Module 15
Tấn Công Trên Mạng Không Dây

Những Nội Dung Chính Trong Chương Này

Giới Thiệu Về Mạng Không Dây

Những Rũi Ro Khi Sử Dụng Mạng Wifi

WEP, WPA Và Những Kỹ Thuật Bẻ Khóa

WEP - Wired Equivalent Privacy

WPA - Wifi Protected Access

Các Dạng Tấn Công Trên Mạng Không Dây

Giới Thiệu Về Mạng Không Dây

Wireless Network hay mạng không dây mà chúng ta cũng thường thấy thông qua thuật ngữ Wifi đã đem đến một cuộc cách mạng thực sự trong vấn đề kết nối và truyền thông. Nhờ có mạng không dây mà ngày nay chúng ta có thể vượt qua những trở ngại thường gặp phải trong mạng sử dụng cáp truyền thống và có khả năng online từ bất cứ nơi đâu. Chính vì vậy mà trong những công ty hay tổ chức thường hay lắp đạt các trạm kết nối không dây như là một điểm truy cập mở rộng đầy thuận tiện cho người dùng.

Vậy mạng không dây là gì ? Đó là hệ thống mạng không dựa trên vật dẫn là các dây nối hay hệ thống cáp mà sử dụng các loại sóng vô tuyến (RF – Radio Frequence). Hầu hết các mạng không dây dựa trên tiêu chuẩn IEEE 802.11 như 802.11a, 802.11b, 802.11g, và 802.11n.

> IEEE là tên viết tắt của tổ chức phi lợi nhuận Institute of Electrical and Electronics Engineers có nghĩa là Viện Các Kỹ Sư Điện Và Điện Tử, được thành lập vào năm 1963 IEEE là một nơi chuyên bành hành các tiêu chuẩn được ứng dụng rộng rãi trong nhiều lĩnh vực của công nghệ thông tin. Nhờ các tiêu chuẩn này mà các hệ thống phần cứng hay phần mềm có thể tương thích và kết nối dễ dàng cho dù được sản xuất bởi những nhà cung cấp khác nhau.

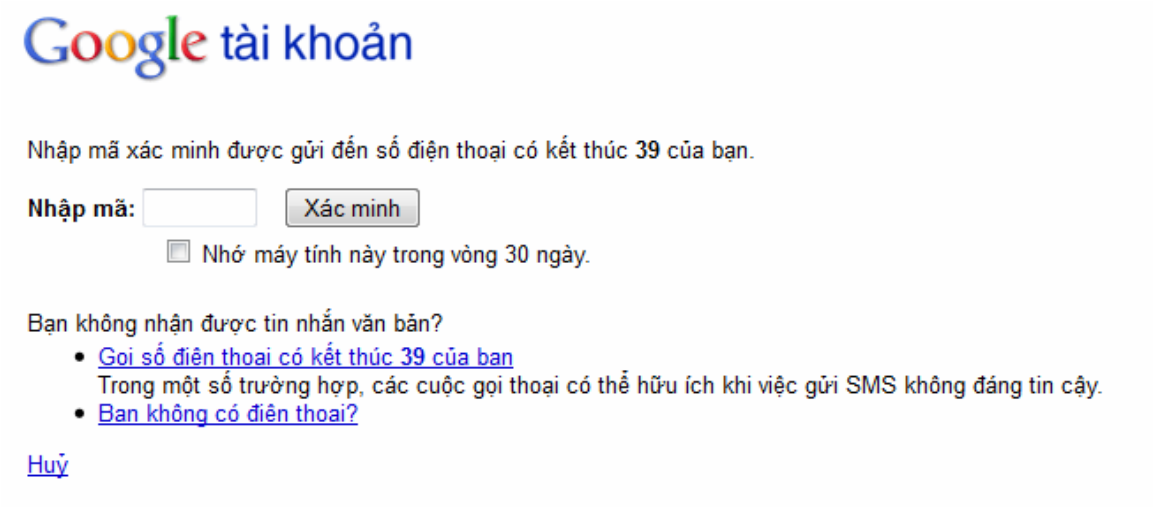
Những công nghệ này đều tồn tại một lổ hỗng bảo mật lớn làm cho hệ thống mạng không dây trở nên thiếu an toàn hơn bất kì hệ thống mạng nào, đó là do cơ chế phát sóng vô tuyến dựa trên nền tảng truyền thông *broadcast* mà ở đó bất cứ máy tính nào cũng có thể nhận được tín hiệu của nhau, miễn là chúng cùng nằm trong một lớp mạng. Bên cạnh đó, công nghệ mã hóa và xác thực dựa trên WEP của các tiêu chuẩn trên đã được chứng minh là không an toàn, có thể bị hacker bẻ khóa và xâm nhập vào hệ thống trong vòng 15 phút. Vì vậy tổ chức Wi-fi Alliance đã tạo ra một tiêu chuẩn nâng là WPA (Wi-Fi Protected Access) và sau đó là WPA2. Chúng ta sẽ thảo luận về những khái niệm này trong phần sau.

