MỤC LỤC

LỜI CẢM ƠN

Em xin chân thành cảm ơn Thầy giáo, Tiến sĩ Phùng Văn Ổn – Giám đốc Trung tâm Tin học Văn phòng Chính Phủ, người đã trực tiếp hướng dẫn tận tình chỉ bảo em trong suốt quá trình làm làm tốt nghiệp.

Em xin chân thành cảm ơn tất cả các thầy cô giáo trong Khoa Công nghệ thông tin - Trường Đại học Dân lập Hải Phòng, những người đã nhiệt tình giảng dạy và truyền đạt những kiến thức cần thiết trong suốt thời gian em học tập tại trường, để em hoàn thành tốt đề tài này.

Tuy có nhiều cố gắng trong quá trình học tập cũng như trong thời gian làm tốt nghiệp nhưng không thể tránh khỏi những thiếu sót, em rất mong được sự góp ý quý báu của tất cả các thầy cô giáo cũng như tất cả các bạn để kết quả của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Hải Phòng, tháng 7 năm 2010

Sinh viên

Phạm Đình Hậu

LỜI MỞ ĐẦU

Ngày nay, hệ thống mạng máy tính đã trở nên rất phổ biến trong hầu hết các hoạt động xã hội, tác động trực tiếp đến nền kỹ thuật và kinh tế của cả nước. Cùng với sự phát triển đó, ngày càng xuất hiện nhiều hơn những cá nhân, nhóm hoặc thậm chí là cả những tổ chức hoạt động với những mục đích xấu nhằm phá hoại các hệ thống mạng máy tính, hệ thống thông tin, gây tác hại vô cùng to lớn đến tính an toàn và bảo mật thông tin trên các hệ thống này.

Chính vì vậy vấn đề an ninh trên mạng đang được quan tâm đặc biệt như: vấn đề bảo mật mật khẩu, chống lại sự truy cập bất hợp pháp , chống lại các virus máy tính, … Đó là lý do em chọn đề tài "Nghiên cứu và đề xuất giải pháp ngăn chặn việc truy cập trái phép vào các hệ thống thông tin tin học qua mạng Internet" nhằm phục vụ cho mục đích thực tế.

Mục đích và nhiệm vụ nghiên cứu:

- Các nguy cơ truy cập hệ thống thông tin tin học bất hợp pháp.
- Đề xuất giải pháp kỹ thuật ngăn chặn truy cập hệ thống thông tin tin học bất hợp pháp.

Phạm vi nghiên cứu:

- Hệ thống thông tin và nguy cơ truy cập bất hợp pháp.
- Các kiểu tấn công cơ bản.
- Phương pháp phát hiện xâm nhập.

CHƯƠNG I : HỆ THỐNG THÔNG TIN VÀ NGUY CƠ TRUY CẬP BẤT HỢP PHÁP

I. HỆ THỐNG THÔNG TIN :

Hệ thống thông tin (Tiếng anh là: Information System) là một tập hợp và kết hợp của các phần cứng, phần mềm và các hệ mạng truyền thông được xây dựng và sử dụng để thu thập, tạo, tái tạo, phân phối và chia sẻ các dữ liệu, thông tin và tri thức nhằm phục vụ các mục tiêu của tổ chức.

Các tổ chức có thể sử dụng các hệ thống thông tin với nhiều mục đích khác nhau:

- Với bên trong, hệ thống thông tin phục vụ việc việc quản trị nội bộ, hệ thống thông tin sẽ giúp đạt được sự liên kết và trao đổi thông tin trong nội bộ, thống nhất hành động, duy trì sức mạnh của tổ chức, đạt được lợi thế cạnh tranh.
- Với bên ngoài, hệ thống thông tin giúp nắm bắt được nhiều thông tin về khách hàng hơn hoặc cải tiến dịch vụ, nâng cao sức cạnh tranh, tạo đà cho phát triển.

II. CÁC NGUY CƠ MẤT AN TOÀN :

Một người hay một nhóm người muốn truy cập vào hệ thống thông tin gọi chung là Hacker có thể vì một lý do này hay một lý do khác. Dưới đây là một số lý do có thể:

- Đơn giản là truy cập vào hệ thống thống thông tin đọc và tìm kiếm thông tin.
- Chỉ là tò mò, giải trí hoặc muốn thể hiện khả năng cá nhân.
- Để xem xét chung chung và có thể gửi cảnh báo đến người quản trị hệ thống.
- Để ăn cắp tài nguyên hệ thống thông tin như: các thông tin về tài khoản ngân hàng, bí mật thương mại, bí mật quốc gia hoặc các thông tin độc quyền, ...
- Phát động chiến tranh thông tin trên mạng, làm tê liệt mạng.

Trong mọi trường hợp, bất kể vì lý do gì thì đằng sau vụ tấn công vào hệ thống thông tin thì thông tin mà kẻ phá hoại muốn lấy nhất là thông tin người quản lý hệ thống bao gồm: tên đăng nhập (Tiếng anh là: username) và mật khẩu (Tiếng anh là: password). Tuy nhiên, mật khẩu đều đã được mã hóa, nhưng điều này không có

nghĩa là mật khẩu luôn được an toàn. "Hacker" có thể dùng chương trình Bộ giải mã mật khẩu (Tiếng anh là: Password Cracker) để tìm mật khẩu bằng cách so sánh chúng với các từ trong một từ điển hoặc Brouce Force. Mức độ thành công của chương trình giải mã phụ thuộc vào tài nguyên của CPU, vào chất lượng của từ điển và một vài lý do khác.

1. Các hiểm họa mất an toàn đối với hệ thống thông tin :

Các hiểm hoạ mất an toàn đối với một hệ thống thông tin có thể được phân loại thành các hiểm hoạ vô tình hay cố ý; các hiểm hoạ chủ động hay thụ động.

Hiểm họa vô tình (Tiếng anh là: Unintentional Threat): Khi người sử dụng tắt nguồn của một hệ thống và khi được khởi động lại, hệ thống ở chế độ single - user (đặc quyền) - người sử dụng có thể làm mọi thứ anh ta muốn đối với hệ thống.

Hiểm họa cố ý (Tiếnh anh là : Intentional Threat):Có thể xảy ra đối với dữ liệu trên mạng hoặc máy tính cá nhân thông qua các tấn công tinh vi có sử dụng các kiến thức hệ thống đặc biệt. Ví dụ về các hiểm họa cố ý: cố tình truy nhập hoặc sử dụng mạng trái phép (Tiếng anh là :Intentional Unauthorized use of corporate network*).*

Hiểm hoạ thụ động (Tiếng anh là: Passive Threat): Không phải là kết quả của việc sửa đổi bất kỳ thông tin nào có trong hệ thống, hoặc thay đổi hoạt động hoặc tình trạng của hệ thống.

Hiểm hoạ chủ động (Tiếng anh là: Active Threat): Là việc sửa đổi thông tin (Tiếng anh là: Data Modification) hoặc thay đổi tình trạng hoặc hoạt động của một hệ thống.

Mối đe dọa và hậu quả tiềm ẩn đối với thông tin trong giao dịch điện tử là rất lớn. Nguy cơ rủi ro đối với thông tin trong giao dịch điện tử được thể hiện hoặc tiềm ẩn trên nhiều khía cạnh khác nhau như: người sử dụng, kiến trúc hệ thống công nghệ thông tin, chính sách bảo mật thông tin, các công cụ quản lý và kiểm tra, quy trình phản ứng, v.v.

2. Các yêu cầu cần bảo vệ hệ thống thông tin :

Mục tiêu cuối cùng của quá trình bảo mật thông tin là nhằm bảo vệ ba thuộc tính của thông tin:

- Tính bí mật (Tiếng anh là: Confidental): Thông tin chỉ được xem bởi những người có thẩm quyền. Lý do cần phải giữ bí mật thông tin vì đó là sản phẩm sở hữu

của tổ chức và đôi khi đó là các thông tin của khách hàng của tổ chức. Những thông tin này mặc nhiên phải giữ bí mật hoặc theo những điều khoản giữa tổ chức và khách hàng của tổ chức.

- Tính toàn vẹn (Tiếng anh là: Integrity): Thông tin phải không bị sai hỏng, suy biến hay thay đổi. Thông tin cần phải xử lý để cách ly khỏi các tai nạn hoặc thay đổi có chủ ý.
- Tính sẵn sàng (Tiếng anh là: Availability): Thông tin phải luôn được giữ trong trạng thái sẵn sàng cung cấp cho người có thẩm quyền khi họ cần.

3. Các biện pháp đảm bảo an toàn hệ thống thông tin :

Trong phần này, chúng ta xem xét một số biện pháp bảo mật cho một hệ thống tin học. Cũng cần phải nhấn mạnh rằng, không có biện pháp nào là hoàn hảo, mỗi biện pháp đều có những mặt hạn chế của nó. Biện pháp nào là hiệu quả, cần được áp dụng phải căn cứ vào từng hệ thống để đưa ra cách thực hiện cụ thể.

Thiết lập quy tắc quản lý

Mỗi tổ chức cần có những quy tắc quản lý của riêng mình về bảo mật hệ thống thông tin trong hệ thống. Có thể chia các quy tắc quản lý thành một số phần:

- Quy tắc quản lý đối với hệ thống máy chủ
- Quy tắc quản lý đối với hệ thống máy trạm
- Quy tắc quản lý đối với việc trao đổi thông tin giữa các bộ phận trong hệ thống, giữa hệ thống máy tính và người sử dụng, giữa các thành phần của hệ thống và các tác nhân bên ngoài.

An toàn thiết bị

- Lựa chọn các thiết bị lưu trữ có độ tin cậy cao để đảm bảo an toàn cho dữ liệu. Phân loại dữ liệu theo các mức độ quan trọng khác nhau để có chiến lược mua sắm thiết bị hoặc xây dựng kế hoạch sao lưu dữ liệu hợp lý.
- Sử dụng các hệ thống cung cấp, phân phối và bảo vệ nguồn điện một cách hợp lý.
- Tuân thủ chế độ bảo trì định kỳ đối với các thiết bị.

Thiết lập biện pháp bảo mật.

Cơ chế bảo mật một hệ thống thể hiện qua quy chế bảo mật trong hệ thống, sự phân cấp quyền hạn, chức năng của người sử dụng trong hệ thống đối với dữ liệu và quy trình kiểm soát công tác quản trị hệ thống. Các biện pháp bảo mật bao gồm:

- Bảo mật vật lý đối với hệ thống. Hình thức bảo mật vật lý khá đa dạng, từ khoá cứng, hệ thống báo động cho đến hạn chế sử dụng thiết bị. Ví dụ như loại bỏ đĩa mềm khỏi các máy trạm thông thường là biện pháp được nhiều cơ quan áp dụng.

- Các biện pháp hành chính như nhận dạng nhân sự khi vào văn phòng, đăng nhập hệ thống hoặc cấm cài đặt phần mềm, hay sử dụng các phần mềm không phù hợp với hệ thống.

+ Mật khẩu là một biện pháp phổ biến và khá hiệu quả. Tuy nhiên mật khẩu không phải là biện pháp an toàn tuyệt đối. Mật khẩu vẫn có thể mất cắp sau một thời gian sử dụng.

+ Bảo mật dữ liệu bằng mật mã tức là biến đổi dữ liệu từ dạng nhiều người dễ dàng đọc được, hiểu được sang dạng khó nhận biết.

+ Xây dựng bức tường lửa, tức là tạo một hệ thống bao gồm phần cứng và phần mềm đặt giữa hệ thống và môi trường bên ngoài như Internet chẳng hạn. Thông thường, tường lửa có chức năng ngăn chặn những thâm nhập trái phép (không nằm trong danh mục được phép truy nhập) hoặc lọc bỏ, cho phép gửi hay không gửi các gói tin.

CHƯƠNG II: CÁC KIỂU TẤN CÔNG CƠ BẢN

I. SNIFFERS:

1. Định nghĩa Sniffers:

Sniffers là một chương trình hay thiết bị có khả năng đón bắt lại các thông tin quan trọng từ giao thông mạng chỉ định đến một mạng riêng.

Sniffing là một kỹ thuật chặn dữ liệu.

Đối tượng mà sniffing lấy:

- Mật khẩu (Tiếng anh là: Password) (từ Email, Web, SMB, FTP, SQL hoặc Telnet)
- Các thông tin về các thẻ tín dụng.
- Văn bản của Email.
- Các tập tin đang đi trên mạng (tập tin Email, FTP hoặc SMB)

2. Mục đích sử dụng Sniffers:

Sniffer thường được sử dụng vào 2 mục đích khác biệt nhau.

- Theo hướng tích cực nó có thể là một công cụ giúp cho các quản trị mạng theo dõi và bảo trì hệ thống mạng của mình.
- Theo hướng tiêu cực nó có thể là một chương trình được cài vào một hệ thống mạng máy tính với mục đích chặn dữ liệu, các thông tin trên đoạn mạng này.

Một số tính năng của Sniffer được sử dụng theo cả hướng tích cực và tiêu cực :

- Tự động chụp các tên người sử dụng (Tiếng anh là: Username) và mật khẩu không được mã hoá (Tiếng anh là: Clear Text Password). Tính năng này thường được các Hacker sử dụng để tấn công hệ thống.

- Chuyển đổi dữ liệu trên đường truyền để những quản trị mạng có thể đọc và hiểu được ý nghĩa của những dữ liệu đó.

- Bằng cách nhìn vào lưu lượng của hệ thống cho phép các quản trị mạng có thể phân tích những lỗi đang mắc phải trên hệ thống lưu lượng của mạng. Ví dụ như : Tại sao gói tin từ máy A không thể gửi được sang máy B …

- Một số Sniffer tân tiến còn có thêm tính năng tự động phát hiện và cảnh báo các cuộc tấn công đang được thực hiện vào hệ thống mạng mà nó đang hoạt động

(Intrusion Detecte Service).

- Ghi lại thông tin về các gói dữ liệu, các phiên truyền…Tương tự như hộp đen của máy bay, giúp các quản trị mạng có thể xem lại thông tin về các gói dữ liệu, các phiên truyền sau sự cố…Phục vụ cho công việc phân tích, khắc phục các sự cố trên hệ thống mạng.

3.Các giao thức có thể sử dụng Sniffing:

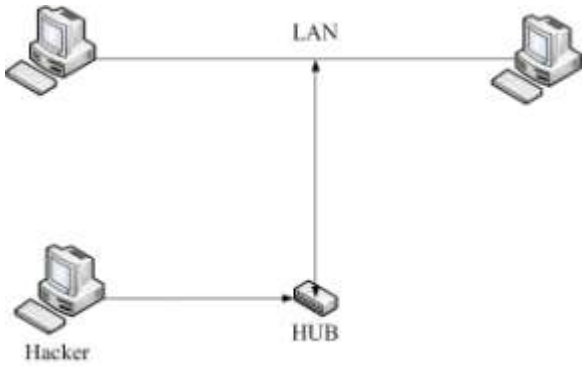
Các Hacker có thể sử dụng Sniffing để tấn công vào các giao thức sau:

- Telnet và Rlogin: Ghi lại các thông tin như: Password, Ussernames.
- HTTP: Các dữ liệu gửi đi mà không mã hóa.
- SMTP, POP, FTP, IMAP: Password và dữ liệu gửi đi không mã hóa.

1. Các loại Sniffing:

1.1 Sniffing thụ động:

Đây là loại Sniffing lấy dữ liệu chủ yếu qua Hub. Nó được gọi là Sniffing thụ động là vì rất khó có thể phát hiện ra loại Sniffing này. Hacker sử dụng máy tính của mình kết nối đến Hub và bắt đầu Sniffing.

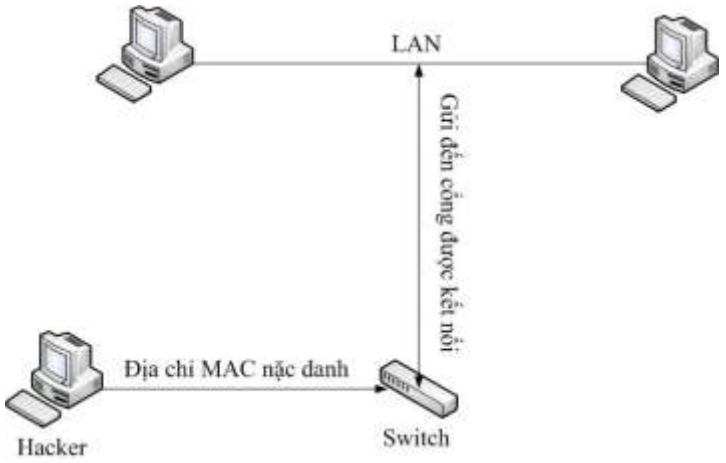


Hình 2.1: Sniffing thụ động.

1.2 Sniffing chủ động:

Đây là loại Sniffing lấy dữ liệu chủ yếu qua Switch, nó rất khó thực hiện và dễ bị phát hiện. Hacker thực hiện loại Sniffing này như sau:

1. Hacker kết nối đến Switch bằng cách gửi địa chỉ MAC nặc danh.
2. Switch xem địa chỉ kết hợp với mỗi khung (Tiếng anh là: Frame).
3. Máy tính trong LAN gửi dữ liệu đến cổng kết nối.



Hình 2.2: Sniffing chủ động.

5. Tìm hiểu về MAC, ARP và một số kiểu tấn công:

5.1 Tìm hiểu MAC, ARP:

MAC: Mỗi thiết bị mạng đều có địa chỉ vật lý - MAC (Medium Access Control Address) và địa chỉ đó là duy nhất. Các thiết bị trong cùng một mạng thường dùng địa chỉ MAC để liên lạc với nhau tại tầng liên kết dữ liệu (Tiếng anh là: Data Link Layer).

ARP (Address Resolution Protocol) : là giao thức sử dụng để chuyển đổi địa chỉ IP thành địa chỉ vật lý – địa chỉ MAC.

Nguyên tắc làm việc của ARP trong một mạng LAN:

Khi một thiết bị mạng muốn biết địa chỉ MAC của một thiết bị mạng nào đó mà nó đã biết địa chỉ ở tầng mạng (IP, IPX…) nó sẽ gửi một ARP request bao gồm địa chỉ MAC của nó và địa chỉ IP của thiết bị mà nó cần biết địa chỉ MAC trên toàn bộ một miền quảng bá (Tiếng anh là: Broadcast). Mỗi một thiết bị nhận được request này sẽ so sánh địa chỉ IP trong request với địa chỉ tầng mạng của mình. Nếu trùng địa chỉ thì thiết bị đó phải gửi ngược lại cho thiết bị gửi ARP request một gói tin (trong đó có chứa địa chỉ MAC của mình). Trong một hệ thống mạng đơn giản, ví dụ như PC A muốn gửi gói tin đến PC B và nó chỉ biết được địa chỉ IP của PC B. Khi đó PC A sẽ phải gửi một ARP broadcast cho toàn mạng để hỏi xem "địa chỉ MAC của PC có địa chỉ IP này là gì ?" Khi PC B nhận được broadcast này, nó sẽ so sánh địa chỉ IP trong gói tin này với địa chỉ IP của nó. Nhận thấy địa chỉ đó là địa chỉ của mình, PC B sẽ gửi lại một gói tin cho PC A trong đó có chứa địa chỉ MAC của B. Sau đó PC A mới bắt đầu truyền gói tin cho B.

Nguyên tắc hoạt động của ARP trong môi trường hệ thống mạng :

Hoạt động của ARP trong một môi trường phức tạp hơn đó là hai hệ thống mạng gắn với nhau thông qua một Router C. Máy A thuộc mạng A muốn gửi gói tin đến máy B thuộc mạng B. Do các broadcast không thể truyền qua Router nên khi đó máy A sẽ xem Router C như một cầu nối hay một trung gian (Tiếng anh là: Agent) để truyền dữ liệu. Trước đó, máy A sẽ biết được địa chỉ IP của Router C (địa chỉ Gateway) và biết được rằng để truyền gói tin tới B phải đi qua C. Tất cả các thông tin như vậy sẽ được chứa trong một bảng gọi là bảng định tuyến (Tiếng anh là: Routing Table). Bảng định tuyến theo cơ chế này được lưu giữ trong mỗi máy. Bảng định tuyến chứa thông tin về các Gateway để truy cập vào một hệ thống mạng nào đó. Ví dụ trong trường hợp trên trong bảng sẽ chỉ ra rằng để đi tới LAN B phải qua port X của Router C. Bảng định tuyến sẽ có chứa địa chỉ IP của port X. Quá trình truyền dữ liệu theo từng bước sau :

- Máy A gửi một ARP request (broadcast) để tìm địa chỉ MAC của port X.
- Router C trả lời, cung cấp cho máy A địa chỉ MAC của port X.
- Máy A truyền gói tin đến port X của Router.
- Router nhận được gói tin từ máy A, chuyển gói tin ra port Y của Router. Trong gói tin có chứa địa chỉ IP của máy B. Router sẽ gửi ARP request để tìm địa chỉ MAC của máy B.
- Máy B sẽ trả lời cho Router biết địa chỉ MAC của mình. Sau khi nhận được địa chỉ MAC của máy B, Router C gửi gói tin của A đến B.

Trên thực tế ngoài dạng bảng định tuyến này người ta còn dùng phương pháp proxyARP, trong đó có một thiết bị đảm nhận nhiệm vụ phân giải địa chỉ cho tất cả các thiết bị khác.Theo đó các máy trạm không cần giữ bảng định tuyến nữa Router C sẽ có nhiệm vụ thực hiện, trả lời tất cả các ARP request của tất cả các máy.

ARP cache:

ARP cache có thể coi như một bảng có chứa một tập tương ứng giữa các phần cứng và địa chỉ Internet Protocol (IP). Mỗi một thiết bị trên một mạng nào đó đều có cache riêng. Có hai cách lưu giữ các entry trong cache để phân giải địa chỉ diễn ra nhanh. Đó là:

* Các entry ARP Cache tĩnh. Ở đây, sự phân giải địa chỉ phải được thêm một cách thủ công vào bảng cache và được duy trì lâu dài.

* Các entry ARP Cache động. Ở đây, các địa chỉ IP và phần cứng được giữ trong cache bởi phần mềm sau khi nhận được kết quả của việc hoàn thành quá trình phân giải trước đó. Các địa chỉ được giữ tạm thời và sau đó được gỡ bỏ.

ARP Cache biến một quá trình có thể gây lãng phí về mặt thời gian thành một quá trình sử dụng thời gian một cách hiệu quả. Mặc dù vậy nó có thể bắt gặp một số vấn đề. Cần phải duy trì bảng cache. Thêm vào đó cũng có thể các entry cache bị "cũ" theo thời gian, vì vậy cần phải thực thi hết hiệu lực đối với các entry cache sau một quãng thời gian nào đó.

