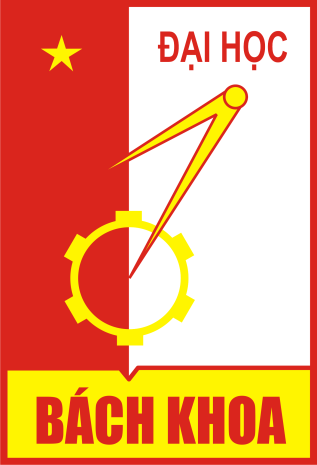


**ĐẠI HỌC BÁCH KHOA HÀ NỘI**

VIỆN CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG

-----🙞🙜🕮🙞🙜-----

****

**BÀI TẬP LỚN**

Môn học: Nhập môn an toàn thông tin

**ĐỀ TÀI**

**ĐIỆN TOÁN ĐÁM MÂY VÀ BẢO MẬT ĐIỆN TOÁN ĐÁM MÂY**

*Giảng viên hướng dẫn:* **PGS.TS. Nguyễn Linh Giang**

*Nhóm sinh viên thực hiện:* ***Nhóm 18***

|  |  |
| --- | --- |
| **Họ và tên** | **MSSV** |
| Nguyễn Ngọc Thọ | 20173387 |
| Nguyễn Hải Dương | 20173059 |
| Hoàng Đình Tuấn | 20173446 |
| Nguyễn Thị Như Hảo | 20173099 |

*Hà Nội, 06/2020*

MỤC LỤC

[Phần 1. Cloud computing 1](#_Toc42514993)

[1.1. Mô hình dịch vụ điện toán đám mây 1](#_Toc42514994)

[1.2. Mô hình triển khai điện toán đám mây 2](#_Toc42514995)

[Phần 2. Tấn công DoS 3](#_Toc42514996)

[2.1. Nhận diện 4](#_Toc42514997)

[2.2. Các phương thức tấn công 5](#_Toc42514998)

[Phần 3. Phát hiện tấn công Dos bằng ma trận hiệp phương sai 5](#_Toc42514999)

[3.1 Ma trận hiệp phương sai (Covariance Matrix) 5](#_Toc42515000)

[3.1.1. Hiệp phương sai 5](#_Toc42515001)

[3.1.2. Ma trân hiệp phương sai 6](#_Toc42515002)

[3.2 Thuật toán phát hiện tấn công 6](#_Toc42515003)

[3.2.1. Thuật toán với ma trận hiệp phương sai 6](#_Toc42515004)

[3.2.2. Mô hình kiến trúc tích hợp trên môi trường đám mây 7](#_Toc42515005)

[3.3. Thí nghiệm và phân tích 8](#_Toc42515006)

[3.3.1. Phương pháp thí nghiệm 1: 8](#_Toc42515007)

[3.3.2. Phương pháp thí nghiệm 2 9](#_Toc42515008)

[3.3.3. Thí nghiệm “Testbed” 9](#_Toc42515009)

# Phần 1. Cloud computing

## Mô hình dịch vụ điện toán đám mây

**Điện toán đám mây** (*cloud computing*), còn gọi là **điện toán máy chủ ảo**, là mô hình điện toán sử dụng các công nghệ máy tính và phát triển dựa vào mạng internet. Thuật ngữ "đám mây" ở đây là lối nói ẩn dụ chỉ mạng internet (dựa vào cách được bố trí của nó trong sơ đồ mạng máy tính) và như sự liên tưởng về độ phức tạp của các cơ sở hạ tầng chứa trong nó. Ở mô hình điện toán này, mọi khả năng liên quan đến công nghệ thông tin đều được cung cấp dưới dạng các "dịch vụ", cho phép người sử dụng truy cập các dịch vụ công nghệ từ một nhà cung cấp nào đó "trong đám mây" mà không cần phải có các kiến thức, kinh nghiệm về công nghệ đó, cũng như không cần quan tâm đến các cơ sở hạ tầng phục vụ công nghệ đó. Theo tổ chức IEEE "*Nó là hình mẫu trong đó thông tin được lưu trữ thường trực tại các máy chủ trên Internet và chỉ được được lưu trữ tạm thời ở các máy khách, bao gồm máy tính cá nhân, trung tâm giải trí, máy tính trong doanh nghiệp, các phương tiện máy tính cầm tay,...*". Điện toán đám mây là khái niệm tổng thể bao gồm cả các khái niệm như phần mềm dịch vụ, Web 2.0 và các vấn đề khác xuất hiện gần đây, các xu hướng công nghệ nổi bật, trong đó đề tài chủ yếu của nó là vấn đề dựa vào Internet để đáp ứng những nhu cầu điện toán của người dùng. Ví dụ, dịch vụ Google Appengine cung cấp những ứng dụng kinh doanh trực tuyến thông thường, có thể truy nhập từ một trình duyệt web, còn các phần mềm và dữ liệu đều được lưu trữ trên các máy chủ.

