Chapter 2

Architecture, Environment, and Installation

Solutions in this chapter:

- Understanding the Soft Architecture
- Configuring and Locking Down Your System
- Installation

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

Introduction

Installing the Metasploit framework (MSF) is quite straightforward. The major difference for version 3.0 is the need to install Ruby and associated libraries, instead of Perl.

Understanding the Soft Architecture

In this section we will discuss tools that you will need to set up your Metasploit environment.

Wireshark

Wireshark (earlier known as Ethereal) is one of the most popular network sniffing and traffic analysis tools. Wireshark runs on Windows as well as a majority of UNIX variants including Linux, Solaris, FreeBSD, and so on. Source tarballs and binaries can be downloaded from www.wireshark.org.

IDA

IDA is one of the most popular debugging tools for Windows. First, IDA Pro is a disassembler, in that it shows the assembly code of a binary (an executable or a dynamic link library [DLL]). It also comes with advanced features that try to make understanding the assembly code as easy as possible. Second, it is also a debugger, in that it allows the user to step through the binary file to determine the actual instructions being executed, and the sequence in which the execution occurs. IDA Pro is widely used for malware analysis and software vulnerability research, among other purposes. IDA Pro can be purchased at www.datarescue.com.

UltraEdit

UltraEdit and EditPlus are powerful text editors and are specially designed for writing code. They support color-coded syntax highlighting for a variety of languages, including Perl and Ruby. UltraEdit can be purchased at www.ultraedit.com.

Nmap/Nessus

Nmap and Nessus are the de facto tools for scanning your network prior to launching exploits. Now that Metasploit can integrate Nessus and Nmap outputs into its own database, and then use that to configure which exploits to run, you definitely need to ensure you have the latest and greatest versions of these software installed on your system. Also, Metasploit can launch Nmap from within the *msfconsole*.

Nmap can be downloaded from www.insecure.org, and Nessus can be downloaded from www.nessus.org. Nmap works for a number of platforms and even has a graphical user interface (GUI) version. Nessus runs in client-server mode. The client is used to select the targets, select the plugins to be used for the testing, manage the sessions, and generate reports. The server does all the hard work of running the tests against the selected targets and communicating the results back to the client.

Configuring and Locking Down Your System

In this section, we will discuss steps for configuring and locking down your system.

Patching the Operating System

Check whether the latest patches have been applied or not with the *up2date* command. This is a Red Hat patch-checking utility, and it also allows for automatic installation of the updated packages.

Removing the Appropriate Services

It is recommended that the services that are not required be disabled. The following services may be removed:

- Network File System (NFS) and related services: autofs, nfs, nfsserver, nfslock
- Unused networking services: routed, gated, zebra, ratvf, snmpd, named, dhcpd, dhclient, dhrelay, nscd, smb
- Mail Services: sendmail, postfix
- Optional network and local services: ATD, LDAP, Kudzu, gpm, RHNSD, YPBIND, Apache, Quota, Quotad, Myself, and so on.
- Printing services: lpr, cups, lprng

For instance, it is required to disable sendmail, so the following command must be issued:

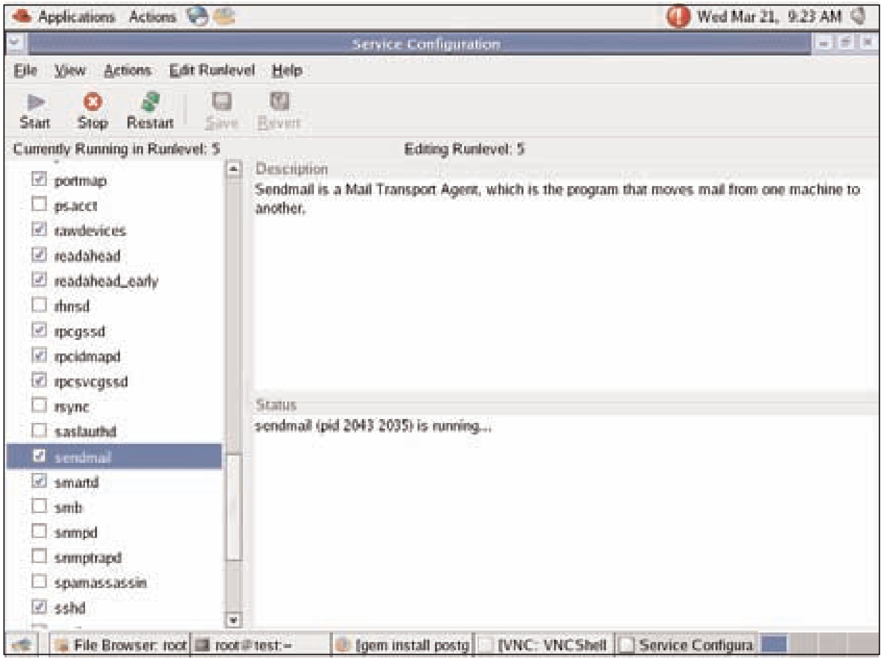
```
Linux#chkconfig --levels 0123456 sendmail off
```

