HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

BÀI TẬP LAB THỰC HÀNH

Môn: Cơ sở an toàn thông tin

Bài 3: Đảm bảo an toàn cho hệ thống thông tin

Hà Nội – 2017

MỤC LỤC

MỤC LỤC 1
DANH MỤC HÌNH 3
1 GIỚI THIỆU BÀI THỰC HÀNH 5
1.1 Mục đích 5
1.2 Yêu cầu 5
1.3 Thời gian thực hiện 5
1.4 Nhóm thực hành 5
2 CƠ SỞ LÝ THUYẾT 6
2.1 Tóm tắt kiến thức lý thuyết môn học 6
2.1.1 Tường lửa 6
2.1.2 Virus 6
2.2 Giới thiệu các công cụ sử dụng trong bài 7
2.2.1 Windows firewall 7
2.2.2 Kaspersky Anti Virus 8
2.2.3 Iptables 8
3 NỘI DUNG THỰC HÀNH 10
3.1 Cài đặt và cấu hình Windows firewall 10
3.1.1 Chuẩn bị môi trường 10
3.1.2 Các bước thực hiện 10
3.1.3 Kết quả mong muốn 18
3.2 Cài đặt phần mềm diệt virus Kaspersky 18
3.2.1 Chuẩn bị môi trường 18

3.2.2 Các bước thực hiện 18
3.2.3 Kết quả mong muốn 21
3.3 Cài đặt và sử dụng Iptables 22
3.3.1 Chuẩn bị môi trường 22
3.3.2 Các bước thực hiện 22
3.3.3 Kết quả mong muốn 30

DANH MỤC HÌNH

Hình 2.1: Chèn và gọi thực hiện mã vi rút 7
Hình 3.1: Mô hình 10
Hình 3.2: Snapshot 10
Hình 3.3: Windows Firewall 11
Hình 3.4: Windows Firewall Properties 12
Hình 3.5: Ping từ PC1 đến PC2 trường hợp 1 12
Hình 3.6: Ping từ PC1 đến PC2 trường hợp 2 13
Hình 3.7: Chọn Custom 14
Hình 3.8: Chọn All programs 14
Hình 3.9: Chọn Protocol type ICMPv4 15
Hình 3.10: Chọn Allow the connection 15
Hình 3.11: Turn Windows feature on or off 16
Hình 3.12: Rule Type 17
Hình 3.13: Protocol and Ports 17
Hình 3.14: Giao diện Perfect KeyLogger 19
Hình 3.15: Thư mục *C:\Program Files\BPK* 19
Hình 3.16: Virus ghi lại các hoạt động 20
Hình 3.17: Cài đặt Kaspersky Internet Security 21
Hình 3.18: Giao diện Kaspersky Internet Security 22
Hình 3.19: Kiểm tra kết nối trước khi chạy Iptables 23
Hình 3.20: Đóng tất cả các cổng 23
Hình 3.21: Giữ lại các kết nối hiện tại và các kết nối liên quan 23
Hình 3.22: HIển thị các kết nối 23
Hình 3.23: Chặn kết nối từ 1 địa chỉ ip 24
Hình 3.24: Các kết nối 24
Hình 3.25: Kiểm tra kết nối với máy chạy Iptables 24
Hình 3.26: Tạo blacklist 24
Hình 3.27: Câu lệnh chặn kết nối từ blacklist 25

Hình 3.28: Truy cập phần mềm Bitvise SSH Client 25
Hình 3.29: Giao diện phần mềm Bitvise SSH Client 26
Hình 3.30: Kết nối ssh thành công 27
Hình 3.31: Tạo luật chặn kết nối SSH 27
Hình 3.32: Hiển thị các kết nối 27
Hình 3.33: Chặn thành công SSH 28
Hình 3.34: Cài đặt và khởi động Apache 29
Hình 3.35: Truy cập vào IP máy chạy Apache 29
Hình 3.36: Tạo luật chặn kết nối đến cổng 80 30
Hình 3.37: Chặn kết nối thành công 30

1 GIỚI THIỆU BÀI THỰC HÀNH

1.1 Mục đích

- Về kiến thức: Bài thực hành cung cấp cho sinh viên môi trường để áp dụng lý thuyết của môn học vào thực tế. Giúp sinh viên cài đặt và cấu hình Windows Firewall, cài đặt và hiểu tác dụng của một loại Antivirus, cài đặt và hiểu tác dụng của Iptables.
- Về kỹ năng: Sau khi thực hành xong, sinh viên có khả năng sử dụng một số công cụ diệt virus và cấu hình Windows Firewall, Iptables.

1.2 Yêu cầu

- Sinh viên nắm được mô hình hoạt động và cấu hình cơ bản của tường lửa bảo vệ hệ thống.
- Sinh viên nắm được mô hình hoạt động và cấu hình cơ bản của các công cụ quét và diệt virus/malware.

1.3 Thời gian thực hiện

- 4 giờ.

1.4 Nhóm thực hành

- 1 sinh viên.

2 CƠ SỞ LÝ THUYẾT

2.1 Tóm tắt kiến thức lý thuyết môn học

2.1.1 Tường lửa

Tường lửa (Firewall) là một bức rào chắn giữa mạng nội bộ (local network) với một mạng khác (chẳng hạn như Internet), điều khiển lưu lượng ra vào giữa hai mạng này. Nếu như không có tường lửa thì lưu lượng ra vào mạng nội bộ sẽ không chịu bất kỳ sự điều tiết nào, còn một khi tường lửa được xây dựng thì lưu lượng ra vào sẽ do các thiết lập trên tường lửa quy định.

Dựa trên vị trí các lớp giao thức mạng, có thể chia tường lửa thành 3 loại:

- Tường lửa lọc gói (Packet-filtering): Áp dụng một tập các luật cho mỗi gói tin đi/đến để quyết định chuyển tiếp hay loại bỏ gói tin.
- Cổng ứng dụng (Application-level gateway): Còn gọi là proxy server, thường dùng để phát lại (relay) traffic của mức ứng dụng.
- Cổng chuyển mạch (Circuit-level gateway): Hoạt động tương tự các bộ chuyển mạch.

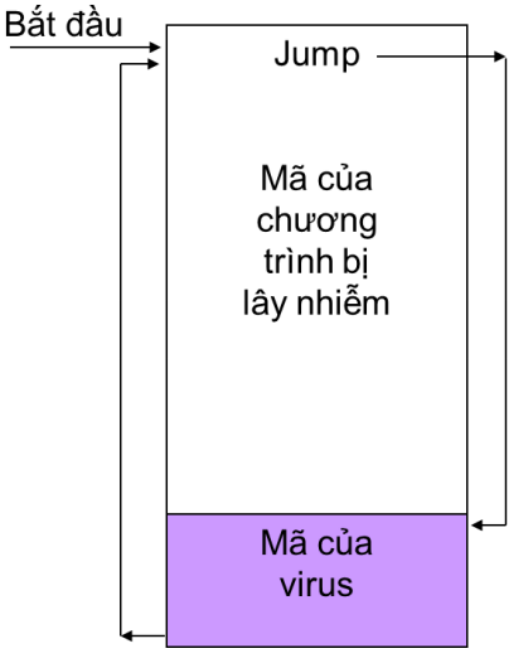
Hầu hết các tường lửa hỗ trợ nhiều kỹ thuật kiểm soát truy nhập, gồm kiểm soát dịch vụ, kiểm soát hướng, kiểm soát người dùng và kiểm soát hành vi.

Tham khảo: **“**Hoàng Xuân Dậu. Bài giảng Cơ Sở An Toàn Thông Tin. Học viện Công nghệ BC-VT, 2016. Mục 5.2. Tường lửa”.

2.1.2 Virus

Vi rút là một chương trình có thể “nhiễm” vào các chương trình khác, bằng cách sửa đổi các chương trình này. Nếu các chương trình đã bị sửa đổi chứa vi rút được kích hoạt thì vi rút sẽ tiếp tục “lây nhiễm” sang các chương trình khác. Tương tự như vi rút sinh học, vi rút máy tính cũng có khả năng tự nhân bản, tự lây nhiễm sang các chương trình khác mà nó tiếp xúc. Có nhiều con đường lây nhiễm vi rút, như sao chép file, gọi các ứng dụng và dịch vụ qua mạng, email...

Vi rút có thể thực hiện được mọi việc mà một chương trình thông thường có thể thực hiện. Khi đã lây nhiễm vào một chương trình, vi rút tự động được thực hiện khi chương trình này chạy. Hình 2.1 minh họa việc chèn mã vi rút vào cuối một chương trình và chỉnh sửa chương trình để khi chương trình được kích hoạt, mã vi rút luôn được thực hiện trước, sau đó mới thực hiện mã chương trình.



Hình 2.1: Chèn và gọi thực hiện mã vi rút

Tham khảo: **"**Hoàng Xuân Dậu. Bài giảng Cơ Sở An Toàn Thông Tin. Học viện Công nghệ BC-VT, 2016. Mục 3.4.5. Viruses".

