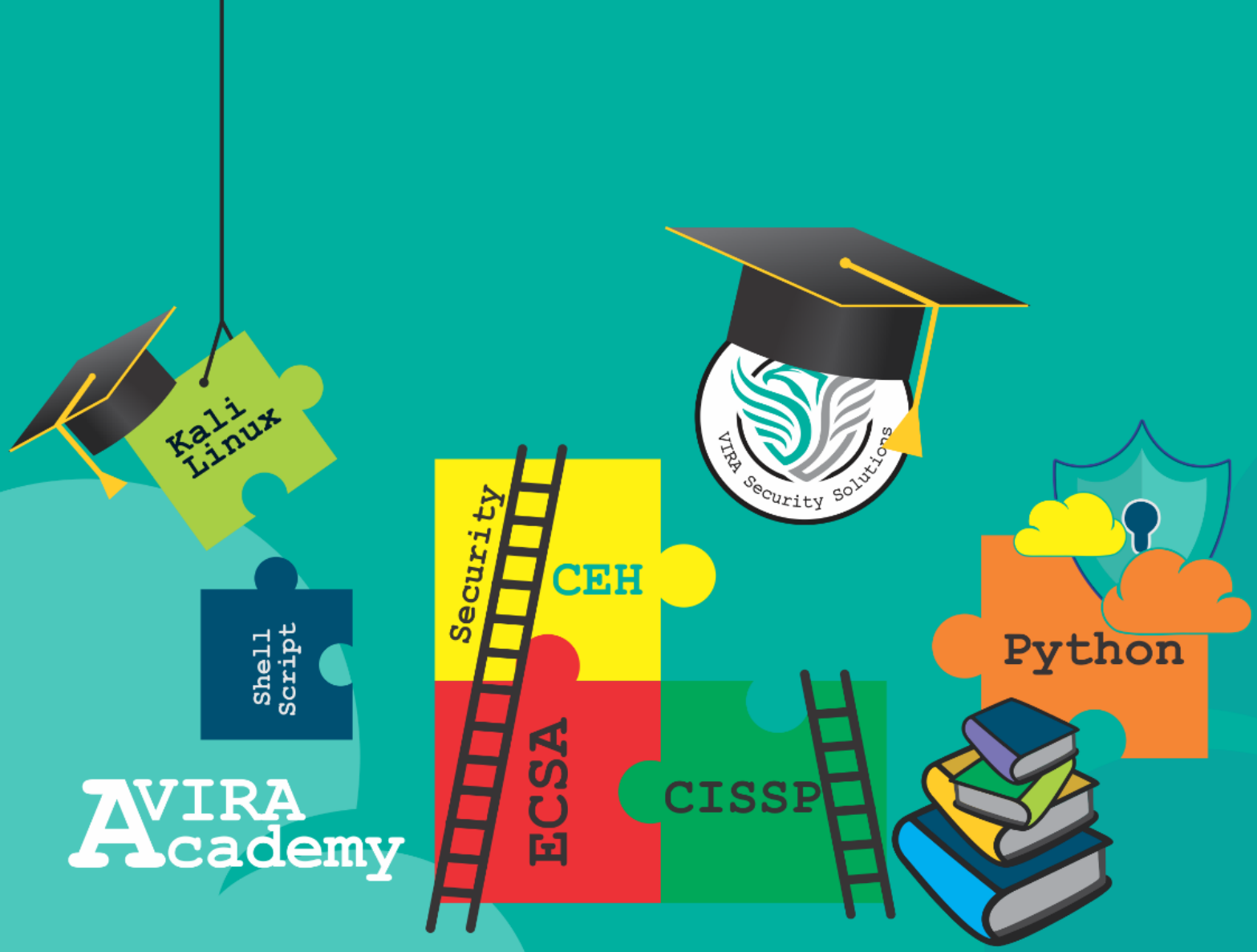

Kali Linux
Shell Script
VIRA Academy
Security
CEH
ECSA
CISSP
VIRA Security Solutions
Python

Linux

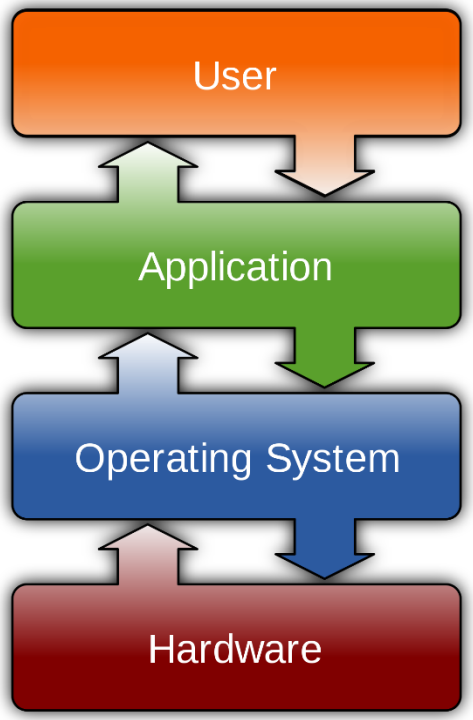
Part1

Mohammad Reza Gerami
mrgerami@aut.ac.ir
gerami@virasecsolutions.com
March 01 2020

Operating system

An operating system (OS) is system software that manages computer hardware and software resources and provides common services for computer programs.

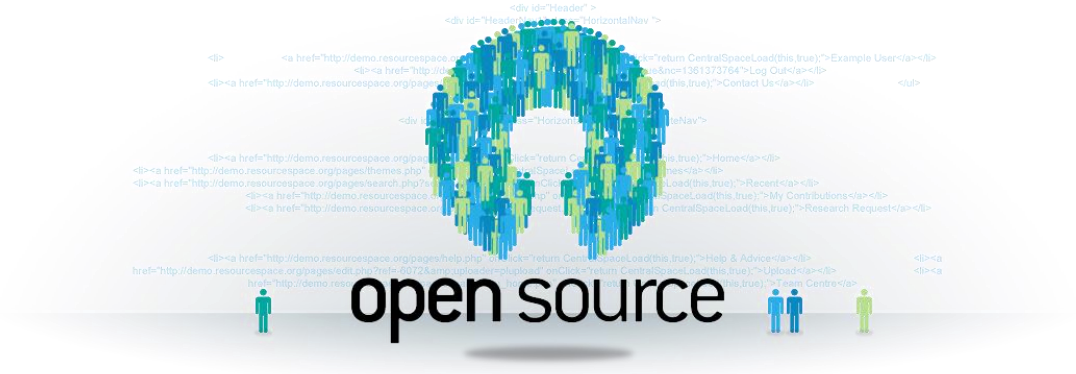
Time-sharing operating systems schedule tasks for efficient use of the system and may also include accounting software for cost allocation of processor time, mass storage, printing, and other resources.



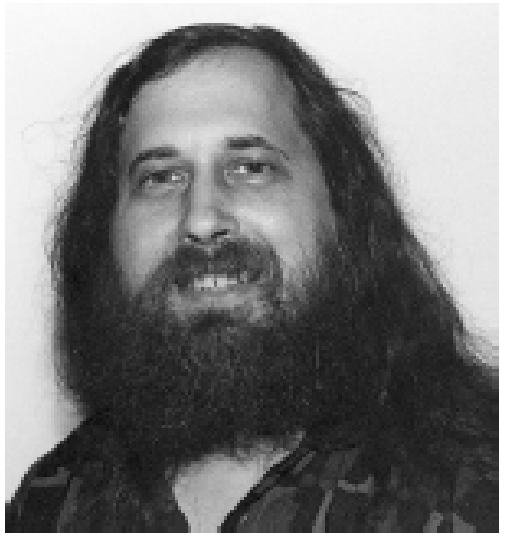
Open-source software

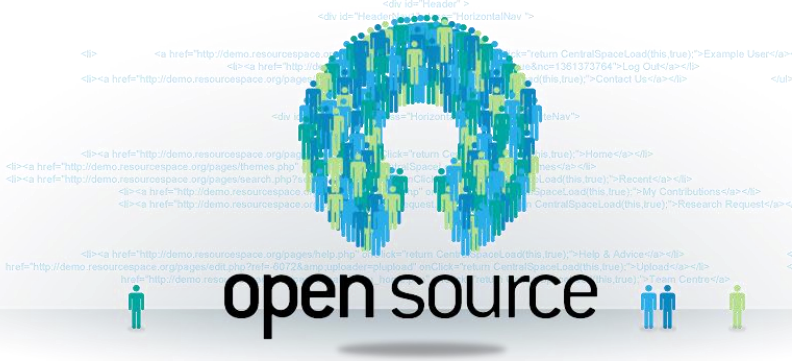
Open-source software (OSS) is a type of computer software with its source code made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose.

Open-source software may be developed in a collaborative public manner. According to scientists who studied it, open-source software is a prominent example of open collaboration.



