Basic Offense: Supplement

# Notes and References

There are other Metasploit modules for Internet Explorer omitted from the list in the chapter, some because they were less reliable on my test systems.

* Internet Explorer 11 VBScript Engine Memory Corruption

exploit/windows/browser/ms16\_051\_vbscript

CVE 2016-0189, MS 16-051

Internet Explorer 11 on Windows 10

Some others are simply quite particular in their requirements.

* MS13-059 Microsoft Internet Explorer CFlatMarkupPointer Use-After-Free

exploit/windows/browser/ms13\_059\_cflatmarkuppointer

CVE 2013-3184, MS13-059

Internet Explorer 9 on Windows 7

Requires mshtml.dll between 9.0.8112.16446 and 9.00.8112.16502, roughly prior to July 2013.

* MS14-012 Microsoft Internet Explorer TextRange Use-After-Free

exploit/windows/browser/ms14\_012\_textrange

CVE 2014-0307, MS14-012

Internet Explorer 9 on Windows 7

Requires mshtml.dll between 9.0.8112.16496 and 9.0.8112.16533, roughly between August 2013 and March 2014.

* MS13-080 Microsoft Internet Explorer SetMouseCapture Use-After-Free

exploit/windows/browser/ie\_setmousecapture\_uaf

CVE 2013-3893, MS13-080

Internet Explorer 9 on Windows 7

Requires Office 2007 or Office 2010

There are other Metasploit modules that attack Adobe Flash Player that were less reliable on my test systems; they include

* Adobe Flash Player AVM Verification Logic Array Indexing Code Execution

exploit/windows/browser/adobe\_flashplayer\_arrayindexing

CVE 2011-2110

Flash Player 10, up to 10.3.181.23

* Adobe Flash Player MP4 'cprt' Overflow

exploit/windows/browser/adobe\_flash\_mp4\_cprt

CVE-2012-0754

Internet Explorer 8 on Windows 7 SP1

Flash Player 10 up to 10.3.183.15, Flash Player 11 up to 11.1.102.62.

* Adobe Flash Player Type Confusion Remote Code Execution

exploit/windows/browser/adobe\_flash\_filters\_type\_confusion

CVE 2013-5331

Internet Explorer 8, 9, or 10 on Windows 7

Flash Player 11.7 up to 11.7.700.252, Flash Player 11.8 up to 11.8.800.168, Flash Player 11.9 up to 11.9.900.152 and other versions

The MS11-003 Microsoft Internet Explorer CSS Recursive Import Use After Free attack on Internet Explorer requires that .NET 2.0.50727 is installed. To determine the version(s) of .NET installed on a system, Microsoft recommends checking the registry (see <http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx> for details). It is possible to query the registry from the command line

C:\Users\Felix Klein>reg query "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP"

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v2.0.50727

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v3.0

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v3.5

This registry query shows .NET 2.0.50727 is installed.

Exercises

1. Test the exploits described in the chapter against the targets developed in the exercises for Chapter 1.
2. /The Metasploit exploit module windows/smb/ms17\_010\_eternalblue\_win8 is a variant of the EternalBlue exploit. Try the exploit against Windows 10-1504 (x64) and/or Windows 8.1 (x64). Does the module work without credentials? Does the module work with non-administrator credentials? Does the module work with administrator credentials?
3. The Firefox PDF.js Privileged Javascript Injection affects Firefox 35 and 36, but none of the standard Linux systems described in Chapter 1 include Firefox 35 or 36 as part of their default install. Download Firefox 35 for Linux from the Firefox archive, and install it on an Ubuntu 14.04 system. Run this version of Firefox, then use the exploit to obtain a shell on the target.
4. Many of the exploits against Adobe Flash are listed as working against Windows 7, Windows 8.1, and Linux, but oddly enough not against Windows 8. As an example, consider exploit/multi/browser/adobe\_flash\_hacking\_team. Examine the (Ruby) source code for this exploit, either locally on the Kali system at /usr/share/metasploit-framework/modules/exploits/multi/browser/adobe\_flash\_hacking\_team\_uaf.rb or online at <https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/browser/adobe_flash_hacking_team_uaf.rb>. The source code includes a set of browser requirements that include the following.

'BrowserRequirements' =>

{

:source => /script|headers/i,

:arch => ARCH\_X86,

:os\_name => lambda do |os|

os =~ OperatingSystems::Match::LINUX ||

os =~ OperatingSystems::Match::WINDOWS\_7 ||

os =~ OperatingSystems::Match::WINDOWS\_81 ||

os =~ OperatingSystems::Match::WINDOWS\_VISTA ||

os =~ OperatingSystems::Match::WINDOWS\_XP

end,

… continues …

In particular, Windows 8 is explicitly not allowed. Modify the source code to allow Windows 8 and try the exploit against a Windows 8 system with Firefox 38.0.5 and Adobe Flash Player 18.0.0.194. Obtain a shell on the target.

1. Microsoft Silverlight is another tool that provides rich content for web browsers. Download Silverlight 5, Build 5.0.61118.0 from December 2011, and install it on a Windows 7 system. Older versions of Silverlight are available directly from Microsoft at the page <http://www.microsoft.com/getsilverlight/locale/en-us/html/Microsoft%20Silverlight%20Release%20History.htm>. Be sure to disable automatic updates. Validate your installation by visiting <http://www.silverlightversion.com/>.   
     
   The Metasploit module titled MS13-022 Microsoft Silverlight ScriptObject Unsafe Memory Access with the name exploit/windows/browser/ms13\_022\_silverlight\_script\_object is able to attack this version of Silverlight. Use it to gain a native Windows Meterpreter shell on the Windows 7 target.
2. Metasploit includes the module auxiliary/server/browser\_autopwn2 which is used to set up a server preconfigured with commonly successful browser exploits. Try the module and evaluate its effectiveness.
3. The module exploit/multi/script/web\_delivery can be used to generate malware. Use it against a Windows target.
4. Meterpreter includes commands to extract data from the clipboard on a Windows target. Test them.