Module 11
Session Hijacking

Những Nội Dung Chính Trong Chương Này

Giới Thiệu Về Session Hijacking

Phân biệt Spoofing và Hijacking

Các dạng tấn công Session Hijacking

Dự Đoán Các Số Hiệu Tuần Tự

Quy Trình Session Hijacking

Công Cụ Tấn Công Session Hijacking

Phòng Chống Session Hijacking

Session Hijacking Là Gì ?

Tiếp theo, chúng ta sẽ tìm hiểu về chủ đề *Session Hijacking*, một hình thức tấn công phổ biến nhắm vào các người dùng mạng xã hội như Facebook hay những hộp thư Gmail, Yahoo. *Session Hijacking là hình thức tấn công vào phiên làm việc giữa client và server cách đánh cắp cookie của người sử dụng sau khi họ đã qua bước xác thực với máy chủ, sau đó sẽ chiếm quyền điều khiển của phiên làm việc này*. *Session* là thuật ngữ nói đến một phiên kết nối giữa hai máy tính trên hệ thống mạng thường được duy trì bởi các giá trị như thời gian tồn tại của session, thông tin cookie của trình duyệt hay các thẻ bài thích hợp. Các bạn có thể xem lại phần giới thiệu về phiên làm việc và quá trình three-way handshake ở những chương trước.

Trong đại hội *Blackhat* năm 2009 một hacker đã làm ngỡ ngàng khán thính giả vì đã trình diễn trực tiếp một phương pháp đột nhập vào hộp thư của phóng viên BBC đang tham dự hội thảo và gởi thư trước mặt cử tọa trong hội trường. Phương pháp tấn công này được chuyên gia bảo mật trên đặt tên là *Side jacking*, một thuật ngữ không thấy xuất hiện trong CEH nhưng cũng thuộc dạng tấn công *Session Hijacking*.

Phân biệt Spoofing và Hijacking

Tấn công *spoofing* khác với dạng tấn công *hijacking*. Vi trong tình huống tấn công *spoofing* các hacker sẽ nghe lén dữ liệu truyền trên mạng từ người gởi đến nơi nhận sau đó sử dụng các thông tin thu thập được giả mạo địa chỉ (hoặc sử dụng ngay các địa chỉ đã lấy trộm) nhằm qua mặt các hệ thống kiểm tra. Trong khi đó hình thức tấn công *hijacking* sẽ làm cho kết nối của nạn nhân đến máy chủ bị ngắt khi đã xác thực thành công sau đó cướp lấy phiên làm việc này của người dùng nhằm vượt qua bước kiểm tra của máy chủ.

Quá trình tấn công *Session Hijacking* gồm có ba bước như sau :

- Dò Tìm Session : Hacker sẽ dò tìm các session đang mở và tính toán giá trị tuần tự của gói tin tiếp theo.
- Tái Đồng Bộ Kết Nối : Hacker gởi các tín hiệu TCP reset (RST) hay FIN để yêu cầu khởi động lại quá trình kết nối đồng thời đóng phiên làm việc cũ.
- Chèn Các Packet Tấn Công : lúc này hacker sẽ gởi đến máy chủ những gói tin TCP với số hiệu tuần tự đã được tính toán thích hợp với phiên làm việc do đó máy chủ sẽ chấp nhận những thông tin này giống như là các dữ liệu hợp lệ tiếp theo của người dùng bị tấn công. Nghĩa là, khi này các hacker có thể gởi đi một thông điệp trên chính Wall của nạn nhân bằng tài khoản Facebook của người bị tấn công như Hình 11.1

Hình 11.1 – Tình huống tấn công Hijacking bằng *Add-on Firesheep* cài trên Firefox, truy cập vào session Facebook của một người dùng khác trên cùng mạng, sau đó gởi thông điệp *Post By FireSheep*.

