Module 8
Sniffer

Những Nội Dung Chính Trong Chương Này

Sniffer Là Gì ?

Những Giao Thức Dễ Bị Tấn Công Bởi Sniffer

Các Công Cụ Sniffer

Active Sniff và Passive Sniff

Thế nào là ARP Poisoning ?

Wireshark Capture Và Ứng Dụng Bộ Lọc

MAC Flooding

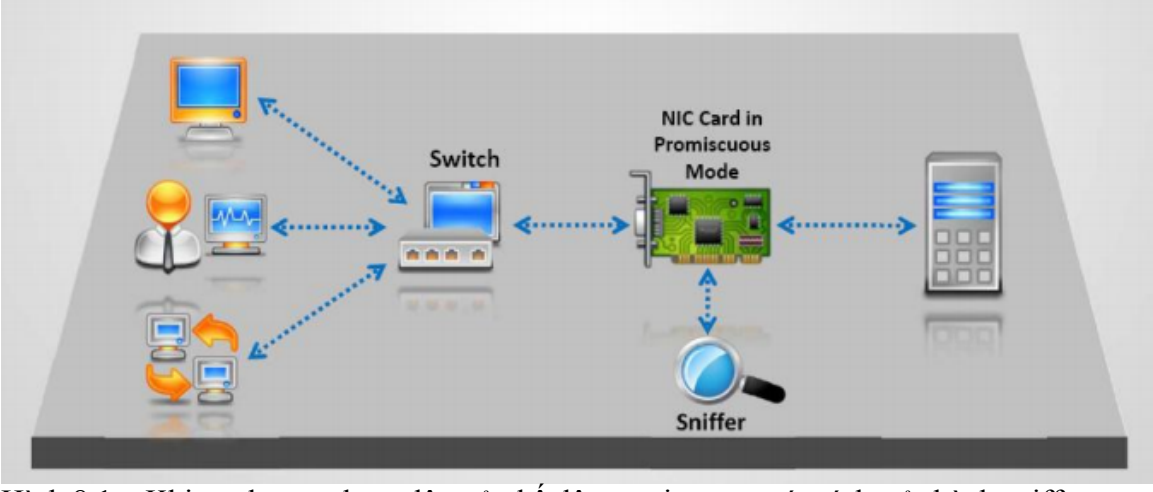
DNS Spoofing

Cách Phòng Chống Sniffer

Sniffer Là Gì ?

Sniffer là thuật ngữ thường dùng của các điệp viên, ám chỉ việc nghe lén thông tin của đối phương. Trong môi trường bảo mật thông tin thì sniffer là những công cụ có khả năng chặn bắt các gói tin trong quá trình truyền và hiển thị dưới dạng giao diện đồ họa hay dòng lệnh để có thể theo dõi dễ dàng. Một số ứng dụng sniffer cao cấp không những có thể đánh cắp các gói tin mà còn ráp chúng lại thành dữ liệu ban đầu như là các thư điện tử hay tài liệu gốc.

Sniffer được dùng để đánh chặn dữ liệu giữa hai hệ thống và tùy thuộc vào công cụ cũng như cơ chế bảo mật được thiết lập mà các hacker có thể đánh cắp các thông bí mật như tài khoản người dùng và mật khẩu đăng nhập vào *Web, FTP, Email, POP3/SMTP* hay các tin nhắn nhanh bằng chương trình Yahoo ! Messenger, Skype, ICQ. Trong chương này chúng ta sẽ thảo luận về cách làm việc của sniffer và những công cụ nghe lén hàng đầu.



