Java vulnerabilities are a prevalent client-side attack vector. In fact, some experts suggest that in light of the security issues that plague Java, users should uninstall or disable the software in their browsers.

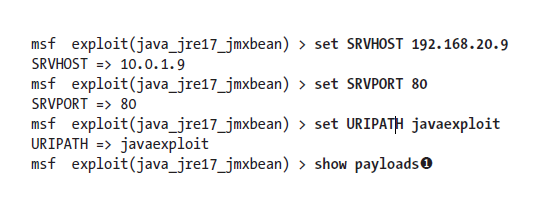
One thing that makes Java attacks so powerful is that one exploit can gain access to multiple platforms. Windows, Mac, and even Linux systems running the Java Runtime Environment ( JRE) in a browser can all be

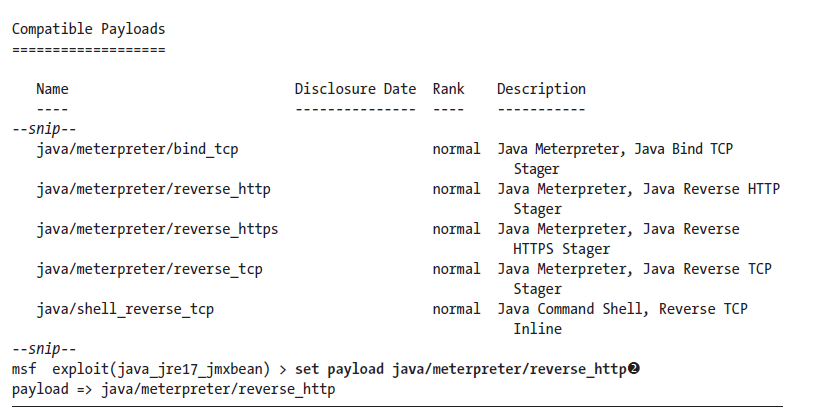
exploited by exactly the same exploit when that browser opens a malicious page. Here are some sample exploits.

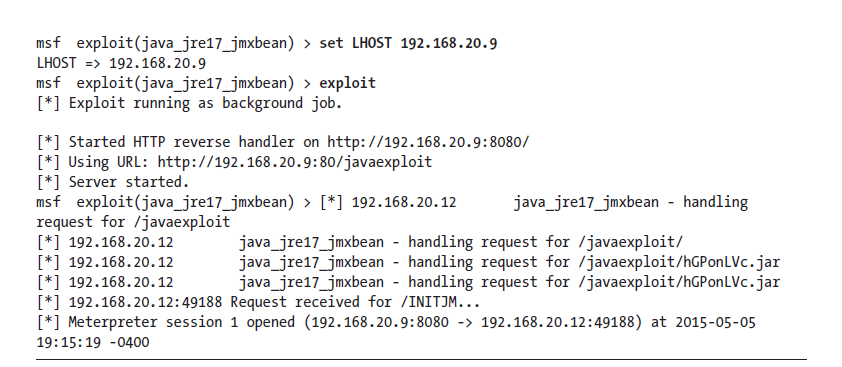
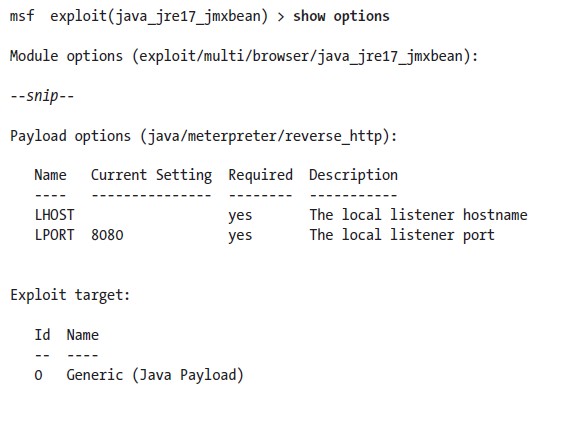
msf > **use exploit/multi/browser/java\_jre17\_jmxbean**

Use of this module is similar to that of the Internet Explorer Aurora exploit.