This ensures that the sendmail daemon is not started at any of the run levels when the server is rebooted next. But the sendmail service is currently running, and it must be stopped by issuing the command:

```
Linux#/etc/init.d/sendmail stop
```

Alternatively, services can also be disabled using the GUI, if it is available, by navigating to **Start | System Settings | Server Settings | Services**, as shown in Figure 2.1.

Figure 2.1 Using the GUI to Disable Services



Currently Running in Runlevel: 5

Editing Runlevel: 5

- ☑ portmap
- ☐ psacct
- ☑ rawdevices
- ☑ readahead
- ☑ readahead_early
- ☐ rhnsd
- ☑ rpcgssd
- ☑ rpcidmapd
- ☑ rpcsvcgssd
- ☐ rsync
- ☐ saslauthd
- ☑ sendmail
- ☑ smartd
- ☐ smb
- ☐ snmpd
- ☐ snmptrapd
- ☐ spamassassin
- ☑ sshd

Description

Sendmail is a Mail Transport Agent, which is the program that moves mail from one machine to another.

Status

sendmail (pid 2043 2035) is running...

Removing Kernel Modules

The kernel is the heart of the Linux operating system. It is also highly configurable. During installation, the kernel parameters can be highly customized to ensure a minimal Linux installation. If the installation has already been done, the kernel can be modified using the *make xconfig* command. This command must be executed from the */usr/src/linux* directory. When this command is issued, the screen that appears shows the various drivers and components that have been chosen as part of the Linux installation, as shown in Figure 2.2.

It is strongly recommended to not install those drivers and components that are not absolutely required for the functionality of the server. It is necessary to have a complete list of the hardware components of the server to make an accurate list of components. For instance, it may not be necessary to install drivers for Universal Serial Bus (USB) support if the server's hardware does not contain any USB ports. Similarly, support for various file systems can be deselected if no purpose is served by these. A suggested list of features that can be disabled is given in Table 2.1. An important point to note here is that the requirement for such functionality is felt later; these drivers and components can always be added with a recompilation of the kernel. The good part is that if the new kernel compilation fails or malfunctions, the old kernel is still available, and it can be chosen when the LILO prompt appears during system boot-up.