Mô hình điện toán đám mây cung cấp nhiều dịch vụ bằng cách chia sẻ cơ sở hạ tầng ( Infrastructure as a Service – IaaS – Cơ sở hạ tầng dưới dạng dịch vụ) hoặc chia sẻ nền tảng (Platform as a Service – PaaS – Nền tảng dưới dạng dịch vụ) hoặc trong các ứng dụng (Software as a Service – SaaS – Phần mềm dưới dạng dịch vụ). Sử dụng công nghệ này có thể giảm chi phí và nỗ lực cần thiết để được sử dụng dịch vụ cũng như giảm yêu cầu quản lý các tài nguyên điện toán này tại địa phương.

Trong (IaaS), các nhà cung cấp đám mây cung cấp tính toán tài nguyên vật lý như một dịch vụ như bộ xử lý và bộ nhớ và thiết bị lưu trữ và mạng. Trong mô hình này, người dùng cuối có thể cài đặt hệ điều hành và ứng dụng của họ trên cơ sở hạ tầng đám mây theo nhu cầu của họ, và họ có tất cả sự cho phép để quản lý các máy ảo của họ. Nhà cung cấp IaaS chính là Amazon và Google và các công ty khác. Ngoài các tài nguyên điện toán vật lý được cung cấp bởi nhà cung cấp cơ sở hạ tầng đám mây, mô hình PaaS cũng tạo điều kiện cho quá trình phát triển ứng dụng bằng cách cung cấp nền tảng phát triển ứng dụng cần có để phát triển và chạy ứng dụng. Do đó không còn cần thiết phải sở hữu cơ sở hạ tầng máy tính tại địa phương. Hơn nữa, mô hình SaaS là ​​mô hình phần mềm nơi tập hợp các phần mềm ứng dụng có sẵn cho người dùng cuối trong môi trường đám mây hoặc bằng điện thoại thông minh và trong các phương tiện trao đổi dữ liệu khác.

## Mô hình triển khai điện toán đám mây

Triển khai các dịch vụ điện toán đám mây có thể cục bộ bên trong tổ chức được gọi là đám mây riêng hoặc có thể được sở hữu và quản lý bởi các bên thứ ba (đám mây công cộng). Các tổ chức có thể chia sẻ tài nguyên điện toán của họ với nhau (Đám mây cộng đồng) hoặc dịch vụ đám mây một hỗn hợp của các mô hình trên (Đám mây lai).

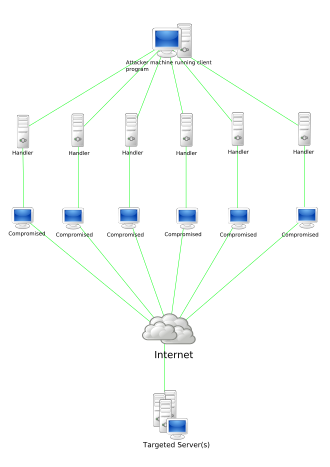
Trong điện toán đám mây riêng, một tổ chức sở hữu cơ sở hạ tầng đám mây và vận hành nó bởi chính nó hoặc bởi bên thứ ba. Cơ sở hạ tầng đám mây có thể được lưu trữ bên trong tiền đề của tổ chức hoặc bên ngoài. Bằng cách sử dụng điện toán đám mây riêng, tổ chức có thể có một đám mây an toàn hơn đám mây công cộng.

Trong khi ở đám mây công cộng, tất cả các tài nguyên điện toán đám mây đều có sẵn cho người dùng cuối thông qua internet. Quyền sở hữu cơ sở hạ tầng đám mây không thuộc về tổ chức mà thuộc về các nhà cung cấp công cộng như Google, Microsoft Azure và Amazon AWS.

