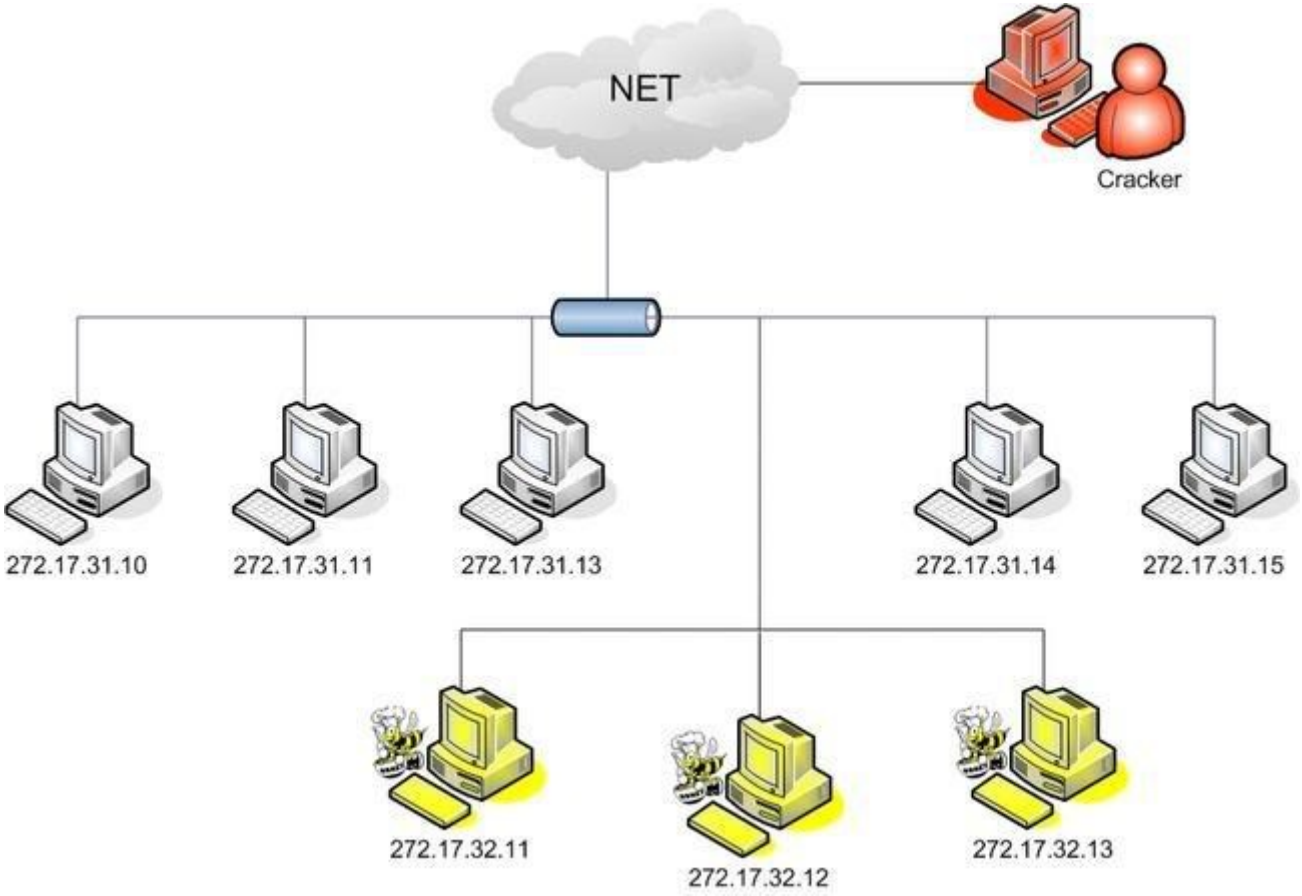
Chương 7.
Mạng Honeynet

I. Giới thiệu chung

I. Giới thiệu chung



Đặt vấn đề

- **Biện pháp bảo vệ chính cho hệ thống mạng:**
  - Tưởng lửa, hệ thống phát hiện và ngăn chặm xâm nhập, anti-virus…
  - Cơ chế hoạt động của các biện pháp này là phát hiện và ngăn chặn dựa trên dấu hiệu, mẫu có sẵn.
- **Hệ thống mạng Honeypot & Honeynet:**
  - Là hệ thống không có giá trị thực, có nhiều lỗ hổng.
  - Thu hút tin tặc tấn công nhằm thu thập hành vi của tin tặc

I. Mạng Honeypot

- Honeypot là hệ thống tài nguyên thông tin được xây dựng giả lập các dịch vụ mạng với rất nhiều các lỗ hổng nhằm thu hút tin tặc.
- Các tài nguyên thông tin mà Honeypot có thể giả lập: dịch vụ mail, web, FTP, DNS…
- Honeypot tương tác trực tiếp với tin tặc và tìm các khai thác các kỹ thuật mà tin tặc sử dụng như: hình thức tấn công, công cụ tấn công, cách thức tiến hành…
- Tổng hợp và gửi thông tin đến người quản trị, từ đó người quản trị có thể đưa ra các phương pháp đối phó để áp dụng vào hệ thống thật sự.

I. Mạng Honeypot

Các dạng Honeypot:

- Mức độ tương tác của Honeypot
- Mục đích triển khai

I. Mạng Honeypot

Mức độ tương tác:

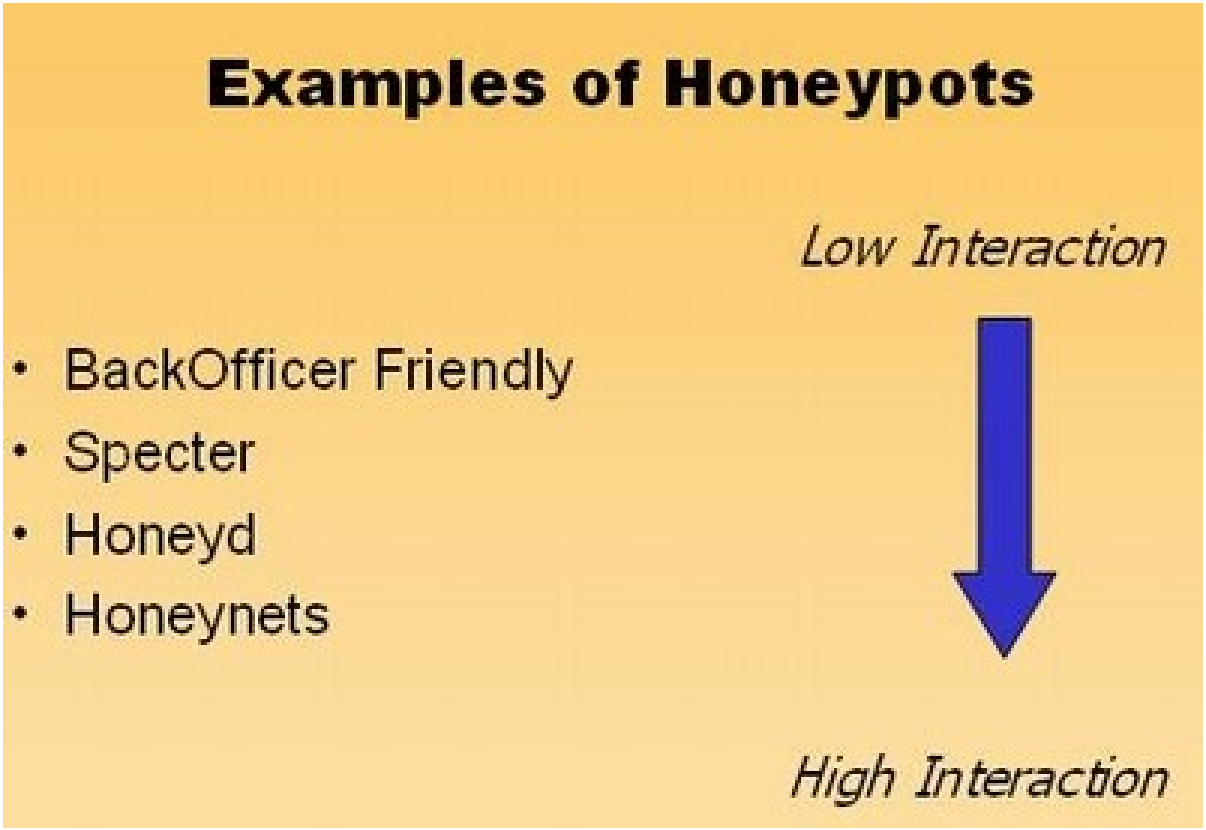
- Honeypot tương tác thấp
- Honeypot tương tác trung bình
- Honeypot tương tác cao

I. Mạng Honeypot

Mức độ tương tác:

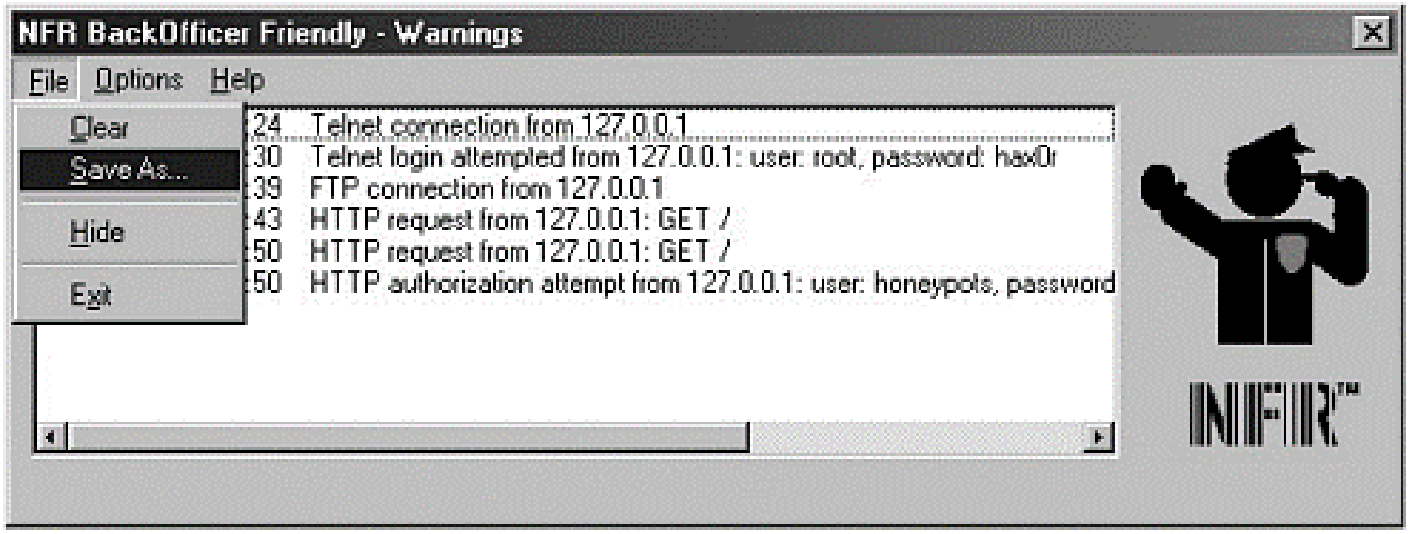
- **Honeypot tương tác thấp:** Mô phỏng giả các dịch vụ, ứng dụng, và hệ điều hành. Mức độ rủi ro thấp, dễ triển khai và quản trị nhưng bị giới hạn về dịch vụ.
- **Honeypot tương tác trung bình:** Mô phỏng nhiều dịch vụ hơn như: webserver. Mailserver, file server, máy chủ xác thực …
- **Honeypot tương tác cao:** Là các dịch vụ, ứng dụng và hệ điều hành thực. Mức độ thông tin thu thập được cao. Nhưng mức độ rủi ro cao, tốn thời gian triển khai và bảo trì.