2.2 Giới thiệu các công cụ sử dụng trong bài

2.2.1 Windows firewall

Windows Firewall được Microsoft giới thiệu ở bản cập nhật Windows XP Service Pack 2 và được bật sẵn theo mặc định. Các dịch vụ mạng trong Windows đã bị cô lập khỏi mạng internet. Thay vì chấp nhận cho mọi giao dịch dữ liệu vào, một hệ thống được bật sẵn tường lửa sẽ ngăn các giao dịch dữ liệu không mong muốn, được diễn ra, trừ khi chủ nhân của hệ thống cho phép.

2.2.2 *Kaspersky Anti Virus*

Kaspersky Anti-Virus là phần mềm chống Virus, bảo vệ người dùng trước các mối đe dọa từ email và luồng traffic trên Internet của hãng sản xuất Kaspersky.

Kaspersky Anti-Virus có các tính năng:

- Công nghệ đám mây bảo vệ theo thời gian thực.
- Ngăn chặn việc khai thác các lỗ hổng của phần mềm.
- Bảo vệ chống bị khóa màn hình.
- Cập nhật cơ sở dữ liệu hiệu quả.
- Cố vấn URL.
- Cố vấn tập tin.
- Phòng chống lừa đảo .
- Theo dõi hệ thống.
- Tiêu thụ ít tài nguyên máy tính.
- Khởi động và tắt máy nhanh chóng.
- Kéo dài thời gian sử dụng pin.
- Tối ưu cho hệ điều hành Windows.
- Gia tăng trải nghiệm người dùng.
- Các tùy chỉnh hợp lý.
- Tự động nâng cấp.
- Tăng cường tính năng quét virus.

2.2.3 *Iptables*

Iptables là Firewall được cấu hình và hoạt động trên nền Console rất nhỏ và tiện dụng, Iptables do Netfilter Organiztion viết ra để tăng tính năng bảo mật trên hệ thống Linux.

Tích hợp tốt với kernel của Linux. Có khả năng phân tích package hiệu quả. Lọc package dựa vào MAC và một số cờ hiệu trong TCP Header. Cung cấp chi tiết các tùy chọn để ghi nhận sự kiện hệ thống. Cung cấp kỹ thuật NAT. Có khả năng ngăn chặn một số cơ chế tấn công theo kiểu DoS.

Cách xử lý gói trong Iptables như sau: tất cả mọi gói dữ liệu đều được kiểm tra bởi Iptables bằng cách dùng các bảng tuần tự xây dựng sẵn. Có 3 loại bảng này gồm:

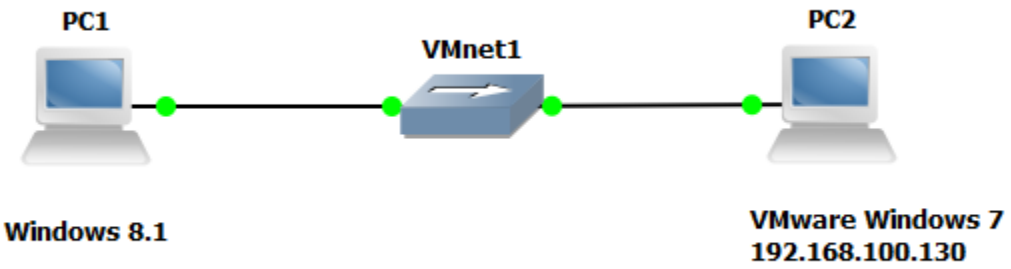
- Mangle: chịu trách nhiệm thay đổi các bits chất lượng dịch vụ trong TCP header như TOS (type of service), TTL (time to live), và MARK.
- Filter: chịu trách nhiệm lọc gói dữ liệu. Nó gồm có 3 quy tắc nhỏ (chain) để giúp bạn thiết lập các nguyên tắc lọc gói:
    - Forward chain : lọc gói khi đi đến đến các server khác.
    - Input chain : lọc gói khi đi vào trong server.
    - Output chain: lọc gói khi ra khỏi server.
- NAT: gồm có 2 loại:
    - Pre-routing chain: thay đổi địa chỉ đến của gói dữ liệu khi cần thiết.
    - Post-routing chain: thay đổi địa chỉ nguồn của gói dữ liệu khi cần thiết.

3 NỘI DUNG THỰC HÀNH

3.1 Cài đặt và cấu hình Windows firewall

3.1.1 Chuẩn bị môi trường

- Chuẩn bị đối tượng:
  - PC1: Máy thật sử dụng hệ điều hành Windows 8.1.
  - PC2: Máy ảo Windows 7 thực hiện cài đặt cấu hình Firewall.
- Mô hình (xem Hình 3.1):



Hình 3.1: Mô hình

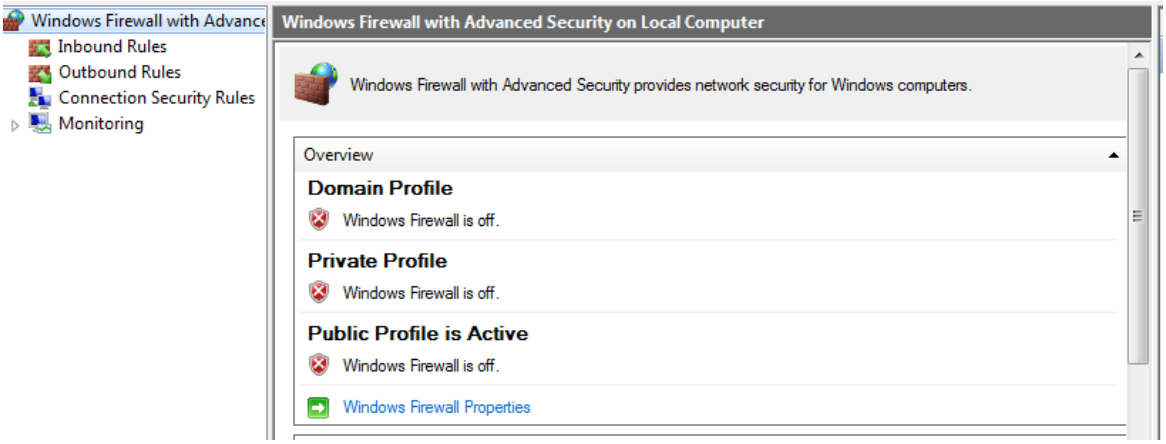
3.1.2 Các bước thực hiện

- Chọn chế độ Snapshot trên Windows7 (xem Hình 3.2):

Hình 3.2: Snapshot

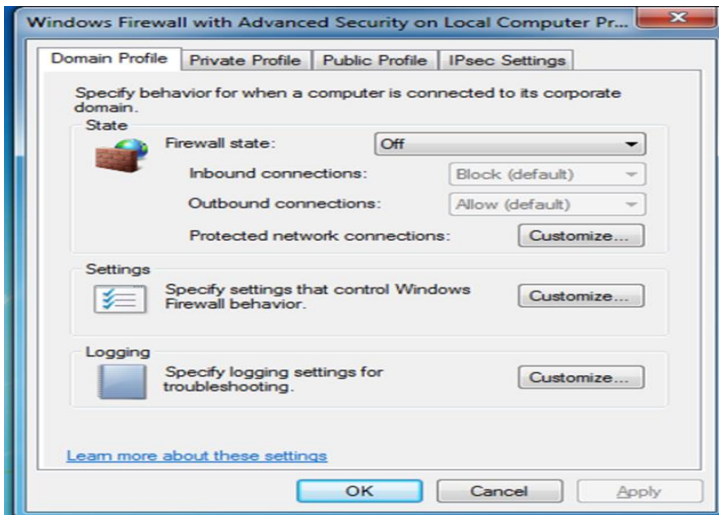
a) Cấu hình Windows Firewall trong trường hợp PingICMP

- **Task 1:** Kích hoạt/vô hiệu hóa Windows Firewall
  - Kích hoạt bằng giao diện đồ họa:
    - Bước 1: Thực hiện theo các bước như sau: Start → Control Panel → Windows Firewall → Advanced settings → Windows Firewall Properties hoặc vào hộp thoại Run gõ wf.msc (xem Hình 3.3):



Hình 3.3: Windows Firewall

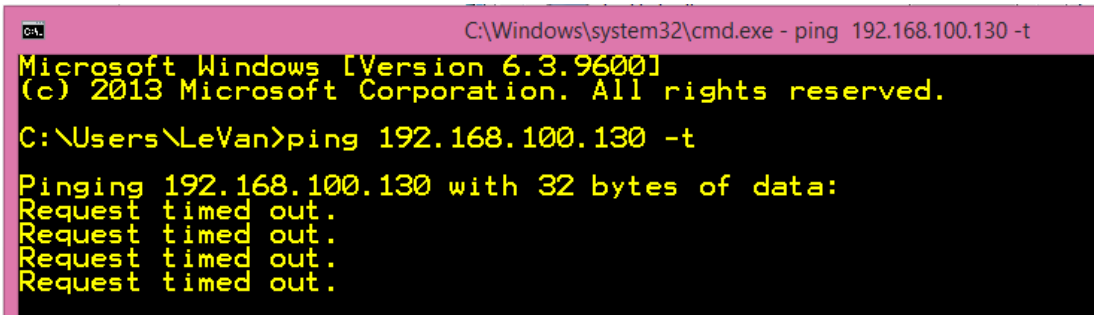
- Bước 2: Thực hiện On/off ở các tab tương ứng (xem Hình 3.4).



