Module 12
Hacking web server

Những Nội Dung Chính Trong Chương Này

Cách Tấn Công Thông Dụng Vào Máy Chủ Web

IIS Unicode Exploit

Tấn Công Web Server Qua Lỗi Của Hệ Thống

Tấn Công Từ Chối Dịch Vụ

Patch Management

Công Cụ Tấn Công

Kiện Toàn Bảo Mật Cho Máy Chủ Web

Sự nổi tiếng của hacker phần lớn là do những cuộc tấn công vào các trang web hay máy chủ web để đánh cắp thông tin thẻ tín dụng, tài khoản ngân hàng hay lấy đi dữ liệu mật và công bố trên website của mình như *Wikileak*. Bởi vì web server hay máy chủ web là các thành phần "online 24/7" của các tổ chức và doanh nghiệp nên chúng thường là các mục tiêu chính để các hacker nhắm tới, một khi đã xâm nhập được vào hệ thống máy chủ web các hacker sẽ tiếp tục dò tìm và thâm nhập đến các hệ thống khác trong mạng nội bộ hay tiến hành *deface* trang web, một khái niệm chúng ta sẽ tìm hiểu sau đây.

Trong vai trò một CEH hay hacker mũ trắng chúng ta cần hiểu rõ những cách thức tấn công mà hacker sử dụng để khai thác thông tin hay các điểm yếu thông dụng của máy chủ web gồm :

- Lỗi cấu hình của phần mềm máy chủ web.
- Lỗi bảo mật của hệ điều hành hay của những ứng dụng chạy trên máy chủ web.
- Thiếu các bản vá lỗi hay hệ thống không được cập nhật đầy đủ, và việc sử dụng các thông tin mặc nhiên sau khi cài đặt cũng là nguyên nhân làm cho máy chủ web bị tấn công.
- Thiếu các chính sách an toàn thông tin và những thủ tục vận hành hợp lý.

Thông qua các khe hỡ này hacker sẽ khai thác để chiếm quyền điều khiển hay thâm nhập vào các máy chủ web, từ đây họ có thể leo thang tấn công sang các thành phần quan trọng khác của hệ thống như thâm nhập mạng nội bộ, tấn công vào máy chủ cơ sở dữ liệu hay các dịch vụ mạng quan trọng khác của tổ chức.

Cách Tấn Công Thông Dụng Vào Máy Chủ Web

Các tình huống tấn công mà hacker thường thực hiện trên các web server là deface web site, đây là thuật ngữ nói đến hành động hacker đột nhập vào web server và thay đổi trang chủ của website bằng một nội dung khác. Ví dụ để lại các lời nhắn mang tính chất chính trị, hay thay đổi hình ảnh nhằm bôi xấu đơn vị chủ quản của website. Đối với những hacker thích khoe thành tích thì những thông điệp để lại là thông tin của chính họ trong thế giới mạng. Sau đây là những phương pháp mà các hacker có thể dùng để tấn công :

- Tìm cách bắt giữ tài khoản quản trị của web server hay web site thông qua nghe lén hay tấn công man in the middle. Một trong những ví dụ điển hình là hacker nghe lén khi quản trị viên bất cẩn sử dụng telnet để điều khiển máy chủ từ xa, hay thậm chí khi web master sử dụng các giao thức an toàn như SSH để truy cập từ xa vẫn có khả năng bị hacker đánh cắp thông tin tài khoản qua hình thức giả mạo chứng chỉ điện tử (*fake certificate*).

- Bẽ khóa mật khẩu quản trị bằng các công cụ brute-force

- Tấn công DNS để điều hướng người dùng sang một trang web khác.

- Tác động lên dịch vụ FTP hay Email server.

- Khai thác các bug (lỗi bảo mật) của ứng dụng web hay web server.

- Lợi dụng các tài nguyên chia sẽ trên máy chủ web được cấu hình không hợp lý, hay việc gán quyền bị sai như cho phép người dùng bất kì được phép upload và thực thi các chương trình.

- Sử dụng các lỗi trong lập trình cơ sở dữ liệu để tiêm các chỉ thị nguy hiểm vào hệ thống mà chúng ta thường nghe đến với thuật ngữ SQL Injection.