Figure 2.2 Linux Kernel Configuration

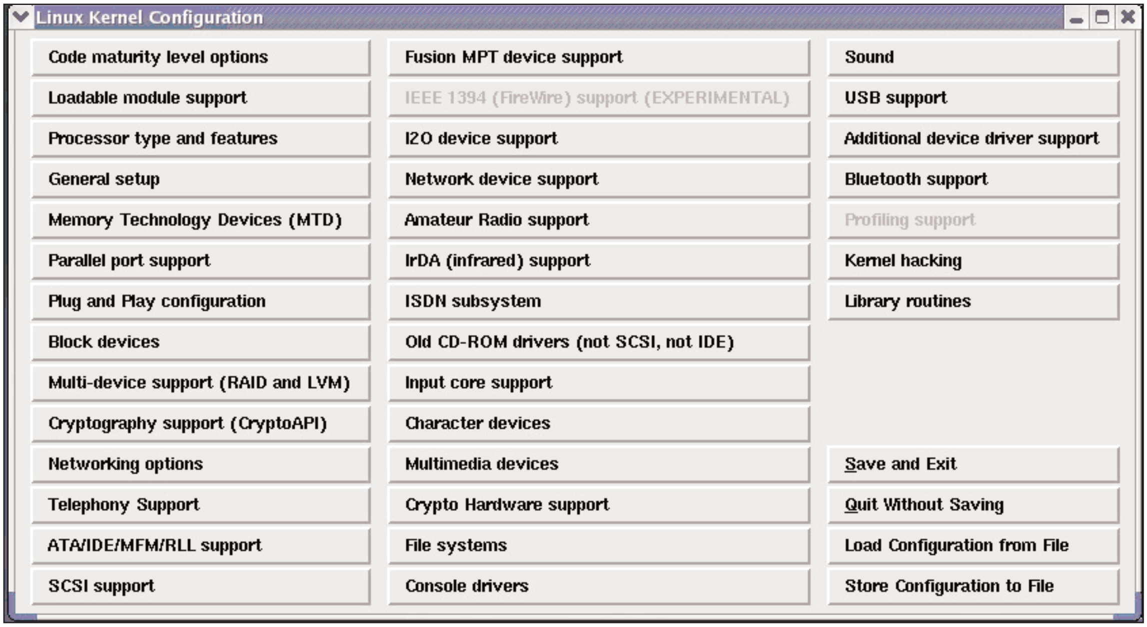


Table 2.1 Kernel Features That May Be Disabled

Kennel Feature	Description
Code maturity level options	Set Prompt for development and/or incomplete code/drivers = n
General setup	Set Process accounting = y (needed for system monitoring) support for a.out binaries = n
Binary emulations of other systems	Set all items that are not used to n
Block devices	Port IDE device support = n
Networking options	Set Internet Protocol (IP): multicasting, IP: advanced router, and wide area network (WAN) router to n. Set all unused protocols to n: IPX, Appletalk, Decnet, all experimental protocols
Network device support	Set PLIP, PPP, and SLIP to n
IrDA (infrared) support	Set the main item to n if IR port is not used

Continued

Table 2.1 continued Kernel Features That May Be Disabled

Kennel Feature	Description
File systems	Set all unused file system types to n. Likely candidates include: ADFS, Amiga FFS, BFS, UMSDOC, EFS, JFFS, JFS, NTFS, OS/2, QNX2.
File systems—Network s file system	Set all unused types to n: Coda, NFS, SMB, NCP If NFS is used, enable NFSv3 support, and enable server support only if the system will export file systems.
Kernel hacking	Set debugging = n

After the configuration is done, the kernel must be recompiled and installed.

Security of the root Account

Linux has the super user called *root*. This account has maximum privileges on the system, and can do just about anything. Most attackers will put all their efforts in trying to gain access to the root account. The Linux operating system is structured in such a way that a lot of the normal day-to-day tasks can be carried out as an ordinary user. Metasploit does not require root privileges to be installed or run.

The tendency to log in as root must be strongly discouraged. Administrators must have their own accounts and must log in to the system using these accounts. Whenever root privileges are required, the administrator must execute the *su* command and enter the password for root. This helps in maintaining accountability when there might be multiple system administrators for a given system. Additionally, the use of *sudo* is strongly recommended. Other measures to keep in mind as far as the root account is concerned are:

- The root account must be used only to carry out tasks that very specifically need to be carried out as root.
- The root account must never be used to execute the *rlogin/rsh/rexec* suite of commands. These commands can be easily exploited. Ensure that a *.rhosts* file does not exist for root.
- The */etc/securetty* file contains the list of terminals that root can log in from. The default setting on Red Hat Linux is to set it to virtual consoles (*vtys*). This ensures that root can log in only from the console, and not from a remote terminal. Ensure that no other entries are added here.

Installation

Now we will show you how to install Metasploit on various operating systems.

Supported Operating Systems

Metasploit works on a wide variety of operating systems, including Windows 2000/XP/2003, Linux, OpenBSD, FreeBSD, and Mac OS X. For Windows, Metasploit requires Cygwin to be installed, and the framework installer comes with a built-in Cygwin installer.

A Complete Step-by-Step Walkthrough of the Installation

The first thing you need to decide is whether you want to run Metasploit on Windows or on a UNIX platform. Incidentally, the majority of Metasploit downloads are for the Windows version. Once you have chosen your platform, download the relevant installation package from the Metasploit Web site. For Windows, you have the option of downloading Metasploit with a built-in Cygwin installer, or just the Metasploit package itself. For UNIX/Linux, the download is a straightforward tar zipped (*.tgz*) file.