Trong mô hình Community Cloud, Một số tổ chức có thể chia sẻ tài nguyên máy tính của họ. Loại mô hình đám mây này có thể được lưu trữ và quản lý cục bộ hoặc trong trang web của bên thứ ba. Trong khi trong đám mây lai, nhiều mô hình triển khai đám mây có thể được sử dụng cùng một lúc (công khai, cộng đồng hoặc riêng tư). Mô hình này có thể hỗ trợ tổ chức công nghệ thông tin để đạt được các dịch vụ đám mây đầy đủ của họ.

# Phần 2. Tấn công DoS

Khi sự tiến bộ của các công nghệ dựa trên Internet và điện toán đám mây đặc biệt, một số thách thức và mối đe dọa đã được xác định, đặc biệt là trong các quan điểm bảo mật. Một trong những mối đe dọa này có liên quan đến sự ổn định của Internet là tấn công từ chối dịch vụ (DoS). Đây là một trong những cuộc tấn công nghiêm trọng nhất. Đây là kiểu tấn công thường xuyên xảy ra trên internet. Kẻ tấn công DoS sử dụng các nút bị xâm nhập trong mạng để nhắm mục tiêu nút nạn nhân được xác định trước bởi một lượng lớn tin nhắn đến, khiến nạn nhân không phản hồi hoặc không hoạt động. Do công nghệ đám mây vẫn đang ở giai đoạn ban đầu và cũng được đặc trưng bởi các tính năng có thể mở rộng và chia sẻ nhiều, DoS có thể gây hại cho mạng dựa trên đám mây hơn so với mạng không phải đám mây. Các nghiên cứu đa dạng đã giải quyết những thách thức này ở các khía cạnh khác nhau.



*Hình 1. Biểu đồ mô tả công cụ DDoS Stachledraht*

Một cuộc tấn công từ chối dịch vụ (*tấn công DoS - viết tắt của Denial of Service*) hay tấn công từ chối dịch vụ phân tán (tấn công DDoS - viết tắt của Distributed Denial of Service) là một nỗ lực làm cho những người dùng không thể sử dụng tài nguyên của một máy tính. Mặc dù phương tiện để tiến hành, động cơ, mục tiêu của tấn công từ chối dịch vụ có thể khác nhau, nhưng nói chung nó gồm có sự phối hợp, sự cố gắng ác ý của một người hay nhiều người để một trang, hay hệ thống mạng không thể sử dụng, làm gián đoạn, 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. Thủ phạm tấn công từ chối dịch vụ thường nhắm vào các trang mạng hay server tiêu biểu như ngân hàng, cổng thanh toán thẻ tín dụng và thậm chí DNS root servers.

Một phương thức tấn công phổ biến kéo theo sự bão hoà máy mục tiêu với các yêu cầu liên lạc bên ngoài, đến mức nó không thể đáp ứng giao thông hợp pháp, hoặc đáp ứng quá chậm. Trong điều kiện chung, các cuộc tấn công DoS được bổ sung bởi ép máy mục tiêu khởi động lại hoặc tiêu thụ hết tài nguyên của nó đến mức nó không cung cấp dịch vụ, hoặc làm tắc nghẽn liên lạc giữa người sử dụng và nạn nhân.

Tấn công từ chối dịch vụ là sự vi phạm chính sách sử dụng internet của IAB (Internet Architecture Board) và những người tấn công hiển nhiên vi phạm luật dân sự.

## 2.1. Nhận diện

US-CERT xác định dấu hiệu của một vụ tấn cống từ chối dịch vụ gồm có:

* Mạng thực thi chậm khác thường khi mở tập tin hay truy cập Website;
* Không thể dùng một website cụ thể;
* Không thể truy cập bất kỳ website nào;
* Tăng lượng thư rác nhận được.

Không phải tất các dịch vụ đều ngừng chạy, thậm chí đó là kết quả của một hoạt động nguy hại, tất yếu của tấn công DoS. Tấn công từ chối dịch cũng có thể dẫn tới vấn đề về nhánh mạng của máy đang bị tấn công. Ví dụ băng thông của router giữa Internet và LAN có thể bị tiêu thụ bởi tấn công, làm tổn hại không chỉ máy tính ý định tấn công mà còn là toàn thể mạng.

