How hacking got easy

METASPLOIT

When it comes to security, public disclosure of vulnerabilities and working exploit code is now common. We look at why this can be both harmful and helpful to securing your systems. **BY KURT SEIFRIED**

Last month, I wrote about the DNS security issues, and I included examples of how to exploit it before the magazine went to print [1]. Since then, a friend and I were discussing how exploitable the DNS issue actually was – I said it was relatively easy to exploit, and he thought that it would be difficult at best.

We both stuck to our guns until he said, “If you think it’s so easy, go write exploit code for it.” My reply was, “Why bother? Someone will write exploit code or a Metasploit module for it within a few days or weeks and release it publicly,” which they did.

This is an interesting change of events – years ago, I would have tried to create a working exploit or traded a favor with someone who knew a guy who knew a guy that had exploit code for it. Now I’m willing to wait a few days or weeks for someone to create and release exploit code publicly, probably in any easy-to-use form, such as a Metasploit module.

Although attackers still create new attacks and use them in secret, the trend is increasing toward public disclosure of vulnerabilities and working exploit code, which is both good and bad.

Exploit Code

Exploit code is a lot like a crowbar – it’s a very useful tool if you need to take a wall down to look at the plumbing behind it, or it's a good way to break into a house to burglarize it.

Exploit code, especially well-packaged exploits such as Metasploit modules, are an invaluable tool for security professionals. We use them to assess the security of our systems and to generate information so we can then write attack signatures. (Writing an attack signature without a network capture is possible, but often painful.) Without exploit code, our jobs would be more difficult, if not completely impossible in some situations.

Attackers use exploit code in virtually identical ways, but with the goal of breaking into and compromising systems, for example, to create botnets or gain access to sensitive information.

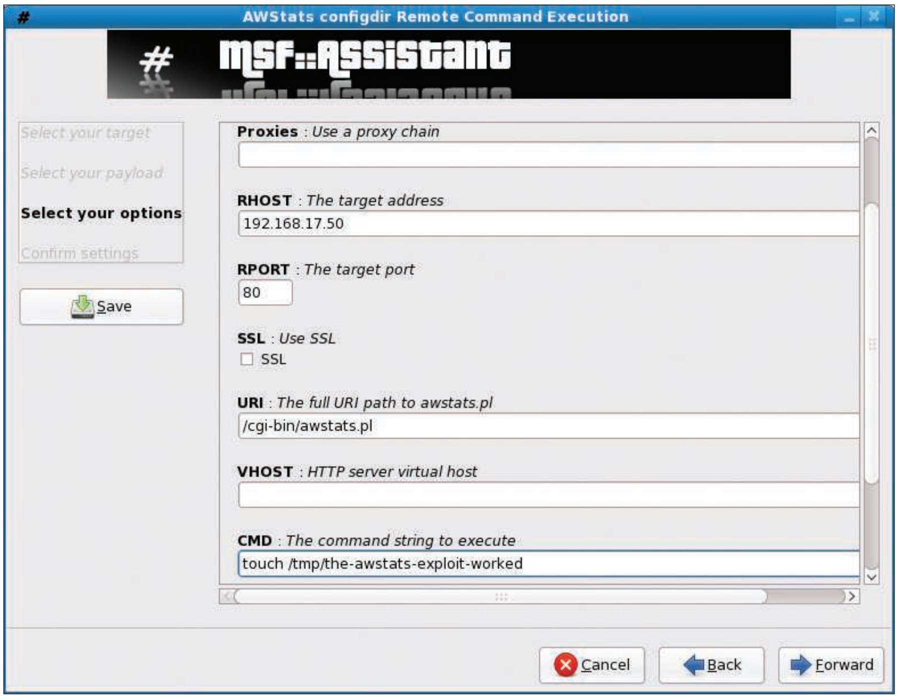
Enter Metasploit

Not only have people started sharing their exploit code, the quality of this code has also risen. Gone are the system- and architecture-specific proof-of-concept exploits of the past that often failed to compile without some serious bug fixing. The frequently buggy shell codes used to run hostile code or commands after the attack succeeds have also evolved. Frameworks for exploitation – of which Metasploit is the most popular open source option – have simplified work for exploit writers, security professionals, and the bad guys.

Metasploit provides command-line, graphical, and web interfaces, with more than 300 exploit modules for a wide

Anatomy of an Exploit

Typically, an exploit comprises two elements: the attack itself, and the shell code. The attack can be any number of things: an integer underflow, a buffer overflow, etc. Ultimately, most of these attacks allow an attacker to modify the contents of system memory, thus allowing them to control the program’s execution and ultimately allowing them to run arbitrary code. Often this code is referred to as shell code, the pointy end of the stick that gets you a shell or remote access and control of the system in question. Shell code is typically specific to operating systems and architecture, and is sometimes restricted in which characters and instructions it can use (because of the presence of program-specific issues or security systems, for example).



