Ethical Hacking Environment Setup



SoftUni Team Technical Trainers







Software University

https://softuni.bg

Have a Questions?



sli.do

#Cyber-Security

Table of Contents



- 1. Prerequisites
- 2. Steps





System Requirements



- CPU => Core i5
- RAM => **16GB**
- GPU => n/a
- SSD => 256 GB



Software Requirements



Vmware Workstation Player

(https://www.vmware.com/products/workstation-player-evaluation.html)

Oracle VM VirtualBox (https://www.virtualbox.org/)

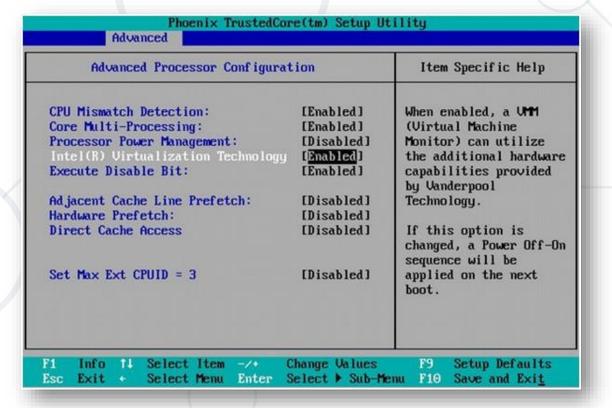




Enable Virtualization in Your BIOS



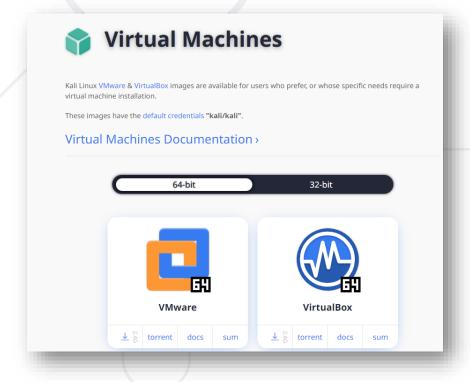
 This step differs from PC vendors, but generally what you need is to access the BIOS and enable the option that allows virtualization



Download Kali-Linux VM



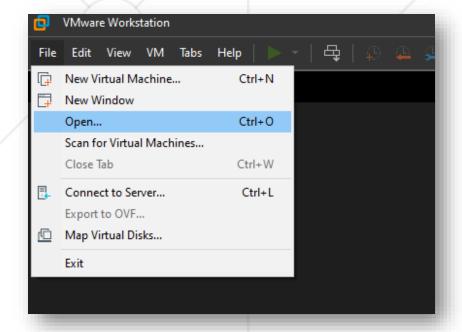
- Navigate to https://www.kali.org/get-kali/#kali-virtual-machines
- Download VM depending on your virtualization software

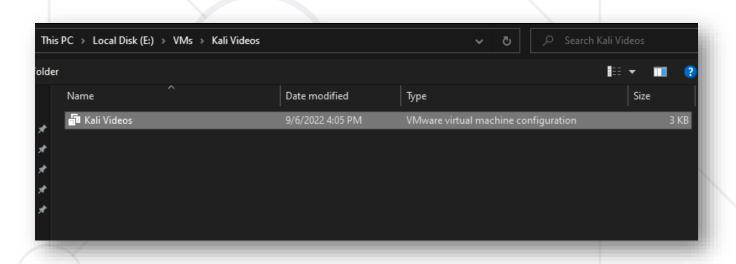


Open the Virtual Machine



- After it was downloaded, open your virtualization software and navigate to file>open
- Navigate to the downloaded vm directory and open the .vmx file