I. Mạng Honeypot



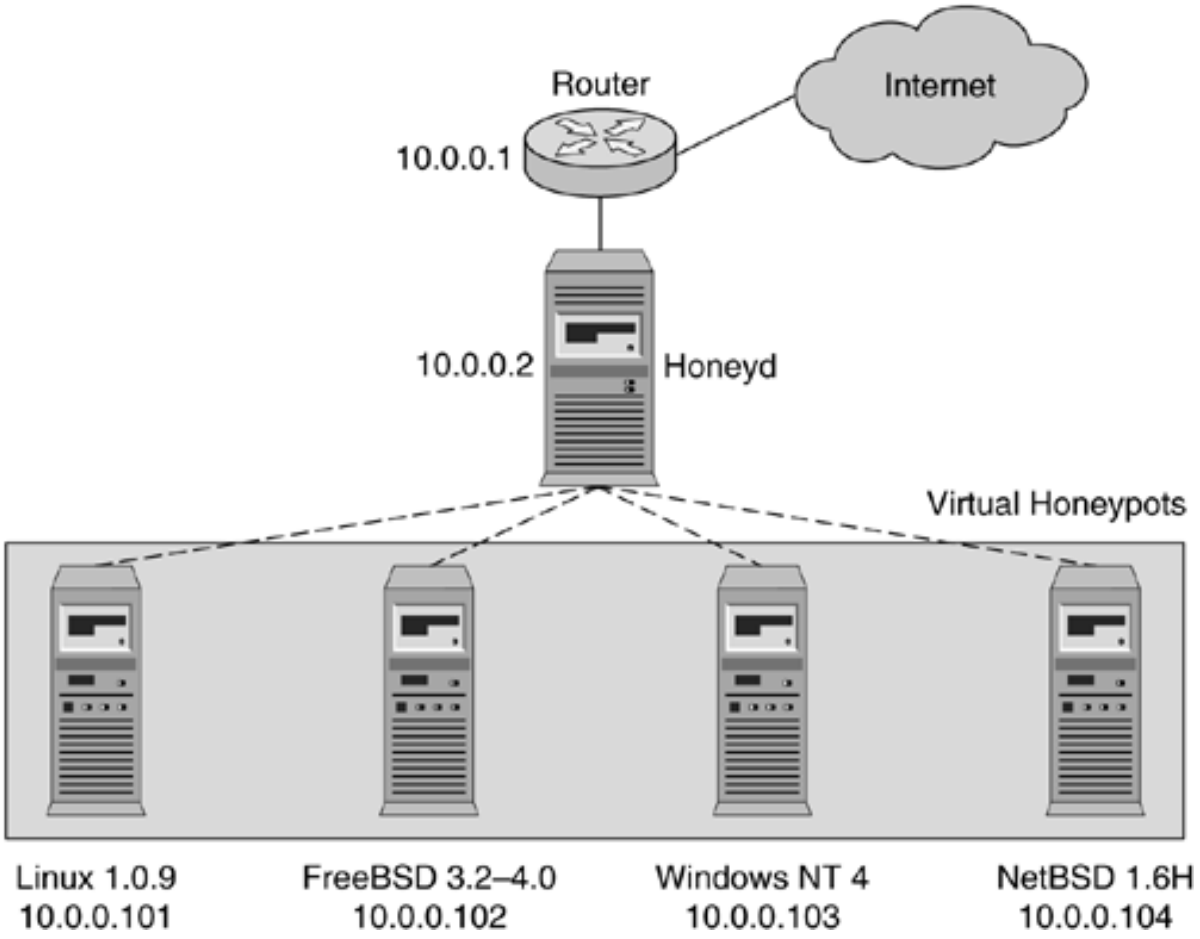
I. Mạng Honeypot

Ví dụ: BackOffice Friendly



I. Mạng Honeypot

Ví dụ: Honeyd



II. Mạng Honeynet

- Honeynet là loại hình honeypot tương tác cao
- Honeynet cung cấp các hệ thống, ứng dụng, dịch vụ thật.
- 3 chức năng chính: Điều khiển dữ liệu, thu thập dữ liệu, phân tích dữ liệu.

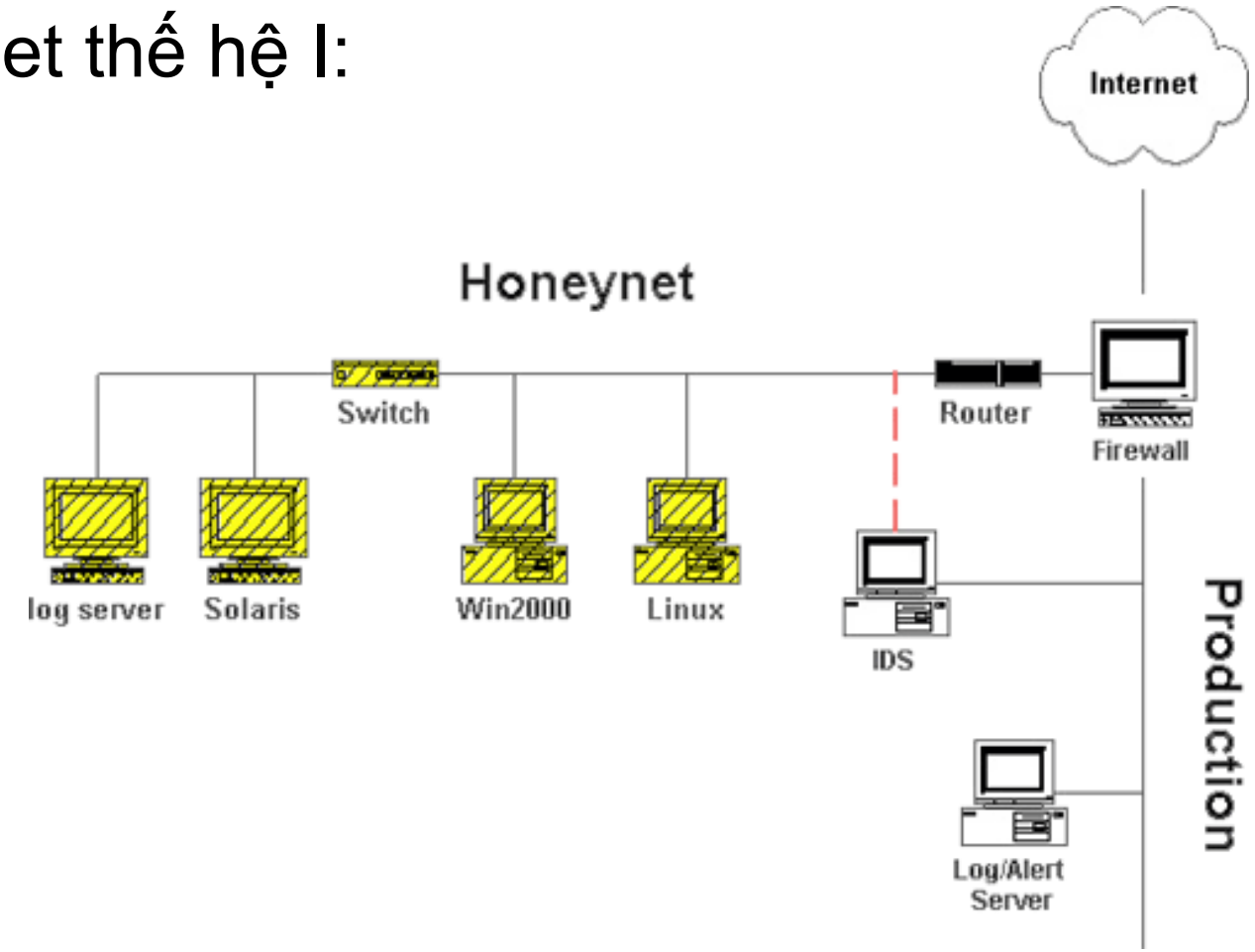
II. Mạng Honeynet

Lịch sử phát triển:

- Honeynet đầu tiên ra đời năm 1999 và được gọi là Gen I.
- Đến năm 2001 Honeynet thế hệ thứ 2 ra đời và được gọi là Gen II.
- Mô hình Gen III ra đời cuối năm 2004. Điểm khác biệt chính là Honeynet Gen III được hỗ trợ thêm nhiều tính năng về quản lý.
- 2005: Honeywall CDROM phiên bản 2-ROO. Dựa vào công nghệ Gen III.