The Windows installation is simply a matter of choosing your installation directory and clicking the **Next** buttons as they appear on screen. At one stage, the installer would ask you to scroll through the Metasploit License agreement, and type in **yes** to continue onto the next stage.

The UNIX/Linux installation requires you to untar and unzip the file to the folder where you want to run Metasploit from. It is not required for Metasploit to be installed as the *root* user, and you can do the installation under a regular user ID.

Understanding Environment Variables and Considerations

Here are some points about installing Metasploit on UNIX and Windows.

UNIX Installation

First, let's discuss a UNIX installation of Metasploit.

Linux (Red Hat-Based Examples)

Once you have downloaded the tar-zipped file from the Metasploit Web site, simply run the *tar –zxvf <installer_filename>* command.

You will need to make sure that you have the Ruby package installed. This is the default on most Red Hat systems, but in case it is missing, you can add it from the installation CD or download the Red Hat Package Manager (RPM) from the Red Hat Web site.

The Framework supports various relational databases. The current list of supported databases includes PostgreSQL, SQLite2, and SQLite3. In order to enable database support, you first need to install the RubyGems (www.rubygems.org/) package. To build the package, run the *emerge rubygems* command. Verify that the *gem* command is in your path.

Next you will need to install ActiveRecord and the Ruby database driver for your selected database, say PostgreSQL. This is done through the *gem install activerecord* and *gem install postgres* commands, respectively.

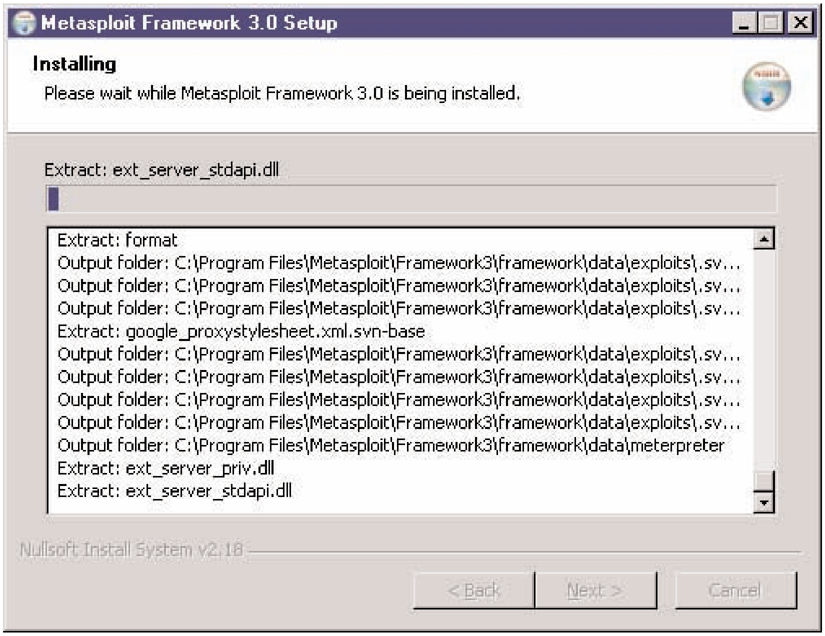
Windows Installation

Now let's discuss a Windows installation of Metasploit.

Using the Binary

Windows installers come in two flavors—with Cygwin and without Cygwin. We look at the example of installing it with Cygwin support. Launching the installer begins the extraction of the files into the specified directory, as shown in Figure 2.3