Tạp chí mạng *seek4media* đã đưa ra một thống kê có đến 50 % các mạng Wifi trên toàn thế giới có khả năng bị tấn công trong vòng 5 giây. Điều này có vẽ cường điệu nhưng nếu tính cả những mạng wifi không có sử dụng cơ chế bảo mật nào (thường được đánh dâu là *Unsecured*) chiếm đến 25 % thì tỉ lệ trên không phải là quá cao. Nhưng cho dù những rũi ro hay các tỉ lệ thống kê như nào thì cũng không thể phủ nhận được tính tiện lợi mà mạng Wifi mang lại. Như vào lúc này đây, khi biên soạn tài liệu này tôi cũng đang sử dụng mạng Wifi trong quán ca phê Nhật Nguyên nhìn xuống bờ hồ Xuân Hương đây thơ một của Đà Lạt ngàn hoa. Trong khi tận hưởng những tiện nghi mà sự tiến bộ của công nghệ mang lại thì tôi có những mối nguy hiểm nào khi đang dùng mạng không dây ?

Trước tiên, đây là hệ thống mạng được bảo vệ bằng mật khẩu ứng dụng công nghệ WPA2 nên có thể an tâm phần nào, vì với kỹ thuật mã hóa này rất khó cho hacker có khả năng bẻ khóa, tuy nhiên những mối nguy hiểm lại đến từ những khách hàng khác vì họ cũng gia nhập cùng lớp mạng do đó có khả năng chặn bắt dữ liệu mà máy tính chúng tôi

truyền trên mạng gồm tài khoản Paypal, hộp thư điện tử, tài khoản quản trị trang web www.security365.vn và bất cứ thông tin nào không được mã hóa.

Và nếu như máy tính của tôi không được cập nhật các bản vá lỗi đầy đủ thì khả năng bị tấn công và chiếm quyền điều khiển từ xa là có thể xảy ra. Tuy nhiên, những mối nguy trên đã được hạn chế khá nhiều vì tôi đang dùng hệ điều hành Windows 7 Ultimate có bản quyền đầy đủ, đã được cập nhật các bản vá lỗi. Tôi kiểm tra hộp thư của mình thông qua một địa chỉ gmail trung gian (sử dụng tính năng forward từ hộp thư khác về hộp thư trung gian này), và địa chỉ email trung gian tôi đang sử dụng có tên là dongduongict@gmail.com đã được bật chức năng bảo vệ 2 lớp, vì vậy ngay cả những hacker mũ đen có đánh cắp được mật khẩu thì cũng không làm gì được, do họ cần phải đánh cắp một trong hai chiếc điện thoại được dùng để nhận mã xác minh.