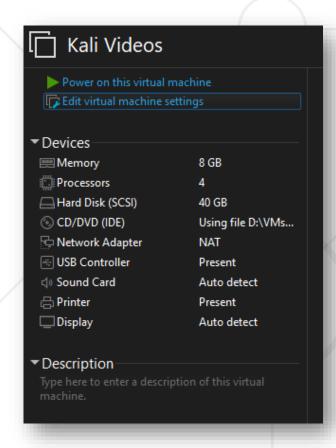


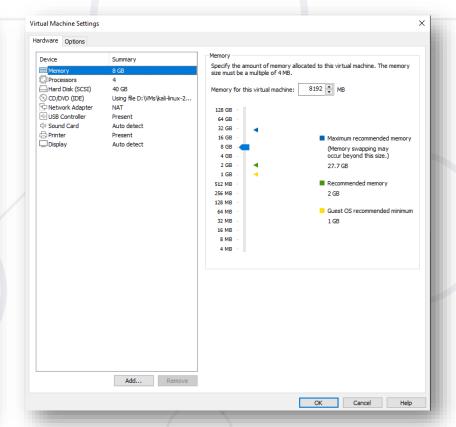


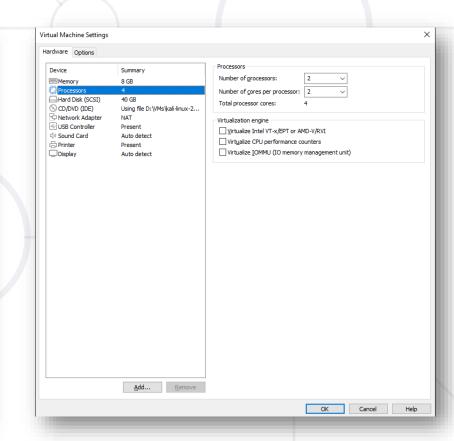
Edit VM Hardware, Based on Your System



Boost CPU, RAM and HDD if needed







Start the Virtual Machine



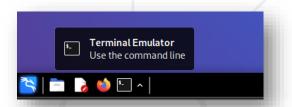
• After it boots, the default login is kali:kali



