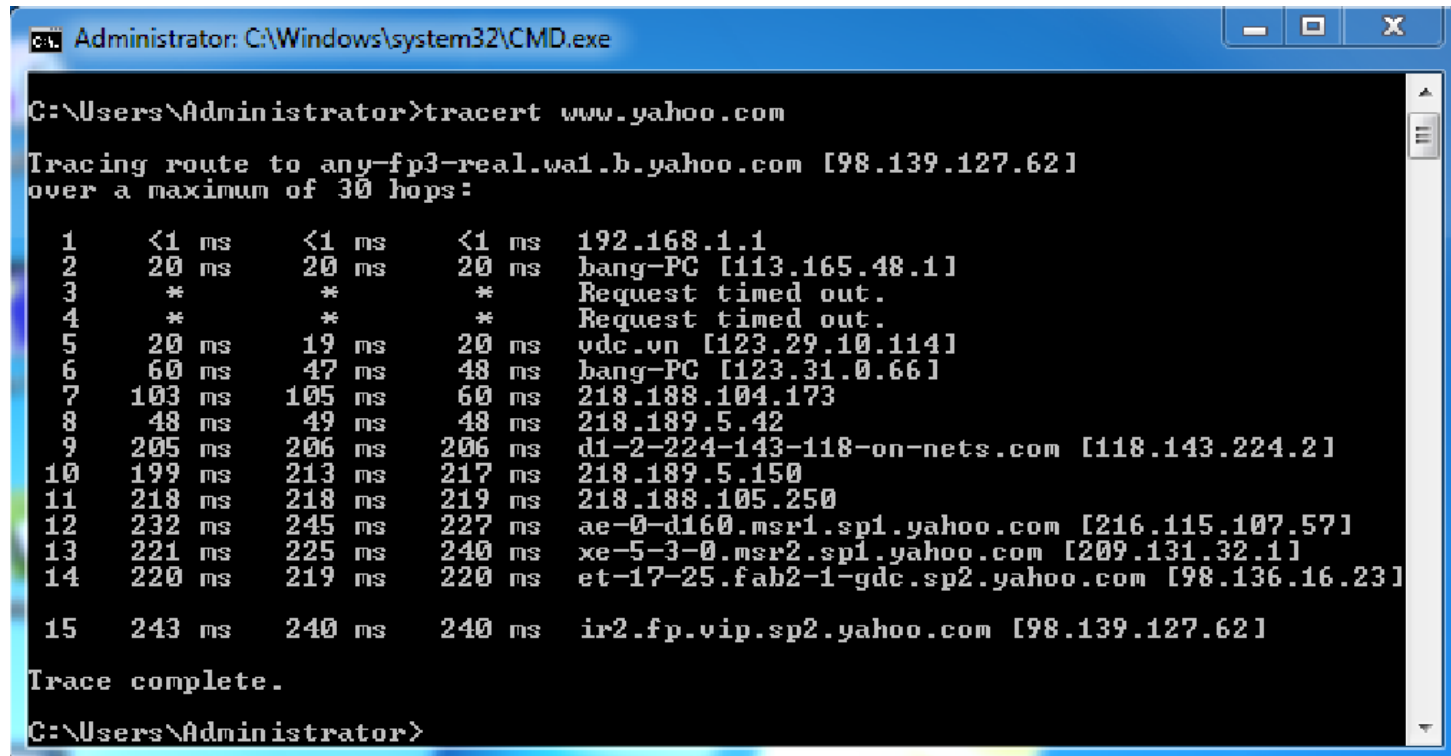
- ❖ Vùng địa chỉ mạng là tập hợp tất cả IP của hệ thống trong mạng.
- ❖ Địa chỉ IP được sử dụng để xác định vị trí, quét và kết nối đến hệ thống mục tiêu.
- ❖ Bạn có thể tìm địa chỉ IP đăng ký trên Internet với ARIN hoặc với IANA.