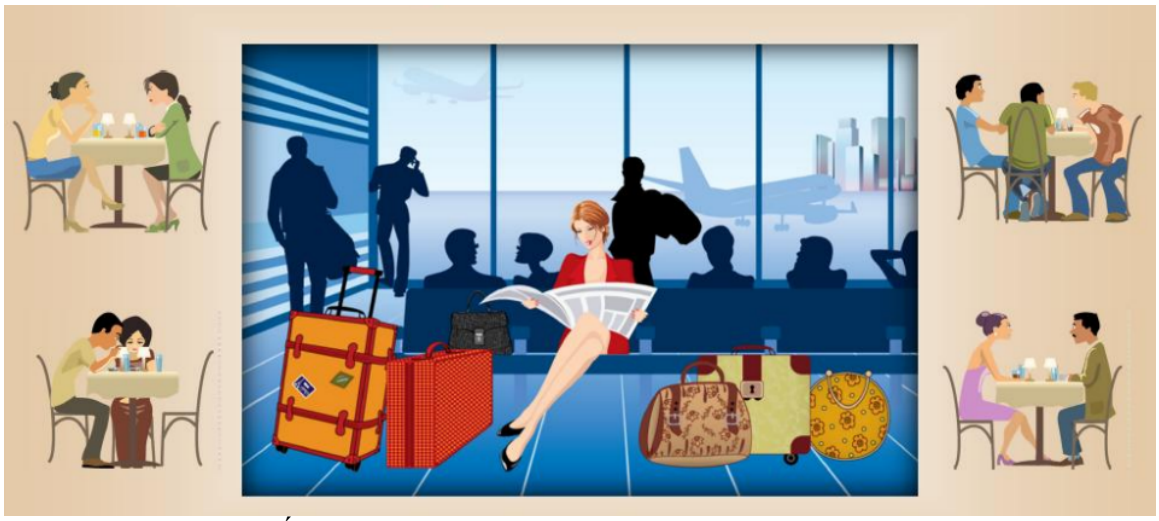


Hình 15.1 – Xác minh hai lớp trên Gmail

Mặc dù vậy, khi tôi đã đăng nhập hộp thư của mình hay đăng nhập vào các trang mạng xã hội thì vẫn có khả năng bị hacker tấn công session hijacking để chiếm lấy quyền kiểm soát bằng những công cụ như ferret và hamster, vì vậy để an toàn tôi chọn ***Luôn sử dụng https*** như hình minh họa sau đây.

Hình 15.2 – Thiết lập sử dụng https trên toàn bộ phiên truyền

Với các cấu hình trên đây thì tôi chỉ mới bảo đảm được sự an toàn cho việc sử dụng email, còn các hệ thống khác như dùng ftp hay đăng nhập trang web quản trị chúng ta cần sử dụng một kết nối an toàn hơn đó là VPN, có rất nhiều ứng dụng VPN miễn phí mà chúng ta có thể dùng khi cần thiết như Hot Pot Shield – một giải pháp mà chúng ta thấy quảng cáo rất nhiều trên mạng khi sử dụng Wifi hay muốn truy cập vào Facebook lúc bị chặn. Do đó, khi cần truy xuất những dữ liệu cần sự an toàn cao ở môi trường public thì các bạn nên ứng dụng VPN, nếu là VPN của cơ quan thì càng tốt, còn nêu không thì phải chọn những nhà cung cấp dịch vụ uy tín, đáng tin cậy.


Hình 15.3 - Các hệ thống mạng không dây công cộng như sân bay, nhà ga, quán ca phê

Những Rũi Ro Khi Sử Dụng Mạng Wifi

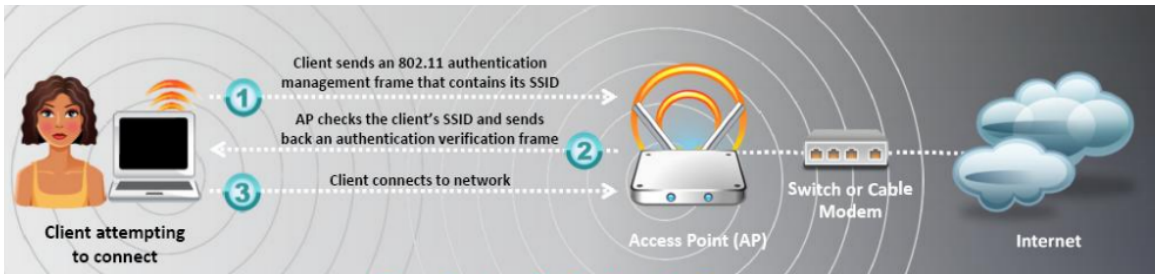
Trước đây, tổ chức an ninh mạng BKIS đã từng cảnh báo các hệ thống wifi ở nhà hay một số doanh nghiệp sử dụng các cấu hình mặc định cho hệ thống quản lý truy cập Wifi

là WAP (Wireless Access Point), với các thông tin mặc định này thì hacker có thể dễ dàng đoán được mật khẩu quản trị của WAP và thay đổi các thông tin cấu hình dẫn đến những mục tiêu nguy hiểm hay chặn bắt thông tin nhạy cảm của người dùng thông qua phương pháp nghe lén. Do đó, trong vai trò CEH hay chuyên gia bảo mật thông tin hệ thống chúng ta có trách nhiệm thay đổi các cấu hình mặc định nhằm nâng cao tính an toàn cho mạng wifi.