Update



- Open terminal and type:
 - sudo apt-get update && sudo apt-get upgrade -y

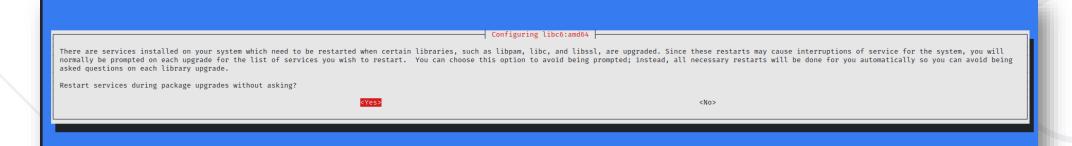


```
-$ sudo apt-get update & sudo apt-get upgrade -y
Hit:1 http://downloads.metasploit.com/data/releases/metasploit-framework/apt lucid InRelease
Hit:2 http://mirrors.netix.net/kali kali-rolling InRelease
Reading package lists ... Done
W: http://downloads.metasploit.com/data/releases/metasploit-framework/apt/dists/lucid/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer required:
  binutils-mingw-w64-i686 binutils-mingw-w64-x86-64 ettercap-common ettercap-graphical gcc-mingw-w64-base gcc-mingw-w64-i686-win32 gcc-mingw-w64-x86-64-win32 gcc-mingw-w64-x86-64-win32 gcc-mingw-w64-x86-64-win32 gcc-mingw-w64-x86-64-win32-runtime libaio1
  libapache2-mod-php libhttp-server-simple-perl libluajit-5.1-2 libluajit-5.1-common libpython3.9-minimal libpython3.9-stdlib libwacom-bin mingw-w64-common mingw-w64-i686-dev mingw-w64-x86-64-dev oracle-instantclient-basic
  python3-dataclasses-json python3-limiter python3-marshmallow-enum python3-mypy-extensions python3-pefile python3-qrcode python3-responses python3-spyse python3-token-bucket python3-typing-inspect python3.9 python3.9-minimal
  sphinx-rtd-theme-common
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  cherrytree cpp g++ gcc gstreamer1.0-plugins-bad 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-core libavcodec59 libavfilter8 libavformat59 libavutil56 libavutil57 libgdal31 libgstreamer-plugins-bad1.0-0
  libpoppler-glib8 libpostproc56 libswresample3 libswresample4 libswscale6 libtiff5 libwacom-bin python3-fonttools python3-jsonschema telnet
 The following packages will be upgraded:
  adwaita-icon-theme apparmor atftpd base-passwd bash bettercap blueman burpsuite busybox cifs-utils clang console-setup console-setup-linux cryptsetup cryptsetup-bin cryptsetup-initramfs dash dictionaries-common diffutils ethtool
  exiv2 firefox-esr gcc-12-base gdal-plugins gir1.2-gdkpixbuf-2.0 gir1.2-gtk-3.0 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 grub-common grub-pc grub-pc-bin grub2-common
   gtk-update-icon-cache ieee-data intel-microcode ipp-usb kali-desktop-core kali-desktop-xfce kali-linux-core kali-linux-firmware kali-menu keyboard-configuration kismet kismet-capture-common kismet-logtools ldap-utils lib32gcc-s1
   ib32stdc++6 libapparmor1 libasan8 libasyncns0 libatomic1 libbson-1.0-0 libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 libcc1-0 libcdio-cdda2 libcdio-paranoia2 libcrypto++8 libcryptsetup12 libcups2 libdaxctl1
  libdebconfcliento libegl-mesa0 libegl1 libevdev2 libewf2 libewf2 libexiv2-27 libexporter-tiny-perl libgbm1 libgcc-12-dev libgcc-s1 libgdbm-compat4 libgdbm6 libgdk-pixbuf-2.0-0 libgdk-pixbuf2.0-bin libgdk-pixbuf2.0-common libgfortran5 libgl1 libgl1-mesa-dri libglapi-mesa libglip2.0-0 libglip2.0-bin libglipmm-2.4-1v5 libglvnd0 libglx-mesa0 libglx0 libgomp1 libgtk-3-0 libgtk-3-bin libgtk-3-common libgtk-4-1 libgtk-4-bin libgtk-4-common libhogweed6
   libhtml-form-perl libhtml-tagset-perl libhttp-date-perl libhunspell-1.7-0 libidn2-0 libitm1 libjavascriptcoregtk-4.0-18 libjavascriptcoregtk-4.1-0 libjemalloc2 libjson-xs-perl libldap-2.5-0 liblsan0 liblz4-1 liblz4-dev libmariadb3
   libmongoc-1.0-0 libmpg123-0 libndctl6 libnet-libidn-perl libnetcdf19 libnettle8 libnfsidmap1 libnftables1 libnftnl11 libnghttp2-14 libnl-3-200 libnl-genl-3-200 libnl-route-3-200 libnm0 libnspr4 libnss3 libobjc-12-dev libobjc4
   libopengl0 libopenh264-6 libopenmpt0 libout123-0 libpam-modules libpam-modules-bin libpam-runtime libpam0g libpango-1.0-0 libpangocairo-1.0-0 libpangoft2-1.0-0 libpangoxft-1.0-0 libpipeline1 libpmem1 libpq5 libpython3.10
   libpython3.10-dev libpython3.10-minimal libpython3.10-stdlib libquadmath0 libreadline8 libsasl2-2 libsasl2-modules-db libsdl2-2.0-0 libsdl2-image-2.0-0 libsdl2-mixer-2.0-0 libsdl2-ttf-2.0-0 li