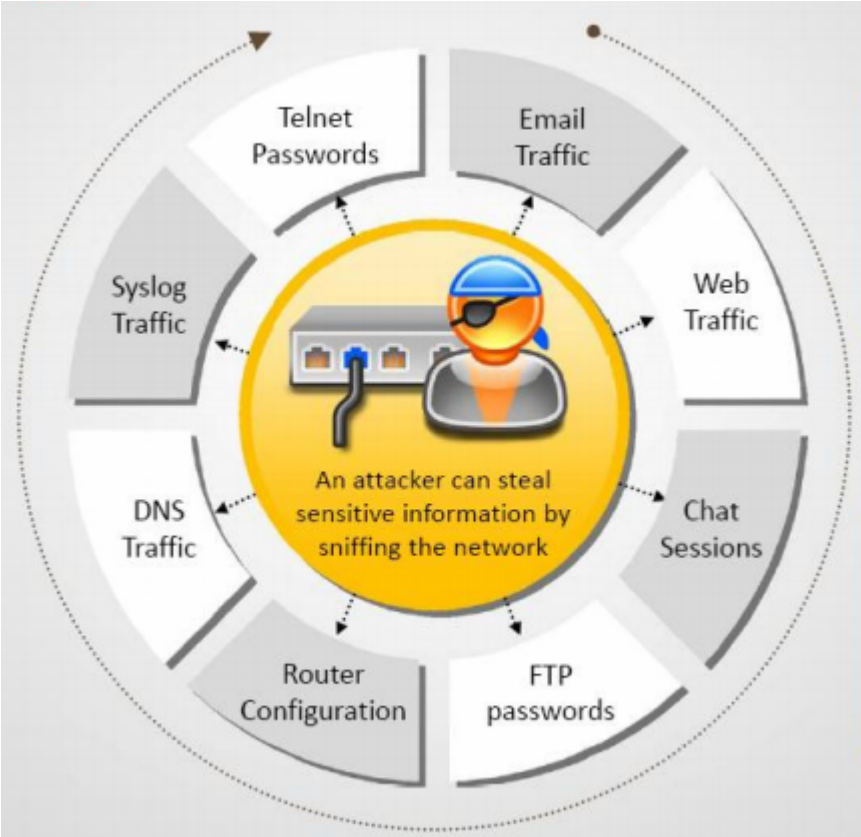
Hình 8.1 – Khi card mạng hoạt động ở chế độ promiscous, máy tính trở thành sniffer

> **Lưu ý** : Thuật ngữ packet (gói tin) dùng để mô tả dữ liệu tại tầng mạng, lớp 3 của mô hình OSI trong khi đó frame đề cập đến dữ liệu tại tầng Data Link (lớp 2). Các frame chứa địa chỉ MAC còn packet chứa địa chỉ IP.

Những Giao Thức Dễ Bị Tấn Công Bởi Sniffer

Thông thường, các máy tính chỉ tiếp nhận các gói tin có địa chỉ đến trùng với địa chỉ MAC của card mạng, những khi một máy tính cài đặt ứng dụng sniffer thì chúng sẽ tiếp nhận tất cả các thông tin cho dù địa chỉ IP nhận có trùng lắp với địa chỉ MAC hay không, khi máy tính hoạt động ở chế độ này được gọi là *promicouse mode* như Hình 8.1, đây là một chế độ đặc biệt mà trong các tổ chức chỉ cho phép quản trị hệ thống hay những người thuộc bổ phận hỗ trợ kỹ thuật được phép sử dụng. Để hoạt động tại chế độ này thì ứng dụng sniffer sẽ cài đặt thêm một chương trình điều khiển đặc biệt cho card mạng, và hầu hết các chương trình sniffer thông dụng hiện nay đều có thể thực hiện chức năng này.

Bất kì giao thức nào không thực hiện mã hóa dữ 1iệu thì về nguyên tắt đều có thể bị hacker tấn công qua hình thức sniffer. Những giao thức thông dụng như HTTP, POP3, Simple Network Mnagement Protocol (SNMP), và giao thức truyền tập tin FTP đều bị sniffer đánh cắp dữ liệu dễ dàng vì thông tin đăng nhập được gởi đi dưới dạng cleartext (không mã hóa).