Các giải pháp cho vấn đề trên gồm có xác thực người dùng với WPA/WPA2 (tuyệt đối không sử dụng WEP), kiểm soát việc gia nhập hệ thống dựa trên địa chỉ MAC của thiết bị mạng hay sử dụng certificate cho quá trình xác thực, yêu cầu phải gia nhập domain mới kết nối được vào mạng wifi …

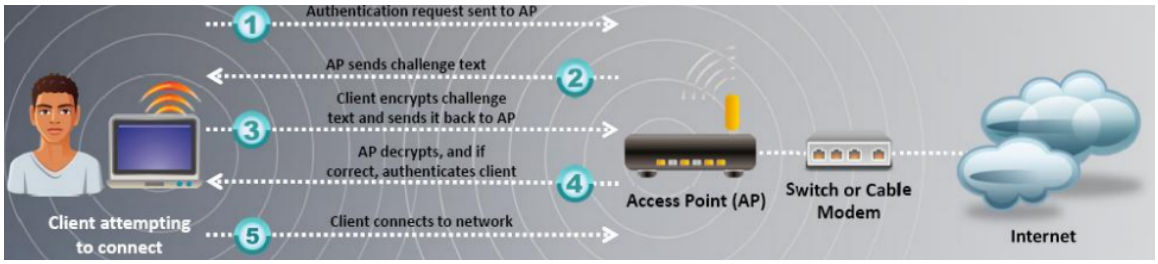
WEP, WPA Và Những Kỹ Thuật Bẻ Khóa

Có hai mô hình xác thực thường được ứng dụng trong các môi trường mạng không dây là Open System và Shared Key Authentication. Với dạng Open System thì các máy tính client có thể gia nhập vào mạng không dây mà không phải trải qua quá trình kiểm tra nào. Như trong hình minh họa bên dưới ta thấy khi người dùng tìm ra một hệ thống mạng không dây dựa trên SSID của chúng và gởi yêu cầu kết nối đến Access Point (AP) sẽ được hồi đáp bằng một thông tin xác nhận (authentication verify frame) dựa trên SSID mà client cần kết nối. Sau đó máy tính client có thể gia nhập vào hệ thống mạng để sử dụng dịch vụ hay truy cập internet.



Hình 15.4 – Xác thực mạng không dây với Open System

Ngược lại, với mô hình Shared Key Authentication khi người sử dụng gởi yêu cầu kết nối đến AP sẽ nhận được thông tin phản hồi là một chuỗi kí tự thử thách với WEP key. Client sẽ mã hóa giá trị thử thách này và gởi lại cho AP, kết quả này sẽ được AP giải mã và so sánh nếu có sự trùng khớp (nghĩa là client nhập vào đúng mật khẩu kết nối) thì quá trình xác thực hoàn tất, client kết nối vào mạng thành công.

