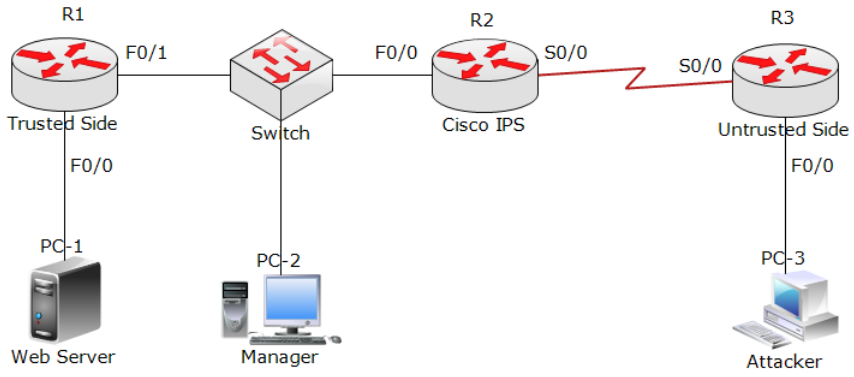
I. Giới thiệu IPS (Intrusion Protection System)

IPS Là hệ thống ngăn chặn xâm nhập, có chức năng tự động theo dõi và ngăn chặn các sự kiện xảy ra trong và ngoài hệ thống mạng, phân tích và ngăn ngừa các vấn đề liên quan tới bảo mật và an ninh. Hệ thống ngăn chặn xâm nhập giám sát các gói tin đi qua và đưa ra quyết định liệu đây có phải là một cuộc tấn công hay một sự truy cập hợp pháp – sau đó thực hiện hành động thích hợp để bảo vệ hệ thống mạng.

II. Bài tập thực hành

Mô hình triển khai



Mô hình minh họa hệ thống gồm mạng nội bộ và thiết bị Cisco IOS IPS, Cisco IOS IPS ngoài chức năng Firewall nó còn có chức năng tìm kiếm, so sánh những lưu lượng có dấu hiệu tấn công vào hệ thống, khi phát hiện có dấu hiệu tấn công nó gửi cảnh báo đến hệ thống cảnh báo hoặc loại bỏ những gói tin mà nó so sánh trùng với các dấu hiệu tấn công hoặc reset lại kết nối.

Bảng địa chỉ IP

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.1.1	255.255.255.0	N/A
	F0/1	192.168.12.1	255.255.255.0	N/A
R2	F0/0	192.168.12.2	255.255.255.0	N/A
	S0/0(DCE)	192.168.23.2	255.255.255.0	N/A
R3	F0/0	192.168.2.1	255.255.255.0	N/A
	S0/0	192.168.23.1	255.255.255.0	N/A
PC-1	NIC	192.168.1.254	255.255.255.0	192.168.1.1
PC-2	NIC	192.168.12.3	255.255.255.0	N/A
PC-3	NIC	192.168.2.2	255.255.255.0	192.168.2.1

Yêu cầu

Phần 1: Cấu hình thiết bị mạng cơ bản

- Cấu hình cơ bản địa chỉ IP cho các Router và PC.
- Cấu hình định tuyến tĩnh trên R2, default route trên R1, R3.
- Cài đặt web server trên PC-1.
- Kiểm tra kết nối giữa các PC và router.

Phần 2: Cấu hình Cisco IPS

- Cài đặt SDM trên PC-2.
- Phát hiện và ngăn chặn tấn công ping of death, scan port, denial of service (dos) vào web server từ PC-3 (attacker).