Các dạng tấn công Session Hijacking

Có hai dạng *Session Hijacking* đó là **chủ động** và **bị động**. Khác biệt chính giữa hai hình thức *hijacking* này phụ thuộc vào sự tác động của hacker lên phiên làm việc của người sử dụng trong môi trường mạng. Ở trạng thái chủ động hacker sẽ tìm các phiên làm việc đang hoạt động và chiếm đoạt nó thông qua các công cụ và tính toán các giá trị tuần tự của gói tin trong *TCP session*. Ngược lại, ở tình huống tấn công *hijacking* thụ động thì các kẻ tấn công chỉ theo dõi và ghi lại tất cả những truyền thông được gởi bởi người sử dụng hợp lệ, các bạn có thể thấy tình huống này rất giống với nghe lén vì nó sẽ thu thập các thông tin quan trọng của người dùng như mật khẩu đăng nhập để tiến hành xác thực cho các lần xâm nhập trái phép sau này trên một *session* khác.

Three-Way Handshake

Chức năng chính của TCP trong mô hình OSI là vận chuyển các gói tin giống như tên gọi của nó là Transmission Control Protocol. Để thực điều này TCP sử dụng các gói tin báo nhận (ACK) cùng với số hiệu tuần tự (sequence number). Tận dụng các số hiệu này là một trong những điểm then chốt của TCP Session Hijacking, do đó để hiểu rõ về dạng tấn công này các bạn cần xem lại các khái niệm cơ bản của quá trình bắt tay ba bước đã trình bày trong phần đầu của giáo trình :

1. Khi người dùng hợp lệ khởi tạo một kết nối đến máy chủ ví dụ kết nối đến trang Facebook để liên lạc với bạn bè hay Flickr để chia sẽ hình ảnh với người thân thì máy tính của anh ta sẽ gởi một gói tin có chứa tín hiệu SYN yêu cầu đồng bộ và một giá trị ISN (I*nitial Sequence Number*) ban đầu .

2. Máy chủ Facebook hay Flickr tiếp nhận gói tin này và phản hồi bằng một thông điệp được thiết lập bằng cờ SYN cùng với ISBN của máy chủ, kèm theo đó là cờ ACK được xác định với số hiệu được khởi tạo của người gởi cộng thêm 1.

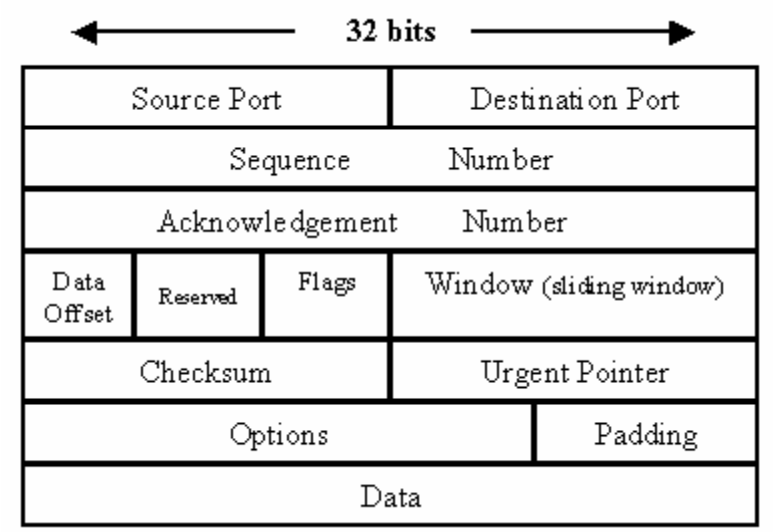
3. Tiếp theo máy tính của người dùng hợp lệ sẽ thông báo bằng gói tin với cờ Ack được thiết lập cùng với giá trị ISN của máy chủ cộng thêm 1 để bắt đầu phiên làm việc.

Kết nối này có khả năng bị đóng khi hết thời gian do mạng bị *lag* (bị trễ) hay kết nối có thể bị kết thúc khi nhận được các yêu cầu là những gói tin với cờ FIN hay RST được đặt.