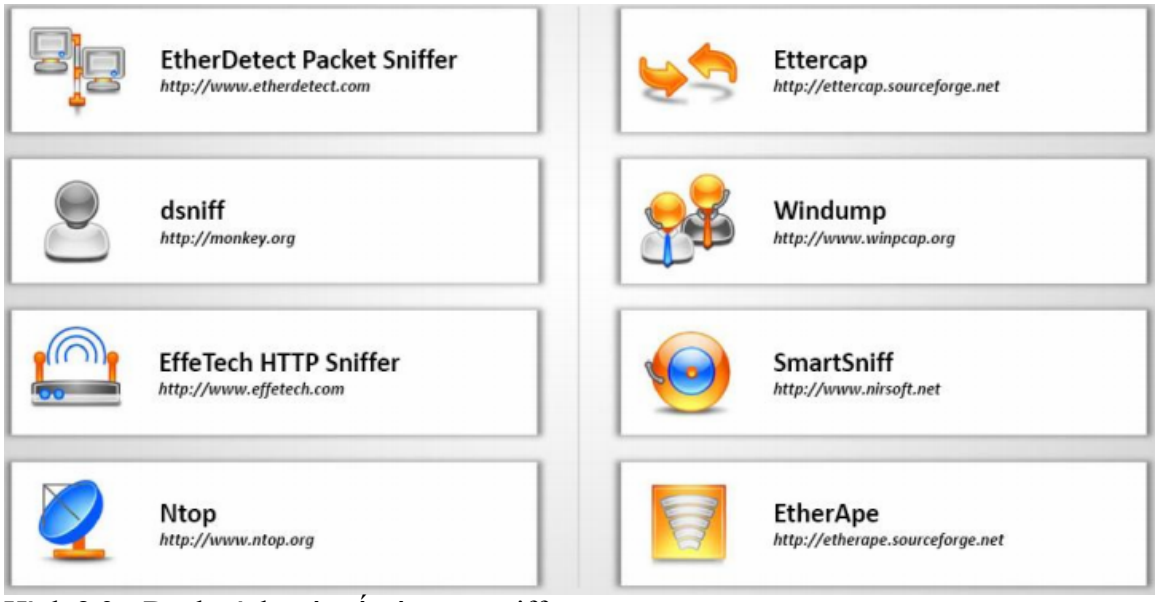
Hình 8.2 - Các ứng dụng và thông tin dễ bị tấn công bởi sniffer

Xem thêm về phần giới thiệu Sniffer tại : http://youtu.be/Y61vSLzv-v0

Các Công Cụ Sniffer

Sniffer không những được sử dụng bởi các hacker mà ngay cả các chuyên gia bảo mật hày những quản trị mạng cũng thường hay sử dụng chúng để dò tìm lỗi, khắc phục sự cố hay tìm kiếm các luồng thông tin bất thường trên hệ thống mạng. Một trong những ứng dụng đó chính là *WireShark*, mà các phiên bản cũ có tên gọi là Ethereal. Hiện nay, WireShark được xếp hạng số 1 trong danh sách các công cụ bảo mật hàng đâu thế giới, hay những công cụ được yêu thích nhất bở các hacker và chuyên gia bảo mật bình chọn tại địa chỉ http://sectools.org/ bởi vì sự mạnh mẽ của nó, ngoài ra Wiresharke còn là ứng dụng nguồn mở và hoàn toàn miễn phí, có thể hoạt động trên cả hệ thống Windows, Linux hay MAC.

Ngoài Wiresharke thì một chương trình nguồn mở khác là Snort cũng có khả năng hoạt động như sniffer trong việc nghe lén các gói tin. Tuy nhiên Snort nổi tiếng vì nó là một hệ thống dò tìm xâm phạm trái phép rất hiệu quả, với khả năng phát hiện sự có mặt của các virus như Conflicker, các cuộc tấn công mạng scan port, tấn công CGI, giả mạo Server Message Block (SMB) hay các dò tìm OS fingerpringting.



Hình 8.3 - Danh sách một số công cụ sniffer.