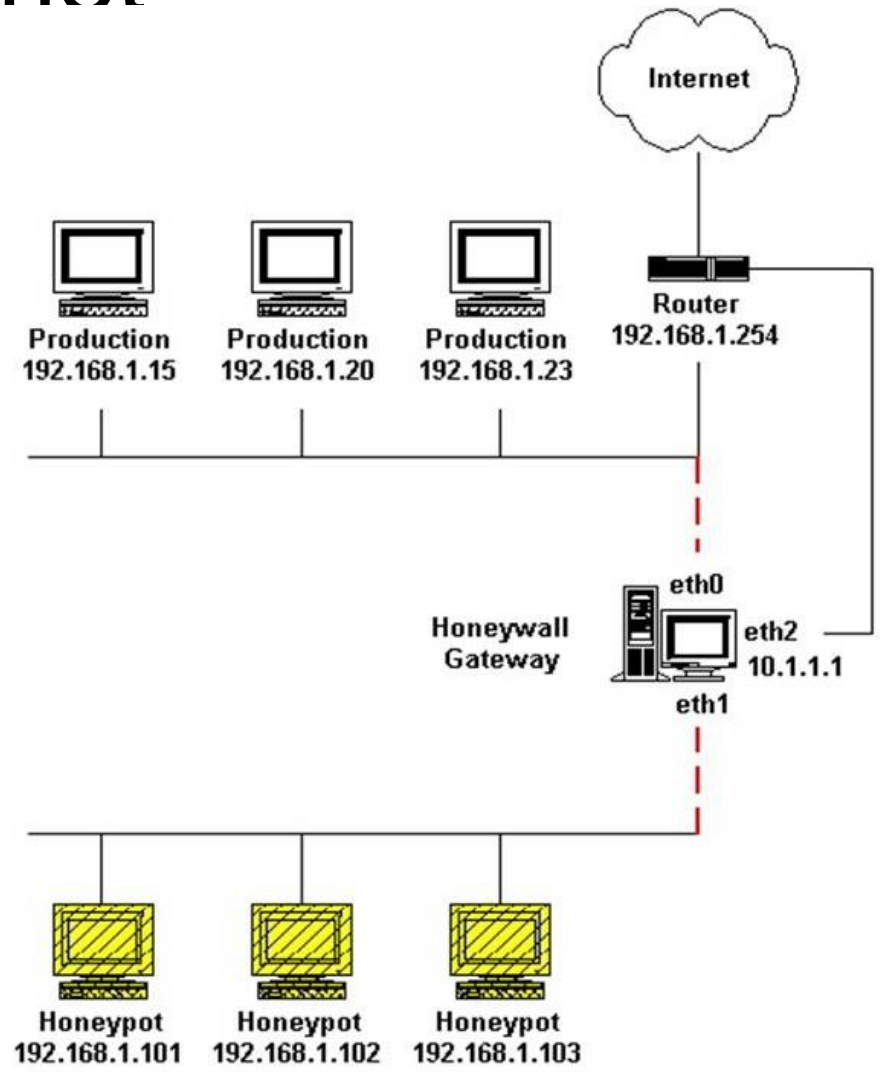
II. Mạng Honeynet

Honeynet thế hệ I:



II. Mạng Honeynet

Honeynet thế hệ II & III:



II. Mạng Honeynet

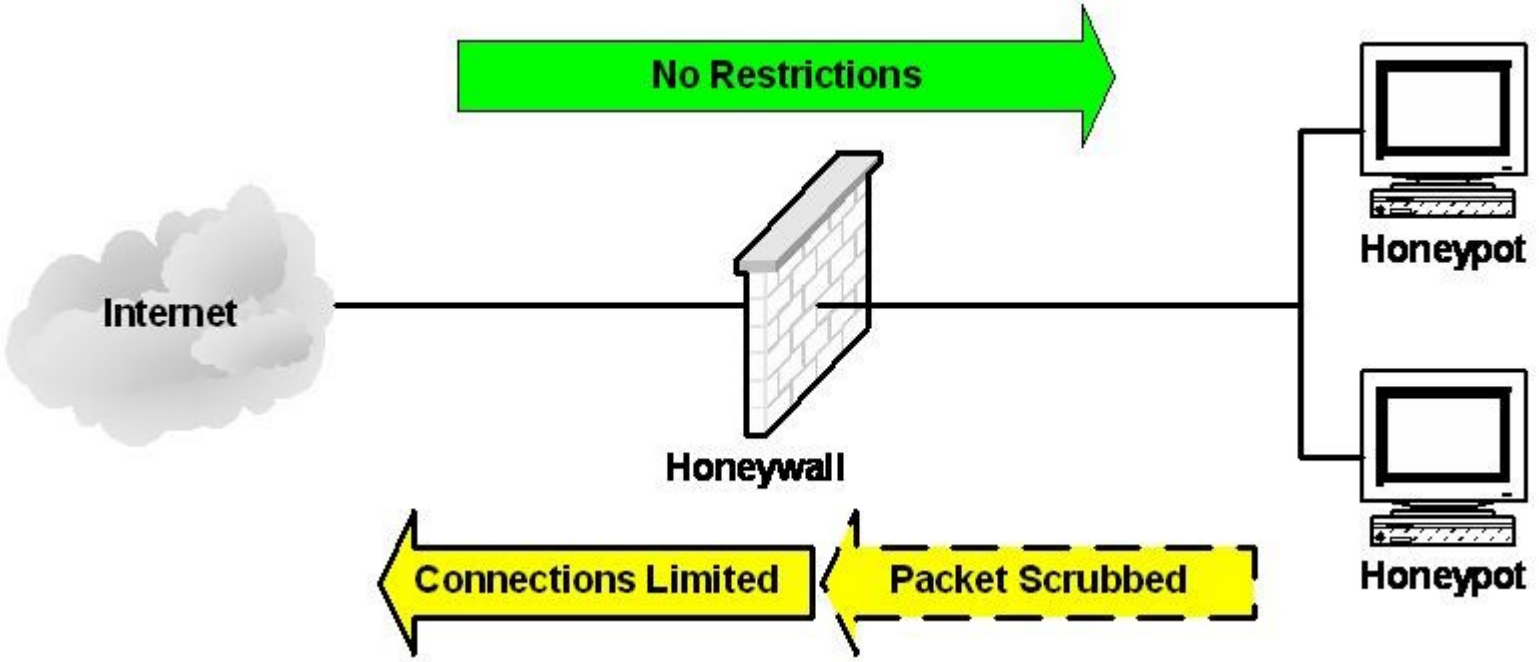
3 chức năng chính:

- Điều khiển dữ liệu
- Thu thập dữ liệu
- Phân tích dữ liệu

II. Mạng Honeynet

Điều khiển dữ liệu:

- Nhằm ngăn chặn tin tặc sử dụng Honeynet để làm bàn đạp tấn công hệ thống mạng bên ngoài.