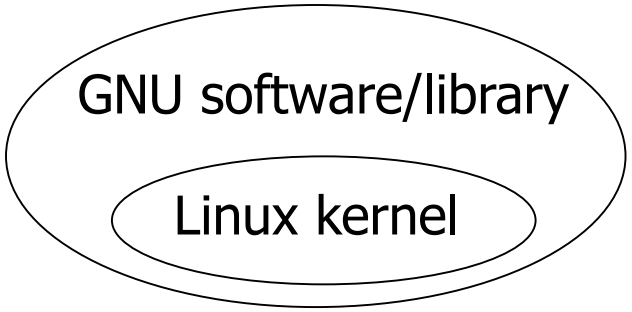
- 1984: Richard Stallman starts GNU project
  - GNU's Not Unix
  - http://www.gnu.org
- Purpose: Free UNIX
  - "Free as in Free Speech, not Free Beer"
- First step: re-implementation of UNIX Utilities
  - C compiler, C library
  - emacs
  - bash
- To fund the GNU project, the Free Software Foundation is founded
  - http://www.fsf.org





- 1991: Linus Torvalds writes 1st version of Linux kernel
  - Initially a research project about the 386 protected mode
  - Linus' UNIX -> Linux
  - Combined with the GNU and other tools forms a complete UNIX system
- 1992: First distributions emerge
  - Linux kernel
  - GNU and other tools
  - Installation procedure
- The rest is history...

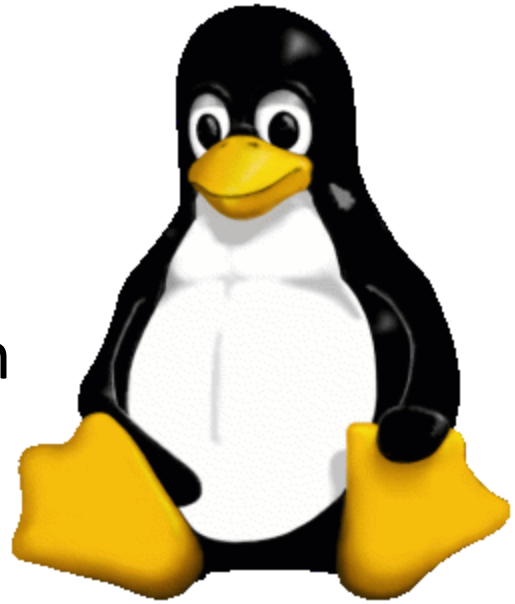
- GNU/Linux System
  - Linux kernel
  - GNU software/library
- Distributions ：
  - Red Hat, Debain, SuSe, Mandrake, Redflag…



Linux

- A free Unix-type operating system developed under the GNU General Public License.
  - Open source
  - Popular
  - Support most of the platforms available

- Linux is a multi-user system, meaning different users can be running various programs on the system, each running instance of a program must be identified uniquely by the kernel.



Linux Distributions

Fedora: Red Hat's community research and development distribution, End of Life (EOL) every six months

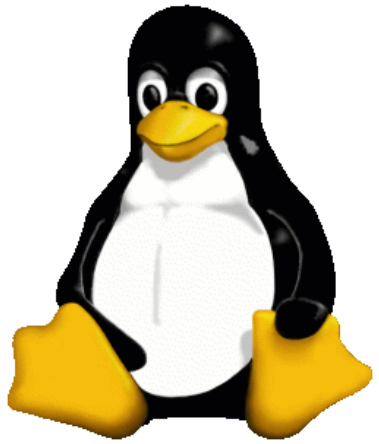
Red Hat Enterprise: Red Hat's production distribution on which they base their Red Hat Network and IT services, EOL approximately ten years

Oracle Linux: Red Hat Enterprise

CentOS: Red Hat Enterprise with all of Red Hat's trademarks removed (we'll use this one, CentOS 6.5)

Debian: a well respected Linux distribution

Ubuntu Desktop: a popular Desktop-oriented distro based on Debian, maintained by Canonical (six month cycle)