Các loại mẫu tin DNS

- ❖ A (Address): Ánh xạ hostname tới địa chỉ IP.
- ❖ SOA (Start of Authority): Xác định DNS Server có nhiệm vụ thông tin miền.
- ❖ CNAME (Canonical Name): Cung cấp tên hay bí danh cho mẫu tin địa chỉ.
- ❖ MX (Mail Exchange): Xác định mail server cho miền
- ❖ SRV (Service): Xác định những dịch vụ như dịch vụ thư mục
- ❖ PTR (Pointer): Ánh xạ địa chỉ IP thành tên máy chủ
- ❖ NS (Name Server): Xác định Name Server khác cho miền

Sử dụng Traceroute trong Thăm dò

- ❖ Traceroute là công cụ ghi vết dạng gói được cài đặt sẵn trong hầu hết các hệ điều hành.



```
Administrator: C:\Windows\system32\CMD.exe

C:\Users\Administrator>tracert www.yahoo.com

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

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    20 ms     20 ms     20 ms     bang-PC [113.165.48.1]
  3    *         *         *         Request timed out.
  4    *         *         *         Request timed out.
  5    20 ms     19 ms     20 ms     vdc.vn [123.29.10.114]
  6    60 ms     47 ms     48 ms     bang-PC [123.31.0.66]
  7    103 ms    105 ms    60 ms     218.188.104.173
  8    48 ms     49 ms     48 ms     218.189.5.42
  9    205 ms    206 ms    206 ms    d1-2-224-143-118-on-nets.com [118.143.224.2]
 10    199 ms    213 ms    217 ms    218.189.5.150
 11    218 ms    218 ms    219 ms    218.188.105.250
 12    232 ms    245 ms    227 ms    ae-0-d160.msrl.sp1.yahoo.com [216.115.107.57]
 13    221 ms    225 ms    240 ms    xe-5-3-0.msrl.sp1.yahoo.com [209.131.32.1]
 14    220 ms    219 ms    220 ms    et-17-25.fab2-1-gdc.sp2.yahoo.com [98.136.16.23]
 15    243 ms    240 ms    240 ms    ir2.fp.vip.sp2.yahoo.com [98.139.127.62]

Trace complete.

C:\Users\Administrator>
```

Theo dõi email (E-mail Tracking)

- ❖ Chương trình ghi vết cho phép người gửi email biết được những gì người nhận đã làm như: đọc, chuyển tiếp, sửa, hay xóa thư.
- ❖ Chương trình ghi vết chèn một tên miền tới địa chỉ thư, chẳng hạn như readnotify.com.
- ❖ Một tập tin đồ họa đơn giản không gây chú ý bởi người nhận được đính kèm vào email.
- ❖ Sau đó, khi một hành động được thực hiện trên email, tập tin đồ họa nối kết trở lại server và thông báo cho người gửi hoạt động này.

Thu thập thông tin qua Web Spider

- ❖ Web Spider có thể được dùng để định vị tất cả loại thông tin trên Internet.
- ❖ Web Spider lùng sục các website để thu thập những thông tin xác định như địa chỉ email.
- ❖ Web Spider sử dụng những cú pháp, như biểu tượng @, để định vị các địa chỉ email và sao chép chúng vào một danh sách.
- ❖ Sau đó, các địa chỉ này được thêm vào cơ sở dữ liệu và có thể được dùng để gửi email một cách tự động tới các địa chỉ này.

Tổng kết

- ❖ Thăm dò là kỹ thuật tìm kiếm thông tin của mục tiêu.
- ❖ Biết làm thế nào để tìm kiếm thông tin của một công ty, thông cáo báo chí, blog và nhóm tin.
- ❖ Sử dụng tất cả các nguồn tài nguyên công cộng có sẵn để tìm thông tin về một công ty mục tiêu và thu thập dữ liệu về mạng và bảo mật hệ thống.
- ❖ Sử dụng Yahoo! People tìm kiếm các công cụ tìm kiếm Internet khác để tìm các nhân viên của công ty mục tiêu.
- ❖ Biết cách để truy vấn thông tin cho mẫu tin DNS cụ thể.

Tổng kết

- ❖ Hiểu làm thế nào để thực hiện Whois tra cứu thông tin cá nhân hoặc công ty.
- ❖ Biết làm thế nào để tìm tên của một công ty mục tiêu bên trong và bên ngoài của tên miền.
- ❖ Biết làm thế nào để xác định vị trí máy chủ web và các thiết bị mạng cơ sở hạ tầng khác của một công ty mục tiêu.
- ❖ Biết làm thế nào để theo dõi email từ một công ty.