Khi nhận được tín hiệu RST thì kết nối sẽ bị đóng và tất cả các gói tin tiếp theo bị từ chối, còn khi nhận được tín hiệu đóng bằng cờ FIN thì các gói tin đang xử lý vẫn được tiếp nhận cho đến khi hoàn tất thì kết nối mới kết thúc. Và việc gởi những tín hiệu với cờ FIN hay RST là phương pháp chính mà các hijacker (những hacker tấn công hijacking) sử dụng để đóng các session của client với server và sau đó chiếm quyền điều khiển, hoạt động như là client hợp lệ.

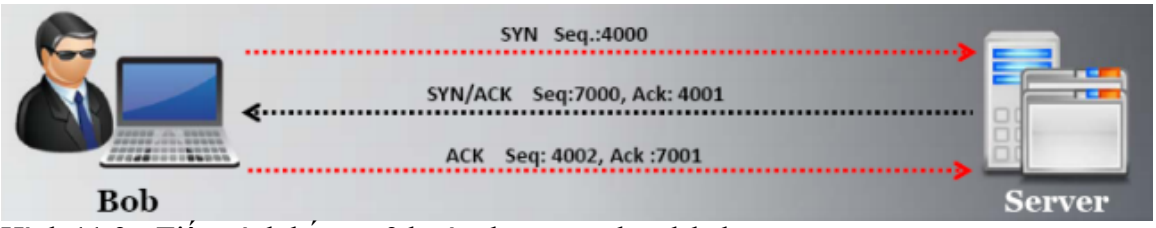
Hacker Dự Đoán Các Số Hiệu Tuần Tự Như Thế Nào ?

TCP là một giao thức hướng liên kết có nhiệm vụ tổng hợp các gói tin (packet) bị phân mãnh khi truyền thành dữ liệu gốc. Vì vậy mỗi packet cần được cấp một giá trị duy nhất theo thứ tự gọi là sequence nember (SN), ngoài ra mỗi packet còn được gán giá trị session để máy nhận có thể hợp nhất các luồng packet thành dữ liệu gốc ban đầu. Nếu các packet không đến đích theo một trật tự như ban đầu thì sequence number sẽ giúp cho việc sắp xếp chúng theo đúng trình tự. Ngoài ra, một hệ thống khởi tạo TCP session bằng cách gởi gói tin với cờ SYN được thiết lập và gói tin này được gọi là synchronize packet có chứa các giá trị khởi tạo ISN (Initial Sequence Number) như Hình 11.2.



Hình 11.2 – Cấu trúc của gói tin

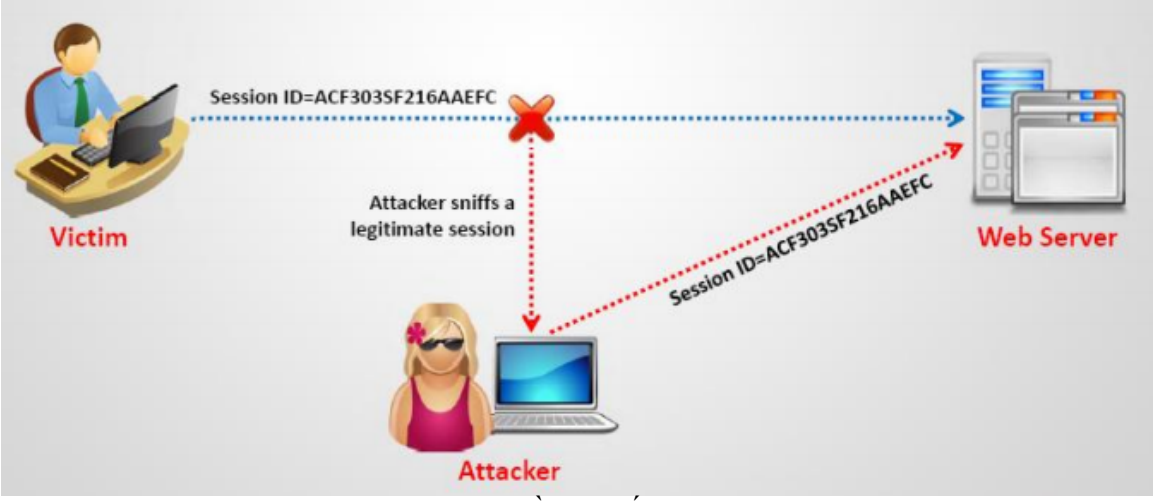
Và khi các gói tin có chứa thông tin báo nhận ACK được gởi đi thì các máy tính sẽ sử dụng số SN của ACK này cộng thêm một đơn vị. Cũng lưu ý là việc cộng một này chỉ áp dụng trong quá trình three-way handshake, với các truyền thông khác thì giá trị cộng thêm bằng với kích thược của gói tin, ví dụ chúng ta truyền 45 byte dữ liệu thì ACK đáp ứng sẽ lấy số SN của ACK nhận cộng với 45.