## 2.2. Các phương thức tấn công

Tấn công từ chối dịch vụ là một loại hình tấn công nhằm ngăn chặn những người dùng hợp lệ được sử dụng một dịch vụ nào đó. Các cuộc tấn công có thể được thực hiện nhằm vào bất kì một thiết bị mạng nào bao gồm là tấn công vào các thiết bị định tuyến, web, thư điện tử và hệ thống DNS,...

Tấn công từ chối dịch vụ có thể được thực hiện theo một số cách nhất định. Có năm kiểu tấn công cơ bản sau đây:

* Nhằm tiêu tốn tài nguyên tính toán như băng thông, dung lượng đĩa cứng hoặc thời gian xử lý
* Phá vỡ các thông tin cấu hình như thông tin định tuyến
* Phá vỡ các trạng thái thông tin như việc tự động reset lại các phiên TCP.
* Phá vỡ các thành phần vật lý của mạng máy tính
* Làm tắc nghẽn thông tin liên lạc có chủ đích giữa các người dùng và nạn nhân dẫn đến việc liên lạc giữa hai bên không được thông suốt.

Một cuộc tấn công từ chối dịch vụ có thể bao gồm cả việc thực thi malware nhằm:

* Làm quá tải năng lực xử lý, dẫn đến hệ thống không thể thực thi bất kì một công việc nào khác.
* Những lỗi gọi tức thì trong microcode của máy tính.
* Những lỗi gọi tức thì trong chuỗi chỉ thị, dẫn đến máy tính rơi vào trạng thái hoạt động không ổn định hoặc bị đơ.
* Những lỗi có thể khai thác được ở hệ điều hành dẫn đến việc thiếu thốn tài nguyên hoặc bị thrashing. VD: như sử dụng tất cả các năng lực có sẵn dẫn đến không một công việc thực tế nào có thể hoàn thành được.
* Gây crash hệ thống.
* Tấn công từ chối dịch vụ iFrame: trong một trang HTML có thể gọi đến một trang web nào đó với rất nhiều yêu cầu và trong rất nhiều lần cho đến khi băng thông của trang web đó bị quá hạn.

# Phần 3. Phát hiện tấn công Dos bằng ma trận hiệp phương sai

## 3.1 Ma trận hiệp phương sai (Covariance Matrix)

### 3.1.1. Hiệp phương sai

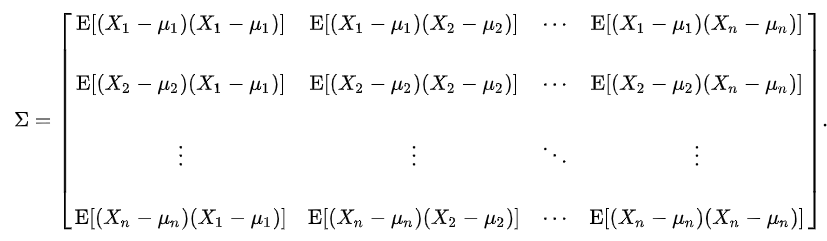
**Hiệp phương sai** là độ đo sự biến thiên cùng nhau của hai biến ngẫu nhiên được tính bằng công thức:



Nếu hai biến có xu hướng thay đổi cùng nhau (nghĩa là, khi một biến có giá trị cao hơn giá trị kỳ vọng thì biến kia có xu hướng cũng cao hơn giá trị kỳ vọng), thì hiệp phương sai giữa hai biến này có giá trị dương. Mặt khác, nếu một biến nằm trên giá trị kỳ vọng còn biến kia có xu hướng nằm dưới giá trị kỳ vọng, thì hiệp phương sai của hai biến này có giá trị âm.

### 3.1.2. Ma trân hiệp phương sai

Ma trận hiệp phương sai của tập hợp m biến ngẫu nhiên là một ma trận vuông (m × m), trong đó các phần tử nằm trên đường chéo (từ trái sang phải, từ trên xuống dưới) lần lượt là phương sai tương ứng của các biến này trong khi các phần tử còn lại (không nằm trên đường chéo) là các hiệp phương sai của đôi một hai biến ngẫu nhiên khác nhau trong tập hợp.