Figure 2.3 Installing the Framework on Windows



Metasploit Framework 3.0 Setup

Installing

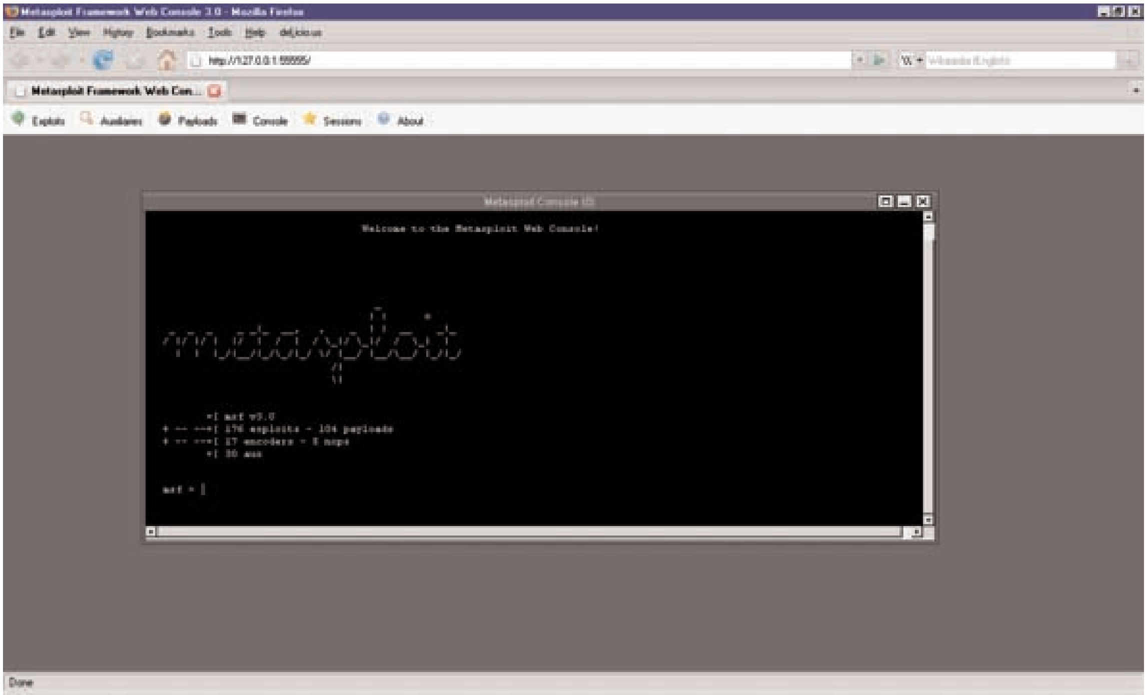
Please wait while Metasploit Framework 3.0 is being installed.

Extract: ext_server_stdapi.dll

```
Extract: format
Output folder: C:\Program Files\Metasploit\Framework3\framework\data\exploits\.sv...
Output folder: C:\Program Files\Metasploit\Framework3\framework\data\exploits\.sv...
Output folder: C:\Program Files\Metasploit\Framework3\framework\data\exploits\.sv...
Extract: google_proxystylesheet.xml.svn-base
Output folder: C:\Program Files\Metasploit\Framework3\framework\data\exploits\.sv...
Output folder: C:\Program Files\Metasploit\Framework3\framework\data\exploits\.sv...
Output folder: C:\Program Files\Metasploit\Framework3\framework\data\exploits\.sv...
Output folder: C:\Program Files\Metasploit\Framework3\framework\data\exploits\.sv...
Output folder: C:\Program Files\Metasploit\Framework3\framework\data\meterpreter
Extract: ext_server_priv.dll
Extract: ext_server_stdapi.dll
```

Upon successful extraction and installation, the *msfconsole* can be launched from within the folder where Metasploit is installed. However, currently, Windows is only partially supported as a platform, and the recommended way of using the *msfconsole* is through the *msfweb* interface, as shown in Figure 2.4.