Thiết bị và phần mềm hỗ trợ

- Phần mềm GNS3
- Phần mềm VMWARE
- 3 router (Cisco IOS C2691 , phiên bản 12.4(16)T hoặc tương đương)
- PC-1: Windows Server với web server

- PC-2: Windows XP, windows 7 với SDM
- PC-2: Windows XP, windows 7 với công cụ superscan, doshttp

Hướng dẫn cấu hình

Phần 1: Cấu hình thiết bị mạng cơ bản

- **Cấu hình cơ bản địa chỉ IP cho các Router và PC:**

Router R1

```
R1# configure terminal
R1(config)# interface f0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1config-if)# exit
R1(config)# interface f0/1
R1(config-if)# ip address 192.168.12.1 255.255.255.0
R1(config-if)# no shutdown
```

Router R2

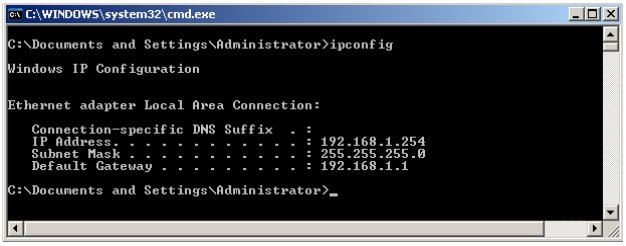
```
R2# configure terminal
R2(config)# interface f0/0
R2(config-if)# ip address 192.168.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface s0/0
R2(config-if)# ip address 192.168.23.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# clock rate 64000
```

Router R3

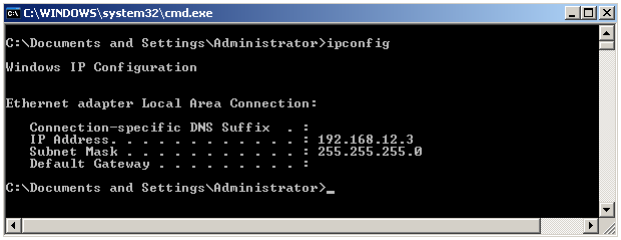
```
R3# configure terminal
R3(config)# interface f0/0
R3(config-if)# ip address 192.168.2.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# exit
```

```
R3(config)# interface s0/0
R3(config-if)# ip address 192.168.23.1 255.255.255.0
R3(config-if)# no shutdown
```

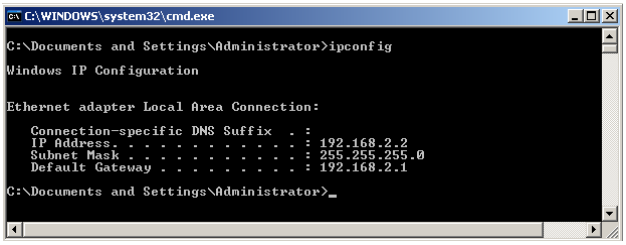
PC-1



PC-2



PC-3



- **Cấu hình định tuyến tĩnh trên R2, default route trên R1, R3:**

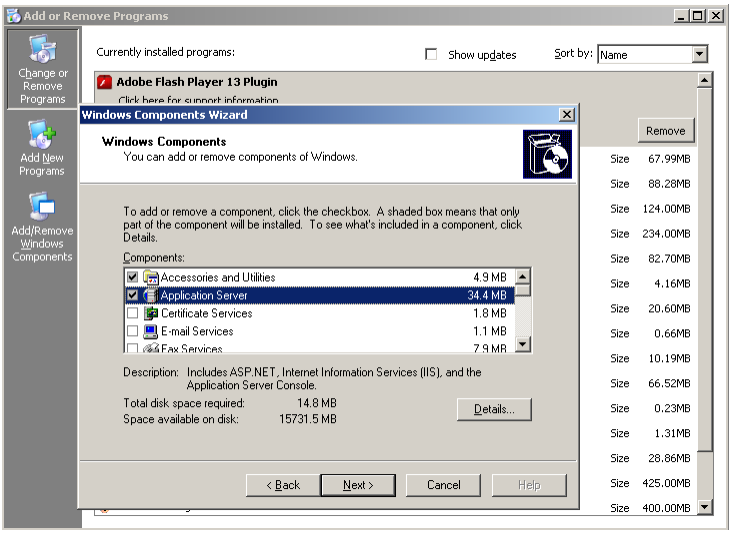
```
Router R1
R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.12.2
Router R2
R2(config)# ip route 192.168.1.0 255.255.255.0 192.168.12.1
R2(config)# ip route 192.168.2.0 255.255.255.0 192.168.23.1
Router R3
R3(config)# ip route 0.0.0.0 0.0.0.0 192.168.23.2
```

- **Cài đặt web server trên PC-1:**

Thực hiện trên windows server 2003:

Vào start → control panel → add or remove programs → add/remove windows components.