5.2 Tấn công kiểu giả mạo ARP:

5.2.1 Giới thiệu:

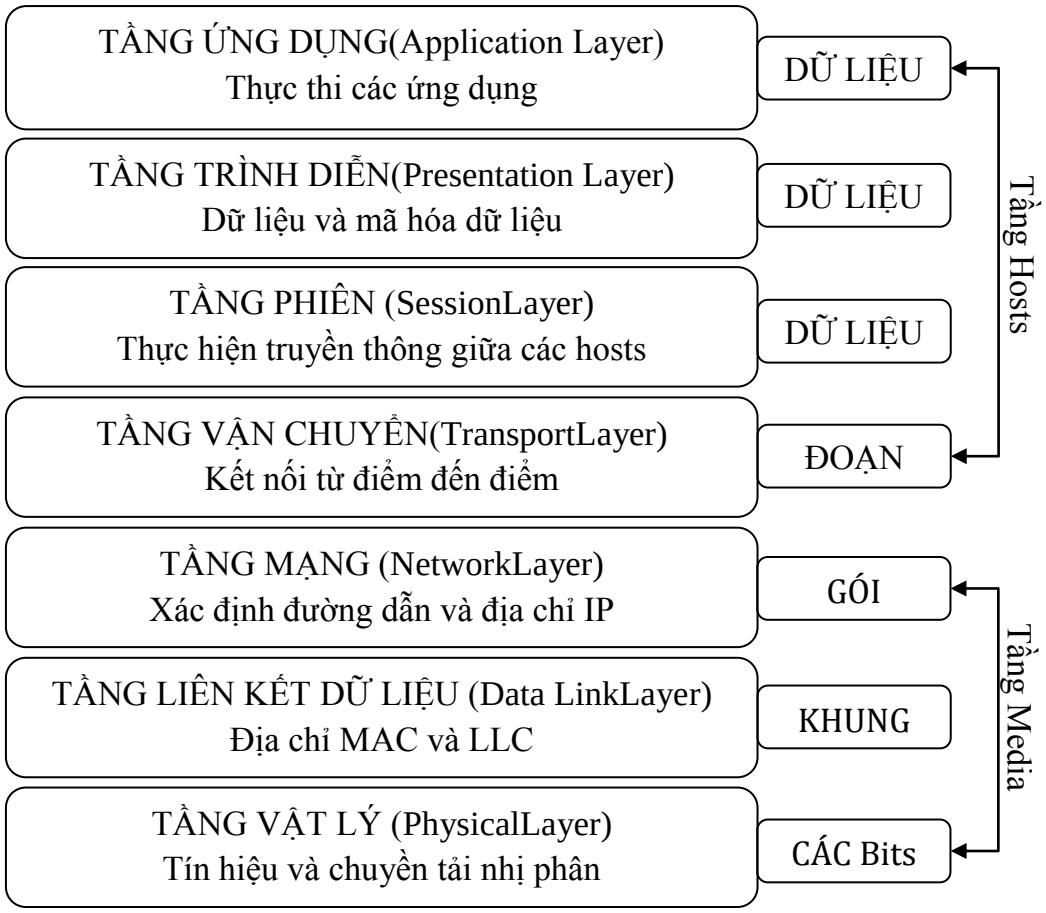
ARP phân giải địa chỉ IP nhận được thành địa chỉ MAC để gửi dữ liệu. Các gói ARP có thể giả mạo gửi dữ liệu đến máy tính của Hacker. Từ đó Hacker có thể khai thác ARP chặn dữ liệu truyền giữa hai máy tính.

Bằng việc làm tràn địa chỉ MAC ở bảng ARP của Switch với hồi đáp ARP ngụy trang, Hacker có thể làm tràn Switch và sau đó chặn các gói tin thu thập dữ liệu.

5.2.2 Cách giả mạo ARP:

Khi một người dùng hợp pháp khởi động kết nối đến một người dùng hợp lệ khác, lúc đó ở tầng 2 – tầng liên kết dữ liệu (Tiếng anh là: Data Link Layer) của mô hình OSI, ARP yêu cầu người nhận và người gửi đợi nhận địa chỉ MAC.

Hacker sẽ thực hiệngiả mạo ARP ở tầng 2 này, vì tầng này thường không được bảo vệ. Miền broadcast có thể trả lời yêu cầu broadcast ARP và hồi đáp đến người gửi bằng địa chỉ MAC giả mạo của người nhận.



Hình 2.3: Các tầng trong mô hình OSI.

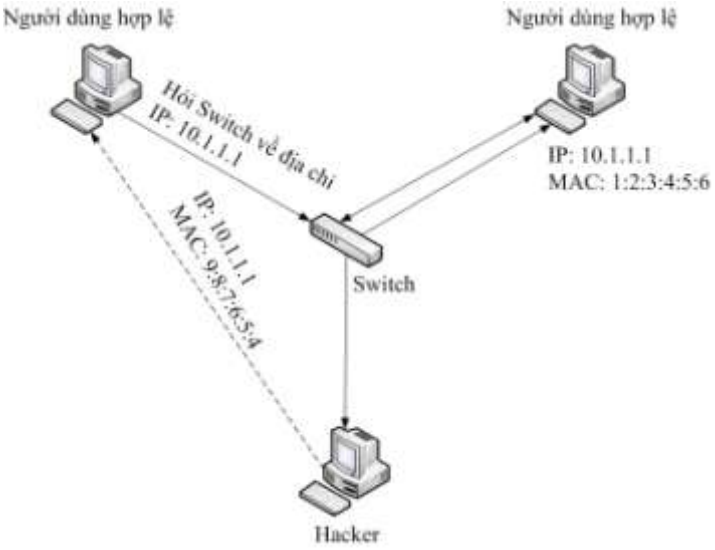
5.2.3 Các bước tấn công ARP:

Một người dùng hợp lệ gửi một yêu cầu ARP đến Switch và hỏi thăm về máy tính có địa chỉ IP là: 10.1.1.1.

Người dùng hợp lệ khác trả lời bằng một ARP, sau đó cung cấp địa chỉ chỉ IP là 10.1.1.1 và địa chỉ MAC là: 1:2:3:4:5:6.

Hacker sẽ lấy các gói tin ARP này sau đó bằng cách anh ta gửi địa chỉ MAC nặc danh của mình cho người dùng hợp lệ.

Thông tin về dịa chỉ IP 10.1.1.1 bây giờ gửi đến địa chỉ MAC: 9:8:7:6:5:4.



Hình 2.4: Các bước tấn công ARP.

Chú ý: Địa chỉ MAC và địa chỉ IP hình 1.4 chỉ mang tính chất minh họa.

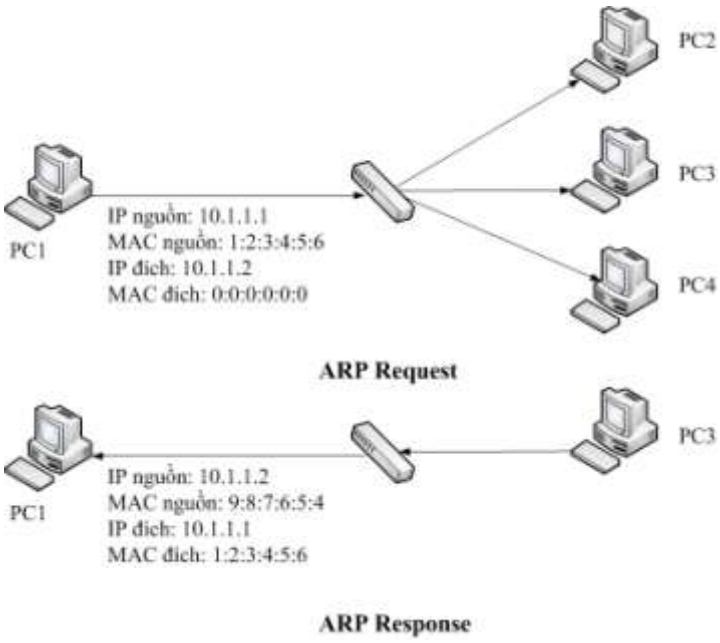
5.3 Tấn công Man-in-the-Middle – Giả mạo ARP Cache:

5.3.1 Tấn công Man-in-the-Middle:

Tấn công Man-in-the-Middle (Viết tắt là: MITM) là một hình thức của hoạt động nghe lén mà trong đó kẻ tấn công thiết lập các kết nối đến máy tính nạn nhân và chuyển tiếp các tin nhắn giữa chúng. Trong trường hợp bị tấn công, nạn nhân cứ tin tưởng là họ đang truyền thông một cách trực tiếp với nạn nhân kia, trong khi đó sự thực thì các luồng truyền thông lại bị thông qua host của kẻ tấn công. Và kết quả là các host này không chỉ có thể thông dịch dữ liệu nhạy cảm mà nó còn có thể gửi xen vào cũng như thay đổi luồng dữ liệu để kiểm soát sâu hơn những nạn nhân của nó.

5.3.2 Truyền thông ARP thông thường:

Giao thức ARP được thiết kế để phục vụ cho nhu cầu thông dịch các địa chỉ giữa tầng thứ hai và tầngthứ ba trong mô hình OSI. Tầng thứ hai – Tầng liên kết dữ liệu (Tiếng anh là: Data Link Layer) sử dụng địa chỉ MAC để các thiết bị phần cứng có thể truyền thông với nhau một cách trực tiếp. Tầng thứ ba – tầng mạng (Tiếng anh là: Network Layer), sử dụng địa chỉ IP để tạo các mạng có khả năng mở rộng trên toàn cầu. Tầng liên kết dữ liệu xử lý trực tiếp với các thiết bị được kết nối với nhau, còn tầng mạng xử lý các thiết bị được kết nối trực tiếp và không trực tiếp. Mỗi tầng có cơ chế phân định địa chỉ riêng, và chúng phải làm việc với nhau để tạo nên một mạng truyền thông.



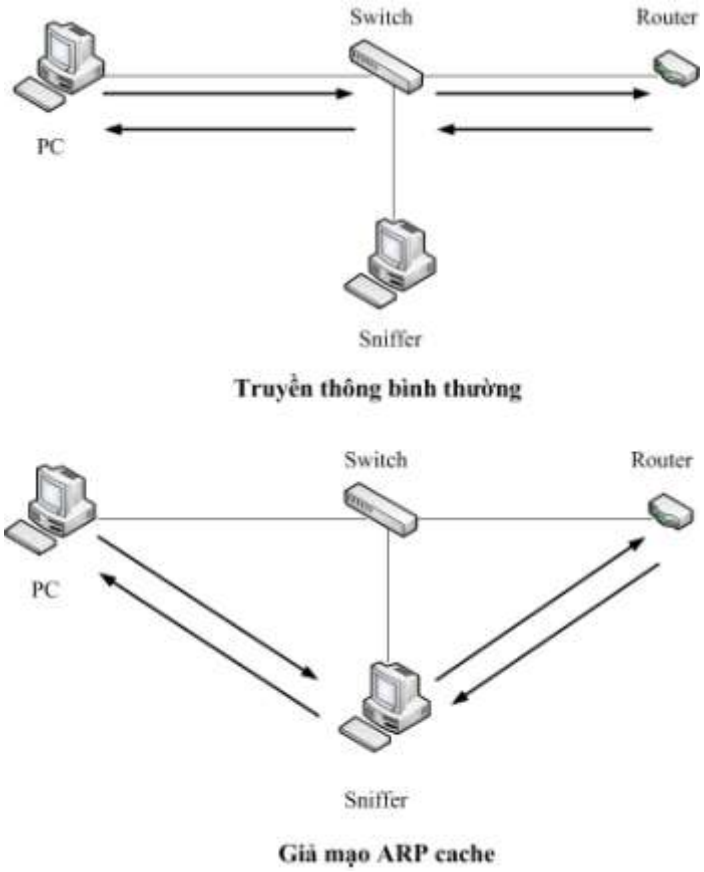
Hình 2.5: Quá trình truyền thông ARP

Thực chất trong vấn đề hoạt động của ARP được tập trung vào hai gói, một gói ARP request và một gói ARP reply. Mục đích của request và reply là tìm ra địa chỉ MAC phần cứng có liên quan tới địa chỉ IP đã cho để lưu lượng có thể đến được đích của nó trong mạng. Gói request được gửi đến các thiết bị trong đoạn mạng, trong khi gửi nó nói rằng: Tôi có địa chỉ IP là: 10.1.1.1, địa chỉ MAC là: 1:2:3:4:5:6. Tôi cần gửi một vài thứ đến người có địa chỉ IP là: 10.1.1.2 nhưng tôi không biết địa chỉ MAC này nằm ở đâu. Nếu ai có địa chỉ IP này thì đáp trả kèm địa chỉ IP của mình. Đáp trả sẽ được gửi đi trong gói ARP reply và cung cấp câu trả lời : Tôi là người mà bạn đang tìm kiếm với địa chỉ IP là 10.1.1.2. Địa chỉ MAC của tôi là9 :8 :7 :6 :5 :4. Khi quá trình này hoàn tất, thiết bị phát sẽ cập nhật bảng ARP cache của nó và hai thiết bị này có thể truyền thông với nhau.

5.3.3 Việc giả mạo Cache :

Việc giả mạo bảng ARP chính là lợi dụng việc không an toàn của giao thức ARP. Không giống như các giao thức khác, chẳng hạn như DNS (có thể được cấu hình để chỉ chấp nhận các nâng cấp động khá an toàn), các thiết bị sử dụng giao thức phân giải địa chỉ (ARP) sẽ chấp nhận nâng cấp bất cứ lúc nào. Điều này có nghĩa rằng bất cứ thiết bị nào có thể gửi gói ARP reply đến một máy tính khác và máy tính này sẽ cập nhật vào bảng ARP cache của nó ngay giá trị mới này. Việc gửi một gói ARP reply

khi không có request nào được tạo ra được gọi là việc gửi ARP "vu vơ". Khi các ARP reply "vu vơ"này đến được các máy tính đã gửi request, máy tính request này sẽ nghĩ rằng đó chính là đối tượng mình đang tìm kiếm để truyền thông, tuy nhiên thực chất họ lại đang truyền thông với một kẻ tấn công.



Hình 2.6: Chặn truyền thông bằng các giả mạo ARP Cache

5.3.4 Sử dụng Cain & Abel giả mạo ARP Cache :

5.3.4.1 Giới thiệu về Cain & Abel :

Cain & Abel là chương trình tìm mật khẩu chạy trên hệ điều hành Microsoft. Nó cho phép dễ dàng tìm ra nhiều loại mật khẩu bằng cách dò tìm trên mạng, phá các mật khẩu đã mã hóa bằng các phương pháp Dictionary, Brute-Force and Cryptanalysis, ghi âm các cuộc đàm thoại qua đường VoIP, giải mã các mật khẩu đã được bảo vệ, tìm ra file nơi chứa mật khẩu, phát hiện mật khẩu có trong bộ đệm, và phân tích các giao thức định tuyến.

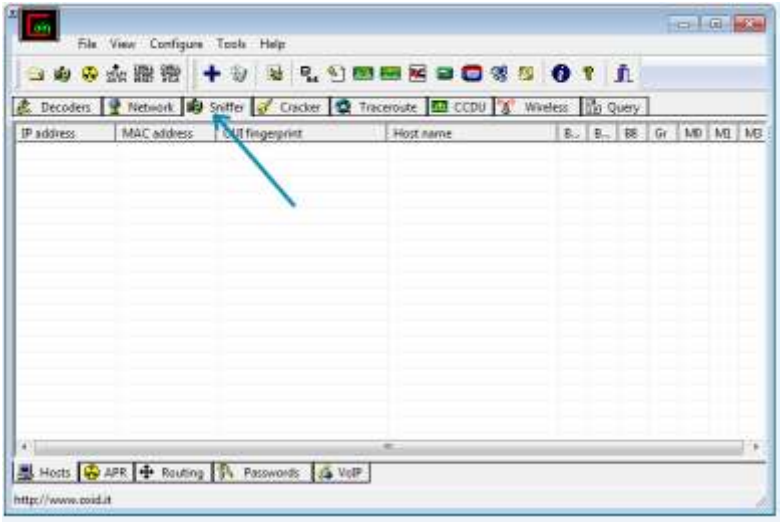
Chương trình này không khai thác những lỗ hổng chưa được vá của bất kỳ phần mềm nào. Nó tập trung vào những khía cạnh, điểm yếu hiện có trong các chuẩn giao

thức, các phương pháp đăng nhập và các kỹ thuật đệm; mục đích chính của công cụ này là tìm ra mật khẩu và những thông tin càn thiết từ nhiều nguồn, tuy vậy, nó cũng sử dụng nhiều công cụ "phi chuẩn" đối với người sử dụng Microsoft Windows.

5.3.4.2 Sử dụng Cain & Abel giả mạo ARP Cache :

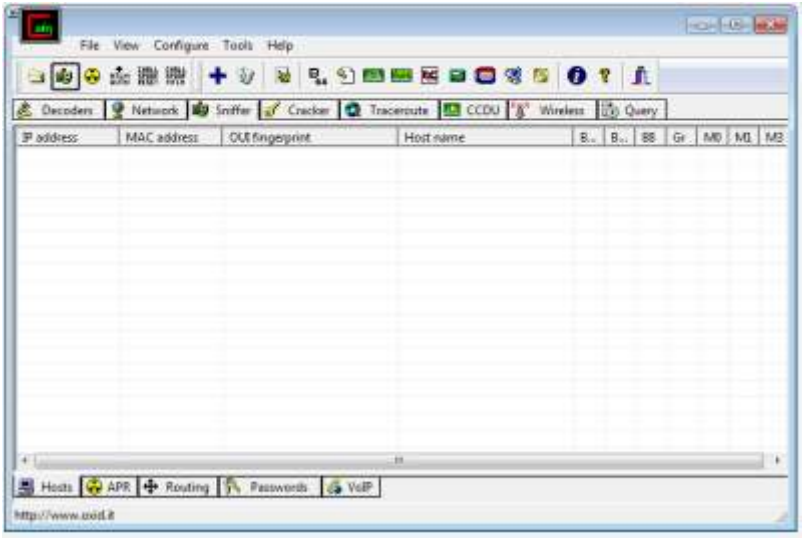
Tải Cain & Abel của Oxid.it tại địa chỉ : http://www.oxid.it/cain.html

Sau khi cài đặt và lần đầu mở Cain & Abel sẽ thấy một loạt các tab ở phía trên cửa sổ. Với mục đích của báo cáo, em sẽ làm việc trong tab Sniffer. Khi kích vào tab này, bạn sẽ thấy một bảng trống.



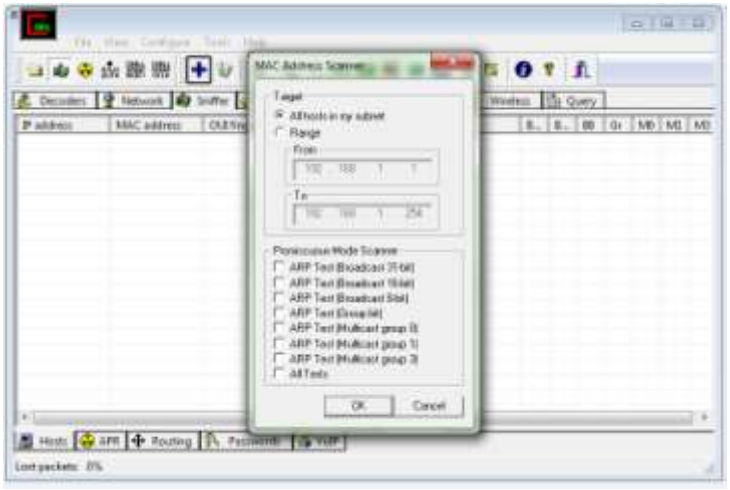
Hình 2.7 : Tab Sniffer của Cain & Abel.

Để điền vào bảng này bạn cần kích hoạt bộ Sniffer đi kèm của chương trình và quét các máy tính trong mạng của bạn. Kích hoạt vào biểu tượng được đánh dấu như hình bên dưới (Biểu tượng giống hình card mạng):



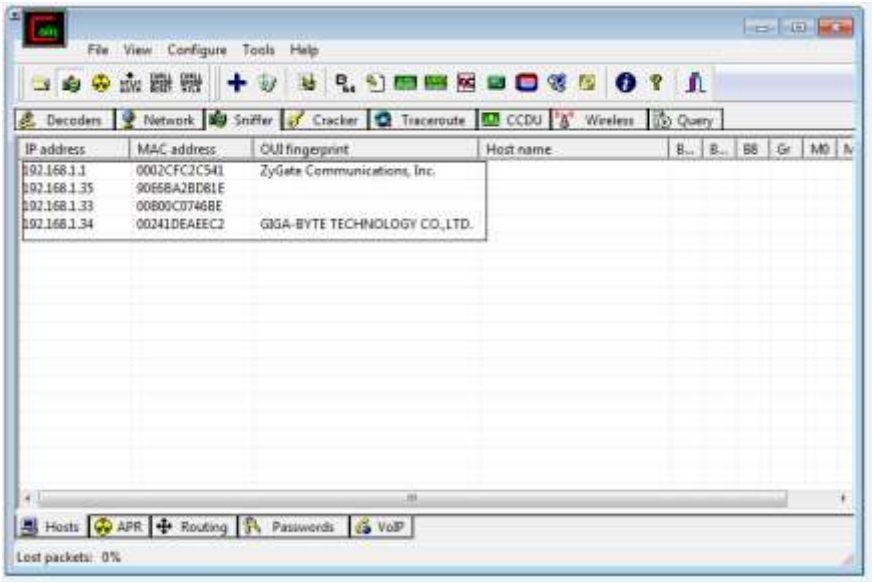
Hình 2.8 : Lựa chọn để quét các máy tính trong mạng.

Chạy lần đầu, bạn sẽ bị yêu cầu chọn giao diện mà mình muốn Sniffer. Giao diện cần phải được kết nối với mạng mà bạn sẽ thực hiện giả mạo ARP Cache của mình trên đó. Khi đã chọn xong giao diện, kích OK để kích hoạt bộ sniffer đi kèm của Cain & Abel. Tại đây, biểu tượng thanh công cụ giống như card mạng sẽ bị nhấn xuống. Nếu không, bạn hãy thực hiện điều đó. Để xây dựng một danh sách các máy tính hiện có trong mạng của bạn, hãy kích biểu tượng giống như ký hiệu (+) trên thanh công cụ chính và kích OK.



Hình 2.9 : Quét các thiết bị trong mạng.

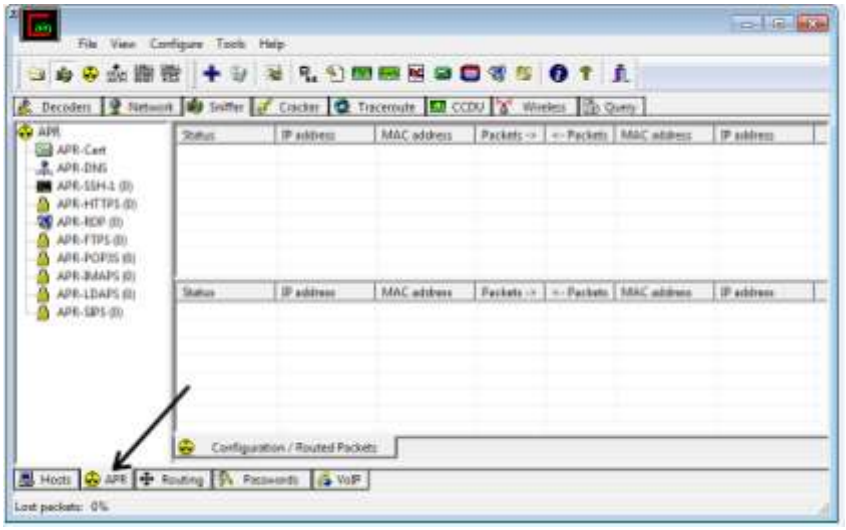
Những khung lưới trống rỗng lúc này sẽ được điền đầy bởi một danh sách tất cả các thiết bị trong mạng của bạn, cùng với đó là địa chỉ MAC, IP cũng như các thông tin nhận dạng của chúng. Đây là danh sách bạn sẽ làm việc khi thiết lập giả mạo ARP Cache.