   libsoup-3.0-common libspeechd2 libssl3 libstdc++-12-dev libstdc++6 libsyn123-0 libtext-wrapi18n-perl libtirpc-common libtirpc-dev libtirpc3 libtsan2 libubsan1 libudisks2-0 liburcu8 liburing2 libuv1 libuv1-dev libvte-2.91-0
   libvte-2.91-common libvulkan1 libwacom-common libwacom9 libwebkit2gtk-4.0-37 libwebkit2gtk-4.1-0 libwpe-1.0-1 libww-mechanize-perl libxatracker2 libxfce4panel-2.0-4 libxml-twig-perl libxnvctrl0 libyara9 libzmg5 locales man-db
  mariadb-client-10.6 mariadb-client-core-10.6 mariadb-common mariadb-server-10.6 mariadb-server-core-10.6 mesa-vulkan-drivers metasploit-framework mpg123 ncat network-manager nfs-common nftables nmap open-vm-tools
  open-vm-tools-desktop openssl postgresql-14 postgresql-client-14 powermgmt-base powershell-empire publicsuffix python3-appdirs python3-attr python3-censys python3-certifi python3-debian python3-distutils python3-django
  python3-filelock python3-gdal python3-gi python3-gi-cairo python3-importlib-metadata python3-kismetcapturebtgeiger python3-kismetcapturefreaklabszigbee python3-kismetcapturertladsb
  python3-kismetcapturertlamr python3-lib2to3 python3-matplotlib-inline python3-pygame python3-pypdf2 python3-pyppeteer python3-setproctitle python3-sortedcontainers python3-speechd python3-tk python3-xmltodict python3.10
  python3.10-dev python3.10-minimal readline-common rsync rsyslog ruby ruby-dev ruby-mime-types ruby-oj ruby-yajl runit-helper scalpel screen speech-dispatcher speech-dispatcher-audio-plugins speech-dispatcher-espeak-ng sqlitebrowser
  stunnel4 sudo thc-pptp-bruter theharvester tmux tree udisks2 unrar vim vim-common vim-runtime vim-tiny xfce4-panel xfce4-screenshooter xfdesktop4 xfdesktop4-data xserver-xorg-video-amdgpu xxd zsh
 283 upgraded, 0 newly installed, 0 to remove and 33 not upgraded.
Need to get 870 MB of archives.
After this operation, 5,180 kB disk space will be freed.
Get:1 http://downloads.metasploit.com/data/releases/metasploit-framework/apt lucid/main amd64 metasploit-framework amd64 6.2.17+20220906102617~1rapid7-1 [289 MB]
Get:2 http://mirrors.netix.net/kali kali-rolling/main amd64 libc-l10n all 2.34-4 [876 kB]
Get:3 http://mirrors.netix.net/kali kali-rolling/main amd64 locales all 2.34-4 [4,091 kB]
9% [3 locales 759 kB/4,091 kB 19%] [1 metasploit-framework 94.8 MB/289 MB 33%]
                                                                                                                                                                                                                                                                                              11.2 MB/s 1min 8s
```

Update



If you see this:



Chose "Yes" by clicking Tab

Download Seclists



- Open terminal and:
 - cd /opt/ (or any other directory of your choice)
 - run "sudo git clone https://github.com/danielmiessler/SecLists"

```
(kali@ kali)-[~]
$ cd /opt

(kali@ kali)-[/opt]
$ sudo git clone https://github.com/danielmiessler/SecLists.git
```

Unpack rockyou



- Open terminal and:
 - Navigate to /usr/share/wordlists
 - run "sudo gzip –d rockyou.txt.gz"

```
(kali@ kali)-[/opt]
$ cd /usr/share/wordlists

(kali@ kali)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz
```



Questions?

















SoftUni Diamond Partners







Coca-Cola HBC Bulgaria









Решения за твоето утре













Trainings @ Software University (SoftUni)



- Software University High-Quality Education,
 Profession and Job for Software Developers
 - softuni.bg, softuni.org
- Software University Foundation
 - softuni.foundation
- Software University @ Facebook
 - facebook.com/SoftwareUniversity







License



- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is copyrighted content
- Unauthorized copy, reproduction or use is illegal
- © SoftUni https://softuni.org
- © Software University https://softuni.bg