Trong cửa sổ windows components wizard, chọn vào dòng application server → next.



Cài đặt dịch vụ web server

Xuất hiện hộp thoại files needed, chỉ đường dẫn tới thư mục i386 chứa file cài web server → finish.

Tạo trang web cho web server, vào my compurter → ổ đĩa c → inetpub → wwwroot. Tạo file index.htm, với nội dung tùy ý.

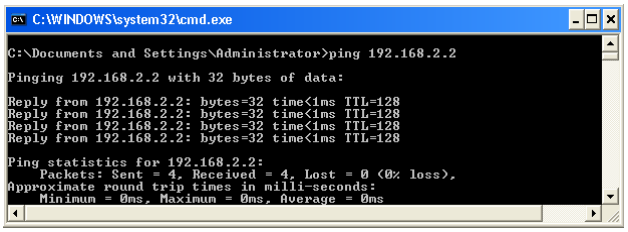
- **Kiểm tra kết nối giữa các PC và router:**

Ping thành công từ R1 đến R3

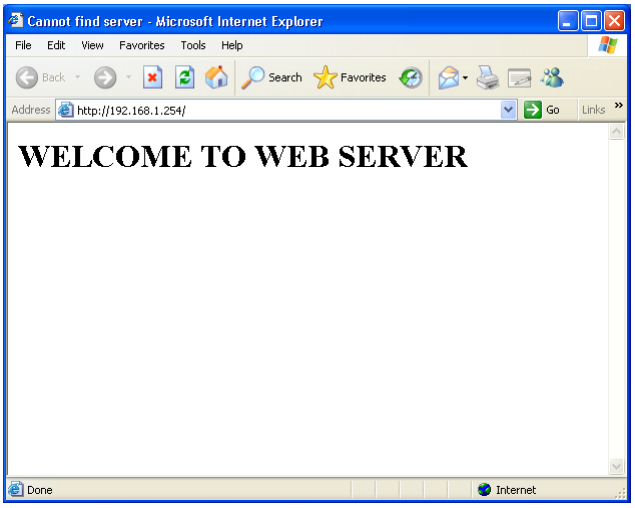
```
R1#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/32/92 ms
```

Ping thành công từ PC-1 đến PC-3



Truy cập web server thành công từ bên ngoài internet (PC-3) hoặc bên trong mạng nội bộ.



Truy cập web server

Phần 2: Cấu hình Cisco IPS

Tạo một tài khoản người dùng và kích hoạt HTTP server trên R2 trước khi truy cập SDM:

```
R2(config)#username sdm privilege 15 password 0 cisco
R2(config)#ip http server
R2(config)#ip http authentication local
```

- **Cài đặt SDM trên PC-2:**

Yêu cầu PC-2 đã cài đặt java-jre phiên bản 6 trở lên.

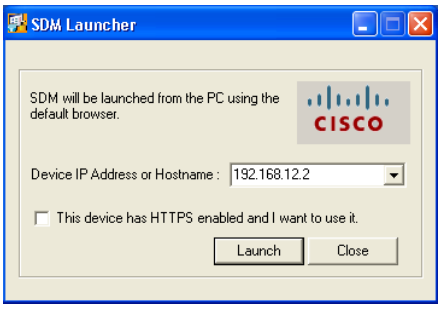
Tải phần mềm Cisco SDM:

Tải SDM phiên bản 2.5 từ đường dẫn
https://drive.google.com/file/d/0B4rIOTvEwpnAMjFIOVk3T2xsWmM/edit

Cài đặt SDM:

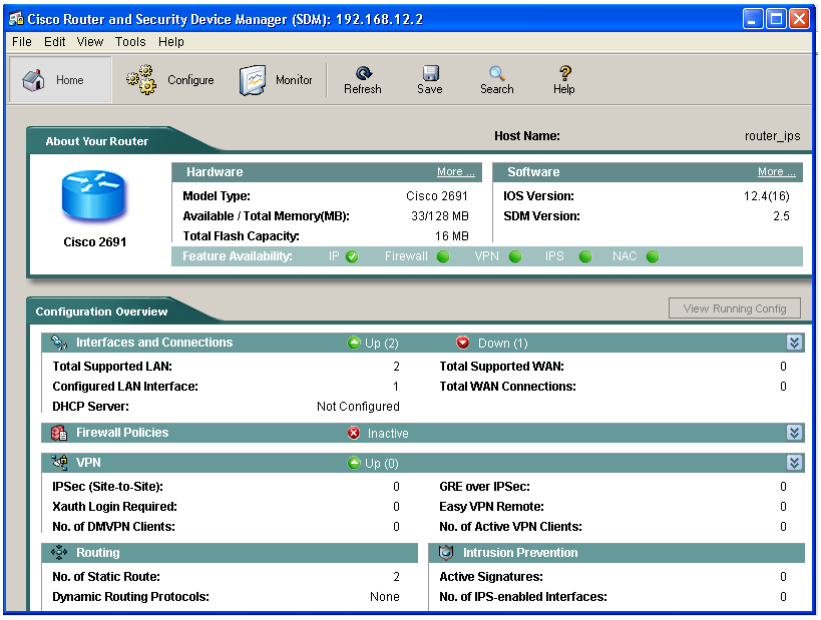
Giải nén thư mục SDM v2.5 vừa tải về, chọn file "setup.exe" để bắt đầu cài đặt, hộp thoại Ciso SDM xuất hiện chọn "next", chấp nhận các điều khoản bản quyền của SDM, chọn "i accept….", trong hộp thoại "install option" chọn "this computer" và nhấn "install" để cài đặt.

Chạy phần mềm Cisco SDM vừa cài đặt, nhập vào IP của R2 (192.168.12.2) trong trường "Device IP Address or Hostname → lauch".



Chương trình khởi động SDM

Tắt chức năng "Block popup Window" ở trình duyệt Web. Đăng nhập với người dùng "sdm" và mật khẩu "cisco".



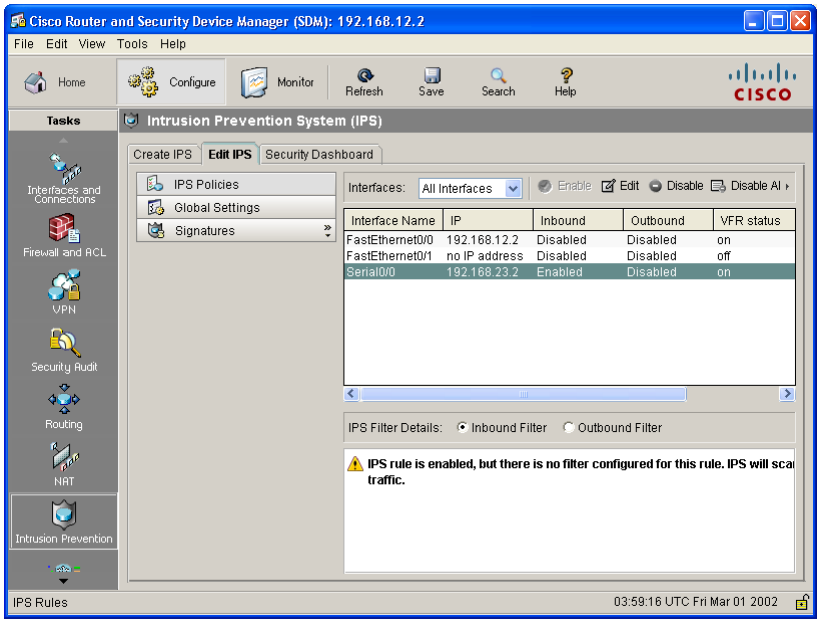
Giao diện chính của SDM

Cấu hình rule cho IPS:

- Menu Configure → chọn Intrusion Prevention (bên trái)→ chọn "Launch IPS Rule Wizard" để bắt đầu cài đặt các rule IPS lên R2.
- SDEE là một công nghệ để báo cáo những sự kiện bảo mật khi kích hoạt IPS trong router, Cisco SDM yêu cầu thông báo sự kiện IPS qua SDEE để cấu hình tính năng Cisco IOS IPS, theo mặc định, thông báo SDEE không được kích hoạt. Cisco SDM sẽ nhắc nhở người dùng để cho phép thông báo sự kiện IPS qua SDEE chọn ok.