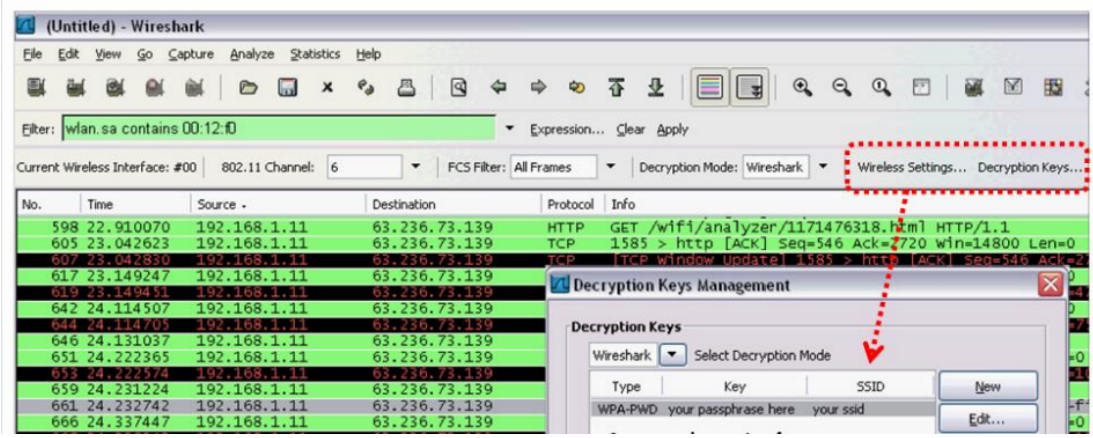


Hình 15.5 - Xác thực mạng không dây với Shared Key Authentication

WEP - Wired Equivalent Privacy

Trong mô hình trên chúng ta thấy AP sử dụng WEP cho quá trình xác thực. Vậy WEP là gì ? Đây là viết tắt của từ Wired Equivalent Privacy, giải pháp bảo mật đầu tiên được ứng dụng cho mạng không dây dựa trên tiêu chuẩn 802.11 dùng cho việc mã hóa dữ liệu trên mạng WLAN (Wireless LAN) cũng như mã hóa khóa chia sẽ (pre-shared key) dùng để xác thực các WLAn Client. WEP sử dụng khóa mã hóa RC4 có độ dài 64 bit hoặc 128 bit để mã hóa dữ liệu tại lớp 2 trong mô hình OSI. Tuy nhiên, trong 64 bit hay 128 bit này thì có 24 bit được dành cho việc tạo các giá trị Initialization Vector (IV). Tiến trình mà RC4 xử dụng các giá trị IV để tạo ra các khóa chia sẽ chính là điểm yếu của WEP và khiến cho nó có khả năng bị bẽ gãy. Các bạn có thể hình dung giá trị của IV được tạo từ sự kết hợp 24 bit do đó nó dễ bị tấn công brute-force nếu như hacker tổng hợp đủ một lượng các gói tin từ Access Point (tối đa khoảng 150.000 gói tin). Trước đây việc chờ đợi để thu thập đủ các gói tín này sẽ mất nhiều thời gian nhưng với các kỹ thuật gởi các yêu cầu giả mạo đến Access Point sẽ giúp cho hacker có thể nhanh chóng tổng hợp đủ dữ liệu và bẻ khóa WEP trong thời gian chưa đầy 5 phút. Một trong những công cụ thường được sử dụng cho dạng tấn công này là Backtrack 5 (phiên bản mới nhất hiện nay) như video minh họa tại địa chỉ sau : http://youtu.be/AYWm1wHr5g0

Ví dụ hacker có thể dùng Cain kết hợp với Airpcap hoặc nghe lén bằng Wireshark và dùng với AirPcap để bẻ khóa như hình minh họa sau :



Hình 15.6 - Hình minh họa khóa WEP bị bẻ với WireShark và Airpcap.

Lưu ý : Các chương trình chuyên dùng cho việc bẻ khóa mạng không dây như WEP đò hỏi phải có những card mạng tương thích, do đó khi sử dụng chúng các bạn nên xem qua danh sách card mạng không dây được hỗ trợ bở các ứng dụng nay như aircrack-ng, kismac. Đây là danh sách các chipset được hỗ trợ : http://www.aircrack-ng.org/doku.php?id=compatibility_drivers

Do WEP là một thuật toán mã hóa yếu nên nó còn được gọi bằng tên *Weak Encryption Protocol*, tuy nhiên trên các hệ thống phần cứng cũ vẫn sử dụng WEP cho nên các router hay modem wifi ngày nay vẫn phải hỗ trợ giao thức này nhằm bảo đảm cho vấn đề tương thích. Ngoài ra, đối với người sử dụng thông thường thì WEP và WPA không gợi lên cho họ ý nghĩ giao thức nào sẽ bảo mật cao hơn, chưa kể đến WEP còn là giao thức được xếp trên theo thứ tự bảng chữ cái cho nên vẫn có rất nhiều lựa chọn cho giải pháp kém bảo mật này.

