Metasploit Basics

Introduction

Metasploit is a hacking framework written in ruby. It is designed to help make writing and executing exploits as simple as possible. This tutorial will walk you through using Metasploit to write a custom exploit.

Running Metasploit

Before launching Metasploit for the first time, there is a little setup you must do in order to write custom exploits. Metasploit automatically loads exploits from `~/.msf3/modules/exploits`. You should create all exploits in this directory. Create this directory by issuing the following command:

```
mkdir -p ~/.msf3/modules/exploits/
```

There is an example exploit provided at http://netsec.cs.northwestern.edu/media/handouts/example.rb which you should use as a template for creating exploits. Download the file and place it in your exploits directory with the following commands:

```
cd ~/.msf3/modules/exploits/
wget http://netsec.cs.northwestern.edu/media/handouts/example.rb
```

Now you're ready to launch Metasploit and use your exploit. Metasploit should already be installed on the machine that you're using, so to start the console, simply run `msfconsole`.

Before executing your exploit, it is useful to understand what some Metasploit commands do. Below are some of the command that you will use most.

- `use exploitname` Tells Metasploit to use the exploit with a specified name.
- `set RHOST hostname_or_ip` Will instruct Metasploit to target the specified remote host.
- `set RPORT host_port` Sets the port that Metasploit will connect to on the remote host.
- `set PAYLOAD generic/shell_bind_tcp` Sets the payload that is used to a generic payload that will give you a shell when a service is exploited.
- `set LPORT local_port` Sets the port number that the payload will open on the server when an exploit is exploited. It is important that this port number be a port that can be opened on the server (*i.e.*it is not in use by another service and not reserved for administrative use), so set it to a random 4 digit number greater than 1024, and you should be fine. You'll have to change the number each time you successfully exploit a service as well.
- `exploit` Actually exploits the service. Another version of `exploit`, `rexploit` reloads your exploit code and then executes the exploit. This allows you to try minor changes to your exploit code without restarting the console.
- `show options` Will show you options that you have set and possibly ones that you might have forgotten to set. Each exploit and payload comes with its own options that you can set. `show exploits` and `show payloads` can also be used to show all exploits and payloads that are built in to Metasploit.

- `help` Will give you basic information on commands not listed here.

All that's left is to issue a series of simple commands. The commands below use the `example` exploit to attack `netsec-vm-2` on port `3000` with the `shell_bind_tcp` payload. When it is successful it will open port `9485` on the target machine and Metasploit will show you a shell.

```
use example
set RHOST netsec-vm-2.cs.northwestern.edu
set RPORT 3000
set PAYLOAD generic/shell_bind_tcp
set LPORT 9485
exploit
```