msf exploit(java\_jre17\_jmxbean) > **show options**



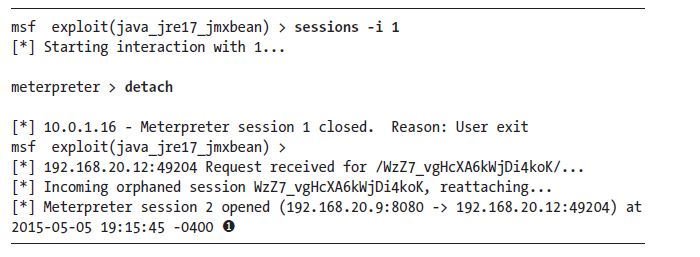




These options should look familiar. The default LPORT option is now 8080 instead of 4444. Notice that both SRVPORT and LPORT default to 8080, so we’ll need to change at least one of them. After you’ve finished setting options, start the exploit server and browse to the malicious page from your Windows 7 target. Either Internet Explorer or Mozilla Firefox will fall victim to this attack as long as you have enabled the vulnerable Java browser plugin.

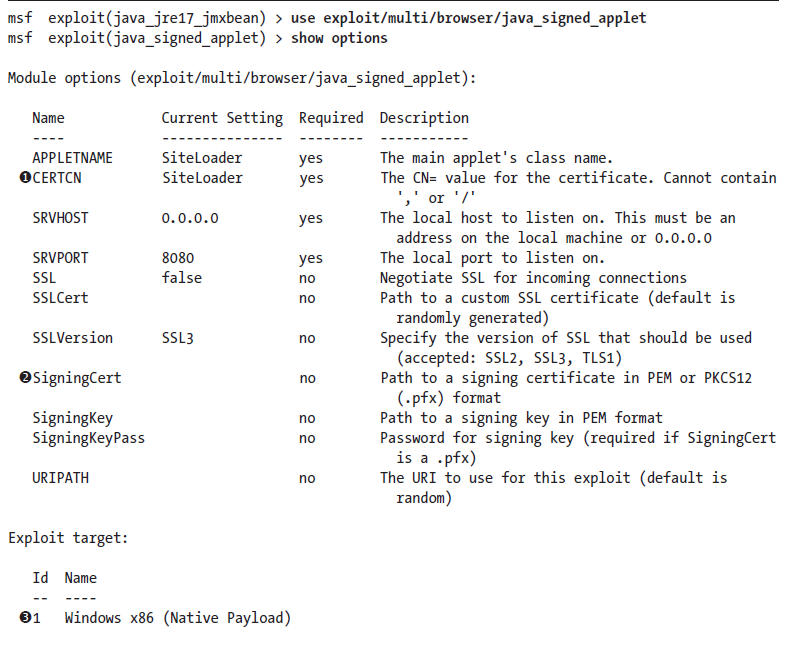
One of the great features of the HTTP and HTTPS Meterpreter payloads, aside from being legitimate HTTP and HTTPS traffic and thus by passing even some traffic-inspecting filters, is their ability to reattach to

a dropped session.



**Signed Java Applet**

Much like the attack against PDF users discussed in “PDF Embedded Executable” on page 228, we can bypass the need for an unpatched Java vulnerability by simply asking users to allow us to run malicious code. You’ve probably seen browser warnings like, “This site would like to run this thing in your browser, how would you like to proceed?” Sometimes even security-savvy users can be convinced to just say “Yes” and bypass this warning without further investigation if they can be convinced that what’s on the other side is useful.