Active Sniff và Passive Sniff

Có hai dạng nghe lén trên mạng là nghe lén chủ động và nghe lén bị động mà chúng ta sẽ gọi bằng thuật ngữ tương ứng là *active sniff* và *passive sniff*. Trong hai dạng nghe lén này thì passive sniff thường khó phát hiện hơn vì hacker chỉ tiến hành lắng nghe trên đường truyền và bắt giữ lại những gói tin mà không có sự tác động đáng kể nào vào hệ thống, thường thì phương pháp này hay ứng dụng trong môi trường mạng kết nối qua thiết bị hub. Vào khoảng đầu năm 2011 khi tôi còn công tác tại công ty Cyrus một nhân viên đã cố tình chặn bắt các thông điệp thư điện tử của phòng quản trị thông qua cơ chế Passive Sniff nhưng đã bị phát hiện.

Trong khi đó, *active sniff* hay nghe lén chủ động tiến hành gởi các tìn hiệu giả mạo ARP (*Address Resolution Protocol*) hay sử dụng các công cụ làm cho hệ thống mạng hoạt động trên nền Switch (các bộ chuyển mạch) bị ngập tràn các gói tin, thông qua đó hacker sẽ đánh cắp những dữ liệu quan trọng của người dùng trong quá trình truyền. Với phương pháp này hacker sẽ nhanh chóng đạt được mục tiêu của mình nhưng bù lại chúng ta có thể dò tìm và phát hiện ra những ai đang tiến hành tấn công.

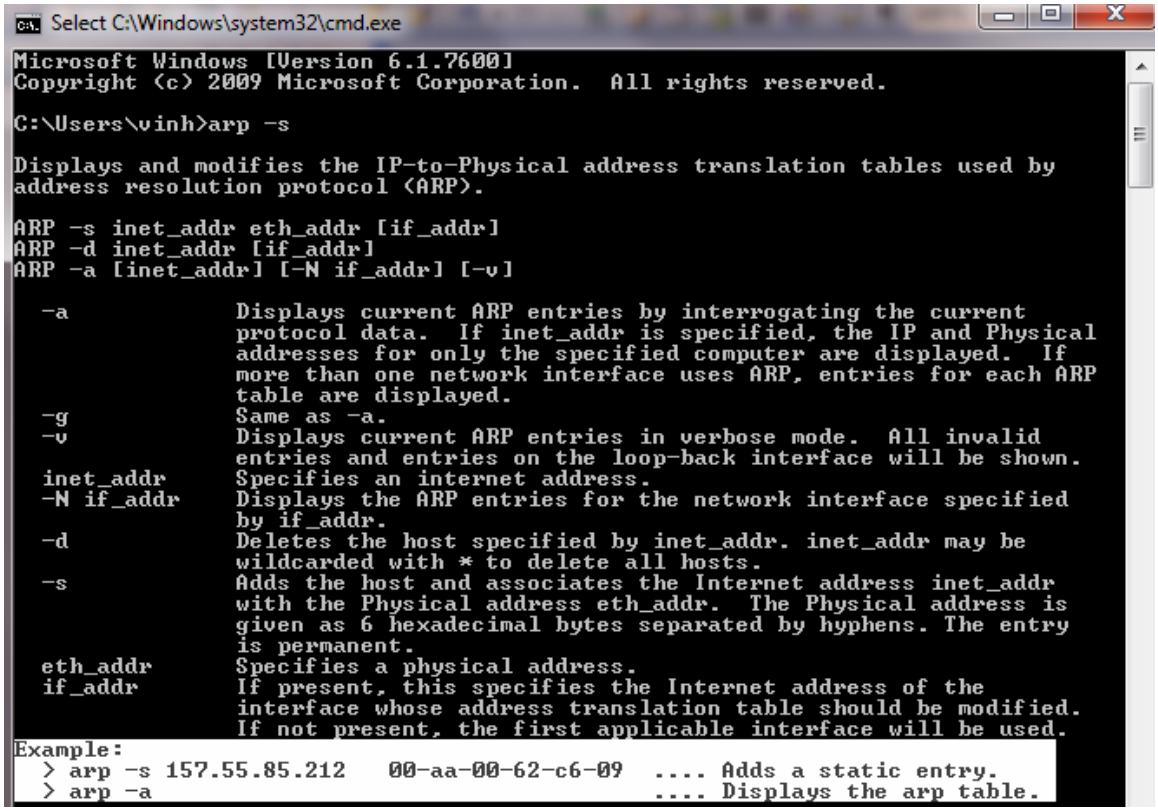
Vậy tại sao các dạng nghe lén trên có thể thành công ? Đó là do trong môi trường mạng kết nối thông qua thiết bị hub thì các gói tin được gởi đi dưới dạng *broadcast*, nghĩa là tất cả các máy tính đều nhận được dữ liệu cho dù địa chỉ nhận có trùng lắp với địa chỉ MAC hay không, do đó hacker chỉ cần đặt hệ thống vào chế độ promocouse là có thể nghe lén được các thông tin một cách dễ dàng với những công cụ như dsniff. Còn đối với hệ thống mạng sử dụng Switch thì khác, ở tình huống này các máy tính truyền thông với nhau theo cơ chế trực tiếp chứ không truyền theo dạng broadcast như tình huống trên, do đó chỉ có máy tính nào có địa chỉ MAC trùng khợp với địa chỉ đích của gói tin mới nhận được các dữ liệu truyền, làm cho hệ thống ít bị nghẽn mạng mà còn phòng tránh được dạng tấn công theo hình thức Passive Sniff.