Hình 2.10 : Danh sách các thiết bị trong mạng

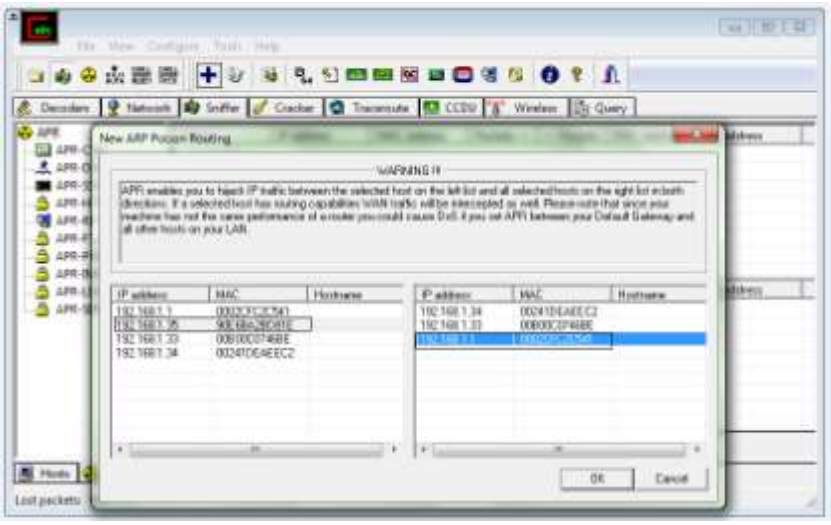
Ở phía dưới cửa sổ chương trình, bạn sẽ thấy một loạt các tab đưa bạn đến các cửa sổ khác bên dưới tiêu đề Sniffer. Lúc này bạn đã xây dựng được danh sách các thiết bị của mình, nhiệm vụ tiếp theo của bạn là làm việc với tab APR. Chuyển sang cửa sổ APR bằng cách kích vào tab đó.

Khi ở trong cửa sổ APR, bạn sẽ thấy hai bảng trống rỗng: một bên phía trên và một phía dưới. Khi thiết lập chúng, bảng phía trên sẽ hiển thị các thiết bị có liên quan trong giả mạo ARP cache và bảng bên dưới sẽ hiển thị tất cả truyền thông giữa các máy tính bị giả mạo.



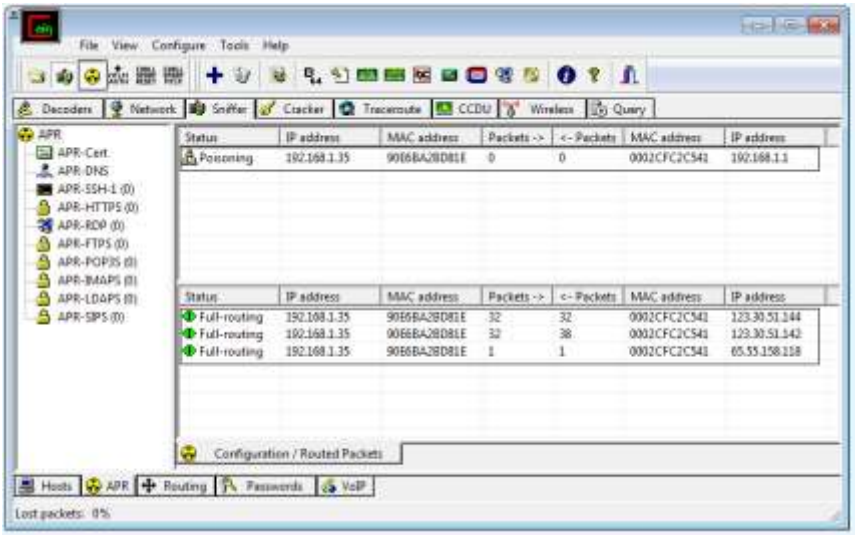
Hình 2.11 : Giao diện Tab ARP

Tiếp tục thiết lập sự giả mạo ARP bằng cách kích vào biểu tượng giống như dấu (+) trên thanh công cụ chuẩn của chương trình. Cửa sổ xuất hiện có hai cột đặt cạnh nhau. Phía bên trái, bạn sẽ thấy một danh sách tất cả các thiết bị có sẵn trong mạng. Kích địa chỉ IP của một trong những nạn nhân, bạn sẽ thấy các kết quả hiện ra trong cửa sổ bên phải là danh sách tất cả các host trong mạng, bỏ qua địa chỉ IP vừa chọn. Trong cửa sổ bên phải, kích vào địa chỉ IP của nạn nhân khác và kích OK.



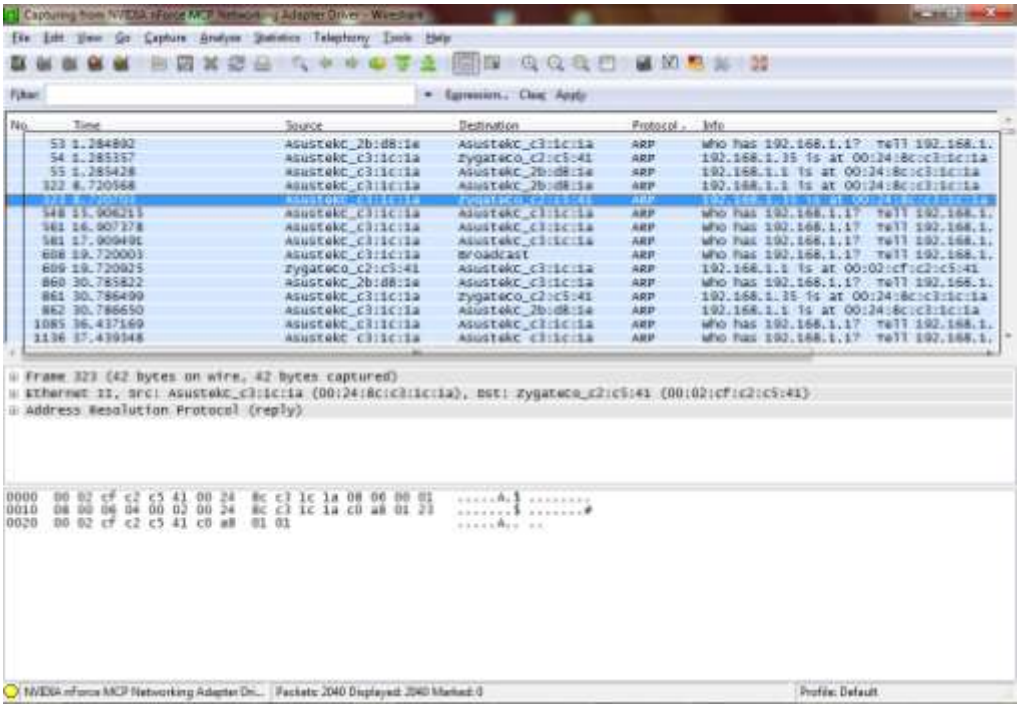
Hình 2.12 : Lựa chọn IP nạn nhân để giả mạo ARP Cache.

Các địa chỉ IP của cả hai thiết bị lúc này sẽ được liệt kê trong bảng phía trên của cửa sổ ứng dụng chính. Để hoàn tất quá trình, kích vào ký hiệu bức xạ (vàng đen) trên thanh công cụ chuẩn. Điều đó sẽ kích hoạt các tính năng giả mạo ARP Cache của Cain & Abel và cho phép hệ thống phân tích của bạn trở thành người nghe lén tất cả các cuột truyền thông giữa hai nạn nhân.



Hình 2.13 : Quá trình giả mạo ARP Cache.

Nếu bạn muốn thấy những gì đang diễn ra, hãy cài đặt Wireshark và lắng nghe từ giao diện khi bạn kích hoạt giả mạo. Bạn sẽ thấy lưu lượng ARP đến hai thiết bị và ngay lập tức thấy sự truyền thông giữa chúng. Tải Wireshark tại địa chỉ: http://www.wireshark.org/download.html



Hình 2.14: Chèn lưu lượng ARP.

Khi kết thúc, hãy kích vào ký hiệu bức xạ (vàng đen) lần nữa để ngừng hành động giả mạo ARP cache.

5.3.5 Biện pháp phòng chống :

5.3.5.1 Bảo mật LAN :

Giả mạo ARP Cache chỉ là một kỹ thuật tấn công mà nó chỉ sống sót khi cố gắng chặn lưu lượng giữa hai thiết bị trên cùng một LAN. Chỉ có một lý do khiến cho bạn lo sợ về vấn đề này là liệu thiết bị nội bộ trên mạng của bạn có bị thỏa hiệp, người dùng tin cậy có ý định xấu hay không hoặc liệu có ai đó có thể cắm một thiết bị không tin cậy vào mạng. Mặc dù chúng ta thường tập trung toàn bộ những cố gắng bảo mật của mình lên phạm vi mạng nhưng việc phòng chống lại những mối đe dọa ngay từ bên trong và việc có một thái độ bảo mật bên trong tốt có thể giúp bạn loại trừ được khả năng tấn công này.

5.3.5.2 Mã hóa ARP Cache :

Một cách có thể bảo vệ chống lại vấn đề không an toàn vốn có trong các ARP request và ARP reply là thực hiện một quá trình "kém động" hơn. Đây là một tùy chọn vì các máy tính Windows cho phép bạn có thể bổ sung các entry tĩnh vào ARP cache. Bạn có thể xem ARP cache của máy tính Windows bằng cách mở nhắc lệnh và

đánh vào đó lệnh arp –a.

Hình 2.15: ARP Cache của máy tính.

Có thể thêm các entry vào danh sách này bằng cách sử dụng lệnh arp –s <IP ADDRESS><MAC ADDRESS>.

Trong các trường hợp, nơi cấu hình mạng của bạn không mấy khi thay đổi, bạn hoàn toàn có thể tạo một danh sách các entry ARP tĩnh và sử dụng chúng cho các client thông qua một kịch bản tự động. Điều này sẽ bảo đảm được các thiết bị sẽ luôn dựa vào ARP cache nội bộ của chúng thay vì các ARP request và ARP reply.

5.3.5.3 Kiểm tra lưu lượng ARP với chương trình của hãng thứ ba :

Tùy chọn cuối cùng cho việc phòng chống lại hiện tượng giả mạo ARP Cache là phương pháp phản ứng có liên quan đến việc kiểm tra lưu lượng mạng của các thiết bị. Bạn có thể thực hiện điều này với một vài hệ thống phát hiện xâm phạm (chẳng hạn như Snort) hoặc thông qua các tiện ích được thiết kế đặc biệt cho mục đích này (như xARP).

5.4 Địa chỉ MAC trùng lặp:

5.4.1 Giới thiệu:

Đây là phương pháp tấn công bằng cách sử dụng Sniffing ở địa chỉ MAC của client, sau đó địa chỉ này kích hoạt phù hợp và đi đến cổng của Switch.

Bằng việc theo dõi mạng, Hacker có thể chặn và sử dụng địa chỉ MAC của người dùng hợp lệ.

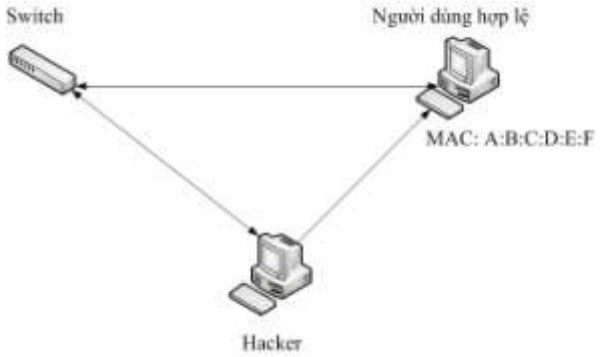
Hacker sẽ nhận tất cả lưu lượng mạng dành cho người dùng hợp lệ. Kỹ thuật này hoạt động ở các Access point của Wireless, ngay cả khi bộ lọc địa chỉ MAC được kích

hoạt.

5.4.2 Tấn công kiểu địa chỉ MAC trùng lặp:

Hacker theo dõi mạng để lấy địa chỉ MAC của người dùng hợp lệ và sau đó sử dụng địa chỉ MAC này kết hợp với cổng của Switch để tấn công người khác.

Switch chỉ cho phép truy cập vào mạng nếu địa chỉ MAC là A:B:C:D:E :F. Lợi dụng điểm này Hacker đã chặn và lấy địa chỉ MAC của người dùng hợp lệ và truy cập vào mạng.



Hình 2.16: Tấn công kiểu địa chỉ MAC trùng lặp.

II. TẤN CÔNG TỪ CHỐI DỊCH VỤ:

1. Tấn công từ chối dịch vụ (DoS):

Tấn công từ chối dịch vụ (Tiếng anh là: Denial of Service – Viết tắt là: DoS) là một cuộc tấn công thực hiện từ một người hoặc một nhóm người nào đó đến hệ thống mục tiêu. Khi cuộc tấn công công xảy ra, trên hệ thống bị tấn công, người dùng không thể truy xuất dữ liệu hay thực hiện bất kỳ một công việc nào.

2. Mục đích tấn công từ chối dịch vụ:

Mục đích của tấn công từ chối dịch vụ là không cho phép ủy quyền truy cập đến máy hoặc dữ liệu, ngăn chặn các người dùng hợp pháp truy cập dịch vụ của hệ thống.

Khi tấn công, Hacker có thể thực hiện các công việc sau:

- Cố gắng làm ngập hệ thống, ngăn chặn việc trao đổi thông tin giữa các kết nối hợp lệ.
- Phá vỡ các kết nối giữa hai máy, ngăn chặn các truy cập đến dịch vụ
- Ngăn chặn các thiết lập đặc biệt đến dịch vụ.
- Phá vỡ hệ thống của một người hoặc một hệ thống chỉ định.

3. Ảnh hưởng của phương thức tấn công:

Ảnh hưởng:

- Mạng mục tiêu bị vô hiệu hóa.
- Vô hiệu hóa việc tổ chức.
- Ảnh hưởng đến uy tín và tài chính của tổ chức bị tấn công.

Phương thức:

- Khi cuộc tấn công sảy ra sẽ:
  - Làm khan hiếm, giới hạn và không thể phục hồi tài nguyên.
  - Ảnh hưởng đến băng thông, bộ nhớ, không gian đĩa, CPU và cấu trúc dữ liệu.
  - Không thể truy cập đến máy tính khác và mạng.
- Phá hủy, thay thế các thông tin cấu hình.
- Phá hủy ở mức vật lý, thay thế các thành phần mạng.

4. Các loại tấn công từ chối dịch vụ:

Tấn công từ chối dịch vụ chia làm hai loại tấn công:

- Tấn công DoS (Denial of Service): Tấn công từ một cá thể hay tập hợp các cá thể.

- Tấn công DdoS (Distributed Denial of Service): Đây là sự tấn công từ một mạng máy tính được thiết kế để tấn công tới một đích cụ thể nào đó.

4.1 Các dạng tấn công DoS:

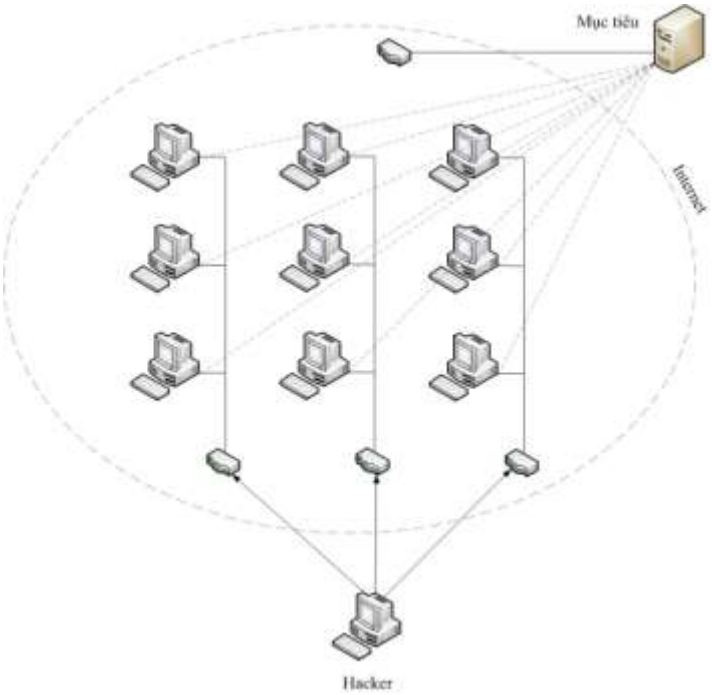
- Smurf.
- Buffer Overflow Attack
- Ping of Death
- Teardrop
- SYN Attack

4.1.1 Smurf:

Người tấn công tạo ra một khối lượng lớn các giao tiếp ICMP (Internetwork Control Message Protocol) đến đại chỉ mạng broadcast thiết lập địa chỉ IP giả rồi đồng loạt gửi đến host của nạn nhân.

Máy tính nạn nhất mất thời gian hồi đáp lại các thông điệp ICMP giả mạo, dẫn đến tình trạng quá tải.

Khi hồi đáp số lượng lớn các ICMP dẫn đến tình trạng ngập tràn mạng và kết nối không thể thực hiện được nữa.



Hình 2.17: Tấn công theo kiểu Smurf.

4.1.2 Tấn công tràn bộ đệm - Buffer Overflow Attack:

Tấn công tràn bộ đệm xuất hiện bất kỳ lúc nào mà chương trình ghi những thông tin vào bộ đệm lớn hơn không gian cho phép của bộ nhớ.

Hacker thực hiện ghi đè các dữ liệu vào các chương trình để chiếm quyền điều khiển và thực hiện các đoạn mã của Hacker.

Nếu gửi thông điệp email mà số tập tinh đính kèm lên đến 256 tập tin thì có thể là nguyên nhân dẫn đến tình trạng tràn bộ đệm.

4.1.3 Tấn công tràn bộ đệm bằng Ping – Ping of Death:

Hacker chủ ý gửi một gói dữ liệu lớn hơn 65536 bytes mà giao thức IP cho phép.

Phân mảnh gói dữ liệu IP thành những đoạn nhỏ hơn.

Phân đoạn có thể cho phép thêm nhiều hơn 65536 bytes. Hệ điều hành không thể kiểm soát các gói có kích thước quá lớn nên dẫn đến tình trạng đóng băng, khởi động lại hoặc hệ thống bị phá hủy.

Rất khó có thể nhận dạng Hacker khi họ gửi dữ liệu vì địa chỉ của họ đã ngụy trang.

4.1.4 Tấn công Teardrop:

Khi một địa chỉ IP nào đó yêu cầu một gói dữ liệu nhưng gói này quá lớn để gửi

đến router kế tiếp, hệ thông sẽ phân chia gói này thành các đoạn nhỏ hơn. Lợi dụng điểm này, Hacker chèn các địa chỉ vào trong những mảnh nhỏ. Địa chỉ IP của Hacker thường nằm trong những offset khó hiểu.

Hệ điều hành không có khả năng nhận những gói tin không thích hợp, vì vậy hệ thống bị treo.

4.1.5 Tấn công SYN – SYN Attack:

Hacker gửi thêm TCP SYN yêu cầu server của nạn nhân xử lý.

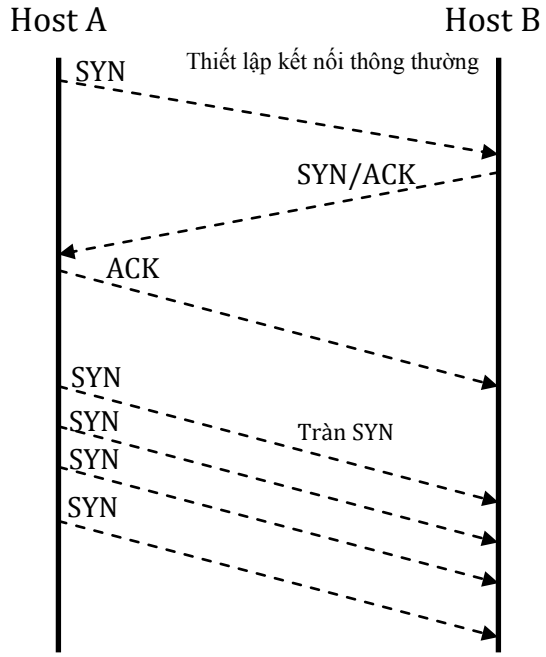
Đây là kiểu tấn công Exploit theo Three – Way handshake (Ba cái bắt tay). Nó sử dụng một tập các gói TCP SYN lớn gửi đến hệ thống nạn nhân với địa chỉ IP giả mạo và dẫn đến việc từ chối dịch vụ trên hệ thống của nạn nhân.

Lợi thế của tấn công này là khai thác sai lầm trong hầu hết các host thực thi TCP Three – Way handshake.

Khi host B nhận yêu cầu SYN từ host A, nó mở một phần kết nối và đưa vào hàng đợi.

Các host nguy hiểm có các Exploits kích thước nhỏ nằm trong hàng đợi để từ đó nó gửi nhiều yêu cầu đến host khác. Nhưng khi nhận hồi đáp từ các host này, nó không trả lại thông báo SYN/ACK.

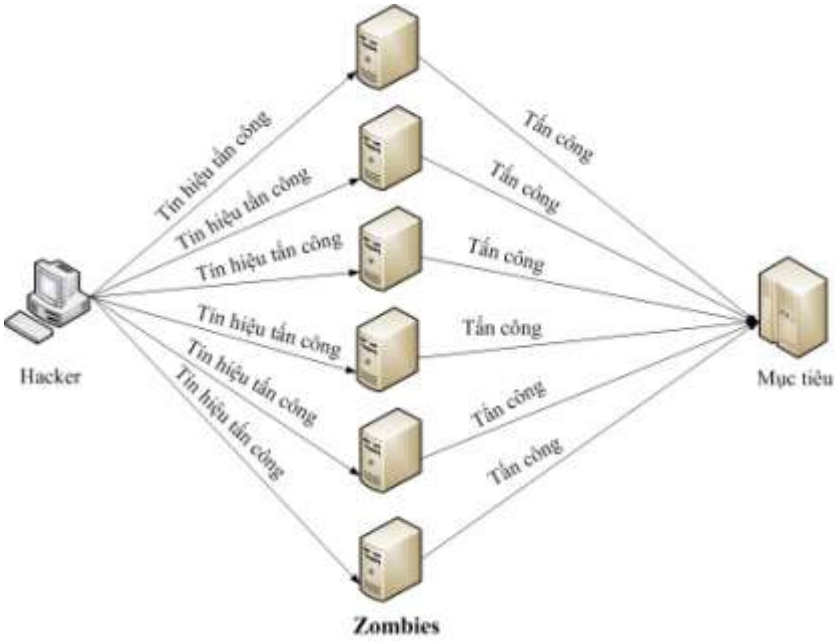
Hàng đợi đang lắng nghe trên hệ thống của nạn nhân sẽ nhanh chóng bị lấp đầy. Chính điều này đã dẫn đến quá trình từ chối dịch vụ trên hệ thống của nạn nhân.



Hình 2.18: Tràn SYN.

4.2 Tấn công DDoS:

Trên Internet, tấn công từ chối dịch vụ phân tán (Tiếng anh là: Distributed Denial of Service – Viết tắt là: DDoS) là cuộc tấn công của nhiều hệ thống đến một mục tiêu. Điều đó làm cho hệ thống của nạn nhân bị quátải và dẫn đến tình trạng tràn hệ thống, các người dùng hợp pháp không thể truy cập tài nguyên và dịch vụ bị từ chối.



Hình 2.19: Tấn công DDoS.

4.2.1 Mạng BOT NET:

4.2.1.1 Ý nghĩa của mạng BOT:

- Khi sử dụng một công cụ tấn công DoS tới một máy chủ đôi khi không gây ảnh hưởng gì cho máy chủ.