II. Mạng Honeynet

Thu thập dữ liệu:

- Thu thập dữ liệu là việc giám sát và ghi lại tất cả hoạt động của các thành phần trong hệ thống Honeynet.
- Honeynet định nghĩa ba lớp quan trọng của chức năng thu thập dữ liệu gồm:
  - Nhật ký của tường lửa
  - Lưu lượng của mạng
  - Các hoạt động của hệ thống

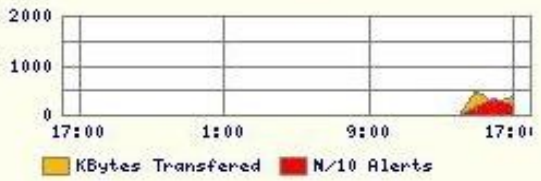
Giao diện phân tích dữ liệu:

Online Honeywalls

Honeywall: 991838165

Created: Thu Jun 9 11:33:45 2011 Last Update: Fri Jun 10 17:27:23 2011

	Bidirectional Flows				Total Flows			
	In		Out		In		Out	
	con	ids	con	ids	con	ids	con	ids
1 Hour	1,847	18	21	1	91,979	19	39	19
24 Hour	4,629	34	2,102	41	5,116	35	2,244	41



Honeywall Details for 991838165

Top 10 Honeypots

Flags	Host	Connections	IDS events
	192.168.1.2	133	24
	192.168.1.190	2,098	6
	192.168.1.1	10	6
	192.168.1.124	6	3
	192.168.1.192	2	2
	192.168.1.150	7	0
	192.168.1.100	2	0
	192.168.1.136	1	0

Top 10 Remote Hosts

Host	Connections	IDS events
10.2.2.2	5,127	34
10.2.2.3	2	1
192.168.63.1	1	0

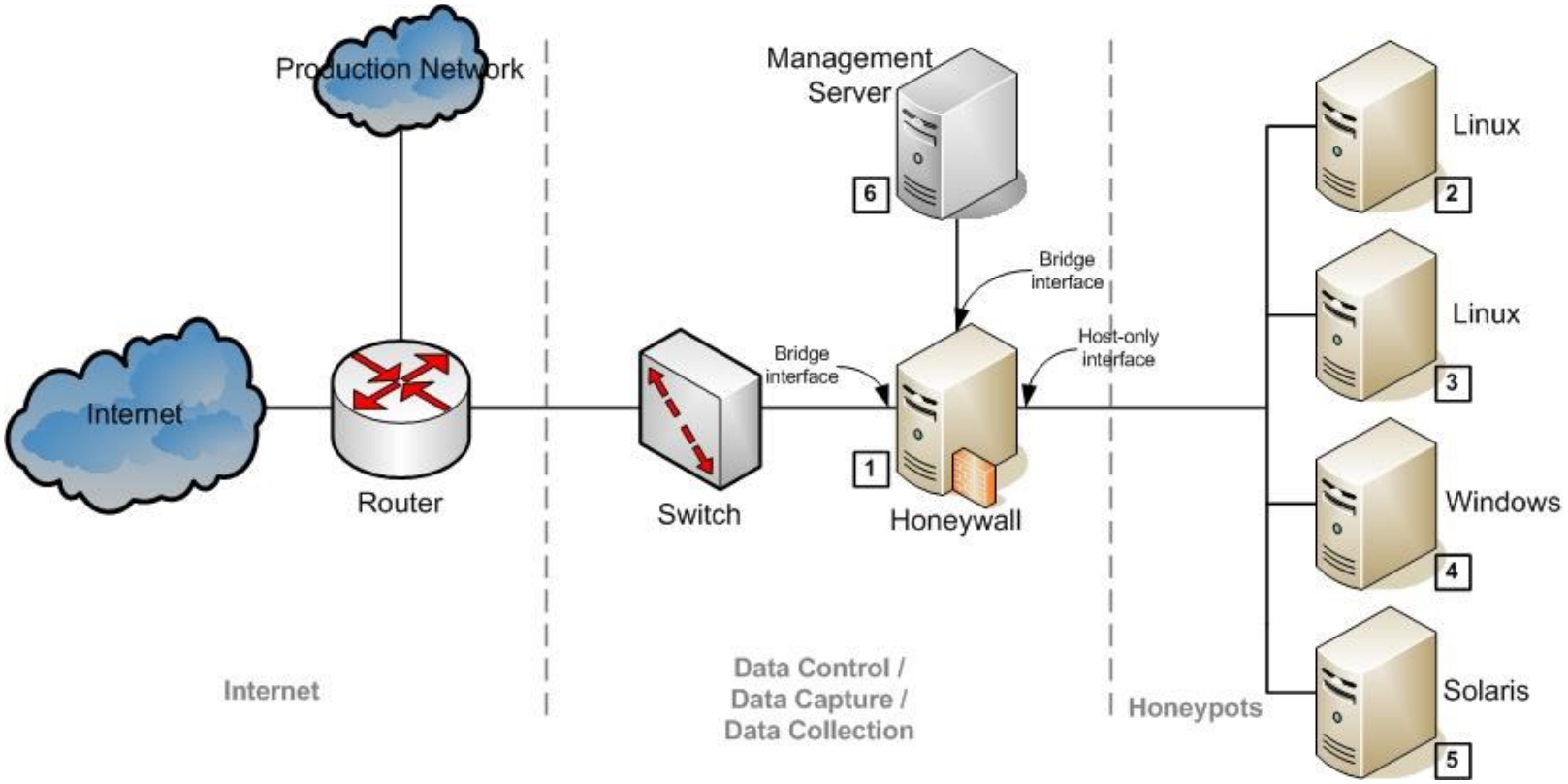
Top 10 Source Ports

Port	Connections	IDS events
8	48	27
1032	7	6
1033	5	5
1030	5	5
1034	4	4
1031	4	4
61082	1,001	2

Top 10 Destination Ports

Port	Connections	IDS events
0	54	27
139	34	22
705	8	8
161	8	7
445	16	6
4444	12	5
3389	12	1