Proxies : *Use a proxy chain*

RHOST : *The target address*
192.168.17.50

RPORT : *The target port*
80

SSL : *Use SSL*
□ SSL

URI : *The full URI path to awstats.pl*
/cgi-bin/awstats.pl

VHOST : *HTTP server virtual host*

CMD : *The command string to execute*
touch /tmp/the-awstats-exploit-worked

Figure 1: The GUI is pretty intuitive ...

variety of programs, services, and operating systems.

Additionally, Metasploit greatly simplifies the process and makes it much more repeatable, which is again good for both the good guys and the bad guys.

Installing Metasploit

Your have two ways to install Metasploit: You can download the packaged tarball or pull the latest version from the project's Subversion source code repository. I prefer the latter because it ensures that you get the latest exploits and current code. The packaged tarballs tend to be at least a few weeks out of date.

Obviously, you will need the Subversion client software, which can be installed with commands such as:

```
# yum install subversion
```

After Subversion is installed, simply go to the directory into which you want to install Metasploit – for example, your home directory – and issue the command:

```
# svn checkout http://metasploit.com⮐
/svn/framework3/trunk/ metasploit
```

This will grab the latest Metasploit framework and exploit modules and put them into a directory called *metasploit*.

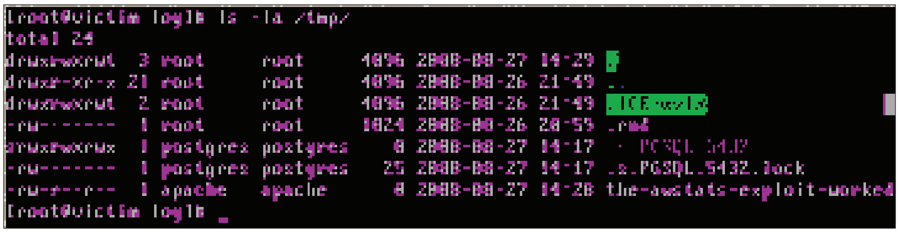
At this point, Metasploit won't work if you don't have Ruby installed, and depending on how you want to access Metasploit – for example, via the web interface or graphical user interface – you will also need a number of Ruby packages:

```
# yum install ruby ruby-irb ⮐
ruby-libs ruby-rdoc ruby-devel ⮐
readline ruby-gtk2 ruby-libglade2 ⮐
rubygems
```

After Ruby and any dependencies are installed, you will need to install Ruby on Rails.

The following command will install version 1.2.2:

```
# gem install -v=1.2.2 rails
```



```
[root@victim log]# ls -la /tmp/
total 24
drwxrwxrwt  3 root     root     4096 2008-08-27 14:29 .
drwxr-xr-x 21 root     root     4096 2008-08-26 21:49 ..
drwxrwxrwt  2 root     root     4096 2008-08-26 21:49 .ICE-unix
-rw-------  1 root     root     1024 2008-08-26 20:59 .rnd
srwxrwxrwx  1 postgres postgres    0 2008-08-27 14:17 .s.PGSQL.5432
-rw-------  1 postgres postgres   25 2008-08-27 14:17 .s.PGSQL.5432.lock
-rw-r--r--  1 apache   apache      0 2008-08-27 14:28 the-awstats-exploit-worked
[root@victim log]# _
```

Figure 2: ... and the results are easy to verify.

Then you can go to the directory in which Metasploit is installed and run the text-based console (*msfconsole*), the web interface (*msfweb*), or the graphical interface (*msfgui*). Next, simply choose anexploit – for example, the AWStats 6.1 and 6.2 remote command execution exploit – and enter the IP address or a range of hosts and the command you want to run. As you can see in the example screenshot, the GUI is pretty intuitive, and the results are easy to verify (Figures 1 and 2).

Conclusion

To protect your systems, you must familiarize yourself with the tools that will be used against them. For example, the attack against AWStats is blocked on Fedora Core 9 when SELinux is in enforcing mode (the default). Metasploit isn't the first, nor is it the most powerful, exploit framework available. Tools such as Core Impact and Immunity Canvas, which include up-to-date exploits, are available as well as commercial support. Other sites, such as Packet Storm and Milw0rm, also make large amounts of exploit code available. Part of a strong defense is a good offense. ■

INFO

[1] "DNS Attacks" by Kurt Seifried, *Linux Magazine*, October 2008: *http://www.linux-magazine.com/issues/2008/95/dns_attacks*

[2] Metasploit: *http://www.metasploit.com/*

[3] Immunity Canvas: *http://www.immunitysec.com/products-canvas.shtml*

[4] Core Impact: *http://www.coresecurity.com/*

[5] Packetstorm: *http://packetstormsecurity.org/*

[6] Milw0rm: *http://www.milw0rm.com/*

THE AUTHOR

Kurt Seifried is an Information Security Consultant specializing in Linux and networks since 1996. He is married and has four cats but no fish (because the cats are more hungry than afraid of water). He often wonders how it is that technology works on a large scale but often fails on a small scale.