Hình 11.3 - Tiến trình bắt tay 3 bước three-way handshake

Nắm được cơ chế này của quá trình bắt tay ba bước hacker đã tạo ra các công cụ có thể xác định giá trị SN của những gói tin, trước tiên hacker sẽ nghe lén truyền thông giữa hai máy tính để rồi xác định giá trị ISN và tính ra giá trị tiếp theo. Tuy nhiên đây không phải là một việc đơn giãn như khi chúng ta trình bày nguyên tắt hoạt động của chúng vì các gói tin di chuyển với tốc độ cực nhanh, nếu như hacker không *sniff* (nghe lén) được gói tin thì họ cũng không thể tiến hành tấn công Session Hijacking. Vì vậy hầu hết các công cụ tấn công Session Hijacking thông dụng đều kèm theo ứng dụng cho phép nghe lén các gói tin nhằm xác định ra giá trị SN.

Vi dụ khi hacker tấn công Side jacking trong môi trường wifi sử dụng bộ công cụ gồm hai chương trình là ferret.exe và hamster.exe (http://erratasec.blogspot.com) , trong đó ferret có nhiệm vụ nghe lén thông tin trên mạng wifi.



Hình 11.4 - Attacker nghe lén đường truyền khi tấn công Session Hijacking

Sau khi nghe lén dữ liệu truyền và xác định được giá trị SN kế tiếp thì các chương trình tấn công sẽ tiến hành giả mạo địa chỉ IP (IP Spoofing) của hệ thống hợp lệ đã khởi tạo session với máy chủ rồi gởi các gói tin với giá trị SN thích hợp nhằm sử dụng session đã được tạo ra và vượt qua quá trình xác thực. Như vậy các bạn sẽ đặt câu hỏi là nếu như cả máy tấn công và nạn nhân cùng gởi các gói tin với giá trị SN thích hợp thì sao ? Thường thì hacker sẽ chạy các chương trình làm cho máy tính của nạn nhân bị *reset* lại kết nối bằng cách gởi các gói tin với cờ RST được đặt.