Ví dụ:

- Giả sử bạn sử dụng công cụ (Tiếng anh là: 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 =>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 => Kết quả sẽ ra sao ?

- Nhưng làm cách nào để có 1000 máy tính kết nối với mạng ? Chúng ta không

thể mua 1000 máy tính kết nối Internet để tấn công và không có bất kỳ ai sử dụng cách này cả. Nhưngkẻ tấn công cóthể xây dựng một mạng gồm hàng nghìn máy tính kết Internet (có mạng BOT lên tới 400.000 máy).

- Khi có trong tay mạng BOT kẻ tấn công sử dụng những công cụ (Tiếng anh là: 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 tải một file trên trang web của bạn. Và đó chính là tấn công từ chối dịch vụ phân tán – DDoS (Distributed Denial of Servcie).

4.2.1.2 Mạng BOT:

- BOT từ viết tắt của từ RoBOT.

- 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 nhóm 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.

4.2.1.3 Mạng BOT NET:

- 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*128 ~ 100Mbps . Đây là một con số thể hiện băng thông mà khó một nhà cung cấp Hosting nào có thể chia sẻ cho mỗi trang web của mình.

4.2.1.4 Mục đích sử dụng mạng BOT NET:

- Tấn công Distributed DenialofService – DdoS: Botnet được sử dụng cho tấn công DDoS.

- Sniffing traffic:Botnet cũng có thể sử dụng các gói tin nó Sniffer .Sau khi lấy

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 ngân hàng trực tuyến, 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.

- Tấn công vào IRC Chat Networks.

- Phishing: Mạng Botnet còn được sử dụng để phishing mail nhằm lấy các thông tin nhạy cảm của người dùng.

4.2.1.5 Các bước xây dựng mạng BotNet:

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 (Đây là Bot được viết bằng C++ trên nền tảng Cross-platform và mã nguồn được tìm trên GPL. 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).

a, 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

b, 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 chia sẻ (Tiếng anh là: Share) mặc định dành cho các ứng dụng quản trị (Administrator or Administrative) Ví dụ như: C$, D$, E$ và print$ bằng cách đoán Tên đăng nhập (Tiếng anh là: Usernames) và Mật

khẩu (Tiếng anh là: 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.

c, 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.

d, Điều khiển tấn công từ mạng BOT NET:

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.

4.2.2 Tấn công DDoS:

4.2.2.1 Một số đặc điểm của tấn công DDoS:

Là cuộc tấn công trên phạm vi rộng lớn nhắm vào các dịch vụ trên hệ thống của nạn nhân.

Khi tấn công DDoS xảy ra, nó sẽ huy động các hệ thống zombies đồng loạt công kích vào mục tiêu chính.

Rất khó phát hiện ra tấn công DDoS vì chúng huy động từ nhiều địa chỉ IP khác nhau.

Hacker có khả năng huy động các tín hiệu tấn công từ chối dịch vụ bằng việc khai thác các tài nguyên trên các Zombies.

4.2.2.2 Không thể ngừng tấn công DdoS:

Khi cuộc tấn công DdoS xảy ra, nó sử dụng hàng ngàn hệ thống zombies. Hệ thống này sẽ kết nối qua Internet. Dựa vào các yếu điểm trên các hệ thống này, Hacker điều khiển nó và cùng tấn công đến hệ thống mục tiêu.

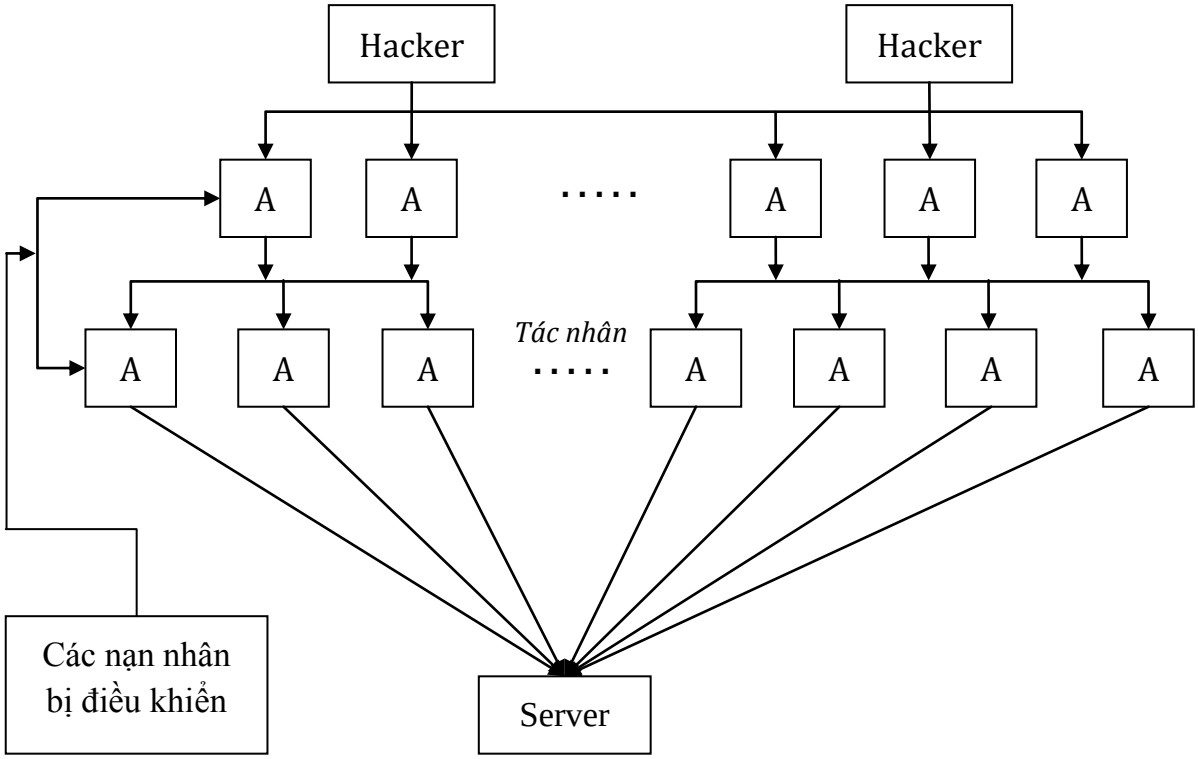
Khi cuộc tấn công DdoS khởi chạy, rất khó có thể ngưng được.

Các gói dữ liệu đến Firewall có thể ngăn chặn, nhưng nó sẽ dễ dàng tràn ngập tại kết nối Internet.

Nếu như nguồn IP là giả mạo, sẽ khong có cách nào để biết được nguồn gốc của cuộc tấn công. Ngược lại, ta có thể phát hiện ra dấu vết nếu nguồn địa chỉ IP là thật.

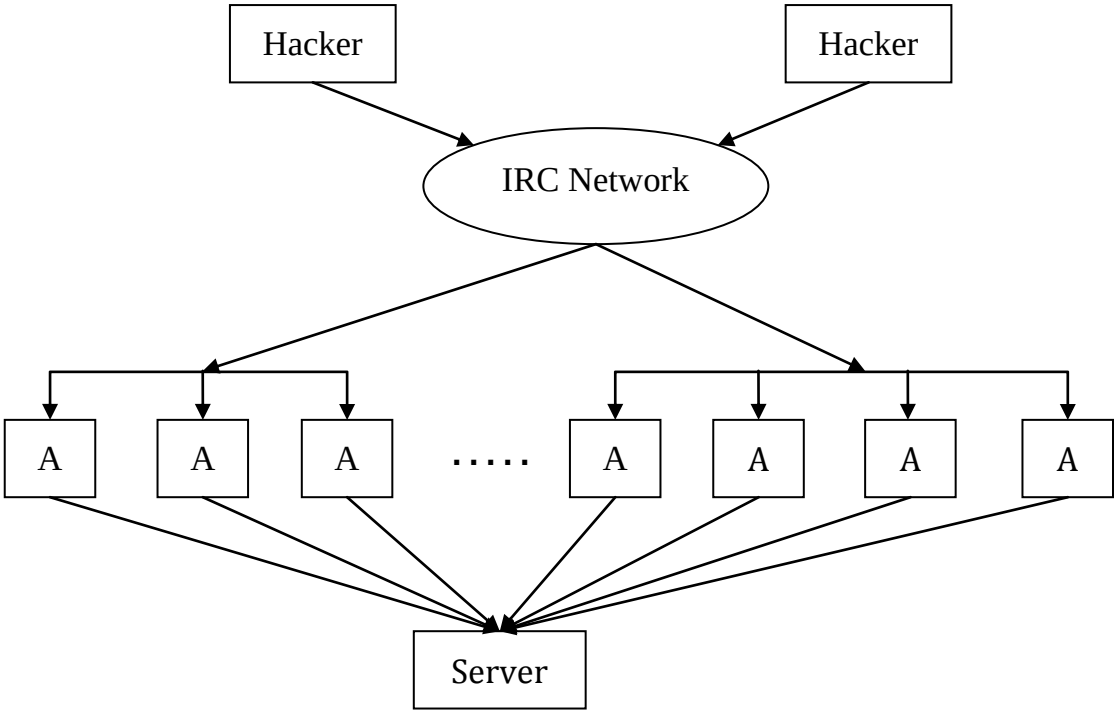
4.2.2.3 Điều khiển các tác nhân tấn công:

Hacker điều khiển các trạm (Agents) trên hệ thống của nạn nhân cùng tấn công đến hệ thống mục tiêu.



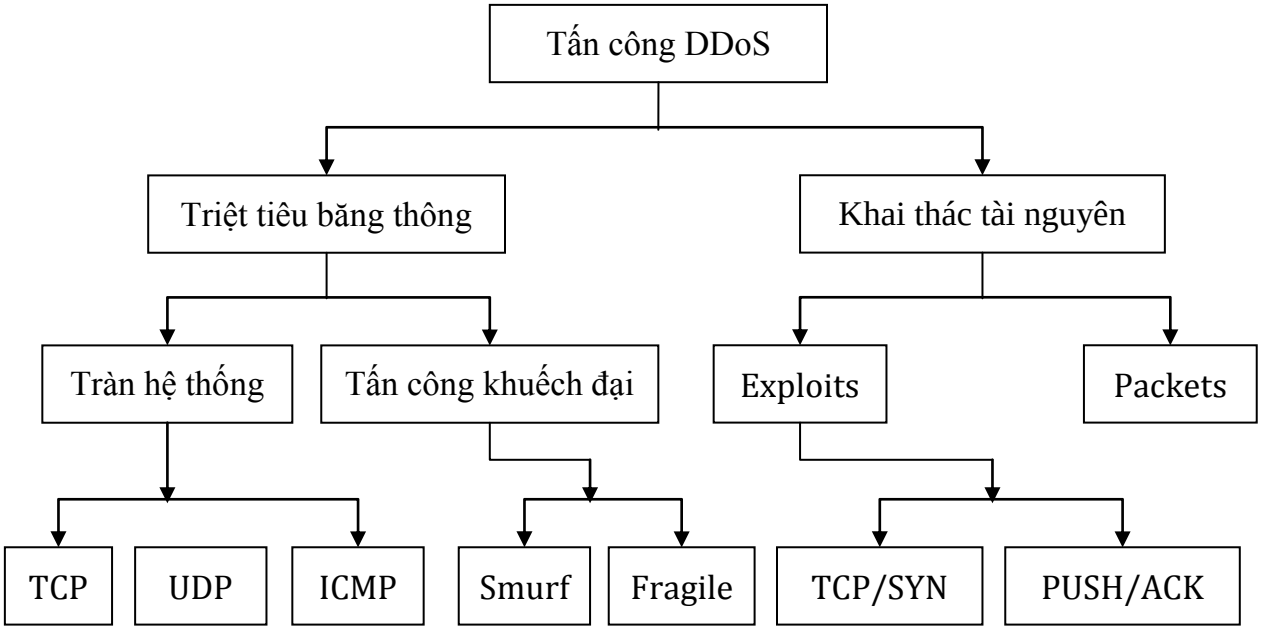
Hình 2.20: Điều khiển các tác nhân tấn công

Ngoài việc tấn công DDoS dựa vào mô hình Agent, Hacker còn tấn công vào hệ thống mục tiêu bằng mô hình IRC.



Hình 2.21: Tấn công DDoS dựa trên nền tảng IRC

4.2.2.4 Phân loại tấn công DDoS:



Hình 1.22: Các loại tấn công DDoS

4.2.2.5 Tấn công từ chối dịch vụ phản xạ nhiều vùng:

Tấn công từ chối dịch vụ phản xạ nhiều vùng – Distributed Reflection Denial of

Services (DRDoS).

a. Giới thiệu:

"Vào lúc 2 giờ sáng ngày 11 - 1 - 2002, Trang web GRC.COM đã bị đánh tung khỏi Internet bằng một kiểu tấn công từ chối dịch vụ mới. Điều kinh ngạc chính là nguồn tấn công được bắt đầu bằng những đường chính của Internet, bao gồm Yahoo.com và cả những IP "gary7.nsa.gov". Chúng tôi đã bị tấn công bởi hàng trăm server mạnh nhất của internet ...

Vào thời điểm chúng tôi tìm ra cách để ngăn chặn cuộc tấn công này và quay lại Internet, 1 072 519 399 packet bị chặn đứng trước khi cuộc tấn công bị dừng ..."

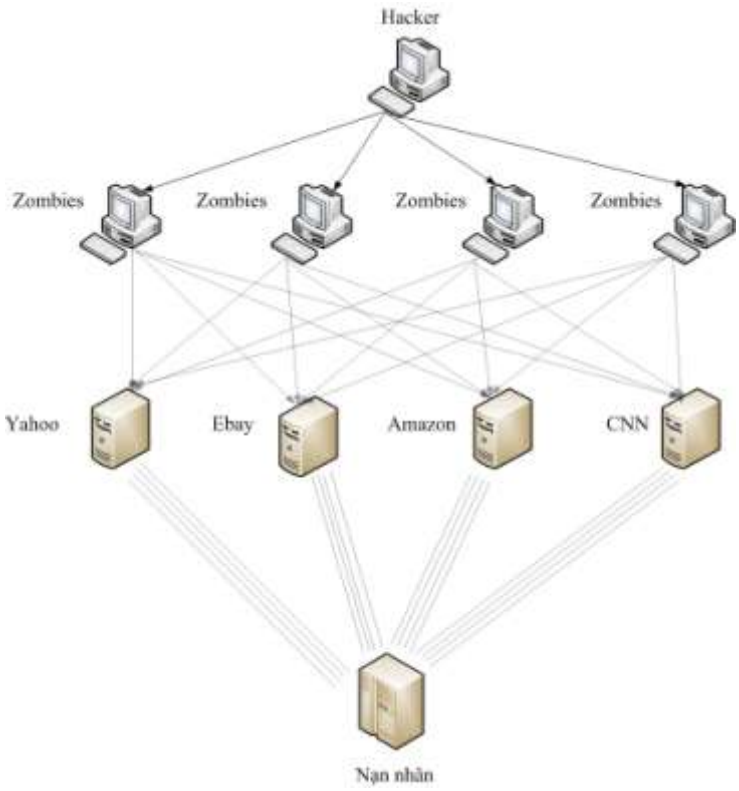
Đây chính là những thông tin được Steve Gibson mô tả trong bài báo về DRDoS mà ông đã gặp ngày 11-1-2002.

b. DRDoS - Thế hệ tiếp theo của DDoS:

Phương pháp SYN attack truyền thống của DoS, phương pháp này dựa trên bước thứ nhất để mở kết nối của TCP để tạo các "open half" kết nối làm Server bị ăn mòn hết tài nguyên. Các SYN packet được gửi trực tiếp đến Server sau khi đã giả mạo IP nguồn. IP giả mạo sẽ là một IP không có thật trên Internet để cho Server không thể nào hoàn thành được kết nối.

Ta có Server A và Victim, giả sử ta gửi một SYN packet đến Server A trong đó IP nguồn đã bị giả mạo thành IP của Victim. Server A sẽ mở mộtkết nối và gủi SYN/ACK packet cho Victim vì nghĩ rằng Victim muốn mở kết nối với mình. Và đây chính là khái niệm của Reflection (Phản xạ).

DRDoS có thể được mô tả như sau:



Hình 2.22: Tấn công DRDoS.

Hacker sẽ điều khiển Spoof SYN generator, gửi SYN packet đến tất cả các TCP Server lớn, lúc này các TCP Server này vô tình thành Zombie cho Hacker để cùng tấn công Victim và làm nghẽn đường truyền của Victim.

5. Phương pháp phòng chống tấn công DDoS:

5.1 Phòng ngừa các điểm yếu của ứng dụng (Application Vulnerabilities):

Các điểm yếu trong tầng ứng dụng có thể bị khai thác gây lỗi tràn bộ đệm dẫn đến dịch vụ bị chấm đứt. Lỗi chủ yếu được tìm thấy trên các ứng dụng mạng nội bộ của Windows, trên các chương trình webserver, DNS, hay SQL database. Cập nhật bản vá (Tiếng anh là: Patching) là một trong những yêu cầu quan trọng cho việc phòng ngừa. Trong thời gian chưa thể cập nhật toàn bộ mạng, hệ thống phải được bảo vệ bằng bản vá ảo (Tiếng anh là: Virtual Patch). Ngoài ra, hệ thống cần đặc biệt xem xét những yêu cầu trao đổi nội dung giữa client và server, nhằm tránh cho server chịu tấn công qua các thành phần gián tiếp (Ví dụ SQL Injection).

5.2 Phòng ngừa việc tuyển mộ zombie:

Zombie là các đối tượng được lợi dụng trở thành thành phần phát sinh tấn công. Một số trường hợp điển hình như thông qua rootkit, hay các thành phần hoạt động

đính kèm trong mail, hoặc trang web, Ví dụ như sử dụng các file jpeg khai thác lỗi của phần mềm xử lý ảnh, các đoạn mã đính kèm theo file flash, hoặc trojan cài đặt theo phishing, hay thông qua việc lây lan worm (Netsky, MyDoom, Sophos). Để phòng chống, hệ thống mạng cần có những công cụ theo dõi và lọc bỏ nội dung (Tiếng anh là: Content Filtering) nhằm ngăn ngừa việc tuyển mộ zombie của hacker.

5.3 Ngăn ngừa kênh phát động tấn công sử dụng công cụ:

Có rất nhiều các công cụ tự động tấn công DoS, chủ yếu là tấn công phân tán DDoS như TFN, TFN2000 (Tribe Flood Network) tấn công dựa trên nguyên lý Smurf, UDP, SYN, hay ICMP; Trinoo cho UDP flood; Stacheldraht cho TCP ACK, TCP NULL, HAVOC, DNS flood, hoặc tràn ngập TCP với packets headers ngẫu nhiên. Các công cụ này có đặc điểm cần phải có các kênh phát động để zombie thực hiện tấn công tới một đích cụ thể. Hệ thống cần phải có sự giám sát và ngăn ngừa các kênh phát động đó.

5.4 Ngăn chặn tấn công trên băng thông:

Khi một cuộc tấn công DDoS được phát động, nó thường được phát hiện dựa trên sự thay đổi đáng kể trong thành phần của lưu lượng hệ thống mạng. Ví dụ một hệ thống mạng điển hình có thể có 80% TCP và 20% UDP và ICMP. Thống kê này nếu có thay đổi rõ rệt có thể là dấu hiệu của một cuộc tấn công. Slammer worm sẽ làm tăng lưu lượng UDP, trong khi Welchi worm sẽ tạo ra ICMP flood. Việc phân tán lưu lượng gây ra bởi các worm đó gây tác hại lên router, firewall, hoặc cơ sở hạ tầng mạng. Hệ thống cần có những công cụ giám sát và điều phối băng thông nhằm giảm thiểu tác hại của tấn công dạng này.

5.5 Ngăn chặn tấn công qua SYN:

SYN flood là một trong những tấn công cổ nhất còn tồn tại được đến hiện tại, dù tác hại của nó không giảm. Điểm căn bản để phòng ngừa việc tấn công này là khả năng kiểm soát được số lượng yêu cầu SYN-ACK tới hệ thống mạng.

5.6 Phát hiện và ngăn chặn tấn công tới hạn số kết nối:

Bản thân các server có một số lượng tới hạn đáp ứng các kết nối tới nó. Ngay bản thân firewall, các kết nối luôn được gắn liền với bảng trạng thái có giới hạn dung lượng. Đa phần các cuộc tấn công đều sinh số lượng kết nối ảo thông qua việc giả mạo. Để phòng ngừa tấn công dạng này, hệ thống cần phân tích và chống được spoofing. Giới hạn số lượng kết nối từ một nguồn cụ thể tới server (Quota).

5.7 Phát hiện và ngăn chặn tấn công tới hạn tốc độ thiết lập kết nối:

Một trong những điểm các server thường bị lợi dụng là khả năng các bộ đệm giới hạn giành cho tốc độ thiết lập kết nối, dẫn đến quá tải khi phải chịu sự thay đổi đột ngột về số lượng sinh kết nối. Ở đây việc áp dụng bộ lọc để giới hạn số lượng kết nối trung bình rất quan trọng. Một bộ lọc sẽ xác định ngưỡng tốc độ kết nối cho từng đối tượng mạng. Thông thường, việc này được bằng số lượng kết nối trong thời gian nhất định để cho phép sự dao động trong lưu lượng.

Các phân tích ở trên được dựa trên những ngầm định cơ bản trong việc bảo vệ hệ thống sau đây:

1. Các thiết bị bảo vệ cần được đặt trên luồng thông tin và thực hiện trực tiếp việc ngăn ngừa. Điều này xuất phát từ lý do cho tốc độ của một cuộc tấn công (Ví dụ khoảng 10.000 đăng ký thành viên trên 1s hướng tới 1 server, hoặc phát tán worm với tốc độ 200ms trên hệ thống mạng Ethernet 100M). Với tốc độ như vậy, cách thức phòng ngừa dạng phát hiện – thông báo ngăn chặn (Host Shun và TCP Reset) không còn phù hợp.

2. Các cuộc tấn công từ chối dịch vụ chủ yếu nhắm tới khả năng xử lý của hệ thống mạng mà đầu tiên là các thiết bị an ninh thông tin. Năng lực xử lý của IPS hoặc các thành phần content filtering là một trong những điểm cần chú ý, đặc biệt ở sự ổn định trong việc xử lý đồng thời các loại lưu lượng hỗn tạp với kích thước gói tin thay đổi.

3. Các cuộc tấn công luôn được tích hợp với sự tổng hợp các phương thức khác nhau. Chính vì vậy, tầm quan trọng của việc phòng ngừa những dấu hiệu lây nhiễm đơn giản là bước đầu tiên để ngăn chặn những cuộc tấn công từ chối dịch vụ.

III. SOCIAL ENGINEERING:

Không có một giải pháp bảo mật hoàn chỉnh nào có thể bảo đảm an toàn cho những lỗ hổng do chính bản thân con người gây ra. Nhắm vào nhược điểm đó, kỹ thuật lừa đảo (Tiếng anh là: Social Engineering) ra đời nhằm khai thác triệt để những yếu điểm từ chính bản thân con người.

1. Tìm hiểu về Social Engineering:

Social Engineering là một phương pháp tấn công vào các mục như: Quá trình ủy quyền, tường lửa, mạng riêng ảo, phần mềm theo dõi màn hình.

Có một số cách và thủ thuật lấy những thông tin nhạy cảm như: Dựa vào sự tín nhiệm trong công việc của công ty, sự sợ hãi của nhân viên và yêu cầu trợ giúp.

Social Engineering có thể lấy các thông tin như: Các thông tin nhạy cảm, ủy quyền, truy cập, ...

