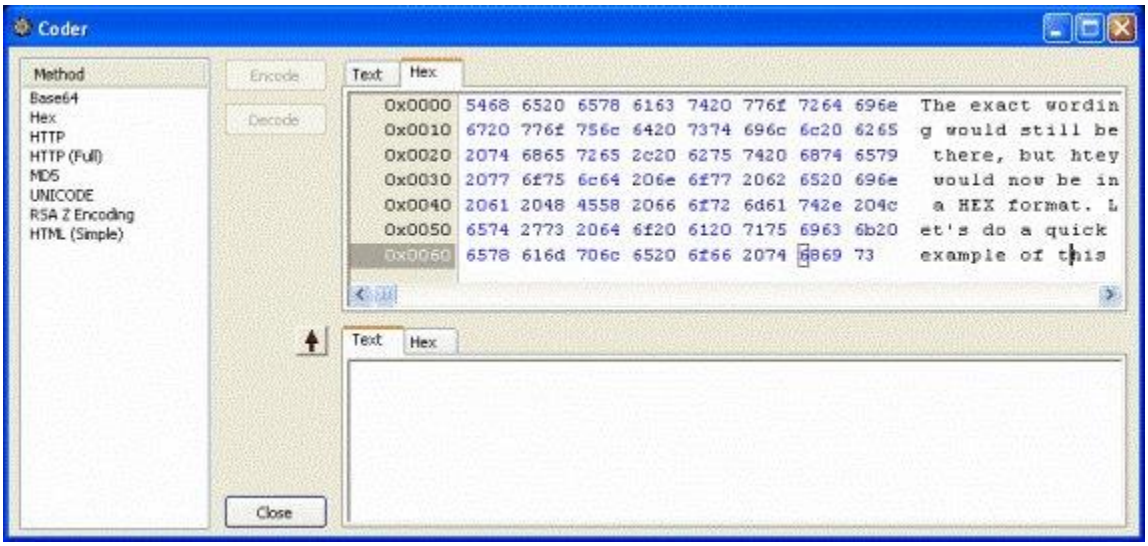
IDS đối với việc tấn công ứng dụng Web

Trong thế giới mạng trước nay luôn tồn tại một thế giới hack ứng dụng web cũng có thể được xem như một thế giới hoang dã. Có nhiều thứ mới và luôn xảy ra không giống như mong đợi. Các tấn công đó thường khai thác lỗ hổng trong các ứng dụng web hay kỹ thuật mã hóa để vòng tránh được sự phòng chống của mạng. Với một môi trường hoạt động liên tục như vậy chúng ta cần phải nắm chắc được những điều cơ bản cốt lõi của vấn đề. Trên hết, các quản trị viên hệ thống cũng như những người bảo mật mạng phải có được kiến thức hiểu biết về vấn đề này. Nếu bạn là người sẽ quản trị và thường xem các hành vi bất thường đối với mạng của mình thì sự khó khăn mà bạn sẽ cảm nhận được đó là làm sao có thể nắm bắt được toàn bộ thế giới hack các ứng dụng web. Có nhiều lĩnh vực liên quan đến nó bạn nên quan tâm nhưng ở đây chúng tôi sẽ giới thiệu cho các bạn một lĩnh vực được thiết lập ở mức cao đó là việc mã hóa.

Mã hóa là gì?

Mã hóa là một quá trình biến đổi thông tin từ một định dạng này sang một định dạng khác. Lấy một ví dụ đó là tất cả các từ được viết trong bài báo này, chúng đang được thể hiện dưới định dạng ASCII. Điều gì sẽ xảy ra nếu mã hóa nó thành định dạng HEX? Ý nghĩa chính xác của các từ trong bài báo vẫn còn y nguyên nhưng lúc này chúng sẽ được hiển thị dưới định dạng HEX. Hãy thực hiện nhanh một ví dụ trong trường hợp này.