Thế nào là ARP Poisoning ?

Mặc dù hệ thống dùng switch có thể bảo vệ bạn trước dạng tấn công passive sniff nhưng về bản chất, giao thức phân giả địa chỉ MAC là ARP rất dễ bị tổn thương khi hacker sử dụng phương pháp "đầu độc ARP" mà theo thuật ngữ của CEH là ARP Poisoning. Vậy ARP Poisoning là gì mà nguy hiểm đến vậy. Để có thể hiệu rõ các bạn nên cài thử ứng dụng Wiresharke trên máy tính của mình sau đó giám sát một quá trình Ping đơn giãn chỉ để gởi các thông điệp ICMP ECHO Request đến một máy tính khác trên mạng chúng ta sẽ thấy kết quả trả về nếu máy đó đang hoạt động, và khi theo dõi qua các chương trình giám sát chúng ta sẽ thấy máy truyền sẽ dùng giao thức ARP tung các tìn hiệu theo dạng *broadcast* để hỏi xem địa chỉ MAC của máy nhận là máy nào ? Khi hệ thống mạng hoạt động bình thường chúng ta sẽ nhận được câu trả lời từ chính chủ nhân của địa chỉ MAC gởi về, nhưng nếu có một hacker đang chạy tiến trình đầu độc ARP thì các bạn sẽ nhận được kết quả giả mạo với địa chỉ MAC của máy tính hacker thông qua những công cụ đầu độc ARP hàng đầu như Cain, Ettercap. Kết quả là thay vì máy tính chúng ta đang mở chương trình duyệt mail như ThunderBird cần kết nối đến default gateway để truyền thông tin đăng nhập đến mail server thì các dữ liệu riêng tư này lại gởi đến cho hacker, sau khi bắt giữ tài khoản và password của người dùng thì máy giả mạo vẫn truyền các dữ liệu trên đến máy chủ email thật sự nhằm bảo dảm phiên truyền vẫn diễn ra thành công và nạn nhân không hề hay biết mình đã bị tấn công. Đây là một ví dụ điển hình của dạng tấn công Man In The Middle hay hiểu theo nghĩa đen là "người đàn ông đứng giữa".