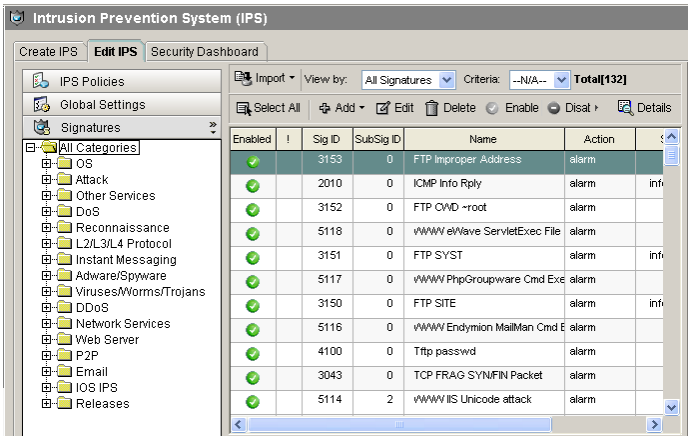
Trong hộp thoại "IPS policies wizard" chọn "next". Chọn cổng s0/0 theo chiều inbound và nhấn "next" khi kết thúc việc lựa chọn.

Chọn vào "Use Built-In Signatures (as backup)" sử dụng các signatures đã được xây dựng trên Cisco IOS và chọn "next" → "finish". Hộp thoại "command delivery status" xuất hiện chọn ok để nạp các signature lên R2.



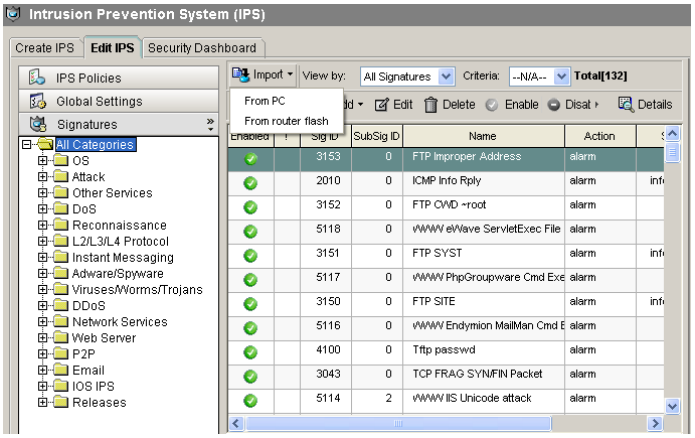
Card mạng IPS đang theo dõi

Chọn configure → intrusion prevention → edit IPS → signatures, để kiểm tra các signature mặc định được nạp lên R2.



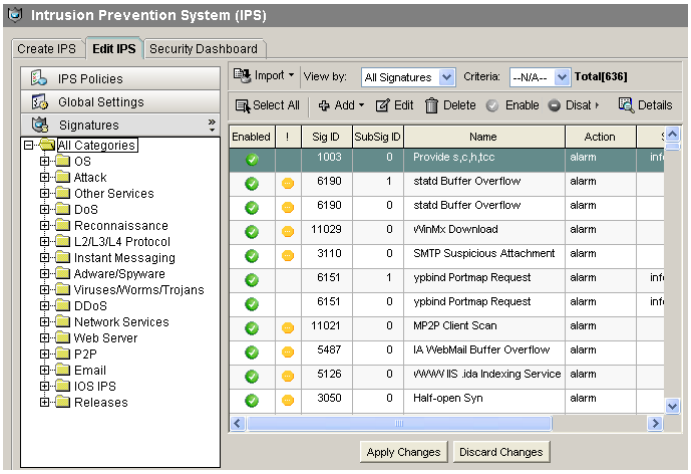
Các signature trên R2

Chọn edit IPS → import → from pc để import thêm signature mới từ file cài đặt sdm.