- Điều hướng người dùng đến các trang web khác thông qua những phương pháp spoofing DHCP, DNS hay đánh cắp cookie nhằm tiến hành tấn công vào phiên làm việc của client và web server (còn được gọi là session hijacking).

IIS Unicode Exploit

IIS Unicode Exploit là một lỗi bảo mật trên các hệ thống máy chủ web chạy trên nền IIS 5 chưa được patch (vá lỗi). Lỗi ảnh hưởng đến các thành phần mở rộng của ISAPI như .ASP hay các kịch bản CGI cho phép hacker có khả năng thao tác trên hệ thống thư mục của máy chủ. Điểm đặc biệt nguy hiểm là các hệ thống IIS 5 được cài đặt mặc định trên Windows 2000 Server nên rất hay bị hacker khai thác, vì nhiều tổ chức khi triển khai các máy chủ trên nền Windows 2000 Server không hề hay biết rằng dịch vụ IIS được cài kèm theo với những điểm yếu chết người mà hacker có thể tấn công để làm gãy đổ toàn bộ hệ thống. Theo thông kê các lỗi bảo mật trên IIS version 5 là những nguyên nhân làm cho các website của nhiều tổ chức tại Việt Nam bị deface.

Hình 12.1 - Giao diện một trang web bị deface

Về cơ bản, Unicode sẽ chuyển đổi các kí tự của bất kì ngôn ngữ nào sang định dạng chung có thể sử dụng trên toàn cầu, mang lại sự thuận tiện cho người dùng trong việc phải suy nghĩ lựa chọn một bảng mã nào để tương thích được với đa số người xem. Các

hacker sẽ tận dụng sự diễn dịch sai do thiếu kiểm soát tính hợp lệ của các dữ liệu đầu vào trên IIS để sao chép, upload hay thậm chí thực thi chương trình trái phép trên máy chủ web. Nếu các bạn cần truy cập vào trang web http://www.netpro.etc thì yêu cầu sẽ được xử lý bằng cách tìm kiếm tập tin index.html hay defaul.html trên thư mục gốc đặt tại *C:\inetpub\wwwroot\index.html* , đây là đường dẫn đến thư mục local trên các web server, đường dẫn này có thể khác nếu như web master tùy biến trong quá trình cài đặt.

Khi chúng ta truy cập đến các nội dung có tên bao gồm những khoảng trắng thì trình duyệt sẽ chuyển kí tự khoảng trắng này thành *%20*, đây là mã Unicode của kí tự khoảng trắng trong bộ mã ASCII. Như vậy thì các hacker cũng sẽ dùng Unicode để diễn dịch các chỉ thị mà chúng muốn web server hiểu và thực thi. Ví dụ khi hacker muốn thực hiện việc hiển thị nội dung của ổ đĩa *C:* trên trình duyệt thì họ cần chạy dòng lệnh cmd.exe trên trình duyệt, đây là một lệnh nội trú trong thư mục */winnt/system32/* của ổ đĩa hệ thống do đó cần phải chuyển ngược lên các thư mục bên trên với lệnh DIRUP mà chúng ta hay dùng thông qua cú pháp như "CD ../../"

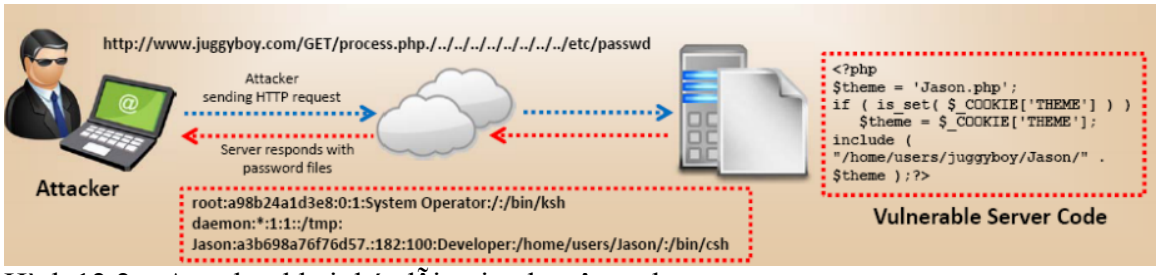
Vậy kẻ tấn công sẽ thử thực hiện dòng lệnh sau trên trình duyệt :