Hình 3.4: Windows Firewall Properties

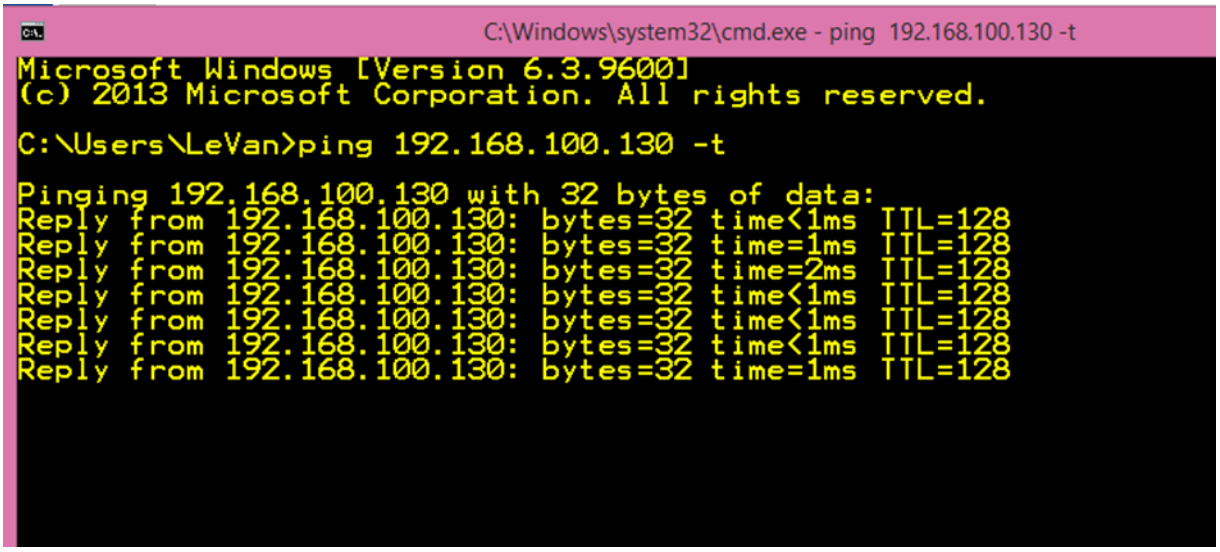
- Kích hoạt vô hiệu hóa bằng dòng lệnh trong Command Line ở quyền Administrator: `netsh advfirewall set allprofiles state on (off)`
  - Chú ý: Sinh viên thực hiện cả hai trường hợp để so sánh kết quả

- **Task 2:** Thực hiện ping từ PC1 đến PC2 trong 2 trường hợp
  - PC2 có Windows Firewall on: Kết quả không ping được (xem Hình 3.5).



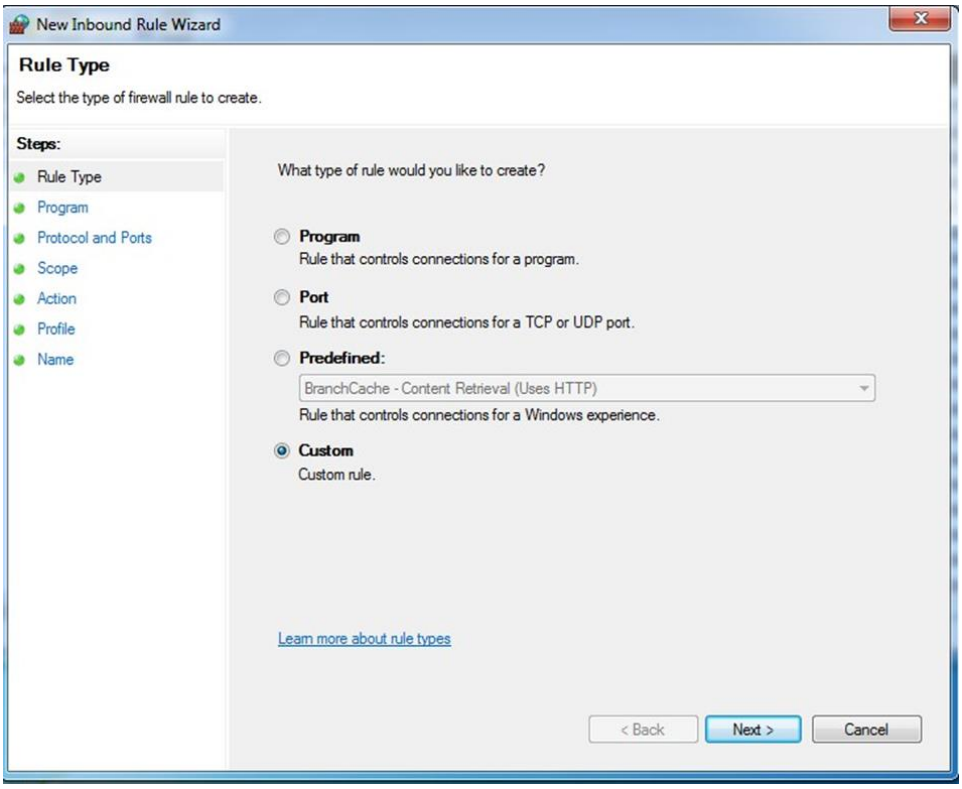
Hình 3.5: Ping từ PC1 đến PC2 trường hợp 1

- PC2 có Windows Firewall off: Kết quả Ping được (xem Hình 3.6).



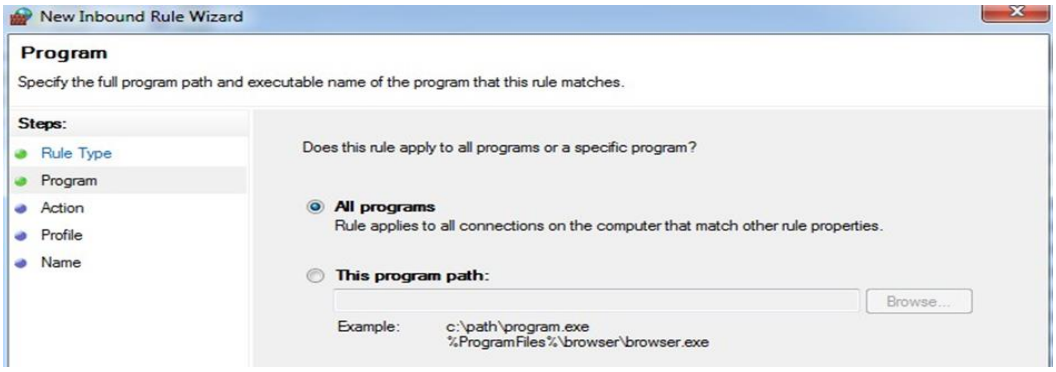
Hình 3.6: Ping từ PC1 đến PC2 trường hợp 2

- **Task 3**: Cho phép Ping khi Windows Firewall đang ở trạng thái on
  - B1: Để Windows Fiwall ở trạng thái on.
  - B2: Thực hiện Ping từ PC1 đến PC2: Kết quả không Ping được.
  - B3: Vào hộp thoại Run gõ ***wf.msc*** → ***Inbound Rules*** → ***New Rule ….*** Cần phân biệt 2 khái niệm:
    - Inbound rule: Chiều từ ngoài vào trong.
    - Outbound rule: Chiều từ trong ra ngoài.
  - B4: Lần lượt chọn các tùy chọn sau:
    - Custom (xem Hình 3.7).