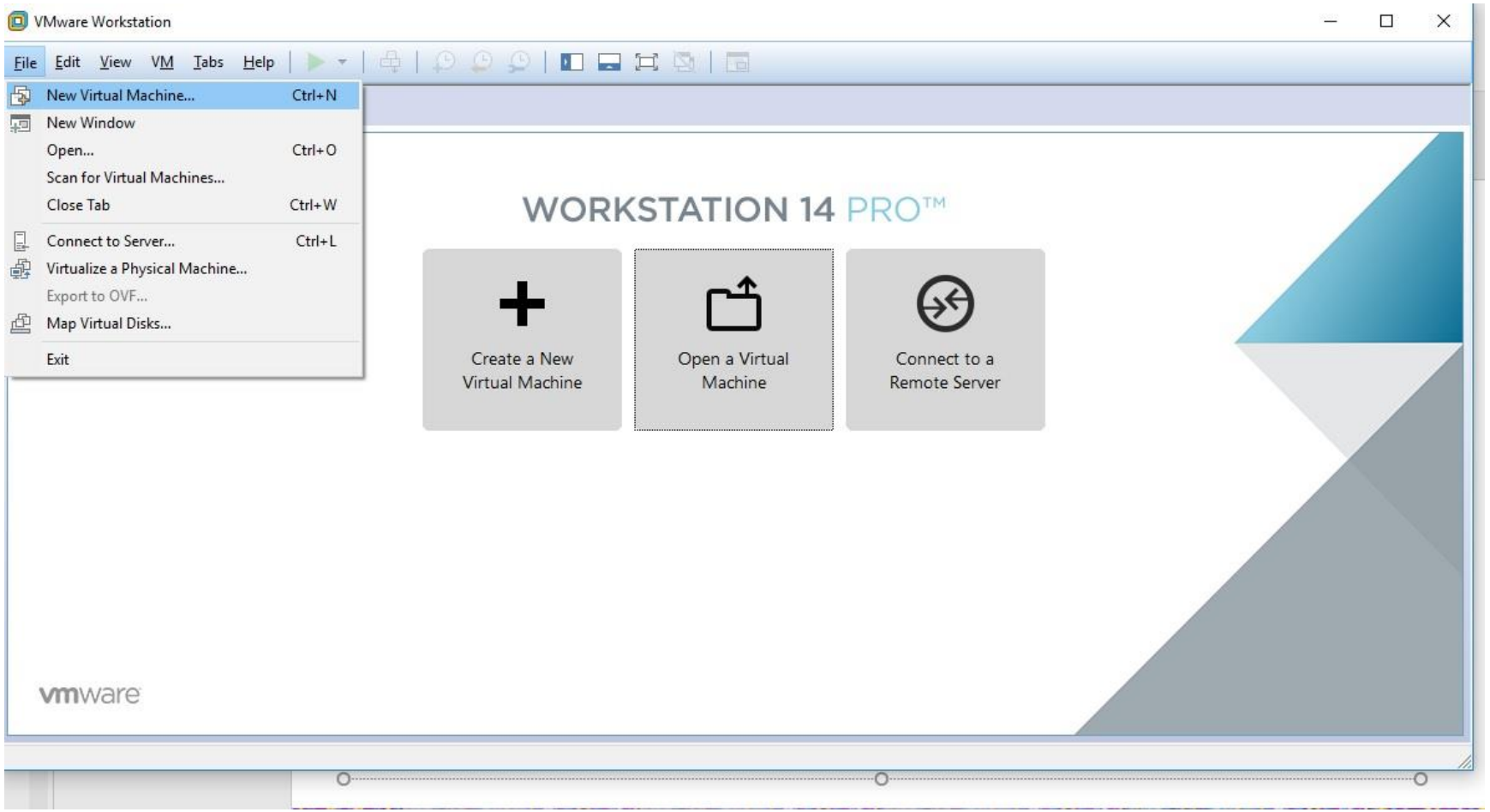
Install CentOS 7 Step by Step

Download The ISO Image

http://mirror.centos.org/centos/7/

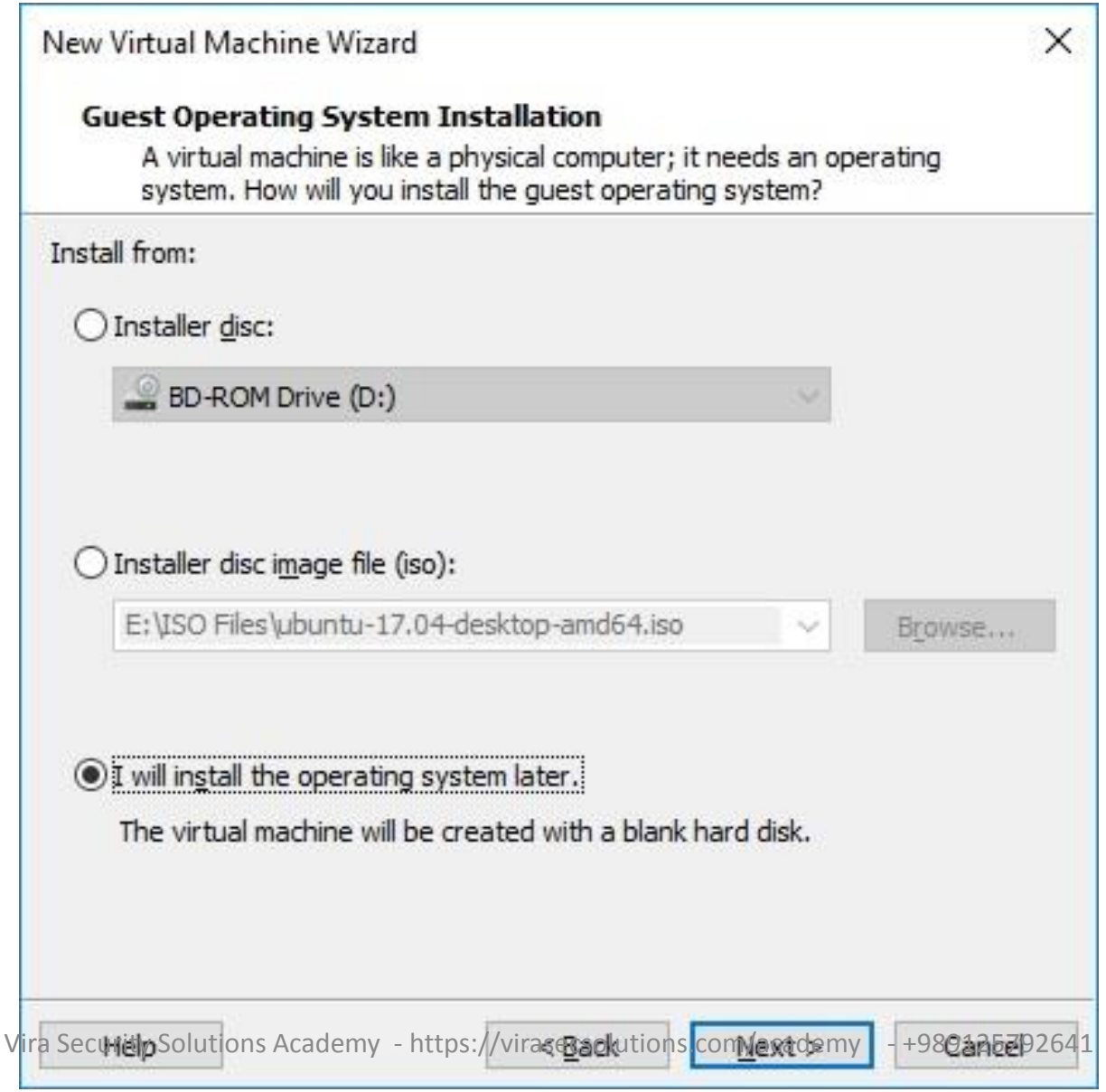
Write on DVD if you want to install on your desktop, laptop or server, if you don’t mount to your virtual machine and install it.