Và thử hình dung, chúng ta là nhà cung cấp các điểm truy cập Wifi có trả phí dành cho người dùng, thì việc hỗ trợ WEP là một điều bắt buộc vì không biết được khách hàng sử dụng các hệ thống phần cứng nào, vì vậy ngày nay Wired Equivalent Privacy hay "*Weak Encryption Protocol*" vẫn được nhiều nơi sử dụng.

WPA (Wifi Protected Access)

Nhằm khắc phục những yếu điểm của WEP, vào nằm 2003 Wi-fi Alliance đã xây dựng một giao thức mới là WPA như là giải pháp thay thế cho WEP mà không cần phải có sự thay đổi về phần cứng, tuy nhiên những thay đổi này chỉ là một phần bổ sung của 802.11i.

Có hai chế được sử dụng trong WPA là Personal và Enterprise nhưng chế độ thường dùng là WPA Personal hay còn gọi là WPA Preshared Key (PSK). Với WPA Personal hệ thống sử dụng một chuỗi ký tự ASCII để xác thực người dùng còn WPA Enterprise sử dụng hệ thống xác thực tập trung RADIUS, nếu như các bạn muốn triển khai hệ thống Wifi xác thực dựa trên thông tin tài khoản của người dùng trong Active Directory thì phải sử dụng chế độ này. Mặc dù WPA Enterprise an toàn và mạnh mẽ hơn so với WPA Personal nhưng do vấn đề triển khai phức tạp nên trong các hệ thống thông thường hay ứng dụng WPA Personal.

WPA sử dụng giao thức TKIP để mã hóa dữ liệu và xác thực người dùng (các máy tính của người sử dụng) cho cả hai trường hợp WPA Personal và WPA Enterprise , TKIP là viết tắt của Temporal Key Integrity Protocol (giao thức toàn vẹn khoá thời gian) có độ an toàn hơn RC4 rất nhiều. Để mã hóa một mạng với WPA Personal (hay PSK), ta cần cung cấp một mật khẩu có độ dài từ 8 đến 63 ký tự. Mật khẩu này sau đó sẽ được kết hợp với SSID thông qua thuật toán TKIP để tạo các khoá mã hoá duy nhất cho từng máy trạm không dây. Các khoá đã được mã hoá này được thay đổi thường xuyên giúp loại bỏ các điểm nhạy cảm mà WEP mang lại.

Đến năm 2004, Wi-Fi Alliance đã công bố đầy đủ tiêu chuẩn IEEE 802.11i với cơ chế xác thực WPA2 như một sợ mở rộng của WPA nhưng sử dụng giao thức mã hóa nâng cao AES, đây là một giao thức được xem như là "không thể bị bẻ khóa", WPA2 có thể sử dụng kết hợp TKIP hay AES trong chế độ mixed mode security cho quá trình mà hóa dữ liệu. Cả WPA Personal và WPA2 Personal sử dụng một chuỗi chia sẽ trước gọi là passphare để xác thức WLAn Client, còn WPA Enterprise và WPA2 Enterprise xác thực WLAN client qua máy chủ RADIUS sử dụng chuẩn 802.1X/Extensible Authenti-cation Protocol (EAP).

Bảng Các Tiêu Chẩn 802.11 Và Giải Pháp WPA Cùng Điểm Yếu

	Mã Hóa	Cơ Chế Xác Thực	Điểm yếu
Original IEEE 802.11 standard	WEP	WEP	Điểm yếu của IV làm cho WEP dễ bị bẻ khóa. Ngoài ra, chỉ có một khóa dùng cho tất cả các WLAN client
WPA	TKIP	Passphrase hay RADIUS (802.1x/EAP)	Passphrase hay pre-shared key yếu có thể bị tấn công và bẻ khóa theo dạng dò từ điển.
WPA2	AES (có thể sử dụng TKIP trong mixed mode)	Passphrase hay RADIUS (802.1x/EAP)	Passphrase hay pre-shared key yếu có thể bị tấn công và bẻ khóa theo dạng dò từ điển.
IEEE 802.11i	AES (có thể sử dụng TKIP trong mixed mode)	Passphrase hay RADIUS (802.1x/EAP)	Passphrase hay pre-shared key yếu có thể bị tấn công và bẻ khóa theo dạng dò từ điển.