Nạp file SDF cho IOS IPS (R2)

Chỉ đường dẫn tới file cài đặt SDM → 256.sdf → open. Chọn "merge" để tiến hành import các signature vào R2 và chọn "apply changes" để tiến hành import các signature.

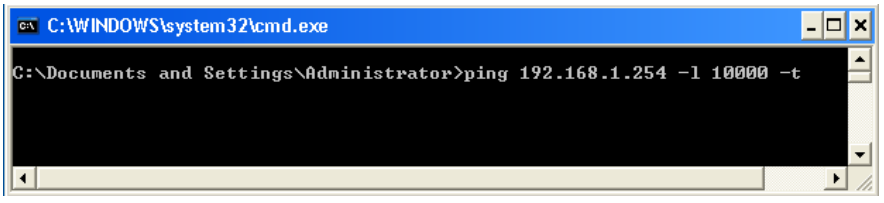


Các signature được import

- **Phát hiện và ngăn chặn tấn công ping of death từ PC-3 (Attacker):**

Phát hiện:

Trên PC-3 thực hiện tấn công ping of death vào PC-1(web server) với số kích thước gói tin là 10000

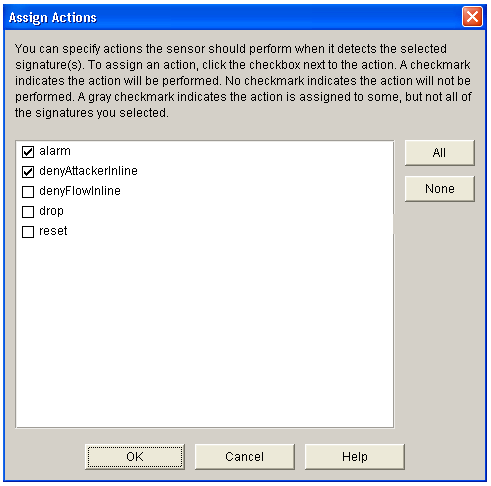


R2 xuất hiện các log thông báo có tấn công ping of death từ PC-3 vào PC-1 với sig id: 2151, name: Large ICMP

```
*Mar  1 00:52:47.739: %IPS-4-SIGNATURE: Sig:2151 Subsig:0 Sev:2 Large ICMP [192.168.2.2:0 -> 192.168.1.254:0]
*Mar  1 00:52:47.743: %IPS-4-SIGNATURE: Sig:2151 Subsig:0 Sev:2 Large ICMP [192.168.2.2:0 -> 192.168.1.254:0]
*Mar  1 00:52:47.743: %IPS-4-SIGNATURE: Sig:2151 Subsig:0 Sev:2 Large ICMP [192.168.2.2:0 -> 192.168.1.254:0]
*Mar  1 00:52:47.747: %IPS-4-SIGNATURE: Sig:2151 Subsig:0 Sev:2 Large ICMP [192.168.2.2:0 -> 192.168.1.254:0]
*Mar  1 00:52:47.751: %IPS-4-SIGNATURE: Sig:2151 Subsig:0 Sev:2 Large ICMP [192.168.2.2:0 -> 192.168.1.254:0]
*Mar  1 00:52:47.755: %IPS-4-SIGNATURE: Sig:2151 Subsig:0 Sev:2 Large ICMP [192.168.2.2:0 -> 192.168.1.254:0]
*Mar  1 00:52:48.743: %IPS-4-SIGNATURE: Sig:2151 Subsig:0 Sev:2 Large ICMP [192.168.2.2:0 -> 192.168.1.254:0]
```

Ngăn chặn:

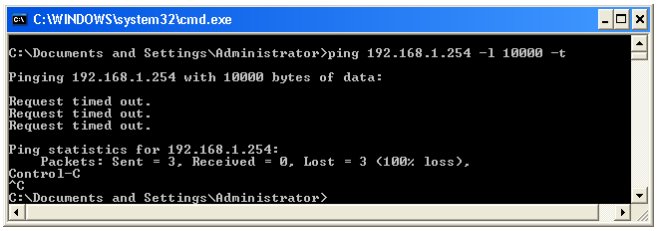
Chọn vào sig id: 2151 → chọn "action" và lựa chọn hành động



Định nghĩa hành động cho dấu hiệu

Chọn vào hành động "alarm và denyAttackerInline" và nhấn ok. Để áp dụng những thay đổi về hành động lên R2 chọn "apply changes".