Hình 1

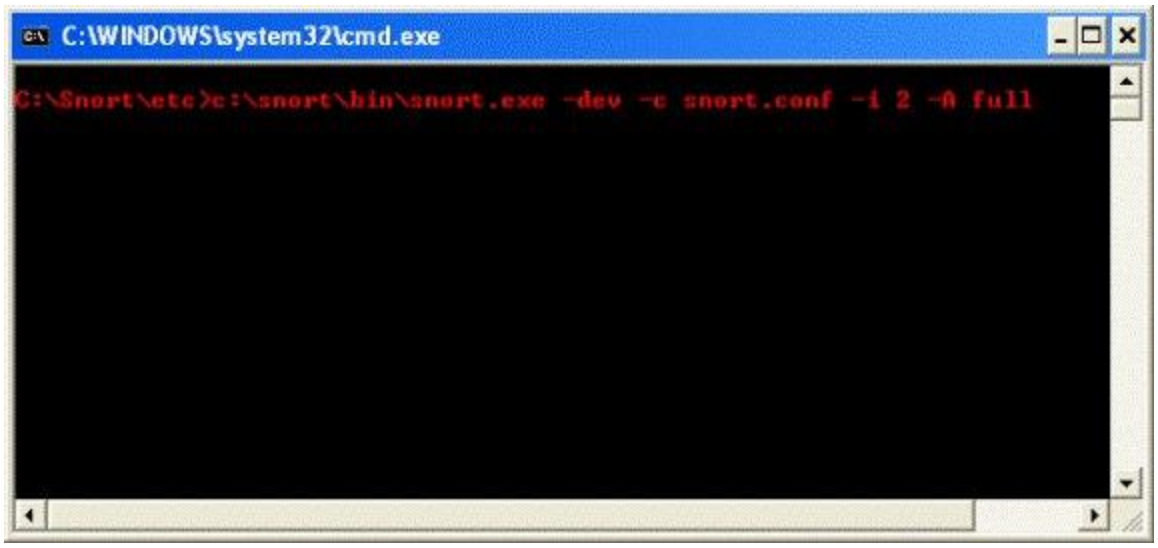
Bây giờ chúng ta có thể thấy trong phần hiển thị cửa sổ bên trong, ở phần bên trái có một số giá trị HEX, còn bên phải có một vài câu có định dạng ASCII mà tác giả bài này đã viết trong đó. Cả hai đều chỉ ý một nội dung nhưng trong các định dạng khác nhau. Chúng ta có thể cho rằng không có giá trị gì khi mang một tài liệu này và mã hóa nó sang một định dạng khác. Tuy nhiên trong một ví dụ điều đó chưa nói hết lên được các vấn đề, mã hóa thực sự sẽ như thế nào với việc hack ứng dụng web thực và trông nó sẽ ra sao? Đây là một câu hỏi thú vị, chúng ta hãy tập trung và giải quyết câu hỏi này. Những gì sẽ sử dụng cho ví dụ của chúng ta là lỗi Directory Traversal cổ điển. Nhiều bạn có thể đoán được một số từ trong chúng, những gì lỗi này cho phép bạn thực hiện là điều hướng đến thư mục cha của website.

Môi trường phân tích

Các công cụ và các chương trình mà chúng tôi sẽ sử dụng để giới thiệu một số tấn công ứng dụng web và có thể phát hiện ra chúng là:

- Snort
- Web browser
- Encoding tool

Bạn có thể thấy được không có nhiều yêu cầu để thực hiện thành công việc hack phát hiện đối với một số ứng dụng web. Bạn cũng có thể sử dụng HTTP proxy bổ sung cho mỗi trình duyệt web hay bất cứ thứ gì bạn thích. Nếu thực hiện điều này cho máy khách thì chúng tôi sẽ sử dụng bộ BURP HTTP proxy. Bây giờ chúng ta sẽ bắt đầu khởi động Snort để nó có thể xem xét và kiểm tra các gói đến máy tính, nơi chúng ta đã có Apache webserver đang chạy.



Hình 2

Bạn có thể thấy được trong hình trên, chúng tôi đã đánh thức và chỉ định Snort thông qua các khóa chuyển đổi –i 2, đó chính là giao diện giúp nó có thể theo dõi. Đây là do chúng tôi đang sử dụng Snort và Apache webserver trong VMware image. Điều đó có nghĩa là sẽ có nhiều NIC cho Snort. Chúng ta phải chỉ ra một thứ để Snort sẽ kiểm tra cho chúng ta. Bây giờ hãy nhìn trong phần màn hình tiếp theo với một ví dụ rất cơ bản trong việc tấn công các ứng dụng web, và như đã đề cập từ trước nó là lỗ hổng Directory Traversal.

Hình 3

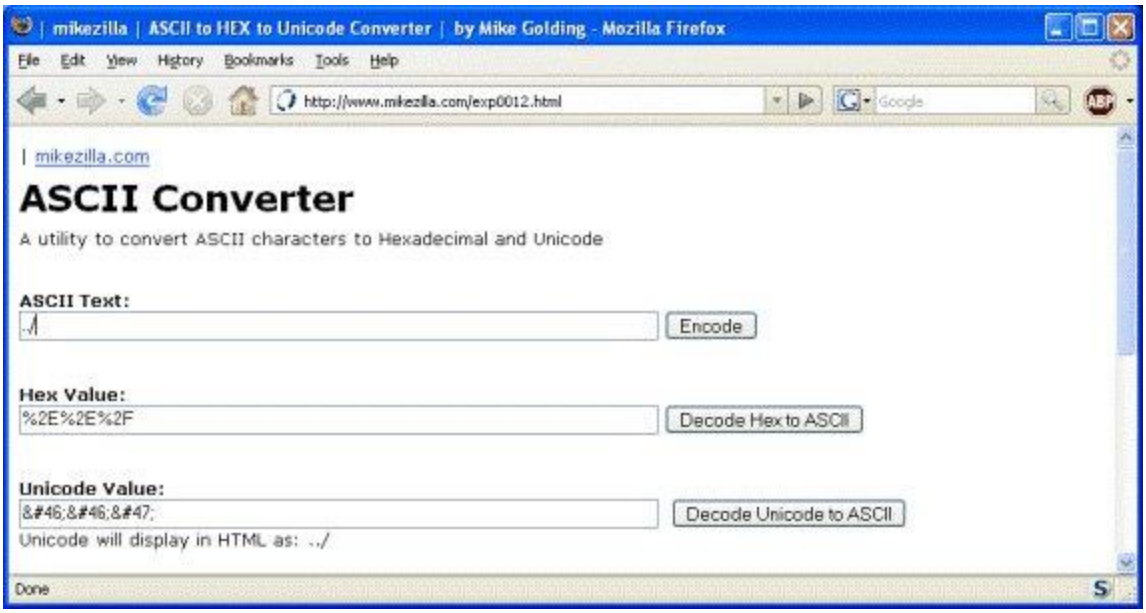
Vậy Apache webserver được đánh thức và đang chạy. Hãy đưa đầu vào Directory Traversal với định dạng gốc của nó và xem xem những gì xảy ra. Trước khi thực hiện điều này hãy bảo đảm rằng bạn phải có Snort đang chạy để xem những gì xảy ra nếu nó phát hiện ra cố gắng tấn công nào đó.