Demo tấn công Man In The Middle : http://youtu.be/RVn6vfYGi1E
Hướng dẫn sử dụng Yahoo Monitor Sniffer : http://youtu.be/vnFBsRJ82ZY

Để ngăn ngừa bị đầu độc ARP các bạn cần gán tĩnh thông tin địa chỉ MAC của các máy tính cần truyền thay vì cập nhật động một cách mặc định. Trên hệ thống Windows các bạn sử dụng lệnh arp –s để cập nhật tĩnh thông tin địa chỉ MAC cho từng máy tính như hình minh họa sau đây :



Tuy nhiên, trên các hệ thống mạng lớn phương pháp này gặp nhiều trở ngại, do đó trên các hệ thống mạng sử dụng switch các bạn nên cấu hình cơ chế port-base security để cho phép một địa chỉ MAC hoạt động trên mỗi port.

Wireshark Capture Và Ứng Dụng Bộ Lọc.

Như đã giới thiệu trước đây, Wiresharke là một phiên bản nâng cao của Ethereal và hoàn toàn miễn phí (download tại http://www.wireshark.org/download.html) . Chương trình này có khả năng bắt giữ hầu hết các gói tin truyền trên hệ thống mạng với mọi giao thức khác nhau. Vì vậy Wiresharke thường được các hacker cũng như chuyên gia bảo mật sử dụng trong quá trình nghe lén hay chẩn đoán, khắc phục sự cố mạng. Tuy nhiên, những truyền thông trên mạng khá nhiều làm cho kết quả hiện thị bị tràn ngập những thông tin làm cho khó theo dõi, do đó các bạn cần nắm một số bộ lọc để loại bốt những kết quả không cần thiết và chỉ hiện thị hay bắt giữ các thông tin đáng quan tâm. Sau đây là một số ví dụ ứng dụng bộ lọc của WireSharke :

└ ip.dst eq www.eccouncil.org— Thiết lập này chỉ bắt giữ các gói tin có địa chỉ đích là trang web www.eccouncil.org
└ ip.src == 192.168.1.1— Thiết lập này chỉ bắt giữ các gói tin đến từ máy tính có địa chỉ IP là 192.168.1.1
└ eth.dst eq ff:ff:ff:ff:ff:ff — Thiết lập này chỉ bắt giữ các gói tin được gởi dưới dạng broadcast tại lớp 2 của mô hình OSI.

Các bạn có thể tham khảo video hướng dẫn về Wiresharke và phân tích một quá trình Three-way Handshake tại : http://www.youtube.com/watch?v=5zOGCHqre84

Hình 8.4 - Hướng dẫn dùng Wireshark

MAC Flooding

Như vậy, các bạn đã thấy sự khác biệt của dạng tấn công passive sniff và active sniff được sử dụng tùy theo hệ thống mạng dùng hub hay switch. Với cơ chế đầu độc ARP các hacker có thể giả mạo địa chỉ MAC để bắt giữ các thông tin trái phép. Ngoài phương pháp này thì hacker có thể sử dụng những công cụ làm tràn ngập mạng bởi các gói tin hay tín hiệu ARP giả mạo để thiết bị switch không hoạt động được theo cơ chế truyền trực tiếp mà phải chuyển qua cách truyền thông broadcast thông thường như các thiết bị hub vẫn hay dùng. Điều này cũng xảy ra khi hệ thống mạng có nhiều tiến trình đầu độc ARP đang diễn ra bằng Ettercap, lúc đó các bạn sẽ thấy đèn tín hiệu của thiết bị switch nhấp nhày liên tục hay thậm chí bị treo buộc phải khởi động lại thì mới hoạt động được.