Các Bước Trong Quá Trình Session Hijacking

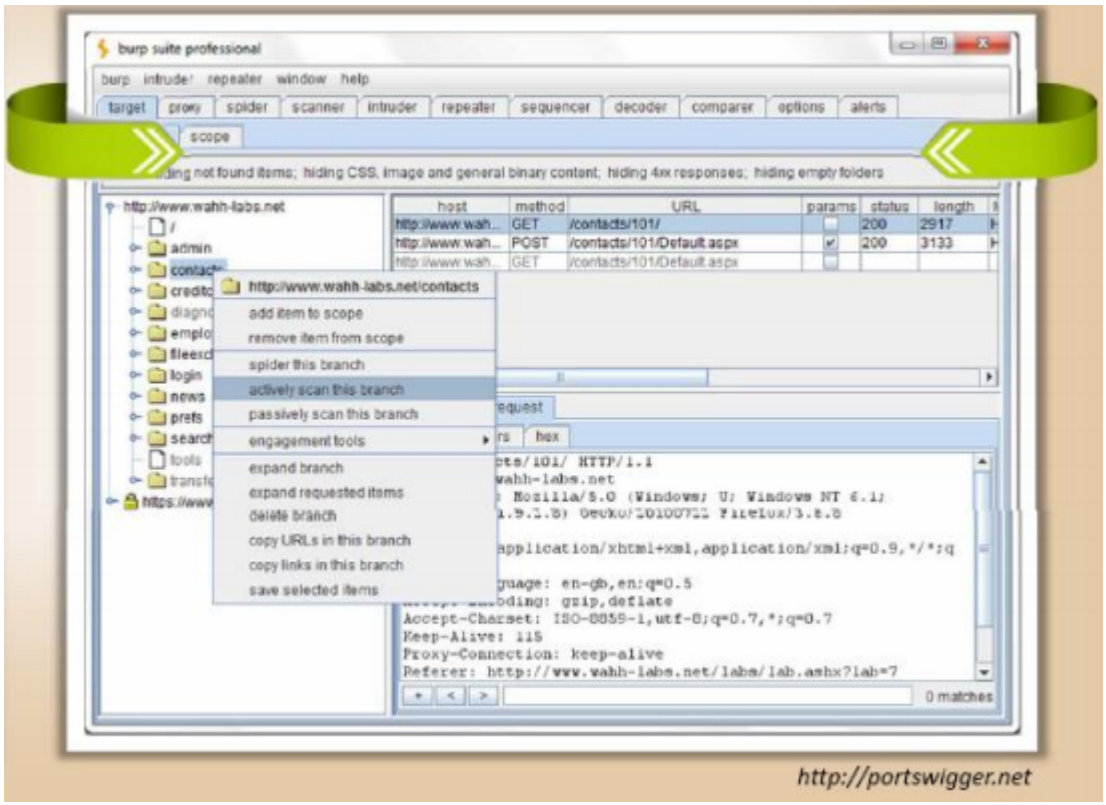
Để tiến hành tấn công Session Hijacking thì hacker cần thực hiện các bước sau :

- **Tracking Session** : Trong bước này hacker cần xác định các session đang hoạt động và tính được giá trị SN kết tiếp của gói tin.
- **Desynchronizing** : Hacker tiến hành đóng kết nối của nạn nhân để chiếm toàn bộ session của họ thông qua các công DoS hay gởi những tín hiệu reset đến máy tính người dùng.
- **Gởi Các Gói Tin Đã Được Chèn Giá Trị SN Hợp Lệ Đến Máy Chủ** : Kết nối như người dùng đã xác thực.