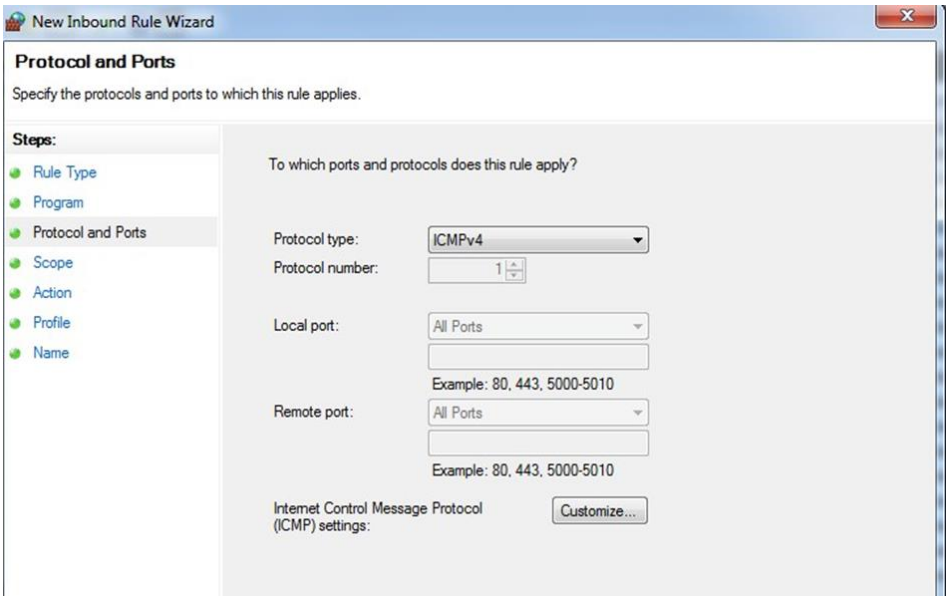
Hình 3.7: Chọn Custom

- All programs (xem Hình 3.8).



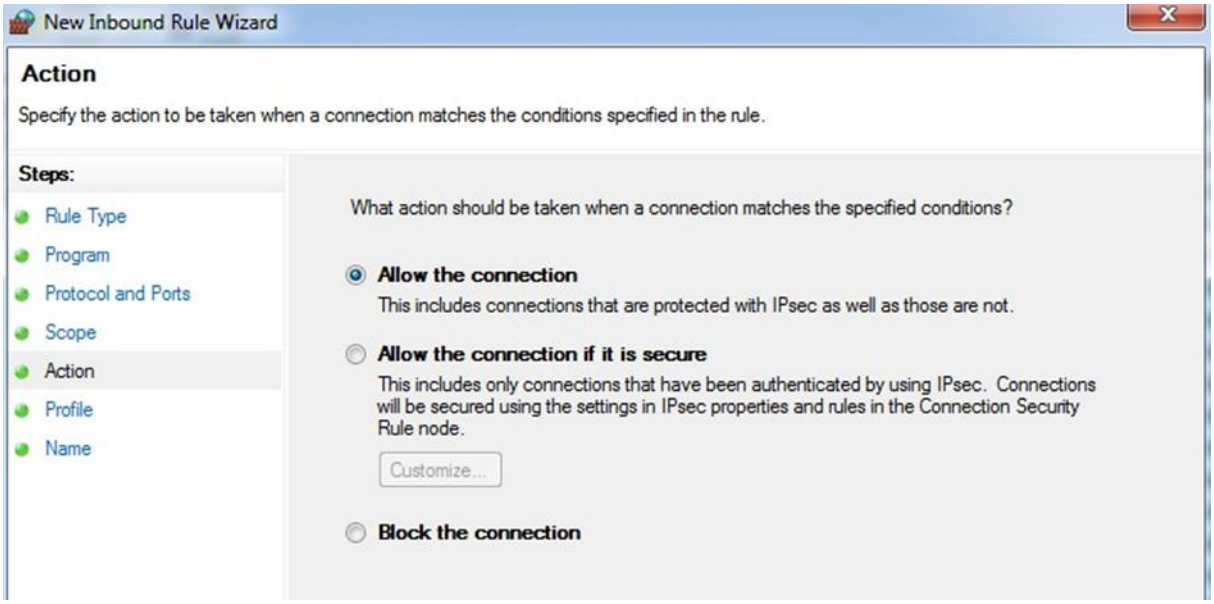
Hình 3.8: Chọn All programs

- Protocol type: ICMPv4 (xem Hình 3.9).



Hình 3.9: Chọn Protocol type ICMPv4

- Next → Next → Allow the connection (xem Hình 3.10).



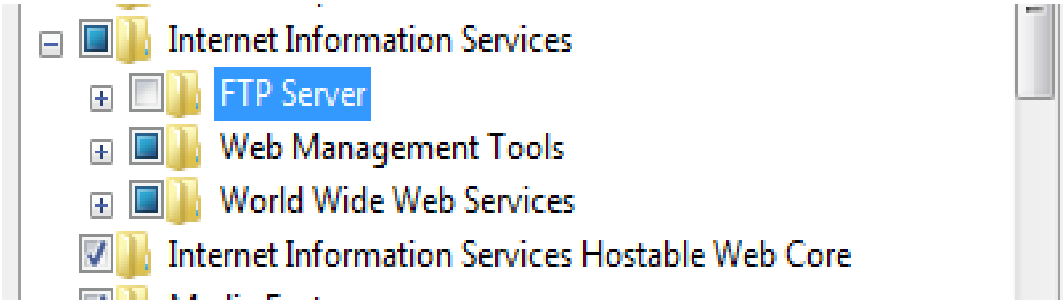
Hình 3.10: Chọn Allow the connection

- Next → Đặt tên Rule ví dụ là: ICMP Allow Inbound → Finish

- B5: Thực hiện Ping từ PC1 đến PC2 và kết quả Ping được.
- B6: Thực hiện vô hiệu hóa và kích hoạt Rule để thấy được kết quả

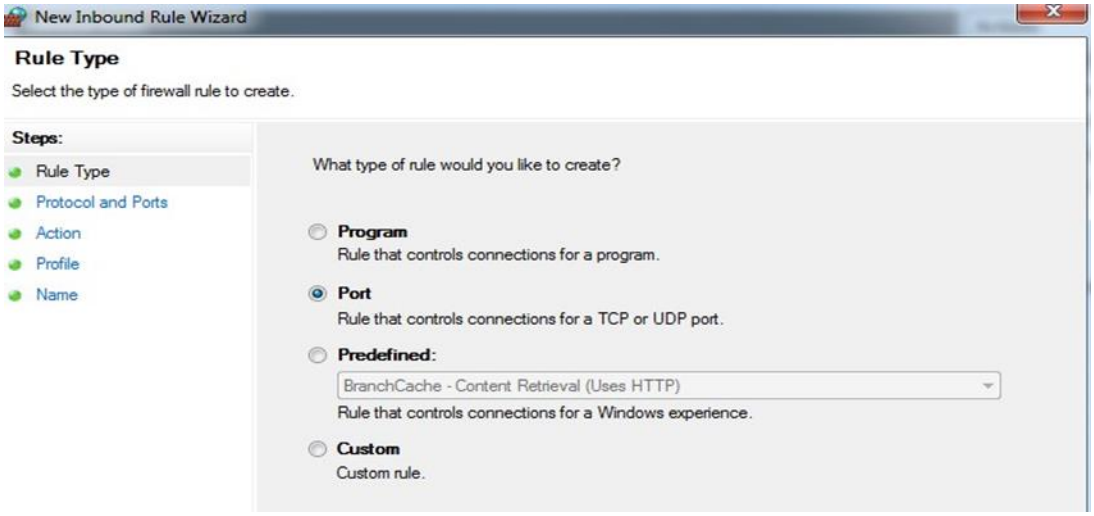
b) Cấu hình Window Firewall trong trường hợp Open Port

- **Task 4**: Thực hiện mở cổng TCP cổng 80 trên WindowsFirewall
  - B1: Enable IIS trên Windows 7: Thực hiện các thao tác sau:
    - Start → Control Panel → Uninstall a program → Turn Windows feature on or off
    - Tích vào các ô: Internet Information Services, Web Management Tools, World Wide Web Services, Internet Information Services Hostable Web Core (xem Hình 3.11):



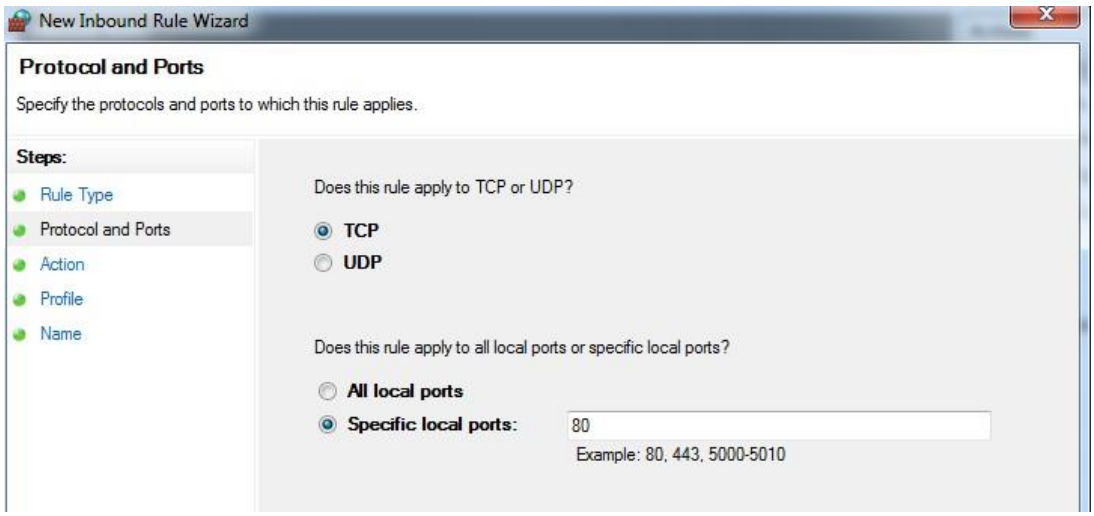
Hình 3.11: Turn Windows feature on or off

  - B2: Đứng trên Windows 7 gõ vào thanh trình duyệt: http://localhost/
  - B3: Đứng trên Windows 8.1 gõ vào thanh trình duyệt http://192.168.100.130/ trong hai trường hợp:
    - Windows Firewall on: Kết quả Fail.
    - Windows Firewall off: Kết quả ok.
  - B4: Trong trường hợp Windows Firewall on thực hiện mở cổng TCP cổng 80 Thực hiện lại **Task 3** và chú ý các keyword sau:
    - **Inbound rule**: chọn **Port** (xem Hình 3.12**)**.