2. Đặc điểm của Social Engineering:

Người ta thường có những điểm yếu trong các chuỗi bảo mật. Vì vậy, muốn phòng thủ tốt thì doanh nghiệp hay tổ chức phải có chính sách đào tạo nhân viên hợp lý.

Social Engineering là một trong những hình thức tấn công khó khăn nhất vì nó không phụ thuộc nhất định vào phần cứng hay phần mềm.

3. Rebecca và Jessica:

Hacker sử dụng từ "**Rebecca"** và **"Jessica"** biểu thị cho kỹ thuật tấn công Social Engineering. Hai từ này có nghĩa là nạn nhân ở mục tiêu mà Hacker có thể dễ dàng thực hiện Social Engineering, ví dụ như người tiếp tân của công ty.

Mỗi công ty thường có một người tiếp tân, đối với những người này, Hacker thường gọi điện hoặc tiếp xúc trực tiếp tìm hiểu một số thông tin thô về mục tiêu.

Ví dụ:

Một Hacker khi muốn tìm hiểu các thông tin về ngân hàng, anh ta sẽ gọi điện cho cô Rebecca (Tiếp tân hoặc nhân viên tổng đài) tìm hiểu một số thông tin sơ bộ về ngân hàng mà anh ta chuẩn bị thâm nhập.

Hacker cũng có thể giả dạng là một khách hàng trực tiếp đến ngân hàng gặp Jessica tìm hiểu về một số chính sách của ngân hàng.

4. Nhân viên văn phòng:

Bất chấp mục tiêu có tường lửa, hệ thống phát hiện xâm nhập hay hệ thống chống Antivirus tốt, Hacker vẫn có thể tìm cách đánh vào lỗ hổng bảo mật.

Một công ty của bạn thiếu những động lực hay những chính sách tốt thúc đẩy sự cống hiến và phương pháp làm việc của nhân viên, thì họ rất có thể là mục tiêu tốt để Hacker khai thác thông tin.

Đối với nhân viên văn phòng, Hacker có thể dùng kỹ thuật Social Engineering lấy các thông tin như: Các chính sách bảo mật, các tài liệu nhạy cảm, mô hình cấu trúc của mạng văn phòng, các mật khẩu.

5. Các loại Social Engineering:

5.1. Dựa vào cá nhân:

Với kỹ thuật này, Hacker có thể lấy các thông tin nhạy cảm thông qua các mối tương tác bằng việc đánh vào các mục như: lòng tin, nỗi sợ hãi và yêu cầu trợ giúp.

5.1.1 Gửi thông điệp cho người dùng hợp lệ:

Với kỹ thuật Hacker thường lấy các thông tin nhạy cảm.

Ví dụ: "Chào chị X, tôi tên là Y, nhân viên văn phòng Z. Tôi đã quên mật khẩu đăng nhập vào hệ thống. Chị có thể giúp tôi lấy lại mật khẩu không?"

5.1.2 Gửi thông điệp cho người dùng quan trọng:

Hacker thường sử dụng kỹ thuật này để lấy các thông tin quan trọng như: Danh sách khách hàng, những tài liệu liên quan đến chiến lược của côngty, ...

Ví dụ: "Xin chào, tôi là C, thư ký của công ty X và hiện đang làm việc trong dự án của công ty. Tôi đã quên mật khẩu hệ thống, ông có thể giúp tôi lấy lại chúng được chứ ?"

5.1.3 Gửi thông điệp cho người hỗ trợ kỹ thuật:

Hacker có thể yêu cầu nhân viên kỹ thuật cấp lại tài khoản và mật khẩu hệ thống bằng cách gửi thông điệp yêu cầu.

Ví dụ: "Thưa ông A, giám đốc kỹ thuật công ty B. Tối qua hệ thống của chúng ta bị treo, bây giờ chúng ta hãy kiểm tra lại xem dữ liệu có bị mất không? Nhân tiện, xin ông vui lòng cấp lại tài khoản và mật khẩu cho tôi."

5.1.4 Nghe lén cuộc đàm thoại:

Nghe lén cuộc đàm thoại cũng là một trong những kỹ năng quan trọng của kỹ thuật Social Engineering. Cách này được Hacker đánh rất cao.

Kỹ thuật được áp dụng trong mục này: Đặt các thiết bị nghe trộm tại nơi có cuộc đàm thoại, rà theo sóng của đối phương, đặt camera theo dõi hoạt động của đối phương hoặc hóa trang thành một nhân viên phục vụ nghe lén.

5.1.5 Nhìn lén từ phía sau:

Nhìn lén phía sau lưng cũng là một cách của kỹ thuật Social Engineering. Khi có điều kiện vào trong phòng làm việc của công ty nào đó, Hacker áp dụng cả kỹ thuật này để theo dõi tài khoản và mật khẩu đăng nhập hệ thống.

Cách nhìn lén này không có nghĩa là ta chỉ quan sát bằng mắt thường mà còn áp dụng cả yếu tố kỹ thuật nữa. Hacker thường gắn cả camera lên những vị trí thuận tiện và kín đáo trên người để tiện theo dõi quá trình đăng nhập của nhân viên. Camera ghi

lại và phân tích những thông tin trong những điều kiện phù hợp.

Những thông tin theo dõi bằng cách này có thể là: tài khoản và mật khẩu hệ thống, mật khẩu ngân hàng, mật khẩu cơ sở dữ liệu.

5.1.6 Tìm thông tin từ rác văn phòng:

Thu thập thông tin từ rác văn phòng cũng là một cách tốt. Với cách này, Hacker có thể tìm các loại thông tin như: Các tài liệu trong thùng rác, rác in ấn, các tài liệu văn phòng bị bỏ đi, ...

Thông tin thu thập có thể là: Hóa đơn điện thoại, thông tin liên hệ, thông tin tài chính, những thông tin liên quan đến điều hành, ...

Để thu thập thông tin này, Hacker thường hóa trang thành người dọn vệ sinh trong công ty. Anh ta thu thập tất cả tài liệu liên quan đến công ty trong những rác bỏ đi.

5.1.7 Thu thập thôngtin:

Ở mỗi người: Nhìn chung, với mỗi người ở công ty mục tiêu, Hacker có thể thu thập các thông tin như: Các kỹ thuật hiện hành, thông tin liên hệ, ...

Ủy quyền cho người thứ ba: Hỏi những người có vị trí quan trọng trong tổ chức mục tiêu để thu thập dữ liệu.

Ví dụ:"Thưa bà X! Hôm qua, Ông Y giám đốc tài chính của công ty mình hỏi tôi về báo cáo kiểm toán tháng này của công ty. Vậy trong hôm nay, bà vui lòng cung cấp những báo cáo này cho tôi nhé!".

5.2 Dựa vào máy tính:

5.2.1 Pop-up của Windows:

Pop-up của Windows là những hộp thoại quảng cáo xuất hiện đột ngột khi người dùng duyệt website hoặc truy cập Internet. Những hộp thoại này yêu cầu người dùng đăng nhập hoặc đăng ký tài khoản trên website nào đó.

5.2.2 Hoaxes và Chain letters:

Hoaxes letters: là các emails đưa ra các thông báo đến người dùng một loại Virus, Trojan hoặc Worm mới có thể làm tổn hại đến hệ thống người dùng.

Chain letters: là các emails chứa thông điệp mời người dùng nhận các quà tặng miễn phí như: Tiền, phần mềm với điều kiện là người dùng phải hồi đáp lại các địa chỉ emails và điền đầy đủ các thông tin cá nhân của họ theo khuôn mẫu định sẵn.

5.2.3 Thông điệp chat:

Lấy thông tin người dùng bằng cách Chat trực tiếp với họ, những thông tin thu thập có thể là: Ngày tháng năm sinh, tên thật, ...

Dữ liệu có thể dùng cho việc bẻ khóa tài khoản của người dùng.

5.2.4 Thư rác:

Những emails gửi đi mà không cần quyền ưu tiên, mục này chủ yếu là dành cho quảng cáo thương mại.

Thông tin thu thập từ những email gửi đi này bao gồm: Các thông tin tài chính, thông tin mạng, ...

5.2.5 Phishing:

Là những email không hợp lệ từ các trang hợp lệ. Chúng xuất hiện, yêu cầu người dùng cung cấp các thông tin về tài khoản hợp lệ về tài khoản của họ.

Phishing có thể sử dụng các mồi nhử như:

- Kiểm tra lại tài khoản của bạn.
- Cập nhật lại các thông tin cá nhân.
- Tài khoản của bạn có thể bị khóa hoặc ngưng hoạt động, ...

Để hạn chế và ngăn chặn Phishing, bạn có thể sử dụng cá công cụ tích hợp có sẵn vào trình duyệt.

5.3 Tấn công bằng tay trong:

Nếu áp dụng các hình thức khai thác không được, kẻ tấn công có thể lợi dụng cơ chế tuyển dụng của mục tiêu để cài người của họ vào hệ thống mục tiêu. Người mà Hacker gửi vào là những người giỏi và có thể vượt qua các cuộc phỏng vấn một cách dễ dàng. Khi đã an toàn trong hệ thống mục tiêu, Hacker thục hiện khai thác thông tin mật của đối phương và gửi ra ngoài.

Những cuộc tấn công từ phía trong hệ thống (Bên trong tường lửa) mức độ thành công là 60%. Các cuộc tấn công này rất dễ thực hiện và rất khó ngăn chặn. Hầu như rất khó phát hiện ra kẻ tấn công.

5.4 Ngăn chặn tấn công tay trong:

Không có giải pháp đơn giản nào có thể ngăn chặn các mối hiểm họa từ bên trong hệ thống. Sau đây là một số giải pháp tình huống có thể hạn chế tấn công từ bên trong:

- Phân chia nhiệm vụ riêng và rõ ràng cho từng người.
- Thay đổi nhiệm vụ của nhân viên theo kỳ.

- Cấp đặc quyền tối thiểu.
- Điều khiển truy cập.
- Theo dõi và kiểm tra thông tin trong file log.
- Có các chính sách hấp dẫn.
- Có các chính sách lưu trữ dữ liệu hợp lý.

6. Mục tiêu tiếp cận của Social Engineering:

- Người tiếp tân.
- Người hỗ trợ nhân sự.
- Các chi nhánh của tổ chức mục tiêu.
- Người dùng và quản trị viên hệ thống.

7. Các nhân tố dẫn đến tấn công:

- Thiếu nhận thức về bảo mật và các thông tin bảo mật.
- Cá nhân hóa các các đơn vị tổ chức.
- Thiếu các chính sách bảo mật thích hợp.
- Dễ dàng truy cập các địa chỉ email và số điện thoại.

8. Tại sao Social Engineering có thể dễ thực hiện ?

- Các chính sách bảo mật mạnh nhưng vẫn còn những điểm yếu đó là: Con người là nhân tố dễ bị ảnh hưởng nhất.
- Rất khó phát hiện ra kỹ thuật Social Engineering.
- Không có phương pháp phòng chống hiệu quả.
- Không có phần mềm hay phần cứng phát hiện kỹ thuật Social Engineering.

9. Các dấu hiệu nhận dạng Hacker:

Một Hacker có những biểu hiện sau:

- Có những yêu cầu khác thường.
- Yêu cầu ủy quyền.
- Có biểu hiện vội vã.
- Không thường xuyên khen hoặc ca ngợi một ai đó trong tổ chức.
- Biểu hiện bối rối khi bị thẩm vấn.
- Đe dọa đối phương nếu không cung cấp thông tin.

10. Các giai đoạn của Social Engineering:

10.1. Nghiên cứu công ty mục tiêu:

Để nghiên cứu công ty mục tiêu, Hacker thường dựa vào các thông tin thu thập

như: Tài liệu rác, website, nhân viên hay trong quá trình thăm quan công ty.

10.2. Chọn lựa nạn nhân:

Trong Social Engineering , Hacker sẽ chọn nạn nhân là những nhân viên rất "nhẹ dạ cả tin", từ những nhân viên này anh ta sẽ thu thập rất nhiều thông tin.

10.3. Phát triển mối quan hệ:

Khi đã chọn lựa nạn nhân thích hợp để khai thác thông tin, Hacker sẽ phát triển mối quan hệ này ngày một tốt đẹp hơn để Social Engineering lâu dài.

10.4. Tận dụng các mối quan hệ:

Khi mối quan hệ đã đạt tới múc tốt đẹp, Hacker sẽ tận dụng các mối quan hệ tốt đẹp này để khai thác các thông tin như:

- Những thông tin về tài khoản người dùng.
- Khai thác các báo cáo tài chính.
- Khai thác các thông tin kỹ thuật của mục tiêu.

11. Thâm nhập vào điểm yếu trong giao tiếp:

Dựa vào những yếu điểm trong giao tiếp, Hacker thực hiện các hoạt động dựa vào tâm lý cá nhân.

11.1. Sự tín nhiệm:

Bằng một hình thức nào đó, Hacker thâm nhập vào công ty đối thủ qua con đường tuyển dụng. Lúc này, Hacker phát triển mối quan hệ và dần lấy được sự tín nhiệm của giám đốc và lòng tin của nhân viên. Hacker sẽ thực hiện tấn công từ bên trong qua các mối quan hệ này để khai thác thông tin.

11.2. Sự ngây ngô:

Những người không có nhiều hiểu biết về bảo mật và không cảnh giác trong trong giao tiếp luôn là mục tiêu của Social Engineering. Từ điểm yếu này, Hacker có thể dễ dàng thâm nhập mục tiêu.

11.3. Sự sợ hãi của nhân viên:

Khi áp dụng nhiều phương pháp mà không khai thác được các thông tin cần thiết, Hacker sẽ thực hiện giải pháp cuối cùng đó là đe dọa. Đe dọa chia làm hai loại:

- Đe dọa bạo lực: Đây là phương pháp dùng bạo lực để ép lấy thông tin. Phương pháp này rất hiếm khi sử dụng trong kỹ thuật Social Engineering vì nó sẽ để lại dấu vết và rất có thể sẽ nhanh chóng bị phát hiện.

- Dựa vào thái độ của nhân viên: Căn cứ vào những điểm yếu trong tâm lý của

nhân viên, Hacker có thể khai thác các thông tin. Điều này có nghĩa là: Hacker phát hiện thấy nhân viên hay đồng nghiệp của mình thường hay sợ điều gì nhất, từ đó anh ta tiến hành đe dọa. Hoặc Hacker phát hiện thấy nhân viên có hành động mờ ám trong công việc, điều này anh ta thực hiện đe dọa để khai thác thông tin.

11.4. Sự tham lam:

Đây là yếu tố cơ bản nhất của con người. Dựa vào yếu điểm này, Hacker có thể đưa ra những mồi nhử hấp dẫn như: Tiền, sự thăng tiến, quà tặng, … để khai thác thông tin.

11.5. Trách nhiệm trong công việc:

Khi đã chiếm được sự tín nhiệm của giám đốc, lúc này, mục tiêu sẽ bị thâm nhập dễ dàng hơn. Vì từ đây, căn cứ vào những yêu cầu trong công việc, anh ta có thể hỏi những thông tin cần thiết phục vụ cho công việc của anh ta trông công ty này.

12. Các phương pháp đối phó:

12.1. Đào tạo nhân viên:

Để hạn chế những cuộc thâm nhập kiểu Social Engineering, công ty của bạn phải có chính sách đào tạo nhân viên tốt, giúp nhân viên nhận ra các phương pháp tấn công của Hacker theo phương pháp này.

12.2. Chính sách mật khẩu:

Để hạn chế các cuộc thâm nhập hệ thống, nhân viên quản trị bảo mật phải cấu hình những chính sách bảo mật mật khẩu thích hợp như:

- Thường xuyên thay đổi mật khẩu.
- Vô hiệu hóa tài khoản Guest.
- Khóa tài khoản sau bao nhiêu lần (Số lần đăng nhập) đăng nhập không thành công.
- Độ dài và độ phức tạp của mật khẩu.

12.3. Đường lối lãnh đạo:

Các thông tin nhạy cảm phải được bảo mật. Nếu những thông tin này mang ra sử dụng thì phải được ủy quyền truy cập.

12.4. Các chính sách bảo mật ở mức vật lý:

Có dấu hiệu nhận diện nhân viên như: phát hành ID Card (Thẻ nhận diện nhân viên), đồng phục, …

Theo dõi và quản lý khách viếng thăm.

Tạo ra những khu vực riêng biệt hạn chế người vào.

Hủy tài liệu bằng những phương pháp bảo mật khi không còn dùng đến nữa.

Có chính sách bảo mật nhân sự.

12.5. Phân loại thông tin:

Thông tin tuyệt mật: Đây là những loại thông tin chỉ dành cho những người có trách nhiệm cao nhất mới được xem và quản lý.

Thông tin nội bộ: Những thông tin chỉ được sử dụng ở môi trường nội bộ công ty.

Thông tin cộng đồng: Đây là những loại thông tin có thể tùy ý sử dụng.

12.6. Đặc quyền truy cập:

Tài khoản Administrator, User và Guest phải ủy quyền truy cập đúng đắn.

Tạo ra các chính sách truy cập tài nguyên hợp lệ và cấp đặc quyền tối thiểu cho những loại tài nguyên trên.

12.7. Kiểm tra nhân viên:

Đặt ra các chính sách giám sát nhân viên một cách chặt chẽ, thường xuyên kiểm tra theo dõi và phát hiện kịp thời những thâm nhập bất hợp pháp.

CHƯƠNG III: PHƯƠNG PHÁP PHÁT HIỆN XÂM NHẬP

Để một hệ thống của công ty nói chung và máy tính của bạn nói riêng được an toàn trong mọi tình huống thì ngoài việc chọn cho máy tính một chương trình diệt Virus đủ mạnh, một tường lửa hiệu quả thì bạn cần hải có một chương trình giúp kiểm tra và phát hiện xâm nhập – Intrusion Detect System (Viết tắt là: IDS).

I. TÌM HIỂU VỀ MỘT SỐ HỆ THỐNG IDS:

1. Giới thiệu:

Các Hacker luôn tìm những mạng máy tính có khả năng thỏa hiệp để phát hiện những lỗ hổng mà Hacker tìm được.

Lựa chọn và điều chỉnh các thiết lập phù hợp trong mạng máy tính của bạn có thể dễ dàng ngăn chặn các truy cập của Hacker.

IDS, Firewall và Honeypot là các kỹ thuật quan trọng có thể giúp ngăn chặn hiệu quả thâm nhập của Hacker từ những mạng thỏa hiệp.

2. Một số thuật ngữ:

Intrusion Detect System (IDS): Đây là hệ thống phát hiện xâm nhập. Chức năng chính của nó là kiểm tra tất cả các hoạt động của mạng: vào và ra, xác định những mẫu đáng nghi ngờ, từ đó chỉ ra một cuộc tấn công có thể xảy ra từ hệ thống thỏa hiệp.

Firewall: Là một chương trình phần mềm hoặc một thiết bị phần cứng có khả năng bảo vệ tài nguyên của mạng riêng từ người dùng hoặc từ những mạng khác.

Honeypot: Là một hệ thống tài nguyên thông tin được xây dựng với mục đích giả dạng, đánh lừa những người sử dụng và kẻ xâm nhập không hợp pháp, thu hút sự chú ý của chúng, ngăn không cho chúng tiếp xúc với hệ thống thật. Honeypot có thể giả dạng bất cứ loại máy chủ nào như: Mail Server, Domain Name Server, Web Server, …. Honeypot sẽ trực tiếp tương tác với tin tặc và tìm cách khai thác thông tin về tin tặc như hình thức tấn công, công cụ tấn công hay cách thức tiến hành.

II. HỆ THỐNG PHÁT HIỆN XÂM NHẬP IDS:

1. Giới thiệu về IDS:

IDS là một hệ thống giám sát lưu thông mạng để từ đó tìm ra các hoạt động khả nghi và đưa ra cảnh báo cho hệ thống và người quản trị. Ngoài ra, IDS cũng đảm nhận

việc phản ứng lại các lưu thông bất thường hay có hại bằng các hành động đã được thiết lập từ trước.

IDS còn có thể phân biệt giữa những tấn công từ bên trong (từ những người trong công ty) hay tấn công từ bên ngoài (từ các Hacker). IDS phát hiện dựa trên các dấu hiệu đặc biệt về các nguy cơ đã biết (giống như các phần mềm diệt virus dựa vào các dấu hiệu đặc biệt để phát hiện và diệt virus) hay dựa trên so sánh lưu thông mạng hiện tại với baseline (Thông số chuẩn được thiết lập sẵn trong hệ thống) để tìm ra các dấu hiệu bất thường. Các IDS thường cho phép người quản trị tự định nghĩa các dấu hiệu mẫu (Các luật) cho việc phát hiện xâm nhập, tấn công. Ngoài ra, một phương pháp đang được tập trung nghiên cứu là phát hiện dựa trên mô hình, để làm cho IDS có khả năng tự học và suy luận thông minh khi có các tấn công mới.

2. Chức năng của IDS:

2.1. Chức năng chính:

Chức năng chính và quan trọng nhất của một hệ thống IDS là giám sát, cảnh báo và bảo vệ.

- Giám sát: Giám sát các lưu lượng mạng, các hành động bất thường và các hoạt động khả nghi.
- Cảnh báo: Khi đã biết các hoạt động bất thường của một (hoặc một nhóm) truy cập nào đó, IDS sẽ đưa ra cảnh báo cho hệ thống và người quản trị.
- Bảo vệ: Dùng những thiết lập mặc định và những cấu hình từ người quản trị để có những hành động chống lại kẻ xâm nhập và phá hoại.

2.2. Chức năng mở rộng:

Phân biệt tấn công từ bên trong và bên ngoài: Đây là chức năng rất hay của IDS, nó có thể phân biệt được đâu là những truy cập hợp lệ (Không hợp lệ) từ bên trong và đâu là cuộc tấn công từ bên ngoài vào hệ thống.

Phát hiện: Dựa vào sự so sánh lưu lượng mạng hiện tại với baseline, IDS có thể phát hiện ra những dấu hiệu bất thường và đưa ra cảnh báo và bảo vệ ban đầu cho hệ thống.

3. Nơi đặt IDS:

Giả sử ta có một mô hình mạng như hình 3.1 các thành phần chính của mô hình này như sau:

- Internal Network: Đây là hệ thống mạng cục bộ, gồm các máy trạm

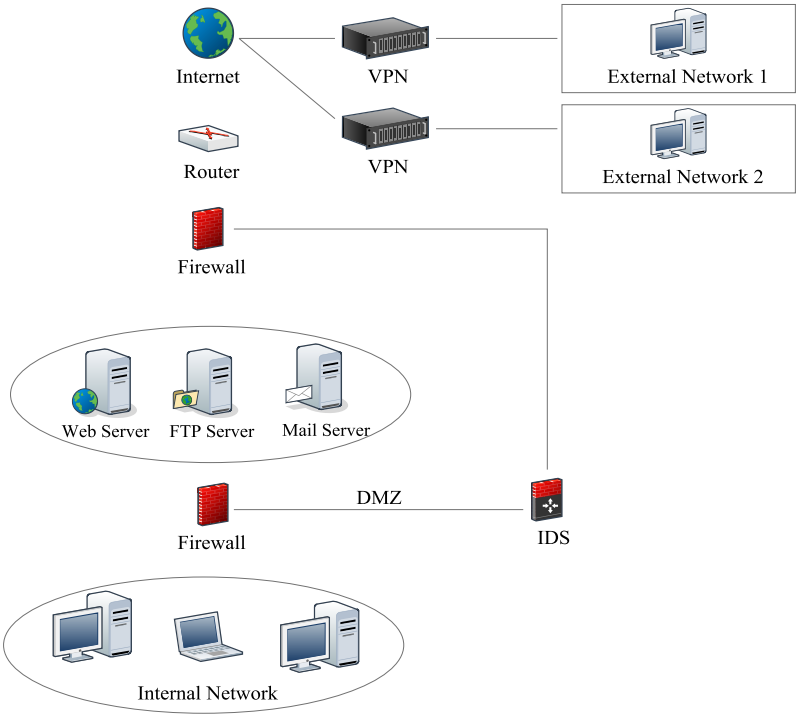
- Firewall: Trong hình này, ta sử dụng hai tường lửa và được đặt ở hai vị trí khác nhau.