Install CentOS 7 Step by Step

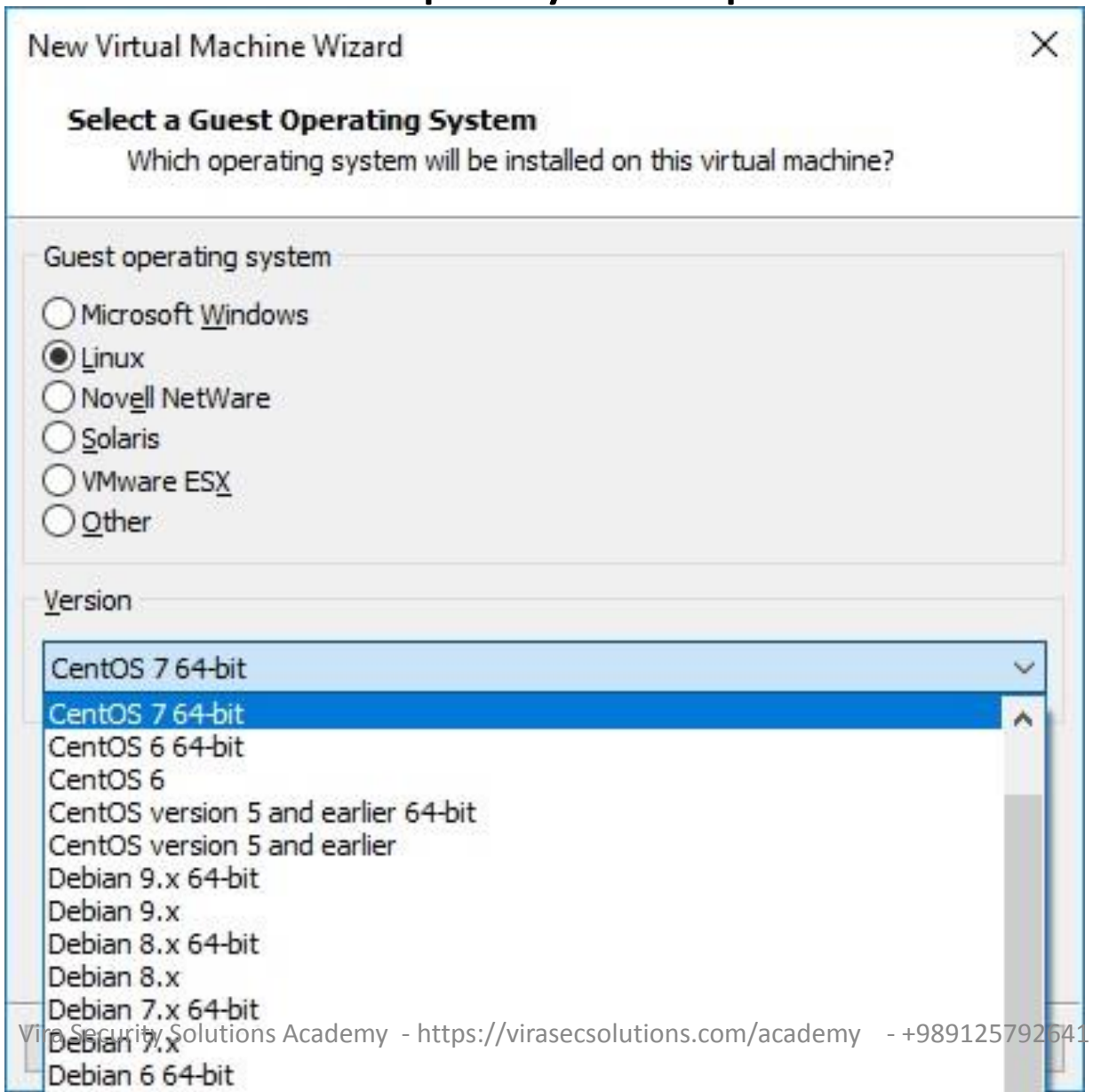


Install CentOS 7 Step by Step

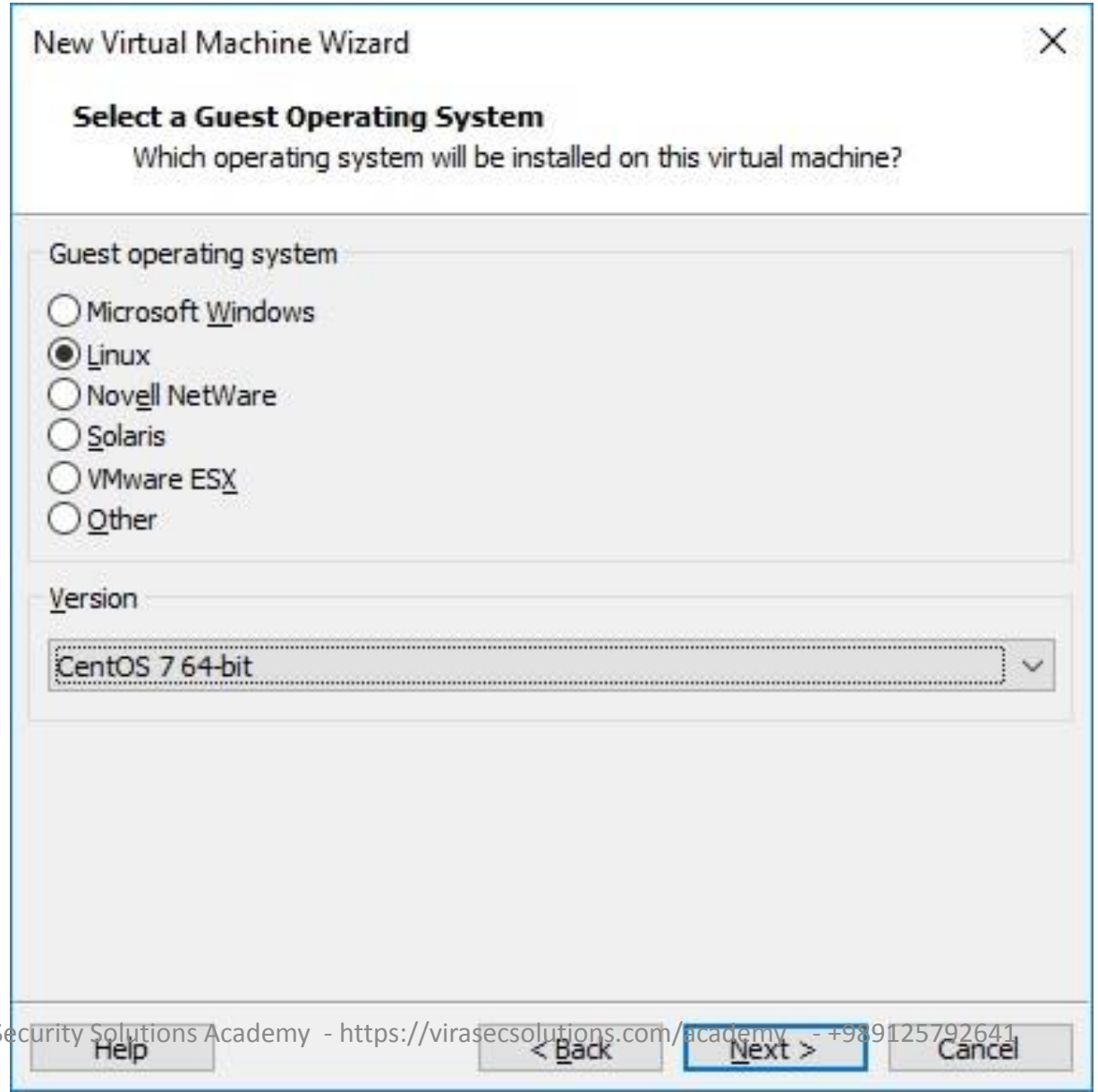
Install CentOS 7 Step by Step



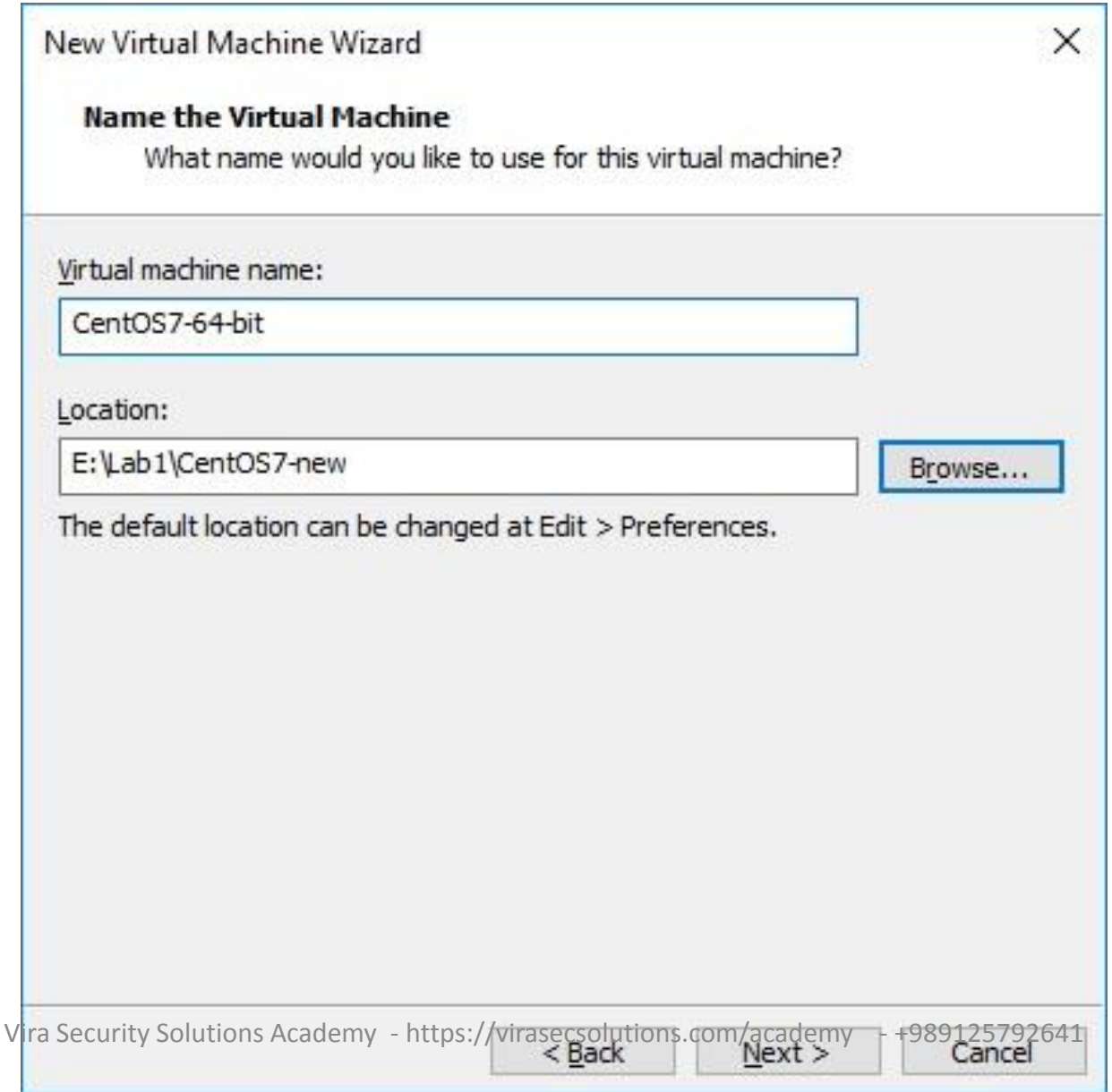
Install CentOS 7 Step by Step



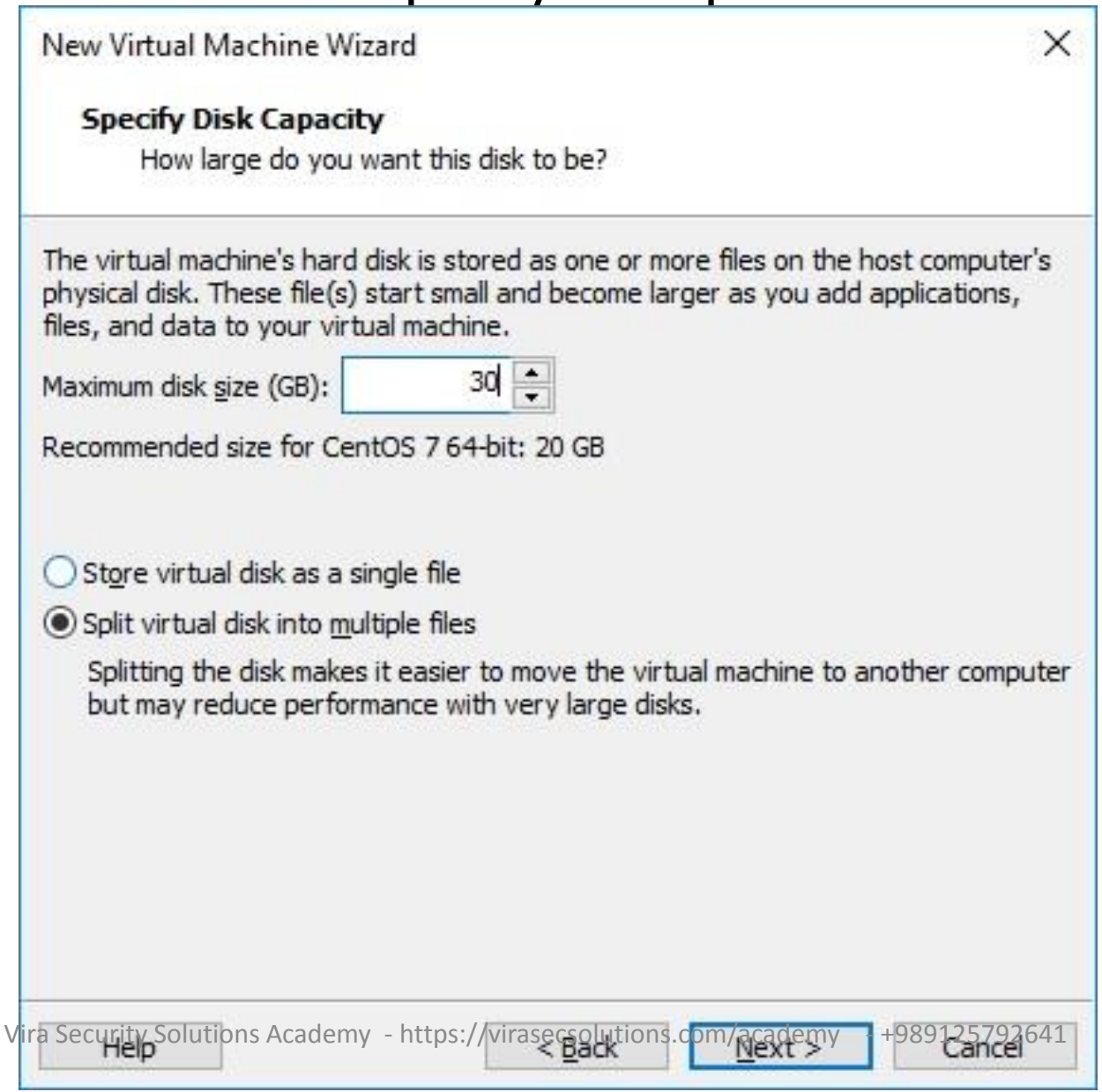
Install CentOS 7 Step by Step



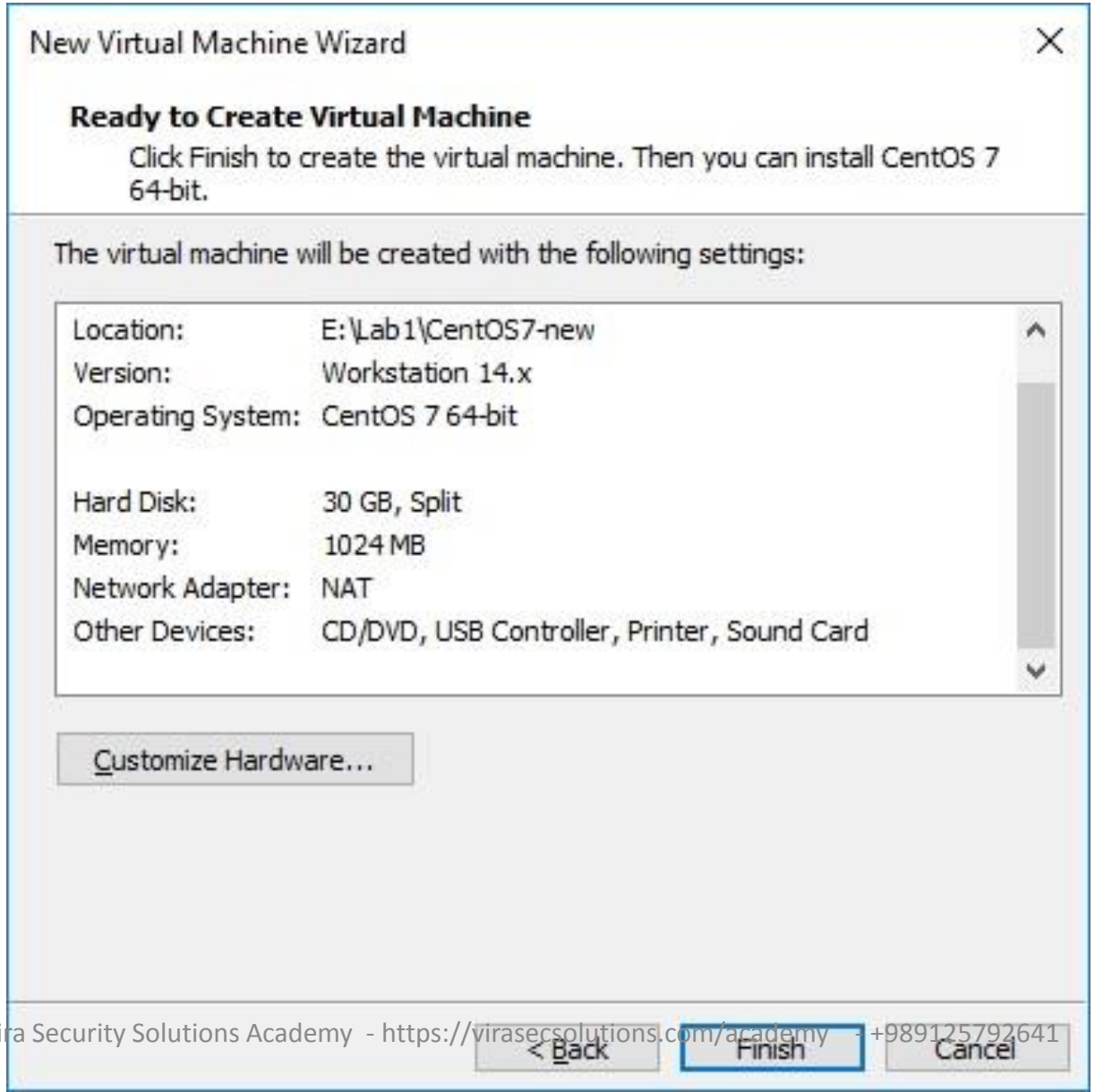
Install CentOS 7 Step by Step



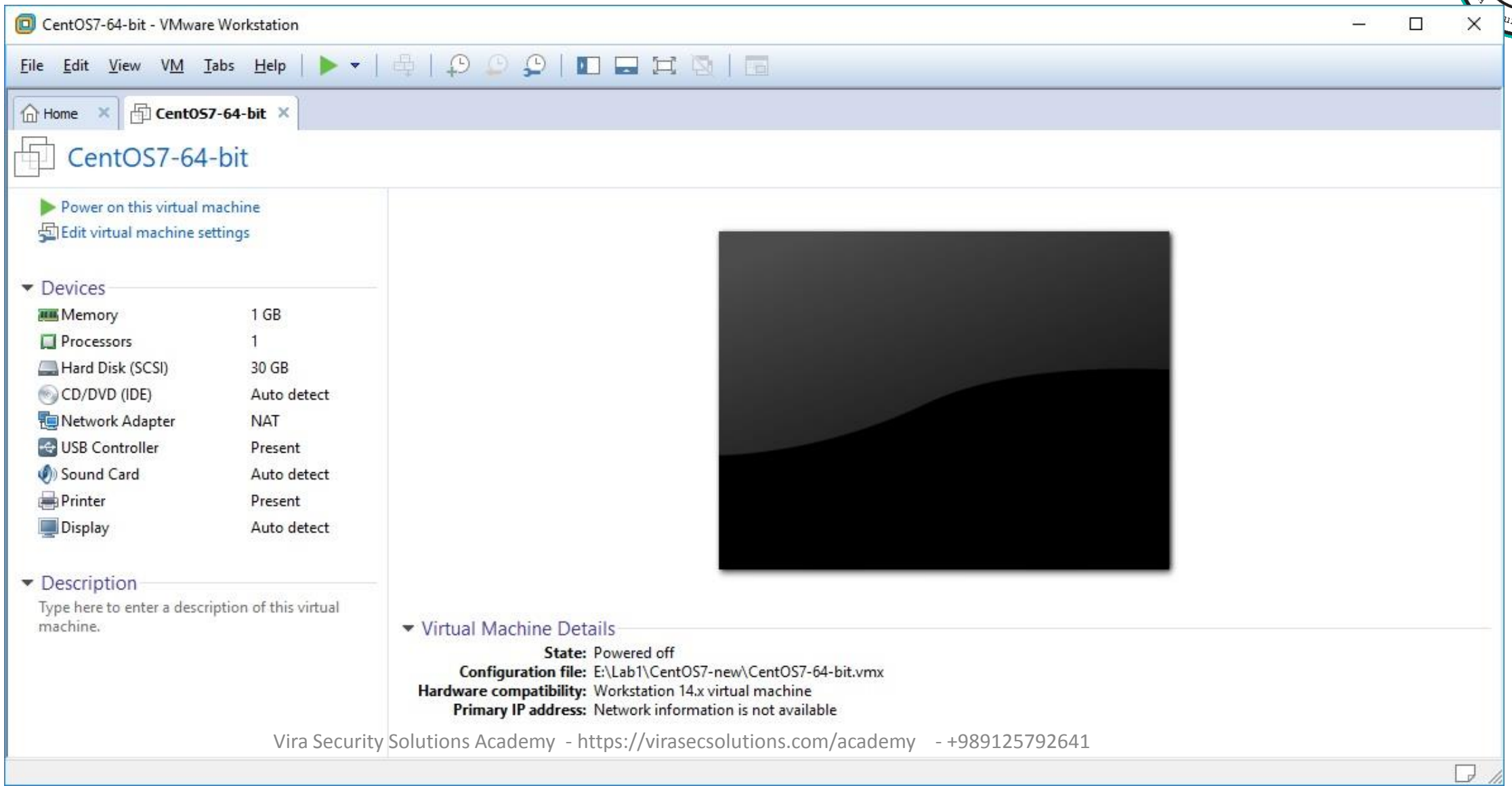
Install CentOS 7 Step by Step



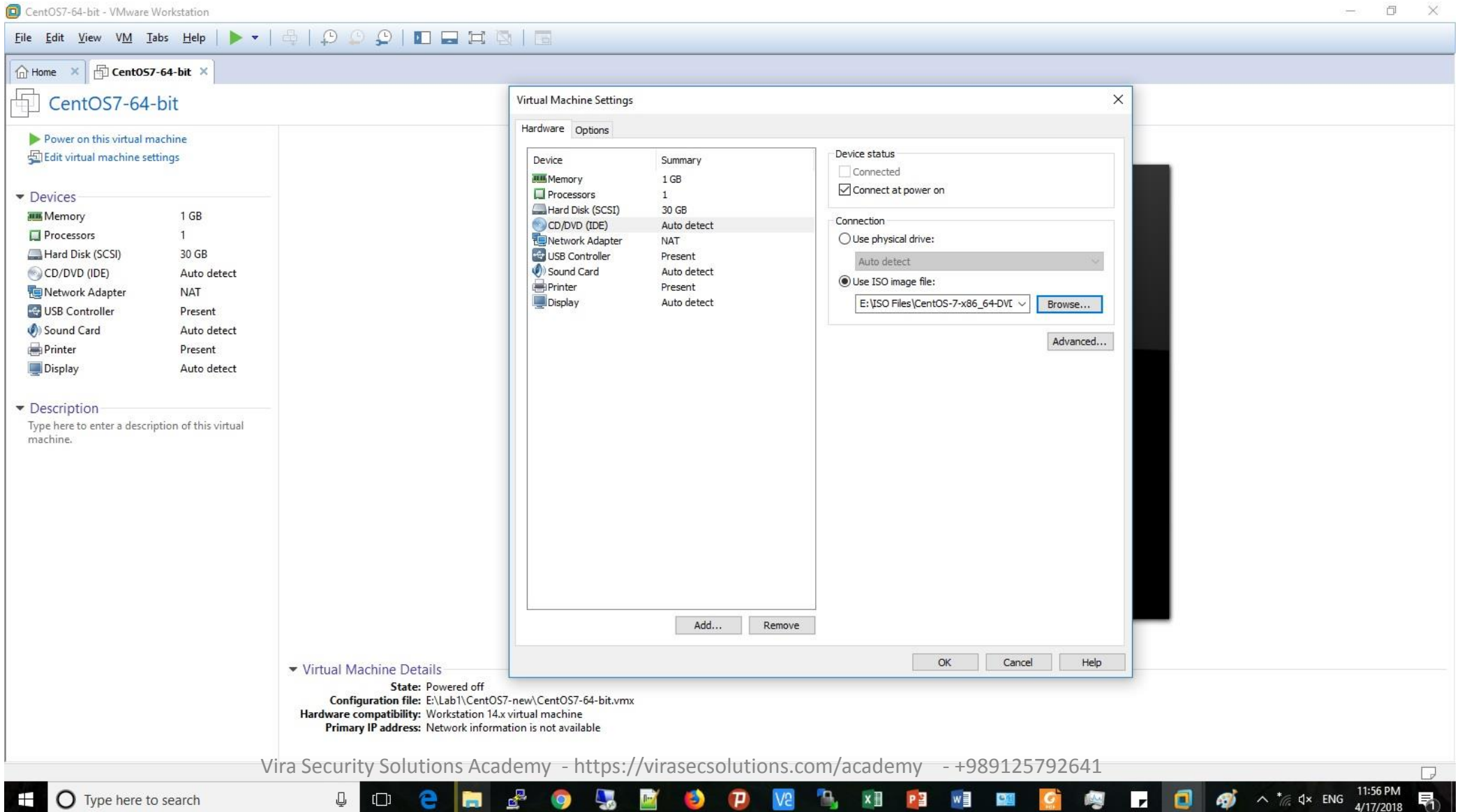
Install CentOS 7 Step by Step

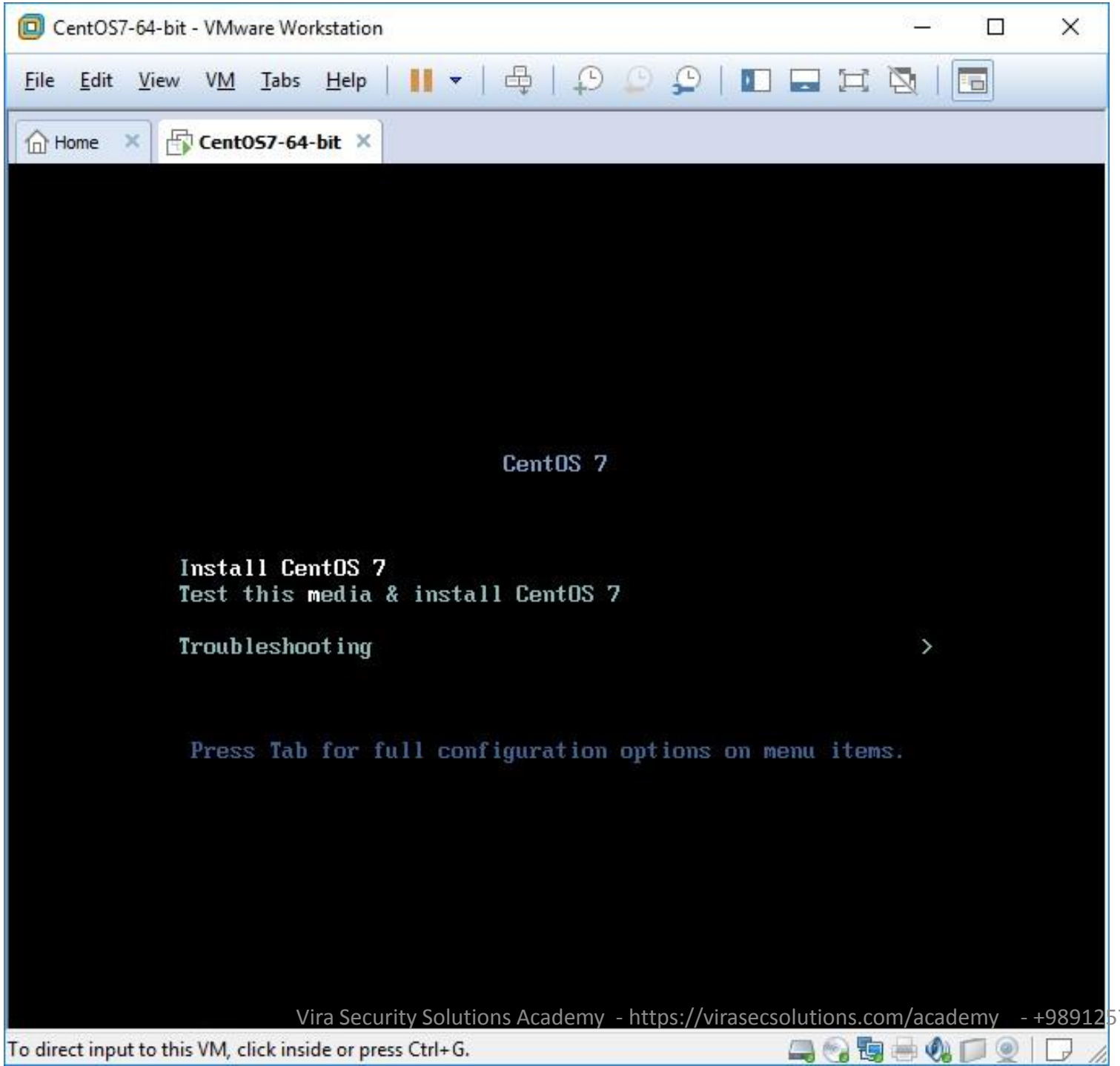


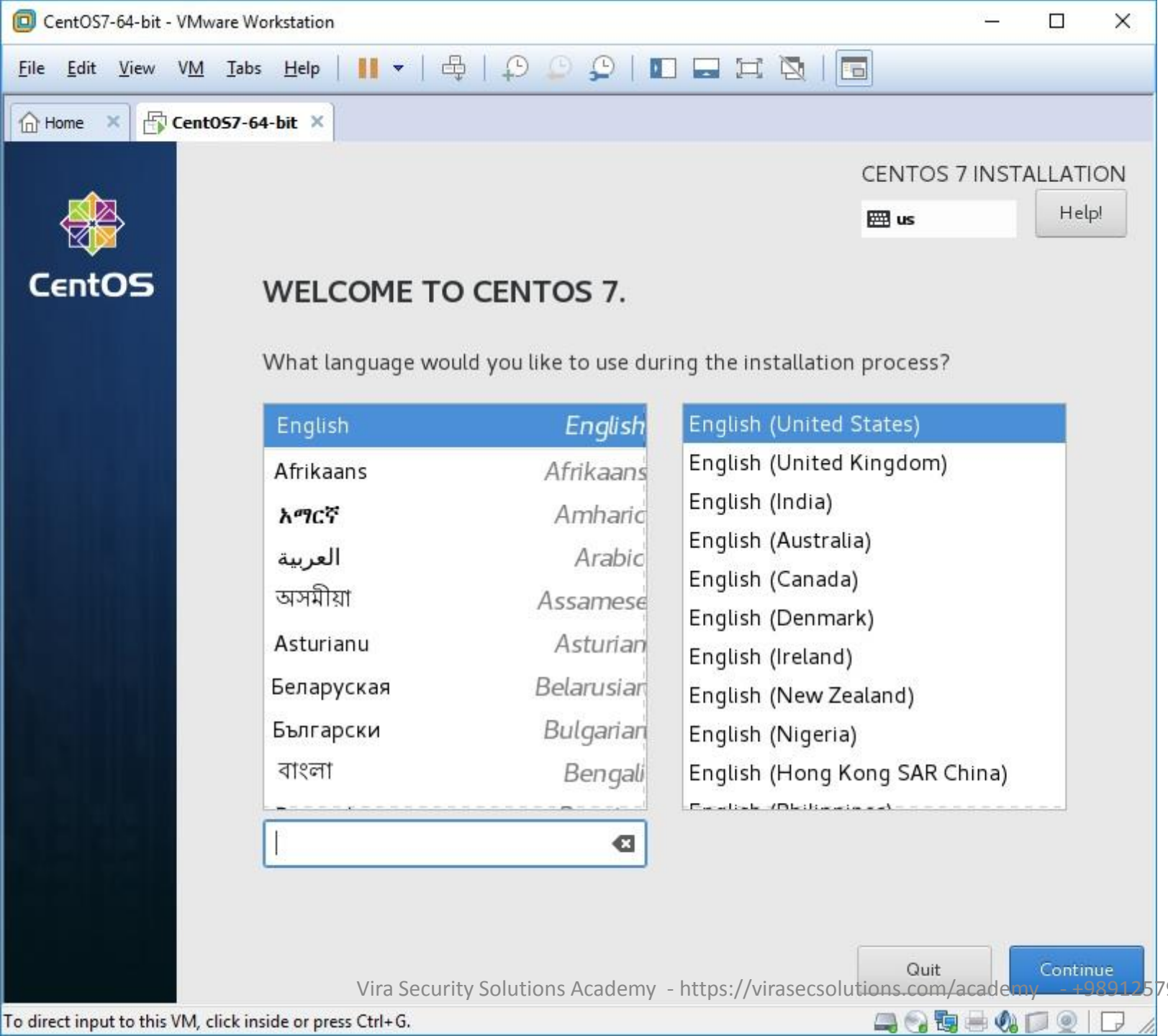
Install CentOS 7 Step by Step

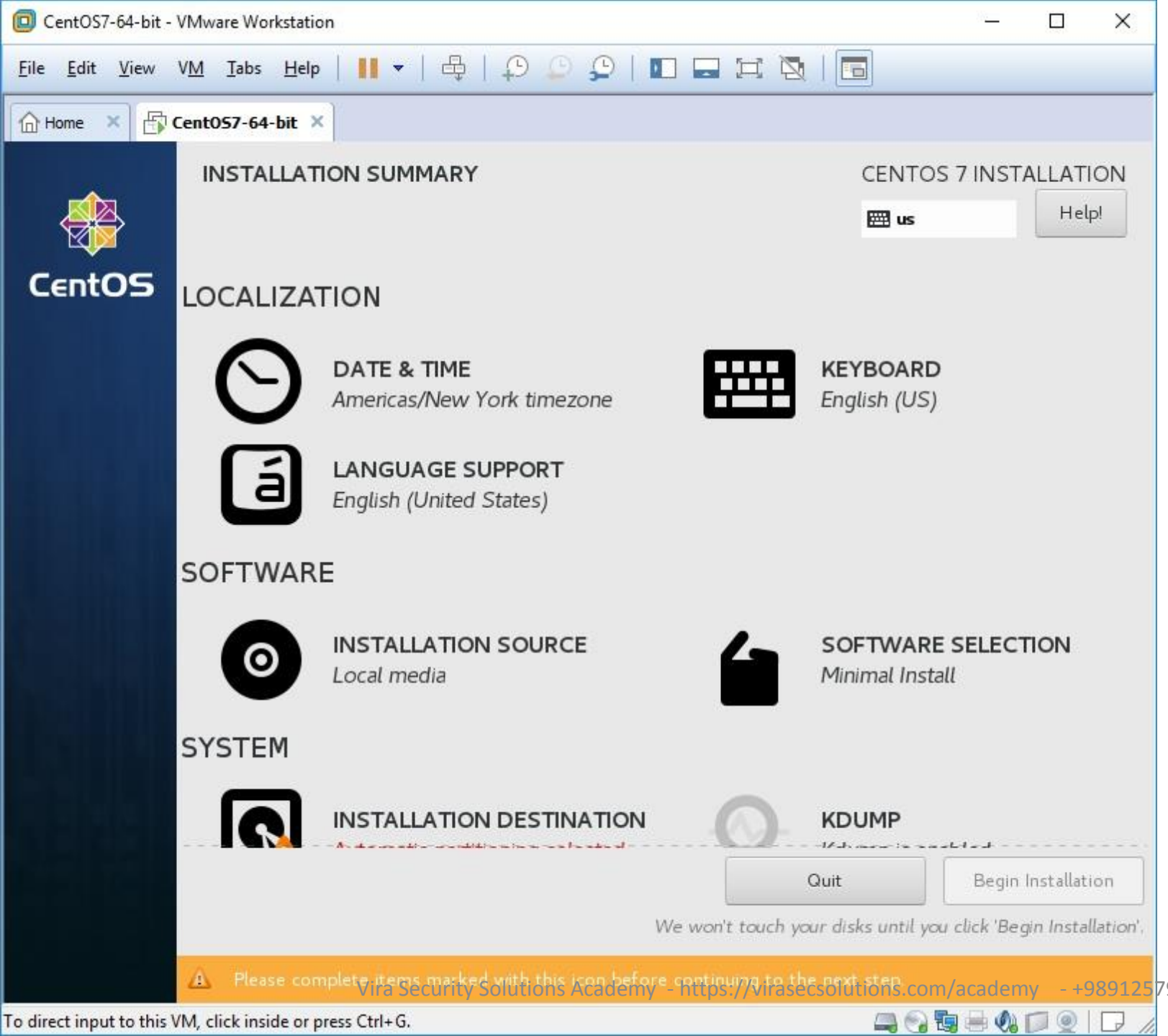


Install CentOS 7 Step by Step




CentOS7-64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
CentOS7-64-bit
CentOS 7
Install CentOS 7
Test this media & install CentOS 7
Troubleshooting
Press Tab for full configuration options on menu items.
To direct input to this VM, click inside or press Ctrl+G.


CentOS7-64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