Hình 3.12: Rule Type

- Chọn **TCP – 80** (xem Hình 3.13).



Hình 3.13: Protocol and Ports

- **Allow the connection →** Đặt tên rule: ***HTTP Allow TCP 80 →*** ***Finish***

- B5: Đứng trên Windows 8.1 gõ vào thanh trình duyệt http://192.168.100.130/ và kết quả là ok.
- B6: Thực hiện kích hoạt và vô hiệu hóa Rule để thấy được kết quả.

3.1.3 Kết quả mong muốn

- Cấu hình đươc Window Firewall trong các trường hợp:
  - PingICMP.
  - OpenPort.

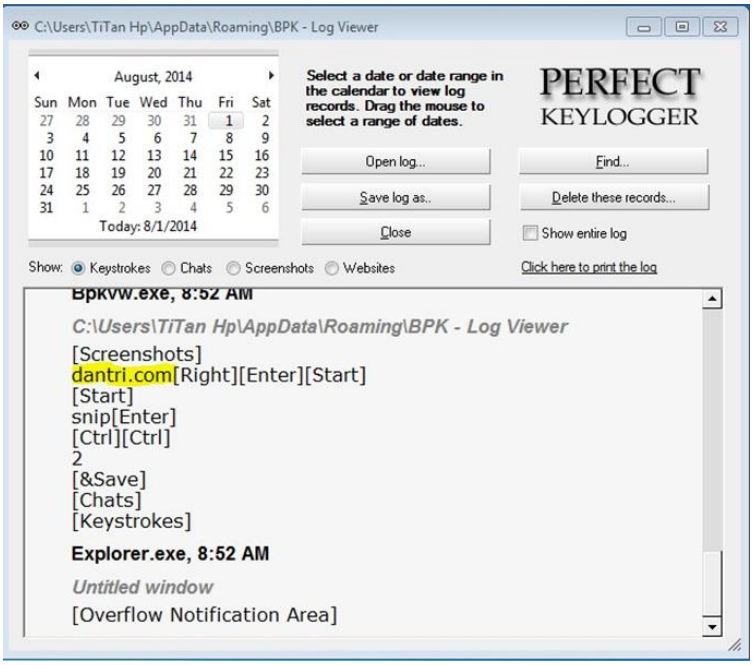
3.2 Cài đặt phần mềm diệt virus Kaspersky

3.2.1 Chuẩn bị môi trường

- Máy ảo Windows 7.
- Một phần mềm giả lập virus, ở đây ta chọn phần mềm PerfectKeylogger.
- Phần mềm diệt virus Kaspersky2013 AV.

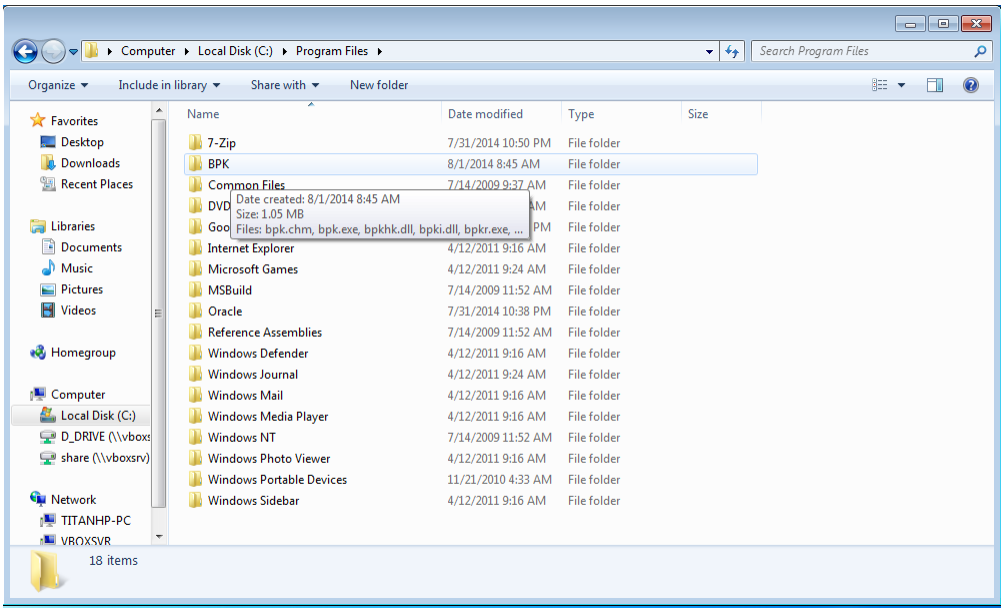
3.2.2 Các bước thực hiện

- **B1:** Cài đặt phần mềm độc hại vào máy tính, cụ thể là phần mềm **Perfect KeyLogger** (xem Hình 3.14**)**. Đặc điểm của phần mềm này:
  - Chạy ngầm trên máy tính nạn nhân.
  - Ghi lại các hoạt động của bàn phím, màn hình, click chuột.
  - Gửi các hoạt động thu được qua Email, hoặc up lên tài khoản FTP đã định trước.



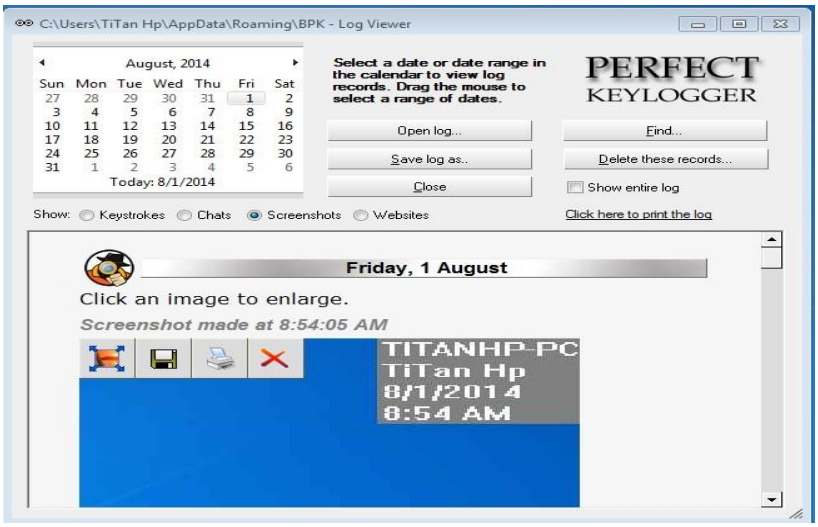
Hình 3.14: Giao diện Perfect KeyLogger

- **<u>Chú ý</u>**: Thư mục sau khi cài đặt phần mềm: ***C:\Program Files\BPK*** (xem Hình 3.15***).***



Hình 3.15: Thư mục *C:\Program Files\BPK*

- B2: Chạy thử phần mềm Keyloger:
  - Virus đã ghi lại các hoạt động của bàn phím và chụp màn hình (xem Hình 3.16).