II.1. Kiến trúc hệ thống

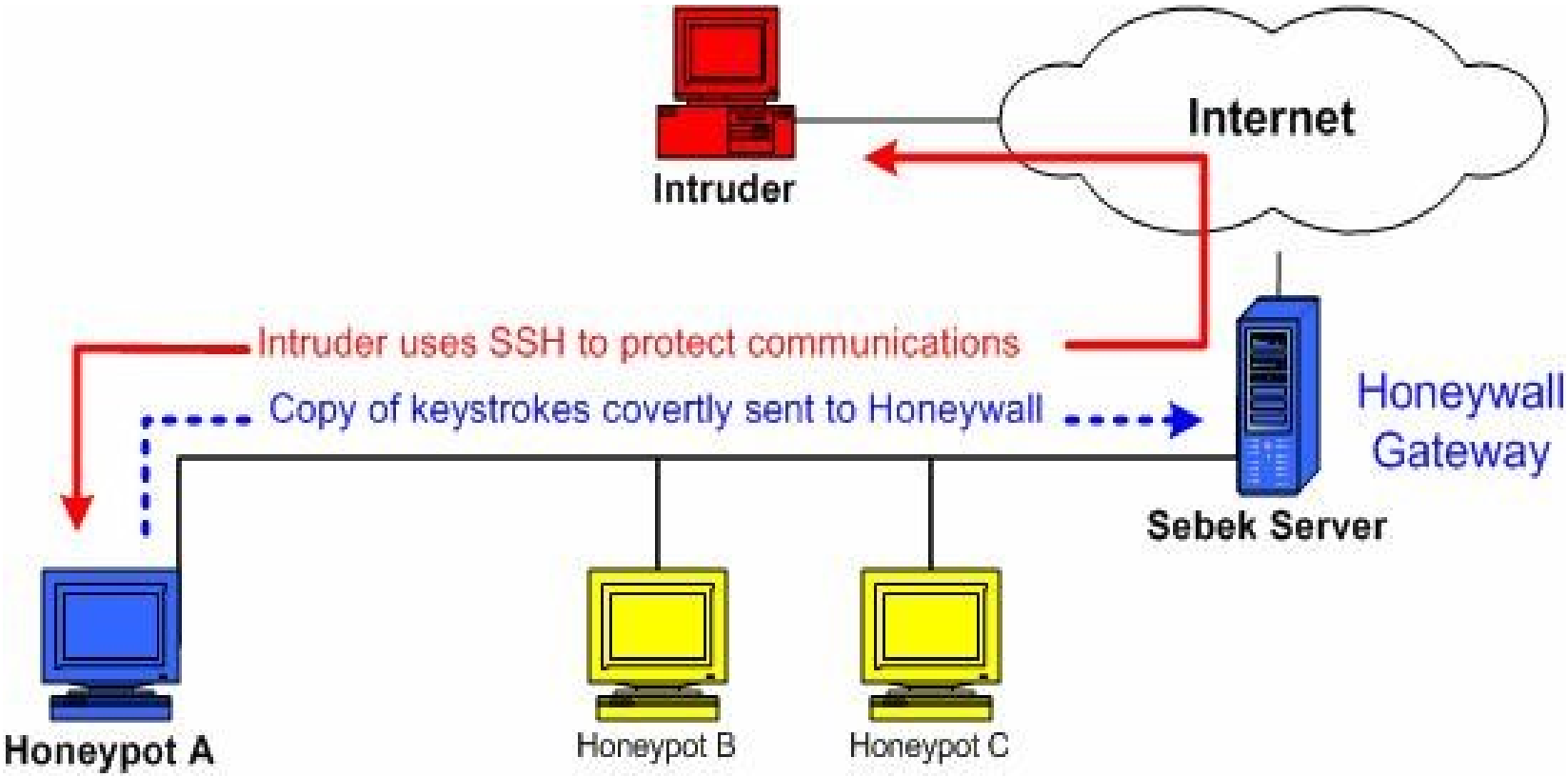


II.1. Kiến trúc hệ thống

- **Honeywall**
  - Iptables
  - Snort (IDS)
  - Sebek Server
  - Cơ sở dữ liệu: MySQL

II.1. Kiến trúc hệ thống

- Công cụ thu thập thông tin Sebek

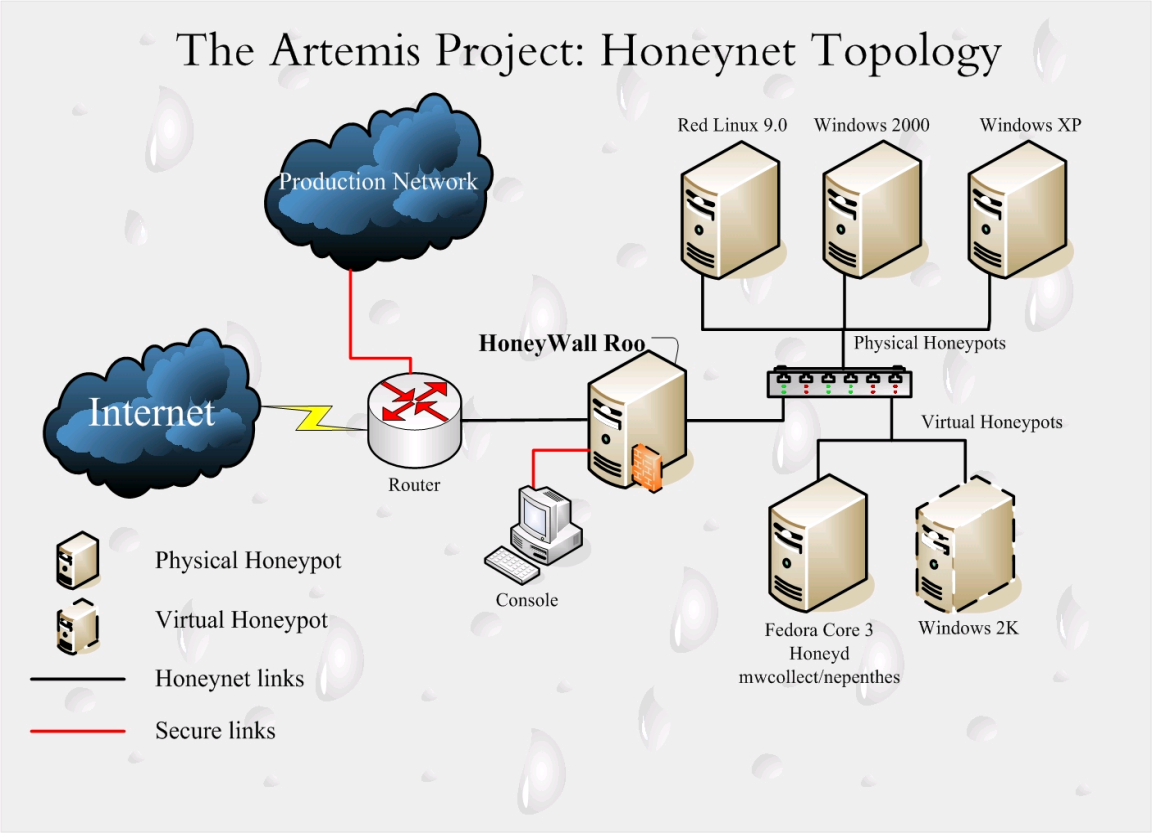


II.1. Kiến trúc hệ thống

- **Honeypots:**
  - Honeypot Windows:
    - Là hệ điều hành phổ biến nhất thế giới, Tồn tại nhiều lỗ hổng và việc khắc phục lỗ hổng lâu.
  - Honeypot Unix-Linux:
    - Là hệ điều hành mã nguồn mở, miễn phí sử dụng. Thích hợp với máy chủ úng dụng mạng do tính ổn định, hiệu năng cao.
- **Cơ sở dữ liệu MySQL:**
  - Lư trữ dữ liệu thu thập được từ Honeypots.