Các Công Cụ Tấn Công Session Hijacking

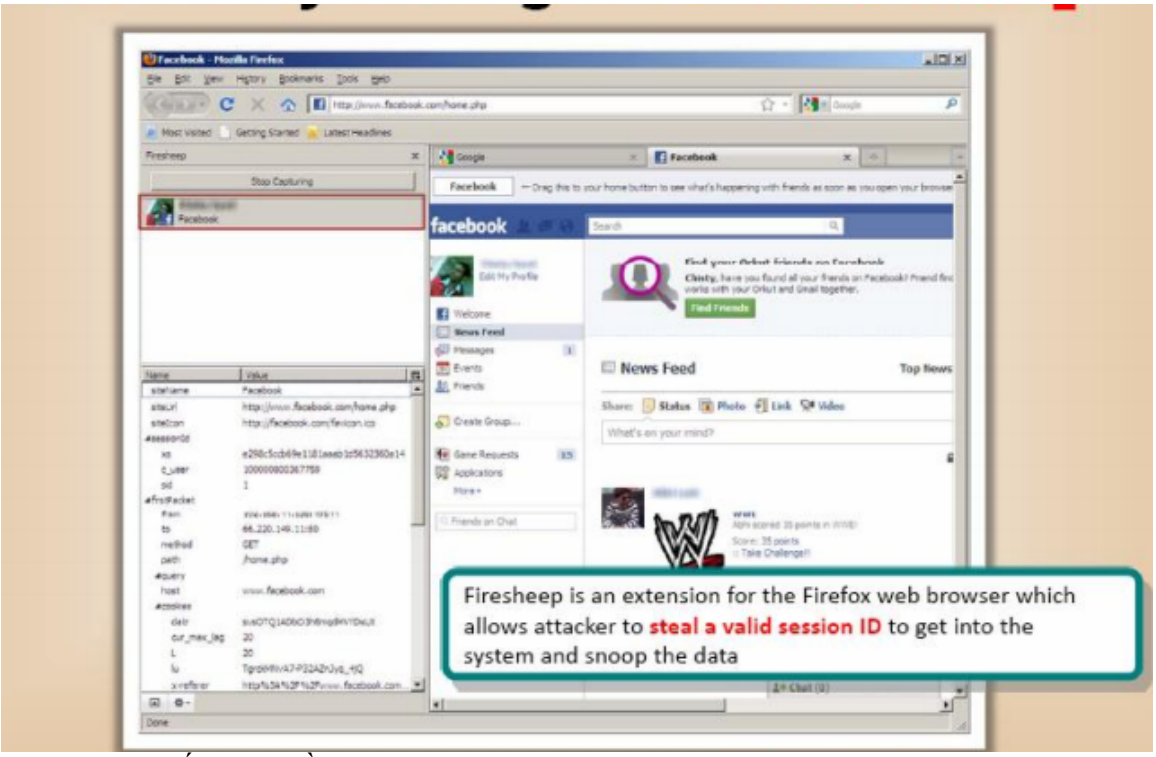
Có khá nhiều công cụ có thể tiến hành tấn công Session Hijacking đã được phát triển trước đây như ***Juggernaut*** chuyên sniff các TCP session trong môi trường mạng hoạt động với hub. Hoặc **Hunt** với chức năng giả mạo địa chỉ MAC với cơ chế *ARP spoofing*, *reset* và giám sát các kết nối, nghe lén đường truyền.

Hiện nay, nhiều công cụ mạnh mẽ khác được phát triển giúp cho hacker có thể tiến hành tấn công Session Hijacking dễ dàng hơn. Trong số đó phải kể đến Burp Suite, ứng dụng có mặt trong danh sách 125 công cụ bảo mật hàng đầu hiện nay có khả năng thay đổi dữ liệu trên quá trình truyền, đánh cướp session hay giả mạo cả các chứng chỉ điện tử dùng trong xác thực ***https***



Hình 11.5 - Giao diện Burp suite

Trong môi trường mạng không dây thì *Firesheep* (http://codebutler.github.com/firesheep/) có lẽ là công cụ nổi tiếng nhất xuất hiện vào khoảng giữa năm 2011, một add-on mạnh mẽ của Firefox (các phiên bản Firefox từ 4 trở lên không cài đặt được Firesheep) cho phép kẻ tấn công dễ dàng nghe lén và đánh cắp session của người dùng khi truy cập Facebook, Flicker … Để chống lại add-on này các bạn nên sử dụng một add-on khác có tên gọi là *Blacksheep* được hack5.org mô tả tại đây http://hak5.org/hack/blacksheep-%E2%80%93-firesheep-defense



Hình 11.6 – Tấn công bằng Firesheep

Ngoài ra, trong quá trình đào tạo về an ninh mạng cho các tổ chức tôi cũng thường hay đề cập đến một ứng dụng thú vị là **Tamper Data**, thường được các hacker sử dụng để thay đổi các tham số truyền đến máy chủ, ví dụ khi người dùng chơi các game online như nông trại trên facebook, bắn chim … họ có thể dễ dàng thay đổi điểm số của mình để đánh lừa máy chủ game. Các bạn có thể tham khảo bài hướng dẫn thực hành về Tamper Data tại http://www.youtube.com/watch?v=Z8yYei50Sxk.