http://www.netpro.etc/scripts/..%255C..%255C/winnt/system32/cmd.exe?/c+dir+c:\

Để hiểu câu lệnh trên chúng ta cần xem qua các tùy chọn của lệnh cmd.exe (các gía trị sau dấu ***?*** được xem là các đối số để thực hiện lệnh và các mã unicode của kí tự ASCII, ở đây **../../** sẽ chuyển thành **%5C** sau đó chuyển đổi các kí tự thêm một lần nữa thì máy chủ web mới hiểu và thực thi được. Dưới đây là một số kí tự ASCII và mã unicode tương ứng :

ASCII.....	UNICODE
%.....	%25
5.....	%35
C.....	%43

Nếu như web server của www.netpro.etc dùng phiên bản IIS 5 chưa được vá lỗi thì trên trình duyệt web sẽ hiển thị toàn bộ nội dung của ở đĩa **C:** trên máy chủ. Tương tự, hacker có thể sử dụng những lệnh khác để tiến hành khai thác sau hơn, chỉ cần chuyển đổi các lệnh thành những mã unicode hợp lệ.



Hình 12.2 – Attacker khai thác lỗi unicode trên web server

Mặc dù đây là một lỗi thuộc dạng hết hạn sử dụng, chỉ dùng để minh họa nhưng nhiều web site chạy trên máy chủ Windows 2000 Server vẫn có thể gặp phải. Website tại Việt Nam bị ảnh hưởng bởi lỗi này như www.cantho.gov.vn và đã từng bị hacker thâm nhập.

Tấn Công Web Server Qua Lỗi Của Hệ Thống

Ngoài các lỗi của máy chủ web thì hacker còn tấn công vào hệ điều hành nếu phát hiện ra các khiếm khuyết bảo mật. Trong thời gian 2010 – 2011 có khá nhiều máy chủ web tại Việt Nam được cài đặt trên Windows Server 2003, và tích hợp cả hệ thống phân giải tên miền DNS đã bị hacker tấn công chiếm quyền điều khiển từ xa với những công cụ như Metasploit Framework. Các bạn có thể tham khảo một bài hướng dẫn thực hành khi đào tạo về an ninh mạng cho Tổng Cụ Hải Quan vào năm 2012 tại http://youtu.be/oImK2NaTnXI.

Tấn Công Từ Chối Dịch Vụ

Trong trường hợp hệ thống được bảo vệ chặt chẽ và hầu như không có điểm yếu thì hacker sẽ tấn công từ chối dịch vụ bằng cách dùng mạng botnet để gởi một số lượng cự lớn các yêu cầu kết nối, dạng tấn công này chúng ta đã biết qua thuật ngữ DDoS. Ngoài ra, khi phần mềm máy chủ web có lỗi cũng có thể bị hacker sử dụng những công cụ tấn công từ chối dịch vụ như OWASP HTTP Post Tool (http://www.youtube.com/watch?v=lYQFF4Ki8_s).

Patch Management

Patch Management là thuật ngữ chỉ tiến trình cập nhật các bản vá lỗi gồm *patch* (các bản vá lỗi tổng quát) và *hotfix* (những xử lý lỗi cho một tình huống khẩn cấp nào đó) của hệ thống để bít lại các lổ hỗng bảo mật ngăn không cho hacker lợi dụng để xâm nhập trái phép. Việc cập nhật các bản vá hay *hotfix* cần được thực hiện đầy đủ bao gồm xác định các phiên bản thích hợp, kịp thời và cần phải kiểm tra trên các máy thử nghiệm nhằm bảo đảm không có những sự cố nào xảy ra khi ứng dụng các bản cập nhật này.

Trong một số tình huống các lổ hỗng đã được phát hiện nhưng nhà sản xuất chưa có bản vá lỗi tương ứng thì chúng ta cần tìm hiểu phương pháp xử lý thủ công như thiết lập các cơ chế kiểm soát riêng hay tạm tắt các dịch vụ nếu thấy cần thiết. Các lỗi dạng này hay được đề cập bằng thuật ngữ *Zero Day* (0-Day).