CentOS7-64-bit
CENTOS 7 INSTALLATION
us
Help!
CentOS
WELCOME TO CENTOS 7.
What language would you like to use during the installation process?
English English
Afrikaans Afrikaans
አማርኛ Amharic
العربية Arabic
অসমীয়া Assamese
Asturianu Asturian
Беларуская Belarusian
Български Bulgarian
বাংলা Bengali
English (United States)
English (United Kingdom)
English (India)
English (Australia)
English (Canada)
English (Denmark)
English (Ireland)
English (New Zealand)
English (Nigeria)
English (Hong Kong SAR China)
Quit
Continue
To direct input to this VM, click inside or press Ctrl+G.


CentOS7-64-bit - VMware Workstation
File Edit View VM Tabs Help
Home
CentOS7-64-bit
INSTALLATION SUMMARY
CENTOS 7 INSTALLATION
us
Help!
CentOS
LOCALIZATION
DATE & TIME
Americas/New York timezone
KEYBOARD
English (US)
LANGUAGE SUPPORT
English (United States)
SOFTWARE
INSTALLATION SOURCE
Local media
SOFTWARE SELECTION
Minimal Install
SYSTEM
INSTALLATION DESTINATION
KDUMP
Quit
Begin Installation
We won't touch your disks until you click 'Begin Installation'.