Những Mối Nguy Hiểm Của Session Hijacking

Có phóng viên của tạp chí nổi tiếng đã mất nhiều thời gian để sưu tâm và viết bài về một vụ án được nhiều người quan tâm, nhưng khi bài báo chuẩn bị lên khuôn thì trên mạng đã xuất hiện rất nhiều tin tức liên quan đến chủ đề này khiến cho chính tác giả phải ngạc nhiên, vì không biết tại sao thông tin đã bị lộ dù anh ta nói rằng mình đã cài đặt đầy đủ chương trình bảo vệ, phòng chống virus …Nguyên nhân là phóng viên này đã sử dụng máy tính trong các quán ca phê Wifi thiếu cẩn trọng bị hacker tấn công Session Hijacking đột nhập vào hộp thư điện tử lấy đi các tin bài quan trọng.

Do đó, trong vài trò của một chuyên gia bảo mật hay CEH chúng ta cần hướng dẫn người dùng tránh sử dụng máy tính trong môi trường công cộng (*un-trusted*) thiếu cẩn trọng, vì dạng tấn công Session Hijacking rất dễ tiến hành, đặc biệt là trong môi trường mạng không dây thì tỉ lệ thành công rất cao. Trong chương trình đào tạo về an toàn thông tin cho các cán bộ của Tổng Cục Hải Quan tôi có trình bày một tình huống Side Jacking để

minh họa tác động của nó và khi học viên thực hành trong môi trường thực tế thì hầu hết đều cho rằng đạt kết quả thành công.

Vậy Làm Sao Phòng Chống Session Hijacking ?

Để phòng chống không bị tấn công Session Hijacking thì chúng ta cần phòng tránh bị nghe lén, một khi hacker không thể nghe lén được thì cũng koh6ng thể tấn công vào session của người dùng. Một torng các giải pháp đế tránh các sniffer chính là mã hóa dữ liệu, mã hóa đường truyền với các kỹ thuật như dùng Secure Shell (SSH thay cho Telnet thông thường) khi quản trị từ xa hay áp dụng Secure Socket Layer (SSL dùng cho truyền thông qua HTTPS).

Ngoài ra chúng ta có thể ngăn không cho hacker tương tác vào đường truyền cũng giúp loại bỏ nguy cơ bị tấn công này, với những giải pháp hữu hiệu như dùng mạng riêng ảo (VPN), hay áp dụng IPSEC. Nhiều ý kiến còn cho rằng khi truy cập internet ở môi trường công cộng hãy dùng các thiết bị DCOM 3G cũng giảm đáng kể nguy cơ mất mát dữ liệu. Sau đây là một số khuyến nghị nhằm ngăn ngừa Session Hijacking :

- Sử dụng mã hóa.
- Ứng dụng các giao thức an toàn.
- Hạn chế các kết nối đầu vào.
- Giảm các truy cập từ xa.
- Có chế độ xác thực mạnh mẽ.
- Huấn luyện cho người dùng, nâng cao nhận thức an toàn thông tin.
- Sử dụng các thông tin truy cập khác nhau cho các tài khoản khác nhau.

Tổng Kết

Trong chương trên chúng ta đã thảo luận về một hình thức tấn công thông dụng, dễ tiến hành và đặc biệt nguy hiểm trên các hệ thống mạng không dây đó là tấn công **Session Hijacking**. Các bạn đã nắm những công cụ mạnh hay được sử dụng hiện nay cũng như các hướng dẫn kèm theo, và trong vai trò CEH chúng ta cần biết rõ tác hại của Session Hijacking cũng như giải pháp phòng chống để có thể bảo vệ dữ liệu cho chính mình và hướng dẫn người dùng các thao tác nhằm bảo vệ tính riêng tư, phòng chống bị mất cắp dữ liệu. Trong phần tiếp theo chúng ta sẽ thảo luận về một chủ đề rất được quan tâm là "Tấn Công Web Server".