Figure 2.4 The *msfconsole* after Installation

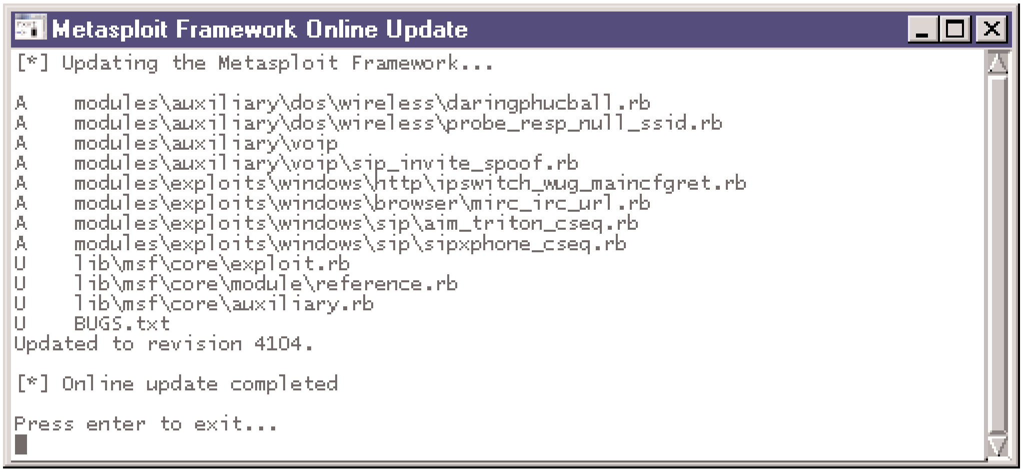

Metasploit Framework Web Console 3.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help del.icio.us
http://127.0.0.1:55555/
Metasploit Framework Web Con...
Exploits
Auxiliaries
Payloads
Console
Sessions
About
Metasploit Console (0)
Done

```
Welcome to the Metasploit Web Console!

       =[ msf v3.0
+ -- --=[ 176 exploits - 104 payloads
+ -- --=[ 17 encoders - 5 nops
       =[ 30 aux

msf >
```

Updating Metasploit

Updating Metasploit is a breeze. On Windows, you simply need to navigate to **Start | Programs | Metasploit | MSF Update**, as shown in Figure 2.5.

Figure 2.5 Updating the Framework



```
[*] Updating the Metasploit Framework...

A    modules\auxiliary\dos\wireless\daringphucball.rb
A    modules\auxiliary\dos\wireless\probe_resp_null_ssid.rb
A    modules\auxiliary\voip
A    modules\auxiliary\voip\sip_invite_spoof.rb
A    modules\exploits\windows\http\ipswitch_wug_maincfgret.rb
A    modules\exploits\windows\browser\mirc_irc_url.rb
A    modules\exploits\windows\sip\aim_triton_cseq.rb
A    modules\exploits\windows\sip\sipxphone_cseq.rb
U    lib\msf\core\exploit.rb
U    lib\msf\core\module\reference.rb
U    lib\msf\core\auxiliary.rb
U    BUGS.txt
Updated to revision 4104.

[*] Online update completed

Press enter to exit...
```

On UNIX, you need to first install the Subversion client by downloading it from http://subversion.tigris.org/project_packages.html. Ensure that when installing Subversion from the tarball, you provide the *—with-ssl* switch to the *./configure* command. Once installed, simply issue the *svn checkout* command (for the first time), and then the *svn update* command every time you wish to update the framework.

Adding New Modules

New payloads, encoders, exploits, and NOP generators can be added to the framework either by running the update commands as explained above, or by developing the module in Ruby as per the framework requirements, and then simply dropping the file into the appropriate folder.

Summary

Installing and getting started with the MSF simply requires you to download the right package. In the case of Linux, this is done by unpacking it, and in the case of Windows, this is done by clicking on **Next** when prompted. Make sure that you have hardened your system prior to installing the framework.

Solutions Fast Track

Understanding the Soft Architecture

☑ Make sure you have the tools complementary to Metasploit, including port scanners such as Nmap, vulnerability scanners such as Nessus, sniffers such as Wireshark, Windows debuggers and disassemblers such as IDA Pro or SoftIce, and code editors such as UltraEdit or EditPlus.

☑ Harden your operating system by following standard security configuration steps such as applying patches and service packs, removing unnecessary services, removing unnecessary software, adding only the necessary users and groups, and avoiding the use of the root login as much as is possible.

Configuring and Locking Down Your System

☑ You should check whether the latest patches have been applied or not with the up2date command.

☑ It is recommended that the services that are not required be disabled.

☑ The tendency to log in as root must be strongly discouraged. Administrators must have their own accounts and must log in to the system using these accounts.

Installation

☑ Metasploit works on a wide variety of operating systems such as Windows 2000/2003/XP, Linux, BSD, and Mac OS X.

☑ For the Windows installer you can either have your own Cygwin environment installed, or use the package that contains the built-in Cygwin installer.

☑ Linux requires Ruby and associated libraries and packages to be installed. Ruby usually is present on most default Linux installations.

☑ To update Metasploit on Windows, use the MSFUpdate utility. On Linux, ensure you have the Subversion client installed, and then run the svn update command from the main Metasploit directory.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Which is the better platform for Metasploit, Linux or Windows?

A: The choice of platform is more or less personal, since the framework works almost the same on both operating systems. However, the majority of Metasploit downloads for its earlier versions were for the Windows platform. For version 3, Windows is only partially supported. My personal choice is Linux, since some of the bleeding-edge features such as database support and wireless exploits first came out for Linux, and then for Windows.