Metasploit Modules and Locations

Almost all of your interaction with Metasploit will be through its many *modules*, which it looks for in two locations. The first is the primary module store under **/usr/share/metasploit-framework/modules/** and the second, which is where you will store custom modules, is under your home directory at **~/.msf4/modules/**.

```
root@kali:~# ls /usr/share/metasploit-framework/modules/
auxiliary  encoders  exploits  nops  payloads  post
```

All Metasploit modules are organized into separate directories, according to their purpose. A basic overview of the various types of Metasploit modules is shown below.

Exploits

In the Metasploit Framework, *exploit* modules are defined as modules that use payloads.

```
root@kali:~# ls /usr/share/metasploit-framework/modules/exploits/
aix        bsdi        firefox  irix       multi    solaris
android    dialup      freebsd  linux      netware  unix
apple_ios  example.rb  hpux     mainframe  osx      windows
```

Auxiliary

Auxiliary modules include port scanners, fuzzers, sniffers, and more.

```
root@kali:~# ls /usr/share/metasploit-framework/modules/auxiliary/
admin    client   dos         gather  scanner  spoof  vsploit
analyze  crawler  example.rb  parser  server   sqli
bnat     docx     fuzzers     pdf     sniffer  voip
```

Payloads, Encoders, Nops

Payloads consist of code that runs remotely, while *encoders* ensure that payloads make it to their destination intact. *Nops* keep the payload sizes consistent across exploit attempts.

```
root@kali:~# ls /usr/share/metasploit-framework/modules/payloads/
singles  stagers  stages
root@kali:~# ls /usr/share/metasploit-framework/modules/encoders/
cmd  generic  mipsbe  mipsle  php  ppc  ruby  sparc  x64  x86
root@kali:~# ls /usr/share/metasploit-framework/modules/nops/
aarch64  armle  mipsbe  php  ppc  sparc  tty  x64  x86
```

Loading Additional Module Trees

Metasploit gives you the option to load modules either at runtime or after msfconsole has already been started. Pass the **-m** option when running msfconsole to load additional modules at runtime:

```
root@kali:~# msfconsole -m ~/secret-modules/
```

If you need to load additional modules from with msfconsole, use the **loadpath** command:

```
msf > loadpath
Usage: loadpath </path/to/modules>

Loads modules from the given directory which should contain subdirectories
for
module types, e.g. /path/to/modules/exploits

msf > loadpath /usr/share/metasploit-framework/modules/
Loaded 399 modules:
    399 payloads
```