Hình 4

Chúng ta hãy xem trong màn hình **../** là những gì Directory Traversal cho ta thấy. Khi bạn gửi nó đến Apache webserver bạn sẽ thấy rằng bản thân nó sẽ không thực hiện bất cứ thứ gì, nó dường như bỏ qua. Chúng ta sẽ xem xét ngắn gọn những gì mà Snort đã phát hiện được. Hãy mã hóa nó trong một định dạng khác.

Hình 5

Những gì chúng ta đã thực hiện lúc này là mã hóa ../ sang môi trường HEX tương đương.



Hình 6

Lúc này, khi gửi lỗ hổng Directory Traversal đã mã hóa HEX đến Apache web browser thì bạn một lần nữa lại thấy không có gì xảy ra. Chúng ta sẽ kiểm tra xem những gì Snort đã nhìn thấy ở phía sau. Hãy thử lại nó một lần nữa với phiên bản mã hóa UNICODE.

Hình 7

Nhập vào đó phiên bản mã hóa mới Directory Traversal này và quan sát những gì xảy ra. Bạn sẽ thấy Apache phản hồi lại một mã trạng thái HTTP 404. Điều đó nghĩa rằng URL không được tìm thấy trên máy chủ. Vì vậy chúng ta phải thử cả ba phiên bản khác nhau đối với Directory Traversal và không cái nào trong chúng làm việc. Hãy kiểm tra xem những gì Snort thông báo.

C:\Snort\etc\log>more alert.ids

[**] [119:18:1] (http_inspect) WEBROOT DIRECTORY TRAVERSAL [**]
05/31-10:18:51.262616 0:17:31:8A:93:7F -> 0:C:29:BA:DC:9E type:0x800 len:0x1F4
192.168.111.2:2780 -> 192.168.111.7:80 TCP TTL:128 TOS:0x0 ID:16806 IpLen:20 Dgm Len:486 DF
*****AP*** Seq: 0x805DCAAC Ack: 0xF13CBB87 Win: 0xFFFF TcpLen: 20**

C:\Snort\etc\log>

Không vấn đề gì với Snort

Với dấu hiệu WEBROOT DIRECTORY TRAVERSAL đã cho chúng ta thấy rằng hack ứng dụng web cũ này đã bị phát hiện bởi Snort. Điều này đã được thực hiện không cần tới việc mã hóa tấn công ../ gốc theo nhiều định dạng khác nhau. Bây giờ chúng ta hãy đề cập đến tấn công Directory Traversal. Có rất ít khả năng điều này sẽ tránh được đối với tất cả các modern IDS. Điều đó có nghĩa rằng, thế giới hack các ứng dụng web là một thế giới khổng lồ. Có khá nhiều kiểu hack khác còn có thể đe dọa chúng ta.

Vấn đề khi nói đến việc tấn công các ứng dụng web là nhiều ứng dụng này không được kiểm tra thích hợp hoặc thậm chí bỏ qua việc thẩm định mã. Như vậy chúng có thể chứa rất nhiều lỗ hổng đối với vô số các tấn công. Một trong những cách đơn giản nhất để tăng kiến thức về hack các ứng dụng web cho bạn là tự cố gắng tái tạo chúng. Không gì giúp một ai đó hiểu tốt hơn bằng tự thực hiện. Khi bạn đã tự đưa mình đến, thì có thể muốn thực hiện điều gì đó khi IDS đang kiểm tra lưu lượng. Điều này sẽ cho bạn có được ý tưởng phát triển các dấu hiệu IDS cho mối đe dọa SQL injection hoặc bất cứ tấn công nào mà bạn đang tái tạo. Các dấu hiệu thường sẽ không được rõ ràng hoặc không tồn tại thì bạn sẽ muốn tự viết, miễn là giải pháp IDS của bạn cho phép. Điều đó sẽ giúp bạn có được một cách nhìn tổng quan nhanh chóng về việc tấn công các ứng dụng web như thế nào và hy vọng nó sẽ khuấy động sự ham tìm tòi bên trong của các bạn.