- IDS: Hệ thống IDS được đặt tại hai tường lửa và hoạt động theo mô hình mạng DMZ.

- Web Server, FTP Server, Mail Server: Các Server này được bao quanh bằng tường lửa và hệ thống IDS để ngăn ngừa và phát hiện các cuộc tấn công cả bên trong lẫn bên ngoài.

- Router: Hệ thống định tuyến, được dùng để truy cập Internet.

- External Network 1,2: Là hai hệ thống mạng độc lập và liên lạc với nhau thông qua VPN (Virtal Private Network)



Hình 3.1: Nơi đặt IDS.

4. Phân loại IDS:

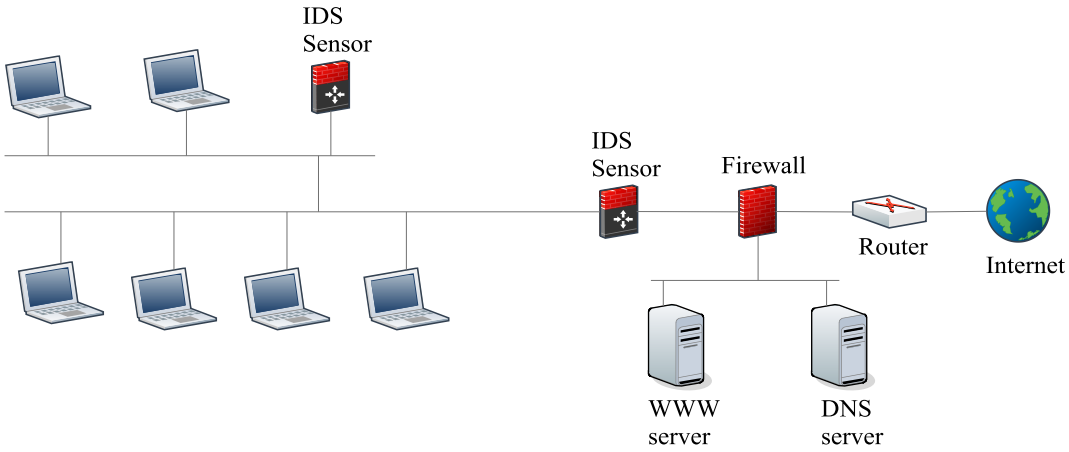
1.1. Network Based IDS (NIDS):

NIDS được đặt trên mạng như một thành phần của đường truyền và thường đặt sau Firewall để phát hiện xâm nhập trái phép từ Internet cho toàn bộ hệ thống mạng nội bộ. Hoặc NIDS có thể đặt tại các phân vùng mạng có nguy cơ tấn công cao mà cần phải được bảo vệ, Ví dụ như phân vùng DMZ, hay phân vùng đặt cơ sở dữ liệu và các phân vùng quan trọng. NIDS làm nhiệm vụ phân tích các gói tin và kiểm tra các dấu hiệu tấn công dựa trên một tập các dấu hiệu mẫu. Nếu phát hiện tấn công, NIDS sẽ ghi

vào log file hoặc gửi đi cảnh báo, cách thức cảnh báo phụ thuộc vào từng hệ thống IDS hoặc cách cấu hình.

Ưu điểm của NIDS: Cho phép quan sát toàn bộ cá gói tin đi qua một mạng hoặc một phân vùng mạng. Nó hoàn toàn trong suốt với người sử dụng và không làm ảnh hưởng đến hoạt động của một máy tính cụ thể nào; dễ dàng trong quản lý, duy trì hoạt động. Hoạt động phát hiện chủ yếu ở tầng mạng nên có thể độc lập với các ứng dụng và các hệ điều hành sử dụng tại máy tính trên mạng.

Hạn chế của NIDS: Thường có nhiều báo động nhầm. NIDS không có khả năng phát hiện được các tấn công trên các dòng dữ liệu đã được mã hóa như VPN, SSL, IPSec. Có thể xảy ra hiện tượng thát cổ chai khi lưu lượng mạng hoạt động ở mức cao.



Hình 3.2: Hệ thống phát hiện xâm nhập NIDS.

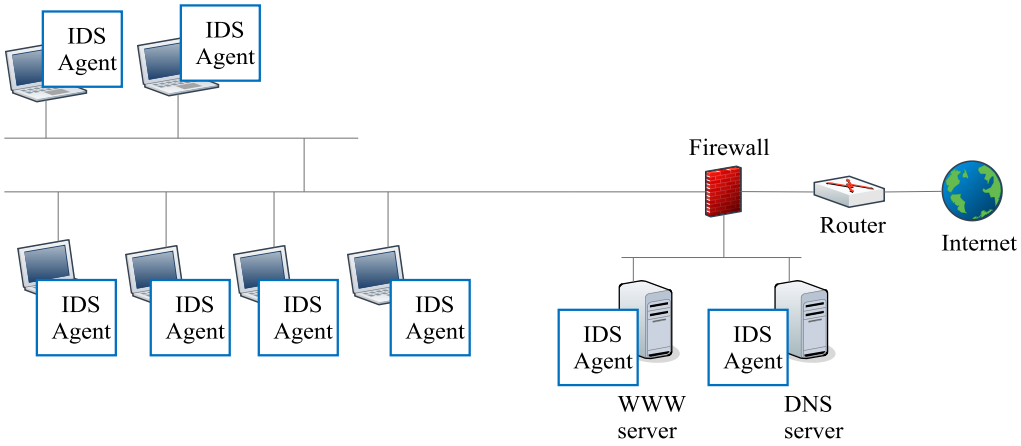
1.2. Host Based IDS (HIDS):

HIDS thường được cài đặt trên mỗi máy tính cần được bảo vệ, để giám sát các hành động trên các dịch vụ hoặc các máy tính có tài nguyên quan trọng và dễ bị tấn công, Ví dụ, máy chủ chạy các ứng dụng quan trọng như: Application Server, Web Server, Mail Server. HIDS thường phát hiện các tấn công dựa trên các hành động truy cập bất thường vào trong hệ thống và gây ra các thay đổi trên hệ thống như: tiến trình, giá trị Registry, thời gian sử dụng bộ nhớ, CPU, …

Ưu điểm của HIDS: Phát hiện các tấn công một cách chính xác hơn đối với từng dịch vụ hoặc từng máy tính. Cho phép ghi lại diễn biến các cuộc tấn công. Có khả năng phân tích các dữ liệu mã hóa.

Hạn chế của HIDS:Làm giảm năng lực xử lý và tiêu tốn các tài nguyên của máy

tính, tốn công sức hơn trong việc triển khai và duy trì, chỉ quan sát được các tấn công cục bộ và không thể phát hiện các cuộc dò quét mạng.



Hình 3.3: Hệ thống phát hiện xâm nhập HIDS.

III. ĐỀ XUẤT SỬ DỤNG GIẢI PHÁP HỆ THỐNG PHÁT HIỆN XÂM NHẬP SNORT:

1. Giới thiệu:

Snort là một IDS, nó là một chương trình được cài đặt trên mạng (hay một máy tính), nhiệm vụ của Snort là giám sát những gói tin vào ra hệ thống của bạn.

Nếu một cuộc tấn công được Snort phát hiện thì nó sẽ phản ứng lại bằng nhiều cách khác nhau phụ thuộc vào cấu hình mà người quản trị thiết lập, Ví dụ như nó có thể gửi thông điệp cảnh báo đến nhà quản trị hay loại bỏ gói tin phát hiện có sự cố bất thường trong các gói tin đó.

Tuy nhiên, Snort chỉ có thể chống lại các cuộc tấn công một cách hiệu quả nếu như nó biết được dấu hiệu (Tiếng anh là: Signature) của các cuộc tấn công đó. Dựa vào đặc điểm này, các Hacker có thể điều chỉnh các cuộc tấn công để thay đổi dấu hiệu của cuộc tấn công đó. Từ đó, các cuộc tấn công này có thể "qua mặt" giám sát của Snort.

Như vậy, để Snort hoạt động hiệu quả thì một trong những yếu tốt quan trọng cần phải chú ý là các luật viết cho Snort. Khi Snort hoạt động, nó sẽ đọc các tập luật, giám sát luồng dữ liệu chạy qua hệ thống và sẽ phản ứng nếu có bất kỳ luồng dữ liệu nào phù hợp với tập luật của nó.

Tập luật có thể được tạo ra để giám sát các công việc quét cổng (Tiếng anh là: Scanning), tìm dấu vết (Tiếng anh là: Footprinting) hoặc nhiều phương pháp khác mà

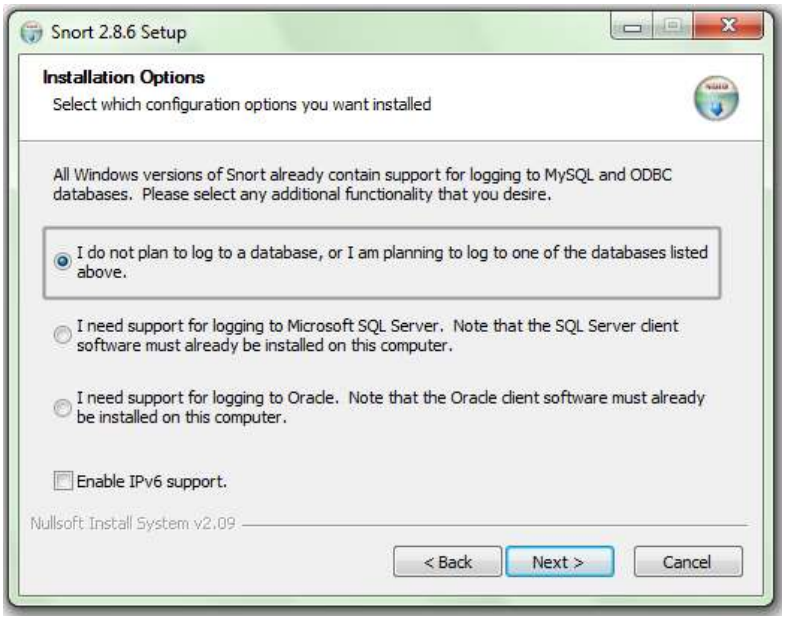
các Hacker dùng để tìm cách chiếm quyền hệ thống. Tập luật có thể được ra bởi người dùng hoặc truy cập đến trang chủ của Snort là: http://www.snort.org để tải về.

2. Cài đặt Snort:

Sử dụng phiên bản Snort: Snort2.8.6

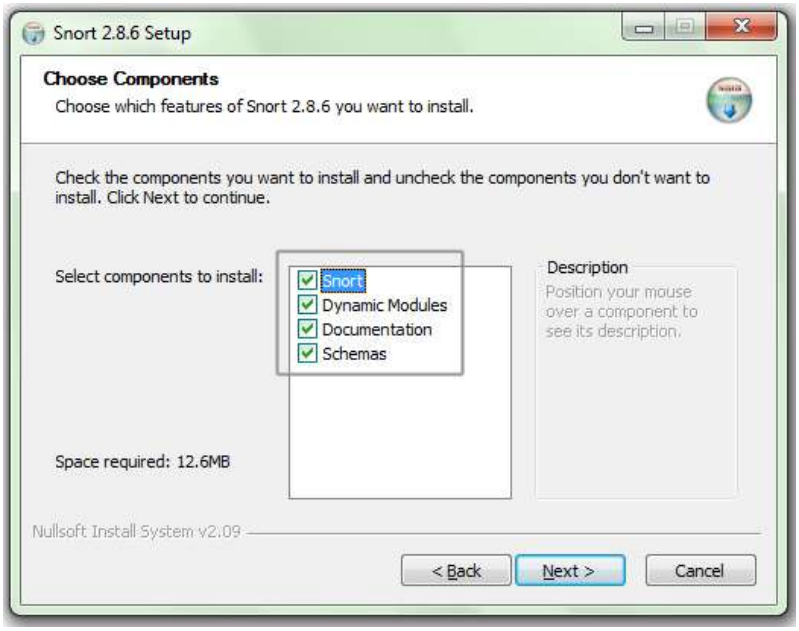
Tại trang License Agreement, nhân nút I Agree để chấp nhận các điều khoản sử dụng Snort.

Tại trang Installation Options, hãy xác định loại cơ sở dữ liệu mà bạn muốn chương trình hỗ trợ. Ví dụ, chọn I do not plan to log to a database, or I am planning to log to one of the database listed above, sau đó nhấn nút để Next tiếp tục.



Hình 3.4: Chọn đối tượng mà bạn muốn chương trình hỗ trợ.

Tại trang Choose Componets, đánh dấu chọn các thành phần cần cài đặt, sau đó nhấn nút Next để tiếp tục.



Hình 3.4: Chọn các thành phần cần cài đặt.

Tại trang Choose Install Location, nhấn nút Browse để thay đổi đường dẫn cài đặt chương trình, sau đó nhấn nút Next để cài đặt Snort. Trong mục này để mặc định là C:\Snort.

Sau khi cài đặt Snort thành công, máy tính sẽ có thêm thư mục Snort tại ổ C. Trong thưc mục C:\Snort có 1 số thư mục:

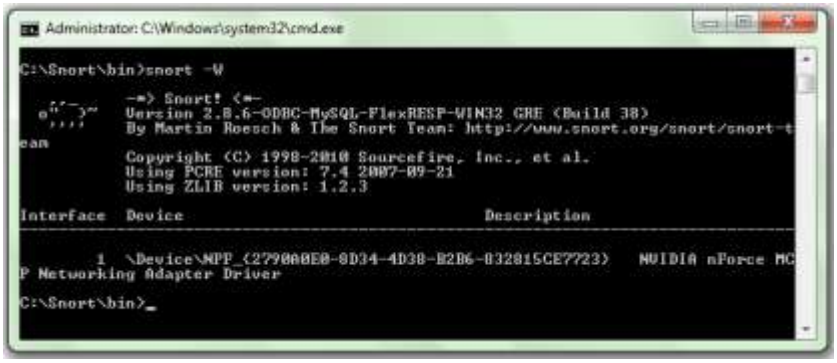
- Bin: Đây là thư mục chứa tập tin thực thi Snort.exe và một số tập tin DLL được gọi khi Snort chạy.
- Contrib: Thư mục này chứa một số chương trình liên kết và một số Add-ons của Snort.
- Doc: Thư mục này chứa các tùy chọn của Snort và một số mô tả về các dấu hiệu.
- Etc: Thư mục này chưa một số tập tin cấu hình của Snort như snort.conf.
- Log: Thư mục này chứa những tập tin nhật ký của chương trình. Khi mới cài đặt và chưa kích hoạt thì thư mục này chưa có tập tin nào.
- Rules: Đây là thư mục rất quan trọng vì nó chứa tất cả các tập tin luật của Snort.
- Schemas: Thư mục này chứa các mô hình cơ sở dữ liệu.

3. Cài đặt Rules cho Snort:

Sử dụng Rules cho Snort: snortrules-snapshot-2860.tar.gz

Giải nén tập tin đó và copy tất cả các thư mục con vào C:\Snort (ghi đè lên các tập tin đã tồn tại).

Kiểm tra sự hoạt động của Snort và WinPcap: Vào Command Prompt gõ lệnh Snort\bin\snort –W . Nếu WinPcap chưa được cài hoặc phiên bản cài đặt không đúng thì thông tin về Driver card mạng trong hệ thống không được hiển thị.

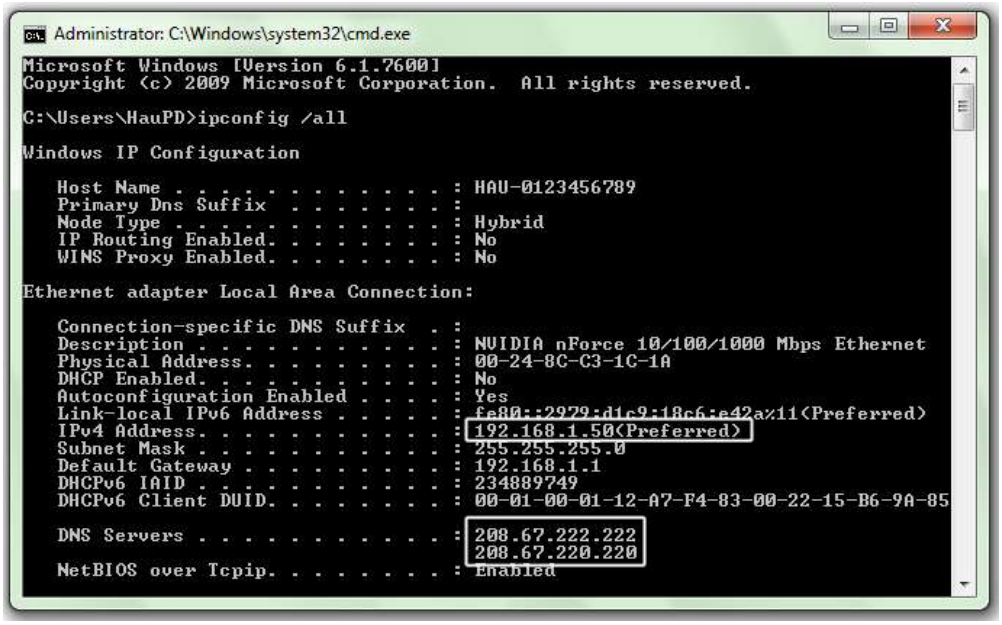


Hình 3.5: Kiểm tra hoạt động của Snort.

4. Cấu hình tập tin Snort.conf:

Tập tin Snort.conf điều khiển mọi thứ về Snort như: Snort sẽ giám sát cái gì, chúng tự bảo vệ ra sao, các luật nào được sử dụng để tìm lưu lượng nguy hiểm, …

Để cấu hình Snort.conf cần kiểm tra thông số IP Address, DNS Servers (Trong báo cáo tốt nghiệp em sẽ thử nghiệm trên máy tính của mình).

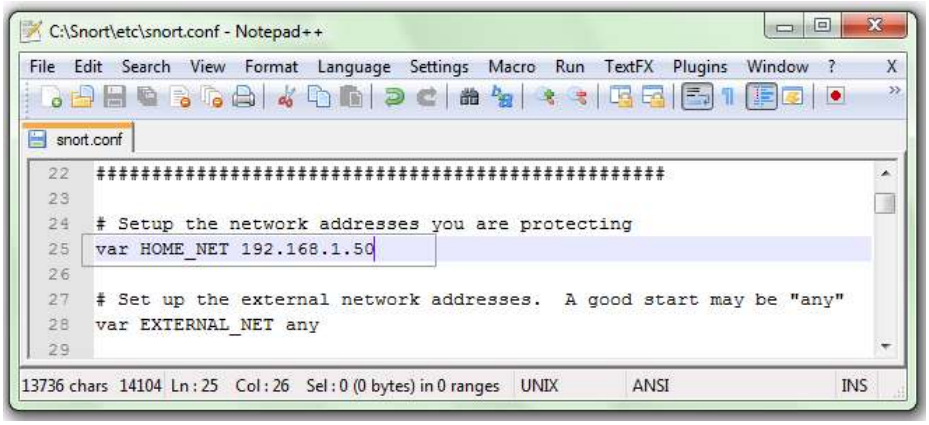


Hình 3.6: Kiểm tra thông số IP và DNS.

Mở tập tin Snort.conf trong thư mục C:\Snort\etc bằng bất kì trình soạn thảo nào (Trong mục này em sử dụng Notepad ++).

Khi tập tin Snort.conf được mở, tìm đến dòng **var HOME_NET any** và thay tham số any bằng địa chỉ IP trên máy tính cần bảo vệ, Ví dụ: 192.168.1.50.

Như vậy, sau khi đổi tham số any, biến mới của dòng **var HOME_NET any**sẽ thành**var HOME_NET 192.168.1.50.** Biến HOME_NET sẽ có chức năng báo cho Snort biết là nó sẽ bảo vệ cho hệ thống có địa chỉ IP là 192.168.1.50.



Hình 3.7: Nhập địa chỉ IP của hệ thống cần Snort bảo vệ.

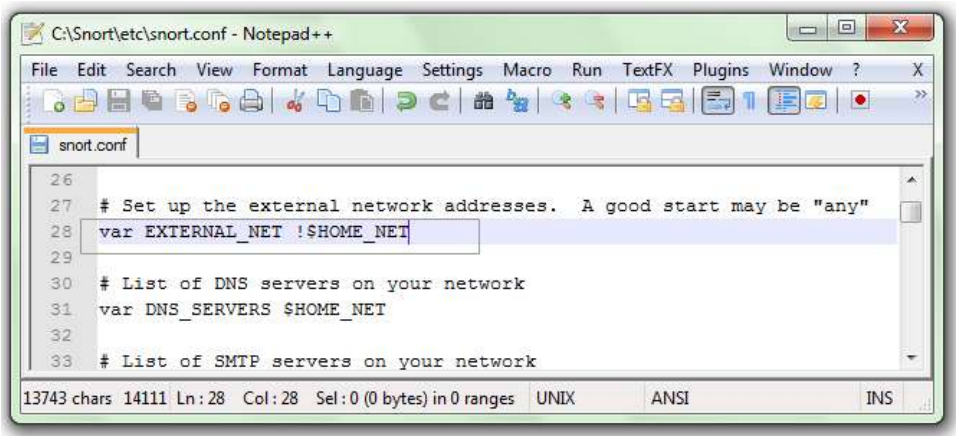
Bạn cũng có thể khai báo một miền địa chỉ IP bằng cách xác định địa chỉ mạng và số bít của Subnet Mask, Ví dụ muốn bảo vệ tất cả các địa chỉ IP của lớp mạng 192.168.1.0 và có Subnet Mask là 255.255.255.0 bạn có thể khai báo **var HOME_NET 192.168.1.0/24.**

Ngoài ra, bạn cũng có thể khai báo một nhóm các địa chỉ IP cần bảo vệ thay vì bảo vệ tòan bộ lớp mạng bằng cách đặt tất cả các địa chỉ IP cần bảo vệ thay vì bảo vệ toàn bộ lớp mạng bằng cách đặt tất cả các địa chỉ IP cần bảo vệ vào trong dấu ngoặc vuông ([ ]) và phân cách nhau bằng dấu phẩy (,) không có dấu khoảng trắng. Ví dụ, cần bảo vệ 3 địa chỉ IP là: 192.138.1.50, 10.10.0.1 và 176.16.0.1 bạn khai báo **var HOME_NET [192.168.1.50,10.10.0.1,176.16.0.1]**

Trong tập tin Snort.conf, tìm đến dòng **var EXTERNAL_NET any**và thay tham số **any** bằng **!$HOME_NET.**

Dấu chấm than (!) trong biến **!$HOME_NET** là cách gọi phủ định, điều này có nghĩa Snort sẽ xác định tất cả các địa chỉ IP trừ địa chỉ 192.168.1.50 là địa chỉ bên ngoài và không thuộc phạm vi bảo vệ của Snort.