Kỹ Thuật DNS Spoofing

Spoofing có nghĩ là giả mạo, vậy thuật ngữ DNS Spoofing hay còn gọi là DNS poisoning là kỹ thuật là cho máy chủ DNS chấp nhận những thông tin phân giải địa chỉ IP giả mạo và lưu trữ các thông tin này trên dữ liệu cache, sau đó là gởi về cho các máy trạm (DNS client) khi các máy này có nhu cầu phân giải các thông tin DNS đã bị hacker giả mạo. Ví dụ như khi các bạn muốn truy cập vào trang web www.netpro.edu.vn thì lại bị phân giải qua địa chỉ IP của www.security365.vn . Điều này thật sự nguy hiểm khi chúng ta truy

cập vào trang paypal hay các tài khoản ngân hàng trực tuyến để thực hiện giao dịch nhưng lại bị dẫn sang những web giả mạo có chủ ý đánh cắp tài khoản của người dùng. Đây là một hình thức tấn công rất nguy hiểm vì người dùng khó mà phát hiện ra một khi đã "tin tưởng" vào máy chủ DNS mà mình đã cấu hình hay được cấu hình. Để có thể tấn công theo hình thức này các hacker sẽ tìm cách khai thác các máy chủ DNS bị lỗi để buộc chúng chấp nhận các thông tin không hợp lệ, đây là một hình thức tấn công gián tiếp nhưng tác động mạnh lên kết quả phân giải của người dùng.

Không giống trong môi trường thật, chúng ta có thể nghi ngờ khi nhận được những chỉ dẫn sai để đi đến một nơi nào đó, các máy tính hoàn toàn tin tưởng khi nhận được các đáp ứng từ nơi mà chúng cho là xuất phát từ những nguồn tin cậy. Sau đây là một số kỹ thuật *DNS Spoofing* thông dụng :

- Intranet spoofing—hoạt động như là một thiết bị trên cùng lớp mạng nội bộ.

- Internet spoofing—hoạt động như một thiết bị trên internet

- Proxy server DNS poisoning—thay đổi các chỉ mục DNS trên proxy server để chuyển hướng người dùng đến một trạm đích khác.

- DNS cache poisoning— thay đổi chỉ mục DNS trên bất kì hệ thống nào để chuyển hướng người dùng đến một trạm đích khác.

Các Công Cụ Tấn Công DNS Spoofing

EtherFlood : Được sử dụng để làm tràn ngập một hệ thống Ethernet switch và làm nó hoạt động như hub. Với cách này hacker có thể bắt giữ tất cả những truyền thông trên lớp mạng chứ không chỉ những gói tin được gởi và nhận từ chính máy của họ.

Dsniff : Gồm tập hợp nhiều công cụ khác nhau có thể chạy trên Windows và Linux (tuy nhiên khi sử dụng Dsniff trên Linux sẽ đạt hiệu quả tốt hơn với đầy đủ các tính nang của nó). Những chức năng mà dsniff cung cấp gồm có bắt giữ các thông điệp thư điện tử với mailsnarf, bắt giữ tập tin với filesnarf, đánh cắp thông điệp chat với msgsnarf… Tuy nhiên, ứng dụng này chỉ hoạt động hiệu quả trong môi trường hub với cơ chế passsive sniff, trên các hệ thống mạng sử dụng Ethernet switch thì dsniff không có tác dụng.

Packet Crafter : Được dùng để tạo ra các gói tin TCP/UDP đã được tùy biến lại ví dụ đổi địa chỉ nguồn của các gói tin hay thiết lập các cờ theo mục đích riêng của hacker như đặt cờ RST yêu cầu hệ thống nhận phải reset lại các kết nối, sữa đổi giá trị tuần tự sequence number …

Cain & Able : Mặc dù dsniff mất tác dụng trong môi trường mạng chuyển mạch với thiết bị switch, nhưng các hacker có thể sử dụng Cain & Able với sức mạnh hơn nhiều có khả năng chặn bắt các gói tin thông qua bước đầu độc ARP để điều

hướng các dữ liệu nhạy cảm về máy của hacker và đánh cắp thông tin nhạy cảm của người dùng. Ngoài ra, cain & Able có khả năng bắt cả những gói tin voice ip của Skype, giả mạo chứng chỉ điện tử để thâm nhập các hộp thư Gmail, Yahoo hay bẻ khóa mật khẩu của hệ thống mạng không dây, mật khẩu mã hóa với MD5.