Các Dạng Tấn Công Trên Mạng Không Dây

Hình thức tấn công thông dụng trên các mạng không dây (WLAN) là eavesdropping hay sniffing, một hình thức nghe lén và đánh cắp thông tin rất dễ tiến hành trên các hệ thống Access Point được cấu hình mặc định vì các gói tin sẽ được truyền theo cách thức không an toàn với cơ chế truyền broadcast mà không có biện pháp mã hóa nào. Do đó những mật khẩu và tài khoản của người dùng trong các giao thức như FTP, POP3, SMTP dễ dàng bị hacker đánh cắp.

Các mạng WLAN được xác định thông qua tên của chúng là SSID, tên này được gởi dưới dạng không mã hóa trong các gói tin beacon, do đó hacker sẽ dễ dàng phát hiện được tên

những hệ thống mạng WLAN. Mặc dù hầu hết các AP có khả năng cấu hình để ẩn các SSID nhằm hạn chế sự tấn công nhưng đây không hẳn là một chức năng đem đến sự an toàn cao, vì có khá nhiều công cụ có thể phát hiện ra các SSID thông qua những gói tin khác mà chúng bắt được trên mạng. Sau đây là một số hình thức tấn công thông dụng khác mà các hacker thường sử dụng.

AP masquerading hay spoofing : Trong tình huống này các hacker giả mạo làm một trạm phát sóng với thông tin cấu hình giống như các AP hợp lệ, nếu người dùng kết nối đến các AP spoofing này thì thông tin của họ sẽ hoàn toàn chuyển đến cho những kẻ tấn công. Trên các hệ thống máy tính MAC ngày nay có chức năng cho phép một máy chia sẽ kết nối với những hệ thống MAC khác, điều này cũng có thể bị các hacker lợi dụng để tạo ra các AP giả mạo.

MAC spoofing là hình thức tấn công giải mạo địa chỉ MAC để vượt qua sự kiểm soát ở mức vật lý của Access Point (AP). Vì dụ khi AP xác thực các máy tính dựa trên địa chỉ vật lý của card mạng thì hacker sẽ áp dụng hình thức giả mạo này.

Denial of Service : Tấn công từ chối dịch vụ không loại trừ đối với bất kì hệ thống hay dịch vụ nào, và các mạng Wi-fi cũng vậy. Một trong những đặc trừng của hệ thống mạng không dây là có tần số sóng gần với các dãi sóng của thiết bị viba và các thiết bị cầm tay khác, và hacker có thể tận dụng điều này để làm nhiễu loạn môi trường của mạng không dây làm cho chúng không hoạt động được. Ngoài ra, có nhiều công cụ có khả năng gởi nhiều yêu cầu xác thực đến AP làm cho các máy tính hợp lệ khác không thể gia nhập hoặc thậm chi làm tê liệt toàn bộ AP để hacker dựng một hệ thống giải mạo như AP masquerading hay spoofing đã trình bày ở phần trên với mục tiêu đánh cắp thông tin của người dùng.

Tổng Kết

Như vậy, qua chương này chúng ta đã tìm hiểu về các hệ thống mạng không dây và những điểm nhạy cảm của chúng. Để bảo đảm an toàn cho các trạm phát sóng Access Point cũng như môi trường mạng không dây các bạn cần lưu ý những điểm sau đây :

- Sử dụng cơ chế lọc địa chỉ MAC đối với các WLAN nếu khả thi.
- Áp dụng WPA / WPA2 hay 802.11i cho các mạng không dây.
- Đối với các dữ liệu quan trọng cần có một kênh truyền thông an toàn chúng ta nên sử dụng các cơ chế mã hóa tại lớp 3 trong mô hình OSI (network layer) như IPSEC, SSL VPN.
- Bảo vệ chặt chẽ cho dữ liệu mật như tài khoản quản trị, tài khoản mail thông qua các phương pháp mã hóa tại tầng ứng dụng như HTTPS, FTP/SSL (FTP), Secure Shell (SSH).
- Và, tuyệt đối không sử dụng WEP. Do đó, cần nâng cấp các hệ thống phần cứng hay máy tính xách tay sử dụng công nghệ cũ để đưa toàn bộ hệ thống mạng không dây vào hoạt động ở mức an toàn cao hơn, ứng dụng những phương pháp bảo vệ tại Layer 2 như WPA/ WPA2, 802.11i