Hình 3.16: Virus ghi lại các hoạt động

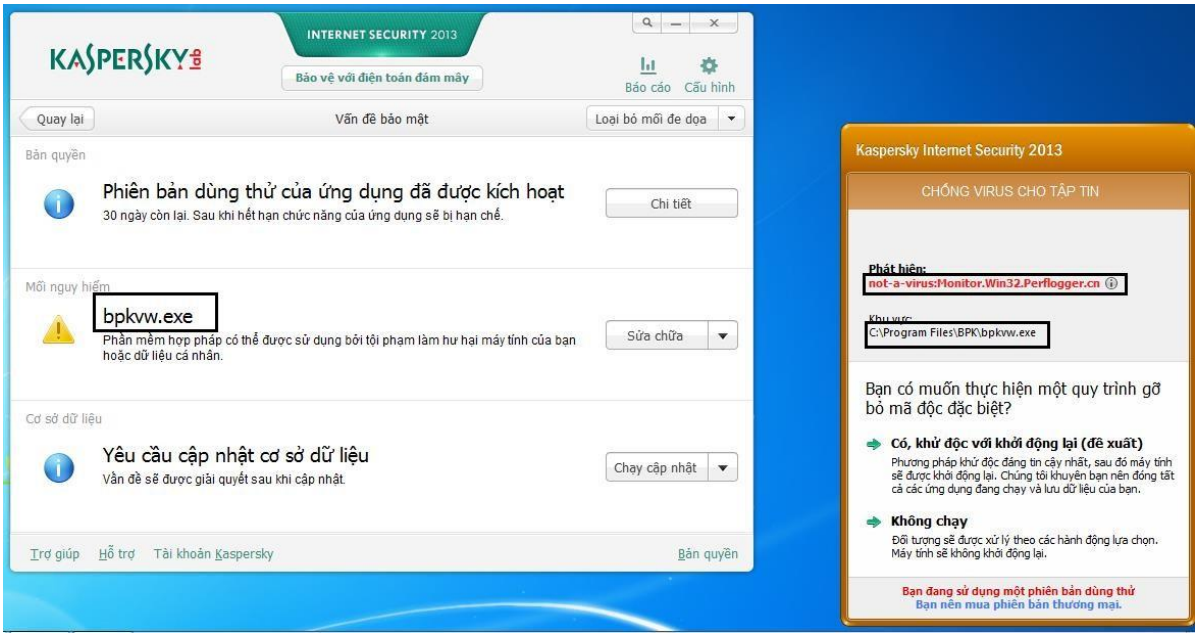
- B3: Cài đặt phần mềm diệt virus Kaspersky Internet Security 2013 (KIS) AV: **Link download**
  - Lưu ý trước khi cài đặt:
    - Gỡ bỏ hết tất cả các phần mềm diệt virus của các hãng khác trên máy tính, nếu không quá trình cài đặt sẽ không thực hiện được.
    - Đảm bảo thời gian trên máy tính phải đúng với hiện tại (bao gồm múi giờ của VN là (GMT +7) Bangkok, Ha Noi, Jakarta; Đồng thời chỉnh giờ, ngày, tháng, năm đúng với hiện tại). Nếu thời gian sai dẫn đến quá trình kích hoạt bản quyền sẽ bị lỗi.
  - Chú ý: Muốn kích hoạt bản quyền thì yêu cầu máy tính phải có kết nối mạng.
  - Kaspersky Internet Security 2013 AV chỉ sử dụng cho máy tính cá nhân, không cài được cho máy chủ.

Hình 3.17: Cài đặt Kaspersky Internet Security

- Các bước cài đặt (xem Hình 3.17):
  - Chọn Cài đặt ngay để bắt đầu quá trình cài đặt.
  - Tại cửa sổ "Chào mừng đến với Kaspersky Internet Security 2013", chọn Cài đặt.
  - Thông báo cài đặt thành công xuất hiện, chọn Hoàn tất để qua bước kích hoạt bản quyền.
- Chú ý: Trong môi trường Lab, ta không cần kích hoạt bản quyền mà chỉ dùng dưới dạng Trial.

3.2.3 Kết quả mong muốn

- Phần mềm Antivirus quét và phát hiện phần mềm gián điệp Perfect Keylogger.
- KIS tự động phát hiện, chặn hành động của Virus (xem Hình 3.18).



Hình 3.18: Giao diện Kaspersky Internet Security

3.3 Cài đặt và sử dụng Iptables

3.3.1 Chuẩn bị môi trường

- Máy ảo Ubuntu (sử dụng Snapshot new).

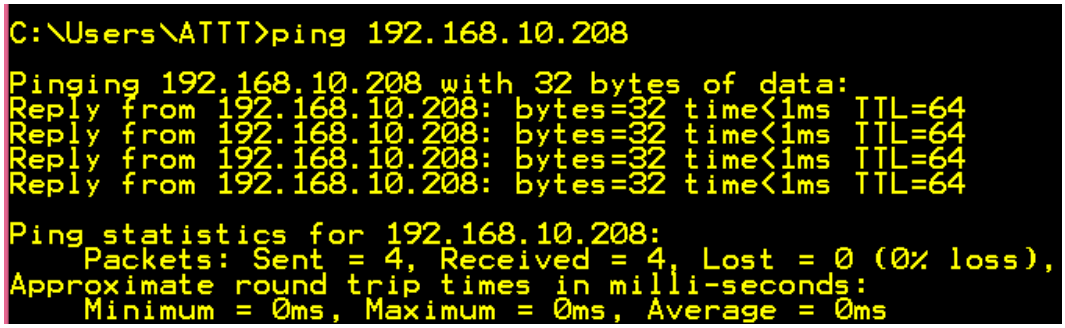
3.3.2 Các bước thực hiện

a) Cài đặt

- Iptables được cài đặt sẵn trong linux, ta kiểm tra bằng lệnh: *$iptables –version* hoặc *$whereis iptables.*

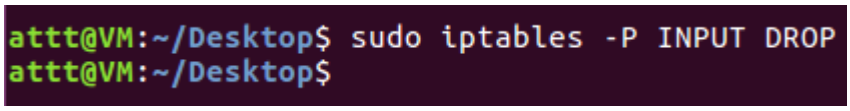
b) Sử dụng

- Chặn kết nối từ 1 máy:
    - Kiểm tra kết nối trước khi chạy Iptables, từ máy windows bật cmd và ping thử đến máy chạy Iptables (xem Hình 3.19).



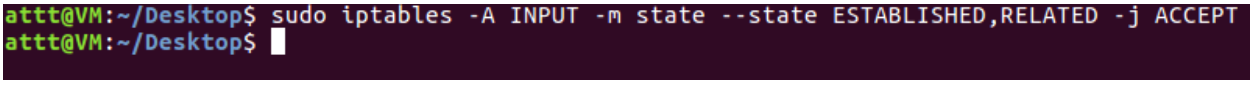
Hình 3.19: Kiểm tra kết nối trước khi chạy Iptables

- Đã thông mạng, nguyên tắc phải tuân theo là đóng tất cả các cổng, sau đó dùng cổng nào thì mở cổng đó (xem Hình 3.20):



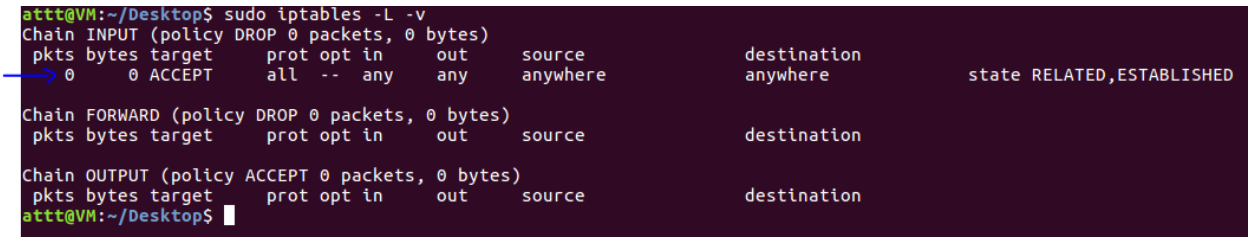
Hình 3.20: Đóng tất cả các cổng

- Sau khi đã DROP hết thì ta giữ lại các kết nối hiện tại và các kết nối liên quan (xem Hình 3.21):



Hình 3.21: Giữ lại các kết nối hiện tại và các kết nối liên quan

- $sudo iptables -L –v //hiển thị các kết nối (xem Hình 3.22):



Hình 3.22: HIển thị các kết nối

- Chặn kết nối từ 1 địa chỉ IP (xem Hình 3.23):
  - $sudo iptables -A INPUT -s 192.168.10.1 -j DROP

```
attt@VM:~$ sudo iptables -A INPUT -s 192.168.10.1 -j DROP
[sudo] password for attt:
```

Hình 3.23: Chặn kết nối từ 1 địa chỉ ip

- $sudo iptables -L –v //hiển thị các kết nối (xem Hình 3.24):

```
attt@VM:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 3 packets, 213 bytes)
 pkts bytes target     prot opt in     out     source               destination
    7   474 DROP       all  --  any    any     192.168.10.1         anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 3 packets, 213 bytes)
 pkts bytes target     prot opt in     out     source               destination
attt@VM:~$
```

Hình 3.24: Các kết nối

- Từ máy windows kiểm tra độ kết nối với máy chạy Iptables (xem Hình 3.25):

```
C:\Users\ATTT>ping 192.168.10.208

Pinging 192.168.10.208 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

Hình 3.25: Kiểm tra kết nối với máy chạy Iptables

- Chặn kết nối từ blacklist:
  - Tạo blacklist (sử dụng bash shell): $black_list=“your list” (xem Hình 3.26).