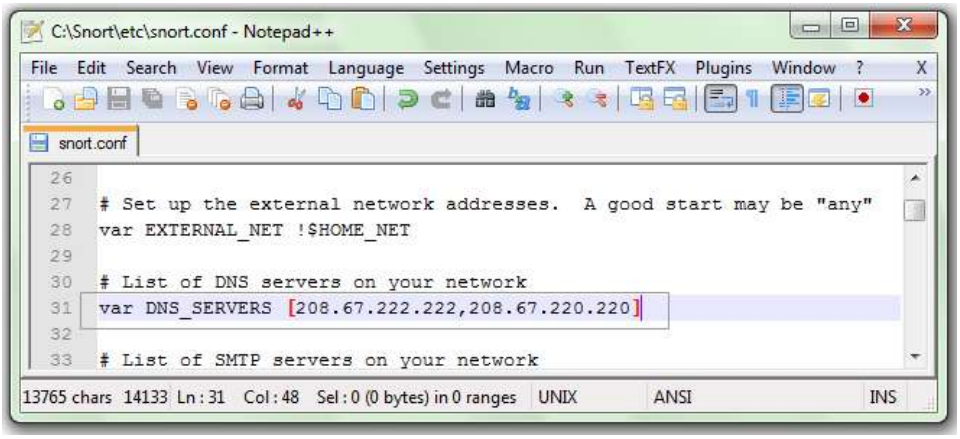
Khi gọi bất kỳ một biến nào trong tập tin Snort.conf thì bạn phải đặt ký tự $ lên đầu của biến được gọi.



Hình 3.8: Khai báo biến EXTERNAL_NET.

Tiếp theo, bạn tìm dòng **var DNS_SERVERS $HOME_NET**, sau đó thay tham số **$HOME_NET** bằng các địa chỉ IP của DNS Server.

Ví dụ, thay biến **$HOME_NET** bằng địa chỉ IP **[208.67.222.222,208.67.220.220]**. Sau khi thay giá trị khai báo thì dòng **var DNS_SERVERS $HOME_NET** thành **var DNS_SERVERS [208.67.222.222,208.67.220.220]**.

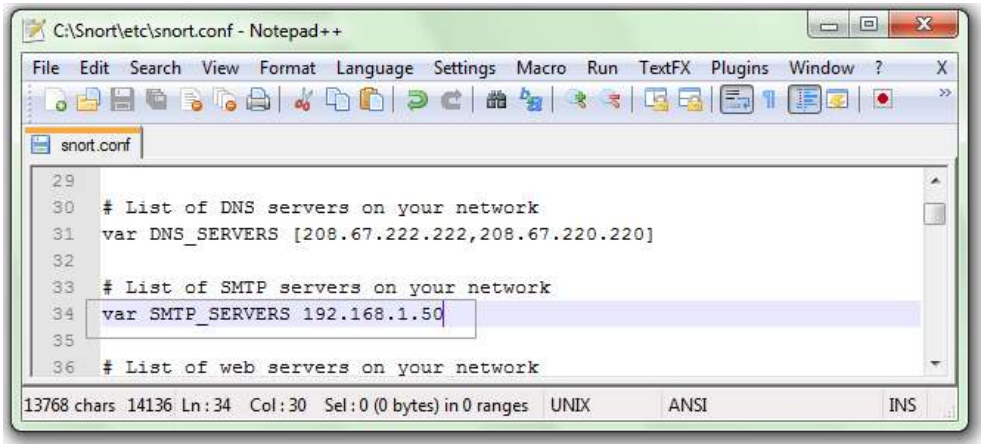


Hình 3.9: Khai báo biến DNS_SERVERS.

Tìm dòng **var SMTP_SERVERS $HOME_NET**và thay tham số **$HOME_NET** bằng địa chỉ IP trên máy tính của bạn.

Ví dụ, thay biến **$HOME_NET** bằng địa chỉ IP **192.168.1.50**. Sau khi thay giá trị khai báo thì dòng **var SMTP_SERVERS $HOME_NET** thành **var**

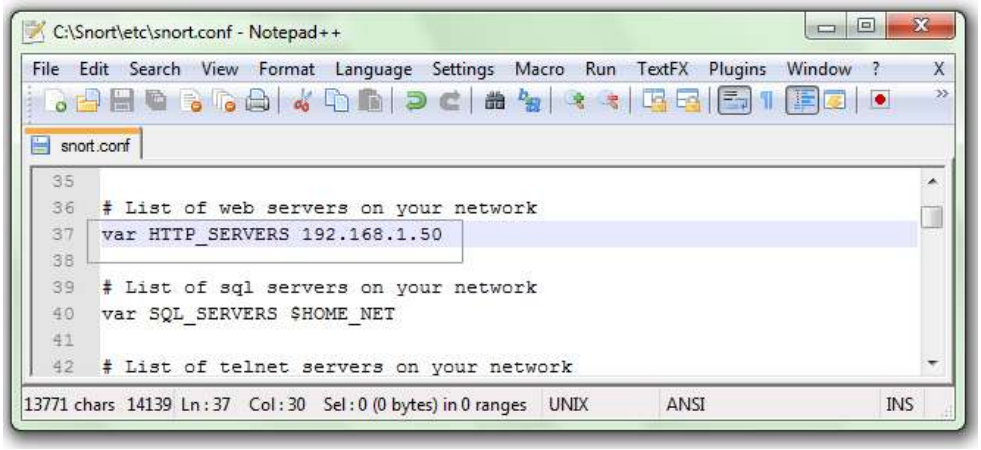
SMTP_SERVERS 192.168.1.50.



Hình 3.10: Khai báo biến SMTP_SERVERS.

Tìm dòng **var HTTP_SERVERS $HOME_NET** sau đó thay tham số **$HOME_NET** bằng địa chỉ IP trên máy tính của bạn.

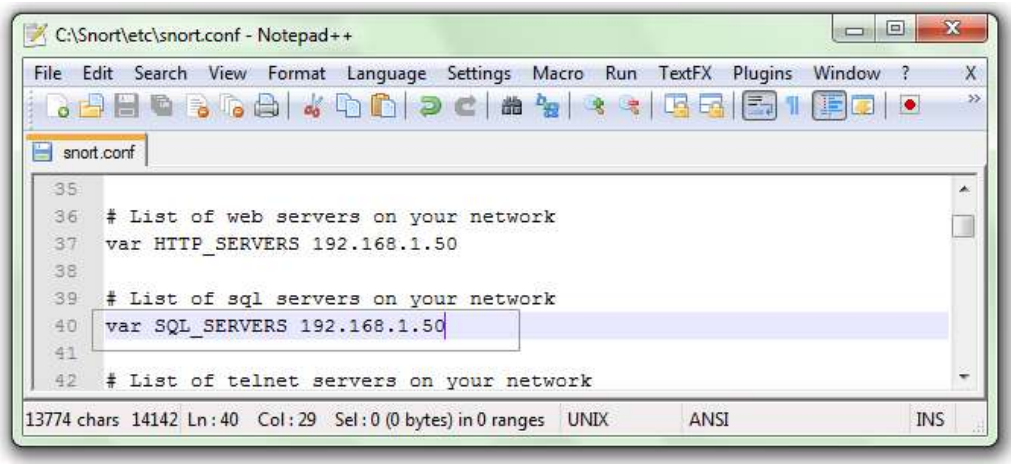
Ví dụ, thay biến **$HOME_NET** bằng địa chỉ IP **192.168.1.50**. Sau khi thay giá trị khai báo thì dòng **var HTTP_SERVERS $HOME_NET** thành **var HTTP_SERVERS 192.168.1.50**.



Hình 3.11: Khai báo biến HTTP_SERVERS.

Tìm dòng **var SQL_SERVERS $HOME_NET** sau đó thay tham số **$HOME_NET** bằng địa chỉ IP trên máy tính của bạn.

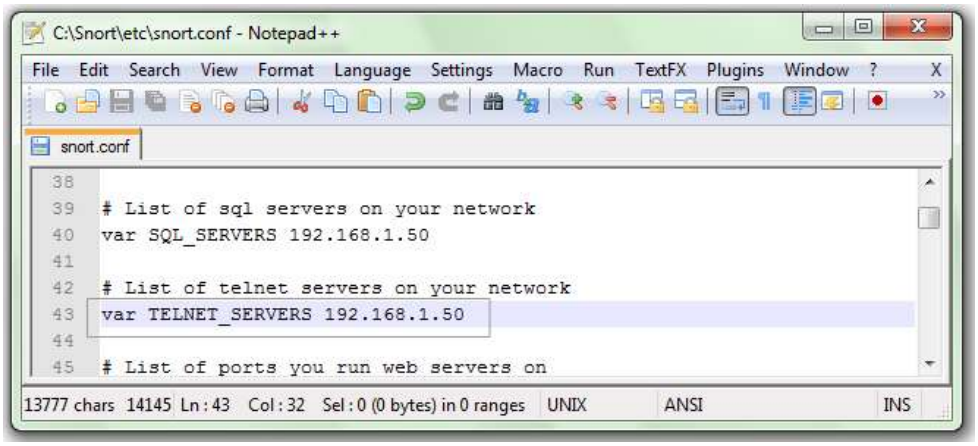
Ví dụ, thay biến **$HOME_NET** bằng địa chỉ IP **192.168.1.50**. Sau khi thay giá trị khai báo thì dòng **var SQL_SERVERS $HOME_NET** thành **var SQL_SERVERS 192.168.1.50**.



Hình 3.12: Khai báo biến SQL_SERVERS.

Tìm dòng **var TELNET_SERVERS $HOME_NET** sau đó thay tham số **$HOME_NET** bằng địa chỉ IP trên máy tính của bạn.

Ví dụ, thay biến **$HOME_NET** bằng địa chỉ IP **192.168.1.50**. Sau khi thay giá trị khai báo thì dòng **var TELNET_SERVERS $HOME_NET** thành **var TELNET_SERVERS 192.168.1.50**.



Hình 3.13: Khai báo biến TELNET_SERVERS.

5. Tìm hiểu về luật của Snort:

5.1. Giới thiệu:

Hầu hết các hành vi xâm nhập đều có một số đặc điểm nhất định, những đặc điểm này được gọi là dấu hiệu. Thông tin về các dấu hiệu này được sử dụng để tạo ra các luật cho Snort.

Người ta thường dựa vào việc phân tích những thông tin của các cuộc tấn công

để lấy thông tin, nhưng thông tin này sẽ được sử dụng để viết ra các luật cho Snort. Căn cứ vào các luật được mô tả, Snort sẽ phát hiện ra những kẻ thâm nhập từ đó đưa ra cảnh báo và gửi thông tin đến người quản trị.

Các dấu hiệu thường lưu trong header của các gói tin nhưng Snort lại phát hiện xâm nhập dựa trên các luật. Các luật của của Snort có thể được sử dụng để kiểm tra nhiều phần khác nhau của gói tin kể cả Header.

Một luật có thể được sử dụng để tạo ra một thông điệp cảnh báo ghi lại thông điệp, … Hầu hết các luật của Snort được viết theo từng dòng đơn. Các luật được phân theo từng nhóm cụ thể, mỗi nhóm này sẽ được lưu lại trong một tập tin, mỗi tập tin luật đều được chứa trong thư mục Rules (C:\Snort\rules) và được gọi (khai báo) trong tập tin snort.conf.

5.2. Cấu trúc luật của Snort:

Tất cả các luật Snort đều có hai phần chính đó là: Header và Options.

Phần Header chứa các thông tin về hành động mà luật sẽ thực hiện và tiêu chuẩn về việc so sánh một luật trên một gói tin.

Phần Option thường chứa một thông điệp cảnh báo và thông tin về phần nào của gói tin được sử dụng để tạo cảnh báo. Một luật có thể phát hiện một hoặc nhiều kiểu xâm nhập.

5.2.1. Cấu trúc của phần Header:

Action: Phần này xác định kiểu hành động sẽ thực hiện khi một tiêu chuẩn được so sánh. Hành động điển hình là việc tạo ra các cảnh báo hoặc ghi lại các thông điệp log.

Protocol: Phần này được sử dụng để áp dụng luật trên gói tin cho một giao thức cụ thể. Đây là tiêu chuẩn đầu tiên được đề cập trong luật. Một số giao thức được sử dụng: TCP, ICMP, UDP, …

Address: Phần này dùng để xác định địa chỉ nguồn và địa chỉ đích. Địa chỉ có thể là của một host, nhiều host hoặc là địa chỉ mạng.

Port: Phần này được áp dụng trong trường hợp TCP hay UDP, xác định cổng nguồn và đích của một gói tin mà luật được áp dụng.

Direction: Phần này xác định địa chỉ và cổng nào được sử dụng, Ví dụ địa chỉ nguồn hay đích.

Ví dụ: Sau đây là một luật dùng để tạo ra thông điệp cảnh báo khi nó phát hiện

một gói tin ping ICMP với TTL là 200:

alert icmp any any -> any any (msg:"Ping with TTL=220";ttl: 100).

Phần trước dấu ngoặc đơn là phần Header của luật, phần đầu phía trong ngoặc đơn là Option.

Header của luật trên chứa các thông tin như: Kiểu thực thi của luật là "alert", nghĩa là xuất ra cảnh báo khi trùng với một dấu hiệu.

- Protocol: Giao thức được sử dụng là ICMP, nghĩa là luật này chỉ được áp dụng trên các gói tin ICMP.
- Địa chỉ nguồn và cổng nguồn: Cả hai phần này đều là "any", nghĩa là luật được áp dụng cho tất cả các gói tin đến từ một nguồn bất kì.
- Direction: Trong ví dụ này, direction được thiết lập từ trái sang phải và sử dụng ký hiệu "->". Điều này chỉ ra rằng số địa chỉ và cổng ở phía bên trái là nguồn và ở phía bên phải là đích. Nó cũng có nghĩa là luật này sẽ được áp dụng trên các gói tin di chuyển từ nguồn tới đích. Bạn cũng có thể sử dụng ký hiệu "<-" để đảo lại ý nghĩa của nguồn và đích. Lưu ý rằng ký hiệu <> cũng có thể sử dụng để chỉ ra hai hướng của nguồn và đích.
- Địa chỉ đích và cổng đích: Cả hai phần trong ví dụ này đều là "any", nghĩa là luật được áp dụng cho tất cả các gói tin đến từ một đích bất kỳ. Phần direction trong phần này không đóng một vai trò gì cả vì luật được áp dụng trên tất cả các gói tin ICMP di chuyển theo bất hỳ hướng nào, vì từ khóa "any" ở cả phần nguồn và đích.

5.2.2. Cấu trúc của phần Options:

Phần Option theo sau phần Header và được đóng gói trong dấu ngoặc đơn. Có thể có một hoặc nhiều Option được cách nhau bởi dấu phẩy. Tất cả các Option được định nghĩa bằng từ khóa. Một số Option cũng chứa các tham số.

Thông thường, một Option có thể có 2 phần : Từ khóa và đối số. Các đối số được phana biệt với từ khóa bằng dấu hai chấm.

Ví dụ : msg "ICMP ISS Pinger";

Trong Option này thì msg là từ khóa và "ICMP ISS Pinger" là đối số của từ khóa.

Một số thành phần khác của phần Option:

- Ack:

Cấu trúc: Ack: <number>.

TCP Header chứa một trường Acknowledgment Number dài 32 bit. Trường này chỉ ra rằng số sequence (sequence number) kế tiếp của người gửi đang chờ hồi đáp. Trường này chỉ có có ý nghĩa khi cờ flag trong trường TCP được thiết lập.

- Content:

Cấu trúc: Content: <straight text>; content: <hex data>.

Snort có khả năng tìm thấy một mẫu dữ liệu trong một gói tin. Mẫu đó có thể tồn tại dưới dạng một chuỗi ASCII hoặc là các ký tự thập lục phân.

- Offset:

Cấu trúc: Offset: <value>.

Từ kháo này được sử dụng kết hợp với từ khóa content. Từ khóa này được sử dụng để tìm kiếm từ một vị trí xác định so với vị trí bắt đầu của gói tin.

- Depth:

Cấu trúc: depth: <value>.

Từ khóa depth cũng được sử dụng kết hợp với từ khóa content để xác định giới hạn trên của việc so sánh mẫu. Có thể sử dụng từ khóa này để xác định một vị trí so với vị trí bắt đầu. Dữ liệu sau vị trí này sẽ không được tìm kiếm để so mẫu.

- Nocase:

Từ khóa nocase được sử dụng kết hợp với từ khóa content. Nó không có đối số. Mục đích là thực hiện việc tìm kiếm trong trường hợp vô tình.

- Content-list:

Cấu trúc: content_list: <filename>.

Từ khóa này được sử dụng cùng với tên của một tập tin và xem tên tập tin như là đối số của nó. Tập tin này chứa một danh sách các chuỗi sẽ được tìm kiếm trong một gói tin. Mỗi chuỗi được đặt trên các dòng khác nhau của file.

- Dsize:

Cấu trúc: dsize: [<|>] <number>.

Từ khóa dsize được sử dụng để tìm chiều dài một phần dữ liệu của gói tin. Nhiều cách tấn công sử dụng lỗ hổng tràn bộ đệm bằng cách gửi các gói tin có kích thước lớn. Sử dụng từ khóa này có thể tìm thấy các gói tin có chiều dài dữ liệu lớn hoặn nhỏ hơn một số các định.

- Flags:

Cấu trúc: flags: <flags>.

Từ khóa này được sử dụng để tìm ra bit flag nào được thiết lập trong TCP Header của gói tin. Mỗi flag có thể được sử dụng như một đối số của từ khóa flags.

- Fragbits:

  Cấu trúc: fragbits: <flag_settings>

  Sử dụng từ khóa này để xác định các bits : RB (Reserved Bits), DF (Don't Fragment Bit), MF (More Fragments Bit) trong IP Header có được bật lên hay không.

- Icmp_id:

  Cấu trúc: icmp_id: <number>.

  Thường được sử dụng để pháthiện một ID cụ thể trong gói tin ICMP.

- Icmp_seq:

  Cấu trúc: icmp_seq: <hex_values>.

  Giống như từ khóa icmp_id

- Itype:

  Cấu trúc: itype: <number>.

  ICMP Header nằm sau IP Header và chứa trường Type. Từ khóa Itype được sử dụng để phát hiện các cách tấn công sử dụng trường type trong ICMP Header của gói tin.

- Icode:

  Cấu trúc: icode: <number>.

  Trong gói tin ICMP, ICMP Header đi sau IP Header. Gói tin này chứa một trường code và từ khóa icode được sử dụng để phát hiện trường code trong header gói tin ICMP.

- Id:

  Cấu trúc: id: <number>.

  Từ khóa này được sử dụng để đối chiếu với trường fragment ID trong header gói tin IP. Mục đích của nó là phát hiện các cách tấn công sử dụng một số ID cố định.

- Ipopts:

  Cấu trúc: ipopts: <ip_option>.

  Header của Ipv4 dài 20 byte. Bạn có thể thêm các tùy chọn vào Header này ở cuối. Chiều dài của phần tùy chọn này có thể lên đến 40 byte. Các tùy chọn được sử dụng cho những mục đích khác nhau, bao gồm:

  - Record Router (rr).

- Time Stamps (ts).
- Loose Source Routing (lsrr).
- Strict Source Routing (ssrr).

- Ip_proto:

Cấu trúc: ip_proto: [!] <name or number>.

Từ khóa ip_proto sử dụng plug-in IP Proto để xác định số giao thức trong Header của IP.

- Logto:

Cấu trúc: logto: <file_name>.

Từ khóa logto được sử dụng để ghi log các gói tin vào một tập tin được chỉ định.

- Msg:

Cấu trúc: msg: <sample_message>.

Từ khóa msg được sử dụng để thêm một chuỗi ký tự vào tập tin log và cảnh báo.

- Priority :

Cấu trúc : priority : <priority_integer>.

Từ khóa priority dùng để gán độ ưu tiên cho một luật, một số được gán cho độ ưu tiên phải là một số nguyên dương.

- React:

Cấu trúc: react: <react_basic_modifier[react_additional_modifier,…]>.

Từ khóa react được sử dụng để kết thúc một phiên, khóa một vài vị trí hoặc dịch vụ.

- Reference:

Cấu trúc: reference: <id system>,<id>.

Từ khóa reference có thể thêm một sự tham khảo đến thông tin tồn tại trên các hệ thống khác trên mạng. Nó không đóng một vai trò nào trong cơ chế phát hiện. Bằng việc sử dụng từ khóa này có thể kết nối đến các thông tin thêm trong thông điệp cảnh báo.

- Resp:

Từ khóa này được sử dụng để đánh bại các hành vi của Hacker bằng cách gửi các gói tin trả lời cho một host để tạo ra một gói tin thỏa luật.

- Rev:

Cấu trúc: rev: <revision interger>.

Từ khóa rev dùng để chỉ ra số revision của luật. Nếu cập nhật luật bạn có thể sử dụng này để phân biệt giữa các phiên bản.

- Rpc:

Cấu trúc: rpc: <số ứng dụng, số thủ tục, số phiên bản>.

Từ khóa rpc được sử dụng để phát hiện các yêu cầu RPC cơ bản.

- Sameip:

Từ khóa sameip được sử dụng để kiểm tra địa chỉ nguồn và địa chỉ đích có giống nhau hay không. Nó không có đối số.

- Seq:

Cấu trúc: seq: <hex_value>.

Từ khóa seq được sử dụng để kiểm tra số thứ tự sequence của gói tin TCP.

- Flow:

Từ khóa flow được dùng để áp dụng một luật của Snort lên các gói tin di chuyển theo một hướng cụ thể. Bạn có thể sử dụng các tùy chọn sau kết hợp với từ khóa flow để xác định hướng. Dưới đâu là một số tùy chọn kết hợp với từ khóa flow:

- to_client.
- to_server.
- from_client.
- from_server.

- Session:

Cấu trúc: session: [printable|all].

Từ khóa session có thể được sử dụng để loại bỏ tất cả dữ liệu của một phiên TCP nào đó.

- Sid:

Cấu trúc: sid: <snort rule id>.

Từ khóa sid được sử dụng để tạo ra một cảnh báo cụ thể.

- Tag:

Cấu trúc: tag: <type>, <count>, <metric>[direction].

Đây là một từ khóa được sử dụng để ghi log các dữ liệu thêm vào từ (hoặc đến) một host xâm nhập khi một luật được kích hoạt.

- Tos:

Cấu trúc: tos: <number>.

Từ khóa tos được sử dụng để phát hiện một giá trị cụ thể trong trường TOS (Type of Service) trên IP Header.

- Ttl:

Cấu trúc: ttl: <number>.

Từ khóa ttl được sử dụng để phát hiện giá trị Time ti Live trong IP Header của gói tin. Từ khóa này có thể được sử dụng cho tất cả các kiểu giao thức xây dựng trên nền IP như: ICMP, UCP và TCP.

- Uricontent:

Cấu trúc: uricontent : [!] “content string”.

Từ khóa uricontent giống với từ khóa content ngoại trừ việc nó được sử dụng để tìm một chuỗi trong phần URI (Uniform Resource Identifier) của gói tin.