Please complete items marked with this icon before continuing to the next step
To direct input to this VM, click inside or press Ctrl+G.

VSF_CentOS-7_64

- Power on this virtual machine
- Edit virtual machine settings
- Upgrade this virtual machine

Devices

Memory	1 GB
Processors	1
Hard Disk (SCSI)	100 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Custom (VMnet0)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Description

Type here to enter a description of this virtual machine.

Virtual Machine Details

State: Powered off
Snapshot: Snapshot 2
Configuration file: E:\Vira_LAB\VSF_CentOS-7_64\VSF_CentOS-7_64.vmx
Hardware compatibility: Workstation 11.x virtual machine
Primary IP address: Network information is not available

Prepare and configuration Linux system

Network Configuration

systemctl restart network

SSH Service Configuration

systemctl restart sshd

Survey and check graphical user interface

User and Group Management

Since Linux is a multi-user operating system, several people may be logged in and actively working on a given machine at the same time. Security-wise, it is never a good idea to allow users to share the credentials of the same account. In fact, best practices dictate the use of as many user accounts as people needing access to the machine.

User and Group Management

Normal users

a user in your Linux system that has limit access

Superuser (root)

This is a powerful user with all the unlimited privileges in your system. This user can do anything, be careful with their user password and instructions.

System users

created by the software's or applications, e.g.: Apache it will create user apache.

User and Group Management

root user UID will be 0

System user UID will be “1 – 499”

Normal Users UID will be “500 – 60000”

User and Group Management

Superuser permissions can be gained either by changing to the root user with the **su** command or using **sudo**.

The latter approach is used by default in Ubuntu and derivatives, and is preferred over the former in other distributions as well.