Lúc này PC-3 không thể ping of death vào PC-1, do rule chặn tấn công ping of death trên R2 đã chặn hành động này.

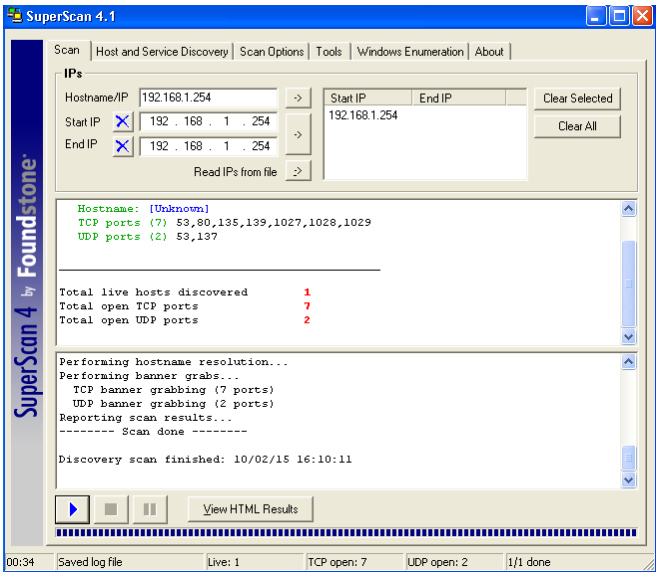


Tấn công ping of death bị chặn

- **Phát hiện và ngăn chặn tấn công scan port từ PC-3 (Attacker):**

Phát hiện:

Trên PC-3 chạy công cụ superscan. Trong tab IPs tiến hành thêm ip của PC-1 (192.168.1.254) vào mục hostname/IP và nhấn vào hình mũi tên tam giác để tiến hành quét port trên PC-1.



Các port đang mở trên PC-1

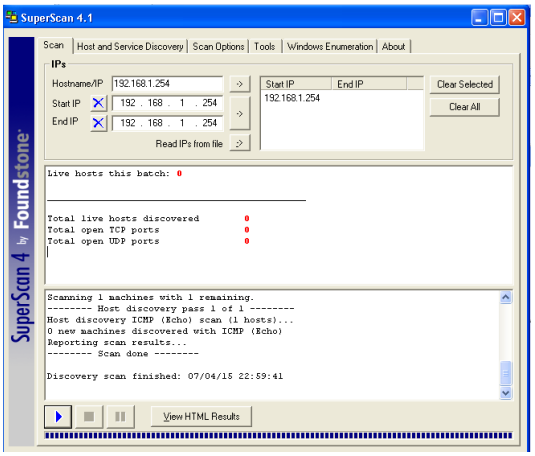
Thông báo log trên R2 phá hiện quá trình scan port từ PC-3

```
*Mar  1 02:56:03.111: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [192.168.2.2:0 -> 192.168.1.254:0]
Router_IPS(config-line)#
*Mar  1 02:56:04.111: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [192.168.2.2:0 -> 192.168.1.254:0]
*Mar  1 02:56:05.087: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [192.168.2.2:0 -> 192.168.1.254:0]
*Mar  1 02:56:06.115: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [192.168.2.2:0 -> 192.168.1.254:0]
*Mar  1 03:00:57.799: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [192.168.2.2:0 -> 192.168.1.254:0]
*Mar  1 03:01:05.467: %IPS-4-SIGNATURE: Sig:4060 Subsig:0 Sev:4 Back Orifice Ping [192.168.2.2:2603 -> 192.168.1.254:31337
]
Router_IPS(config-line)#
*Mar  1 03:01:05.491: %IPS-4-SIGNATURE: Sig:4600 Subsig:0 Sev:4 IOS Udp Bomb [192.168.2.2:2605 -> 192.168.1.254:514]
*Mar  1 03:01:05.983: %IPS-4-SIGNATURE: Sig:6054 Subsig:0 Sev:3 DNS Version Request [192.168.2.2:2630 -> 192.168.1.254:53]
```