Trong đó : 

## 3.2 Thuật toán phát hiện tấn công

### 3.2.1. Thuật toán với ma trận hiệp phương sai

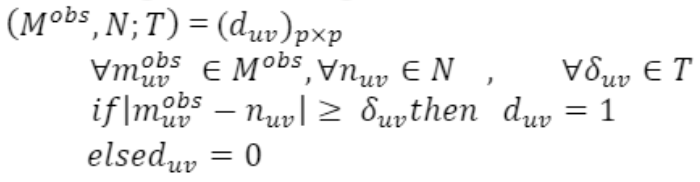
Các gói tấn công bất thường là luôn được tích lỹ nhanh chóng cho một nạn nhân đơn lẻ gây cạn kiệt các nguồn tài nguyên. Các thuộc tính thống kê trong khoảng thời gian đó sẽ phản ánh các đặc tính về lưu lượng của cuộc tấn công sẽ khác với lưu lượng bình thường. Do đó, chúng ta có thể sử dụng các thuộc tính thống kê của các mẫu theo trình tự thời gian để phát hiện tấn công lũ lụt. Để thể hiện tính tương quan, chúng ta sử dụng ma trận hiệp phương sai mô hình các chuỗi mẫu có độ dài bằng nhau cố định. Mỗi phần tử trong ma trận hiệp phương sai mô tả mối tương quan giữa hai tính chất quan sát được tương ứng.

Trong phương pháp ma trận hiệp phương sai, phương thức thống kê sẽ được sử dụng trong phân tích hành vi lưu lượng mạng. Các đặc trưng được lựa chọn như cờ TCP FIN, RST, FIN và TCP retires flag. Thuật toán bắt đầu với một bản ghi lưu lượng mạng như một đầu vào. Sau khi xử lý, đầu ra của thuật toán là xác định xem có cuộc tấn công DoS xảy ra không thoe các giá trị của ma trận nhị phân. Khi tất cả các giá trị bên trong dãy nhị phân là số 0 thì không có cuộc tấn công nào xả ra, ngược lại các cuộc tấn công được phát hiện theo các bước:

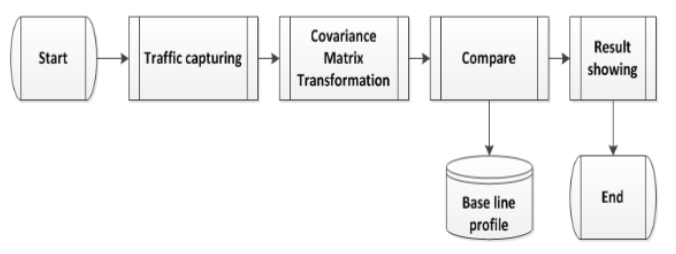
- Bản ghi các đặc trưng mạng như là các biến ngẫu nhiên

- Thuật toán sẽ tính ma trận hiệp phương sai Mobs của tập các biến ngẫu nhiên

- Sau đó, ma trận nhị phân được xác định theo công thức:



Trong đó, v – u là tọa độ trong ma trận hiệp phương sai, T là giá trị trong ma trận ngưỡng.



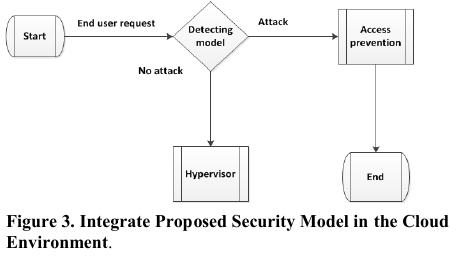
Hình 2. Thuật toán phát hiện tấn công lũ lụt bằng ma trận hiệp phương sai

### 3.2.2. Mô hình kiến trúc tích hợp trên môi trường đám mây

Mô hình phát hiện được đề xuất gồm 2 giai đoạn. Đầu tiên là giai đoạn đào tạo, tập trung vào việc xây dựng một hồ sơ của một hành vi lưu lượng bình thường (hồ sơ cơ sở). Nó có thể được thực hiện bằng cách bắt lưu lượng mạng truy cập bình thường và chuyển nó thành ma trận hiệp phương sai.

Bươc thứ 2, ma trận hiệp phương sai ở bước một được so sánh với một ma trận hiệp phương sai mới của một bản ghi lưu lượng mạng mới mà có thể là bình thường hoặc khác thường.