User and Group Management

Adding a New Regular Account

To begin, let's create a new user named vira using Ubuntu and CentOS as representative distributions.
Note: you must be a Superuser for adding a new user

```
#  adduser   vira
```

Set password for your user:

```
# passwd   vira
```

User and Group Management

Adding a new regular group

To begin, let's create a new group named students:

```
# addgroup students
```

User and Group Management

Assign User and Group for a file

Syntax :

```
#  chown user:group filename
```

Sample :

```
# chown vira:student filename
```

User and Group Management

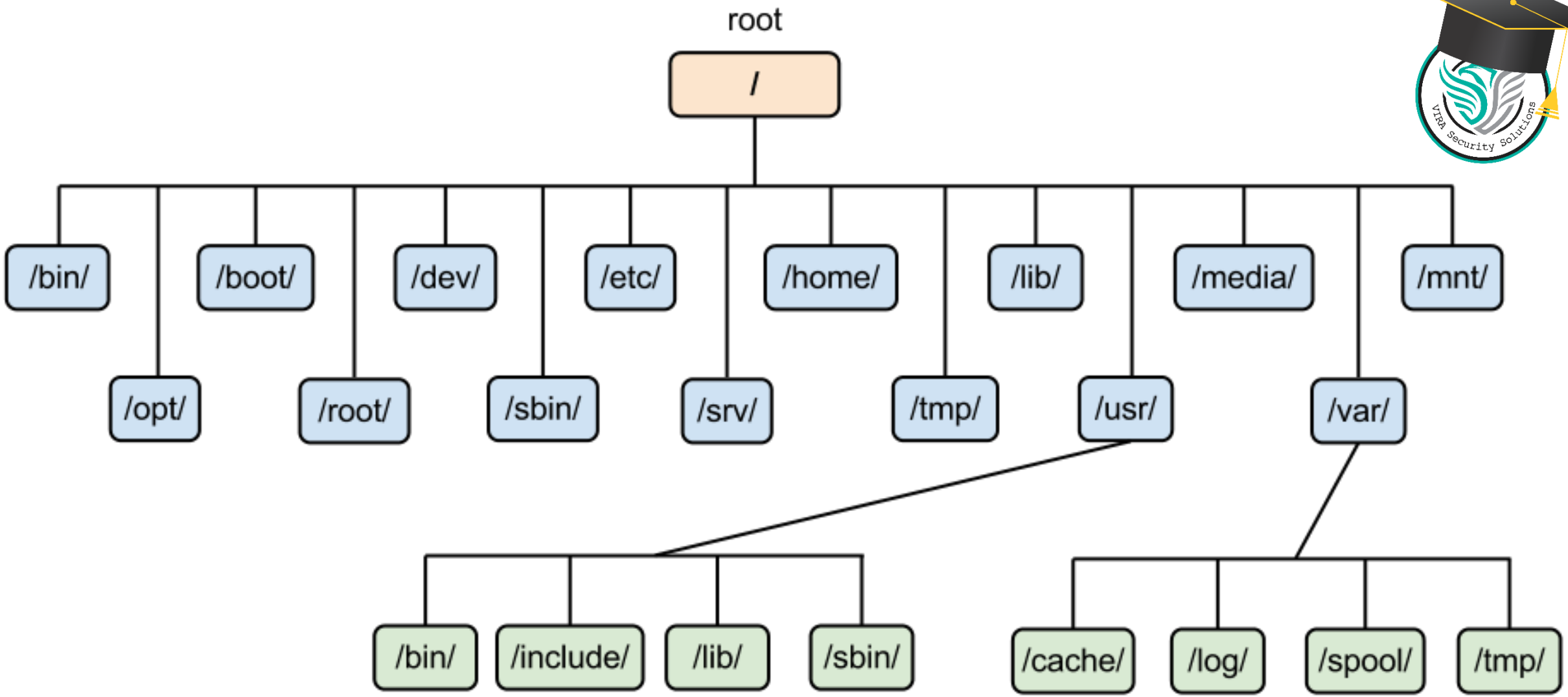
When a new user account is added to the system, the following operations are performed.
1. His/her home directory is created (/home/vira by default).
2. The following hidden files are copied into the user's home directory, and will be used to provide environment variables for his/her user session.

.bash_logout
.bash_profile
.bashrc

File System

The Unix file system looks like an inverted tree structure.

You start with the root directory, denoted by /, at the top and work down through sub-directories underneath it.


root
/
/bin/
/boot/
/dev/
/etc/
/home/
/lib/
/media/
/mnt/
/opt/
/root/
/sbin/
/srv/
/tmp/
/usr/
/var/
/bin/
/include/
/lib/
/sbin/
/cache/
/log/
/spool/
/tmp/


Root Directory of the Whole File System
/
/bin
User Binaries
/boot
Boot Loader Files
/dev
Device Files
/etc
System Configuration Files
/home
User Home Directories
/lib
Libraries and Kernel Modules
/media
Removeable Media Mount Point
/mnt
Mount Point For Temporary Mounted File Systems
/opt
Add-On Application Software Packages
/sbin
System Binaries
/srv
Data For Services
/tmp
Temporary Files
/usr
User Utilities And Applications
/var
Variable Files
/root
Home Directory for the Root User
/proc
Virtual File System

File System

Each node is either a file or a directory of files, where the latter can contain other files and directories.

You specify a file or directory by its path name, either the full, or absolute, path name or the one relative to a location.

The full path name starts with the root, /, and follows the branches of the file system, each separated by /, until you reach the desired file, e.g.:

/home/gerami/test

File System

A relative path name specifies the path relative to another, usually the current working directory that you are at. Two special directories :

. the current directory

.. the parent of the current directory

Structure of Standard Directories in Unix/Linux

- **/ The ancestor of all directories on the system; all other directories are subdirectories of this directory, either directly or through other subdirectories.**
- **/bin Essential tools and other programs (or binaries).**
- **/dev Files representing the system's various hardware devices. For example, you use the file `/dev/cdrom' to access the CD–ROM drive.**
- **/etc Miscellaneous system configuration files, startup files, etc.**

Structure of Standard Directories in Unix/Linux

- **/home** The home directories for all of the system's users.
- **/lib** Essential system library files used by tools in `/bin'.
- **/proc** Files that give information about current system processes.
- **/root** The superuser's home directory, whose username is root. (In the past, the home directory for the superuser was simply `/'; later, `/root' was adopted for this purpose to reduce clutter in `/'.)
- **/sbin** Essential system administrator tools, or system binaries.
- **/tmp** Temporary files.
- **/usr** Subdirectories with files related to user tools and applications

Linux / UNIX: Rules For Naming File And Directory Names

All file names are case sensitive. So filename virasec.txt ViraSec.txt VIRASEC.txt all are three different files.

You can use upper and lowercase letters, numbers, “.” (dot), and “_” (underscore) symbols.

Most modern Linux and UNIX limit filename to 255 characters (255 bytes). However, some older version of UNIX system limits filenames to 14 characters only.

A filename must be unique inside its directory. For example, inside /home/gerami directory you cannot create a **demo file** and **demo directory** name.

Linux / UNIX: Rules For Naming File And Directory Names

Reserved Characters And Words

Avoid using the following characters from appearing in file names:

/
>
<
|
:
&

Please note that Linux and UNIX allows white spaces, <, >, |, \, :, (,), &, ;, as well as wildcards such as ? and *, to be quoted using \ symbol.

Escaped :

Managing Users & Groups

Adding User Accounts

To add a new user account, you can run either of the following two commands as root.

adduser [new_account]

useradd [new_account]

#adduser gerami

Managing Users & Groups

When a new user account is added to the system, the following operations are performed.

1. His/her home directory is created (/home/gerami by default).

2. The following hidden files are copied into the user's home directory, and will be used to provide environment variables for his/her user session.

.bash_logout

.bash_profile

.bashrc

3. A mail spool is created for the user at /var/spool/mail/gerami.

4. A group is created and given the same name as the new user account.

Managing Users & Groups

Enter password for user you create:

passwd username => passwd gerami

Enter Old password and then Enter your new password

If you are root user, you need to enter your new password only.

Managing Users & Groups

You can access to your groups list and name in following file:

/etc/group

Use the combined -aG, or --append --groups options, followed by a comma separated list of groups.

```
usermod --append --groups students,vira gerami
usermod -a -G students,vira gerami
```

Check the groups:

```
groups
```

Managing Users & Groups

Deleting user accounts

userdel --remove [username]

Deleting a group

groupdel [group_name]

Managing Users & Groups

There are four main user administration files

- **/etc/passwd** – Keeps the user account and password information. This file holds the majority of information about accounts on the Unix system.
- **/etc/shadow** – Holds the encrypted password of the corresponding account. Not all the systems support this file.
- **/etc/group** – This file contains the group information for each account.
- **/etc/gshadow** – This file contains secure group account information.

Managing Users & Groups

There are four main user administration files

- **/etc/passwd** – Keeps the user account and password information. This file holds the majority of information about accounts on the Unix system.
- **/etc/shadow** – Holds the encrypted password of the corresponding account. Not all the systems support this file.
- **/etc/group** – This file contains the group information for each account.
- **/etc/gshadow** – This file contains secure group account information.

Managing Users & Groups

Sr.No.	Command & Description
1	**useradd** Adds accounts to the system
2	**usermod** Modifies account attributes
3	**userdel** Deletes accounts from the system
4	**groupadd** Adds groups to the system
5	**groupmod** Modifies group attributes
6	**groupdel** Removes groups from the system