Log thông báo quá trình scan port

Ngăn chặn:Quá trình scan port sử dụng công cụ superscan sẽ gửi gói icmp req tới PC-1, nên để ngăn chặn quá trình scan port sử dụng công cụ này, chỉ cần áp dụng chính sách ngăn chặn đối với rule này. Chọn vào sig id: 2004 → chọn "action" và lựa chọn hành động "alarm và denyAttackerInline" và nhấn ok. Để áp dụng những thay đổi về hành động lên R2 chọn "apply changes".

Lúc này PC-3 không thể scan port vào PC-1.

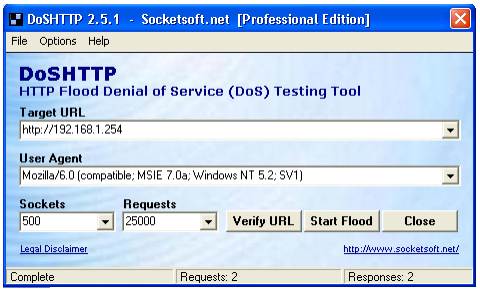


Quá trình scan port đã bị chặn

- **Phát hiện và ngăn chặn tấn công denial of service (dos) vào web server từ PC-3 (Attacker):**

Phát hiện:

Trên PC-3 chạy công cụ doshttp phiên bản 2.5.1. Trong mục target URL, nhập vào đường dẫn truy cập web server(http://192.168.1.254), với số socket là: 500, request: 25000. Sau đó nhấn start flood để tiến hành tấn công.



Tấn công dos vào web server

R2 xuất hiện các log thông báo có tấn công từ chối dịch vụ vào web server từ PC-3 vào PC-1 với sig id: 3051, name: TCP connection window size DOS.

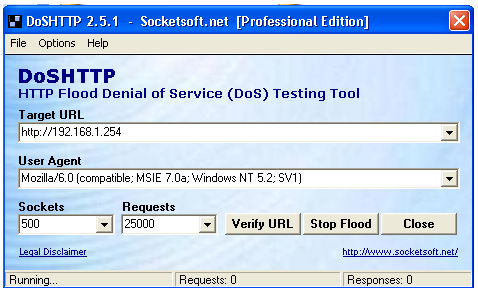
```
*Mar  1 02:40:01.355: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.2.2:3432 -> 192.16
8.1.254:80]
Router_IPS(config-line)#
*Mar  1 02:40:03.247: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.2.2:4563 -> 192.16
8.1.254:80]
Router_IPS(config-line)#
*Mar  1 02:40:04.743: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.2.2:1758 -> 192.16
8.1.254:80]
Router_IPS(config-line)#
*Mar  1 02:40:06.247: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.2.2:2758 -> 192.16
8.1.254:80]
Router_IPS(config-line)#
*Mar  1 02:40:08.023: %IPS-4-SIGNATURE: Sig:3051 Subsig:1 Sev:4 TCP Connection Window Size DoS [192.168.2.2:3758 -> 192.16
```

Log thông báo tấn công từ chối dịch vụ vào web server

Ngăn chặn:

Chọn vào sig id: 3051, có subsigID là 1 → chọn "action" và lựa chọn hành động "alarm và denyAttackerInline" và nhấn ok. Để áp dụng những thay đổi về hành động lên R2 chọn "apply changes".

Lúc này PC-3 không thể tấn công từ chối dịch vụ vào web server, do rule chặn tấn công từ chối dịch vụ vào web server trên R2 đã chặn hành động này.



Tấn công dos vào web server đã bị từ chối