Để thực thi được trên môi tường đám mây, mô hình được đưa ra:



Hình 3. Tích hợp mô hình bảo mật trên môi trường đám mây

## 3.3. Thí nghiệm và phân tích

Mục đích của thí nghiệm này là kiểm tra tính hiệu quả của phương pháp ma trận hiệp phương sai để phát hiện flooding based DoS.

Thí nghiệm gồm hai PC được kết nối với cùng một bộ định tuyến. Một trong số họ là nạn nhân và một người là kẻ tấn công.

Nạn nhân sử dụng máy ảo VMware Player chạy Ubuntu 11, IP 192.168.5.129. Kẻ tấn công sử dụng IP 192.168.0.101.

Hyenaetool đã được sử dụng để tạo ra cuộc tấn công. Công cụ mạng AthTekNetWalk đã được sử dụng để giám sát và nắm bắt lưu lượng mạng.

Việc thu thập lưu lượng mạng và tính toán giá trị thống kê cờ IP được thực hiện trong năm phút cho mỗi phút một cách độc lập. Ma trận hiệp phương sai được tính cho tất cả các bước, thực hiện như trong tài liệu ở trên.

### 3.3.1. Phương pháp thí nghiệm 1:

Trong tài liệu nghiên cứu này, phần thực hiện đã được hoàn thành trong hai giai đoạn:

* Giai đoạn đào tạo tập trung vào xây dựng đường cơ sở.
* Giai đoạn thứ hai (giai đoạn thử nghiệm) tập trung vào phần phát hiện tấn công.

Việc thực hiện phụ thuộc vào luồng lưu lượng mạng là ma trận đầu vào và ma trận bất thường làm đầu ra theo các giai đoạn sau:

**Giai đoạn đào tạo:**

* Bắt dòng lưu lượng mạng bình thường.
* Phân đoạn lưu lượng mạng bình thường.
* Tóm tắt lưu lượng mạng bình thường.
* Tính toán ma trận hiệp phương sai dòng lưu lượng mạng thông thường (Xây dựng đường cơ sở).

**Giai đoạn thử nghiệm:**

* Bắt dòng lưu lượng mạng bất thường.
* Phân đoạn lưu lượng mạng bất thường.
* Tóm tắt lưu lượng mạng bất thường.
* Tính toán ma trận hiệp phương sai lưu lượng mạng bất thường.
* Phát hiện dòng lưu lượng mạng bất thường. Nếu ma trận thu được toàn là 0 thì không bị tấn công và ngược lại.

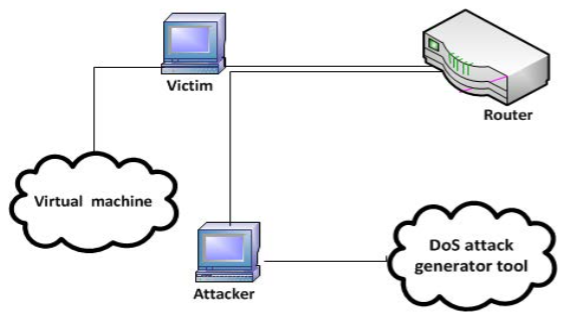
### 3.3.2. Phương pháp thí nghiệm 2

Hai thử nghiệm đầu tiên đang nắm bắt lưu lượng truy cập bình thường ở tốc độ truy cập internet khác nhau và thử nghiệm thứ ba là bắt lưu lượng truy cập bất thường sau khi tạo cuộc tấn công. Sau khi tất cả lưu lượng truy cập bị bắt được chuyển đổi thành ma trận hiệp phương sai tương ứng, 3 ma trận hiệp phương sai được so sánh để phát hiện sự bất thường giữa lưu lượng truy cập bình thường và bất thường. Nhờ đó phát hiện tấn công DoS.

### 3.3.3. Thí nghiệm “Testbed”

Thí nghiệm “testbed” được sử dụng để cài đặt model phát hiện. Nó bao gồm hạ tầng mạng cục bộ kết nối với internet. Mạng nhỏ này gồm 2 PC, 1 trong chúng là nạn nhân, còn lại là kẻ tấn công. Máy tính nạn nhân là máy ảo Ubuntu. Kẻ tấn công dùng kết nối internet để tấn công nạn nhân.

Thí nghiệm bao gồm AthTekNet Walk tool để bắt và lọc lưu lượng. Sử dụng MSExcel để phân tích ma trận. Như trong hình 5.



Hình 4. Mô hình thí nghiệm "Testbed"