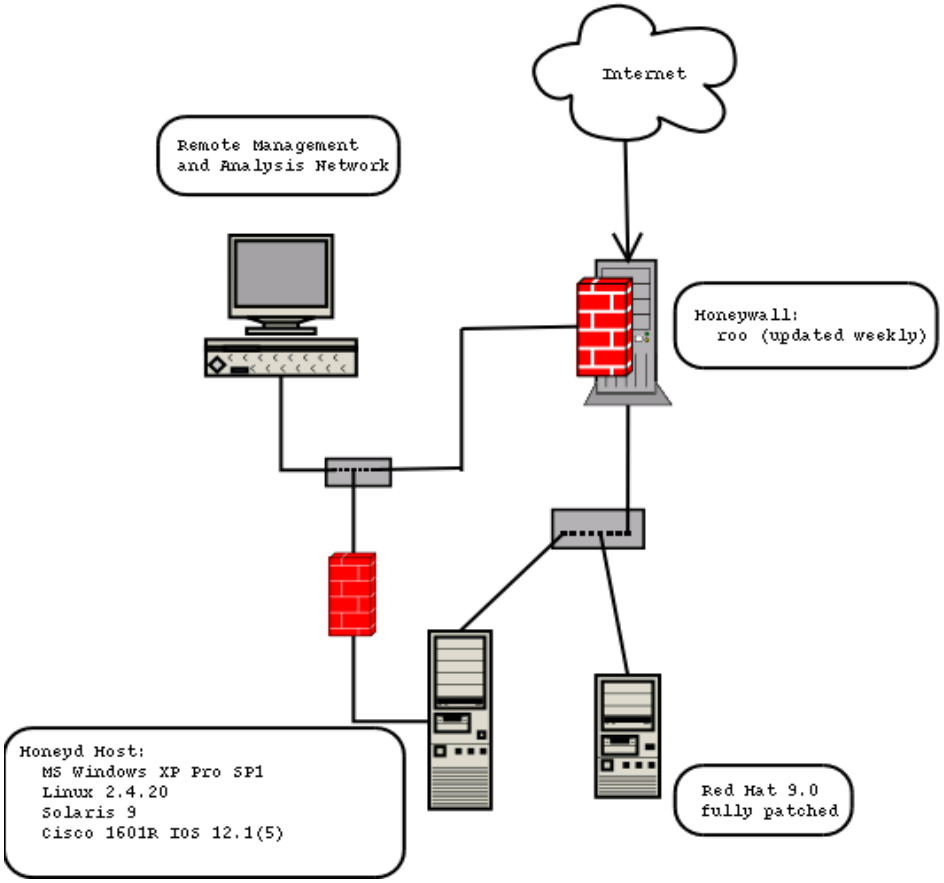
II.2. Một số dự án

- Dự án Honeynet của Bắc Kinh, Trung Quốc:



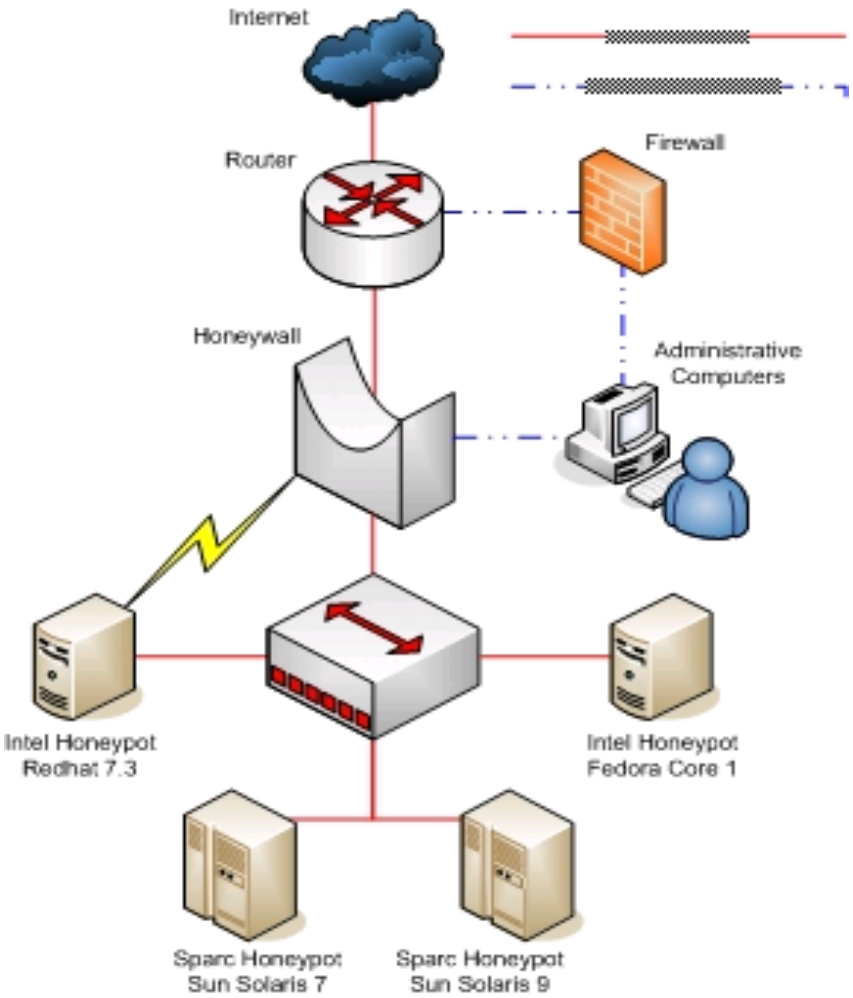
II.2. Một số dự án

- Dự án Honeynet của Hy Lạp:

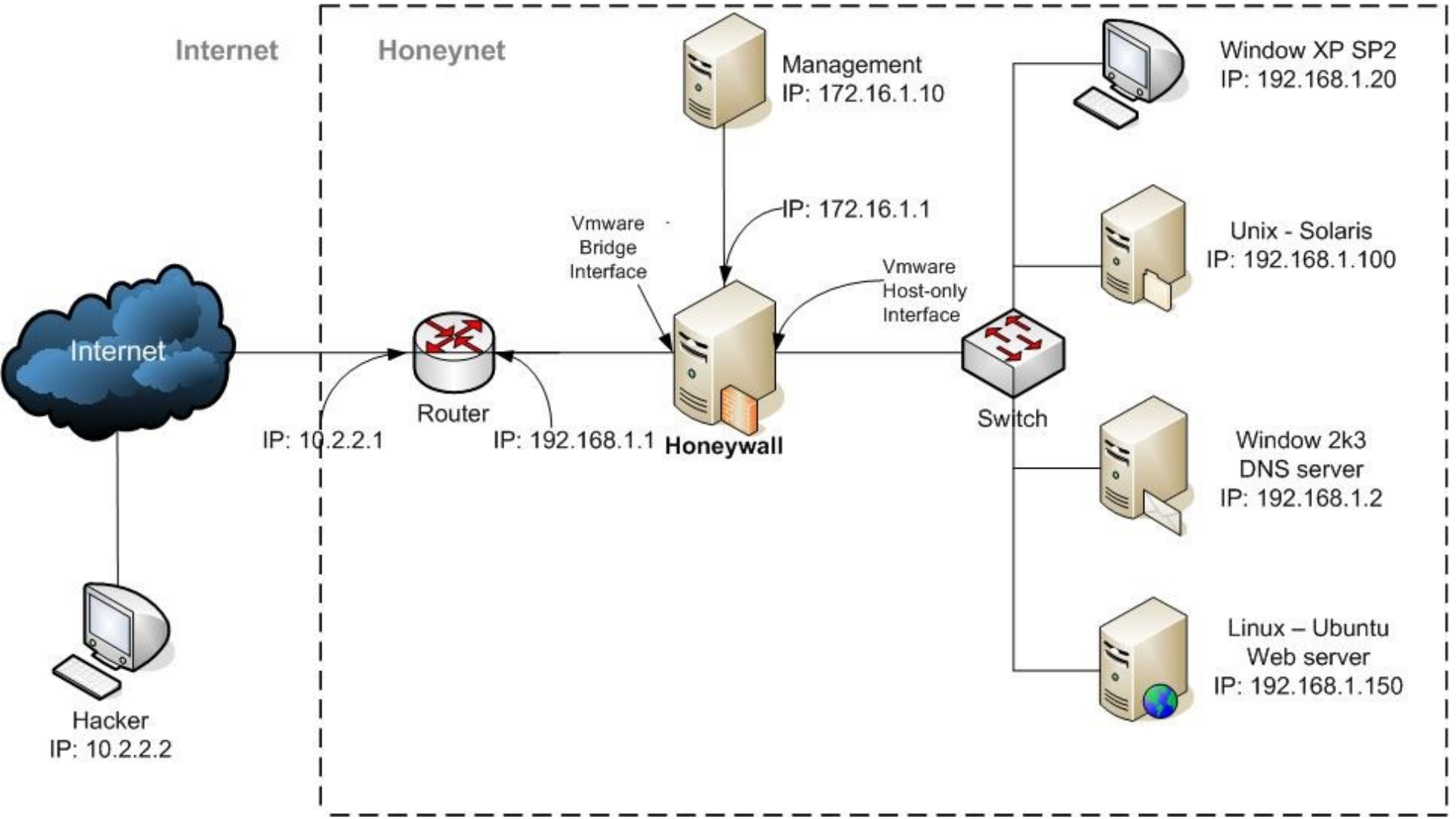


II.2. Một số dự án

- Dự án Honeynet của Anh:



II.3. Mạng Honeynet thử nghiệm



II.3. Mạng Honeynet thử nghiệm

- Thực hiện tấn công vào Honeynet
  - Quét thăm dò dịch vụ và lỗ hổng.
  - Khai thác lỗ hổng MS08_067 (cổng 445) trong Honeypot DNS.
  - Tạo tài khoản mới và thêm vào nhóm quản trị Administrators.

II.3. Mạng Honeynet thử nghiệm

- Phân tích cách thức thực hiện của tin tặc.

```
06/22-01:37:23.920086 0:C:29:22:71:A4 -> 0:C:29:60:46:6A type:0x800 len:0x4E
10.2.2.2:37166 -> 192.168.1.2:53 UDP TTL:63 TOS:0x0 ID:0 IpLen:20 DgmLen:64 DF
Len: 36
37 82 01 00 00 01 00 00 00 00 00 00 03 77 77 77  7............www
0A 68 6F 6E 65 79 6E 65 74 33 61 03 6E 65 74 00  .honeynet3a.net.
00 01 00 01                                      ....
```

- Phân tích một gói tin của Snort ta biết được:
  - Thời gian truy vấn.
  - Địa chỉ và cổng nguồn, địa chỉ và cổng đích.
  - Giao thức sử dụng: UDP
  - Dịch vụ: DNS
- Tin tặc đang truy vấn DNS với tên miền: www.honeynet3a.net

II.3. Mạng Honeynet thử nghiệm

- Phân tích các gói tin tiếp theo.

```
06/22-01:45:20.121420 0:C:29:60:46:6A -> 0:C:29:22:71:A4 type:0x800 len:0x3C
192.168.1.2:1039 -> 10.2.2.2:4444 TCP TTL:128 TOS:0x0 ID:1398 IpLen:20 DgmLen:46 DF
***AP*** Seq: 0x8E34FC35  Ack: 0x7039BA31  Win: 0xF9F7  TcpLen: 20
0D 0A 43 3A 5C 3E                                 ..C:\>

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

06/22-01:45:36.571189 0:C:29:22:71:A4 -> 0:C:29:60:46:6A type:0x800 len:0x50
10.2.2.2:4444 -> 192.168.1.2:1039 TCP TTL:63 TOS:0x0 ID:29797 IpLen:20 DgmLen:66 DF
***AP*** Seq: 0x7039BA31  Ack: 0x8E34FC3B  Win: 0x16D0  TcpLen: 20
6E 65 74 20 75 73 65 72 20 63 61 6F 74 75 61 6E  net user caotuan
20 31 32 33 20 2F 61 64 64 0A                     123 /add.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

06/22-01:46:11.164748 0:C:29:22:71:A4 -> 0:C:29:60:46:6A type:0x800 len:0x61
10.2.2.2:4444 -> 192.168.1.2:1039 TCP TTL:63 TOS:0x0 ID:29802 IpLen:20 DgmLen:83 DF
***AP*** Seq: 0x7039BA4B  Ack: 0x8E34FC82  Win: 0x16D0  TcpLen: 20
6E 65 74 20 6C 6F 63 61 6C 67 72 6F 75 70 20 61  net localgroup a
64 6D 69 6E 69 73 74 72 61 74 6F 72 73 20 63 61  dministrators ca
6F 74 75 61 6E 20 2F 61 64 64 0A                  otuan /add.
```

⇨ Tin tặc thực hiện leo thang đặc quyền.

II.3. Mạng Honeynet thử nghiệm

- Giải pháp
  - Đóng các cổng 445 khi máy chủ kết nối với Internet.
  - Thường xuyên cập nhật bản vá cho hệ điều hành.
  - Xây dựng thiết bị tường lửa và hệ thống phát hiện xâm nhập kiểm soát luồng dữ liệu vào ra của mạng.