```
black_list="192.168.10.1 192.168.11.11"
```

Hình 3.26: Tạo blacklist

  - Câu lệnh chặn kết nối từ blacklist (xem Hình 3.27):

    $for i in $black_list;do enter

    >iptables -A INPUT –i eth0 -s $i -j DROP

    >done

```
attt@VM:~/Desktop$ for i in $back_list;do
> iptables -A INPUT -i eth0 -s $i -j DROP
> done
attt@VM:~/Desktop$
```

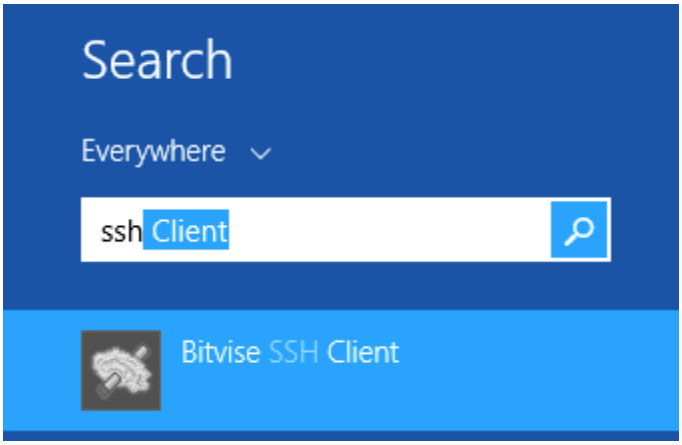
Hình 3.27: Câu lệnh chặn kết nối từ blacklist

Với eth0 là card mạng của mình.

- Như vậy các máy có ip trong blacklist sẽ không kết nối được với máy chạy Iptables nữa.

- Tạo roles cho phép truy cập SSH:

  - Thử truy cập SSH đến máy chạy iptables chưa chặn SSH:
    Từ windows khởi động phần mềm Bitvise SSH Client (xem Hình 3.28).



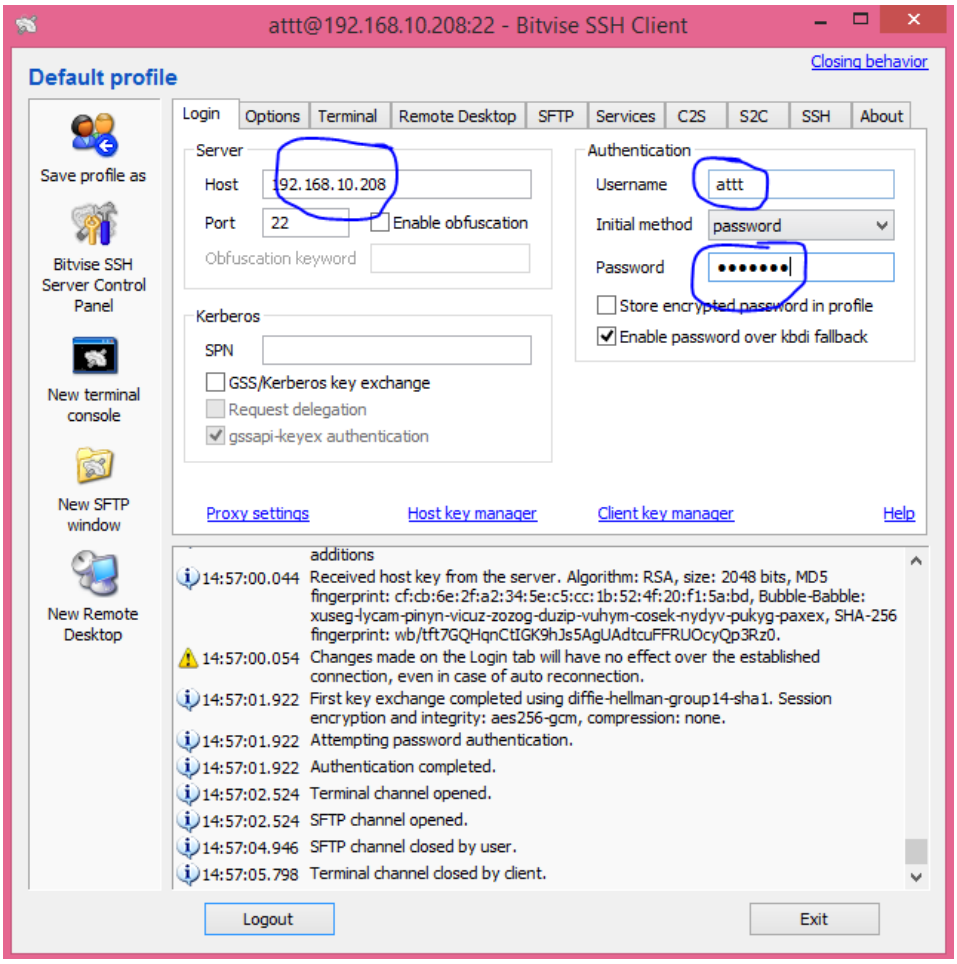
Hình 3.28: Truy cập phần mềm Bitvise SSH Client

  - Nhập thông tin vào phần mềm Bitvise SSH Client (xem Hình 3.29):

    host: IP của máy ảo ubuntu

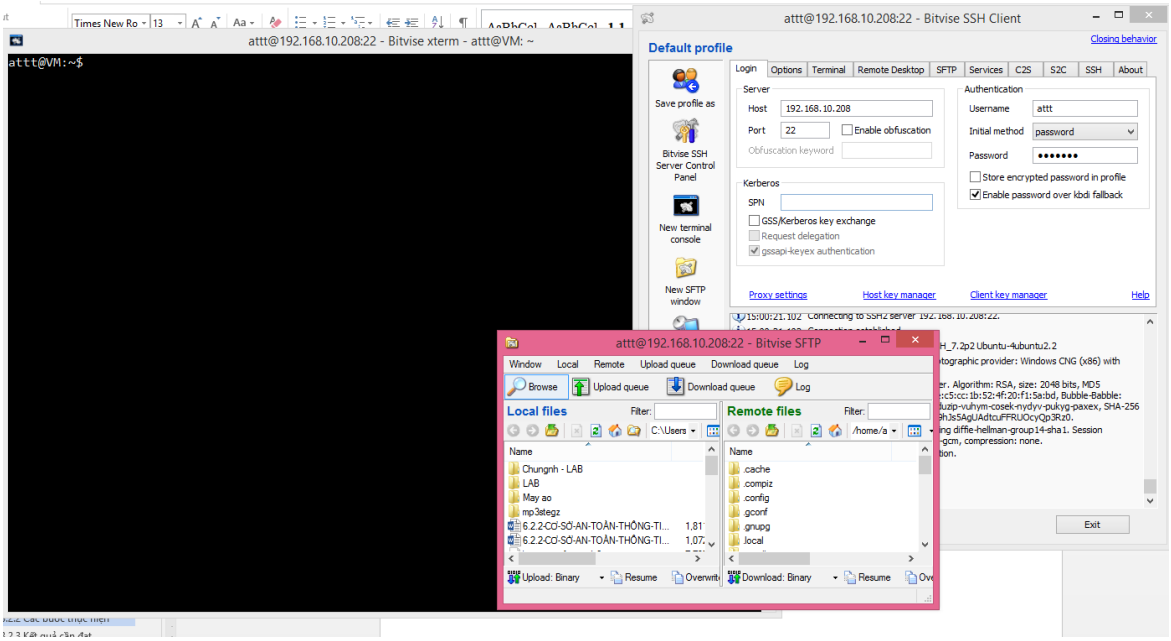
    User: attt

    Password: cdit@123



Hình 3.29: Giao diện phần mềm Bitvise SSH Client

⇨ Như vậy là kết nối ssh thành công (xem Hình 3.30):



Hình 3.30: Kết nối ssh thành công

- Tạo luật chặn kết nối SSH (xem Hình 3.31):

  $sudo iptables -A INPUT -p tcp --dport 22 -j DROP