CHƯƠNG IV: XÂY DỰNG PHẦN MỀM QUẢN LÝ CÁC IP TỪ BÊN NGOÀI TRUY CẬP VÀO HỆ THỐNG

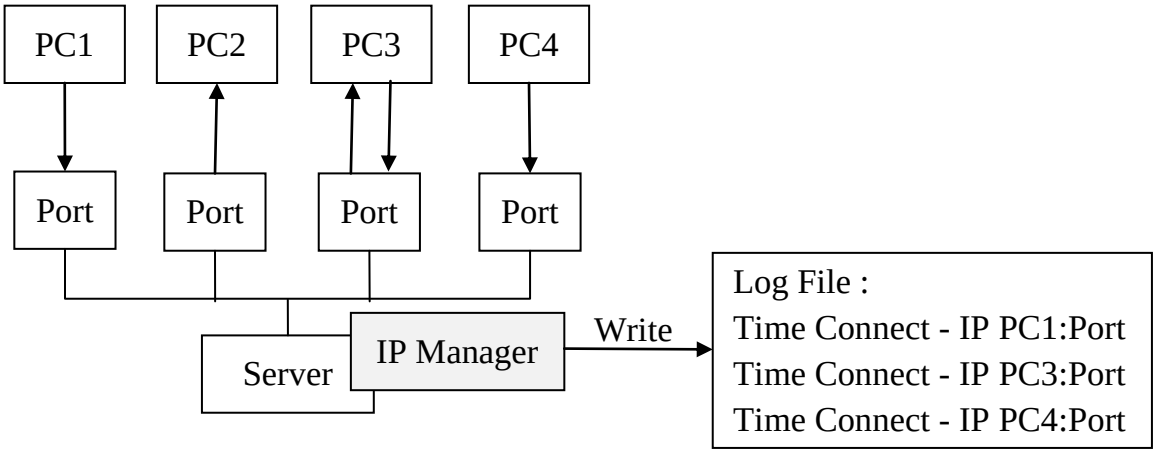
I. BÀI TOÁN :

Ngày nay, hệ thống mạng máy tính đã trở nên rất phổ biến trong hầu hết các hoạt động xã hội, tác động trực tiếp đến nền kỹ thuật và kinh tế của cả nước. Cùng với sự phát triển đó, ngày càng xuất hiện nhiều hơn những các nhân, nhóm hoặc thậm chí là cả những tổ chức hoạt động với những mục đích xấu nhằm phá hoại các hệ thống mạng máy tính, hệ thống thông tin, gây tác hại vô cùng to lớn đến tính an toàn và bảo mật thông tin trên các hệ thống này.

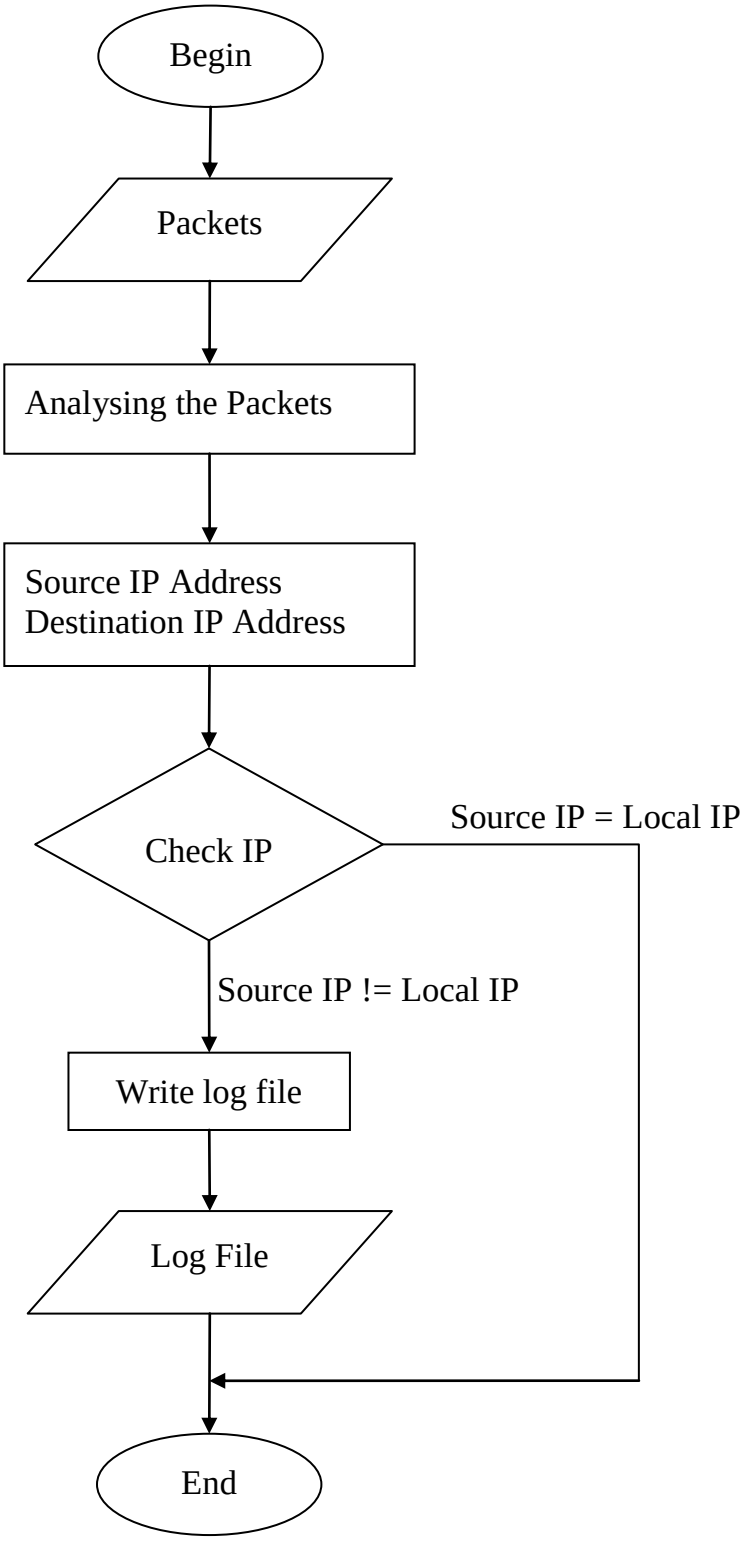
Qua quá trình nghiên cứu đề tài "Nghiên cứu và đề xuất giải pháp ngăn chặn việc truy cập trái phép vào các hệ thống thông tin tin học qua mạng Internet" và từ thực tế, việc phát hiện các truy cập vào hệ thống thường dựa vào các thông tin ghi trong file log của hệ thống. Nhưng việc quản lý file log của hệ điều hành chưa thực sự "mềm dẻo" nên các hãng thứ 3 luôn phát triển thêm các ứng dụng bảo mật tương tự.

Trong đồ án này, em viết một ứng dụng có chức năng tương tự file log. Ứng dựng sẽ ghi lại tất cả các thông tin IP truy cập vào máy tính bao gồm : Thời gian truy cập, địa chỉ IP, cổng kết nối.

II. THUẬT TOÁN :



Hình 4.1: Mô tả hoạt động chương trình.



Hình 4.2: Sơ đồ giải thuật.

III. MÔ TẢ CHỨC NĂNG PHẦN MỀM :

1. Chức năng quản lý IP truy cập vào hệ thống :

Khởi động chương trình, vào Menu chọn IP Manager để bắt đầu quá trình kiểm tra IP kết nối vào máy tính.

Khi có 1 kết nối đến máy tính, chương trình đón bắt tất cả thông tin về Source IP Address, Destination IP Address và Port.

Hàm kiểm tra IP xem vào hay ra khỏi hệ thống :

// Code :

```
static bool check;
public void checkIP ()
{
   DateTime dtIPConnect = new DateTime();
   IPGlobalProperties properties =
                                        IPGlobalProperties.GetIPGlobalProperties();
   while (check)
   {
      TcpConnectionInformation[] connect =
                                        properties.GetActiveTcpConnections();
      dtIPConnect = DateTime.Now;
      String strChuoi = null;
      try
      {
         for (int i = 0; i < connect.Length; i++)
         {
            strChuoi = dtIPConnect.Hour
               + ":" + dtIPConnect.Minute
               + ":" + dtIPConnect.Second
               + ":" + dtIPConnect.Millisecond
               + "\t"
               + connect[i].RemoteEndPoint
               + "\n\n" + strChuoi;
            WriteLogFile.WriteLog(
            Convert.ToString(connect[i].RemoteEndPoint.Address),
             Convert.ToString(connect[i].RemoteEndPoint.Port),
             dtIPConnect.Hour + ":"
```

```
                + dtIPConnect.Minute + ":"
                + dtIPConnect.Second + ":"
                + dtIPConnect.Millisecond);
            }
            setText(Convert.ToString(strChuoi));
            Thread.Sleep(1000);
        }
        catch (Exception ex)
        {
            MessageBox.Show(ex.Message, "Manager IP Connect to PC",
                                MessageBoxButtons.OK, MessageBoxIcon.Error);
        }
    }
}
```

Khi biết được IP đó là vào hay ra, chương trình sẽ ghi thông tin vào log file: Thời gian kết nối (Thời gian hiện tại của hệ thống) - Địa chỉ IP:Cổng kết nối. Tên log file có dạng: 2010_06_24_LOG.log.

Hàm ghi thông tin đón bắt được vào log file:

//Code:

```
public class WriteLogFile
{
    static string m_baseDir = null;
    static WriteLogFile()
    {
  m_baseDir = Directory.GetCurrentDirectory() + @"\Log\";
        Directory.CreateDirectory(m_baseDir);
     }

     public static string GetFilenameYYYMMDD(string suffix, string extension)
     {
         return System.DateTime.Now.ToString("yyyy_MM_dd")
                                            + suffix
                                            + extension;
```

```
        }

        public static void WriteLog(String _IP,String _Port, String _DateTime)
        {
            try
            {
                string filename = m_baseDir
                        + GetFilenameYYYMMDD("_LOG", ".log");
                StreamWriter sw = new StreamWriter(filename, true);
                sw.WriteLine(_DateTime + "\t" + _IP + ":" + _Port);
                sw.Close();
            }
            catch (Exception)
            {}
        }
    }
```

Sau thời gian 1 giây, chương trình lại quét IP một lần và tiếp tục ghi thông tin vào log file.

2. Chức năng đọc thông tin log file :

Khởi động chương trình, vào Menu chọn Read Log để bắt đầu quá trình đọc các thông tin đã ghi lại được.

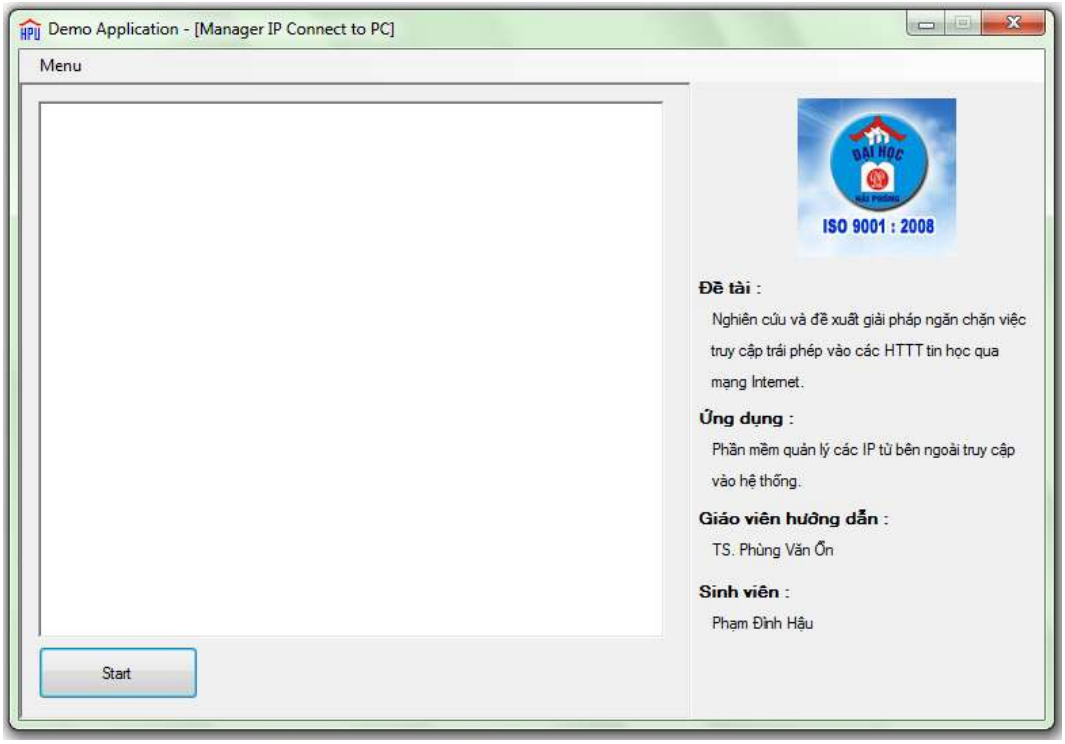
Chọn Browse để đến nơi lưu trữ các Log File, Chương trình sẽ đọc từng dòng 1 trong log file và hiển thị :

//Code :

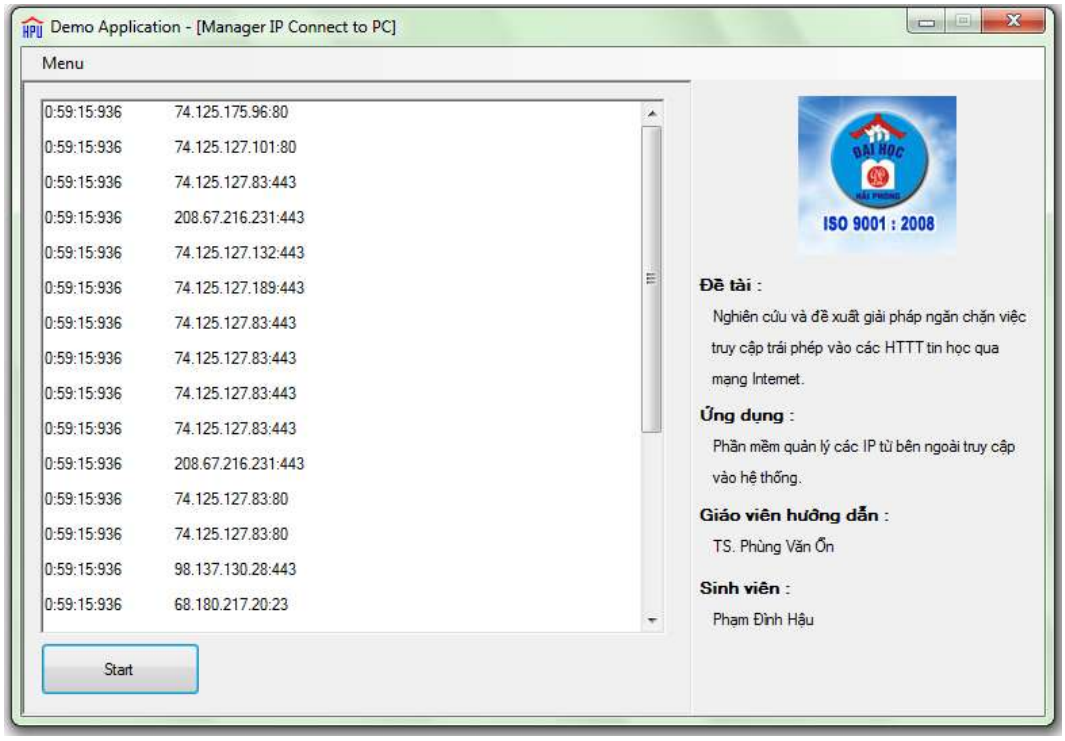
```
Stream _Stream = null;
OpenFileDialog _openFile = new OpenFileDialog();
_openFile.InitialDirectory = Directory.GetCurrentDirectory() + @"\Log\";
_openFile.Filter = "Log files (*.log)|*.log";
_openFile.FilterIndex = 2;
 _openFile.RestoreDirectory = true;
 if (_openFile.ShowDialog() == DialogResult.OK)
{
```

```
try
{
    if ((_Stream = _openFile.OpenFile()) != null)
    {
        using (_Stream)
        {
                txtLinkLog.Text = _openFile.FileName;
                String _log = "";
                String line = "";
                StreamReader sr = new StreamReader( _openFile.FileName );
                while ((line = sr.ReadLine()) != null)
                {
                _log=_log+line+"\n";
                }
                rtfReadLog.Text = _log;
        }
    }
}
catch (Exception ex)
{
    MessageBox.Show("Error: Could not read file from disk. Original error: "
                                                        + ex.Message);
}
}
```

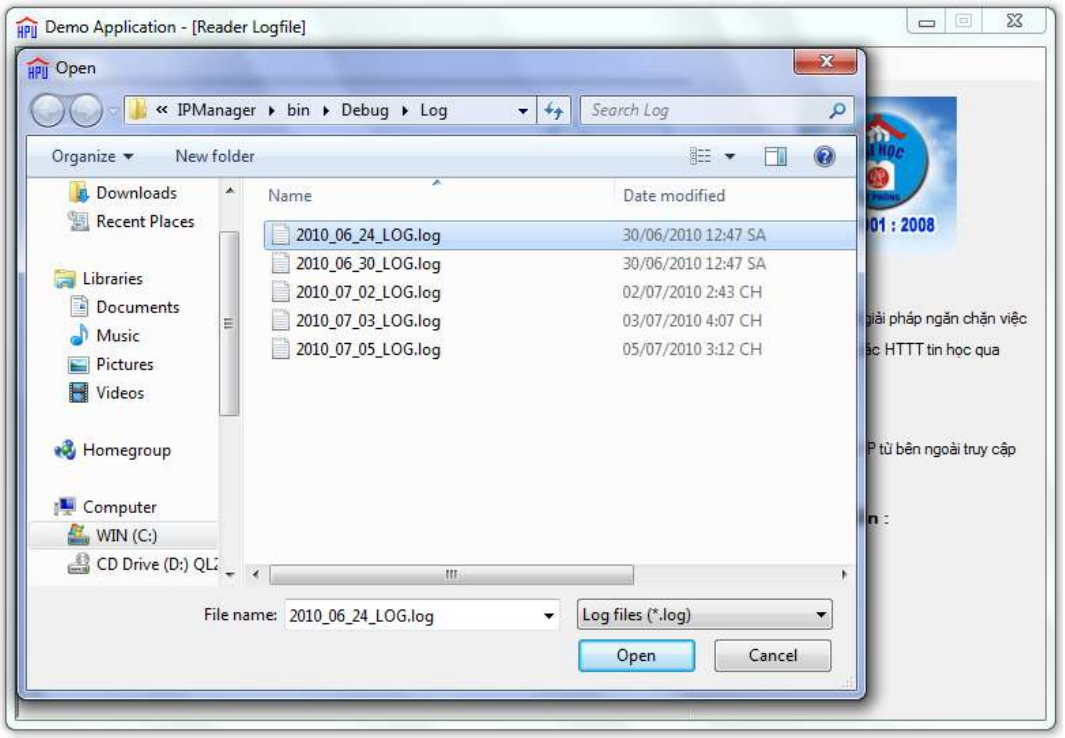
IV. MINH HỌA GIAO DIỆN CHƯƠNG TRÌNH :



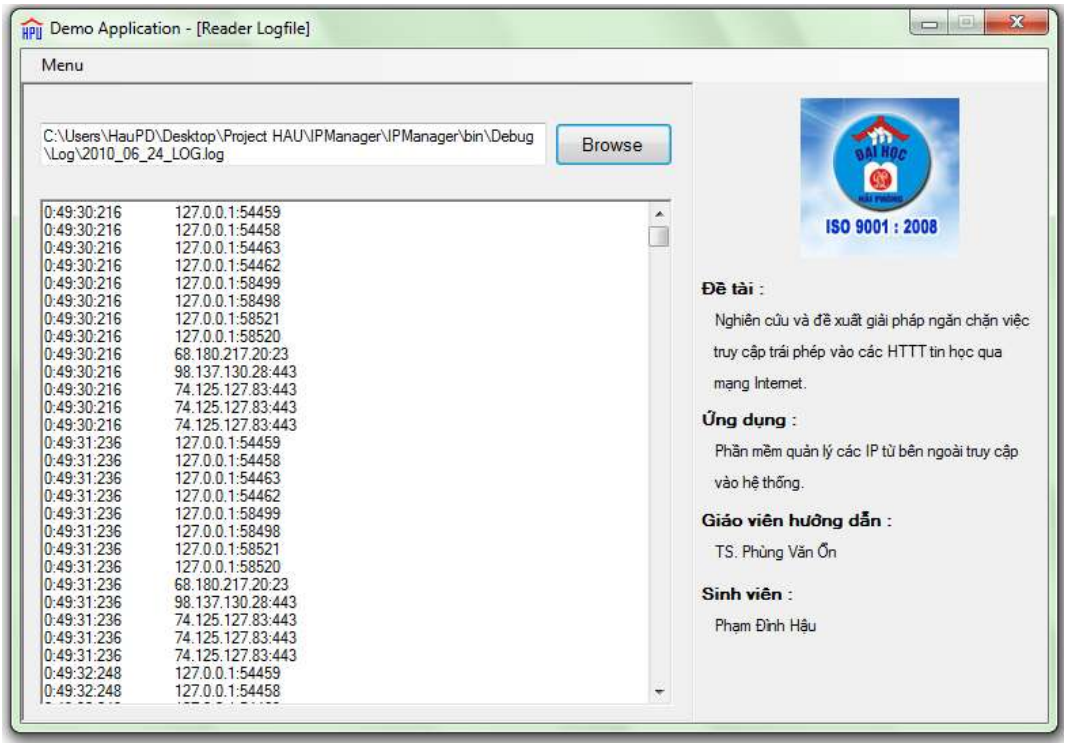
Hình 4.3: Giao diện chính của chương trình.



Hình 4.4: Giao diện hiển thị các IP hiện tại đang truy cập vào hệ thống.



Hình 4.5: Giao diện chọn log file để đọc.



Hình 4.6: Giao diện hiển thị thông tin trong log file.

KẾT LUẬN

An toàn hệ thống thông tin và các giải pháp an toàn đang là vấn đề được quan tâm và ngày càng được chú trọng hiện nay.Vì vậy nghiên cứu và đưa ra những giải pháp giải quyết vấn đề này hết sức cần thiết và phải được triển khai một các mạnh mẽ và hiệu quả.

Thời gian làm đồ án không phải ngắn và cũng không đủ dài để em tìm hiểu đầy đủ các vấn đề về an toàn hệ thống thông tin. Em đã tìm hiểu cơ bản về hệ thống thông tin, các nguy cơ mất an toàn, một số kiểu tấn công cơ bản và cách phòng chống. Qua quá trình tìm hiểu em đã xây dựng được chương trình quản lý các IP từ bên ngoài truy cập vào hệ thống. Chương trình thực hiện đầy đủ chức năng đã đề ra : ghi lại thời gian truy cập, địa chỉ IP, cổng kết nối.

Hướng phát triển tiếp theo của đồ án là :

- Tìm hiểu sâu thêm về các kỹ thuật truy cập trái phép và đưa ra phương pháp phòng chống có hiệu quả.
- Phần mềm em xây dựng bước đầu đã thực hiện được chức năng quản lý IP từ bên ngoài truy cập vào hệ thống, nhưng chưa đưa ra được cảnh báo cụ thể.

Trong quá trình làm đồ án không tránh khỏi thiếu sót, em kính mong thầy cô giúp đỡ cho báo cáo tốt nghiệp của em hoàn thiện hơn.

Em xin chân thành cảm ơn các thầy các cô!

TÀI LIỆU THAM KHẢO

1. Trang web http://vi.wikipedia.org
2. Trang web http://en.wikipedia.org
3. Trang web http://www.oxid.it/cain.html
4. Trang web http://hvaonline.net
5. Tìm hiểu các kiểu tấn công cơ bản và phương pháp phòng chống – Vũ Đình Cường.
6. Cách bảo vệ dữ liệu quan trọng và phương pháp phát hiện thâm nhập – Vũ Đình Cường.
7. Snort Users Manual 2.8.6 – The Snort Project