Công Cụ Tấn Công

N-Stalker Web Application Security Scanner cho phép chúng ta kiểm tra các ứng dụng web có khả năng bị khai thác thông qua các điểm yếu như XSS, SQL injection, buffer overflow hay không.

Metasploit Framework là một ứng dụng miễn phí được tích hợp sẵn nhiều mã khai thác và payload nguy hiểm chuyên dùng để tấn công các web server. Phiên bản hiện nay của Metasploit là Version 4.2 có thể chạy trên hệ thống Windows hay Linux 32 / 64 bit. Ngoài ra, các bạn có thể chạy Metasploit trực tiếp mà không cần cài đặt trên đĩa Live DVD BackTrack 5 R1 (phiên bản mới nhất vào thời điểm hiện tại).

Core Impact và SAINT Vulnerability Scanner là những công cụ khai thác thương mại chuyên dùng cho mục đích kiểm tra và tấn công các phần mềm máy chủ web.

OWASP HTTP Post Tool là công cụ tấn công và kiểm định bảo mật cho máy chủ web được phát triển bởi OWASP, có thể tấn công từ chối dịch vụ các máy chủ web sử dụng Apache bị lỗi.

Phương Pháp Kiện Toàn Bảo Mật Cho Máy Chủ Web

Để phòng chống bị tấn công các *administrator* của máy chủ web hay *web master* cần tiến hành thao tác kiện toàn bảo mật thường được gọi là tiến trình ***hardening***, sau đây là một số bước mà các CEH cần thực hiện để tăng độ vững chắc cho máy chủ :

- Thay đổi tên tài khoản quản trị, không dùng tên mặc dịnh là administrator và dùng các mật khẩu mạnh, được thay đổi thường xuyên.

- Tắt các trang web và trang FTP mặc định.

- Gỡ bỏ các ứng dụng không cần thiết trên máy chủ như dịch vụ WebDAV. *Cần lưu ý WebDAV là một trong những tác nhân chính làm cho các website ở Việt Nam bị hacker tấn công*. Các lổ hỗng của WebDAV xuất hiện trong IIS phiên bản 6 chưa được vá.

- Cấu hình máy chủ web ngăn không cho duyệt thư mục.

- Đặt các thông báo nhằm cảnh báo hacker không được thâm nhập trái phép và phá hoại với những hình phạt tương ứng mà pháp luật quy định.

- Áp dụng các bản vá lỗi và cập nhật mới nhất cho hệ điều hành và cho cả các ứng dụng chạy trên hệ điều hành này.

- Tiến hành kiểm ta các khu vực tiếp nhận dữ liệu đầu vào nhằm loại bỏ khả năng bị khai thác thông qua hình thức chèn mã độc hay các chỉ thị nguy hiểm.

- Tắt chức năng quản trị từ xa nếu không thật sự cần thiết.

- Bật chức năng auditing và logging để ghi lại các chứng cứ và dấu vế mà hacker để lại.

- Sử dụng firewall ở giữa web server và internet để kiểm tra chặt chẽ các yêu cầu truy cập và luồng dữ liệu. Chỉ mở những cổng cần thiết như 80, 443, 22 …

- Thay thế phương pháp gởi dữ liệu với hàm GET bằng hàm POST để không hiện thị thông tin khi truyền từ client đến server.

Tổng Kết

Đề phòng chống và bảo vệ cho các máy chủ web cũng tương tự như các hệ thống máy chủ khác đó là chúng ta cần tiền hành hardening các máy tính dùng để cài phần mềm web server, thông thường các máy được áp dụng chế độ bảo mật cao nhất như vậy được gọi là Bastion Host. Thường xuyên kiểm tra lỗi bảo mật của hệ thống và các ứng dụng với những chương trình quét lỗi mạnh mẽ như Retina, GFI NSS hay NESSUS. Lọc và thay thế các kí tự đặc biệt mà hacker hay dùng để tấn công như phòng tránh cross site scripting ta có thể thay thế các kí tự “<” và “>” với “<” và “>” .