```
attt@VM:~$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
[sudo] password for attt:
```

Hình 3.31: Tạo luật chặn kết nối SSH

- $sudo iptables -L –v //hiển thị các kết nối (xem Hình 3.32):

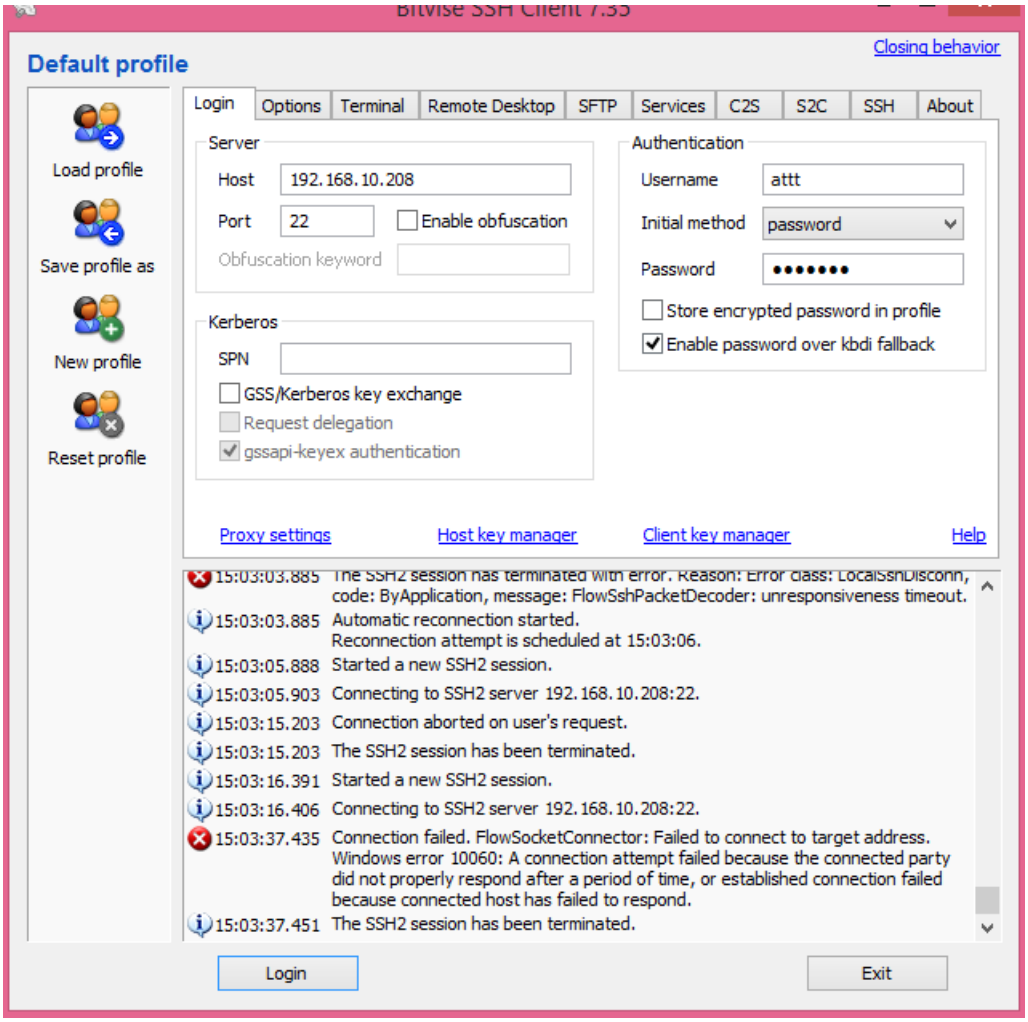
```
attt@VM:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
attt@VM:~$
```

Hình 3.32: Hiển thị các kết nối

- Thử kết nối lại bằng SSH Client (xem Hình 3.33):



Hình 3.33: Chặn thành công SSH

⇨ Chặn thành công SSH.

- Chặn truy cập đến cổng 80 của dịch vụ HTTP:

  - Cài đặt và khởi động Apache (xem Hình 3.34):

    $sudo apt-get install apache2 (nếu có rồi thì kiểm tra status)

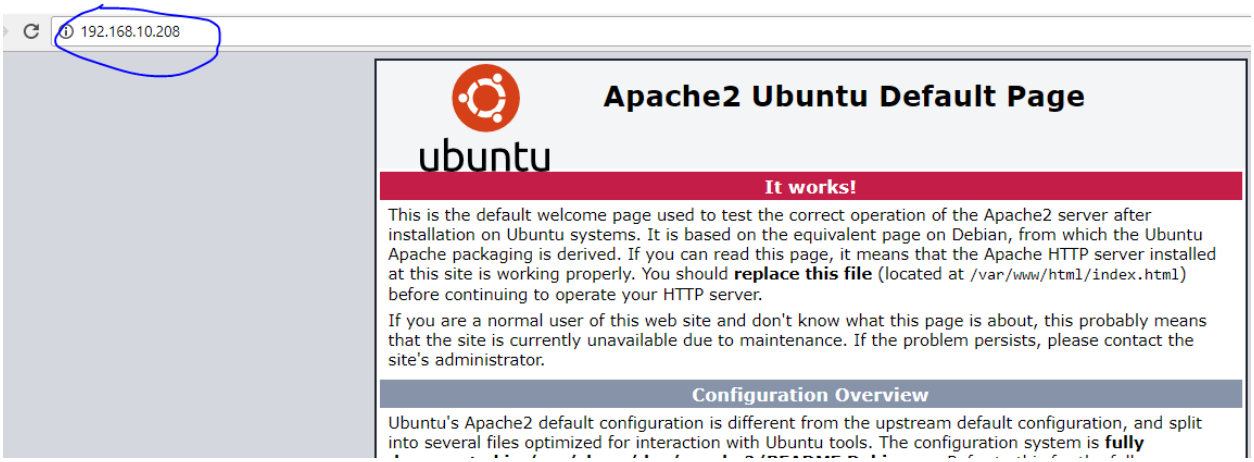
    $sudo service apache2 status

```
attt@VM:~$ sudo service apache2 status
● apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since T3 2017-11-14 15:19:35 ICT; 2min 53s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 3729 ExecStop=/etc/init.d/apache2 stop (code=exited, status=0/SUCCESS)
  Process: 3751 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/apache2.service
           ├─3771 /usr/sbin/apache2 -k start
           ├─3774 /usr/sbin/apache2 -k start
           └─3775 /usr/sbin/apache2 -k start

Th11 14 15:19:34 VM systemd[1]: Starting LSB: Apache2 web server...
Th11 14 15:19:34 VM apache2[3751]:  * Starting Apache httpd web server apache2
Th11 14 15:19:34 VM apache2[3751]: AH00558: apache2: Could not reliably determine the server's fully qu
Th11 14 15:19:35 VM apache2[3751]:  *
Th11 14 15:19:35 VM systemd[1]: Started LSB: Apache2 web server.
lines 1-18/18 (END)
```

Hình 3.34: Cài đặt và khởi động Apache

- Từ trình duyệt của windows truy cập vào IP máy chạy Apache (xem Hình 3.35):



Hình 3.35: Truy cập vào IP máy chạy Apache

⇨ Đã thông kết nối.

- Tạo luật chặn kết nối đến cổng 80 (xem Hình 3.36):

  $sudo iptables -A INPUT -p tcp --dport 80 -j DROP

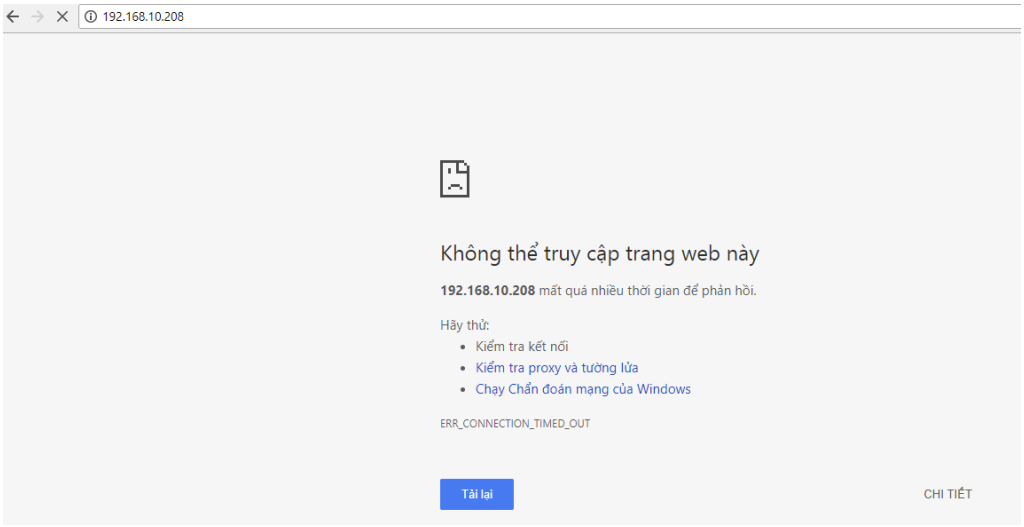
```
attt@VM:~$ sudo iptables -A INPUT -p tcp --dport 80 -j DROP
attt@VM:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   17  1788 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
attt@VM:~$
```

Hình 3.36: Tạo luật chặn kết nối đến cổng 80

- Truy cập lại từ trình duyệt (xem Hình 3.37):



Hình 3.37: Chặn kết nối thành công

⇨ Chặn kết nối thành công.

3.3.3 Kết quả mong muốn

- Sinh viên biết sử dụng cơ bản Iptables.
- Chặn cổng 22 của SSH, cổng 80 của HTTP, chặn kết nối từ 1 IP.