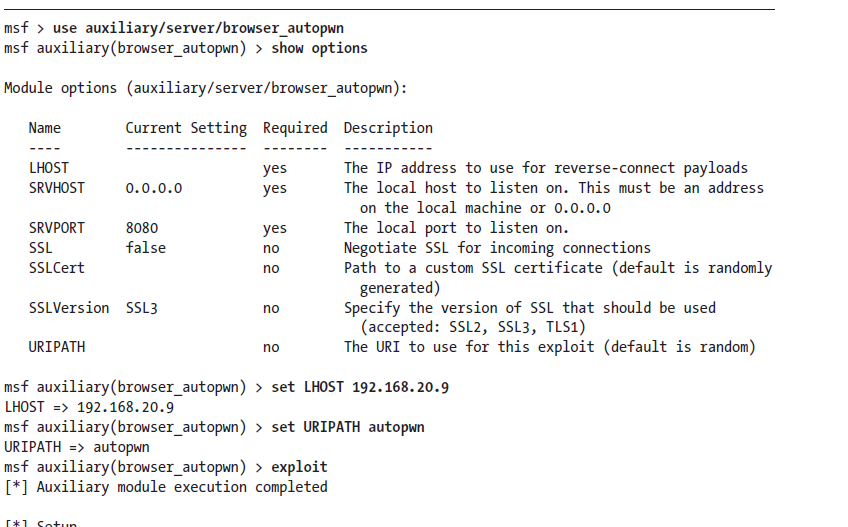
Browse to the Metasploit server from your Windows 7 target, and you should be prompted to run the applet, as shown in Figure 10-2. The security warning informs you that if this applet is malicious, it will have access

to the system and lets you know you should run the application only if the publisher is trusted. Because we didn’t use a signing certificate that is trusted by the browser certificate chain, the warning says in big letters that

the publisher is unknown.

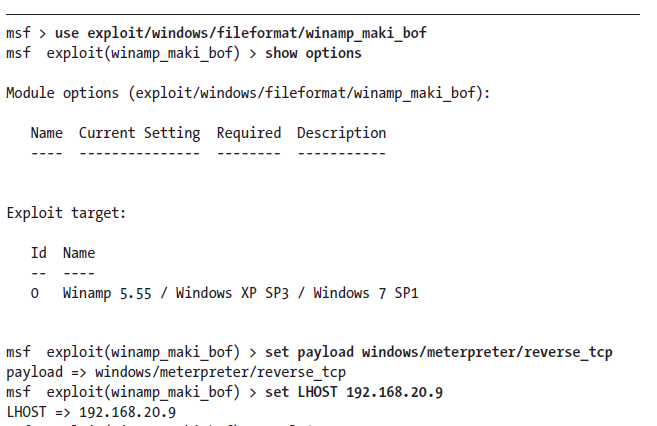
Browser auto pawn

**(Read how browser auto pawn works?)**



***Winamp***

we trick the user into replacing a configuration file for the Winamp music player program. When the user next opens the program, the evil configuration file will be processed regardless of which music file the user opens. The Metasploit module we’ll use is *exploit/windows/fileformat/winamp\_maki\_bof*, which exploits a buffer overflow issue in Winamp version 5.55.



Choose a compatible Windows payload as shown. Once the malicious Maki file has been generated, copy it to the Apache web server directory, and set up a payload handler. (An example of setting up the handler is included in Listing 10-11 on page 227, Book: Georgia.) Now we need to package this malicious file in such a way that a user may be convinced to load it in Winamp. We can create a new Winamp skin by copying one of the skins packaged with Winamp. We can replace the *mcvcore.maki* file from our example skin with our malicious one. It doesn’t matter what our skin actually looks like, because it will cause Winamp to hang and send us our session in Metasploit.

In Windows 7, make a copy of the default Bento Winamp skin folder from *C:\Program Files\Winamp\Skins* and copy it to Kali. Rename the folder *Bento* to *Rocketship*. Replace the file *Rocketship\scripts\mcvcore.maki* with the

malicious file we just created in Metasploit. Zip the folder and copy it to the web server. In the next chapter we will look at methods of creating believable social-engineering campaigns, but suffice it to say, if we can convince users that this malicious skin will make their Winamp look like aÂ€rocket ship, we might be able to convince users to install it. Switch to Windows 7, download the zipped skin from the Kali web server, unzip it, and save the folder to *C:\Program Files\Winamp\Skins*

Now open Winamp, go to **Options**4**Skins**, and choose **Rocketship.** Once you select the malicious skin, Winamp will appear to close, and you will receive a session in your Metasploit handler.