SMAC : Dùng để thay đổi địa chỉ MAC của một hệ thống, cho phép hacker giả mạo địa chỉ phần cứng khi tấn công vào một mục tiêu nào đó, qua mặt được cơ chế kiểm tra dựa trên địa chỉ MAC.

MAC Changer : Công cụ dùng để thay đổi địa chỉ MAC trên Unix/Linux, cho phép hacker giả mạo địa chỉ phần cứng và cả thông tin của nhà sản xuất.

WinDNSSpoof : Một công cụ đơn giãn chạy trên Windows dùng để giả mạo địa thông tin DNS. Thông thường, hacker kết hợp WinDNSSpoof với một ứng dụng có khả năng đầu độc ARP để mang lại hiệu quả cho WinDNSSpoof trên các hệ thống mạng dùng thiết bị swicth.

Distributed DNS Flooder : Có khả năng gởi một số lượng lớn các yêu cầu truy vấn đến máy chủ DNS, tạo ra một cuộc tấn công từ chối dịch vụ (DOS) khiến cho máy chủ DNS không thể đáp ứng các yêu cầu thật của máy khách.

Cách Phòng Chống Sniffer

Để phòng chống bị nghe lén hay đánh cắp thông tin chúng ta cần cẩn thận khi truy cập tại các hệ thống mạng công cộng như sân bay, quán cà phê wifi. Trong trường hợp cần phải kiểm tra thư hay truy cập thông tin bí mật trên những hệ thống mạng không an toàn nên sử dụng cơ chế mã hóa hay dùng VPN. Có những giải pháp VPN miễn phí rất hiệu quả trong môi trường mạng không dây như giải pháp dùng Hot Pot Shield (http://anchorfree.com/)

Ngoài ra, các bạn có thể cài đặt chương trình dò tìm và phát hiện các sniffer ở trên mạng như XARP, ứng dụng này sẽ cảnh báo ngay khi phát hiện có một dấu hiệu khả nghi xuất hiện như có máy tính đang hoạt động ở chế độ *promicouse* hay đang tiến hành ARP poisoning. Các bạn có thể download chương trình XARP tại đây http://www.chrismc.de

Nếu hệ thống mạng được quản lý thông qua máy chủ Active Directory thì giải pháp phòng chống đơn giãn như đã đề cập cấu hình địa chỉ MAC tĩnh đối với default gateway cho tất cả các máy tính thông qua chính sách an ninh của toàn vùng kết hợp với một kịch bản chạy khi khởi động, để tất cả các máy tính đề được cập nhập thông tin này sau khi khởi động. Vì chúng ta cập nhật thông tin này thông qua lệnh arp –s thông thường thì khi máy tính khởi động lại dữ liệu trên sẽ bị xóa.

Các bạn có thể tham khảo bài hướng dẫn của tôi về phòng chống sniffer theo cơ chế này tại đại chỉ http://www.youtube.com/watch?v=SfW3a-KZdPo

Tổng Kết

Như vậy, trong chương này chúng ta đã thảo luận về một chủ đế rất quan trọng đó là tấn công dưới dạng nghe lén. Các bạn đã phân biệt được thế nào là Active Sniff và Passive Sniff cũng như thế nào là MAC Flooding, DNS Spoofing kèm theo đó là những giả pháp phòng chống thích hợp. Có một bài thực hành phòng chống sniffer mà tôi đã trình bày trogn chương trình đào tạo CEH là sử dụng công cụ AntiNetcut 3, đây là ứng dụng chạy được trên hệ thống Windows XP, Windows 7 và hoàn toàn miễn phí. Khi cài đặt công cụ này các bạn có thể bảo vệ mình khỏi sự dòm ngó của các sniffer một cách tư động.

Trong chương tới chúng ta sẽ tìm hiểu về dạng tấn công phi kỹ thuật Social Engineering.